#dimbootcamp

E-Commerce Law, Data Privacy Law, Cybercrime Law

Janette Toral

http://digitalfilipino.com/influencer

#dimbootcamp

E-Commerce Law (Republic Act 8792)

Janette Toral

http://digitalfilipino.com/influencer

E-Commerce Law – Republic Act 8792

- It gives legal recognition of electronic data messages, electronic documents, and electronic signatures. (section 6 to 13)”

E-Commerce Law – Republic Act 8792

- Allows the formation of contracts in electronic form. (section 16)”

E-Commerce Law – Republic Act 8792

- Makes banking transactions done through ATM switching networks absolute once consummated. (section 16)”

E-Commerce Law – Republic Act 8792

- Parties are given the right to choose the type and level of security methods that suit their needs. (section 24)”

E-Commerce Law – Republic Act 8792

- Provides the mandate for the electronic implementation of transport documents to facilitate carriage of goods. This includes documents such as, but not limited to, multi-modal, airport, road, rail, inland waterway, courier, post receipts, transport documents issued by freight forwarders, marine/ ocean bill of lading, non-negotiable seaway bill, charter party bill of lading. (section 25 and 26)”

E-Commerce Law – Republic Act 8792

- Mandates the government to have the capability to do e-commerce within 2 years or before June 19, 2002. (section 27)”

E-Commerce Law – Republic Act 8792

- Mandates RPWeb to be implemented. RPWeb is a strategy that intends to connect all government offices to the Internet and provide universal access to the general public. The Department of Transportation and Communications, National Telecommunications Commission, and National Computer Center will come up with policies and rules that shall lead to substantial reduction of costs of telecommunication and Internet facilities to ensure the implementation of RPWeb. (section 28)”

E-Commerce Law – Republic Act 8792

- Made cable, broadcast, and wireless physical infrastructure within the activity of telecommunications. (section 28)”

E-Commerce Law – Republic Act 8792

- Empowers the Department of Trade and Industry to supervise the development of e-commerce in the country. It can also come up with policies and regulations, when needed, to facilitate the growth of e-commerce. (section 29)”

E-Commerce Law – Republic Act 8792

- Provided guidelines as to when a service provider can be liable. (section 30)”

E-Commerce Law – Republic Act 8792

- Authorities and parties with the legal right can only gain access to electronic documents, electronic data messages, and electronic signatures. For confidentiality purposes, it shall not share or convey to any other person. (section 31 and 32)”

Cybercrime Penalties under Electronic Commerce Act (Republic Act 8792)

HACKING OR CRACKING

UNAUTHORIZED ACCESS INTO OR INTERFERENCE IN A COMPUTER SYSTEM/SERVER OR INFORMATION AND COMMUNICATION SYSTEM; OR ANY ACCESS IN ORDER TO CORRUPT, ALTER, STEAL, OR DESTROY USING A COMPUTER OR OTHER SIMILAR INFORMATION AND COMMUNICATION DEVICES, WITHOUT THE KNOWLEDGE AND CONSENT OF THE OWNER OF THE COMPUTER OR INFORMATION AND COMMUNICATIONS SYSTEM, INCLUDING THE INTRODUCTION OF COMPUTER VIRUSES AND THE LIKE, RESULTING IN THE CORRUPTION, DESTRUCTION, ALTERATION, THEFT OR LOSS OF ELECTRONIC DATA MESSAGES OR ELECTRONIC DOCUMENT

PENALTIES

PUNISHED BY A MINIMUM FINE OF ONE HUNDRED THOUSAND PESOS **(P100,000·00)** AND A MAXIMUM COMMENSURATE TO THE DAMAGE INCURRED AND A MANDATORY IMPRISONMENT OF **SIX (6)** MONTHS TO **THREE (3)** YEARS

PIRACY

THE UNAUTHORIZED COPYING, REPRODUCTION, DISSEMINATION, DISTRIBUTION, IMPORTATION, USE, REMOVAL, ALTERATION, SUBSTITUTION, MODIFICATION, STORAGE, UPLOADING, DOWNLOADING, COMMUNICATION, MAKING AVAILABLE TO THE PUBLIC, OR BROADCASTING OF PROTECTED MATERIAL, ELECTRONIC SIGNATURE OR COPYRIGHTED WORKS INCLUDING LEGALLY PROTECTED SOUND RECORDINGS OR PHONOGRAMS OR INFORMATION MATERIAL ON PROTECTED WORKS, THROUGH THE USE OF TELECOMMUNICATION NETWORKS

