

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



'16 JUL 20 P4:03

SENATE
S.B. No. 688

RECEIVED BY:

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, 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.

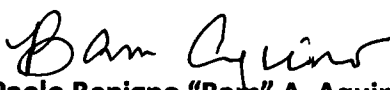
The Center will develop a range of standards to use software and tools for analytics on massive amounts of data being generated from the use of the Internet and other technology.

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.

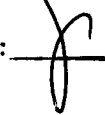

Senator Paolo Benigno "Bam" A. Aquino IV



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

'16 JUL 20 P 4:03

SENATE
S.B. No. 688

RECEIVED BY: 

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. Title.** - This Act shall be known as the "*Big Data Act*".

2 **SEC. 2. Declaration of Policy.** - The State recognizes the vital role of
3 communication and information in nation-building. Access to official records, and to
4 documents and papers pertaining to official acts, transactions, or decisions as well as
5 to government research data as basis for policy development, shall be afforded the
6 citizen, subject to such limitations as may be provided by law. Further, the State also
7 recognizes that Science and Technology are essential for national development and
8 progress. The State shall give priority to research and development, invention,
9 innovation, and their utilization; and to science and technology education, training,
10 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,
14 reliable and timely data. The establishment of the Big Data Center shall also ensure
15 that existing government data are also maximized as supported by the Open Data
16 Philippines 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 **SEC. 3. Definition of Terms.** - As used in this Act, the following terms shall
21 mean:

- 1 a. *Big Data*- datasets, whose volume is beyond the ability of typical database
2 software tools to capture, store, manage and analyze within a tolerable
3 elapsed period of time.
- 4 b. *Crowdsourcing*- the process of soliciting information, ideas or feedback from a
5 large group of people.
- 6 c. *Data Anonymity*- process of ensuring that personal information cannot be
7 linked to a particular unique name of a citizen.
- 8 d. *Issue* - a fundamental problem with broad economic and scientific impact,
9 whose solution will require the application of high-performance computing
10 resources.
- 11 e. *Opt-In*- Permission given by the individual to volunteer particular personal
12 data for Big Data analytics.

13 **SEC. 4. *Establishment of the Center.*** - There shall be established a Big Data
14 Center that shall be attached to the Philippine Statistical Research and Training
15 Institute (PSRTI). The National Big Data Center in the Philippines shall be hereinafter
16 referred to as the "Big Data Center" (BDC).

17 **SEC. 5. *Powers and Functions.*** - The Big Data Center shall have the following
18 powers and functions:

- 19 a. Develop a Big Data research program that will address emerging
20 development issues;
- 21 b. Build partnerships with both public sector agencies and private sector
22 agencies for the conduct of research that examines digital data
23 sources for producing alternative statistics to meet information
24 requirements for socio-economic development goals;
- 25 c. Provide government and development partners with valuable
26 information generated from alternative near real time data sources
27 that shall complement statistics generated by the Philippine Statistics
28 Authority (PSA) and other statistics producing agencies in the
29 Philippine Statistical System;
- 30 d. Establish and administer capacity building activities on Big Data
31 analytics for various partner institutions.

32 **SEC. 6. *Composition.*** - The Big Data Center shall be composed of the Office of
33 the Director and the Offices of the following Divisions: a) *Open Data Division*; b)
34 *Partnerships Division*; c) *Data Analytics and Storage Division*; and, d) *Privacy and*
35 *Data Anonymity Division*.

36 **SEC. 7. *Office of the Director.*** - The Office of the Director shall consist of the
37 Director and his or her immediate staff.

1 **SEC. 8. Director.** - The Director shall be appointed by the PSRTI Board of
2 Directors.

