

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



Senate
Office of the Secretary

14 MAY -7 P1:28

SENATE
S.B. No. 2214

RECEIVED

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

AN ACT
INSTITUTIONALIZING THE ESTABLISHMENT OF THE PHILIPPINE BIG DATA CENTER

EXPLANATORY NOTE

The world we live in is in constant change. With these changes, more data are being collected, stored, accessed, analyzed, re-analyzed and disseminated.

Big Data has risen as an alternative source of information. It refers to datasets whose volume is beyond the ability of typical database software tools to capture, store, manage and analyze within a tolerable elapsed period of time.

Today, Big Data from information-sensing smart phones, social media and the Internet, remote sensing and climate sensors is more available and accessible.

Thus, an establishment of a technology center that facilitates Big Data is proposed in order for policy and services to be more relevant to the changing needs of the people.

With the help of the Philippine Big Data Center, disaster response teams will be armed by important information and other data needed during emergency situations and calamities.

The Bill proposes an infrastructure where Big Data is utilized for research and development, and invention and innovation.

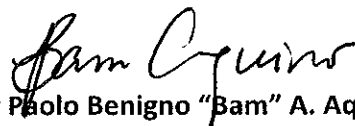
The Center will develop a range of standards to use software and tools for analytics on massive amounts of data being generated from the use of the Internet and other technology.

The Center will also be responsible for disseminating and communicating the knowledge gained from its research activities to its stakeholders in both the public and private sectors. The analysis from Big Data will help policy makers to be more responsive to the needs of the public.

Furthermore, the Center will respect the right to privacy of the Filipinos, ensuring data anonymity, establish opt-in permissions and uphold transparency in its data analytics processes.

The passage of this bill will pioneer and institutionalize a technological breakthrough that will support the public and private sectors. It boosts the efforts of the State for more advanced, sustained and inclusive developmental progress.

In view of the foregoing, the approval of this bill is earnestly sought.

A handwritten signature in black ink, appearing to read "Bam Aquino". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Senator Paolo Benigno "Bam" A. Aquino IV



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

14 MAY -7 P1:28

SENATE
S.B. No. 2214

RECEIVED BY: *[Signature]*

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

AN ACT
INSTITUTIONALIZING THE ESTABLISHMENT OF THE PHILIPPINE BIG DATA CENTER

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

1 **SECTION 1. Short Title.** - This Act shall be known as the "Big Data Act of 2014".

2 **SECTION 2. Declaration of Policy.**-

3 The State recognizes the vital role of communication and information in nation-
4 building. Access to official records, and to documents and papers pertaining to official
5 acts, transactions, or decisions as well as to government research data as basis for policy
6 development, shall be afforded the citizen, subject to such limitations as may be
7 provided by law. Further, the State also recognizes that Science and Technology are
8 essential for national development and progress. The State shall give priority to research
9 and development, invention, innovation, and their utilization; and to science and
10 technology education, training, and services.

11 In line with these basic constitutional guarantees it shall be the policy of the
12 state to revolutionize government's efforts in promoting and maintaining an efficient
13 government statistical system that provides adequate, accessible, consistent, reliable
14 and timely data. The establishment of the Big Data Center shall also ensure that existing
15 government data are also maximized as supported by the Open Data Philippines
16 program pursuant to E.O. 43 or the overall governance framework.

17 The Big Data Center shall pave the way that will allow our country to make
18 strides in government statistical services that adheres to the ideals and vision of the
19 government in serving the interest of society and the welfare of our nation.

20 **SECTION 3. Definition of Terms.** - As used in this Act, the following terms are defined as
21 follows:

22 **(a) Big Data-** refers to datasets whose volume is beyond the ability of typical
23 database software tools to capture, store, manage and analyze within a tolerable
24 elapsed period of time.

25 **(b) Crowdsorce-** process of soliciting information, ideas or feedback from a
26 large group of people.

1 **(c) Data Anonymity-** process of ensuring that personal information cannot be
2 linked to a particular unique name of a citizen.

3 **(d) Issue -** a fundamental problem with broad economic and scientific impact,
4 whose solution will require the application of high-performance computing resources.