PENALTIES

MINIMUM FINE OF ONE HUNDRED THOUSAND PESOS (P100,000·00) AND A MAXIMUM COMMENSURATE TO THE DAMAGE INCURRED AND A MANDATORY IMPRISONMENT OF **SIX (6)** MONTHS TO **THREE (3)** YEARS

OTHER VIOLATIONS IN E-COMMERCE LAW

CONSUMER ACT AND ALL OTHER LAWS

REPUBLIC ACT NO. 7394 AND OTHER RELEVANT OR PERTINENT LAWS THROUGH TRANSACTIONS COVERED BY OR USING ELECTRONIC DATA MESSAGES OR ELECTRONIC DOCUMENTS

PENALTIES

PENALIZED WITH THE SAME PENALTIES AS PROVIDED IN THOSE LAWS

OTHER VIOLATIONS IN E-COMMERCE LAW

OTHER VIOLATIONS OF THE PROVISIONS OF THIS ACT

EX. OBLIGATION OF CONFIDENTIALITY, LAWFUL ACCESS, AMONG OTHERS

PENALTIES

MAXIMUM PENALTY OF ONE MILLION PESOS (P1,000,000.00) OR SIX (6) YEARS IMPRISONMENT

#dimbootcamp

Data Privacy Law (Republic Act 10173)

Janette Toral

http://digitalfilipino.com/influencer

Data Privacy Law (Republic Act 10173)

- Data subject refers to an individual whose personal information is processed.”

Data Privacy Law (Republic Act 10173)

- Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:
  - A person or organization who performs such functions as instructed by another person or organization; and
  - An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

Data Privacy Law (Republic Act 10173)

- Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject."

Data Privacy Law (Republic Act 10173)

- It applies to processing of personal information (section 3g) and sensitive personal information (Section 3L).”

Data Privacy Law (Republic Act 10173)

- Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.”

Data Privacy Law (Republic Act 10173)

- Sensitive personal information refers to personal information:
  - Race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
  - Health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
  - Issued by government agencies peculiar to an individual. E.g. social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
  - Specifically established by an executive order or an act of Congress to be kept classified.

Data Privacy Law (Republic Act 10173)

- Created the National Privacy Commission to monitor the implementation of this law. (section 7)

Data Privacy Law (Republic Act 10173)

- Gave parameters on when and on what premise can data processing of personal information be allowed. Its basic premise is when a data subject has given direct consent. (section 12 and 13)

Data Privacy Law (Republic Act 10173)

- Companies who subcontract processing of personal information to 3rd party shall have full liability and can't pass the accountability of such responsibility. (section 14)

Data Privacy Law (Republic Act 10173)

- Data subject has the right to know if their personal information is being processed. The person can demand information such as the source of info, how their personal information is being used, and copy of their information. One has the right to request removal and destruction of one's personal data unless there is a legal obligation that required for it to be kept or processed. (Section 16 and 18)

Data Privacy Law (Republic Act 10173)

- If the data subject has already passed away or became incapacitated (for one reason or another), their legal assignee or lawful heirs may invoke their data privacy rights. (Section 17)

Data Privacy Law (Republic Act 10173)

- Personal information controllers must ensure security measures are in place to protect the personal information they process and be compliant with the requirements of this law. (Section 20 and 21)

Data Privacy Law (Republic Act 10173)

- In case a personal information controller systems or data got compromised, they must notify the affected data subjects and the National Privacy Commission. (Section 20)

Data Privacy Law (Republic Act 10173)

- Heads of government agencies must ensure their system compliance to this law (including security requirements). Personnel can only access sensitive personal information off-site, limited to 1000 records, in government systems with proper authority and in a secured manner. (Section 22)

Data Privacy Law (Republic Act 10173)

- Government contractors who have existing or future deals with the government that involves accessing of 1000 or more records of individuals should register their personal information processing system with the National Privacy Commission. (Section 25)

Data Privacy Law (Republic Act 10173)

- Provided penalties (up to 5 million as per sec. 33) on the processing of personal information and sensitive personal information based on the following acts:
  - Unauthorized processing (sec. 25)
  - Negligence (sec. 26)
  - Improper disposal (sec. 27)
  - Unauthorized purposes (sec. 28)
  - Unauthorized access or intentional breach (sec. 29)
  - Concealment of security breaches (sec. 30)
  - Malicious (sec. 31) and unauthorized disclosure (sec. 32)

Data Privacy Law (Republic Act 10173)

- If at least 100 persons are harmed, the maximum penalty shall apply (section 35).

