Code of Ethics & Professional Conduct

ACM Code of Ethics

1. GENERAL ETHICAL PRINCIPLES:

1.1 Contribute to Society and Human Well-being
1.2 Avoid Harm to Others
1.3 Be Honest and Trustworthy
1.4 Be Fair and Take Action Not to Discriminate
1.5 Honor Property Rights, Including Copyrights and Patents
1.6 Give Proper Credit for Intellectual Property
1.7 Respect the Privacy of Others
1.8 Honor Confidentiality

2. PROFESSIONAL RESPONSIBILITIES:

2.1 Aim for high-quality work.
2.2 Keep learning and updating skills..
2.3 Honor privacy and property rights.
2.4 Spread Tech Awareness: Educate about tech's impact.
2.5 Support Ethical Policies
2.6 Protect information and systems.
2.7 Follow ethical guidelines.
2.8 Resolve conflicts fairly.
2.9 Get feedback for improvement.
2.10 Evaluate its ethical impact on society.

3. PROFESSIONAL LEADERSHIP PRINCIPLES:

3.1 Prioritize People's Well-being
3.2 Encourage Good Behavior
3.3 Make Work Better for Everyone
3.4 Follow and Promote Ethical Rules
3.5 Provide Learning Opportunities
3.6 Be Careful When Changing Systems
3.7 Take Care of Important Systems

4. COMPLIANCE WITH THE CODE:

4.1 Follow and Support the Code
4.2 Encourage Others to Follow the Code

Human Rights and Fundamental Rights

What Are Human Rights?
Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Everyone is entitled to these rights, without discrimination.

Universal Declaration of Human Rights
The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 by General Assembly resolution 217 A as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected.

Economic, social and cultural rights
The International Covenant on Economic, Social and Cultural Rights entered into force in 1976. The human rights that the Covenant seeks to promote and protect include:

- the right to work in just and favorable conditions;
- the right to social protection, to an adequate standard of living and to the highest attainable standards of physical and mental well-being;
- the right to education and the enjoyment of benefits of cultural freedom and scientific progress.

Civil and political rights
The International Covenant on Civil and Political Rights and its First Optional Protocol entered into force in 1976. The Second Optional Protocol was adopted in 1989.
The Covenant deals with such rights as freedom of movement; equality before the law; the right to a fair trial and presumption of innocence; freedom of thought, conscience and religion; freedom of opinion and expression; peaceful assembly; freedom of association; participation in public affairs and elections; and protection of minority rights. It prohibits arbitrary deprivation of life; torture, cruel or degrading treatment or punishment; slavery and forced labour; arbitrary arrest or detention; arbitrary interference with privacy; war propaganda; discrimination; and advocacy of racial or religious hatred.

Human Rights and the UN System
Human rights is a cross-cutting theme in all UN policies and programmes in the key areas of peace and security, development, humanitarian assistance, and economic and social affairs. As a result, virtually every UN body and specialized agency is involved to some degree in the protection of human rights. Some examples are the right to development, which is at the core of the Sustainable Development Goals; the right to food, championed by the UN Food and

Agriculture Organization, labor rights, defined and protected by the International Labour Organization, gender equality, which is promulgated by UN Women, the rights of children, indigenous peoples, and disabled persons.
Human Rights Day is observed every year on 10 December.

Fundamental Rights

The fundamental rights of the people of Bangladesh have been enshrined in the constitution of the country. All past laws inconsistent with these rights are made void by the Constitution, and it enjoins upon the State not to make any law inconsistent with these rights. Certain rights may, however, remain suspended under the provisions of Articles 141(a), 141(b) and 141(c) during an emergency arising out of a threat to the country's security or economic life.
Fundamental rights give the citizens dignity of life in an atmosphere of freedom and justice beyond the man-made fetters that had constricted their physical and mental horizons. The fundamental rights of the people in Bangladesh are listed under **Articles 27 to 44 of Part III,** and the jurisdiction of the high court Division of the Supreme Court to enforce the rights is defined in Article 102 of Part VI of the Constitution of 1972.

Articles 27 and 28 of the Constitution guarantee equal protection of the law for all citizens, regardless of religion, race, caste, sex, or place of birth. **Articles 31 and 32** ensure that every citizen enjoys the protection of the law and is treated in accordance with it. **Article 29** guarantees equality of opportunity for all citizens in employment or office in the Republic, regardless of their background. However, special provisions may be made for backward citizens to secure adequate representation in the service of the Republic. **Article 33** ensures that arrested individuals are informed of their arrest grounds and have the right to consult a legal practitioner. They must be produced by a magistrate within 24 hours, and no person can be detained beyond this time without magistrate authority. **Article 34** prohibits forced labor and any contravention is punishable by law. **Article 35** ensures no person is convicted of any offense except for violation of a law in force at the time of the offense, and no person is subjected to torture or cruel, inhuman, or degrading punishment or treatment. **Article 36** grants citizens the right to freely move, reside, settle, and leave and return to Bangladesh, subject to reasonable restrictions in the public interest. **Articles 37 and 38** of the Constitution guarantee citizens the right to form associations, assemble, and participate in public meetings peacefully, without arms, subject to law restrictions. **Article 39** guarantees freedom of thought and conscience, speech, expression, and press freedom, with restrictions for security, friendly relations, and morality. **Article 40** guarantees citizens the right to enter any lawful profession, occupation, and conduct any lawful trade or business, unless law restrictions are imposed. **Article 41** of the Constitution grants citizens the right to practice religion, establish religious institutions, and acquire property. **Article 42** ensures property acquisition and disposal only by law. **Article 43** protects citizens' privacy and security in homes. **Article 44** guarantees citizens the right to move the High Court Division for constitutional enforcement.