5 **(e) Opt-In-** Permission given by the individual to volunteer particular personal
6 data for Big Data analytics.

7 **SECTION 4. Establishment of the Center.-** There shall be established a Big Data Center
8 that shall be attached to the Philippine Statistical Research and Training Institute
9 (PSRTI). The National Big Data Center in the Philippines shall be hereinafter referred to
10 as the “Big Data Center” (BDC).

11 **SECTION 5. Powers and Functions. -** The Big Data Center shall have the following powers
12 and functions:

13 a. Develop a Big Data research program that will address emerging
14 development issues;

15 b. Build partnerships with both public sector agencies and private sector
16 agencies for the conduct of research that examines digital data sources
17 for producing alternative statistics to meet information requirements for
18 socio-economic development goals;

19 c. Provide government and development partners with valuable
20 information generated from alternative near real time data sources that
21 shall complement statistics generated by the Philippine Statistics
22 Authority (PSA) and other statistics producing agencies in the Philippine
23 Statistical System;

24 d. Establish and administer capacity building activities on Big Data analytics
25 for various partner institutions.

26 **SECTION 6. Composition. -** The Big Data Center shall be composed of the Office of the
27 Director and the Offices of the following Divisions: a) *Open Data Division*; b)
28 *Partnerships Division*; c) *Data Analytics and Storage Division*; and, d) *Privacy and Data*
29 *Anonymity Division*

30 **SECTION 7. Office of the Director. –** The Office of the Director shall consist of the
31 Director and his or her immediate staff.

32 **SECTION 8. Director. -** The Director shall be appointed by the PSRTI Board of Directors.

33 The Director shall have the following powers and functions:

34 a. Ensure the development and regular updating of the Big Data Laboratory
35 Research Program;

36 b. Implement the Big Data Program and monitor the progress of the
37 research activities of the Center;

- 1 c. Convene quarterly the Technical Advisory Committee on Big Data, Open
2 Data Division, Partnerships Division, Data Analytics and Storage Division
3 and the Privacy and Data Anonymity Division as defined in this Act for an
4 independent assessment of the research activities and the Big Data
5 Program;
- 6 d. Submit to the President of PSRTI an Annual Report on the
7 accomplishments of the Center;

8 **SECTION 9. *Technical Advisory Committee on Big Data.*** -

9 A Technical Advisory Committee on Big Data shall be created in order to provide
10 guidance to the Big Data Center and PSRTI on the program and activities of the Center.
11 TAC members shall have a tenure of three (3) years and shall be composed of an
12 appointive chair and four appointive members who are experts from the following
13 disciplinary groups:

- 14 a. Social Science (anthropology, economics, political science, psychology
15 and sociology);
- 16 b. Natural and Geological Science;
- 17 c. Statistics;
- 18 d. Computer Science;
- 19 e. Information Technology;

20 **SECTION 10. *Open Data Division.*** -

21 An Open Data Division shall be created to perform the following functions:

- 22 a. Fully utilize and maximize existing Open Data from different government
23 agencies for data analytics to aid in the development of the country;
- 24 b. Provide recommendations to different agencies on what other data shall
25 be provided by the government in order to come up with a more
26 comprehensive set of information available for data analytics;
- 27 c. Shall have the power to demand information deemed as Open Data from
28 government agencies;
- 29 d. Ensure that the Big Data Center runs parallel with the Open Data
30 initiative by amalgamating existing government information and
31 providing data analytics towards the discovery of new and innovative
32 solutions for government services;
- 33 e. Provide, publish and make available for download in universally accepted
34 format such as, but not limited to plain text, comma-separated values
35 spreadsheet, or open standard multimedia data readily verifiable through
36 a checksum standard as determined by the Internet Engineering Task
37 Force or similar globally recognized standards organization;

- 1 f. Work towards the transparency not just of information deemed public by
2 Open Data standards but openness in the processes within the Big Data
3 Center;