Data Privacy Law (Republic Act 10173)

- For public officers (working in government), an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied. (sec. 36)

e-Commerce BOOT CAMP

Cybercrime Prevention Act of 2012 (Republic Act 10175)

Twitter: @digitalfilipino #ecombootcamp

Confidentiality, Integrity, Availability of Computer Systems (Sec. 4 (a))

- (1) *Illegal access* – The access to the whole or any part of a computer system without right.
- (2) *Illegal interception* – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

Confidentiality, Integrity, Availability of Computer Systems (Sec. 4 (a))

- *3.* ***Data Interference***
  Unauthorized alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, and including the introduction or transmission of viruses.
- Authorized action can also be covered by this provision if the action of the person went beyond agreed scope resulting to damages stated in this provision.

Confidentiality, Integrity, Availability of Computer Systems (Sec. 4 (a))

- *4.* ***System Interference***
  Unauthorized hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data messages, and including the introduction or transmission of viruses.
- Authorized action can also be covered by this provision if the action of the person went beyond agreed scope resulting to damages stated in this provision.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) up to a maximum amount commensurate to the damage incurred or BOTH.
- If committed against critical infrastructure:
  - Reclusion temporal (imprisonment for twelve years and one day up to twenty years) or a fine of at least Five hundred thousand pesos (P500,000) up to a maximum amount commensurate to the damage incurred or BOTH

Confidentiality, Integrity, Availability of Computer Systems (Sec. 4 (a))

- (5) *Misuse of devices*
  - (i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:
    - (aa) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or
    - (bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.
  - (ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with the intent to use said devices for the purpose of committing any of the offenses under this section.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of not more than Five hundred thousand pesos (P500,000) or both.

Confidentiality, Integrity, Availability of Computer Systems (Sec. 4 (a))

- (6) *Cyber-squatting*. The acquisition of domain name over the Internet in bad faith to profit, mislead, destroy reputation, and deprive others from the registering the same, if such a domain name is:
  - (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
  - (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name, and
  - (iii) Acquired without right or with intellectual property interests in it.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) up to a maximum amount commensurate to the damage incurred or BOTH.
- If committed against critical infrastructure:
  - Reclusion temporal (imprisonment for twelve years and one day up to twenty years) or a fine of at least Five hundred thousand pesos (P500,000) up to a maximum amount commensurate to the damage incurred or BOTH

Computer-related Offenses (Section 4 b)

- (1) *Computer-related Forgery*:
  - (i) The input, alteration, or deletion of computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or
  - (ii) The act of knowingly using computer data which is the product of computer-related forgery as defined here, for the purpose of perpetuating a fraudulent or dishonest design.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) up to a maximum amount commensurate to the damage incurred or BOTH.

Computer-related Offenses (Section 4 b)

- (2) *Computer-related Fraud*. The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent; *Provided*, That if no damage has yet been caused, the penalty imposed shall be one (1) degree lower.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) up to a maximum amount commensurate to the damage incurred or BOTH.
- *Provided*, That if no damage has yet been caused, the penalty imposed shall be one (1) degree lower.

Computer-related Offenses (Section 4 b)

- (3) *Computer-related Identity Theft*. The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right. *Provided*, That if no damage has yet been caused, the penalty imposed shall be one (1) degree lower.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) up to a maximum amount commensurate to the damage incurred or BOTH.

Content-related offenses (Section 4. c)

- (1) *Cybersex* – The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

Penalty

- *Prision mayor* (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) but not exceeding One million pesos (P1,000,000) or BOTH.

Content-related offenses (Section 4. c)

- (2) *Child Pornography* – The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system.
- *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775.

Content-related offenses (Section 4. c)

- STRUCK DOWN by Supreme Court
  - (3) *Unsolicited Commercial Communications* – The transmission of commercial communication with the use of computer system which seek to advertise sell, or offer for sale products and services are prohibited

Content-related offenses (Section 4. c)

- (4) Libel. Unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended committed through a computer system or any other similar means which may be devised in the future.
- **Revised Penal Code Art. 355 states** *Libel means by writings or similar means*. — A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means, shall be punished by prision correccional in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action which may be brought by the offended party.

Penalty

- *Penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.*

ELECTRONIC LIBEL AND CYBERCRIME PREVENTION ACT OF 2012

Libel is defined under the *Revised Penal Code Section 355*

1930

Art. 355. Libel means by writings or similar means. — A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, *or any similar means,* shall be punished by prision correccional in its minimum and medium periods **or** a fine ranging from 200 to 6,000 pesos, **or both**, in addition to the civil action which may be brought by the offended party.