Crimes & Punishments under the Digital Security Act 2018

Digital Security Act: An Act to make provisions for ensuring digital security and identification, prevention, suppression and trial of offenses committed through digital device and for matters ancillary thereto.

17. Punishment for illegal access to any critical information infrastructure, etc.-

a) Access - punished with imprisonment for 7yrs or fine Taka 25 lac or with both.
b) Harm - punished with imprisonment for 14yrs or fine Taka 1 crore or with both.
c) 2nd time or repeatedly - punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both.

18. Illegal access to computer, digital device, computer system, etc. and punishment

a) Access - punished with imprisonment for 6 months or fine Taka 2 lac or with both.
b) Harm - punished with imprisonment for 3yrs or fine Taka 10 lac or with both.
c) 2nd time or repeatedly - he shall be liable to double of the punishment provided for that offense.

19. Damage of computer, computer system, etc. and punishment.

(1) If any person -

(a) collects any data, data-storage, information or any extract of it from any computer, computer system or computer network, or collects information with moveable stored data-information of such computer, computer system or computer network, or collects copy or extract of any data; or

(b) intentionally inserts or tries to insert any virus or malware or harmful software into any computer or computer system or computer network; or

(c) willingly causes or tries to cause harm to data or data-storage of any computer, computer system, computer network, or causes or tries to cause harm to any programme saved in the computer, computer system, or computer network; or

(d) obstructs or tries to obstruct a valid or authorized person to access into any computer, computer system or computer network by any means; or

(e) willingly creates or sells or tries to create or sell spam or sends unsolicited electronic mails without permission of the sender or receiver, for marketing any product or service; or

(f) takes service of any person, or deposits or tries to credit the charge fixed for the service to the account of any other person fraudulently or by means of unfair interference to any computer, computer system or computer network,

Punishment - punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

2nd time or repeatedly - punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both.

20. Offense and punishment related to modification of computer source code.
(1) If any person intentionally or knowingly hides or damages or modifies the source code used in any computer programme, computer system or computer network, or tries to hide, damage or modify the source code, programme, system or network through another person, and if such source code is preservable or maintainable, then such act of the person shall be an offense.
(2) **Punishment -** If any person commits any offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 3 (three) lac, or with both.
(3) **Second time or repeatedly,** he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.

21. Punishment for making any kind of propaganda or campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag.
Punishment - punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 1 (one) crore, or with both.
Second time or repeatedly - he shall be punished with imprisonment for life, or with fine of Taka 3 (three) crore, or with both.

22. Digital or electronic forgery.
(1) If any person commits forgery by using any digital or electronic medium, then such act of the person shall be an offense. (Explanation - digital or electronic forgery" means to operate, without right or in excess of the right given or by means of unauthorized practice, erroneous data or programme, information or wrong activity, information system, computer or digital network by producing, changing, deleting and hiding input or output of any computer or digital device by a person.)
Punishment - If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.
Second time or repeatedly - punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

23. Digital or electronic fraud.
(1) If any person commits fraud by using any digital or electronic medium, then such act of the person shall be an offense.
Punishment - If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.
Second time or repeatedly - punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

24. Identity fraud or personation.
(1) If any person, intentionally or knowingly, by using any computer, computer programme, computer system, computer network, digital device, digital system or digital network-

(a) holds the identity of another person or exhibits the personal information of another person as his own in order to deceive or cheat; or
(b) holds the personal identity of any person, alive or dead, as his own by forgery in order to- (i) get or cause to get benefit for himself or for any other person; (ii) acquire any property or any interest therein; (iii) cause harm to a natural person or individual by personating another, then such act of the person shall be an offense.
Punishment - If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.
Second time or repeatedly - punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

25. Transmission, publication, etc. of offensive, false or threatening data information.
(1) If any person, through any website or any other digital medium,
(a) intentionally or knowingly transmits, publishes or propagates any data-information which he knows to be offensive, false or threatening in order to annoy, insult, humiliate or malign a person; or
(b) publishes or propagates or abets to publish or propagate any information, as a whole or partly, which he knows to be propaganda or false, with an intention to affect the image or reputation of the country, or to spread confusion, then such act of the person shall be an offense.
Punishment - If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 3 (three) lac, or with both.
Second time or repeatedly - punished with imprisonment for a term not exceeding 5(five) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

26. Punishment for unauthorized collection, use etc. of identity information.-
(1) If any person collects, sells, possesses, provides or uses identity information of any other person without lawful authority, then such act of the person shall be an offense.
Punishment - If any person commits any offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.
Second time or repeatedly - punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both

27. Offense and punishment for committing cyber terrorism:
If any person
(a) creates obstruction to make legal access, or makes or causes to make illegal access to any computer or computer network or internet network with an intention to jeopardize the integrity, security and sovereignty of the State and to create a sense of fear or panic in the public or a section of the public; or

(b) creates pollution or inserts malware in any digital device which may cause or likely to cause death or serious injury to a person; or

(c) affects or damages the supply and service of daily commodities of the public or creates adverse effects on any critical information.

Punishment:

If any person commits an offense under sub-section

(1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both

. (3) If any person commits the offense referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both.

28.Publication, broadcast, etc. of information on a website or in any electronic format that hurts religious values or sentiment.

