SUBJECT: MEDIA AND INFORMATION LITERACY
TOPIC: Legal, Ethical and Societal Issues in Media and Information

PREPARED BY: Lyka A. Casipag **GRADE: 12**
SEMESTER: FIRST **WEEK:9**

Quest:

- puts into action their personal resolve to combat digital divide, addiction, and bullying; MIL11/12LESI-IIIg-19
- enumerates opportunities and challenges in media and information; MIL12LESI-IIIg-23

Mission 1.

Instructions: Identify what type of cyber bullying is being asked in the statement below. Encircle the letter of the correct answer.

1. It deliberates excluding someone from an online group.

a. Exclusion b. harassment c. notion d. cyber stalking

2. Posting or sending cruel gossip to damage a person's reputation and relationships with friends, family and acquaintances.

a. Notion b. cyber threats c. gossip d. harassment

3. It is repeatedly posting or sending offensive, rude, and insulting messages.

a. harassment b. outing and trickery c. gossip d. notion

4. Breaking into someone 's email or other online account and sending messages that will cause embarrassment or damage to the person's reputation and affect his or her relationship with other.

a. Notion b. cyber stalking c. gossip d. harassment

5. Tricking someone into revealing secrets or embarrassing information, which is then shared online.

a. Digital divide b. outing and trickery c. notion d. cyber threats

EQUIP:

What is Digital divide?

refers to the gap between those who benefit from the Digital Age and those who don't.[1][2] People without access to the Internet and other information and communication technologies are put at a disadvantage, as they are unable or less able to obtain digital information, shop online, participate democratically, or learn and offer skills. This resulted in programs to give computers and related services to people without access.

What is Addiction?

Addiction is a biopsychosocial disorder characterized by compulsive engagement in rewarding stimuli despite adverse consequences. Despite the involvement of a number of

psychosocial factors, a biological process—one that is induced by repeated exposure to an addictive stimulus—is the core pathology that drives the development and maintenance of an addiction, according to the "brain disease model" of addiction.[3] However, some scholars who study addiction argue that the brain disease model is incomplete and misleading.

What is Cyber bullying?

Cyber bullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyber bullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyber bullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyber bullying crosses the line into unlawful or criminal behavior.

The most common places where cyber bullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tiktok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities

TYPES OF CYBER BULLYING

1. **Exclusion-** deliberates excluding someone from an online group.
2. **Gossip-** posting or sending cruel gossip to damage a person's reputation and relationships with friends, family and acquaintances.
3. **Harassment-**repeatedly posting or sending offensive, rude, and insulting messages.
4. **Notion-**breaking into someone 's email or other online account and sending messages that will cause embarrassment or damage to the person's reputation and affect his or her relationship with other.
5. **Outing and trickery-**tricking someone into revealing secrets or embarrassing information, which is then shared online.
6. **Cyber stalking-**posting and sending unwanted or intimidating messages, which may include threats.
7. **Cyber threats –**remarks on the internet threatening or implying violent behavior, displaying suicidal tendencies.

LAWS IN THE PHILIPPINES ON MEDIA AND INFORMATION

Intellectual Property Rights in the Philippines or <u>Republic Act No. 8293</u>

Intellectual Property Rights in the Philippines or <u>Republic Act No. 8293</u>

According to the **Republic of the Philippines** in the **REPUBLIC ACT 8293** *part 1, section 1, "This Act shall be known as the "Intellectual Property Code of the Philippines.".* This act aims to secure and protect the original work of the owner and shall give credits to the owner. The plans of other people couldn't be copied because of the security of this law. This act also includes the i*ntellectual property office, law on*

patents, law on trademarks, service marks, and trade names, law on copyrights and lastly the *final provision*.

A.) What are the limitations on copyright?

According to ***Chapter 8, Section 184*** of The Intellectual Property Code of the Philippines There are eleven limitations of copyright here in the Philippine. Copyright is a collection of all rights enjoyed by the creator and/or an author of an artistic or literary work. This shows what we can and can't do to the intellectual property. The limitations of the copyright is that when it expires, it will not be valid and it will not longer protect the work of the author.

B.) Why does the law limit copyright?

Taken from Chapter 8, Section 184.2 of The Intellectual Property Code of the Philippines we limit copyright because this shall be interpreted in such a way as to allow the work to be used in a manner which does not conflict with the normal exploitation of the work and does not unreasonably prejudice the right holder's legitimate interests.

