

'13 JUL 24 19:24

SENATE
Senate Bill No. 1091

REC'D

BY: 

Introduced by: Senator Paolo Benigno "Bam" A. Aquino IV

EXPLANATORY NOTE

In today's increasingly wired and interconnected society, Internet connectivity has become more than just a luxury, and certainly more than just a tool for the educated and the elite. It is essential in the provision of basic government and private sector services, in sharing educational information to our students, in the conduct of everyday business, and even in gathering real-time, life-saving information.

For instance, we saw during the onslaught of Ondoy and Pepeng in 2009—and in the natural disasters following these—how the Philippine online community worked together from behind computers and mobile phones to send crucial information about flooded areas, missing persons, areas in need of immediate rescue and relief, fundraising efforts, and many others. In an age of climate change and harsher weather conditions, being connected and "in the know" could spell the difference between life and death.

Internet-enabled platforms and services have likewise given birth to new industries, which in turn have opened up hundreds of thousands of jobs for ordinary Filipinos. The Business Process Outsourcing (BPO) and Knowledge Process Outsourcing (KPO) industries, for example, would not be able to survive without the infrastructure for secure Internet connectivity. Likewise, a growing number of freelancers, start-up entrepreneurs, online marketers, and the like have been able to find gainful employment and livelihood thanks to Internet technology. Even loan services and fundraising efforts have been powered by the Internet, making it more accessible for groups with great ideas to get the funding support that they need.

Beyond these, the Internet and social media have become integral to ensuring transparency, accountability, and good governance not only in the Philippines but also in many corners of the world. For many, the Internet represents a lifeline to citizen watchdog groups and media organizations that shine the light on truth where it is most needed. Internet-enabled platforms have become complementary tools for democracy, allowing for debate and discourse, the free exchange of ideas, and open access to public servants. Moreover, developments in the social media space have made it possible for government to engage with its constituents on a one-to-one level, bringing government service directly in the hands of hands of the people.

It is for these reasons, and many more, that we seek to support the **Magna Carta for Philippine Internet Freedom (MCPIF)**, in order to push for universal access to the Internet, the freedom and the ability to access public information online, freedom of speech, the right to create without fear of intellectual property infringement, and many other rights that are afforded Filipinos as citizens of a democratic republic.

Specifically, we wish to push for a provision that makes **free WIFI** (also: wireless local areas network or WLAN) access mandatory for designated public spaces within local government units (LGUs), such as city or municipal halls, and the like. Public WIFI access will ensure that the Internet and other digital or social media platforms may be used by LGUs and their citizens for such functions as: the provision of basic government services (e.g., business registration, the accessing of government data online, etc.); real-time monitoring and disaster response coordination during times of natural and man-made disasters; data gathering, transmission, and monitoring during local elections; online training and capacity-building, and many others.

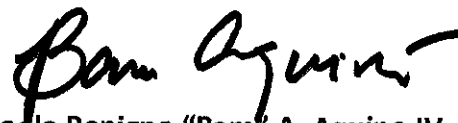
Just as the MCPIF upholds many of our civil liberties, it likewise protects citizens' privacy online and also outlines the limitations of Internet use. For instance, as defined in Part I Section 2 (f):

“The Internet has the potential to become a theater of war, and that ICT can be developed into weapons of mass destruction; thus, consistent with the national interest and the Constitution, the State shall pursue a policy of no first use of cyberweapons against foreign nations, and shall implement plans, policies, programs, measures, and mechanisms to provide cyberdefense of Philippine Internet and ICT infrastructure resources;”

The MCPIF also tackles such issues as hacking, Internet libel, hate speech, child pornography, cyber crime, human trafficking, and a host of other issues.

Finally, to exercise jurisdiction over the Philippines' ICT sector and the mapping out of the country's ICT roadmap and systems, the MCPIF proposes the establishment of a Department of Information and Communications Technology (DICT), which, as defined here, “shall be the primary policy, planning, coordinating, implementing, regulating and administrative entity of the executive branch of the government that will plan, promote and help develop the country's ICT sector and ensure reliable and cost-efficient communications facilities, other multimedia infrastructure and services.”

The world is changing at breakneck speed, and we believe that a piece of legislature such as the Magna Carta for Philippine Internet Freedom will enable us to manage the winds of change.

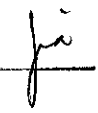


Senator Paolo Benigno “Bam” A. Aquino IV

SIXTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
First Regular Session)

'13 JUL 24 A9:24

SENATE
S. B. No. 1091

RECEIVED BY: 

Introduced by: Senator Paolo Benigno "Bam" A. Aquino IV

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

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

Part I. General Provisions.

1 *Section 1. Short Title.* – This Act shall be known as “The Magna Carta for Philippine Internet
2 Freedom of 2013.”

3
4 *Section 2. Declaration of Policy.* –

5
6 (a) The State affirms that all the rights, guarantees, and privileges provided by the Bill of
7 Rights and the Constitution, as well as those established under general principles of
8 international law and under treaties and conventions to which the Philippines is a signatory,
9 shall govern in the use, development, innovation, and invention of information and
10 communications technology (ICT) and the Internet by the Filipino people.

11
12 (b) The State affirms its commitment to the people and to all nations that, in the crafting
13 of laws and regulations governing the use of the Internet and of ICT, these shall be subject to
14 the parameters set forth under the Constitution.

15
16 (c) The State reaffirms the vital role of communication and information in nation-
17 building, as stated in Article II, Section 24, of the Constitution;

18
19 (d) The growth of the Internet and ICT both depend on and contribute to the growth of
20 the economy, advances in science and technology, and the development of human capital, and
21 encourage democratic discourse and nation-building;

22
23 (e) The public and private sector have a role in the development, invention, and
24 innovation for the Internet and for ICT, through domestic, international, and transnational

1 efforts; thus, the State shall encourage development, invention, and innovation through and for
2 the Internet and ICT in cooperation with the private sector, other nations, and international
3 bodies;

4
5 (f) The State recognizes that network bandwidth is a finite resource that is limited by
6 technological advancements and by telecommunications infrastructure and investment; thus,
7 the State shall encourage the development of information and communications technology and
8 infrastructure;

9
10 (g) The Internet and ICT further enable participative governance, transparency, and
11 accountability in government; thus, the State reaffirms its policy of full public disclosure of all
12 its transactions involving public interest and to develop plans, policies, programs, measures,
13 and mechanisms using the Internet and ICT in the implementation of its policy of full public
14 disclosure;

15
16 (h) The State recognizes the basic right of all persons to create, access, utilize and share
17 information and knowledge through ICT, and shall promote the Internet and ICT as a means for
18 all to achieve their full potential, promote their sustainable development, and improve their
19 quality of life;

20
21 (i) The growth of the Internet and ICT affect peace and order and the enforcement of
22 law within the national territory and across other nations; thus, the State reaffirms its policy of
23 cooperation and amity with all nations, and its adoption of generally accepted principles of
24 international law as part of the law of the land, in the pursuit of peace and order and in the
25 enforcement of law;

26
27 (j) The Internet has the potential to become a theater of war, and that ICT can be
28 developed into weapons of mass destruction; thus, consistent with the national interest and
29 the Constitution, the State shall pursue a policy of "no first use" of cyberweapons against
30 foreign nations, and shall implement plans, policies, programs, measures, and mechanisms to
31 provide cyberdefense of Philippine Internet and ICT infrastructure resources; and,

32
33 (k) Art and culture can be created on devices, on networks, and on the Internet; thus,
34 the State shall pursue a policy that promotes the Internet and information and communications
35 technology, and the innovation therein and thereof, as instruments of life, liberty, and the
36 pursuit of happiness.

37
38
39 **Part 2. Definition of Terms.**

40
41 *Section 3. Definition of Terms.* – When possible, definitions shall be adopted from those
42 established by the International Telecommunications Union (ITU), the Internet Engineering Task
43 Force (IETF), the World Wide Web Consortium (WWWC), and the Internet Corporation for
44 Assigned Numbers and Names (ICANN), and other international and transnational agencies
45 governing the development, use, and standardization of information and communications
46 technology and the Internet. For purposes of this Act, the following terms shall mean:

1 (j) Computer – Any device or apparatus which, by electronic, electro-mechanical or
2 magnetic impulse, or by other means, is capable of receiving, recording, transmitting,
3 storing, processing, retrieving, or producing information, data, figures, symbols or other
4 modes of written expression according to mathematical and logical rules or of
5 performing any one or more of those functions.
6

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

11 (l) Configuration – The way a device, computer, computer system, or network is set up.
12

13 (m) Content – Data that can be readily understood by a user immediately upon access,
14 which may include but is not limited to text, pictures, video, or any combination thereof.
15 The word is synonymous to information. Data that is readable and usable only by and
16 between devices, computers, systems or networks, such as traffic data, is not content.
17

18 (n) Control – The use of resources, modification of the configuration, and otherwise
19 exertion of a directing influence on the operation of a device, computer, system, or
20 network.
21

22 (o) Critical infrastructure – The systems and assets, whether physical or virtual, so vital
23 to the Philippines that the incapacity or destruction of such systems and assets would
24 have a debilitating impact on national security, economy, public health or safety, or any
25 combination of those matters.
26

27 (p) Critical network – An information and communications system or network of
28 systems, whether physical or virtual, so vital to the Philippines that the incapacity or
29 destruction of such a network would have a debilitating impact on national security,
30 economy, public health or safety, or any combination of those matters.
31

32 (q) Cryptography – The discipline which embodies principles, means, and methods for
33 the transformation of data in order to hide its information content, prevent its
34 undetected modification and/or prevent its unauthorized use.
35

36 (r) Cyber environment – The environment comprised of users, networks, devices, all
37 software, processes, information in storage or transit, applications, services, and
38 systems that can be connected directly or indirectly to networks or the Internet.
39

40 (s) Cyberattack – An attack by a hostile foreign nation-state or violent non-state actor on
41 Philippine critical infrastructure or networks through or using the Internet or
42 information and communications technology. The term may also be used to mean an
43 assault on system security that derives from an intelligent threat, *i.e.*, an intelligent act
44 that is a deliberate attempt to evade security services and violate the security policy of a
45 system.
46

47 (t) Cybercrime – Any unlawful act punishable by this law or other relevant laws

1 committed through or using the Internet or information and communications
2 technology.

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

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

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

17
18 (x) Cyberspace – A global domain within the information environment consisting of the
19 interdependent network of information systems infrastructures including the Internet,
20 telecommunications networks, computer systems, and embedded processors and
21 controllers, or the virtual space constituted by a computer network with a set of
22 distributed applications and its users.

23
24 (y) Cyberterrorism – A violation of the Human Security Act of 2007 committed through
25 or using the Internet or information and communications technology.

26
27 (z) Cyberwarfare – The damaging, disruptive, saboteurish, or infiltrative actions, or
28 analogous acts of a belligerent nature, by a nation-state or violent non-state actor
29 against the Philippines, its government, or its citizens, with the intent to cause damage
30 and disruption to the people, property, infrastructure, or systems of the Philippines,
31 through or using computers, information and communications technology, networks, or
32 the Internet.

33
34 (aa) Data – The reinterpretable representation of information in a formalized manner
35 suitable for communication, interpretation, or processing, or information represented in
36 a manner suitable for automatic processing.

37
38 (i) Data, private – Any and all data that does not fall under the definition of
39 public data.

40
41 (ii) Data, public – Data which is available to the public without access being
42 restricted by requirements of membership, non-disclosure agreements or similar.

43
44 (iii) Data, traffic – Data that is readable and usable only solely by and between
45 devices, computers, systems or networks, used for purposes of facilitating the transfer
46 of information between devices, computers, systems or networks.

47

1 (a) Access – The ability and means to communicate with or otherwise interact with a
2 device, computer, system or network, to use resources to handle information, to gain
3 knowledge of the information the device, computer, system, or network contains, or to
4 control device or system components and functions.

5
6 (b) Administrator – A person or role with privileged access and control over a network or
7 a multi-user computing environment responsible for the operation and the maintenance
8 of the network or computing environment.

9
10 (i) Network administrator – A person or role responsible for the operation and
11 the maintenance of a network.

12
13 (ii) Systems administrator – A person or role responsible for managing a multi-
14 user computing environment.

15
16
17 (c) Availability – The ability of a device or set of devices to be in a state to perform a
18 required function under given conditions at a given instant of time or over a given time
19 interval, assuming that the required external resources are provided.

20
21 (d) Bandwidth – The capacity of a transmission medium to carry data.

22
23 (e) Bot – A computer program or software installed in a device, computer, computer
24 system, or network capable of performing automated tasks over the Internet, without
25 the knowledge or consent of the user or owner of the device computer, system, or
26 network, with control ceded to a third party, usually malicious. Bot may also refer to the
27 individual device that is infected with such programs or software.

28
29 (i) Botnet – A network of computers infected with bots.

30
31
32 (f) Cache – A temporary storage of recently accessed data or information, which may be
33 stored in the local storage medium of a device or computer, or in the storage media of a
34 network, for purposes of speeding up subsequent retrievals of data or information from
35 the Internet or networks.

36
37 (g) Chief Information Officer (CIO) – A third-ranking career executive in charge of the
38 information and communications technology/information technology/management
39 information systems (ICT/IT/MIS) office in a department, bureau or government-owned
40 or -controlled corporation/government financial institution, including legislative, judicial
41 and constitutional offices.

42
43 (h) Code – The symbolic arrangement of data or instructions in a computer program or a
44 set of such instructions.

45
46 (i) Component – Any individual part of a device.
47

1
2 (ab) Device – The material element or assembly of such elements intended to perform a
3 required function.
4

5 (ac) 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

8 (ad) Encryption – An encoding scheme that produces meaningless information to all
9 observers except those with the decryption key made for the purpose.
10

11 (ae) End user license agreement – The legal agreement between two parties, one of
12 which is the user, that stipulates the terms of usage of a device, software, or service.
13

14 (af) Equipment – A single apparatus or set of devices or apparatuses, or the set of main
15 devices of an installation, or all devices necessary to perform a specific task.
16

17 (i) Data processing equipment – Equipment used to process data electronically.
18

19 (ii) Network equipment – Equipment used to allow data communication between
20 devices, computers, systems, networks, or the Internet.
21

22 (iii) Storage equipment – Equipment used to store data in an electronic form,
23 and allow the retrieval of data by electronic means.
24

25
26 (ad) Executable – The ability of a code, script, software, or computer program to be run
27 from start to finish in a device or computer, and providing a desired result.
28

29 (ae) Free and open-source software – Liberally licensed software whose license grants
30 users the right to use, copy, study, change, and improve its design through the
31 availability of its source code.
32

33 (af) Hardened – The state of reduced vulnerability to unauthorized access or control or
34 to malicious attacks of a device, computer, network, or information and
35 communications technology infrastructure.
36

37 (ag) Hardware – The collection of physical elements that comprise a device, equipment,
38 computer, system, or network.
39

40 (ah) High-speed connection – A service that provides data connection to networks and
41 the Internet that has data rates faster than what is generally available to the general
42 public.
43

44 (ai) High-volume connection – A service that provides data connection to the networks
45 and the Internet that allows volumes of uploadable and/or downloadable data larger
46 than what is generally available to the general public.
47

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

6
7 (i) Private information – Refers to any of these three classes of information:

8
9 (1) any information whether recorded in a material form or not, from
10 which the identity of an individual is apparent or can be reasonably and directly
11 ascertained by the entity holding the information, or when put together with
12 other information would directly and certainly identify an individual;

13
14 (2) Any and all forms of data which under the Rules of Court and other
15 pertinent laws constitute privileged communication; and,

16
17 (3) any information whose access requires the grant of privileges by a
18 duly-constituted authority, which may include but is not limited to a systems or
19 network administrator.

20
21
22 (ii) Sensitive private information – Refers to personal information:

23
24 (1) About an individual's race, ethnic origin, marital status, age, color, and
25 religious, philosophical or political affiliations;

26
27 (2) About an individual's health, education, genetic or sexual life of a
28 person, or to any proceeding for any offense committed or alleged to have been
29 committed by such person, the disposal of such proceedings, or the sentence of
30 any court in such proceedings;

31
32 (3) Issued by government agencies peculiar to an individual which
33 includes, but not limited to, social security numbers, previous or current health
34 records, licenses or its denials, suspension or revocation, and tax returns; and

35
36 (4) Specifically established by an executive order or an act of Congress to
37 be kept classified.

38
39
40 (iii) Public information – Any information that is not restricted by virtue of the
41 preceding definitions and can be readily accessed by any interested member of the
42 public.

43
44
45 (ak) Information and communications technology – The integration of real-time
46 communication services, non-real-time communication services, and
47 telecommunications, computers, software, hardware, storage, and devices, which

1 enable users to access, store, transmit, and manipulate information.

2
3 (al) Internet – The global system of interconnected computer networks linked by various
4 telecommunications technologies and that uses the standard Internet protocol suite.

5
6 (am) Medium – A material used for specific purposes.

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

12
13 (ii) Transmission medium – The physical material through which a data
14 communication signal is transmitted, which includes but is not limited to twisted-pair
15 copper wire, coaxial cable, optical fiber, and air.

16
17
18 (an) Network – A collection of computers, devices, equipment, and other hardware
19 interconnected by communication channels that allow sharing of resources and
20 information.

21
22 (i) Open network – A network, such as the Internet, which allows any entity or
23 device to interconnect with freely at any time and become a user or part of the
24 network, provided the entity or device uses the same or compatible communications
25 protocols, and which allows any user to cease interconnectivity with freely at any time,
26 provided the user does so in a manner that does not compromise the security protocols
27 of the open network or of other users.

28
29 (ii) Private network – A network which is operationally private by nature and not
30 universally accessible by the general public.

31
32 (iii) Public network - A network which provides services to the general public.

33
34
35 (ao) Offline – The state of being disconnected from the Internet or networks.

36
37 (ap) Online – The state of being connected to the Internet or a network.

38
39 (aq) Ownership – Ownership is defined by the Civil Code.

40
41 (i) Privately-owned – Ownership as provided for by the Civil Code of the
42 Philippines by a natural person or a juridical person under Article 44 paragraph (3) of the
43 Civil Code.

44
45 (ii) Publicly-owned – Ownership as provided for by the Civil Code of the
46 Philippines by a juridical person under Article 44 paragraphs (1) and (2) of the
47 Civil Code.

1
2
3 (ar) Physical plant – The building, structure, and infrastructure necessary to support and
4 maintain a facility.

5
6 (as) Platform – The hardware architecture and/ or software framework, including
7 application frameworks, whose combination allows a user to run software.

8
9 (at) Privacy – May refer to any of these definitions, or a combination of these
10 definitions:

11
12 (i) the right guaranteed and protected by the Constitution;

13
14 (ii) the right of individuals to control or influence what personal information
15 related to them may be collected, managed, retained, accessed, and used or
16 distributed;

17
18 (iii) the protection of personally identifiable information; and,

19
20 (iv) a way to ensure that information is not disclosed to anyone other than the
21 intended parties (also known as "confidentiality").

22
23
24 (au) Privilege – A right that, when granted to an entity, permits the entity to perform an
25 action.

26
27 (i) Privileged access – The completely unrestricted access of a user to the
28 resources of a device, computer, system, or network.

29
30 (ii) Privileged control – The completely unrestricted ability of a user to use the
31 resources, modify the configuration, and otherwise exert a directing influence on the
32 operation of a device, computer, system, or network.

33
34
35 (av) Processing – The act of performing functions or activities on data or information.

36
37 (i) Processing (Data Privacy Act) – Any operation or any set of operations
38 performed upon personal information including, but not limited to, the collection,
39 recording, organization, storage, updating or modification, retrieval, consultation, use,
40 consolidation, blocking, erasure or destruction of data. (RA 10173)

41
42 (ii) Data processing – Any process to enter data and summarize, analyze or
43 otherwise convert data into usable information.

44
45 (iii) Information processing – The transformation of information in one form to
46 information in another form through an algorithmic process.