(1) If any person or group willingly or knowingly publishes or broadcasts or causes to publish or broadcast anything in a website or any electronic format which hurts religious sentiment or values, with an intention to hurt or provoke the religious values or sentiments, then such act of the person shall be an offense.

Punishment:

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (3) If any person commits the offense referred to in sub-section (1) for the **second time or repeatedly**, he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 20 (twenty) lac, or with both.

29. Publication, transmission, etc. of defamatory information

.(1) If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in website or in any other electronic format,

punishment:

He shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 5 (five) lac, or with both.

(2) If any person commits the offense referred to in sub-section (1) for the **second time or repeatedly,** he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

30. Offense and punishment for e-transaction without legal authority

. (1) If any person

(a) without legal authority, makes e-transaction over electronic and digital means from any bank, insurance or any other financial institution or any organization providing mobile money service.

or (b) makes any e-transaction though the e-transaction is, from time to time, declared illegal by the Government or Bangladesh Bank, then such act of the person shall be an offense.

Punishment:

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.

(3) If any person commits the offense referred to in sub-section (1) for the **second time or repeatedly,** he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

31. Offense and punishment for deteriorating law and order, etc

.(1) If any person intentionally publishes or transmits anything in website or digital layout that creates enmity, hatred or hostility among different classes or communities of the society, or destroys communal harmony, or creates unrest or disorder, or deteriorates or advances to deteriorate the law and order situation, then such act of the person shall be an offense.

Punishment:

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 5 (five) lac, or with both.

(3) If any person commits the offense referred to in sub-section (1) for the **second time or repeatedly,** he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

32. Offense and punishment for breaching secrecy of the Government.

(1) If any person commits or abets to commit an offense under the Official Secrets Act, 1923 (Act No. XIX of 1923) by means of computer, digital device, computer network, digital network or any other digital means,

Punishment:

he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both.

(2) If any person commits the offense referred to in sub-section (1) for the s**econd time or repeatedly**, he shall be punished with imprisonment for life, or with fine not exceeding Taka 1 (one) crore, or with both.

33. Punishment for holding, transferring data-information illegally, etc

(1)If any person preserves or abets to preserve any data-information of any governmental, semi-governmental, autonomous or statutory organization, or any financial or commercial organization by making illegal access to any of its computer or digital system in order to make any addition or deletion, or hand over or transfer, then such act of the person shall be an offense.

Punishment:

(2) If any person commits an offense under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka10 (ten) lac, or with both.

(3) If any person commits the offense referred to in sub-section (1) **for the second time or repeatedly**, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 15 (fifteen) lac, or with both.

34. Offence related to hacking and punishment thereof -
Punishment:
.(1) If any person commits hacking, it shall be an offence, and for this, he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both.
2) If any person commits the offence referred to in sub-section (1) **for the second time or repeatedly,** he shall be punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both.

35. Abetment of committing an offence and punishment thereof
.(1) If any person abets to commit an offence under this Act, then such act of the person shall be an offence.
Punishment:
(2) In case of abetment of committing an offence, the person abetted to commit the offence shall be punished with the same punishment as is provided for the offence

36. Offence committed by a company.
(1) Where an offence under this Act is committed by a company, every owner, chief executive, director, manager, secretary, partner or any other officer or employee or representative of the company who has direct involvement with the offence shall be deemed to have committed the offence unless he proves that the offence was committed without his knowledge or he exercised all due diligence to prevent the offence.
Punishment:
(2) If the company referred to in sub-section (1) is a legal entity, it may be accused or convicted separately, in addition to accusing or convicting the persons mentioned above, but only fine may be imposed upon the company under the concerned provision.

37. Power to issue order for compensation.
If any person causes financial loss to any other person by means of digital or electronic forgery under section 22, digital or electronic fraud under section 23 and identity fraud or personation under section 24, then the Tribunal may issue order to compensate the person affected with money equivalent to the loss caused, or such amount of money as it considers to be sufficient.

38. The service provider not to be responsible.
No service provider shall be liable under this Act or rules made thereunder for facilitating access to any data-information, if he proves that the offence or breach was committed without his knowledge or he exercised all due diligence to prevent the offence.

Crimes and punishments under the ICT act 2006

54. Penalty for damage to computer, computer system, etc—If someone, without permission, does any of the following to a computer, computer system, or network:

a)Accessing to Destroy or Collect Information:
- Enters a computer to destroy or collect information.

b)Downloading, Copying, Extracting Data:
- Takes data from a computer without permission.

c)Introducing Viruses:
- Puts harmful stuff (viruses) into a computer.

d)Damaging Data or Programs:
- Harms or destroys data or programs in a computer.

e)Disrupting Computer Systems:
- Disturbs the normal functioning of a computer or network.

f)Denying Authorized Access:
- Blocks authorized people from accessing a computer.

g)Assisting Unauthorized Access:
- Helps someone else get into a computer without permission.

h)Spamming and Unwanted Emails:
- Sends a lot of unwanted emails for advertising.

i)Manipulating Services for Payment:
- Charges someone else for services by tampering with a computer.

Punishment:
- If someone does these things, they could go to jail for up to ten years or be fined up to ten lakhs Taka, or both.

Explanation:
1. Computer Contaminant:
- Instructions meant to mess up or take control of a computer.
2. Computer Database:
- Information stored in a computer in the form of text, image, audio, or video, intended for computer use.
3. Computer Virus:
- Harmful instructions that damage or affect how a computer works.