3 The Director shall have the following powers and functions:

- 4 a. Ensure the development and regular updating of the Big Data
5 Laboratory Research Program;
- 6 b. Implement the Big Data Program and monitor the progress of the
7 research activities of the Center;
- 8 c. Convene quarterly the Technical Advisory Committee on Big Data,
9 Open Data Division, Partnerships Division, Data Analytics and Storage
10 Division and the Privacy and Data Anonymity Division as defined in
11 this Act for an independent assessment of the research activities and
12 the Big Data Program;
- 13 d. Submit to the President of PSRTI an Annual Report on the
14 accomplishments of the Center;

15 **SEC. 9. Technical Advisory Committee on Big Data.** - A Technical Advisory
16 Committee on Big Data shall be created in order to provide guidance to the Big Data
17 Center and PSRTI on the program and activities of the Center. TAC members shall
18 have a tenure of three (3) years and shall be composed of an appointive chair and
19 four appointive members who are experts from the following disciplinary groups:

- 20 a. Social Science (anthropology, economics, political science, psychology
21 and sociology);
- 22 b. Natural and Geological Science;
- 23 c. Statistics;
- 24 d. Computer Science; and
- 25 e. Information Technology;

26 **SEC. 10. Open Data Division.** - An Open Data Division shall be created to
27 perform the following functions:

- 28 a. Fully utilize and maximize existing Open Data from different
29 government agencies for data analytics to aid in the development of
30 the country;

- 1 b. Provide recommendations to different agencies on what other data
2 shall be provided by the government in order to come up with a more
3 comprehensive set of information available for data analytics;
- 4 c. Shall have the power to demand information deemed as Open Data
5 from government agencies;
- 6 d. Ensure that the Big Data Center runs parallel with the Open Data
7 initiative by amalgamating existing government information and
8 providing data analytics towards the discovery of new and innovative
9 solutions for government services;
- 10 e. Provide, publish and make available for download in universally
11 accepted formats such as, but not limited to plain text, comma-
12 separated values spreadsheet, or open standard multimedia data
13 readily verifiable through a checksum standard as determined by the
14 Internet Engineering Task Force or similar globally recognized
15 standards organization; and
- 16 f. Work towards the transparency not just of information deemed
17 public by Open Data standards but openness in the processes within
18 the Big Data Center.

19 **SEC. 11. Partnership Division.** - A Partnership Division shall be
20 created to perform the following functions:

- 21 a. Synergize with entities engaged in the operation and/or provision of
22 information and communications, telecommunications and other
23 multi-media infrastructures that include, but are not limited to, social
24 media, Internet search engines, remote sensing and other available
25 sources of data from existing information and communications
26 technology tools;
- 27 b. Collaborate with data partners by coming up with an agreement that
28 shall allow mobile companies, internet companies to share the data
29 they have that can be used for the analysis in the Big Data Center;
- 30 c. Establish confidentiality, privacy, process of analytics and ownership
31 of information in the Big Data holdings to partners; and
- 32 d. For the PSRTI and BDC to workout an agreement for research that will
33 provide technical/statistical services to the partners in order to test
34 new tools and eventually mainstream approaches for the application
35 of the new digital data sources for the industries;

36 **SEC. 12. Data Analytics and Storage Division.** - A Data Analytics and Storage
37 Division shall be created to perform the following functions.

- 1 a. Inspect, clean, transform and model data with the goal of discovering
2 useful information, suggesting conclusions and supporting decision
3 making;
- 4 b. Determine the appropriate data analysis technique that can help not
5 just in purely descriptive purposes but also predictive purposes as
6 may be deemed necessary;
- 7 c. Work towards efficiency in data storage utilizations by using less
8 storage and space that can house the same amount of data and can
9 ultimately reduce capital and operating costs; and
- 10 d. Provide for, but not limited to Operating Systems Security Specialists,
11 Applications Security Specialists as well as Network Security
12 Specialists to ensure the integrity of data and infrastructure;

13 **SEC. 13. Privacy and Data Anonymity Division.** – A Privacy and Data
14 Anonymity Committee shall be created to ensure at all times the confidentiality of any
15 personal information that comes to its knowledge and possession. The Committee
16 shall ensure that the following standards on privacy shall be followed:

- 17 a. Ensure protection and security of any personal information that
18 comes to its knowledge and possession;
- 19 b. Anonymize personal data even before going through the processing of
20 data analytics. The data used and processed shall be in the form of
21 anonymized data where the information gathered and processed may
22 not be traced to a particular unique name of a citizen;
- 23 c. Establish opt-in permissions or a more secure permission system
24 given the particular for stakeholders whose data shall be used;
- 25 d. Ensure that individuals or organizations are held accountable for
26 protecting, securing and using personal data;
- 27 e. Bring to authorities offenses to the violations defined in this Act;
- 28 f. Ensure transparency and openness in the processes within the Big
29 Data Center particularly in data analytics; and
- 30 g. Implement compliance measures for privacy standards as well as the
31 adherence to the Data Privacy Act and other relevant privacy rules set
32 by law;

33 The use and availability of accurate and complete information whenever it is
34 required shall be limited to authorized users and shall be subject to the provisions of

1 Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012,
2 Commonwealth Act No. 591, otherwise known as An Act Creating the Bureau of
3 Census and Statistic and further governed by Section 26 of RA 10625 otherwise known
4 as the Philippine Statistical Act of 2013 and other applicable laws. Nothing in this
5 Act shall be construed as to have amended or repealed Republic Act No. 1405,
6 otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426,
7 otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510,
8 otherwise known as the Credit Information System Act (CISA).

9 **SEC. 14. Violations on Data Privacy. -**

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

21 b. *Unauthorized modification.* – It shall be unlawful for any person to
22 intentionally modify data, networks, storage media where data is
23 stored, equipment through which networks are run or maintained,
24 the physical plant where the data or network equipment is housed,
25 without authority granted by the Internet service provider,
26 telecommunications entity, or other such person providing Internet or
27 data services having possession or control of the data or network, or
28 to intentionally modify intellectual property published on the Internet
29 or on other networks without the consent of the person having
30 ownership, possession, or control of the intellectual property, or
31 without legal grounds, even if the modification is performed without
32 malice.

33 c. *Unauthorized authorization or granting of privileges.* – It shall be
34 unlawful for any person to intentionally provide a third party
35 authorization or privileges to access or modify data, networks,
36 storage media where data is stored, equipment through which
37 networks are run or maintained, the physical plant where the data or
38 network equipment is housed, without authority granted by the
39 Internet service provider, telecommunications entity, or other such
40 person providing Internet or data services having possession or
41 control of the data or network, or to intentionally provide a third
42 party authorization to access or modify intellectual property
43 published on the Internet or on other networks without the consent

1 of the person having ownership, possession, or control of the
2 intellectual property, or without legal grounds, even if the
3 authorization to access or perform modifications was granted without
4 malice.

5 d. *Unauthorized disclosure.* – It shall be unlawful for any authorized
6 person to intentionally disclose or cause the disclosure to a third
7 party or to the public any private data being transmitted through the
8 Internet or through public networks, or any data being transmitted
9 through private networks, without legal grounds, even if the
10 disclosure was done without malice.

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

16 **SEC. 15. *Violation of Data Security.* –**

17 a. *Hacking.* – It shall be unlawful for any unauthorized person to
18 intentionally access or to provide a third party with access to, or to
19 hack or aid or abet a third party to hack into, data, networks, storage
20 media where data is stored, equipment through which networks are
21 run or maintained, the physical plant where the data or network
22 equipment is housed. The unauthorized access or unauthorized act of
23 providing a third party with access to, or the hacking into, data,
24 networks, storage media where data is stored, equipment through
25 which networks are run or maintained, the physical plant where the
26 data or network equipment is housed shall be presumed to be
27 malicious.