1
2 (aw) Protocol – A defined set of procedures adopted to ensure communication, or a set
3 of rules for data transmission in a system interlinking several participants.
4

5 (ax) Publication – The act of making works available to the public by wire or wireless
6 means in such a way that interested members of the public may access these works
7 from a place and time individually chosen by them.
8

9 (ay) Script – A computer program or sequence of instructions that is interpreted or
10 carried out by another computer program instead of directly by a computer, device, or
11 equipment.
12

13 (az) Security – The ability to prevent fraud as well as the protection of information
14 availability, integrity and confidentiality.
15

16 (i) Security, behavioral – The use of laws, regulations, policies, procedures,
17 instructions and the like to influence or restrict behavior for purposes of maintaining
18 security.
19

20 (ii) Security, electronic – The use of computer programs, software, code, scripts,
21 devices, or equipment for purposes of maintaining security.
22

23 (iii) Security, physical – The use of locks, gates, security guards, and other
24 analogous means, for purposes of maintaining security.
25

26
27 (ba) Service – A set of functions offered to a user by another person or by an
28 organization.
29

30 (bb) Service quality – The collective effect of service performance which determines the
31 degree of satisfaction of a user of the service.
32

33 (bc) Software – The set of programs, procedures, algorithms and its documentation
34 concerned with the operation of a data processing system, computer, device, or
35 equipment.
36

37 (bd) Software application – Software designed to help a user perform a specific task or
38 set of tasks.
39

40 (be) State - The Republic of the Philippines, any of its political subdivisions, departments
41 and agencies, including but not limited to government owned or controlled corporations
42 or government corporate entities.
43

44 (bf) Telecommunications – A service or system of interconnected entities providing the
45 ability to exchange and interchange data between points or from a point to multiple
46 points.
47

1 (bg) Universal access - The provision of adequate and reliable facilities at reasonable
2 charges in all areas within Philippine jurisdiction, as far as is technologically sound and
3 practicable and subject only to technological and reasonable economic limitations,
4 without any discrimination on the basis of gender, sexual orientation, religious belief or
5 affiliation, political belief or affiliation, ethnic or regional affiliation, citizenship, or
6 nationality.

7
8 (bh) Upload – The transfer of data or information to the Internet or a network from a
9 device or computer, initiated by the user.

10
11 (bi) Uptime – The time a device, equipment, computer, or network can be left
12 unattended without suffering failure, or needing to be undergo administrative or
13 maintenance purposes.

14
15 (bj) User – Any person, whether natural or juridical, or any entity that makes use of a
16 part or whole of the resources of a device, equipment, computer, system, network,
17 software, software application, code, or script.

18
19 (bk) Virus – Any computer program, code, or script that implements unauthorized
20 and/or undesirable changes to a device, computer, equipment, system, or network. For
21 purposes of this Act, the term may be used synonymously with malware, spyware,
22 worms, trojans, and the like.

23 24 25 **Part 3. Internet Rights and Freedoms**

26 27 *Section 4. Right to freedom of speech and expression on the Internet. –*

28
29 (a) The State shall, within its jurisdiction:

30
31 (i) Protect and promote the freedom of speech and expression on the Internet;

32
33 (ii) Protect the right of the people to petition the government via the Internet for
34 redress of grievances;

35
36 (iii) Protect the right of any person to publish material on or upload information
37 to the Internet; and,

38
39 (iv) Not promote censorship or the restriction of the viewing of any content on
40 the Internet, until after the issuance of an appropriate Order pursuant to the provisions
41 of this Section

42
43
44 (b) A person's right to publish content on the Internet, or to remove one's own
45 published content or uploaded data, is recognized as integral to the constitutional right to free
46 expression and shall not be subject to any licensing requirement from the State.

47

1 (c) Any State action that constitutes prior restraint or subsequent punishment in
2 relation to one's Internet's rights shall be authorized only upon a judicial order issued in
3 conformity with the procedure provided under Section 5 of this Act. Provided, that
4 notwithstanding Section 5, any such judicial order issued upon motion of the Republic of the
5 Philippines, any of its political subdivisions or agencies including government-owned or
6 controlled corporations, shall be issued only upon the following grounds:

7
8 (i) the nature of the material or information subject of the Order creates a clear
9 and present danger of a substantive evil that the state has a right or duty to prevent;

10
11 (ii) the material or information subject of the Order is not protected expression
12 under the standards of the community or the audience toward which the material or
13 information is directed; and

14
15 (iii) the publication of the material or the uploading of the information subject of
16 the Order will constitute a criminal act punishable by laws enumerated in Section 5 of
17 this Act.

18
19
20 (d) No person shall be compelled to remove published content or uploaded data from
21 the Internet that is beyond the said person's capacity to remove. The party seeking to compel
22 the removal of the content or data has the burden to prove that the person being compelled
23 has the capacity to remove from the Internet the specific content or data. For purposes of this
24 section, content or data retained in web archives or mirror sites are presumed to be content
25 and data that is beyond the capacity of the person being compelled to remove.

26
27
28 *Section 5. Promotion of universal access to the Internet. –*

29
30 (a) The State shall, within its jurisdiction, protect and promote universal access to the
31 Internet.

32
33 (b) A person's right to unrestricted access to the Internet may, upon discretion of the
34 appropriate Cybercrime Court whose jurisdiction is defined in this Act, be suspended as an
35 accessory penalty upon final conviction for any of the following criminal offenses:

36
37 (i) The felonies of robbery, theft, estafa, falsification, malversation, and
38 usurpation of authority or official functions, as defined in appropriate penal laws,
39 committed by through or using the Internet or information and communications
40 technology;

41
42 (ii) Any criminal offense defined and punishable in the following special penal
43 laws: the Anti-Trafficking in Persons Act of 2003 (RA 9208), the Anti-Graft and Corrupt
44 Practices Act, the Code of Conduct and Ethical Standards for Public Officials and
45 Employees (RA 6713), the Anti-Money Laundering Act of 2001 (RA 9160), the Violence
46 Against Women and Children Act (RA 9262), the Special Protection of Children Against
47 Abuse, Exploitation, and Discrimination Act (RA 7610), the Child and Youth Welfare

1 Code (PD 603), the Anti-Child Pornography Act of 2009 (RA 9775), the Human Security
2 Act of 2007 (RA 9732), or the Data Privacy Act of 2012 (RA 10173), committed through
3 or using the Internet or information and communications technology; or
4

5 (iii) Any criminal offense defined and punishable by this Act.
6
7

8 The right of person accused of any of the above offenses to unrestricted access to the
9 Internet may be suspended or limited by the court of competent jurisdiction pending final
10 judgment upon a showing, following notice and hearing, that there is a strong likelihood that
11 the accused will be able to facilitate the commission of the offense so charged unless such
12 order were issued.
13

14
15 (c) It is presumed that all persons have the right to unrestricted access to the Internet,
16 subject to the parameters established under this Act. Any voluntary restriction or waiver of
17 such right must be established by preponderance of evidence.
18

19 Any final judicial relief that seeks to limit or suspend, in whole or in part, one's right to
20 unrestricted access to the Internet, shall be determined in accordance with the appropriate
21 law, including but not limited to the Civil Code and this Act. Any civil action that seeks as a
22 relief, in part or in whole, the limitation or suspension of a person's right to unrestricted access
23 to the Internet, shall be filed exclusively with the Cybercrime Courts.
24

25 No court shall issue any provisional Order suspending the right to unrestricted access to
26 the Internet of any person without prior notice and hearing, and only upon the grounds for the
27 issuance of a preliminary injunction under the Rules of Court.
28

29 (d) The authority of the State to suspend one's right to unrestricted Internet access is
30 confined solely to the courts of competent jurisdiction and may not be exercised by any
31 government agency, notwithstanding any contrary provisions of law. The right of the State to
32 infringe a person's right to unrestricted Internet access shall be governed by Section 5 of this
33 Act.
34

35 (e) No person or entities offering Internet access for free, for a fee, or as an extra
36 offering separate from the services already being offered, including but not limited to any hotel,
37 restaurant, commercial establishment, school, religious group, organization, or association,
38 shall restrict access to the Internet or any other public communications network from within its
39 private network, or limit the content that may be accessed by its employees, students,
40 members, or guests, without a reasonable ground related to the protection of the person or
41 entity from actual or legal threats, the privacy of others who may be accessing the network, or
42 the privacy or security of the network as provided for in the Data Privacy Act of 2012 (RA
43 10173) and this Act.
44

45 (f) The State, through the Department of Information and Communication Technology in
46 coordination with the Department of Tourism, Commission on Higher Education, and Local
47 Government Units, shall provide free WIFI access in designated public areas. This provision

1 does not prejudice the Department of Information and Communication Technology from
2 partnering with private entities to accomplish this goal.

3 (g) These public areas may include but not be limited to the following:

- 4 1. common areas of local government offices;
- 5 2. train stations;
- 6 3. bus stations;
- 7 4. tourism spots;
- 8 5. National Heritage spots;
- 9 6. public parks; and
- 10 7. designated areas within State Universities and Colleges.

11
12
13 *Section 6. Right to privileged access to and control of devices. –*

14
15 (a) The State shall, within its jurisdiction, protect the right of a person to gain or attain
16 privileged access or control over any device over which the person has property rights.

17
18 (b) Any person involved in the wholesale or retail of devices may install, implant, or
19 otherwise put in a device a component, a configuration, or code that shall restrict the operation
20 of a device; *Provided*, the installation or implantation is for the sole purpose of ensuring the
21 privacy or security of the interconnection or interoperability of the device with public or private
22 networks or Internet or information and communications technology infrastructure; *Provided*
23 *further*, that notice is provided to potential buyers of the device of the presence of the
24 component, configuration, and code; *Provided further*, that the buyer may request the removal
25 or modification of the component, configuration, or code prior to purchase from the seller and
26 shall assume all risks attendant to such removal or modification. Removal or modification of
27 the component, configuration, or code by any person except the seller, manufacturer, or duly
28 authorized representative may be cause for a waiver of the warranty of the device.

29
30 (c) Unless otherwise provided by law, any person who has property rights over any
31 device may, by physical, electronic, or any other means, gain or attain privileged access or
32 control to such device; *Provided*, the gain or attainment of privileged access or control was not
33 intended to circumvent the protection of or cause the actual infringement on intellectual
34 property rights of another person.

35
36
37 *Section 7. Protection of the freedom to innovate and create without permission. –*

38
39 (a) The State shall, within its jurisdiction, protect and promote the freedom to innovate
40 and create without need for permission. No person shall restrict or deny another person the
41 right to develop new information and communications technologies, without due process of
42 law or authority vested by law.

43
44 (b) Subject to such conditions as provided for in the Intellectual Property Code and
45 other relevant laws, no person shall be denied access to new information and communications

1 technologies, nor shall any new information and communications technologies be blocked,
2 censored, suppressed, or otherwise restricted, without due process of law or authority vested
3 by law.

4
5 (c) No person who shall have created, invented, innovated, or otherwise developed a
6 new information and communications technology shall be penalized for the actions of the users
7 of the new information and communications technology.

8
9
10 *Section 8. Right to privacy of data. –*

11
12 (a) The State shall, within its jurisdiction, promote the protection of the privacy of data
13 for all persons.

14
15 (b) Any person shall have the right to employ means such as encryption or cryptography
16 to protect the privacy of the data or networks which such person owns or otherwise possesses
17 real rights over.

18
19 (c) Subject to such conditions as provided for in the Data Privacy Act of 2012 (RA 10173)
20 and other relevant laws, no person shall access the private data of another person.

21
22 (d) The State shall, within its jurisdiction, guarantee a person's right of privacy over his
23 or her data or network rights, and such person's rights employ reasonable means to protect
24 such right of privacy.

25
26 (e) The State is required to ensure the appropriate level of privacy of the data and of the
27 networks maintained by it. Failure to do so shall be penalized by this Act and other relevant
28 laws.

29
30 (f) Except upon a final ruling from the courts, issued in accordance with this act, no
31 person may compel an agency or instrumentality of the State maintaining data or networks to
32 reduce the level of privacy of the data or of the networks.

33
34
35 *Section 9. Right to security of data. –*

36
37 (a) The State shall, within its jurisdiction, promote the protection of the security of data
38 for all persons.

39
40 (b) Any person shall have the right to employ means, whether physical, electronic, or
41 behavioral, to protect the security of his or her data or networks over which the person has
42 ownership.

43
44 (c) No third party shall be granted access to the private data or networks of a person by
45 an Internet service provider, telecommunications entity, or such person providing Internet or
46 data services, except upon a final court order issued in accordance with Section 5 of this Act. It
47 shall be a condition precedent to the filing of such action for access to private data that the

1 person owning such data be first properly notified of such a request by the Internet service
2 provider, telecommunications entity, or such person providing Internet or data services, and
3 that such person has refused to grant the requested access. A person shall not be deemed to
4 have been properly notified unless the person has *acknowledged the notification of the request*
5 for access and has agreed to grant or refuse access.
6

7 (d) No third party granted the right to access the private data or networks of a person by
8 an Internet service provider, telecommunications entity, or other such person providing
9 Internet or data services, shall be given any property rights over the data being accessed, the
10 media where the private data is stored, the equipment through which the network is run or
11 maintained, or the physical plant where the network equipment is housed, beyond the right to
12 access the private data or network, unless otherwise granted such rights by the courts following
13 the appropriate action and final order.
14

15 (e) No person shall be deprived of his or her device, network equipment, or physical
16 plant that may be the subject of an appropriate complaint filed in connection with this Act,
17 except:
18

19 (ii) Upon a lawful warrant issued in connection with the appropriate criminal
20 case by the courts in accordance with the Rules of Court; *Provided*, that there must first
21 be a determination from the courts that the data, information, or contents cannot be
22 separated from the device, network equipment, or physical plant; and,
23

24 (ii) Upon a final decision by the courts issued in accordance with Section 5 of this
25 Act.
26
27

28 (f) The State shall be required to ensure the appropriate level of security of the data and
29 of the networks, whether private or public, that it maintains. Failure to do so shall be penalized
30 by this Act and other relevant laws.
31

32 (h) It shall be unlawful for any person to compel an agency or instrumentality of the
33 State maintaining data or networks to reduce the level of security of the data or of the
34 networks being maintained.
35
36

37 *Section 10. Protection of intellectual property. –*
38

39 (a) The State shall, within its jurisdiction, protect the intellectual property published on
40 the Internet of all persons, in accordance with the Intellectual Property Code of the Philippines
41 (RA 8293), as amended, and other relevant laws.
42

43 (b) It shall be presumed that any content published on the Internet is copyrighted,
44 unless otherwise explicitly provided for by the author, subject to such conditions as provided
45 for in the Intellectual Property Code of the Philippines (RA 8293), as amended, and other
46 relevant laws.
47

1 (c) Subject to the Intellectual Property Code of the Philippines (RA 8293), as amended,
2 and other relevant laws, no Internet service provider, telecommunications entity, or such
3 person providing Internet or data services shall have intellectual property rights over derivative
4 content that is the result of creation, invention, innovation, or modification by a person using
5 the service provided by the Internet service provider, telecommunications entity, or such
6 person providing Internet or data services, unless such content is a derivative work of content
7 already owned by or assigned to the Internet service provider, telecommunications entity, or
8 such person providing Internet or data services acting as a content provider. The exception to
9 the intellectual property rights of the person must be explicitly provided for via an end user
10 license agreement to which both parties have agreed, and the existence of the derivative
11 content must be dependent on the service provided by the Internet service provider,
12 telecommunications entity, or such person providing Internet or data services.

13
14 (d) Notwithstanding existing provisions of law, it shall be presumed that the parents or
15 guardians of a minor shall have provided agreement and shall be bound to the terms of an end
16 user license agreement should the minor in their care signify agreement to the end user license
17 agreement.

18
19 (e) Notwithstanding existing provisions of law, it shall be presumed that any
20 infringement of intellectual property rights by a minor was done with the knowledge and
21 consent of his parents or guardians.

22
23
24 *Section 11. Protection of the Internet as an open network. –*

25
26 (a) The State shall, within its jurisdiction, protect and promote the Internet as an open
27 network.

28
29 (b) No person or entity shall restrict or deny the interconnection or interoperability of a
30 device, an equipment, or a network that is capable of such interconnection or interoperability
31 to the Internet, to other public networks, or to other Internet service providers,
32 telecommunications entities, or other such persons providing Internet or data services, without
33 due process of law or authority vested by law. *Provided*, Customer premises equipment as
34 redefined by this Act, shall not be covered by the requirements under this Section. *Provided*,
35 *further*, The interoperability of a device, an equipment, or a network within a private network
36 may be restricted by the duly authorized system and/or network administrators of the private
37 network, subject to the provisions of the Data Privacy Act of 2012 (RA 10173) and other
38 relevant laws.

39
40
41 *Section 12. Promotion of network neutrality. –* No person or entity shall restrict the flow of data
42 or information on the Internet on the basis of content, nor shall any person institute and
43 employ means or methods to favor the flow of information on the Internet of one class of data
44 or information over another on the basis of content, except:

45
46 (a) if the data or information whose flow is being favored is used to solely to manage
47 the security or service quality of a network, or of an Internet or data service, and;

1
2 (b) the data or information whose flow is being favored cannot be used for any other
3 purpose other than the management of security or service quality of the network.
4

5
6 *Section 13. Promotion of the use of the Internet and information and communications*
7 *technology for purposes of transparency in governance and freedom of information. -*
8

9 (a) The State recognizes that the Internet and ICT can facilitate the dissemination of
10 information and the promotion of transparency in governance. Therefore, subject to the
11 provisions of the Data Privacy Act of 2012 (RA10173) and applicable laws on government
12 information classification, the State shall, within practicable and economically reasonable limits,
13 provide for and maintain a system that shall allow the public to view and download public
14 information on plans, policies, programs, documents, and records of government.
15

16 (b) The State shall publish and make available for download, in readily processed
17 formats, such as plain text documents, comma-separated values spreadsheets, or open
18 standard multimedia data, and its authenticity readily verifiable through a checksum standard
19 as determined by the Internet Engineering Task Force or a similar globally recognized standards
20 organization, the following government public information, in the interest of transparency and
21 good governance:
22

23 (i) Audited financial statements, and budget and expenditure records;
24

25 (ii) Statements of assets, liabilities, and net worth, as prescribed by the Code of
26 Conduct and Ethical Standards of Public Officials and Employees (RA 6713);
27

28 (iii) Performance review results, as prescribed by the Anti-Red Tape Act of 2007
29 (RA 9485) and other relevant laws;
30

31 (iv) Laws, rules, regulations, memorandum circulars and orders, letters of
32 instruction, office orders, and other executive issuances required to be published in the
33 Official Gazette or submitted to the Office of the National Administrative Registrar, or
34 which are essential to the performance of duties of public officials and employees; and,
35

36 (v) Other such information of the State that does not fall within any valid claim of
37 executive privilege.
38

39
40 (c) The State shall ensure that any format used for the files available for download are in
41 common use, platform independent, machine readable, or is based on an underlying open
42 standard, developed by an open community, affirmed and maintained by a standards body and
43 such open standard must be fully documented and publicly available. Such files must be:
44

45 (i) In easily processed formats, such as plain text documents, comma-separated
46 values spreadsheets, and open multimedia formats;
47

1 (ii) Without restrictions that would impede the re-use of that information;
2 *Provided*, that the State shall not be precluded from charging reasonable fees to cover
3 the cost of organizing, maintaining, and publishing such information; *Provided further*,
4 that the State shall not be precluded from publishing the information in supplemental
5 file formats as the public may so request; and,
6

7 (ii) Have their authenticity verifiable through a checksum standard determined
8 by the Internet Engineering Task Force or similar globally reputable organization.
9

10
11 The Bureau of Product Standards of the Department of Trade and Industry shall be
12 responsible for setting the standards for the file formats to be used by the State in the
13 publication of government public information, in accordance with the provisions of this Act.
14

15 (d) The State shall maintain websites or applications with mechanisms to allow for the
16 public to provide feedback, lodge complaints, or report instances of malfeasance or
17 misfeasance. Such mechanisms shall not disallow anonymous feedback, complaints, or reports,
18 and the State shall take appropriate steps to protect persons making feedback, complaints, or
19 reports from retaliation or persecution.
20

21 22 **Part 4. The Department of Information and Communications Technology** 23

24 *Section 14. The Department of Information and Communications Technology. -*
25

26 (a) There is hereby created the Department of Information and Communications
27 Technology, or DICT.
28

29 (b) The DICT shall be the primary policy, planning, coordinating, implementing,
30 regulating and administrative entity of the executive branch of the government that will plan,
31 promote and help develop the country's ICT sector and ensure reliable and cost-efficient
32 communications facilities, other multimedia infrastructure and services. The DICT shall likewise
33 be responsible for overseeing the government's integrated and strategic ICT systems and
34 improving the acquisition, utilization and optimization of government's ICT in order to improve
35 the productivity, efficiency, effectiveness and responsiveness of national and local government
36 programs. The DICT shall furthermore be responsible for ensuring the application of ICT to the
37 various processes and functions of the government.
38

39
40 *Section 15. Strategic objectives of the DICT. -* In fulfilling its mandate, the DICT shall be guided
41 by the following strategic objectives:
42

43 (a) Ensure the provision of a strategic, reliable, cost-efficient and citizen-centric ICT
44 infrastructure, systems and resources as instruments of nation-building and global
45 competitiveness;
46

47 (b) Foster a policy environment that will promote a broader market-led ICT and ICT-

1 enabled services sector, a level playing field, partnership between the public and the private
2 sectors, strategic alliance with foreign investors and balanced investments between high-
3 growth and economically depressed areas;

4
5 (c) Foster and accelerate the convergence of ICT facilities;

6
7 (d) Ensure universal access and high-speed connectivity at fair and reasonable costs;

8
9 (e) Ensure the availability and accessibility of ICT services in areas not adequately served
10 by the private sector;

11
12 (f) Promote and encourage the widespread use, creative development and access to ICT
13 with priority consideration on the requirements for growth of the Philippine ICT industry;

14
15 (g) Promote and assist the development of local and national content application and
16 services in the area of ICT by sourcing or providing funds and construction assistance for ICT-
17 hubs and/or technical support to local-based providers in these endeavors and in the marketing
18 of the local products to the global community;

19
20 (h) Establish a strong and effective regulatory and monitoring system that will ensure
21 investor and consumer protection and welfare, and foster a healthy competitive environment;

22
23 (i) Promote the development of ICT expertise in the country's human capital to enable
24 Filipinos to compete in a fast-evolving information and communication age;

25
26 (j) Ensure the growth of ICT and ICT-enabled industries;

27
28 (k) Protect the rights of individuals to privacy and confidentiality of their personal
29 information;

30
31 (l) Encourage the use of ICT in support of efforts or endeavors for the development and
32 promotion of the country's agriculture, arts and culture, history, education, public health and
33 safety, and other socio-civic purposes;

34
35 (m) Ensure the security of ICT infrastructure and assets of individuals and businesses;
36 and

37
38 (n) Empower, through the use of ICT, the disadvantaged segments of the population,
39 including persons with disabilities (PWDs) or who are differently-abled.