4. Damage:
- Messing with a computer resource by destroying, altering, deleting, adding, modifying, or rearranging it.

55. Punishment for tampering with computer source code.--(1) If someone, on purpose, hides, destroys, or changes any computer source code used for a computer, program, system, or network.
- Especially when the law says that the source code must be kept.

2) If someone does this, they could go to jail for up to three years, or be fined up to three lakhs Taka, or both.

Explanation:
- "Computer Source Code":
- It's like the recipe for a computer program. It includes the list of instructions, commands, design, and analysis of how a computer resource works, in any form. Messing with this is a big no-no, and if caught, it could mean time in jail or a hefty fine.

56. Punishment for hacking with computer system.-- If someone, with the intention to cause harm or knowing that they might cause harm:
- Does something to a computer system that destroys, deletes, or changes information, making it less valuable or useful.
- Illegally accesses a computer, computer network, or any electronic system that doesn't belong to them and causes damage.

2.)If someone does these things, they could go to jail for up to ten years, be fined up to one crore Taka, or both.

57. Punishment for publishing fake, obscene or defaming information in electronic form.--
- If someone purposefully puts out material on a website or in electronic form that is fake, obscene, or likely to corrupt people who might come across it.
- If the material could harm public order, damage the reputation of the state or individuals, hurt religious beliefs, or provoke negative actions against a person or organization.

2.)- If someone does this, they could go to jail for up to ten years and be fined up to one crore Taka.

58. Punishment for failure to surrender licence.--(1) Where any Certifying Authority fails to surrender a license under section 34 of this Act, the person in whose favour the licence is issued, the
failure of the person shall be an offense.
(2) Whoever commits offense under sub-section (1) of this section he shall be punishable

with imprisonment for a term which may extend to six months, or with fine which may extend to Taka
ten thousands, or with both.

59. Punishment for failure to comply with order.--(1) Any person who fails to comply with any order made under section 45 of this Act, then this activity of his will be regarded as an offense.

(2) Whoever commits offense under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to one year, or with fine which may extend to Taka
one lakh, or with both.

60. Punishment for failure to comply with order made by the Controller in emergency -- (1) Any person who fails to comply with any order made under section 46 of this Act, then this activity
of his will be regarded as an offense.

(2) Whoever commits offense under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to five years, or with fine which may extend to Taka
five lakhs, or with both.

61. Punishment for unauthorized access to protected systems.--(1) Any person who secures access or attempts to secure access to protected system in contraventions of section 47 of this Act, then this activity of his will be regarded as an offense.

(2) Whoever commits offense under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka
ten lakhs, or with both.

62. Punishment for misrepresentation and obscuring information.--Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for
obtaining any license or Digital Signature Certificate shall be regarded as an offense.

(2) Whoever commits any offense under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

63. Punishment for disclosure of confidentiality and privacy.--1. If someone accesses confidential information (electronic records, books, registers, correspondence, etc.) while doing their job under this Act or any related rules, they cannot disclose that information to anyone else without the permission of the person it belongs to.

2. This means that if, for example, a police officer sees your personal information while investigating a crime, they cannot share that information with anyone else without your permission.

3. The punishment for breaking this law is up to two years in jail, a fine of up to Taka two lakhs, or both.

64. Punishment for publishing false Digital Signature Certificate— Nobody should share or make available a Digital Signature Certificate to others if they know:

- The certifying authority listed in the certificate didn't issue it.
- The person mentioned in the certificate didn't accept it.
- The certificate has been canceled or suspended.

- The only exception is if the certificate is being shared to verify a digital signature created before the suspension or revocation.

2.) - If someone breaks these rules, they could go to jail for up to two years, be fined up to two lakhs Taka, or both.

65. Punishment for publishing Digital Signature Certificate for fraudulent purpose etc.--
Whosoever knowingly creates and publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be regarded as an offence.
(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakh, or with both.
66. Punishment for using computer for committing an offence.--(1) Whosoever knowingly assists committing crimes under this Act, using any computer, e-mail or computer network, resource or
system shall be regarded as an offence.
(2) Whoever aids committing any offence under sub-section (1) of this section he shall be punishable with the punishment provided for the core offence.

67. Offenses committed by companies etc.-If a company breaks the law under this Act, the people involved in the company, like directors, managers, secretaries, partners, officers, and staff, can be held responsible.
Each of them is considered guilty of the offense unless they can prove they didn't know about it or did everything they could to prevent it.
Explanation:

"Company":
Refers to any business entity, including corporations, commercial firms, partnerships, cooperatives, associations, organizations, or any group of individuals working together.
"Director" (for commercial firms):
Includes partners or members of the Board of Directors in the context of a commercial firm

Intellectual Property of ICT products

What is Intellectual Property :

*Intellectual property rights are the rights given to persons over the creations of their minds, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce. Intellectual property is the product of human intellect including creativity, concepts, inventions, industrial models, trademarks, songs, literature, symbols, names, brands, etc.

Intellectual property rights do not differ from other property rights. They allow their owner to completely benefit from his/ her product which was initially an idea that developed and crystallized. They also entitled him/her to prevent others from using dealing with or tampering with his / her product without prior permission from him/ her. He/ she can in fact legally sue them and force them to stop and compensate for any damages.

Materials of Intellectual Property of ICT products:

Intellectual Property (IP) in the context of Information and Communication Technology (ICT) products covers a wide range of materials and concepts. Here are some key aspects of intellectual property related to ICT products:

1. **Patents:**
- **Definition:** Exclusive rights granted to inventors for new, useful, and non-obvious inventions or processes.
- **Materials:** Detailed technical descriptions, diagrams, and claims that define the scope of protection.