C.) What are the economic rights of authors, as prescribed in the law?

The economic rights of authors based from *Chapter 5, Section 177* of The Intellectual Property Code of the Philippines are the following:

177.1. Reproduction of the work or substantial portion of the work;
177.2. Dramatization, translation, adaptation, abridgment, arrangement or other transformation of the work;
177.3. The first public distribution of the original and each copy of the work by sale or other forms of transfer of ownership;
177.4. Rental of the original or a copy of an audiovisual or cinematographic work, a work embodied in a sound recording, a computer program, a compilation of data and other materials or a musical work in graphic form, irrespective of the ownership of the original or the copy which is the subject of the rental; (n)
177.5. Public display of the original or a copy of the work;
177.6. Public performance of the work; and
177.7. Other communication to the public of the work. (Sec. 5, P. D. No. 49a)

D.) How can one own a copyright?

Based from Chapter 6, Section 178 of The Intellectual Property Code of the Philippines one can own copyright by if you create something on your own time, for your own purposes, you already own it and you are the copyright owner.Once you've created a new literary work, video, musical composition or piece of art, it is important that your creative rights to that work be protected through registration of a copyright that establishes ownership and date of completion.

E.) To whom can copyright be transferred or assigned? How can this be done?

There may be a time when you wish to transfer your copyright rights to another. Transferring such rights usually takes place through a license or assignment. Copyright can be transferred with the use of the law.

As a citizen, we should be the one who should make a move to prevent copyright infringement and other things that can violate intellectual property.

REPUBLIC ACT NO. 10627]

AN ACT REQUIRING ALL ELEMENTARY AND SECONDARY SCHOOLS TO ADOPT POLICIES TO PREVENT AND ADDRESS THE ACTS OF BULLYING IN THEIR INSTITUTIONS

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

SECTION 1. *Short Title*. – This Act shall be known as the "Anti-Bullying Act of 2013".

SEC. 2. *Acts of Bullying*. – For purposes of this Act, "bullying" shall refer to any severe or repeated use by one or more students of a written, verbal or electronic expression, or a physical act or gesture, or any combination thereof, directed at another student that has the effect of actually causing or placing the latter in reasonable fear of physical or

emotional harm or damage to his property; creating a hostile environment at school for the other student; infringing on the rights of the other student at school; or materially and substantially disrupting the education process or the orderly operation of a school; such as, but not limited to, the following:

a. Any unwanted physical contact between the bully and the victim like punching, pushing, shoving, kicking, slapping, tickling, headlocks, inflicting school pranks, teasing, fighting and the use of available objects as weapons;

b. Any act that causes damage to a victim's psyche and/or emotional well-being;

c. Any slanderous statement or accusation that causes the victim undue emotional distress like directing foul language or profanity at the target, name-calling, tormenting and commenting negatively on victim's looks, clothes and body; and

d. Cyber-bullying or any bullying done through the use of technology or any electronic means.

SEC. 3. *Adoption of Anti-Bullying Policies.* – All elementary and secondary schools are hereby directed to adopt policies to address the existence of bullying in their respective institutions. Such policies shall be regularly updated and, at a minimum, shall include provisions which:

(a) Prohibit the following acts:

(1) Bullying on school grounds; property immediately adjacent to school grounds; at school-sponsored or school-related activities, functions or programs whether on or off school grounds; at school bus stops; on school buses or other vehicles owned, leased or used by a school; or through the use of technology or an electronic device owned, leased or used by a school;

(2) Bullying at a location, activity, function or program that is not school-related and through the use of technology or an electronic device that is not owned, leased or used by a school if the act or acts in question create a hostile environment at school for the victim, infringe on the rights of the victim at school, or materially and substantially disrupt the education process or the orderly operation of a school; and

(3) Retaliation against a person who reports bullying, who provides information during an investigation of bullying, or who is a witness to or has reliable information about bullying;

(b) Identify the range of disciplinary administrative actions that may be taken against a perpetrator for bullying or retaliation which shall be commensurate with the nature and gravity of the offense: *Provided*, That, in addition to the disciplinary sanctions imposed upon a perpetrator of bullying or retaliation, he/she shall also be required to undergo a rehabilitation program which shall be administered by the institution concerned. The parents of the said perpetrator shall be encouraged by the said institution to join the rehabilitation program;