40
41
42 *Section 16. Powers and Functions of the DICT.* – To carry out its mandate, the DICT shall exercise
43 the following powers and functions:

44
45 (a) Formulate, recommend and/or implement national policies and guidelines in the ICT
46 sector that will promote wider use and development of ICT, and its applications, such as e-
47 commerce, in coordination with the Department of Trade and Industry (DTI), among others;

1
2 (b) Initiate, harmonize and/or coordinate all ICT plans and initiatives of government
3 agencies to ensure overall consistency and harmony with e-governance objectives, in particular,
4 and national objectives, in general;

5
6 (c) Represent and negotiate for Philippine interests on matters pertaining to ICT in
7 international bodies;

8
9 (d) Develop and maintain national ICT development plans and establish and administer
10 comprehensive and integrated programs for ICT with due consideration to advances in
11 convergence and other emerging technologies; and for this purpose, invite any agency,
12 corporation or organization, whether public or private, whose development programs in ICT are
13 integral parts thereof, to participate and assist in the preparation and implementation of
14 various ICT programs for the benefit of the Filipino people;

15
16 (e) Leverage resources and activities in the various National Government Agencies
17 (NGAs) for database building activity, information and resource sharing and agency networking
18 linkages;

19
20 (f) Design, implement and ensure the protection of an integrated government
21 information and communications infrastructure development program that will coordinate all
22 relevant government entities, taking into consideration the inventory of existing and projected
23 manpower, plans, programs, proposals, software and hardware, and the installed systems and
24 programs;

25
26 (g) Provide an integrated framework in order to optimize all government ICT resources
27 and networks and the identification and prioritization of all e-governance systems and
28 applications as provided for in the Government Information Systems Plan and/or the Medium-
29 Term Development Plan (MTDP);

30
31 (h) Coordinate and support the generation and/or acquisition of all necessary resources
32 and facilities as may be appropriate in and for the development, marketing, growth and
33 competitiveness of the Philippine ICT and ICT-enabled services sector;

34
35 (i) Develop, implement and improve, in coordination with concerned government
36 agencies and industry associations, the government's ICT application capabilities and determine
37 the personnel qualification and other standards essential to the integrated and effective
38 development and operation of government information and communications infrastructure;

39
40 (j) Encourage and establish guidelines for private sector funding of ICT projects for
41 government agencies in order to fast-track said projects which provide reasonable cost-
42 recovery mechanisms for the private sector including, but not limited to, build-operate-transfer
43 (BOT) and Public-Private Partnership (PPP) mechanisms;

44
45 (k) Assess, review and provide direction to ICT research and development programs of
46 the government in coordination with the Department of Science and Technology (DOST) and
47 other institutions concerned;

1
2 (l) Establish and prescribe rules and regulations for the establishment, operation and
3 maintenance of ICT facilities in areas not adequately served by the private sector, in
4 consultation with the private business sector, local government units (LGUs) and the academe;
5

6 (m) Administer and enforce all laws, standards, rules and regulations governing ICT;
7

8 (n) Ensure the protection of ICT-related intellectual property rights in coordination with
9 the Intellectual Property Office (IPO), the Optical Media Board (OMB) and other concerned
10 agencies;
11

12 (o) Protect the rights of consumer and business users to privacy, security and
13 confidentiality in coordination with concerned agencies;
14

15 (p) Harmonize, synchronize and coordinate with appropriate agencies all ICT and e-
16 commerce policies, plans and programs;
17

18 (q) Coordinate with the DTI in the promotion of trade and investment opportunities in
19 ICT and ICT-enabled services;
20

21 (r) Promote strategic partnership and alliances among and between local and
22 international ICT firms and institutions, research and development, educational and training
23 institutions, and technology providers, developers, and manufacturers to speed up industry
24 growth and enhance global competitiveness, in coordination with concerned agencies;
25

26 (s) Plan and/or implement such activities as may be appropriate and/or necessary to
27 enhance the competitiveness of Philippine workers, firms and small-to-medium enterprises in
28 the global ICT market and ICT-enabled services market in coordination with concerned
29 agencies;
30

31 (t) Undertake initiatives to promote ICT and ICT-enabled services in education and
32 training and the development, promotion and application of ICT in education in a manner that
33 is consistent with national goals and objectives, and responsive to the human resources needs
34 of the ICT and ICT-enabled services sector in particular in coordination with concerned
35 agencies;
36

37 (u) Maximize the use of existing government assets and infrastructure by encouraging
38 private sector investments and partnerships in its operation to achieve total digital inclusion
39 and access to the global information highway; and
40

41 (v) Formulate guidelines and policies defining the manner of cooperation among
42 Internet service providers, telecommunications companies, and law enforcement agencies
43 during official investigations on violations of existing laws relating to ICT.
44
45

46 *Section 17. Composition of the DICT. –*
47

1 (a) The DICT shall be headed by a Secretary to be appointed by the President, subject to
2 confirmation by the Commission on Appointments. The President shall also appoint not more
3 than four (4) Undersecretaries and four (4) Assistant Secretaries.

4
5 (b) Any person appointed as a Secretary, Undersecretary, or Assistant Secretary of the
6 Department must be a citizen and resident of the Philippines, of good moral character, of
7 proven integrity and with at least seven (7) years of proven competence and expertise in either
8 of the following: information and communications technology, information technology service
9 management, information security management, cybersecurity, data privacy, e-commerce, or
10 human capital development.

11
12 (c) At least one (1) of the Undersecretaries and one (1) of the Assistant Secretaries shall
13 be a Professional Electronics Engineer as provided for by RA 9292, as amended. At least one (1)
14 of the Undersecretaries and one (1) of the Assistant Secretaries shall be a member of the
15 Philippine Bar. The Assistant Secretaries referred to herein shall be career officers with
16 appropriate eligibilities as prescribed by the Civil Service Commission.

17
18
19 *Section 18. Secretary of ICT.* – The authority and responsibility for the exercise of the mandate
20 of the DICT and for the discharge of its powers and functions shall be vested in the Secretary of
21 ICT, hereinafter referred to as the SICT, who shall have supervision and control over the DICT.
22 For such purposes, the SICT shall:

23
24 (a) Provide executive direction and supervision over the entire operations of the DICT
25 and its attached agencies;

26
27 (b) Establish policies and standards for the effective, efficient and economical operation
28 of the DICT, in accordance with the programs of the government;

29
30 (c) Rationalize delivery systems necessary for the effective attainment of the objectives
31 of the DICT, including the creation of such offices as may be necessary to ensure the fulfillment
32 of the DICT's mandate, subject to the approval of the Department of Budget and Management
33 (DBM);

34
35 (d) Review and approve requests for financial and manpower resources of all operating
36 offices of the DICT;

37
38 (e) Designate and/or appoint all officers and employees of the DICT, except the
39 Undersecretaries, Assistant Secretaries, Regional and Assistant Regional Directors, and
40 Commissioners and Deputy Commissioners, in accordance with civil service laws, rules and
41 regulations;

42
43 (f) Establish coordinative mechanisms to ensure the successful implementation of
44 national ICT policies, initiatives and guidelines in coordination with concerned government
45 units, LGUs, public and private interest groups, including nongovernment organizations (NGOs)
46 and people's organizations (POs);

1 (g) Advise the President on the promulgation of executive and administrative orders and
2 regulatory and legislative proposals on matters pertaining to ICT development and promotion;
3

4 (h) Serve as member of the Government Procurement Policy Board as established by
5 Republic Act No. 9184, otherwise known as the "Government Procurement Reform Act";
6

7 (i) Formulate such rules and regulations and exercise such other powers as may be
8 necessary to implement the objectives and purposes of this Act; and
9

10 (j) Perform such other tasks as may be provided by law or assigned by the President
11 from time to time.
12
13

14 *Section 19. Regional Offices.* – Subject to the concurrence of the Department of Budget and
15 Management and the approval of the President, the DICT may be authorized to establish,
16 operate and maintain a regional office in each of the administrative regions of the country, as
17 the need arises. The regional office shall be headed by a Regional Director, who may be assisted
18 by one (l) Assistant Regional Director. The regional offices shall have, within their respective
19 administrative regions, the following functions:
20

21 (a) Implement laws, policies, plans, programs, projects, rules and regulations of the
22 Department;
23

24 (b) Provide efficient and effective service to the people;
25

26 (c) Coordinate with regional offices of other departments, offices and agencies;
27

28 (d) Coordinate with LGUs; and
29

30 (e) Perform such other functions as may be provided by law or assigned by the SICT.
31
32

33 *Section 20. Periodic Performance Review.* – The SICT is hereby required to formulate and
34 enforce a system of measuring and evaluating periodically and objectively the performance of
35 the DICT and to submit the same annually to the President and to appropriate congressional
36 committees.
37
38

39 *Section 21. Council of Chief Information Officers.* – Every department and agency of the national
40 government or its equivalent office in any constitutional body, state college or university and
41 government-owned and -controlled corporation is hereby directed to appoint or designate at
42 least a third (3rd) ranking official as a Chief Information Officer.
43

44 The Council of Chief Information Officers shall be composed of eleven (11) members
45 with fixed terms of office, to be appointed by the SICT from sectoral representatives of
46 government departments, constitutional bodies, the academe, LGUs, professional ICT-oriented
47 organizations, and private sector ICT-oriented NGOs. The SICT shall be the Chairperson of the

1 Council.

2

3 The Council shall serve as a coordinating body to assist the SICT in the establishment of
4 policies, standards, rules and guidelines for ICT initiatives. The Secretary shall convene the
5 Council en banc or by sector at least once every semester within a calendar year.

6

7

8 *Section 22. National Telecommunication Commission.* – The National Telecommunications
9 Commission or its successor agency shall be attached to the DICT. It shall be responsible for the
10 development, implementation, and enforcement of regulations, standards, instructions, and
11 orders governing ICT infrastructure. The NTC shall be responsible for dispute resolution, and
12 administrative and quasi-judicial proceedings, in the event of civil violations of this Act.

13

14

15 *Section 23. National Data Privacy Commission.* – The National Data Privacy Commission, as
16 provided for by the Data Privacy Act of 2012 (RA 10173), as amended, shall be attached to the
17 DICT. It shall be responsible for the development, implementation, and enforcement of
18 regulations, standards, instructions, and orders governing data privacy and security. The NDPC
19 shall be responsible for dispute resolution, and administrative and quasi-judicial proceedings, in
20 the event of civil violations of this Act.

21

22

23 *Section 24. ICT Legal Affairs Office.* – The DICT shall establish an ICT Legal Affairs Office,
24 independent of the NTC and the NDPC, and independent of its other offices. The ICT Legal
25 Affairs office shall be responsible for providing technical assistance to state prosecutors in the
26 event of violations of this Act, and shall be responsible for the filing of cases against persons
27 performing violations of this Act.

28

29

30 *Section 25. Telecommunications Office.* – The Telecommunications Office or its successor
31 agency shall be attached to the DICT. It shall be responsible for development of national ICT
32 infrastructure primarily in and up to unserved and underserved areas, and the promotion of the
33 use of ICT infrastructure in unserved and underserved areas. The President may, at his
34 discretion, dissolve the Telecommunications Office for reasons of underperformance or
35 nonperformance.

36

37

38 *Section 26. National Information and Communications Technology Institute.* – The National
39 Computer Center and the National Telecommunications Training Institute shall be combined
40 into the National Information and Communications Technology Institute (NICTI). The NICTI shall
41 be attached to the DICT, and shall be primarily responsible for the development, discretion, and
42 control of information and communications technology as a national resource, such as the
43 acquisition and utilization of computers and related devices, data communications, information
44 systems, software development, and manpower development. It shall be tasked to coordinate
45 all activities related to information technology development in the country, and shall be
46 primarily responsible for the training of government personnel in information and
47 communications technology. The NICTI shall also be tasked to ensure the implementation of an

1 integrated national information and communications technology program.

2

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

5

6

7 *Section 27. Freedom of Information and the Official Gazette.* – The DICT and the Official Gazette
8 may establish a clearinghouse for government public information, with the responsibility of
9 publishing online and periodically updating government public information, to promote
10 transparency and citizen engagement through the use of information and communications
11 technology.

12

13

14 *Section 28. Compliance with RA 6656.* – The laws and rules on government reorganization as
15 provided for in Republic Act No. 6656, otherwise known as the Reorganization Law, shall govern
16 the reorganization processes of the DICT.

17

18

19 *Section 29. Sectoral and Industry Task Forces.* – The DICT may create sectoral and industry task
20 forces, technical working groups, advisory bodies or committees for the furtherance of its
21 objectives. Additional private sector representatives, such as from the academe, the federation
22 of private industries directly involved in ICT, professional ICT-oriented organizations, as well as
23 other NGAs, LGUs and government-owned and -controlled corporations (GOCCs), may be
24 appointed to these working groups. Government IT professionals may also be tapped to
25 partake in the work of the Department through these working groups.

26

27

28 *Section 30. Structure and Staffing Pattern.* – The DICT shall determine its organizational
29 structure and create new divisions or units as it may deem necessary, subject to the approval of
30 the DBM, and shall appoint officers and employees of the Department in accordance with the
31 Civil Service Law, rules and regulations.

32

33

34 *Section 31. Magna Carta for Scientists, Engineers, Researchers and other S & T Personnel in the*
35 *Government.* – Employees of the DICT shall be covered by the Magna Carta for Scientists,
36 Engineers, Researchers and other Science & Technology Personnel in the Government (RA
37 8439).

38

39

40 *Section 32. Separation from Service.* –

41

42 (a) Employees separated from the service as a result of the reorganization shall, within
43 ninety (90) days therefrom, receive the retirement benefits to which they may be entitled
44 under existing laws, rules and regulations.

45

46 (b) Incumbents whose positions are not included in the new position structure and
47 staffing pattern of the DICT or who are not reappointed shall be deemed separated from the

1 service, whether permanent, temporary, contractual or casual employees, and shall, within
2 ninety (90) days therefrom, receive the retirement benefits to which they may be entitled to
3 under existing laws, rules and regulations.

4
5
6 **Part 5. Regulations for the Promotion of Internet Rights and Freedoms.**

7
8 *Section 33. Declaration of Compliance with Treaty Obligations and International Conventions. –*

9
10 (a) The State recognizes that the Internet itself is possible through the standardization of
11 units across multiple jurisdictions.

12
13 (b) The standards for networks and the Internet, as set by the International
14 Telecommunications Union (ITU), the Internet Engineering Task Force (IETF), the World Wide
15 Web Consortium (WWWC), and the Internet Corporation for Assigned Numbers and Names
16 (ICANN), and their successors-in-interest are hereby adopted. No agency or instrumentality of
17 the State shall issue rules and regulations contrary to these.

18
19 (c) The State recognizes that the rights and obligations in the use of networks and the
20 Internet that shall be guaranteed and imposed by this Act are subject to its treaty obligations
21 and obligations under instruments of international law.

22
23 (d) The State reaffirms its compliance to the treaties and international conventions to
24 which it is a signatory, to wit, the International Covenant on Civil and Political Rights (ICCPR),
25 the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the Convention
26 on the Rights of the Child (CRC), the Convention on the Elimination of All Forms of Racial
27 Discrimination (ICERD), the Convention on the Elimination of All Forms of Discrimination
28 Against Women (CEDAW), the Convention on the Rights of Persons with Disabilities (CRPD), the
29 United Nations Convention against Transnational Organized Crime, the United Nations
30 Convention against Corruption, the Geneva Convention, the United Nations Convention on
31 Certain Conventional Weapons, the Rome Statute of the International Criminal Court, the
32 Convention on Cybercrime (Budapest Convention), and the General Agreement on Tariffs and
33 Trade (GATT), among others. No agency or instrumentality of the State shall issue rules and
34 regulations governing the use of networks and the Internet contrary to these.

35
36 (e) The State shall keep abreast with and be guided by developments of the Internet and
37 of information and communications technology under international law and shall continually
38 design and implement policies, laws, and other measures to promote the objectives of this Act.

39
40
41 *Section 34. The State as the Primary Duty Bearer. –* The State, as the primary duty-bearer, shall
42 uphold constitutional rights, privileges, guarantees, and obligations in the development and
43 implementation of policies related to the Internet and information and communication
44 technology. The State shall fulfill this duty through law, policy, regulatory instruments,
45 administrative guidelines, and other appropriate measures, including temporary special
46 measures.

1
2 *Section 35. Duties of the State Agencies and Instrumentalities. –*
3

4 (a) *Internet and Information and Communications Technology Policy.* – Subject to
5 provisions of this Act, the Department of Information and Communications Technology shall be
6 the lead agency for oversight over the development and implementation of plans, policies,
7 programs, measures, and mechanisms in the use of the Internet and information and
8 communications technology in the Philippines.
9

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

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

22 (d) *Information and Communications Technology Infrastructure Development. –*
23

24 (i) Subject to provisions of this Act, the Department of Information and
25 Communications Technology shall have responsibility to develop and implement plans,
26 policies, programs, measures, and mechanisms for the development of information and
27 communications technology infrastructure in the Philippines and the promotion of
28 investment opportunities to this end.
29

30 (ii) ICT infrastructure and facilities, including the civil works components thereof,
31 fall within private sector infrastructure or development projects as defined under
32 Republic Act No. 6957, as amended by Republic Act No. 7718, and may, upon the
33 discretion of the National Government or local government units, be the subject of the
34 contractual arrangements authorized under the said law. *Provided,* that the DICT shall
35 be the implementing agency of such projects to be implemented by the national
36 government; *Provided, further,* that the DICT shall have the right to require its prior
37 concurrence to such projects implemented by local government units, through duly
38 promulgated regulations that specify, among others, the requisite threshold contract
39 prices that would require prior concurrence of the DICT.
40

41 (iii) The procurement by the national government or by local governments of
42 ICT-related goods and services which will not be implemented under Republic Act No.
43 6957, as amended by Republic Act No. 7718, shall be governed by Republic Act No.
44 9184.
45

46 (iv) The development and operation of information and communications
47 technology infrastructure and facilities is hereby declared as a preferred area of

1 investment and shall be included in the annual Investment Priority Plan issued in
2 accordance with the Omnibus Investments Code. Subject to the contrary factual
3 determination of the Board of Investments, an entity involved in the development and
4 operation of information and communications technology infrastructure and facilities is
5 presumed to be entitled to register as a registered enterprise under the Investment
6 Priorities Plan; *Provided*, that an enterprise that proposes to operate a public utility or
7 public service shall be subject to the equity requirements imposed by the Constitution
8 and by applicable laws; *Provided, further*, that any such entity which intends to operate
9 in a special economic zone or in a tourism economic zone as defined by applicable law
10 shall be entitled to receive the additional investment incentives granted to such zone-
11 registered enterprises in accordance with the applicable law; *Provided, finally*, that
12 nothing in this Section shall be construed to limit the available incentives to which an
13 entity may be entitled to under Republic Act No. 6957, as amended.

14
15 (v) The implementing rules of the registration of the entity involved in the
16 development or operation information and communications technology as well as the
17 incentives provided herein shall be developed by the Board of Investments together
18 with the DICT and the Department of Finance.

19
20 (vi) Subject to joint oversight by the DICT, the DOF, the Department of Budget
21 and Management, and the Commission on Audit, the NEDA may establish a venture
22 capital corporation to encourage research and development of information and
23 communications technology in the Philippines.