4 **SECTION 11. Partnership Division. -**

5 A Partnership Division shall be created to perform the following functions:

- 6 a. Synergize with entities engaged in the operation and/or provision of
7 information and communications, telecommunications and other multi-
8 media infrastructures that include, but are not limited to, social media,
9 Internet search engines, remote sensing and other available sources of
10 data from existing information and communications technology tools;
- 11 b. Collaborate with data partners by coming up with an agreement that
12 shall allow mobile companies, internet companies to share the data they
13 have that can be used for the analysis in the Big Data Center;
- 14 c. Establish confidentiality, privacy, process of analytics and ownership of
15 information in the Big Data holdings to partners;
- 16 d. For the PSRTI and BDC to workout an agreement for research that will
17 provide technical/statistical services to the partners in order to test new
18 tools and eventually mainstream approaches for the application of the
19 new digital data sources for the industries;

20 **SECTION 12. Data Analytics and Storage Division. -**

21 A Data Analytics and Storage division shall be created to perform the following
22 functions:

- 23 a. Inspect, clean, transform and model data with the goal of discovering
24 useful information, suggesting conclusions and supporting decision
25 making;
- 26 b. Determine the appropriate data analysis technique that can help not just
27 in purely descriptive purposes but also predictive purposes as may be
28 deemed necessary;
- 29 c. Work towards efficiency in data storage utilizations by using less storage
30 and space that can house the same amount of data and can ultimately
31 reduce capital and operating costs;
- 32 d. Provide for, but not limited to Operating Systems Security Specialists,
33 Applications Security Specialists as well as Network Security Specialists to
34 ensure the integrity of data and infrastructure;

35 **SECTION 13. Privacy and Data Anonymity Division. -**

36 A Privacy and Data Anonymity Committee shall be created to ensure at all times
37 the confidentiality of any personal information that comes to its knowledge and
38 possession. The Committee shall ensure that the following standards on privacy shall be
39 followed:

- 1 a. Ensure protection and security of any personal information that comes to
2 its knowledge and possession;
- 3 b. Anonymize personal data even before going through the processing of
4 data analytics. The data used and processed shall be in the form of
5 anonymized data where the information gathered and processed may
6 not be traced to a particular unique name of a citizen;
- 7 c. Establish opt-in permissions or a more secure permission system given
8 the particular for stakeholders whose data shall be used;
- 9 d. Ensure that individuals or organizations are held accountable for
10 protecting, securing and using personal data;
- 11 e. Bring to authorities offenses to the violations defined in this act;
- 12 f. Ensure transparency and openness in the processes within the Big Data
13 Center particularly in data analytics;
- 14 g. Implement compliance measures for privacy standards as well as the
15 adherence to the Data Privacy Act and other relevant privacy rules set by
16 law;

17 The use and availability of accurate and complete information whenever it is
18 required shall be limited to authorized users and shall be subject to the provisions of
19 Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012,
20 Commonwealth Act No. 591, otherwise known as An Act Creating the Bureau of Census
21 and Statistic and further governed by Section 26 of RA 10625 otherwise known as the
22 Philippine Statistical Act of 2013 and other applicable laws. Nothing in this Act shall
23 be construed as to have amended or repealed Republic Act No. 1405, otherwise known as
24 the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign
25 Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit
26 Information System Act (CISA).

27 **SECTION 14. Violations on Data Privacy. -**

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

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

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

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

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

29 **Section 15. Violation of Data Security.** –

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

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

1 unauthorized modification of intellectual property published on the
2 Internet or on other networks, shall be presumed to be malicious.

3 c. *Phishing.* –

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

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

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

22 **Section 16. *Illegal and Arbitrary Seizure.* –**

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

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

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

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

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

16 **Section 17. Penalties.** -

17 a. Violation of Unauthorized access – Shall be punished with imprisonment
18 ranging from one (1) year to three (3) years and a fine of not less than Five
19 hundred thousand pesos (Php500,000.00) but not more than Two million
20 pesos (Php2,000,000.00).

21 b. Violation of Unauthorized modification - Shall be punished with
22 imprisonment ranging from one (1) year to three (3) years and a fine of not
23 less than Five hundred thousand pesos (Php500,000.00) but not more than
24 Two million pesos (Php2,000,000.00).

25 c. Violation of Unauthorized granting of privileges - Shall be punished with
26 imprisonment ranging from one (1) year to three (3) years and a fine of not
27 less than Five hundred thousand pesos (Php500,000.00) but not more than
28 Two million pesos (Php2,000,000.00).