2. **Copyright:**
- **Definition:** Exclusive rights granted to the creators of original works, such as software code, literary works, and artistic creations.
- **Materials:** Source code, object code, documentation, graphics, and other creative expressions.

3. **Trademarks:**
- **Definition:** Protection for symbols, names, and slogans used to identify and distinguish goods or services.
- **Materials:** Logos, brand names, product names, and other identifiers associated with ICT products.

4. **Trade Secrets:**

- **Definition:** Information that provides a business advantage over competitors and is kept confidential.
- **Materials:** Algorithms, formulas, manufacturing processes, and other confidential business information.

5. **Design Patents:**
- **Definition:** Protection for the ornamental design of functional items.
- **Materials:** Visual design elements of hardware or user interfaces in ICT products.

6. **Open Source Licenses:**
- **Definition:** Licensing terms that allow the sharing, modification, and distribution of software's source code.
- **Materials:** Source code and associated documentation under open-source licenses.

7. **Utility Models:**
- **Definition:** Similar to patents but typically cover minor inventions and have a shorter duration.
- **Materials:** Technical descriptions and claims similar to those in a patent.

8. **Contracts and Agreements:**
- **Definition:** Legal agreements that define the terms and conditions of use, distribution, or development of ICT products.
- **Materials:** Licensing agreements, end-user license agreements (EULAs), and other contractual documents.

9. **Domain Names:**
- **Definition:** Internet addresses that provide a recognizable identity to websites.
- **Materials:** The domain name itself and related materials used for online presence.

10. **Industrial Designs:**
- **Definition:** Protection for the visual design of objects, including the shape, surface ornamentation, and aesthetics.
- **Materials:** Design elements related to the physical appearance of hardware components in ICT products.

11. **Digital Rights Management (DRM):**
- **Definition:** Technologies and techniques to control the access and usage of digital content.
- **Materials:** DRM-protected content and associated technologies.

It's important for individuals and organizations involved in the development, distribution, or use of ICT products to be aware of these intellectual property concepts and seek appropriate legal

advice to protect their rights and avoid infringement. IP laws can vary by jurisdiction, so understanding the relevant laws in your region is crucial.

Tangible materials:

Tangible materials are physical substances that can be touched, seen, and measured. Examples of tangible materials include items like wood, metal, plastic, and concrete, which can be used in construction, manufacturing, or other physical applications.(money(abstract)/ gold).

Immaterial:

Immaterial refers to something that lacks material or physical substance, existing in a non-physical or abstract form. For example, a company's reputation is immaterial as it is a perception or concept rather than a tangible object; it exists in the minds of individuals based on their experiences and interactions with the company rather than having a physical presence.(stokes- company shares,good will of business).

Moveable :

Moveable property refers to assets that can be physically moved or transported and are not fixed in one location. Examples of moveable property include vehicles, machinery, furniture, and inventory, as these items can be relocated or transferred from one place to another based on the owner's needs or business requirements. Unlike real estate or immovable property, moveable assets are not permanently attached to a specific location.

Immoveable:

Immovable property refers to land and any structures permanently attached to it, such as buildings. Unlike movable property, which can be easily transported, immovable property is characterized by its fixed and permanent nature. For example, a residential house and the land it sits on are considered immovable property, as the structure is affixed to the land and cannot be moved without significant effort and alteration.

*why does computer become your property :

A computer becomes your property through a legal process of acquisition, typically involving purchase or transfer of ownership. When you buy a computer, you acquire ownership rights, and the device becomes your property. For example, if you purchase a laptop from a retail store, the transaction involves a transfer of ownership, and you gain the right to use, modify, and dispose of the computer as you see fit.

Ownership of a computer is often accompanied by a proof of purchase, such as a receipt or an invoice, which establishes your legal claim to the device. Additionally, the computer may come with an end-user license agreement (EULA) that outlines the terms and conditions of use. Your

ownership rights extend to the physical hardware of the computer as well as any software that may be included, subject to the terms specified in the licensing agreements.

It's important to note that while you may own the physical computer, some software may be licensed rather than sold, meaning you have the right to use it but do not own it outright. Understanding the terms of ownership and licensing agreements is crucial in determining your rights and responsibilities regarding the computer and its components.

OR, (eta sir er option deya option gula dye likha by cahtgpt)
The computer becomes your property through a confluence of labor, merit, personality, and the reward theory. Through the investment of labor, individuals dedicate time and effort to acquire, assemble, and configure the computer, contributing to its creation. The merit aspect comes into play as the ownership of the computer is often tied to the skills, knowledge, and expertise demonstrated by the individual in effectively utilizing and maintaining the system.

Personality factors influence ownership as individuals personalize their computers with preferences, applications, and data, creating a unique digital environment reflective of their identity. The reward theory underscores the notion that ownership results from the recognition and compensation for one's efforts—whether through direct purchase, professional acquisition, or other means of obtaining the computer. Together, these elements contribute to the sense of ownership and investment in the computer as a personal and valuable asset.

Creative commons license as an alternative:

A Creative Commons (CC) license is an alternative licensing system that allows creators to retain some of their rights while permitting others to use, share, and build upon their work under certain conditions. CC licenses are designed to provide a flexible and standardized way for authors, artists, and other creators to grant permissions to the public regarding the use of their intellectual property. There are several types of Creative Commons licenses, each with its own set of permissions, ranging from allowing only non-commercial use to permitting derivative works or modifications.