24
25
26 (e) *Human Resources, Skills and Technology Development for Information and*
27 *Communications Technology.* – Subject to provisions of this Act, the Department of Information
28 and Communications Technology, the Department of Science and Technology, and the
29 Technical Education and Skills Development Authority shall have the joint responsibility to
30 develop and implement plans, policies, programs, measures, and mechanisms for the
31 development of human resources, skills development, and technology development for
32 information and communications technology infrastructure in the Philippines.

33
34 (f) *Information and Communications Technology Education.* – Subject to provisions of
35 this Act, the Department of Information and Communications Technology, the Department of
36 Education, and the Commission on Higher Education shall have the joint responsibility to
37 develop and implement plans, policies, programs, measures, and mechanisms for information
38 and communications technology education in the Philippines.

39
40 (g) *Intellectual Property Rights Protection in Cyberspace.* – Subject to provisions of this
41 Act and other relevant laws, the Intellectual Property Office shall, within Philippine jurisdiction,
42 be primarily responsible for the protection of intellectual property rights in cyberspace. As
43 official registrar and repository of copies of published works, the National Library and the
44 National Archives shall assist the Intellectual Property Office in the protection of copyright.

45
46
47 *Section 36. Amendments to the Public Telecommunications Policy Act of the Philippines.* –

1
2 (a) Jurisdiction over the provision and regulation of Internet and information and
3 communications technology services shall be vested with the National Telecommunications
4 Commission, in accordance with the succeeding provisions.

5
6 (b) Article III, Section 5 of Public Telecommunications Policy Act of the Philippines (RA
7 7925) is hereby amended to read:

8
9 *Section 5. Responsibilities of the National Telecommunications Commission.* - The
10 National Telecommunications Commission (Commission) shall be the principal
11 administrator of this Act and as such shall take the necessary measures to implement
12 the policies and objectives set forth in this Act. Accordingly, in addition to its existing
13 functions, the Commission shall be responsible for the following:

14
15 a) Adopt an administrative process which would facilitate the entry of
16 qualified service providers and adopt a pricing policy which would generate
17 sufficient returns to encourage them to provide basic telecommunications,
18 **NETWORK, AND INTERNET** services in unserved and underserved areas;

19
20 b) Ensure quality, safety, reliability, security, compatibility and inter-
21 operability of telecommunications, **NETWORK, AND INTERNET** services in
22 conformity with standards and specifications set by international radio,
23 telecommunications, **NETWORK, AND INTERNET** organizations to which the
24 Philippines is a signatory;

25
26 c) Mandate a fair and reasonable interconnection of facilities of
27 authorized public network operators and other providers of
28 telecommunications, **NETWORK, AND INTERNET** services through appropriate
29 modalities of interconnection and at a reasonable and fair level of charges,
30 which make provision for the cross subsidy to unprofitable local exchange
31 service areas so as to promote telephone [density], **MOBILE PHONE, NETWORK,**
32 **AND BROADBAND DENSITY** and provide the most extensive access to basic
33 telecommunications, **NETWORK, AND INTERNET** services available at affordable
34 rates to the public;

35
36 xxx

37
38 e) Promote consumers' welfare by facilitating access to
39 telecommunications, **NETWORK, AND INTERNET SERVICES** whose infrastructure
40 and network must be geared towards the needs of individual and business users,
41 **AND BY DEVELOPING AND IMPLEMENTING STANDARDS, PLANS, POLICIES,**
42 **PROGRAMS, MEASURES, AND MECHANISMS, INCLUDING ARBITRATION,**
43 **QUASI-JUDICIAL, AND PROSECUTORIAL MECHANISMS, TO PROTECT THE**
44 **WELFARE OF CONSUMERS AND USERS OF TELECOMMUNICATIONS, NETWORK,**
45 **AND INTERNET SERVICES;**

46
47 xxx

1
2
3 (b) Article III, Section 6 of the Public Telecommunications Policy Act of the Philippines is
4 hereby amended to read:

5
6 *Section 6. Responsibilities of and Limitations to Department Powers.* - The
7 Department of [Transportation and Communications (DOTC)] **INFORMATION AND**
8 **COMMUNICATIONS TECHNOLOGY (DICT)** shall not exercise any power which will tend
9 to influence or effect a review or a modification of the Commission's quasi-judicial
10 functions.

11
12 In coordination with the Commission, however, the Department shall, in
13 accordance with the policies enunciated in this Act, be responsible for:

14
15 xxx

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

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

28
29 xxx

30
31 (c) Article IV of the Public Telecommunications Policy Act of the Philippines is hereby
32 amended to include the following provisions:

33
34 **SECTION 10A. LOCAL INTERNET SERVICE PROVIDER. – A LOCAL INTERNET**
35 **SERVICE PROVIDER SHALL:**

36
37 **(A) PROVIDE UNIVERSAL INTERNET CONNECTION SERVICE TO ALL**
38 **SUBSCRIBERS WHO APPLIED FOR SUCH SERVICE, WITHIN A REASONABLE**
39 **PERIOD AND AT SUCH STANDARDS AS MAY BE PRESCRIBED BY THE**
40 **COMMISSION AND AT SUCH TARIFF AS TO SUFFICIENTLY GIVE IT A FAIR**
41 **RETURN ON ITS INVESTMENTS.**

42
43 **(B) BE PROTECTED FROM UNCOMPENSATED BYPASS OR OVERLAPPING**
44 **OPERATIONS OF OTHER TELECOMMUNICATIONS ENTITIES IN NEED OF**
45 **PHYSICAL LINKS OR CONNECTIONS TO ITS CUSTOMERS IN THE AREA EXCEPT**
46 **WHEN IT IS UNABLE TO PROVIDE, WITHIN A REASONABLE PERIOD OF TIME**
47 **AND AT DESIRED STANDARD, THE INTERCONNECTION ARRANGEMENTS**

1 REQUIRED BY SUCH ENTITIES.

2
3 (C) HAVE THE FIRST OPTION TO PROVIDE PUBLIC OR PRIVATE NETWORK
4 ACCESS OR INTERNET ACCESS NODES OR ZONES IN THE AREA COVERED BY ITS
5 NETWORK.

6
7 (D) BE ENTITLED TO A FAIR AND EQUITABLE REVENUE SHARING
8 ARRANGEMENT WITH THE INTERNET EXCHANGE, INTERNET DATA CENTER,
9 INTERNET GATEWAY FACILITY, OR SUCH OTHER CARRIERS CONNECTED TO ITS
10 BASIC NETWORK.

11
12 PROVIDED THAT THE SERVICE IT PROVIDES IS SOLELY DEPENDENT ON EXISTING
13 NETWORKS BEING OPERATED AND MAINTAINED BY AT LEAST ONE OTHER
14 TELECOMMUNICATIONS ENTITY, A LOCAL INTERNET SERVICE PROVIDER NEED NOT
15 SECURE A FRANCHISE.

16
17 A CABLE TV FRANCHISE MAY PROVIDE LOCAL INTERNET CONNECTION,
18 NETWORK, OR DATA TRANSMISSION SERVICES WITHOUT A SEPARATE FRANCHISE;
19 PROVIDED, THAT THE OPERATION OF INTERNET CONNECTION, NETWORK, OR DATA
20 TRANSMISSION SERVICE BY THE CABLE TV FRANCHISE SHALL BE GOVERNED BY THIS
21 ACT AND OTHER RELEVANT LAWS.

22
23 THE PROVISION OF INTERNET CONNECTION, NETWORK, OR DATA
24 TRANSMISSION SERVICES SHALL BE ALSO BE GOVERNED BY THE PUBLIC SERVICE ACT,
25 AS AMENDED, AND OTHER RELEVANT LAWS GOVERNING UTILITIES.

26
27 **SECTION 10B. INTERNET EXCHANGE.** – THE NUMBER OF ENTITIES ALLOWED TO
28 PROVIDE INTERNET EXCHANGE SERVICES SHALL NOT BE LIMITED, AND AS A MATTER
29 OF POLICY, WHERE IT IS ECONOMICALLY VIABLE, AT LEAST TWO (2) INTERNET
30 EXCHANGES SHALL BE AUTHORIZED: PROVIDED, HOWEVER, THAT A LOCAL INTERNET
31 SERVICE PROVIDER SHALL NOT BE RESTRICTED FROM OPERATING ITS OWN INTERNET
32 EXCHANGE SERVICE IF ITS VIABILITY IS DEPENDENT THERETO. SUCH INTERNET
33 EXCHANGE SHALL HAVE THE FOLLOWING OBLIGATIONS:

34
35 (A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET EXCHANGES IN
36 THE SAME CATEGORY AND WITH ALL LOCAL INTERNET SERVICE PROVIDERS
37 AND OTHER TELECOMMUNICATIONS ENTITIES, UPON APPLICATION AND
38 WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR AND REASONABLE
39 LEVEL CHARGES, IN ORDER THAT INTERNET AND NETWORK SERVICES ARE
40 MADE POSSIBLE; AND

41
42 (B) IT SHALL HAVE THE RIGHT TO ESTABLISH AND OPERATE ITS OWN
43 NETWORK FACILITIES THROUGH WHICH INTERNATIONAL NETWORKS OR
44 INTERNATIONAL GATEWAY FACILITIES SHALL BE ABLE TO COURSE THEIR
45 MESSAGES OR SIGNALS.

46
47 (C) IT SHALL COMPLY WITH INTERNATIONAL AND GENERIC

1 ENGINEERING REQUIREMENTS AND STANDARDS OF OPERATION FOR
2 INTERNET EXCHANGES.

3
4 **SECTION 10C. INTERNET DATA CENTER.** – THE NUMBER OF ENTITIES ALLOWED
5 TO PROVIDE INTERNET DATA CENTER SERVICES SHALL NOT BE LIMITED, AND AS A
6 MATTER OF POLICY, WHERE IT IS ECONOMICALLY VIABLE, AT LEAST TWO (2) INTERNET
7 DATA CENTERS SHALL BE AUTHORIZED: PROVIDED, HOWEVER, THAT A LOCAL
8 INTERNET SERVICE PROVIDER OR CONTENT PROVIDER SHALL NOT BE RESTRICTED
9 FROM OPERATING ITS OWN INTERNET DATA CENTER IF ITS VIABILITY IS DEPENDENT
10 THERETO. SUCH INTERNET DATA CENTER SHALL HAVE THE FOLLOWING OBLIGATIONS:

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

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

23
24 (C) IT SHALL COMPLY WITH INTERNATIONAL AND GENERIC
25 ENGINEERING REQUIREMENTS AND STANDARDS OF OPERATION FOR
26 NETWORK AND DATA CENTERS.

27
28 **SECTION 10D. INTERNET GATEWAY FACILITY.** – ONLY ENTITIES WHICH WILL
29 PROVIDE INTERNET EXCHANGE SERVICES OR INTERNET DATA CENTER SERVICES, AND
30 CAN DEMONSTRABLY SHOW TECHNICAL AND FINANCIAL CAPABILITY TO INSTALL AND
31 OPERATE AN INTERNATIONAL GATEWAY FACILITY, SHALL BE ALLOWED TO OPERATE
32 AS AN INTERNET GATEWAY FACILITY.

33
34 THE ENTITY SO ALLOWED SHALL BE REQUIRED TO PRODUCE A FIRM
35 CORRESPONDENT OR INTERCONNECTION RELATIONSHIPS WITH MAJOR OVERSEAS
36 TELECOMMUNICATIONS AUTHORITIES, CARRIERS, OVERSEAS INTERNET GATEWAYS,
37 NETWORKS, AND INTERNET SERVICE PROVIDERS WITHIN ONE (1) YEAR FROM THE
38 GRANT OF THE AUTHORITY.

39
40 THE INTERNET GATEWAY FACILITY SHALL ALSO COMPLY WITH ITS
41 OBLIGATIONS TO PROVIDE INTERNET EXCHANGE SERVICES IN UNSERVED OR
42 UNDERSERVED AREAS WITHIN THREE (3) YEARS FROM THE GRANT OF THE AUTHORITY
43 AS REQUIRED BY EXISTING REGULATIONS: PROVIDED, HOWEVER, THAT SAID
44 INTERNET GATEWAY FACILITY SHALL BE DEEMED TO HAVE COMPLIED WITH THE SAID
45 OBLIGATION IN THE EVENT IT ALLOWS AN AFFILIATE THEREOF TO ASSUME SUCH
46 OBLIGATION AND WHO COMPLIES THEREWITH.

1 FAILURE TO COMPLY WITH THE ABOVE OBLIGATIONS SHALL BE A CAUSE TO
2 CANCEL ITS AUTHORITY OR PERMIT TO OPERATE AS AN INTERNET GATEWAY FACILITY.
3

4 **SECTION 10E. CONTENT PROVIDER.** – EXCEPT FOR BUSINESS PERMITS AND
5 OTHER REGULATORY REQUIREMENTS AS PROVIDED FOR BY THE CONSUMER ACT OF
6 THE PHILIPPINES, AS AMENDED, AND OTHER RELEVANT LAWS, AND PROVIDED THAT
7 THE TRANSMISSION OF ITS CONTENT IS SOLELY DEPENDENT ON EXISTING NETWORKS
8 BEING OPERATED AND MAINTAINED BY AT LEAST ONE OTHER
9 TELECOMMUNICATIONS ENTITY, A CONTENT PROVIDER FOR COMMERCIAL OR NON-
10 COMMERCIAL PURPOSES NEED NOT SECURE A FRANCHISE, LICENSE, OR PERMIT TO
11 OPERATE IN THE PHILIPPINES.
12

13 SUBJECT TO THE NATURE OF THE CONTENT THAT IS PROVIDED BY THE
14 CONTENT PROVIDER FOR COMMERCIAL PURPOSES, LAWS SUCH AS PAGCOR CHARTER,
15 AS AMENDED, THE MTRCB CHARTER, AS AMENDED, AND OTHER RELEVANT LAWS,
16 SHALL BE DEEMED APPLICABLE TO THE CONTENT PROVIDER.
17

18
19 (d) Article IV, Section 11 of the Public Telecommunications Policy Act of the Philippines
20 is hereby amended to read:
21

22 *Section 11. Value-added Service Provider.* – Provided that [it does not put up its
23 own network] **THE SERVICE IT PROVIDES IS SOLELY DEPENDENT ON EXISTING**
24 **NETWORKS BEING OPERATED AND MAINTAINED BY AT LEAST ONE OTHER**
25 **TELECOMMUNICATIONS ENTITY**, a VAS provider need not secure a franchise. A VAS
26 provider shall be allowed to competitively offer its services and/or expertise, and lease
27 or rent telecommunications equipment and facilities necessary to provide such
28 specialized services, in the domestic and/or international market in accordance with
29 network compatibility.
30

31 Telecommunications entities may provide VAS, subject to the additional
32 requirements that:
33

34 (a) prior approval of the Commission is secured to ensure that such VAS
35 offerings are not cross-subsidized from the proceeds of their utility operations;
36

37 (b) other providers of VAS are not discriminated against in rates nor
38 denied equitable access to their facilities; and,
39

40 (c) separate books of accounts are maintained for the VAS.
41

42 **THE PROVISION OF HIGH-SPEED OR HIGH-VOLUME INTERNET CONNECTION OR**
43 **DATA TRANSMISSION SERVICES AS A SERVICE SEPARATE FROM NORMAL INTERNET**
44 **CONNECTION OR DATA TRANSMISSION SERVICES SHALL NOT BE CLASSED AS A VALUE-**
45 **ADDED SERVICE.**
46
47

1 (e) Article V, Section 14 of the Public Telecommunications Policy Act of the Philippines is
2 hereby amended to read:

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

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

21
22
23 (f) Article VII, Section 20 of The Public Telecommunications Policy Act of the Philippines
24 is hereby amended to read:

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

28
29 xxx

30
31 **(C) RIGHT TO BE GIVEN THE FIRST INTERNET OR NETWORK**
32 **CONNECTION WITHIN TWO (2) MONTHS OF APPLICATION FOR SERVICE,**
33 **AGAINST DEPOSIT; OR WITHIN THREE (3) MONTHS AFTER TARGETED**
34 **COMMENCEMENT OF SERVICE IN THE BARANGAY CONCERNED PER THE**
35 **ORIGINAL SCHEDULE OF SERVICE EXPANSION APPROVED BY THE**
36 **COMMISSION, WHICHEVER DEADLINE COMES LATER;**

37
38 **(d) Regular, timely and accurate billing, courteous and efficient service**
39 **at utility business offices and by utility company personnel;**

40
41 **(E) TIMELY CORRECTION OF ERRORS IN BILLING AND THE IMMEDIATE**
42 **PROVISION OF REBATES OR REFUNDS BY THE UTILITY WITHOUT NEED FOR**
43 **DEMAND BY THE USER; AND;**

44
45 **(f) Thorough and prompt investigation of, and action upon complaints.**
46 **The utility shall endeavor to allow complaints [over the telephone] TO BE**
47 **RECEIVED BY POST AND OVER MEANS USING TELECOMMUNICATIONS**

1 FACILITIES OR THE INTERNET, WHICH SHALL INCLUDE BUT SHALL NOT BE
2 LIMITED TO VOICE CALLS, SHORT MESSAGE SERVICE (SMS) MESSAGES,
3 MULTIMEDIA MESSAGE SERVICE (MMS) MESSAGES, OR EMAIL, and shall keep a
4 record of all [written or phoned-in] complaints received and the actions taken to
5 address these complaints;
6

7 SUBJECT TO THE FILING OF A FORMAL REQUEST TO THE UTILITY, A USER MAY
8 REQUEST THE IMMEDIATE TERMINATION OF SERVICE, WITHOUT THE IMPOSITION OF
9 FEES OR PENALTIES, AND WITH THE REFUND OF ANY FEES OR CHARGES ALREADY PAID
10 BY THE USER, SHOULD A UTILITY NOT CONSISTENTLY COMPLY WITH PRECEDING
11 PARAGRAPHS (A), (D), (E), (F), OR ANY OTHER MINIMUM PERFORMANCE STANDARDS
12 SET BY THE COMMISSION.
13

14 SUBJECT TO STANDARDS SET BY THE COMMISSION, REASONABLE FEES OR
15 PENALTIES MAY BE IMPOSED BY THE UTILITY, OR MAY BE DEDUCTED FROM ANY FEES
16 OR CHARGES ALREADY PAID BY THE USER, SHOULD A USER REQUEST THE IMMEDIATE
17 TERMINATION OF SERVICE; PROVIDED THAT:
18

19 (1) THE UTILITY IS ABLE TO SHOW THAT THE REQUEST IS NOT BASED ON
20 A NONCOMPLIANCE WITH PRECEDING PARAGRAPHS (A), (D), (E), (F), OR ANY
21 OTHER MINIMUM PERFORMANCE STANDARDS SET BY THE COMMISSION; OR,
22

23 (2) THE UTILITY HAS EVIDENCE THAT THE NON-COMPLIANCE HAS NOT
24 RECURRED, IS NOT RECURRING, NOR WILL RECUR IN THE FUTURE; OR THE
25 UTILITY HAS EVIDENCE THAT THE NONCOMPLIANCE WAS DUE TO FACTORS
26 BEYOND ITS CONTROL; OR THE UTILITY HAS PROVIDED IMMEDIATE REFUND
27 OR REBATE TO THE USER UPON DETECTION OF THE NONCOMPLIANCE; OR THE
28 UTILITY HAS EVIDENCE THAT IT HAS EXERTED ITS BEST EFFORTS TO RESOLVE
29 THE NONCOMPLIANCE AND RESTORE THE SERVICE TO THE LEVEL AGREED
30 BETWEEN THE UTILITY AND THE USER WITHIN SEVEN (7) DAYS OF THE
31 REQUEST FOR IMMEDIATE TERMINATION; AND THE UTILITY SHALL COMPLY
32 WITH IMMEDIATE TERMINATION OF SERVICE, WITHOUT THE IMPOSITION OF
33 FEES OR PENALTIES, AND REFUND ANY FEES OR CHARGES ALREADY PAID BY
34 THE USER WITHOUT NEED FOR DEMAND SHOULD THE SERVICE NOT BE
35 RESTORED WITHIN THE SEVEN (7) DAY PERIOD, WITHIN THREE (3) DAYS AFTER
36 THE TERMINATION OF SERVICE.
37

38 SUBJECT TO STANDARDS SET BY THE COMMISSION, PENALTIES MAY BE
39 IMPOSED ON A UTILITY THAT IS UNABLE TO COMPLY WITH PRECEDING PARAGRAPHS
40 (B) AND (C). THE COMMISSION MAY IMPOSE ADDITIONAL PENALTIES IF THE UTILITY
41 DOES NOT REFUND ANY DEPOSITS, FEES, OR CHARGES ALREADY PAID BY THE USER
42 WITHOUT NEED FOR DEMAND WITHIN THREE (3) DAYS AFTER THE DEADLINE AGREED
43 UPON BETWEEN THE USER AND THE UTILITY.
44

1 (a) No Internet service provider, Internet exchange, Internet data center, Internet
2 gateway facility, telecommunications entity, or person providing Internet connection, network,
3 or data transmission services shall:

4
5 (i) Fail to provide a service, or network services on reasonable, and
6 nondiscriminatory terms and conditions such that any person can offer or provide
7 content, applications, or services to or over the network in a manner that is at least
8 equal to the manner in which the provider or its affiliates offer content, applications,
9 and services free of any surcharge on the basis of the content, application, or service;

10
11 (ii) Refuse to interconnect facilities with other facilities of another provider of
12 network services on reasonable, and nondiscriminatory terms or conditions;

13
14 (iii) Block, impair, or discriminate against, or to interfere with the ability of any
15 person to use a network service to access, to use, to send, to receive, or to offer lawful
16 content, applications, or services over the Internet;

17
18 (iv) Impose an additional charge to avoid any conduct that is prohibited by
19 subscription;

20
21 (v) Prohibit a user from attaching or using a device on the Internet service
22 provider's network that does not physically damage or materially degrade other users'
23 utilization of the network;

24
25 (vi) Fail to clearly and conspicuously disclose to users, in plain language, accurate
26 information concerning any terms, conditions, or limitations on the network service; or,

27
28 (vii) Impose a surcharge or other consideration for the prioritization or offer of
29 enhanced quality of service to data or protocol of a particular type, and must provide
30 equal quality of service to all data or protocol of that type regardless of origin or
31 ownership.