29 d. Violation of Unauthorized disclosure - imprisonment ranging from three
30 (3) years to five (5) years and a fine of not less than Five hundred thousand
31 pesos (Php500,000.00) but not more than Two million pesos
32 (Php2,000,000.00).

33 e. Violation of Data Privacy Act through ICT –

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

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

44 iii. Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal

- 1 Information Due to Negligence) through ICT – imprisonment ranging
2 from one (1) year to three (3) years and a fine of not less than Five
3 hundred thousand pesos (Php500,000.00) but not more than Two
4 million pesos (Php2,000,000.00).
- 5 iv. Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
6 Personal Information Due to Negligence) through ICT – imprisonment
7 ranging from three (3) years to six (6) years and a fine of not less than
8 Five hundred thousand pesos (Php500,000.00) but not more than
9 Four million pesos (Php4,000,000.00).
- 10 v. Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal
11 of Personal Information) through ICT – imprisonment ranging from six
12 (6) months to two (2) years and a fine of not less than One hundred
13 thousand pesos (Php100,000.00) but not more than Five hundred
14 thousand pesos (Php500,000.00).
- 15 vi. Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal
16 of Sensitive Personal Information) through ICT – imprisonment
17 ranging from one (1) year to three (3) years and a fine of not less than
18 One hundred thousand pesos (Php100,000.00) but not more than
19 One million pesos (Php1,000,000.00).
- 20 vii. Violation of Section 28 (a) of the Data Privacy Act (Processing of
21 Personal Information for Unauthorized Purposes) through ICT –
22 imprisonment ranging from one (1) year and six (6) months to five (5)
23 years and a fine of not less than Five hundred thousand pesos
24 (Php500,000.00) but not more than One million pesos
25 (Php1,000,000.00).
- 26 viii. Violation of Section 28 (b) of the Data Privacy Act (Processing of
27 Sensitive Personal Information for Unauthorized Purposes) through
28 ICT – imprisonment ranging from two (2) years to seven (7) years and
29 a fine of not less than Five hundred thousand pesos (Php500,000.00)
30 but not more than Two million pesos (Php2,000,000.00).
- 31 ix. Violation of Section 30 of the Data Privacy Act (Concealment of
32 Security Breaches Involving Sensitive Personal Information) through
33 ICT – imprisonment of one (1) year and six (6) months to five (5) years
34 and a fine of not less than Five hundred thousand pesos
35 (Php500,000.00) but not more than One million pesos
36 (Php1,000,000.00).
- 37 x. Violation of Section 33 of the Data Privacy Act (Combination or Series
38 of Acts) through ICT – imprisonment ranging from three (3) years to
39 six (6) years and a fine of not less than One million pesos
40 (Php1,000,000.00) but not more than Five million pesos
41 (Php5,000,000.00).
- 42 f. Violation of Hacking – imprisonment ranging from one (1) year to three
43 (3) years and a fine of not less than Five hundred thousand pesos
44 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