For instance, a creator may choose to apply a CC BY-SA (Attribution-ShareAlike) license to their work, which allows others to copy, distribute, display, and perform the work, as well as create derivative works based on it, even commercially, as long as they give the original creator credit and license any new creations under the same terms. Creative Commons licenses thus provide a legal framework that strikes a balance between the protection of the creator's rights and the encouragement of collaboration and sharing within the creative community.

Right to Information Act 2009

Chapter 2

Right to, Preservation of, Publication of and Access to Information

4. Right to information: Every citizen shall have the right to information from the authority, and the authority shall, on demand from a citizen, be bound to provide him with the information.

5. Preservation of information:

(1) Every authority shall prepare catalog and index of all information and preserve it in an appropriate manner.

(2) Every authority shall, within a reasonable time-limit, preserve in computer all such information as it thinks fit for preservation in computer, and shall connect them through a country-wide network to facilitate access to information.

(3) The Information Commission shall, by regulations, frame instructions to be followed by every authority for the preservation and management of information and all authority shall follow the instructions.

6. Publication of information:

1) Every authority shall publish and publicize all information pertaining to any decision taken, proceeding or activity executed or proposed by indexing them in such a manner as may easily be accessible to the citizens.

2) In publishing and publicizing information under sub-section (1), no authority shall conceal any information or limit its easy access.

3) Every authority shall publish a report every year which shall contain the following information :-

   (a) Particulars of its organisational structure, activities, responsibility of the officers and employees, or description and process of decision making.

   (b) Lists of all laws, Acts, Ordinance, rules, regulations, notifications, directives, manuals, etc. of the authority including the classification of all information lying with the authority.

   (c) Description of the terms and conditions under which a citizen may get services from the authorities in obtaining any license, permit, grant, consent, approval or other benefits and of such conditions that require the authority to make transactions or enter into agreements with him.

(d) Particulars of the facilities ensuring right to information of the citizens, and the full name, designation, address, and, in cases where applicable, fax number and e-mail address of the assigned officer.

4) If the authority frames any policy or takes any important decision, it shall publish all such policies and decisions and shall, if necessary, explain the reasons and causes in support of such policies and decisions.

5) The report prepared by authority under this section shall be made available free of charge for public information and its copies shall be stocked for sale at nominal price.

6) All the publications made by the authority shall be made available to the public at a reasonable price.

7) The authority shall publish and publicise the matters of public interest through press notes or through any other means.

8) The Information Commission shall, by regulations, frame instructions to be followed by the authority for publishing, publicising and obtaining information and all the authority shall follow them.

7. Publication of or providing with certain types of information not mandatory: Notwithstanding anything contained in any other provisions of this Act, no authority shall be bound to provide with the following information, namely:

(a) any such information that may, if disclosed, cause a threat to the security, integrity and sovereignty of Bangladesh

(b) any such information relating to any aspect of foreign policy that may affect the existing relationship with any foreign country or international organisation or any regional alliance or organization.

(c) any secret information received from a foreign government.

(d) any information relating to inherent secrets of commercial or business nature, copyright or intellectual property right that may, if published, affect the intellectual property right of a third party.

(e) any of the following information that may, if disclosed, be gainful or damaging to any particular individual or organization, namely :

(i) any advance information about income tax, customs, VAT and law relating to excise duty, budget or change in the tax rate;

(ii) any advance information about changes relating to exchange rate and interest rate;

(iii) any advance information about the management and supervision of the financial institutions including banks;

(f) any such information that may, if disclosed, obstruct the enforcement of law or incite any offence;

(g) any such information that may, if disclosed, endanger the security of public or impede the due judicial process of a pending case;

(h) any such information that may, if disclosed, offend the privacy of the personal life of an individual;
(i) any such information that may, if disclosed, endanger the life or physical safety of any person;
(j) any such information given in confidence to any law enforcement agency by a person;
(k) any matter pending before any court of law and which has been expressly forbidden to be published by any court of law or tribunal or the disclosure of which may constitute contempt of court;
(l) any such information that may, if disclosed, impede the process of investigation;
(m) any such information that may, if disclosed, affect any investigation process of offence and the arrest and prosecution of offender;
(n) any such information which is, according to law, liable to be published only for a certain period of time;
(o) any such information that is generated through technical or scientific experiment, and is expedient to keep secret for strategic or commercial reasons;
(p) any such information pertaining to a purchase process before it is complete or a decision has been taken about it;
(q) any such information that may be prejudicial to the special rights of the House of the Nation;
(r) any secret information of a person which is protected by law;
(s) any advance, information relating to question papers of an examination or marks given;
(t) Any document including summaries to be placed before the Cabinet or, as the case may be, before the Council of Advisers and information relating to discussions and decisions of such meetings :
Provided that after taking any decision by the Cabinet or, as the case may be, by the Council of Advisors, the reasons of taking such decisions and the basis upon which the decisions are taken may be disclosed :
Provided further that the concern authority shall take prior approval from Information Commission for withholding information under this section.

8.Request for information:

(1) Under this Act a person may apply to the officer-in-charge requesting for information either in writing or through electronic means or through e-mail.
(2) The request made under sub-section (1) shall include the following information, namely :

I. Name, address of the person making request, in applicable cases, his fax number and email address;
II. Correct and clear description of the information sought for;

III. Other related information so that the location of the information sought for may be easily found out;

IV. Description of the modes how he wants to have the information, that is making inspection, having copy, taking note or any other approved method.