32
33
34 (b) Nothing in this section shall be construed as to prevent an Internet service provider,
35 Internet exchange, Internet data center, Internet gateway facility, telecommunications entity,
36 or person providing Internet connection, network, or data transmission services from taking
37 reasonable and nondiscriminatory measures:

38
39 (i) To manage the function of a network on a system-wide basis, provided that
40 such management function does not result in the discrimination between content,
41 application, or services offered by the provider or user;

42
43 (ii) To give priority to emergency communications;

44
45 (iii) To prevent a violation of law; or to comply with an order of the court
46 enforcing such law;

47

1 (iv) To offer consumer protection services such as parental controls, provided
2 users may refuse to enable such services, or opt-out; or,

3
4 (v) To offer special promotional pricing or other marketing initiatives.

5
6
7 (c) An Internet service provider, Internet exchange, Internet data center, Internet
8 gateway facility, telecommunications entity, or person providing Internet connection, network,
9 or data transmission services may provide for different levels of availability, uptime, or other
10 service quality standards set by the National Telecommunications Commission for services
11 using prepaid, postpaid, or other means of payment; *Provided*, that minimum levels of
12 availability, uptime, and other service quality standards set by the Commission shall not be
13 different between services using prepaid, postpaid, or other means of payment.

14
15
16 *Section 38. Amendments to the Intellectual Property Code of the Philippines. –*

17
18 (a) Part IV, Chapter II, Section 172 of the Intellectual Property Code of the Philippines
19 (RA 8293) is hereby amended to read:

20
21 *Section 172. Literary and Artistic Works. – 172.1.* Literary and artistic works,
22 hereinafter referred to as "works", are original intellectual creations in the literary and
23 artistic domain protected from the moment of their creation and shall include in
24 particular:

25
26 xxx

27
28 (n) **CODE, SCRIPTS, COMPUTER PROGRAMS, SOFTWARE APPLICATIONS,**
29 **AND OTHER SIMILAR WORK, WHETHER EXECUTABLE IN WHOLE OR AS PART OF**
30 **ANOTHER CODE, SCRIPT, computer programs, SOFTWARE APPLICATION OR**
31 **OTHER SIMILAR WORK;**

32
33 xxx

34
35 172.2. Works are protected by the sole fact of their creation, irrespective of
36 their mode or form of expression **OR PUBLICATION**, as well as of their content, quality
37 and purpose.

38
39
40 (b) Part II, Chapter V, Section 177 of the Intellectual Property Code of the Philippines (RA
41 8293) shall be amended to read:

42
43 *Section 177. Copyright, [or] COPYLEFT, AND OTHER Economic Rights. – THE*
44 **ECONOMIC RIGHTS OVER ORIGINAL AND DERIVATIVE LITERARY AND ARTISTIC WORKS**
45 **SHALL BE ANY OF THE FOLLOWING:**

46
47 **177.1 COPYRIGHT – SUBJECT TO THE PROVISIONS OF CHAPTER VIII,**

1 ECONOMIC RIGHTS UNDER THIS SECTION SHALL CONSIST OF THE EXCLUSIVE
2 RIGHT TO CARRY OUT, AUTHORIZE OR PREVENT THE FOLLOWING ACTS:

3
4 XXX

5
6 177.2. COPYLEFT – IS THE EXERCISE OF ECONOMIC RIGHTS OVER
7 ORIGINAL AND DERIVATIVE WORKS, INCLUDING FREE AND OPEN-SOURCE
8 SOFTWARE, WHERE THE AUTHOR IRREVOCABLY ASSIGNS TO THE PUBLIC,
9 EITHER PARTIALLY OR FULLY, ONE OR SEVERAL RIGHTS IN COMBINATION, THE
10 RIGHT TO USE, MODIFY, EXTEND, OR REDISTRIBUTE THE ORIGINAL WORK.
11 UNDER COPYLEFT, ANY AND ALL WORKS DERIVED FROM THE ORIGINAL WORK
12 SHALL BE COVERED BY THE SAME LICENSE AS THE ORIGINAL WORK.
13 DECLARATION OF A COPYLEFT LICENSE SHALL BE SUFFICIENT IF A STATEMENT
14 OF THE APPLICABLE COPYLEFT LICENSE IS STIPULATED ON A COPY OF THE
15 WORK AS PUBLISHED.
16

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

28 177.4 EXCEPT WITH RESPECT TO ECONOMIC RIGHTS UNDER COPYLEFT,
29 THE AUTHOR OR COPYRIGHT OWNER SHALL HAVE THE OPTION TO DECLARE
30 THE TYPE OF LICENSE OR ECONOMIC RIGHTS THAT MAY BE EXERCISED BY THE
31 PUBLIC IN RELATION TO THE WORK; PROVIDED THAT, FAILURE OF THE AUTHOR
32 OR COPYRIGHT OWNER TO MAKE SUCH DECLARATION SHALL BE CONSTRUED
33 AS CLAIM OF ECONOMIC RIGHTS UNDER SECTION 177.1.
34

35
36 (c) Part II, Chapter VII, Section 180 of the Intellectual Property Code of the Philippines
37 (RA 8293) shall be amended to read:
38

39 *Section 180. Rights of Assignee of Copyright.* – 180.1. The **ECONOMIC RIGHTS**
40 **UNDER SECTION 177.1** may be assigned in whole or in part. Within the scope of the
41 assignment, the assignee is entitled to all the rights and remedies which the assignor or
42 licensor had with respect to the copyright.
43

44 XXX

45
46 180.3. The submission of a literary, photographic or artistic work to a
47 newspaper, magazine or periodical for publication, shall constitute only a license to

1 make a single publication unless a greater right is expressly granted. **IN THE CASE OF**
2 **POSTING TO A WEBSITE OR AN ONLINE VERSION OF A NEWSPAPER, MAGAZINE, OR**
3 **PERIODICAL, ENABLING ACCESS TO THE WHOLE OR PORTION OF THE WORK VIA**
4 **AUTOMATIC CONTENT SYNDICATION OR SEARCH RESULTS SHALL NOT CONSTITUTE**
5 **VIOLATION OF THE LICENSE UNLESS THE CONTRARY IS EXPRESSLY PROVIDED IN A**
6 **WRITTEN AGREEMENT BETWEEN COPYRIGHT OWNER AND PUBLISHER/HOST/SERVICE**
7 **PROVIDER.** If two (2) or more persons jointly own a copyright or any part thereof,
8 neither of the owners shall be entitled to grant licenses without the prior written
9 consent of the other owner or owners.

10
11 xxx

12
13
14 (d) Part II, Chapter VII, Section 182 of the Intellectual Property Code of the Philippines
15 (RA 8293) shall be amended to read:

16
17 *Section 182. Filing of Assignment or License **OF COPYRIGHT.*** – An assignment or
18 exclusive license may be filed in duplicate with the National Library upon payment of
19 the prescribed fee for registration in books and records kept for the purpose. Upon
20 recording, a copy of the instrument shall be returned to the sender with a notation of
21 the fact of record. Notice of the record shall be published in the IPO Gazette.

22
23 xxx

24
25
26 (e) Part II, Chapter VII, Section 187 of the Intellectual Property Code of the Philippines
27 (RA 8293) shall be amended to read:

28
29 *Section 187. Reproduction of Published Work.* – 187.1. Subject to the provisions
30 of Section 177 [and subject to the provisions] in relation to the provision of Subsection
31 187.2, the private reproduction of a published work in a single copy, where the
32 reproduction is made by a natural person exclusively for research and private study,
33 shall be permitted, without the authorization of the owner of copyright in the work.

34
35 2. The permission granted under Subsection 187.1 shall not extend to the
36 reproduction of:

37
38 xxx

39
40 (c) A compilation of **RAW** data, **HAVING NOT UNDERGONE DATA AND**
41 **INFORMATION PROCESSING**, and other materials;

42
43 xxx

44
45 **(E) THE CONTENTS OF A WEBSITE, IF SUCH DOWNLOADING IS FOR THE**
46 **PURPOSE OF CREATING A BACK-UP COPY FOR ARCHIVAL PURPOSES, OR**
47 **EXCLUSIVELY TO TEMPORARILY FACILITATE THE EXECUTION OF COMPUTER**

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

6 XXX
7
8

9 (f) Part II, Chapter IX, Section 192 of the Intellectual Property Code of the Philippines (RA
10 8293) shall be amended to read:
11

12 *Section 192. Notice of [Copyright] APPLICABLE ECONOMIC RIGHTS.* – Each copy
13 of a work published or offered for sale may contain a notice bearing the name of the
14 copyright owner, and the year of its first publication, and, in copies produced after the
15 creator's death, the year of such death. **IN CASE OF FAILURE OF THE AUTHOR OR
16 COPYRIGHT OWNER TO INDICATE THE LICENSE APPLICABLE FOR THE WORK, IT SHALL
17 BE PRESUMED THAT THE COPYRIGHT OWNER ADOPTED COPYRIGHT UNLESS INTENT
18 TO THE CONTRARY IS PROVEN.**
19
20

21 *Section 39. Content Fair Use.* –
22

23 (a) Subject to the provisions of the Intellectual Property Code of the Philippines (RA
24 8293), as amended, and this Act and other relevant laws, the viewing of online content on any
25 computer, device, or equipment shall be considered fair use.
26

27 (b) Subject to the provisions of the Intellectual Property Code of the Philippines, as
28 amended, this Act, and other relevant laws, the viewing, use, editing, decompiling, or
29 modification, of downloaded or otherwise offline content on any computer, device, or
30 equipment shall be considered fair use; *Provided*, that the derivative content resulting from
31 editing, decompiling, or modification shall be subject to the provisions of the Intellectual
32 Property Code of the Philippines (RA 8293), as amended, this Act, and other relevant laws
33 governing derivative content.
34

35 (c) It shall be presumed that any person who shall upload to, download from, edit,
36 modify, or otherwise use content on the Internet or telecommunications networks shall have
37 done so with full knowledge of the nature of the intellectual property protections applicable to
38 the content.
39
40

41 *Section 40. Amendments to the E-Commerce Act.* – Subject to the provisions of this Act,
42 paragraphs (a) and (b) of Section 33 of the Electronic Commerce Act of 2000 (RA 8792) are
43 hereby repealed.
44
45

46 *Section 41. Amendments to the Data Privacy Act.* –
47

1 (a) Subject to the provisions of this Act, Section 7 of the Data Privacy Act of 2012 (RA
2 10173) is hereby amended in part to read:

3
4 Section 7. *Functions of the National DATA Privacy Commission.* – To administer
5 and implement the provisions of this Act, and to monitor and ensure compliance of the
6 country with international standards set for data protection, there is hereby created an
7 independent body to be known as the National DATA Privacy Commission, which shall
8 have the following functions:...

9
10 (b) Subsequent mentions of “National Privacy Commission” are hereby amended to be
11 consistent with the amendment above.

12
13 (c) Subject to the provisions of this Act, Sections 29, 31, and 32 of the Data Privacy Act of
14 2012 are repealed.

15
16 (d) Subject to the provisions of this Act, Section 6 of the Data Privacy Act of 2012 is
17 amended to include the provisions on extraterritoriality as provided for by Section 67 of this
18 Act.

19
20
21 *Section 42. Repeal of the Cybercrime Prevention Act.* – The Cybercrime Prevention Act of 2012
22 (RA 10175) is repealed in its entirety.

23
24
25 **Part 6. Cybercrimes and Other Prohibited Acts.**

26
27 *Section 43. Network sabotage.* –

28
29 (a) *Direct network sabotage.* – It shall be unlawful for any person to cause or attempt to
30 cause the stoppage or degradation of Internet or network operations of another person,
31 through electronic means such as denial of service (DoS) attacks or distributed denial of service
32 (DDoS) attacks, through physical destruction of devices, equipment, physical plant, or
33 telecommunications cables including cable TV transmission lines and other transmission media,
34 or through other means, except if the stoppage or degradation has been done in the normal
35 course of work or business by a person authorized to stop, modify, or otherwise control
36 network operations of the other person.

37
38 (b) *Indirect network sabotage.* – It shall be unlawful for any person to install, infect,
39 implant, or otherwise put in a device, equipment, network, or physical plant any means of
40 performing stoppage, degradation, or modification of Internet or network operations, or data
41 or information processing, such as but not limited to bots, or to interconnect, establish, or
42 otherwise create a network of software, devices, equipment, or physical plants with the means
43 of performing stoppage, degradation, or modification of Internet or network operations, or
44 data or information processing, such as but not limited to botnets, except if the installation or
45 interconnection has been done in the normal course of work or business by a person
46 authorized to stop, modify, or otherwise control network operations or data or information
47 processing of the network.

1
2 (c) *Criminal negligence not presumed in unintentional network sabotage.* – Except upon
3 a final ruling from the courts, issued following due notice and hearing, criminal negligence shall
4 not be presumed to be the cause of the unintentional stoppage or degradation of Internet or
5 network operations by a person authorized to stop, modify, or otherwise control network
6 operations, or by accident, unforeseen occurrences, or acts of God.

7
8
9 *Section 44. Failure to Provide Reasonable Security for Data and Networks.* –

10
11 (a) *Failure to provide security.* – It shall be unlawful for any Internet service provider,
12 telecommunications entity, or other such person providing Internet or data services to
13 intentionally or unintentionally fail to provide appropriate levels of security for data, networks,
14 storage media where data is stored, equipment through which networks are run or maintained,
15 or the physical plant where the data or network equipment is housed.

16
17 (b) *Negligent failure to provide security.* – Negligence resulting to acts in violation of the
18 Data Privacy Act of 2012 (RA 10175) using a device, network equipment, or physical plant
19 connected to the Internet, public networks, private networks, or telecommunications facilities
20 shall constitute a violation of the preceding paragraph, without prejudice to prosecution under
21 the Data Privacy Act of 2012 (RA 10175).

22
23 (c) *Negligent failure to provide security presumed to be the result of criminal negligence.*
24 – The unintentional failure for any Internet service provider, telecommunications entity, or
25 other such person providing Internet or data services to provide appropriate levels of security
26 for data, networks, storage media where data is stored, equipment through which networks are
27 run or maintained, or the physical plant where the data or network equipment is housed shall
28 be presumed to be the result of criminal negligence, except upon a final ruling from the courts,
29 issued following due notice and hearing.

30
31
32 *Section 45. Violation of Data Privacy.* –

33
34 (a) *Unauthorized access.* – It shall be unlawful for any person to intentionally access
35 data, networks, storage media where data is stored, equipment through which networks are
36 run or maintained, the physical plant where the data or network equipment is housed, without
37 authority granted by the Internet service provider, telecommunications entity, or other such
38 person providing Internet or data services having possession or control of the data or network,
39 or to intentionally access intellectual property published on the Internet or on other networks
40 without the consent of the person having ownership, possession, or control of the intellectual
41 property, or without legal grounds, even if access is performed without malice.

42
43 (b) *Unauthorized modification.* – It shall be unlawful for any person to intentionally
44 modify data, networks, storage media where data is stored, equipment through which
45 networks are run or maintained, the physical plant where the data or network equipment is
46 housed, without authority granted by the Internet service provider, telecommunications entity,
47 or other such person providing Internet or data services having possession or control of the

1 data or network, or to intentionally modify intellectual property published on the Internet or on
2 other networks without the consent of the person having ownership, possession, or control of
3 the intellectual property, or without legal grounds, even if the modification is performed
4 without malice.

5
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
8 data, networks, storage media where data is stored, equipment through which networks are
9 run or maintained, the physical plant where the data or network equipment is housed, without
10 authority granted by the Internet service provider, telecommunications entity, or other such
11 person providing Internet or data services having possession or control of the data or network,
12 or to 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
17 (d) *Unauthorized disclosure.* – It shall be unlawful for any authorized person to
18 intentionally disclose or cause the disclosure to a third party or to the public any private data
19 being transmitted through the Internet or through public networks, or any data being
20 transmitted through private networks, without legal grounds, even if the disclosure was done
21 without malice.

22
23 (e) *Violation of Data Privacy Act through ICT.* – It shall be unlawful to perform acts in
24 violation of the Data Privacy Act of 2012 (RA 10175) using a device, network equipment, or
25 physical plant connected to the Internet, public networks, private networks, or
26 telecommunications facilities.

27
28
29 *Section 46. Violation of Data Security.* –

30
31 (a) *Hacking.* – It shall be unlawful for any unauthorized person to intentionally access or
32 to provide a third party with access to, or to hack or aid or abet a third party to hack into, data,
33 networks, storage media where data is stored, equipment through which networks are run or
34 maintained, the physical plant where the data or network equipment is housed. The
35 unauthorized access or unauthorized act of providing a third party with access to, or the
36 hacking into, data, networks, storage media where data is stored, equipment through which
37 networks are run or maintained, the physical plant where the data or network equipment is
38 housed shall be presumed to be malicious.

39
40 (b) *Cracking.* – It shall be unlawful for any unauthorized person to intentionally modify
41 or to crack data, networks, storage media where data is stored, equipment through which
42 networks are run or maintained, the physical plant where the data or network equipment is
43 housed, or for any unauthorized person to intentionally modify intellectual property published
44 on the Internet or on other networks. The unauthorized modification or cracking of data,
45 networks, storage media where data is stored, equipment through which networks are run or
46 maintained, the physical plant where the data or network equipment is housed, or
47 unauthorized modification of intellectual property published on the Internet or on other

1 networks, shall be presumed to be malicious.

2
3 (c) *Phishing.* –

4
5 (i) It shall be unlawful for any unauthorized person to intentionally acquire or to
6 cause the unauthorized acquisition, or identity or data theft, or phishing of private data,
7 security information, or data or information used as proof of identity of another person.
8 The unauthorized acquisition or causing to acquire, or identity or data theft, or phishing
9 of private data, security information, or data or information used as proof of identity of
10 another person shall be presumed to be malicious.

11
12 (ii) Malicious disclosure of unwarranted or false information relative to any
13 personal information or personal sensitive information obtained by him or her as
14 defined by Section 31 of the Data Privacy Act of 2012 (RA 10175) shall constitute
15 phishing.

16
17
18 (d) *Violation of Data Privacy Act in series or combination with hacking, cracking, or*
19 *phishing.* – It shall be unlawful to perform acts in violation of the Data Privacy Act of 2012 (RA
20 10175) using a device, network equipment, or physical plant connected to the Internet, public
21 networks, private networks, or telecommunications facilities performed in series or
22 combination with acts prohibited by the preceding paragraphs.

23
24
25 *Section 47. Illegal and Arbitrary Seizure.* –

26
27 (a) *Illegal Seizure.* – It shall be unlawful for any person to seize data, information, or
28 contents of a device, storage medium, network equipment, or physical plant, or to seize any
29 device, storage medium, network equipment, or physical plant connected to the Internet or to
30 telecommunications networks of another person without his consent, or to gain possession or
31 control of the intellectual property published on the Internet or on public networks of another
32 person without his consent, except upon a final ruling from the courts, issued following due
33 notice and hearing.

34
35 (b) *Aiding and Abetting Illegal Seizure.* – It shall be unlawful for any person to aid or abet
36 the seizure of data, information, or contents of a device, storage medium, network equipment,
37 or physical plant, or to seize any device, storage medium, network equipment, or physical plant
38 connected to the Internet or to telecommunications networks of another person without his
39 consent, or to gain possession or control of the intellectual property published on the Internet
40 or on public networks of another person without his consent, except upon a final ruling from
41 the courts, issued following due notice and hearing, allowing the person to perform such
42 seizure, possession, or control.