Decriminalizing libel requires amending the Revised Penal Code.

2000

E-Commerce Law (Republic Act 8792) empowered all existing laws to recognize electronic documents as evidence (commercial / non-commercial).

Libel is a crime in Cybercrime Law Section 4c (4)

2012

Libel. – The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended committed through a computer system or any other similar means which may be devised in the future.

***If a case is filed by a complainant, only 1 case to be prosecuted under Cybercrime Law.**

* Can be charge under Revised Penal Code also if concurrently committed in traditional means.

Pressing the like button and posting comments doesn't mean you are automatically committing libel. They are considered as "protected expression".

If proven guilty, imprisonment can be up to

8

years or payment of fines (amount to be set in IRR) or both

85% of Cybercrime case dockets involves libel (DOJ).

SOURCE: http://bit.ly/ptv4forum
http://bit.ly/edangara

infographics by: DIGITAL FILIPINO .com

Other Offenses (Section 5)

- ***(a) Aiding or Abetting in the commission of cybercrime*** – Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

Other Offenses (Section 5)

- ***(b) Attempt in the commission of cybercrime*** Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

Penalty

- Imprisonment of *one (1) degree lower than that of the prescribed penalty for the offense* or a fine of at least One hundred thousand pesos (P100,000) but not exceeding Five hundred thousand pesos (P500,000) or both.

Revised Penal Code

- Section 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act. *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

Corporate Liability (Section 9)

- When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on:
  - (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority;
  - (b) an authority to take decisions on behalf of the juridical person. *Provided*, That the act committed falls within the scope of such authority; or
  - (c) an authority to exercise control within the juridical person,
- It also includes commission of any of the punishable acts made possible due to the lack of supervision or control.

Penalty

- For sanctioned actions, Juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (P10,000,000).For neglect such as misuse of computer resources that resulted to cybercrime committed in organization physical or virtual premises or resources, juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (P5,000,000).
- Criminal liability may still apply to the natural person.

Section 7. Liability on other laws

- Struck down by the Supreme Court.

Law Enforcement Authorities (Section 10. LEA)

- The National Bureau of Investigation and the Philippine National Police shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

Duties of LEA Section 11

- To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post operation, and investigation results and such other documents as may be required to the Department of Justice for review and monitoring.

Section 12 Real time collection of data

- Struck down by Supreme Court

Basis for Court Warrant Issuance

- The court warrant under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing:
  - (1) that there are reasonable grounds to believe that any of the crimes enumerated herein above has been committed, or is being committed, is about to be committed;
  - (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution or, or to the prevention of any such crimes, and
  - (3) that there are no other means readily available for obtaining such evidence.

Preservation of Computer Data (Sec. 13)

- The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum of six (6) months period from the date of the transaction.
- Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.
- Law enforcement authorities may order a one-time extension of another six (6) months. *Provided*, That once computer data preserved, transmitted or stored by service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

Disclosure of Computer Data (Sec. 14)

- Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his / its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

Section 15. Search, Seizure, Examination of Computer Data.

- Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties. Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:
  - (a) To secure a computer system or a computer data storage medium.
  - (b) To make and retain a copy of those computer data secured.
  - (c) To maintain the integrity of the relevant stored computer data.
  - (d) To conduct forensic analysis or examinations of the computer data storage medium; and
  - (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Section 15. Search, Seizure, Examination of Computer Data.

- Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information to enable the undertaking of the search, seizure and examination.
- Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

Section 16. *Custody of Computer Data*

- .All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanies by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who access the deposit, among other relevant data.
- The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court.
- The package so deposited shall not be opened or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

Section 17. *Destruction of Computer Data*.

- Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination.

Section 18. *Exclusionary Rule*.

- Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

Section 19. *Restricting or Blocking Access to Computer Data*.

- Struck down by the Supreme Court.

Section 20. *Non-compliance*.

- Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of prision correccional in its maximum period or a fine of One hundred thousand pesos (P100,000) or both for each and every non-compliance with an order issued by law enforcement authorities.

Section 21. Jurisdiction

- The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act including any violation committed by a Filipino national regardless of the place of commission.
- Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situation in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.
- There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

Sec. 22 International Cooperation

- All relevant international instruments on international cooperation in criminal maters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense shall be given full force and effect.

#dimbootcamp

See you at the next webinar!

http://digitalfilipino.com/influence