(3) The request for information under this section shall be made in a form printed by the authority, or as the case may be, in prescribed format :

Provided that if the form is not printed or is not easily available or if the format has not yet been prescribed, request may be made for information by inserting information mentioned in sub-section (2) on a piece of white paper, or in electronic form or through e-mail.

(4) In the case of obtaining information under sub-section (1), the person making the request shall pay reasonable fees as may be prescribed by the officerin-charge for such information.

(5) The Government may, in consultation with the Information Commission, fix the fees for having any information by notification in the official Gazette, and, if necessary, may fix the price of information, or as the case may be, may exempt an individual or a class of individuals or any other class from paying such price.

(6) Every authority shall prepare and publicise a list of information to be supplied free of cost upon an instruction of the Information Commission.

9. Procedure for providing information:

1. The designated officer shall, on receipt of a request under sub-section (1) of section 8, provide the information to the applicant within 20 (twenty) working days from the date of receiving the request.
2. Notwithstanding anything contained in sub-section (1), if more than one unit or authority are involved with the information sought for, such information may be provided within 30 (thirty) working days.
3. Despite anything contained in sub-section (1) and (2), if the officer-incharge, due to any reason, fails to provide the information sought for, he shall inform the applicant the reasons thereof in writing within 10 (ten) working days.
4. Notwithstanding anything contained in sub-section (1) and (2), if a request made under sub-section (1) of section 8 is relating to the life and death, arrest and release from jail of any person, the officer-in-charge shall provide preliminary information thereof within 24 (twenty-four) hours.
5. Where the officer-in-charge fails to provide information within the timeframe as mentioned in sub-section (1), (2) or (4), it shall be presumed that the request for information has been rejected.
6. When any information sought for is available with the officer-in-charge, he shall determine a reasonable price of that information and shall request the applicant to pay the price within 5(five) working days.

7. For determining the price under sub-section (6), the price shall not exceed the actual expense of providing information such as cost of printing electronic format or photocopying or print-out.
8. Where an officer-in-charge thinks that the request made for information under sub-section (1) of section 8 is appropriate, and such information has been supplied by a third party or a third party's interest is involved in it and the third party has considered it as secret information, the officer-in-charge shall cause a notice to be served upon the third party within 5(five) working days for written or oral opinion, and if the third party gives any opinion in response to such notice, the officer-in-charge shall take into consideration such opinion and make a decision in respect of providing information to the applicant.
9. Notwithstanding anything contained in section 7, no request for information may be totally rejected on the ground that it is associated with information that is not mandatory for publication, and the portion of the requested information which in not mandatory for publication and is reasonably separable form the portion shall be provided to the applicant.
10. Where access to the record or a part thereof is required to be provided to a perceptual handicapped, the officer-in-charge shall provide assistance to him to enable him to access such information and such assistance shall deem to include any assistance which is required for such inspection.

Pornography Control Act 2012

THE government of Bangladesh has recently enacted the anti-pornography law. The law is observed to be rigid by its nature and drawn criticism from different quarters of the society. The aim of the act is to control the spread of pornography across the country.

According to section 2 of the Pornography Control Act, the definition of pornography includes nude or half nude video and still pictures. Furthermore, it also defines as pornography, any material that is likely to increase sexual sensation or desires.

According to the 2012 Act, the users of the apps may easily be subject to section 8(1) of the act that mentions a punishment of a maximum of 8 years along with a fine of up to TK 200,000, just for capturing the image or video.

Again, according to Section 8(3), for dispersing such material using the internet and the cell phone the user may receive up to 5 years of imprisonment and a maximum fine that is the same as the previous section.

ধারাসমূহ:

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন:

১। (১) এই আইন পর্নোগ্রাফি নিয়ন্ত্রণ আইন, ২০১২ নামে অভিহিত হইবে।
(২) ইহা অবিলম্বে কার্যকর হইবে।

2|সংজ্ঞা:

"পর্নোগ্রাফি" অর্থ—
(১) যৌন উত্তেজনা সৃষ্টিকারী কোন অশ্লীল সংলাপ, অভিনয়, অঙ্গভঙ্গি, নগ্ন বা অর্ধনগ্ন নৃত্য যাহা চলচ্চিত্র, ভিডিও চিত্র, অডিও ভিজ্যুয়াল চিত্র, স্থির চিত্র, গ্রাফিকস বা অন্য কোন উপায়ে ধারণকৃত ও প্রদর্শনযোগ্য এবং যাহার কোন শৈল্পিক বা শিক্ষাগত মূল্য নেই;

(২) যৌন উত্তেজনা সৃষ্টিকারী অশ্লীল বই, সাময়িকী, ভাস্কর্য, কল্পমূর্তি, মূর্তি, কার্টুন বা লিফলেট;

(৩) উপ-দফা (১) বা (২) এ বর্ণিত বিষয়াদির নেগেটিভ ও সফট বার্সন;

(ঘ) "পর্নোগ্রাফি সরঞ্জাম" অর্থ পর্নোগ্রাফি উৎপাদন, সংরক্ষণ, ধারণ বা প্রদর্শনের উদ্দেশ্যে ব্যবহৃত ক্যামেরা, কম্পিউটার বা কম্পিউটার যন্ত্রাংশ, সিডি, ভিসিডি, ডিভিডি, অপটিক্যাল ডিভাইস, ম্যাগনেটিক ডিভাইস, মোবাইল ফোন বা উহার যন্ত্রাংশ এবং যে কোনো ইলেক্ট্রনিক, ডিজিটাল বা অন্য কোন প্রযুক্তিভিত্তিক ডিভাইস;