(c) Establish clear procedures and strategies for:

(1) Reporting acts of bullying or retaliation;

(2) Responding promptly to and investigating reports of bullying or retaliation;

(3) Restoring a sense of safety for a victim and assessing the student's need for protection;

(4) Protecting from bullying or retaliation of a person who reports acts of bullying, provides information during an investigation of bullying, or is witness to or has reliable information about an act of bullying; and

(5) Providing counseling or referral to appropriate services for perpetrators, victims and appropriate family members of said students;

(d) Enable students to anonymously report bullying or retaliation: *Provided, however*, That no disciplinary administrative action shall be taken against a perpetrator solely on the basis of an anonymous report;

(e) Subject a student who knowingly makes a false accusation of bullying to disciplinary administrative action;

(f) Educate students on the dynamics of bullying, the anti-bullying policies of the school as well as the mechanisms of such school for the anonymous reporting of acts of bullying or retaliation;

(g) Educate parents and guardians about the dynamics of bullying, the anti-bullying policies of the school and how parents and guardians can provide support and reinforce such policies at home; and
(h) Maintain a public record of relevant information and statistics on acts of bullying or retaliation in school: *Provided*, That the names of students who committed acts of bullying or retaliation shall be strictly confidential and only made available to the school administration, teachers directly responsible for the said students and parents or guardians of students who are or have been victims of acts of bullying or retaliation.
All elementary and secondary schools shall provide students and their parents or guardians a copy of the anti-bullying policies being adopted by the school. Such policies shall likewise be included in the school's student and/or employee handbook and shall be conspicuously posted on the school walls and website, if there is any.
The Department of Education (DepED) shall include in its training programs, courses or activities which shall provide opportunities for school administrators, teachers and other employees to develop their knowledge and skills in preventing or responding to any bullying act.
SEC. 4. *Mechanisms to Address Bullying*. – The school principal or any person who holds a comparable role shall be responsible for the implementation and oversight of policies intended to address bullying.
Any member of the school administration, student, parent or volunteer shall immediately report any instance of bullying or act of retaliation witnessed, or that has come to one's attention, to the school principal or school officer or person so designated by the principal to handle such issues, or both. Upon receipt of such a report, the school principal or the designated school officer or person shall promptly investigate. If it is determined that bullying or retaliation has occurred, the school principal or the designated school officer or person shall:
(a) Notify the law enforcement agency if the school principal or designee believes that criminal charges under the Revised Penal Code may be pursued against the perpetrator;
(b) Take appropriate disciplinary administrative action;
(c) Notify the parents or guardians of the perpetrator; and
(d) Notify the parents or guardians of the victim regarding the action taken to prevent any further acts of bullying or retaliation.
If an incident of bullying or retaliation involves students from more than one school, the school first informed of the bullying or retaliation shall promptly notify the appropriate administrator of the other school so that both may take appropriate action.
SEC. 5. *Reporting Requirement.* – All schools shall inform their respective schools division superintendents in writing about the anti-bullying policies formulated within six (6) months from the effectively of this Act. Such notification shall likewise be an administrative requirement prior to the operation of new schools.
Beginning with the school year after the effectively of this Act, and every first week of the start of the school year thereafter, schools shall submit a report to their respective schools division superintendents all relevant information and statistics on acts of bullying or retaliation. The schools division superintendents shall compile these data and report the same to the Secretary of the DepED who shall likewise formally transmit a comprehensive report to the Committee on Basic Education of both the House of Representatives and the Senate.
SEC. 6. *Sanction for Noncompliance*. – In the rules and regulations to be implemented pursuant to this Act, the Secretary of the DepED shall prescribe the appropriate administrative sanctions on school administrators who shall fail to comply with the requirements under this Act. In addition thereto, erring private schools shall likewise suffer the penalty of suspension of their permits to operate.
SEC. 7. *Implementing Rules and Regulations*. – Within ninety (90) days from the effectively of this Act, the DepED shall promulgate the necessary rules and regulations to implement the provisions of this Act.