- 1 g. Violation of Cracking – imprisonment ranging from one (1) year to three
2 (3) years and a fine of not less than Five hundred thousand pesos
3 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).
- 4 h. Violation of Phishing – imprisonment ranging from one (1) year and six
5 (6) months to five (5) years and a fine of not less than Five hundred
6 thousand pesos (Php500,000.00) but not more than One million pesos
7 (Php1,000,000.00).
- 8 i. Violation of Data Privacy Act (with hacking, cracking, or phishing) –
- 9 i. Violation of Section 25 (a) of the Data Privacy Act (Unauthorized
10 Processing of Personal Information) with hacking, cracking, or
11 phishing – shall be penalized by imprisonment ranging from one (1)
12 year to three (3) years and a fine of not less than Five hundred
13 thousand pesos (Php500,000.00) but not more than Two million
14 pesos (Php2,000,000.00).
- 15 ii. Violation of Section 25 (b) of the Data Privacy Act (Unauthorized
16 Processing of Sensitive Personal Information) with hacking, cracking,
17 or phishing – shall be penalized by imprisonment ranging from three
18 (3) years to six (6) years and a fine of not less than Five hundred
19 thousand pesos (Php500,000.00) but not more than Four million
20 pesos (Php4,000,000.00).
- 21 iii. Violation of Section 26 (a) of the Data Privacy Act (Accessing
22 Personal Information Due to Negligence) with hacking, cracking, or
23 phishing – shall be penalized by imprisonment ranging from one (1)
24 year to three (3) years and a fine of not less than Five hundred
25 thousand pesos (Php500,000.00) but not more than Two million
26 pesos (Php2,000,000.00).
- 27 iv. Violation of Section 26 (b) of the Data Privacy Act (Accessing
28 Sensitive Personal Information Due to Negligence) with hacking,
29 cracking, or phishing – shall be penalized by imprisonment ranging
30 from three (3) years to six (6) years and a fine of not less than Five
31 hundred thousand pesos (Php500,000.00) but not more than Four
32 million pesos (Php4,000,000.00).
- 33 v. Violation of Section 27 (a) of the Data Privacy Act (Improper
34 Disposal of Personal Information) with hacking, cracking, or phishing –
35 shall be penalized by imprisonment ranging from six (6) months to
36 two (2) years and a fine of not less than One hundred thousand pesos
37 (Php100,000.00) but not more than Five hundred thousand pesos
38 (Php500,000.00).
- 39 vi. Violation of Section 27 (b) of the Data Privacy Act (Improper
40 Disposal of Sensitive Personal Information) with hacking, cracking, or
41 phishing – shall be penalized by imprisonment ranging from one (1)
42 year to three (3) years and a fine of not less than One hundred
43 thousand pesos (Php100,000.00) but not more than One million
44 pesos (Php1,000,000.00).

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

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

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

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

24 j. Violation of Illegal seizure of ICT– shall be punished with imprisonment of
25 *prision correccional* or a fine of not more than Five hundred thousand
26 pesos (PhP500,000.00) or both.

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

30 l. Violation of Arbitrary seizure of ICT– Shall be punished with imprisonment
31 of *prision correccional* in its maximum period or a fine of not more than
32 Five hundred thousand pesos (PhP500,000.00) or both.

33 m. Violation of Instigating arbitrary seizure of ICT – shall be punished with
34 imprisonment of *prision correccional* or a fine of not more than Five
35 hundred thousand pesos (PhP500,000.00) or both.

36 **SECTION 18. Ownership of Data.-**

37 Data that comes to the possession and knowledge of the Big Data Center shall be
38 deemed as property of public dominion. Unprocessed data that comes to the possession
39 of the Center shall be considered property of public dominion for public service where
40 its use is limited to authorized persons in government. Processed data of the Center
41 which shall take the form of official reports and studies shall be deemed as property of
42 public dominion for public use such that it is intended for the use of anybody. Data
43 partners may define the ownership of data based on the partnership agreements with
44 the government taking into consideration the context of the need of such data.

1 **SECTION 19. *Funding.*** -

2 There shall be included in the budget of NEDA under the annual General
3 Appropriations Act an amount of Two Hundred Million Pesos (P200,000,000.00) as the
4 initial operating fund of the Big Data Center.

5 After the first year of implementation, such sums as may be necessary to fund
6 the Big Data Center shall be included in the budget of NEDA under the annual General
7 Appropriations Act.

8 Contributions, donations, bequests, grants and loans from domestic and/or
9 foreign sources, government appropriations and other incomes accruing from the
10 operations shall be allowed to be received and added to the funds and to be utilized
11 exclusively by the Center.

12 **SECTION 20. *Repealing Clause.*** - All laws, decrees, executive orders, rules and
13 regulations and other issuances or parts thereof which are inconsistent with this Act are
14 hereby repealed, amended or modified accordingly.

15 **SECTION 21. *Separability Clause.*** - If any provision of this Act shall be declared
16 unconstitutional or invalid, the other provisions not otherwise affected shall remain in
17 full force and effect.

18 **SECTION 22. *Effectivity Clause.*** - This Act shall take effect after fifteen (15) days from its
19 publication in at least two (2) newspapers of general circulation.

20 Approved,