28 b. *Cracking.* – It shall be unlawful for any unauthorized person to
29 intentionally modify or to crack data, networks, storage media where
30 data is stored, equipment through which networks are run or
31 maintained, the physical plant where the data or network equipment
32 is housed, or for any unauthorized person to intentionally modify
33 intellectual property published on the Internet or on other networks.
34 The unauthorized modification or cracking of data, networks, storage
35 media where data is stored, equipment through which networks are
36 run or maintained, the physical plant where the data or network
37 equipment is housed, or unauthorized modification of intellectual
38 property published on the Internet or on other networks, shall be
39 presumed to be malicious.

40 c. *Phishing.* –

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

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

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

20 **SEC. 16. *Illegal and Arbitrary Seizure.* –**

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

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

40 c. *Arbitrary Seizure.* – It shall be unlawful for any public officer or
41 employee to seize data, information, or contents of a device, storage

1 medium, network equipment, or physical plant, or to seize any device,
2 storage medium, network equipment, or physical plant connected to
3 the Internet or to telecommunications networks, or to gain
4 possession or control of intellectual property published on the
5 Internet or on public networks, without legal grounds.

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

19 **SEC. 17. Penalties. -**

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

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

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

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

36 e. Violation of Data Privacy Act through ICT –

37 i. Violation of Section 25 (a) of the Data Privacy Act (Unauthorized
38 Processing of Personal Information) through ICT – imprisonment
39 ranging from one (1) year to three (3) years and a fine of not less

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

1 (7) years and a fine of not less than Five hundred thousand pesos
2 (Php500,000.00) but not more than Two million pesos
3 (Php2,000,000.00).

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

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

15 f. Violation of Hacking – imprisonment ranging from one (1) year to three
16 (3) years and a fine of not less than Five hundred thousand pesos
17 (Php500,000.00) but not more than Two million pesos
18 (Php2,000,000.00).

19 g. Violation of Cracking – imprisonment ranging from one (1) year to
20 three (3) years and a fine of not less than Five hundred thousand pesos
21 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

22 h. Violation of Phishing – imprisonment ranging from one (1) year and six
23 (6) months to five (5) years and a fine of not less than Five hundred
24 thousand pesos (Php500,000.00) but not more than One million pesos
25 (Php1,000,000.00).

26 i. Violation of Data Privacy Act (with hacking, cracking, or phishing) –

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

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

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

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

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

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

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

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

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

24 **SEC. 18. Ownership of Data.-** Data that comes to the possession and
25 knowledge of the Big Data Center shall be deemed as property of public dominion.
26 Unprocessed data that comes to the possession of the Center shall be considered
27 property of public dominion for public service where its use is limited to authorized
28 persons in government. Processed data of the Center which shall take the form of
29 official reports and studies shall be deemed as property of public dominion for public
30 use such that it is intended for the use of anybody. Data partners may define the
31 ownership of data based on the partnership agreements with the government taking
32 into consideration the context of the need of such data.

33 **SEC. 19. Funding.** -There shall be included in the budget of NEDA under the
34 annual General Appropriations Act an amount of Two Hundred Million Pesos
35 (P200,000,000.00) as the initial operating fund of the Big Data Center.

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

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

5 **SEC. 20. *Implementing Rules and Regulations.*** – Within sixty (60) days from
6 the effectivity of this Act, the Philippine Statistics Authority (PSA) shall promulgate
7 the necessary rules and regulations for the effective implementation of this Act.
8

9 **SEC. 21. *Separability Clause.*** - Should any provision herein be declared
10 unconstitutional, the same shall not affect the validity of the other provisions of this
11 Act.

12 **SEC. 22. *Repealing Clause.*** - All laws, decrees, orders, rules, and regulations
13 or other issuances or parts inconsistent with the provisions of this Act are hereby
14 repealed or modified accordingly.

15 **SEC. 23. *Effectivity.*** - This Act shall take effect fifteen (15) days after its
16 publication in the Official Gazette or in two (2) newspapers of general circulation in
17 the Philippines.

18 *Approved,*