SEC. 8. *Separability Clause*. – If, for any reason, any provision of this Act is declared to be unconstitutional or invalid, the other sections or provisions hereof which are not affected thereby shall continue to be in full force or effect.
SEC. 9. *Repealing Clause*. – All laws, decrees, orders, rules and regulations or parts thereof which are inconsistent with or contrary to the provisions of this Act are hereby repealed, amended or modified accordingly.
SEC. 10. *Effectively*. – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

REPUBLIC ACT NO. 10175
AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

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

CHAPTER I
PRELIMINARY PROVISIONS
Section 1. *Title.* — This Act shall be known as the ***"Cybercrime Prevention Act of 2012".***
Section 2. *Declaration of Policy.* — The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by

facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.
Section 3. *Definition of Terms.* — For purposes of this Act, the following terms are hereby defined as follows:
(a) *Access* refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.
(b) *Alteration* refers to the modification or change, in form or substance, of an existing computer data or program.
(c) *Communication* refers to the transmission of information through ICT media, including voice, video and other forms of data.
(d) *Computer* refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.
(e) *Computer data* refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

(f) *Computer program* refers to a set of instructions executed by the computer to achieve intended results.
(g) *Computer system* refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media.
(h) *Without right* refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law.
(i) *Cyber* refers to a computer or a computer network, the electronic medium in which online communication takes place.
(j) *Critical infrastructure* refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.
(k) *Cybersecurity* refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
(l) *Database* refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system.
(m) *Interception* refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.
(n) *Service provider* refers to:
(1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and
(2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service.
(o) *Subscriber's information* refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established:
(1) The type of communication service used, the technical provisions taken thereto and the period of service;
(2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and
(3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
(p) *Traffic data* or non-content data refers to any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II
PUNISHABLE ACTS

Section 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:(a) Offenses against the confidentiality, integrity and availability of computer data and systems

Illegal Access- The access to the whole or any part of a computer system without right.

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.

Data Interference-The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

System Interference-The intentional alteration or reckless 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 message, without right or authority, including the introduction or transmission of viruses.

Misuse of Devices- 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 w

Cyber- Squatting-The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from 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.

- **COMPUTER – RELATED OFFENSES**

Computer- Related Forgery-) The input, alteration, or deletion of any 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

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:

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:

- **CONTENT – RELATED OFFENSES**

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.

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 (1) one degree higher than that provided for in Republic Act No. 9775

Unsolicited commercial communication-The transmissions of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

(i) There is prior affirmative consent from the recipient; or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or
(iii) The following conditions are present:
(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject. receipt of further commercial electronic messages (opt-out) from the same source;
(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and
(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.
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.

- **OTHER OFFENSES**

Aiding of 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.
Attempt in the Commission in Cybercrime-Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

Mission 2. What I Have Learned

Instructions: Let's summarize our lesson by answering the following questions:

1.What is cybercrime?

_____

_____

2. Enumerate examples of cybercrime?

_____

_____

3. We can combat cybercrime by:

_____

_____

4. We can protect ourselves from cybercrime by:

_____

_____

Mission 3: Solve Me!

Instruction: Give the possible effects of the given online acts as well as solution to address them.

PROBLEM	EFFECT	SOLUTIONS
Digital Divide		

Bullying		
Computer Addiction		

Additional Activities

Instruction: Create a short rap that suggest ways on how to stop cyber bullying. Use the space below.

_____
_____
_____
_____
_____
_____

References:

- Media and Information Literacy Curriculum Guide
- Media and Information Literacy by Magpile
  Liquigan, Boots C., Media and Information Literacy, 2016, Diwa Learning Systems Inc.
- https://What Is Cyberbullying | StopBullying.gov
- https:// Republic Act No. 10175 (lawphil.net)
- http://www.lawphil.net/statutes/repacts/ra1997/ra_8293_1997.html
- http://www.wipo.int/wipolex/en/text.jsp?file_id=129343
- http://smallbusiness.chron.com/copyright-own-work-3060.html
- https://www.youtube.com/watch?v=00AUE1ZBNKI
- Republic Act No. 10627 | Official Gazette of the Republic of the Philippines
- LEGAL, ETHICAL AND SOCIETAL ISSUES IN MEDIA, INFORMATION AND TECHNOLOGY by Jhun Gutierrez (prezi.com)
- Digital divide - Wikipedia
- Addiction - Wikipedia
- https://www.subcribd.com