43
44 (c) *Arbitrary Seizure.* – It shall be unlawful for any public officer or employee to seize
45 data, information, or contents of a device, storage medium, network equipment, or physical
46 plant, or to seize any device, storage medium, network equipment, or physical plant connected
47 to the Internet or to telecommunications networks, or to gain possession or control of

1 intellectual property published on the Internet or on public networks, without legal grounds.

2

3 (d) *Instigating Arbitrary Seizure.* – It shall be unlawful for any person to instruct a public
4 officer or employee to perform the seizure of data, information, or contents of a device,
5 storage medium, network equipment, or physical plant, or to seize any device, storage medium,
6 network equipment, or physical plant connected to the Internet or to telecommunications
7 networks of another person without his consent, or to gain possession or control of the
8 intellectual property published on the Internet or on public networks of another person without
9 his consent, except upon a final ruling from the courts, issued following due notice and hearing,
10 providing the person with authority to perform such seizure, possession, or control and
11 delegate the same to a public officer or employee with the authority to perform such seizure,
12 possession, or control.

13

14

15 *Section 48. Infringement of Intellectual Property Rights.* –

16

17 (a) *Copyright infringement.* –

18

19 (i) Subject to the Intellectual Property Code of the Philippines and the laws
20 governing fair use, it shall be unlawful for any person to publish or reproduce on the
21 Internet, in part or in whole, any content that he does not have any economic rights
22 over, or does not acknowledge and comply with the terms of copyright or license
23 governing the intellectual property rights enjoyed by the content being published or
24 reproduced, or falsely claims having intellectual property rights over the content he
25 does not own.

26

27 (ii) Non-attribution or plagiarism of copyleft content shall constitute
28 infringement.

29

30 (iii) Non-attribution or plagiarism of free license or public domain content shall
31 constitute infringement, but shall not be subject to damages.

32

33 (iv) Subject to the Intellectual Property Code of the Philippines and the laws
34 governing fair use, it shall be unlawful for any person to reverse-engineer any whole or
35 part of any computer program, software, code, or script, whether or not executable,
36 that is the subject of a copyright, and that he does not have any property rights over, or
37 does not acknowledge and comply with the terms of copyright or license governing the
38 intellectual property rights enjoyed by the computer program being reverse-engineered.

39

40

41 (b) *Piracy.* – Subject to the Intellectual Property Code of the Philippines, it shall be
42 unlawful for any person to publish and reproduce, with intent to profit, on the Internet or on or
43 through information and communications technologies, in part or in whole, any content, or
44 computer program, software, code, or script, whether or not executable, that he does not have
45 any property rights over.

46

47 (c) *Cybersquatting.* – Subject to the Intellectual Property Code of the Philippines and

1 other relevant laws, and the Uniform Domain Name Dispute Resolution Policy of the Internet
2 Corporation for Assigned Names and Numbers (ICANN) or any policy of ICANN or successor-in-
3 interest superseding it, it shall be unlawful for any person to register or otherwise acquire, in
4 bad faith to profit or to damage, a domain name that is:

5
6 (i) Similar, identical, or confusingly similar to an existing trademark registered
7 with the appropriate government agency at the time of the domain name registration;
8 or

9
10 (ii) Identical or in any way similar with the name of a person other than the
11 registrant, in case of a personal name.

12
13
14 (d) *Unreasonable restriction of device privileges.* – Subject to Section 6 of this Act, it shall
15 be unlawful for any person engaged in the wholesale or retail of devices or equipment to, by
16 physical, electronic, or any other means, provide unreasonable restrictions on a device or
17 equipment.

18
19
20 *Section 49. Fraud via ICT.* – It shall be unlawful for any person who knowingly by means of a
21 device, equipment, or physical plant connected to the Internet, to telecommunications
22 networks, a network of a government agency, the government network, a private network or
23 any protected computer or device, or in connivance with a third party with access to the same,
24 shall use the Internet, telecommunications networks, private networks, or government
25 networks for the purpose of deceiving or defrauding another of money, goods, or property, or
26 to do the same by or through exceeding authorized access.

27
28
29 *Section 50. ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons.* –

30
31 (a) *ICT-Enabled Prostitution.* – It shall be unlawful for any person who, by means of a
32 device, equipment, or physical plant connected to the Internet or to telecommunications
33 networks, or in connivance with a third party with access to the same, shall use the Internet or
34 telecommunications networks for the purpose of enabling the exchange of money or
35 consideration for services of a sexual or lascivious nature, or facilitating the performance of
36 such services; *Provided*, the services shall be performed by one or more unwilling third-party
37 adults under threat or duress.

38
39 (b) *ICT-Enabled Trafficking in Persons.* –

40
41 (i) The performance of acts prohibited by Section 5 of R.A. No. 9208, or the
42 “Anti-Trafficking in Persons Act of 2003,” as amended, by means of a device, storage
43 medium, network equipment, or physical plant connected to the Internet or to
44 telecommunications networks shall be deemed unlawful.

45
46 (ii) The commission of acts prohibited by the Anti-Trafficking in Persons Act of
47 2003, as amended, through or using devices, equipment, or physical plants connected to

1 the Internet or to telecommunications networks shall be penalized by the applicable
2 provisions of the Anti-Trafficking in Persons Act of 2003, as amended.

3
4 (iii) Section 5 (c) of the Anti-Trafficking in Persons Act of 2003 shall be amended
5 to read:

6
7 *Section 5. Acts that Promote Trafficking in Persons.* – The following acts
8 which promote or facilitate trafficking in persons, shall be unlawful:

9
10 xxx

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

21
22 xxx

23
24
25 *Section 51. ICT-Enabled Child Prostitution and ICT-Enabled Child Trafficking.* –

26
27 (a) *ICT-Enabled Child Prostitution.* -

28
29 (i) The performance of acts prohibited by Sections 5 and 7 of R.A. No. 7610, or
30 the “Special Protection of Children Against Abuse, Exploitation and Discrimination Act,”
31 as amended, by means of a device, storage medium, network equipment, or physical
32 plant connected to the Internet or to telecommunications networks shall be deemed
33 unlawful.

34
35 (ii) Section 5, paragraphs (a) 2 and (c) of the “Special Protection of Children
36 Against Abuse, Exploitation and Discrimination Act” shall be amended to read:

37
38 *Section 5. Child Prostitution and Other Sexual Abuse.* –

39
40 xxx

41
42 (2) Inducing a person to be a client of a child prostitute by
43 means of written or oral advertisements or other similar means;
44 **OR TO KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE**
45 **DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO**
46 **THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS WITH**
47 **THE PRIMARY PURPOSE OF INDUCING A PERSON TO BE A CLIENT**

1 OF A CHILD PROSTITUTE OR THROUGH THE CONNIVANCE WITH
2 A THIRD PARTY WITH ACCESS TO THE SAME INDUCE A PERSON
3 TO BE A CLIENT OF A CHILD PROSTITUTE;
4

5 xxx
6

7 (c) Those who derive profit or advantage therefrom, whether as
8 manager or owner of the establishment where the prostitution takes
9 place, or of the sauna, disco, bar, resort, place of entertainment or
10 establishment serving as a cover or which engages in prostitution in
11 addition to the activity for which the license has been issued to said
12 establishment; **OR THOSE WHO DERIVE PROFIT OR ADVANTAGE**
13 **THEREFROM, WHETHER AS AUTHOR, ADMINISTRATOR, OR**
14 **AUTHORIZED USER OF THE DEVICE, EQUIPMENT, NETWORK, PHYSICAL**
15 **PLANT, OR WEBSITE CONNECTED TO THE INTERNET OR TO**
16 **TELECOMMUNICATIONS NETWORKS CREATED OR ESTABLISHED WITH**
17 **THE PURPOSE OF INDUCING A PERSON TO ENGAGE IN CHILD**
18 **PROSTITUTION.**
19

20 xxx
21

22
23 (b) *ICT-Enabled Child Trafficking.* –
24

25 (i) Section 7 of the “Special Protection of Children Against Abuse, Exploitation
26 and Discrimination Act” shall be amended to read:
27

28 Section 7. *Child Trafficking.* – Any person who shall engage in trading and
29 dealing with children including, but not limited to, the act of buying and selling of
30 a child for money, or for any other consideration, or barter, **OR TO KNOWINGLY,**
31 **WILLFULLY AND INTENTIONALLY PROVIDE DEVICES, EQUIPMENT, OR PHYSICAL**
32 **PLANTS CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS**
33 **NETWORKS, OR THROUGH THE CONNIVANCE WITH A THIRD PARTY WITH**
34 **ACCESS TO THE SAME, FOR THE PRIMARY PURPOSE OF SUCH TRADING AND**
35 **DEALING WITH CHILDREN,** shall suffer the penalty of *reclusion temporal* to
36 *reclusion perpetua*. The penalty shall be imposed in its maximum period when
37 the victim is under twelve (12) years of age.
38

39 (ii) The commission of acts prohibited by the “Special Protection of Children
40 Against Abuse, Exploitation and Discrimination Act,” as amended, through or using
41 devices, equipment, or physical plants connected to the Internet or to
42 telecommunications networks shall be penalized by the applicable provisions of the
43 “Special Protection of Children Against Abuse, Exploitation and Discrimination Act,” as
44 amended.
45

46
47 *Section 52. Internet Libel, Hate Speech, Child Pornography, and Other Expression Inimical to the*

1 *Public Interest.* –

2
3 (a) *Internet libel.* –

4
5 (i) Internet libel is a public and malicious expression tending to cause the
6 dishonor, discredit, or contempt of a natural or juridical person, or to blacken the
7 memory of one who is dead, made on the Internet or on public networks.

8
9 (ii) *Malice as an essential element of internet libel.* – Internet libel shall not lie if
10 malice or intent to injure is not present.

11
12 (iii) *Positive identification of the subject as an essential element of internet libel.*
13 – Internet libel shall not lie if the public and malicious expression does not explicitly
14 identify the person who is the subject of the expression, except if the content of the
15 expression is sufficient for positive and unequivocal identification of the subject of the
16 expression.

17
18 (iv) *Truth as a defense.* – Internet libel shall not lie if the content of the
19 expression is proven to be true, or if the expression is made on the basis of published
20 reports presumed to be true, or if the content is intended to be humorous or satirical in
21 nature, except if the content has been adjudged as unlawful or offensive in nature in
22 accordance with existing jurisprudence.

23
24 (v) *Exceptions to internet libel.* – The following acts shall not constitute internet
25 libel:

26
27 (1) Expressions of protest against the government, or against foreign
28 governments;

29
30 (2) Expressions of dissatisfaction with the government, its agencies or
31 instrumentalities, or its officials or agents, or with those of foreign governments;

32
33 (3) Expressions of dissatisfaction with non-government organizations,
34 unions, associations, political parties, religious groups, and public figures;

35
36 (4) Expressions of dissatisfaction with the products or services of
37 commercial entities;

38
39 (5) Expressions of dissatisfaction with commercial entities, or their
40 officers or agents, as related to the products or services that the commercial
41 entities provide;

42
43 (6) Expressions of a commercial entity that are designed to discredit the
44 products or services of a competitor, even if the competitor is explicitly
45 identified;

46
47 (7) An expression made with the intention of remaining private between

1 persons able to access or view the expression, even if the expression is later
2 released to the public; and,

3
4 (8) A fair and true report, made in good faith, without any comments or
5 remarks, of any judicial, legislative or other official proceedings, or of any
6 statement, report or speech delivered in said proceedings, or of any other act
7 performed by public officers in the exercise of their functions, or of any matter
8 of public interest.

9
10
11 (b) *Internet hate speech.* –

12
13 (i) Internet hate speech is a public and malicious expression calling for the
14 commission of illegal acts on an entire class of persons, a reasonably broad section
15 thereof, or a person belonging to such a class, based on gender, sexual orientation,
16 religious belief or affiliation, political belief or affiliation, ethnic or regional affiliation,
17 citizenship, or nationality, made on the Internet or on public networks.

18
19 (ii) *Call for the commission of illegal acts as an essential element for internet hate*
20 *speech.* – Internet hate speech shall not lie if the expression does not call for the
21 commission of illegal acts on the person or class of persons that, when they are done,
22 shall cause actual criminal harm to the person or class of persons, under existing law.

23
24 (iii) *Imminent lawless danger as an essential element for internet hate speech.* –
25 Internet hate speech shall not lie if the expression does not call for the commission of
26 illegal acts posing an immediate lawless danger to the public or to the person who is the
27 object of the expression.

28
29
30 (c) *Internet child pornography.* –

31
32 (i) The performance of acts prohibited by Sections 4 and 5 of R.A. No. 9775, or
33 the “Anti-Child Pornography Act of 2009,” as amended, by means of a device, storage
34 medium, network equipment, or physical plant connected to the Internet or to
35 telecommunications networks shall be deemed unlawful.

36
37 (ii) The commission of acts prohibited by the Anti-Child Pornography Act of 2009,
38 as amended, through or using devices, equipment, or physical plants connected to the
39 Internet or to telecommunications networks shall be penalized by the applicable
40 provisions of the Anti-Child Pornography Act of 2009, as amended.

41
42 (iii) Sections 4 (e) and (f) of the Anti-Child Pornography Act of 2009 shall be
43 amended to read:

44
45 xxx

46
47 (e) To knowingly, willfully and intentionally provide a venue for the

1 commission of prohibited acts as, but not limited to, dens, private rooms,
2 cubicles, cinemas, houses or in establishments purporting to be a legitimate
3 business; **OR TO KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE**
4 **DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO THE INTERNET OR**
5 **TO TELECOMMUNICATIONS NETWORKS FOR THE PRIMARY PURPOSE OF**
6 **PUBLICATION, OFFERING, PRODUCTION, SELLING, DISTRIBUTION,**
7 **BROADCASTING, EXPORT, OR IMPORTATION OF CHILD PORNOGRAPHY;**
8

9 (f) For film distributors, theaters, **INTERNET SERVICE PROVIDERS**, and
10 telecommunication companies, by themselves or in cooperation with other
11 entities, to distribute any form of child pornography;
12

13 xxx
14

15
16 (d) *Internet child abuse.* –
17

18 (i) The performance of acts prohibited by Section 9 of the Special Protection of
19 Children Against Abuse, Exploitation and Discrimination Act, as amended, by means of a
20 device, storage medium, network equipment, or physical plant connected to the
21 Internet or to telecommunications networks shall be deemed unlawful.
22

23 (ii) The commission of acts prohibited by the Special Protection of Children
24 Against Abuse, Exploitation and Discrimination Act, as amended, through or using
25 devices, equipment, or physical plants connected to the Internet or to
26 telecommunications networks shall be penalized by the applicable provisions of the
27 Special Protection of Children Against Abuse, Exploitation and Discrimination Act, as
28 amended.
29

30 (iii) Section 9 of the Special Protection of Children Against Abuse, Exploitation
31 and Discrimination Act shall be amended to read:
32

33 *Section 9. Obscene Publications and Indecent Shows.* – Any person who
34 shall hire, employ, use, persuade, induce or coerce a child to perform in obscene
35 exhibitions and indecent shows, whether live, in video, or through the Internet
36 or telecommunications networks, or model in obscene publications or
37 pornographic materials or to sell or distribute or **CAUSE THE PUBLICATION IN**
38 **THE INTERNET OR THROUGH TELECOMMUNICATIONS NETWORKS** the said
39 materials shall suffer the penalty of *prision mayor* in its medium period.
40

41 xxx
42

43
44 (e) *Expression inimical to the public interest.* –
45

46 (i) Except upon a final ruling from the courts, issued following due notice or
47 hearing, no expression made on the Internet or on public networks that is not defined in

1 this section shall be deemed unlawful and inimical to the public interest.

2
3 (ii) *Imminent lawless danger as an essential element of expression inimical to*
4 *public interest.* – No expression shall be deemed inimical to the public interest if the
5 expression does not call for the commission of illegal acts posing an immediate lawless
6 danger to the public.

7
8
9 *Section 53. Sabotage of critical networks and infrastructure, acts of cyberterrorism, and*
10 *cyberespionage.* –

11
12 (a) *Sabotage of critical networks and infrastructure.* – The commission of acts prohibited
13 by Section 42 (Network Sabotage), Section 44 (Violation of Data Privacy), Section 45 (Violation
14 of Data Security), and Section 46 (Illegal and Arbitrary Seizure of ICT), shall be penalized one
15 degree higher; *Provided*, the offense was committed against critical data, network, Internet, or
16 telecommunications infrastructure, whether publicly or privately owned.

17
18 (b) *Cyberterrorism.* –

19
20 (i) The performance of acts prohibited by Sections 3, 4, 5, and 6 of the Human
21 Security Act of 2007 (RA9732) as amended, and Sections 4, 5, 6, and 7 of the Terrorism
22 Financing Prevention and Suppression Act of 2012 (RA 10168), or the by means of a
23 device, storage medium, network equipment, or physical plant connected to the
24 Internet or to telecommunications networks shall be deemed unlawful.

25
26 (ii) The commission of acts prohibited by the Human Security Act of 2007, as
27 amended, through or using devices, equipment, or physical plants connected to the
28 Internet or to telecommunications networks shall be penalized by the applicable
29 provisions of the Human Security Act of 2007, as amended.

30
31 (iii) Section 3 of the Human Security Act of 2007 shall be amended to read:

32
33 *Section 3. Terrorism.* – Any person who commits an act punishable under
34 any of the following provisions of the Revised Penal Code:

35
36 xxx

37
38 6. Presidential Decree No. 1866, as amended (Decree Codifying
39 the Laws on Illegal and Unlawful Possession, Manufacture, Dealing in,
40 Acquisition or Disposition of Firearms, Ammunitions or Explosives); and,

41
42 **7. SECTION 25 (NETWORK SABOTAGE), SECTION 27 (VIOLATION**
43 **OF DATA PRIVACY), AND SECTION 28 (VIOLATION OF DATA SECURITY)**
44 **OF THE MAGNA CARTA FOR PHILIPPINE INTERNET FREEDOM**
45 **COMMITTED AGAINST CRITICAL DATA, NETWORK, INTERNET, OR**
46 **TELECOMMUNICATIONS INFRASTRUCTURE, WHETHER PUBLICLY OR**
47 **PRIVATELY OWNED,**

1
2 xxx
3
4

5 (c) *ICT-Enabled Financing of Terrorism.* –
6

7 (i) The commission of acts prohibited by the Terrorism Financing Prevention and
8 Suppression Act of 2012, as amended, through or using devices, equipment, or physical
9 plants connected to the Internet or to telecommunications networks shall be penalized
10 by the applicable provisions of the Terrorism Financing Prevention and Suppression Act
11 of 2012, as amended.
12

13 (ii) Section 4 of the Terrorism Financing Prevention and Suppression Act of 2012
14 shall be amended to read:
15

16 *Section 4. Financing of Terrorism.* –
17

18 xxx
19

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

24 **ANY PERSON WHO, BY MEANS OF A DEVICE, STORAGE MEDIUM,
25 NETWORK EQUIPMENT, OR PHYSICAL PLANT CONNECTED TO THE INTERNET OR
26 TO TELECOMMUNICATIONS NETWORKS, OR IN CONNIVANCE WITH A THIRD
27 PARTY WITH ACCESS TO THE SAME, SHALL KNOWINGLY, WILLFULLY, AND
28 INTENTIONALLY FACILITATE THE ORGANIZATION OR DIRECTION OF OTHERS TO
29 COMMIT THE FINANCING OF TERRORISM UNDER THE PRECEDING
30 PARAGRAPHS SHALL LIKEWISE BE GUILTY OF AN OFFENSE AND SHALL SUFFER
31 THE SAME PENALTY AS HEREIN PRESCRIBED.**
32

33 xxx
34
35

36 (d) *Cyber-espionage.* – Article 117 of the Revised Penal Code shall be amended to read:
37

38 *Art. 117. Espionage.* — The penalty of *prision correccional* shall be inflicted upon
39 any person who:
40

41 xxx
42

43 **2. WITHOUT AUTHORITY THEREFOR, OR EXCEEDING THE AUTHORITY
44 GRANTED BY THE STATE, AND BY MEANS OF A DEVICE, EQUIPMENT, OR
45 PHYSICAL PLANT CONNECTED TO THE INTERNET, TO TELECOMMUNICATIONS
46 NETWORKS, A NETWORK OF THE STATE, A PRIVATE NETWORK, OR ANY
47 PROTECTED DEVICE, COMPUTER, SYSTEM, OR NETWORK, OR IN CONNIVANCE**

1 WITH A THIRD PARTY WITH ACCESS TO THE SAME, SHALL USE THE INTERNET,
2 TELECOMMUNICATIONS NETWORKS, NETWORKS OF THE STATE, OR PRIVATE
3 NETWORKS TO OBTAIN ANY DATA OR INFORMATION OF A CONFIDENTIAL
4 NATURE RELATIVE TO THE DEFENSE OF THE PHILIPPINES OR ANY DATA OR
5 INFORMATION CLASSIFIED BY LAW AS STATE SECRETS; OR
6

7 3. Being in possession, by reason of the public office he holds, of the
8 articles, data, or information referred to in the preceding paragraphs, discloses
9 their contents to a representative of a foreign nation **OR HOSTILE NON-STATE**
10 **ACTOR.**
11

12 XXX
13

14
15 **Part 7. National Cybersecurity, Cyberdefense, Counter-Cyberterrorism, and**
16 **Counter-Cyberespionage.**
17

18 *Section 54. Cyberwarfare and National Defense. –*
19

20 (a) It shall be unlawful for any person, or military or civilian agency, or instrumentality of
21 the State to initiate a cyberattack against any foreign nation, except in the event of a
22 declaration of a state of war with the foreign nation.
23

24 (b) Subject to the Geneva Convention, the Hague Convention, the United Nations
25 Convention on Certain Conventional Weapons, other international treaties and conventions
26 governing the conduct of warfare, Philippine law, and on authority by the President of the
27 Philippines or by his designated officers, an authorized person or military agency may engage in
28 cyberdefense *in defense of the Filipino* people, territory, economy, and vital infrastructure in
29 the event of a cyberattack by a foreign nation, enemy violent non-state actor, insurgent group,
30 or terrorist organization.
31

32 (c) Any person who initiates an unauthorized and unlawful cyberattack against a foreign
33 nation shall be prosecuted under Commonwealth Act 408, as amended, or applicable military
34 law, without prejudice to criminal and civil prosecution.
35

36
37 *Section 55. National Cybersecurity and Protection of Government Information and*
38 *Communications Technology Infrastructure. –*
39

40 (a) The Secretary of National Defense shall assist the President in the protection and
41 conduct of the national cybersecurity, and the conduct of cyberdefense and the protection of
42 national government information and communications technology infrastructure.
43

44 (b) The Armed Forces of the Philippines shall be tasked with ensuring the physical and
45 network security of critical government and military information and communications
46 infrastructure. The Philippine National Police shall assist private and public owners, operators,
47 and maintainers in ensuring the physical and network security of critical information and

1 communications infrastructure.

2
3 (c) Local government units shall be responsible for cyberdefense within their
4 jurisdiction. The Secretary of the Interior and Local Government, with the assistance of the
5 Secretary of National Defense, shall be assist local government units in the development of
6 plans, policies, programs, measures, and mechanisms for cybersecurity and cyberdefense of at
7 the local government level and the protection of local government systems, networks, and
8 information and communications technology infrastructure.

9
10 (d) When national interest and public safety so require, and subject to the approval of
11 Congress in a special session called for the purpose, the President may be granted the authority
12 to direct the cyberdefense and cybersecurity of local government units; *Provided*, that Congress
13 may not grant such authority for a period longer than 90 days.

14
15
16 *Section 56. Amendments to the AFP Modernization Act.* – Section 5 of the AFP Modernization
17 Act (RA 7898) shall be amended to include:

18
19 *Section 5. Development of AFP Capabilities.* – The AFP modernization program shall be
20 geared towards the development of the following defense capabilities:

21
22 xxx

23
24 (d) Development of cyberdefense capability. – [The modernization of the AFP
25 further requires the development of the general headquarters capabilities for
26 command, control, communications, and information systems network.] **THE
27 PHILIPPINE AIR FORCE (PAF), BEING THE COUNTRY'S FIRST LINE OF EXTERNAL
28 DEFENSE, SHALL DEVELOP ITS CYBERDEFENSE CAPABILITY. THE CYBERDEFENSE
29 CAPABILITY SHALL ENABLE THE AFP TO:**

30
31 **(1) DETECT, IDENTIFY, INTERCEPT AND ENGAGE, IF NECESSARY, ANY
32 ATTEMPTED OR ACTUAL PENETRATION OR CYBERATTACK OF PHILIPPINE
33 GOVERNMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY
34 INFRASTRUCTURE, AS WELL AS CRITICAL INFORMATION AND
35 COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE WITHIN PHILIPPINE
36 JURISDICTION;**

37
38 **(2) PROVIDE CYBERDEFENSE SUPPORT TO PHILIPPINE ARMED FORCES
39 AND POLICE FORCES, AND;**

40
41 **(3) PROVIDE, AND IF PRACTICABLE, INVENT OR INNOVATE, THROUGH
42 FILIPINO SKILLS AND TECHNOLOGY, ITS OWN REQUIREMENTS FOR NATIONAL
43 CYBERDEFENSE.**

44
45
46 **(E) DEVELOPMENT OF CYBERINTELLIGENCE CAPABILITY. – THE INTELLIGENCE
47 SERVICE OF THE ARMED FORCES OF THE PHILIPPINES (ISAFP) OR ITS SUCCESSOR**

1 SERVICE, SHALL DEVELOP ITS CYBERINTELLIGENCE CAPABILITY. THE
2 CYBERINTELLIGENCE CAPABILITY SHALL ENABLE THE AFP TO:
3

4 (1) DETECT ANY THREAT AGAINST PHILIPPINE GOVERNMENT
5 INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE, AS
6 WELL AS CRITICAL INFORMATION AND COMMUNICATIONS TECHNOLOGY
7 INFRASTRUCTURE WITHIN PHILIPPINE JURISDICTION, AND IDENTIFY THE
8 SOURCE OF THE THREAT, WHETHER HOSTILE NATION-STATES, NON-STATE
9 ACTORS, CYBERTERRORISTS, OR CRIMINALS;

10
11 (2) PROVIDE CYBERINTELLIGENCE SUPPORT TO PHILIPPINE ARMED
12 FORCES AND POLICE FORCES, AND;

13
14 (3) PROVIDE, AND IF PRACTICABLE, INVENT OR INNOVATE, THROUGH
15 FILIPINO SKILLS AND TECHNOLOGY, ITS OWN REQUIREMENTS FOR NATIONAL
16 CYBERINTELLIGENCE.
17

18
19 (F) DEVELOPMENT OF GOVERNMENT AND MILITARY INFORMATION AND
20 COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE HARDENED AGAINST
21 CYBERATTACK. — THE COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEM
22 SERVICE, ARMED FORCES OF THE PHILIPPINES (CEISSAFP) OR ITS SUCCESSOR SERVICE,
23 SHALL CONTINUALLY ENSURE THAT GOVERNMENT AND MILITARY INFORMATION AND
24 COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE ARE HARDENED AGAINST
25 CYBERATTACK.
26

27 xxx
28

29
30 *Section 57. Counter-Cyberterrorism. —*
31

32 (a) The Philippine National Police, supported by applicable military, law enforcement,
33 and government services, offices, and agencies, shall be the lead law enforcement agency
34 responsible for plans, policies, programs, measures, and mechanisms to detect, identify, and
35 prevent cyberterrorist attacks on Philippine government information and communications
36 technology infrastructure, as well as publicly- and privately-owned information and
37 communications technology infrastructure within Philippine jurisdiction, and the detection,
38 identification, pursuit, apprehension, and the gathering of evidence leading to the conviction of
39 persons committing cyberterrorism.
40

41 (b) The National Bureau of Investigation, supported by applicable military, law
42 enforcement, and government services, offices, and agencies, shall be the lead law
43 enforcement agency responsible for plans, policies, programs, measures, and mechanisms to
44 detect, identify, and prevent transnational cyberterrorist attacks on Philippine government
45 information and communications technology infrastructure, as well as publicly- and privately-
46 owned information and communications technology infrastructure within Philippine jurisdiction
47

1 (c) Subject to the provisions of an existing treaty to which the Philippines is a signatory
2 and to any contrary provision of any law of preferential application, and subject to the
3 concurrence of the Secretary of Justice and the Secretary of Foreign Affairs, the Director of the
4 National Bureau of Investigation may cooperate with or request the cooperation of foreign or
5 international law enforcement agencies in the detection, identification, pursuit, apprehension,
6 and the gathering of evidence leading to the conviction of persons who, although physically
7 outside the territorial limits of the Philippines, have committed or are attempting to commit
8 acts of cyberterrorism within Philippine jurisdiction.

9
10
11 **Section 58. Counter-Cyberespionage. –**

12
13 (a) The National Intelligence Coordinating Agency, supported by applicable military, law
14 enforcement, and government services, offices, and agencies, shall be the lead agency
15 responsible for plans, policies, programs, measures, and mechanisms to detect, identify, and
16 prevent cyberespionage attempts and incidents.

17
18 (b) The National Bureau of Investigation, supported by applicable military, law
19 enforcement, and government services, offices, and agencies, shall be the lead agency
20 responsible for detection, identification, pursuit, apprehension, and the gathering of evidence
21 leading to the conviction of persons committing cyberespionage.

22
23
24 **Part 8. Penalties.**

25
26 **Section 59. Applicability of the Revised Penal Code and other special laws. –** Nomenclature
27 notwithstanding, the provisions of Book I of the Revised Penal Code shall apply suppletorily to
28 the provisions of this Act, whenever applicable.

29
30 The provisions of special laws shall apply as provided for by this Act.

31
32
33 **Section 60. Penalties For Specific Violations of The Magna Carta for Philippine Internet Freedom.**
34 – The following penalties shall be imposed for specific violations of this Act:

35
36 (a) Violation of Section 42 (a) (Direct network sabotage) – Shall be punished with
37 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
38 (PhP500,000.00) or both.

39
40 (b) Violation of Section 42 (b) (Indirect network sabotage) - Shall be punished with
41 imprisonment of *prision correccional* in its medium period or a fine of not more than three
42 hundred thousand pesos (PhP300,000.00) or both.

43
44 (c) Violation of Section 43 (a) (Failure to provide security) - Shall be punished with
45 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
46 (PhP500,000.00) or both.

1 (d) Violation of Section 43 (b) (Negligent failure to provide security) - Shall be punished
2 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
3 pesos (PhP500,000.00) or both.

4
5 (e) Violation of Section 44 (a) (Unauthorized access) – Shall be punished with
6 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
7 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
8 (Php2,000,000.00).

9
10 (f) Violation of Section 44 (b) (Unauthorized modification) - Shall be punished with
11 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
12 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
13 (Php2,000,000.00).

14
15 (g) Violation of Section 44 (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
20 (h) Violation of Section 44 (d) (Unauthorized disclosure) - imprisonment ranging from
21 three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos
22 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

23
24 (i) Violations of the Section 44 (e) (Violation of Data Privacy Act through ICT) –

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

30
31 (ii) Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing of
32 Sensitive Personal Information) through ICT – imprisonment ranging from three (3)
33 years to six (6) years and a fine of not less than Five hundred thousand pesos
34 (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

35
36 (iii) Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
37 Information Due to Negligence) through ICT – imprisonment ranging from one (1) year
38 to three (3) years and a fine of not less than Five hundred thousand pesos
39 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

40
41 (iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
42 Personal Information Due to Negligence) through ICT – imprisonment ranging from
43 three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos
44 (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

45
46 (v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
47 Personal Information) through ICT – imprisonment ranging from six (6) months to two

1 (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but
2 not more than Five hundred thousand pesos (Php500,000.00).

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

8
9 (vii) Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
10 Information for Unauthorized Purposes) through ICT – imprisonment ranging from one
11 (1) year and six (6) months to five (5) years and a fine of not less than Five hundred
12 thousand pesos (Php500,000.00) but not more than One million pesos
13 (Php1,000,000.00).

14
15 (viii) Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive
16 Personal Information for Unauthorized Purposes) through ICT – imprisonment ranging
17 from two (2) years to seven (7) years and a fine of not less than Five hundred thousand
18 pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

19
20 (ix) Violation of Section 30 of the Data Privacy Act (Concealment of Security
21 Breaches Involving Sensitive Personal Information) through ICT – imprisonment of one
22 (1) year and six (6) months to five (5) years and a fine of not less than Five hundred
23 thousand pesos (Php500,000.00) but not more than One million pesos
24 (Php1,000,000.00).

25
26 (x) Violation of Section 33 of the Data Privacy Act (Combination or Series of Acts)
27 through ICT – imprisonment ranging from three (3) years to six (6) years and a fine of
28 not less than One million pesos (Php1,000,000.00) but not more than Five million pesos
29 (Php5,000,000.00).

30
31
32 (j) Violation of Section 45 (a) (Hacking) – imprisonment ranging from one (1) year to
33 three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but
34 not more than Two million pesos (Php2,000,000.00).

35
36 (k) Violation of Section 45 (b) (Cracking) – imprisonment ranging from one (1) year to
37 three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but
38 not more than Two million pesos (Php2,000,000.00).

39
40 (l) Violation of Section 45 (c) (Phishing) – imprisonment ranging from one (1) year and
41 six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos
42 (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

43
44 (m) Violation of Section 45 (d) (Violation of Data Privacy Act with hacking, cracking, or
45 phishing) –

46
47 (i) Violation of Section 25 (a) of the Data Privacy Act (Unauthorized Processing of

1 Personal Information) with hacking, cracking, or phishing – shall be penalized by
2 imprisonment ranging from one (1) year to three (3) years and a fine of not less than
3 Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos
4 (Php2,000,000.00).

5
6 (ii) Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing of
7 Sensitive Personal Information) with hacking, cracking, or phishing – shall be penalized
8 by imprisonment ranging from three (3) years to six (6) years and a fine of not less than
9 Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos
10 (Php4,000,000.00).

11
12 (iii) Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
13 Information Due to Negligence) with hacking, cracking, or phishing – shall be penalized
14 by imprisonment ranging from one (1) year to three (3) years and a fine of not less than
15 Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos
16 (Php2,000,000.00).

17
18 (iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
19 Personal Information Due to Negligence) with hacking, cracking, or phishing – shall be
20 penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not
21 less than Five hundred thousand pesos (Php500,000.00) but not more than Four million
22 pesos (Php4,000,000.00).

23
24 (v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
25 Personal Information) with hacking, cracking, or phishing – shall be penalized by
26 imprisonment ranging from six (6) months to two (2) years and a fine of not less than
27 One hundred thousand pesos (Php100,000.00) but not more than Five hundred
28 thousand pesos (Php500,000.00).

29
30 (vi) Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
31 Sensitive Personal Information) with hacking, cracking, or phishing – shall be penalized
32 by imprisonment ranging from one (1) year to three (3) years and a fine of not less than
33 One hundred thousand pesos (Php100,000.00) but not more than One million pesos
34 (Php1,000,000.00).

35
36 (vii) Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
37 Information for Unauthorized Purposes) with hacking, cracking, or phishing – shall be
38 penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years
39 and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more
40 than One million pesos (Php1,000,000.00).

41
42 (viii) Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive
43 Personal Information for Unauthorized Purposes) with hacking, cracking, or phishing –
44 shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a
45 fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than
46 Two million pesos (Php2,000,000.00).

47

1 (ix) 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

7 (x) Violation of Section 33 of the Data Privacy Act (Combination or Series of Acts)
8 with hacking, cracking, or phishing – Shall be penalized by imprisonment ranging from
9 three (3) years to six (6) years and a fine of not less than One million pesos
10 (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).
11

12
13 (n) Violation of Section 46 (a) (Illegal seizure of ICT) – shall be punished with
14 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
15 (PhP500,000.00) or both.
16

17 (o) Violation of Section 46 (b) (Aiding and abetting illegal seizure of ICT) – shall be
18 punished with imprisonment of *prision correccional* in its minimum period or a fine of not more
19 than Four hundred thousand pesos (PhP400,000.00) or both.
20

21 (p) Violation of Section 46 (c) (Arbitrary seizure of ICT) – Shall be punished with
22 imprisonment of *prision correccional* in its maximum period or a fine of not more than Five
23 hundred thousand pesos (PhP500,000.00) or both.
24

25 (q) Violation of Section 46 (d) (Instigating arbitrary seizure of ICT) – shall be punished
26 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
27 pesos (PhP500,000.00) or both.
28

29 (r) Violation of Section 47 (a) (i) (Copyright infringement) – any person infringing a
30 copyright shall be liable to pay to the copyright proprietor or his assigns or heirs such actual
31 damages, including legal costs and other expenses, as he may have incurred due to the
32 infringement as well as the profits the infringer may have made due to such infringement, and
33 in proving profits the plaintiff shall be required to prove sales only and the defendant shall be
34 required to prove every element of cost which he claims, or, in lieu of actual damages and
35 profits, such damages which to the court shall appear to be just and shall not be regarded as
36 penalty.
37

38 (s) Violation of Section 47 (a) (ii) (Plagiarism of copyleft) – The same penalty for a
39 violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this
40 Section.
41

42 (t) Violation of Section 47 (a) (iii) (Plagiarism of public domain content) – While this
43 constitutes infringement, it shall not be subject to the payment of damages or to any other
44 penalty.
45

46 (u) Violation of Section 47 (a) (iv) (Reverse engineering) – The same penalty for a
47 violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this

1 Section.

2

3 (v) Violation of Section 47 (b) (Piracy through ICT) – The same penalty for a violation of
4 Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

5

6 (w) Violation of Section 47 (c) (Cybersquatting) – The same penalty for a violation of
7 Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

8

9 (x) Violation of Section 47 (d) (Unreasonable restriction of device privileges) – shall be
10 punished with a fine of not less than one hundred thousand pesos (PhP 100,000.00) or more
11 than two million pesos (PhP 2,000,000.00).

12

13 (y) Violation of Section 48 (Fraud via ICT) – shall be punished with imprisonment of
14 *prision correccional* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a
15 maximum amount that is double the amount of damage incurred, whichever is higher, or both
16 imprisonment and fine.

17

18 (z) Violation of Section 49 (a) (ICT-enabled prostitution) – shall be punished with
19 imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos
20 (PhP200,000.00) up to a maximum amount of Five hundred thousand pesos (PhP500,000.00),
21 or both.

22

23 (aa) Violation of Section 49 (b) (ICT-enabled trafficking in persons) –

24

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

28

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

32

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

36

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

40

41

42 (ab) Violation of Section 50 (a) (ICT-enabled child prostitution) – Violation of Section 5 of
43 the Special Protection of Children Against Abuse, Exploitation and Discrimination Act through
44 ICT – *reclusion temporal* in its medium period to *reclusion perpetua*.

45

46 (ac) Violation of Section 50 (b) (ICT-enabled child trafficking) – Violation of Section 7 of
47 the Special Protection of Children Against Abuse, Exploitation and Discrimination Act through

1 ICT – *reclusion temporal* to *reclusion perpetua*. The penalty shall be imposed in its maximum
2 period when the victim is under twelve (12) years of age.

3
4 (ad) Violation of Section 51 (a) (Internet libel) – This shall only give rise to civil liability
5 and the amount shall be commensurate to the damages suffered.

6
7 (ae) Violation of Section 51 (b) (Internet hate speech) – This shall only give rise to civil
8 liability and the amount shall be commensurate to the damages suffered.

9
10 (af) Violation of Section 51 (c) (Internet child pornography) – Violation of the Anti-Child
11 Pornography Act through ICT – Shall be punished according to the provisions of Section 15 of
12 the Anti-Child Pornography Act of 2009 (RA 9775)

13
14 (ag) Violation of Section 51 (d) (Internet child abuse) – Violation of Section 9 of the
15 Special Protection of Children Against Abuse, Exploitation and Discrimination Act through ICT -
16 Shall be punished with imprisonment of *prision mayor* in its medium period. If the child used as
17 a performer, subject or seller/ distributor is below twelve (12) years of age, the penalty shall be
18 imposed in its maximum period.

19
20 (ah) Violation of Section 51 (e) (Internet expression inimical to the public interest) – This
21 shall only give rise to civil liability and the amount shall be commensurate to the damages
22 caused by the Internet expression.

23
24 (ai) Violation of Section 52 (b) (Cyberterrorism) – The commission of acts prohibited by
25 the Human Security Act of 2007, as amended, through or using devices, equipment, or physical
26 plants connected to the Internet or to telecommunications networks shall be penalized by the
27 applicable provisions of the Human Security Act of 2007, as amended.

28
29 (aj) Violation of Section 52 (c) (ICT-enabled financing of terrorism) – The commission of
30 acts prohibited by the Terrorism Financing Prevention and Suppression Act of 2012, as
31 amended, through or using devices, equipment, or physical plants connected to the Internet or
32 to telecommunications networks shall be penalized by the applicable provisions of the
33 Terrorism Financing Prevention and Suppression Act of 2012, as amended.

34
35 (ak) Violation of Section 52 (d) (Cyberespionage) – The commission of acts prohibited by
36 Article 117 of the Revised Penal Code, as amended, through or using devices, equipment, or
37 physical plants connected to the Internet or to telecommunications networks shall be penalized
38 by the applicable provisions of the Revised Penal Code, as amended.

39
40
41 *Section 61. Penalties for Violations of the Magna Carta for Philippine Internet Freedom Affecting*
42 *Critical Networks and Infrastructure.* – As prescribed by Section 52 (a) of this Act, a penalty one
43 degree higher shall be imposed on the specific violations of the Magna Carta for Philippine
44 Internet Freedom if committed against critical networks or information and communications
45 technology infrastructure.

1 *Section 62. Penalties for Other Violations of The Magna Carta for Philippine Internet Freedom. –*
2 A fine of not more than Five hundred thousand pesos (PhP 500,000.00) shall be imposed for a
3 violation of other sections of the law not covered by the preceding sections.

4
5
6 *Section 63. Penalties for Violations of The Magna Carta for Philippine Internet Freedom*
7 *Committed by a Public Official or Employee. –*

8
9 (a) Except as explicitly provided by the preceding sections, the next higher penalty shall
10 be imposed for a violation or negligence resulting in the violation of this Act if the violation or
11 negligence resulting in the violation is committed by a public official or employee in connection
12 with his duties.

13
14 (b) If the penalty imposed for the act or negligence resulting in the violation of this Act is
15 civil liability or civil liability and a fine, then an additional penalty of a fine of not less Two
16 hundred thousand pesos (PhP 200,000.00) but not more than Five hundred thousand pesos
17 (PhP 500,000.00) shall be imposed on the public official or employee.

18
19
20 *Section 64. Liability Under the Data Privacy Act, the Intellectual Property Code, the Optical*
21 *Media Act, the Anti-Child Pornography Act of 2009, the Special Protection of Children Against*
22 *Abuse, Exploitation and Discrimination Act, the Revised Penal Code, and Other Laws. –*

23
24 (a) A prosecution under this act shall bar any further prosecution of the act as a violation
25 of any provision of the Data Privacy Act, the Intellectual Property Code, the Optical Media Act,
26 the Anti-Child Pornography Act of 2009, the Anti-Trafficking in Persons Act, and other special
27 laws, except:

28
29 (i) if the act was performed through the use of a device, equipment, or physical
30 plant connected to the Internet or to telecommunications networks, or in connivance
31 with a third party with access to the same; and,

32
33 (ii) if the act could not have been performed through the use the said device,
34 equipment, or physical plant connected to the Internet or to telecommunications
35 networks, or the said third party with access to the same, and; c) if the act is part of a
36 series of or combination with other unlawful acts, these acts being performed without
37 the use of a device, equipment, or physical plant connected to the Internet or to
38 telecommunications networks, or in connivance with a third party with access to the
39 same.

40
41
42 (b) A prosecution under this act shall bar any further prosecution of the act as a
43 violation of the Revised Penal Code and other special laws, except:

44
45 (i) if the act was performed through the use of a device, equipment, or physical
46 plant connected to the Internet or to telecommunications networks, or in connivance
47 with a third party with access to the same;

1
2 (ii) if the violation could not have been performed through the use the said
3 device, equipment, or physical plant connected to the Internet or to
4 telecommunications networks, or the said third party with access to the same;

5
6 (iii) if the act involves the transmission of data through the Internet or
7 telecommunications networks; and

8
9 (iv) if the act is part of a series of or combination with other unlawful acts, these
10 acts being performed without the use of a device, equipment, or physical plant
11 connected to the Internet or to telecommunications networks, or in connivance with a
12 third party with access to the same.

13
14
15 *Section 65. Competent law enforcement agencies. –*

16
17 (a) *Department of Justice (DOJ).* – The Department of Justice may create an Office of
18 Cybercrime, which shall be designated as the central authority in the enforcement of this Act,
19 and all matters related to international mutual assistance and extradition, as provided for by
20 this Act.

21
22 (b) *National Bureau of Investigation (NBI).* – The National Bureau of Investigation may
23 create a Cybercrime Division, which shall be responsible for matters related to enforcement of
24 this Act. It shall cooperate with the division responsible for matters related with transnational
25 crime, other divisions, and other government agencies in the enforcement of this Act.

26
27 (c) *Philippine National Police (PNP).* – The Criminal Investigation and Detection Group
28 (CIDG) of the Philippine National Police may create a Cybercrime Office, which shall be
29 responsible for matters related to enforcement of this Act. The PNP shall, within the extent
30 practicable, establish cybercrime desks in police stations, and shall cooperate with other
31 government agencies in the enforcement of this Act.

32
33
34 *Section 66. Cybercrime courts. –*

35
36 (a) *Designation of Cybercrime Courts and Promulgation of Procedural Rules.* – The
37 Supreme Court shall designate the court or courts, manned by judges of competence, integrity,
38 probity and independence in the practice of law, and competent in matters related to the
39 Internet and information and communications technology, that will hear and resolve cases
40 brought under this Act and shall promulgate the rules of pleading, practice and procedure to
41 govern the proceedings brought under this Act.

42
43 (b) *Qualifications of the Presiding Judges of cybercrime courts.* – No person shall be
44 appointed a Presiding Judge of the Cybercrime Court unless he:

45
46 (i) is a natural-born citizen of the Philippines;

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

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

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

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

15
16
17 *Section 67. Jurisdiction of cybercrime courts. –*

18
19 (a) *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
23 (b) *Suit filed at the residence of the accused for criminal violations of the Magna Carta*
24 *for Philippine Internet Freedom.* – Except in cases that are extraterritorial, foreign, international,
25 and transnational in nature, all suits related to criminal violations of this Act shall be filed at the
26 cybercrime court having jurisdiction over the residence of the accused.

27
28 (c) *Suit filed at the cybercrime court agreed upon by the parties for civil violations of the*
29 *Magna Carta for Philippine Internet Freedom.* – Except in cases that are extraterritorial, foreign,
30 international, and transnational in nature, all suits related to civil violations of this Act shall be
31 filed at the cybercrime court agreed upon by the parties. Should the parties be unable to reach
32 an agreement, the Court of Appeals shall determine the cybercrime court that shall have
33 jurisdiction over the case.

34
35
36 *Section 68. Extraterritorial application of the Magna Carta for Philippine Internet Freedom. –*
37 Subject to the provision of an existing treaty of which the Philippines is a State Party, and to any
38 contrary provision of any law of preferential application, the provisions of this Act shall apply:

39
40 (a) to individual persons who, although physically outside the territorial limits of the
41 Philippines, commit, conspire or plot to commit any of the crimes defined and punished in this
42 Act inside the territorial limits of the Philippines;

43
44 (b) to individual persons who, although physically outside the territorial limits of the
45 Philippines, commit any of the said crimes on board a Philippine ship or aircraft;

46
47 (c) to individual persons who commit any of said crimes within any embassy, consulate,

1 or diplomatic premises belonging to or occupied by the Philippine government in an official
2 capacity;

3
4 (d) to individual persons who, although physically outside the territorial limits of the
5 Philippines, commit said crimes against Philippine citizens or persons of Philippine descent,
6 where their citizenship or ethnicity was a factor in the commission of the crime; and,

7
8 (e) to individual persons who, although physically outside the territorial limits of the
9 Philippines, commit said crimes directly against the Philippine government or critical
10 information and communications technology infrastructure in the Philippines.

11 12 13 **Part 9. Implementing Rules and Regulations.**

14 15 *Section 69. General Implementing Rules and Regulations for the Implementation of the Magna* 16 *Carta for Philippine Internet Freedom. –*

17
18 (a) The Secretary of Information and Communication Technology, the Commissioner of
19 the National Telecommunications Commission, the Commissioner of the National Data Privacy
20 Commission, and the Chief of the Telecommunications Office, or their duly authorized and
21 appointed delegates, an appointee from the academe or the business sector, and an appointee
22 from civil society or professional ICT-oriented organizations, shall be jointly responsible for the
23 creation of general implementing rules and regulations (IRR) of this Act. The Solicitor-General
24 shall participate to ensure that the IRR is not in conflict with this Act, with other laws, with
25 other IRRs of this Act, and with generally accepted principles of international human, civil, and
26 political rights.

27
28 (b) The General Implementing Rules and Regulations for the Implementation of the
29 Magna Carta for Philippine Internet Freedom shall be made public after its approval.

30
31 (c) The President shall implement the General Implementing Rules and Regulations for
32 the Implementation of the Magna Carta for Philippine Internet Freedom through the applicable
33 agencies and instrumentalities of the Executive.

34 35 36 *Section 70. Implementing Rules and Regulations for Information and Communications* 37 *Technology Infrastructure Development. –*

38
39 (a) The Secretary of Information and Communication Technology, the Secretary of
40 Finance, the Director-General of the National Economic and Development Authority, and the
41 Chairman of the Board of Investments, or their duly authorized and appointed delegates, an
42 appointee from civil society or professional ICT-oriented organizations, and an appointee from
43 the business sector shall be jointly responsible for the creation of implementing rules and
44 regulations (IRR) of this Act towards the development of information and communications
45 technology infrastructure. The Solicitor-General shall participate to ensure that the IRR is not in
46 conflict with this Act, with other laws, with other IRRs of this Act, and with generally accepted
47 principles of international human, civil, and political rights.

1
2 (b) The IRR for ICT Infrastructure Development shall be made public after its approval.
3

4 (c) The President shall implement the IRR for Information and Communications
5 Technology Infrastructure Development through the applicable agencies and instrumentalities
6 of the Executive.
7

8
9 *Section 71. Implementing Rules and Regulations for Cybercrime Law Enforcement. –*
10

11 (a) The Secretary of Information and Communication Technology, the Secretary of
12 Justice, the Secretary of Interior and Local Government, the Secretary of Social Welfare and
13 Development, the Secretary of Foreign Affairs, the Director-General of the National Bureau of
14 Investigation, and the Director-General of the Philippine National Police, or their duly
15 authorized and appointed delegates, an appointee from the academe, an appointee from civil
16 society, and an appointee from a professional ICT-oriented organization shall be jointly
17 responsible for the creation of implementing rules and regulations (IRR) of this Act towards
18 cybercrime and law enforcement. The Solicitor-General and the Chairman of the Commission
19 on Human Rights shall participate to ensure that the IRR is not in conflict with this Act, with
20 other laws, with other IRRs of this Act, and with generally accepted principles of international
21 human, civil, and political rights.
22

23 (b) The IRR for Cybercrime and Law Enforcement shall be made public after its approval.
24

25 (c) The President shall implement the IRR for Cybercrime and Law Enforcement through
26 the applicable agencies and instrumentalities of the Executive.
27

28
29 *Section 72. Implementing Rules and Regulations for Information and Communications*
30 *Technology Education, Training, and Human Resources. –*
31

32 (a) The Secretary of Information and Communication Technology, the Secretary of
33 Education, the Secretary of Science and Technology, the Commissioner of Higher Education, the
34 Director-General of the Technical Education and Skills Development Authority, the Head of the
35 National Telecommunications Training Institute, or their duly authorized and appointed
36 delegates, and an appointee from the academe shall be jointly responsible for the creation of
37 implementing rules and regulations (IRR) of this Act towards information and communications
38 technology education, training and human resources. The Solicitor-General and the Secretary of
39 Labor and Employment shall participate to ensure that the IRR is not in conflict with this Act,
40 with other laws, with other IRRs of this Act, and with generally accepted principles of
41 international human, civil, and political rights.
42

43 (b) The IRR for ICT Education, Training and Human Resources shall be made public after
44 its approval.
45

46 (c) The President shall implement the IRR for ICT Education, Training and Human
47 Resources through the applicable agencies and instrumentalities of the Executive.

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
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47

Section 73. Implementing Rules and Regulations for Information and Communications Technology Research and Development. –

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

(b) The IRR for ICT Research and Development shall be made public after its approval.

(c) The President shall implement the IRR for ICT Research and Development through the applicable agencies and instrumentalities of the Executive.

Section 74. Implementing Rules and Regulations for National Cyberdefense, Cyberintelligence, Counter-Cyberterrorism, and Counter-Cyberespionage. –

(a) The Secretary of National Defense, the Secretary of Interior and Local Government, or their duly authorized and appointed delegates, the Chief of Staff of the Armed Forces of the Philippines (AFP), the commanding general of the unit of the Philippine Air Force tasked with national cyberdefense, the commanding officer of the Intelligence Service, Armed Forces of the Philippines (ISAFP), the commanding officer of the Communication Electronics and Information Systems Service, Armed Forces of the Philippines (CEISSAFP), and the Director-General of the Philippine National Police shall be jointly responsible for the creation of implementing rules and regulations (IRR) of this Act towards ensuring national cyberdefense, cyberintelligence, counter-cyberterrorism, and counter-cyberespionage. The Secretary of Information and Communication Technology shall provide technical advice. The Solicitor-General and the Chairman of the Commission on Human Rights shall participate to ensure that the IRR is not in conflict with this Act, with other laws, with other IRRs of this Act, and with generally accepted principles of international human, civil, and political rights.

(b) The IRR for National Cyberdefense, Cyberintelligence, Counter-Cyberterrorism, and Counter-Cyberespionage shall be made public after its approval.

(c) Subject to the approval of the President, and subject to the advice and consent of the Joint Select Committee on Military and Intelligence Affairs of the House of Representatives and the Senate, the Secretary of National Defense, the Secretary of Interior and Local Government, or their duly authorized and appointed delegates, the Chief of Staff of the Armed Forces of the Philippines (AFP), the commanding general of the unit of the Philippine Air Force tasked with national cyberdefense, the commanding officer of the Intelligence Service, Armed Forces of the Philippines (ISAFP), the commanding officer of the Communication Electronics and Information

1 Systems Service, Armed Forces of the Philippines (CEISSAFP), and the Director-General of the
2 Philippine National Police shall prepare a National Cyberdefense and Cybersecurity Plan every
3 three years.

4
5 (d) The President shall have the power to implement the National Cyberdefense and
6 Cybersecurity Plan.

7
8 (e) The contents of the current and past National Cyberdefense and Cybersecurity Plans
9 shall be covered by executive privilege and shall be considered state secrets, and any
10 unauthorized disclosure shall be punishable to the fullest extent possible by relevant laws.
11

12 *Section 75. Implementing Rules and Regulations for the Provision of Free WIFI Access*

13 The Secretary of Information and Communication Technology, Secretary of Tourism and the
14 Secretary of Finance shall formulate and promulgate the implementing rules and regulations of
15 this Act towards the designation of selected public areas for free WIFI access.

16
17 *Section 76. Periodic Review of the Implementing Rules and Regulations of the Magna Carta for*
18 *Philippine Internet Freedom. –*

19
20 (a) Mandatory and periodic reviews of the implementing rules and regulations of the
21 Magna Carta for Philippine Internet Freedom shall be done by the offices designated by this Act
22 to create implementing rules and regulations. Such reviews shall be performed no less than
23 every three years and no more than every five years, to keep pace with technological
24 advancements and other changes.

25
26 (b) Periodic reviews of the implementing rules and regulations and the recommendation
27 of the improvement of the Magna Carta for Philippine Internet Freedom shall be done by the
28 offices designated by this Act to create implementing rules and regulations, to keep pace with
29 technological advancements and other changes.

30
31
32 **Part 10. Final Provisions.**

33
34 *Section 76. Appointment of the Secretary of Information and Communications Technology. –*
35 Subject to confirmation by the Commission on Appointments, the President shall appoint the
36 Secretary of Information and Communications Technology within 30 days of the effectivity of
37 this Act.

38
39
40 *Section 77. Release of Initial Appropriations. –* Subject to government budgetary and audit
41 procedures, the Department of Budget and Management shall release appropriations to the
42 Secretary of Information and Communications Technology for purposes of implementing this
43 Act within 30 days of his appointment.
44
45

1 *Section 78. Preparation of Implementing Rules and Regulations.* – Within 90 days of the release
2 of initial appropriations, implementing rules and regulations shall have been prepared and
3 approved. The National Cyberdefense and Cybersecurity Plan shall be prepared, approved, and
4 implemented within 90 days of the approval of the implementing rules and regulations.

5
6
7 *Section 79. Compliance of Government ICT Infrastructure and Critical Networks, Data, and*
8 *Internet Infrastructure.* –

9
10 (a) Within 180 days of the approval of the implementing rules and regulations,
11 government agencies and instrumentalities shall have secured their private network and data
12 infrastructure. Penalties as prescribed by this Act shall be imposed for noncompliance.

13
14 (b) Within 270 days of the approval of the implementing rules and regulations,
15 government agencies and instrumentalities shall have secured their public network, data, and
16 Internet infrastructure. Penalties as prescribed by this Act shall be imposed for noncompliance.

17
18 (c) Within one (1) year of the approval of the implementing rules and regulations, all
19 Internet service providers, Internet exchanges, Internet data centers, Internet gateway
20 facilities, telecommunications entities, and persons providing Internet connection, network, or
21 data transmission services shall have met the minimum standards of privacy and security for
22 their private and public network, data, and Internet infrastructure. Penalties as prescribed by
23 this Act shall be imposed for noncompliance.

24
25 (d) Within 90 days of the approval of the implementing rules and regulations, all
26 Internet service providers, Internet exchanges, Internet data centers, Internet gateway
27 facilities, telecommunications entities, and persons providing Internet connection, network, or
28 data transmission services shall have met the minimum standards of interconnectivity and
29 interoperability of their information and communications technology infrastructure.
30 Administrative penalties shall be prescribed for noncompliance.

31
32 (e) Within 180 days of the approval of the implementing rules and regulations, all
33 Internet service providers, Internet exchanges, Internet data centers, Internet gateway
34 facilities, telecommunications entities, and persons providing Internet connection, network, or
35 data transmission services shall have met the minimum standards of service quality.
36 Administrative penalties shall be prescribed for noncompliance.

37
38
39 *Section 80. Public Information Campaign for the Magna Carta for Philippine Internet Freedom*
40 *and its Implementing Rules and Regulations.* –

41
42 (a) The Office of the President, the Presidential Communications Development and
43 Strategic Planning Office or its successor agency, the Philippine Information Agency or its
44 successor agency, and the Department of Interior and Local Government through the
45 information offices of local government units, shall be jointly responsible for information
46 campaigns to ensure nationwide awareness of the Magna Carta for Philippine Internet Freedom
47 and its implementing rules and regulations.

1
2 (b) The Department of Education and the Department of Social Welfare and
3 Development may provide age-appropriate information campaigns in schools to ensure
4 nationwide awareness of the *Magna Carta for Philippine Internet Freedom*, its Implementing
5 rules and regulations, and the safe use of the Internet and information and communications
6 technology for children of school age and for out-of-school youths.
7

8
9 *Section 81. Initial funding requirements. –*

10
11 (a) DICT – An initial appropriation of fifteen million pesos (PHP 15,000,000) shall be
12 drawn from the national government for purposes of establishment and operation of the DICT,
13 exclusive of the existing appropriations of its subordinate agencies, which shall accrue to the
14 DICT budget.
15

16 (b) DOJ – The initial funding requirements for the implementation of this Act of the DOJ
17 shall be charged against the current appropriations of the DOJ.
18

19 (c) NBI – The initial funding requirements for the implementation of this Act of the NBI
20 shall be charged against the current appropriations of the NBI.
21

22 (d) PNP – The initial funding requirements for the implementation of this Act of the PNP
23 shall be charged against the current appropriations of the PNP.
24

25 (e) IRR – An initial appropriation of five million pesos (PHP 5,000,000), to be disbursed
26 by the Secretary of Information and Communications Technology, shall be drawn from the
27 national government for purposes of the preparation of the Implementing Rules and
28 Regulations of this Act.
29

30 (f) PIA – An appropriation of five million pesos (PHP 5,000,000) may be drawn from the
31 national government for purposes of the information dissemination campaign on this Act by
32 the PIA.
33

34 (g) Other agencies – The initial funding requirements for the implementation of this Act
35 by other agencies shall be charged against the current appropriations of the respective
36 agencies.
37

38
39 *Section 82. Succeeding appropriations. –* Such sums as may be necessary for the
40 implementation of this Act shall be included in the agencies' yearly budgets under the General
41 Appropriations Act.
42

43
44 *Section 83. Separability clause. –* If any provision or part hereof is held invalid or
45 unconstitutional, the remainder of the law or the provisions not otherwise affected shall
46 remain valid and subsisting.
47

1
2
3
4
5
6
7
8
9

Section 84. Repealing clause – Any law, presidential decree or issuance, executive order, letter of instruction, administrative order, rule, or regulation contrary to, or inconsistent with, the provisions of this Act is hereby repealed, modified, or amended accordingly.

Section 85. Effectivity clause. – This Act shall take effect fifteen (15) days after its online publication in the Official Gazette. Within seven (7) days after its online publication, this Act shall be published on (2) newspapers of general circulation.