৩। আইনের প্রাধান্য:

আপাততঃ বলবৎ অন্য আইনে যাহা কিছুই থাকুক না কেন, এই আইনের বিধানাবলী প্রাধান্য পাইবে।

৪। পর্নোগ্রাফি সংরক্ষণ ও বাজারজাতকরণ ইত্যাদি নিষিদ্ধ:

পর্নোগ্রাফি উৎপাদন, সংরক্ষণ, বাজারজাতকরণ, বহন, সরবরাহ, ক্রয়, বিক্রয়, ধারণ বা প্রদর্শন করা যাইবে না।

৫। তদন্ত:

(১) এই আইনের অধীন সংঘটিত কোন অপরাধ তদন্তের ক্ষেত্রে পুলিশ সাব-ইন্সপেক্টর বা তাহার সমপদমর্যাদার নিম্নে নহেন এমন কোন কর্মকর্তা তদন্তকারী কর্মকর্তা হিসাবে ফৌজদারী কার্যবিধির বিধানাবলী অনুযায়ী তদন্ত করিবেন।

(২) এই আইনের অধীন সংঘটিত কোন অপরাধ তদন্তের সময়সীমা হইবে ৩০ (ত্রিশ) কার্যদিবস এবং যুক্তিসঙ্গত কারণে উক্ত সময়সীমার মধ্যে তদন্ত কার্য সমাপ্ত করা সম্ভব না হইলে, পুলিশ সুপার বা সমপদমর্যাদার কর্মকর্তা বা প্রযোজ্য ক্ষেত্রে, তদূর্ধ্ব কর্মকর্তার অনুমোদনক্রমে, অতিরিক্ত ১৫ (পনের) কার্যদিবস সময় বৃদ্ধি করা যাইবে।

(৩) উপ-ধারা (২) এ উল্লিখিত সময়সীমার মধ্যে যুক্তিসংগত কারণে কোন তদন্ত কার্য সমাপ্ত করা সম্ভব না হইলে, আদালতের অনুমোদনক্রমে, অতিরিক্ত আরো ৩০ (ত্রিশ) কার্যদিবস সময় বৃদ্ধি করা যাইবে।

৬। তল্লাশী, জব্দ ইত্যাদি:

(১) পুলিশ সাব-ইন্সপেক্টর এর নিম্নে নহেন এমন কর্মকর্তা অথবা সরকারের নিকট হইতে ক্ষমতাপ্রাপ্ত অন্য কোন উপযুক্ত ব্যক্তি বা কর্তৃপক্ষ ফৌজদারী কার্যবিধিতে বর্ণিত পদ্ধতি অনুসরণ করিয়া অপরাধের সহিত জড়িত কোন ব্যক্তিকে তাৎক্ষণিক গ্রেফতারের ক্ষেত্রে বা কোন পর্নোগ্রাফি সরঞ্জাম উদ্ধার বা জব্দের ক্ষেত্রে তল্লাশী কার্য পরিচালনা করিতে পারিবেন।

(২) তল্লাশীকালে জব্দকৃত সফ্ট কপি, রূপান্তরিত হার্ড কপি, সিডি, ভিসিডি, ডিভিডি, কম্পিউটার বা অন্য কোন ডিভাইস বা এক্সেসরিজ, মোবাইল ফোন বা উহার যন্ত্রাংশ, অপরাধ সংঘটনে ব্যবহৃত অন্য কোন যন্ত্র বা যন্ত্রাংশ বা সরঞ্জাম, ইলেক্ট্রনিক উপায়ে ধারণকৃত কোন তথ্য বা মেমোরি, ইত্যাদি আদালতে সাক্ষ্য হিসাবে ব্যবহার করা যাইবে।

(৩) এই আইনের অধীন সংঘটিত কোন অপরাধ তদন্তকালে বাংলাদেশ টেলিকমিউনিকেশন রেগুলেটরি কমিশন বা অন্য কোন সরকারি উপযুক্ত কর্তৃপক্ষ, মোবাইল অপারেটর, ইন্টারনেট সার্ভিস প্রোভাইডার, বৈধ ভিওআইপি সার্ভিস প্রোভাইডারসহ সরকারি বা সরকারের নিকট হইতে লাইসেন্স বা অনুমোদনপ্রাপ্ত অন্য কোন উপযুক্ত কর্তৃপক্ষের নিকট স্বাভাবিক কার্য প্রক্রিয়ার অংশ হিসাবে সংরক্ষিত তথ্য অথবা তদন্তকালে তদন্তকারী কর্মকর্তা কর্তৃক সংগৃহীত কোন বিশেষ তথ্য আদালতে সাক্ষ্য হিসাবে ব্যবহার করা যাইবে।

৭। বিশেষজ্ঞ মতামতের সাক্ষ্যমূল্য :

এই আইনের অধীন সংঘটিত কোন অপরাধ তদন্তকালে উপযুক্ত কর্তৃপক্ষ কর্তৃক সনদপ্রাপ্ত কারিগরী বিশেষজ্ঞ অথবা যে সকল প্রক্রিয়ায় উক্ত অপরাধ সংঘটিত হইয়াছে সেই সকল বিষয়ে সরকারি, স্বায়ত্তশাসিত, আধা-স্বায়ত্তশাসিত প্রতিষ্ঠানের কারিগরী বিভাগের দায়িত্বে নিয়োজিত ব্যক্তিবর্গের অথবা সরকারের নিকট হইতে লাইসেন্স বা অনুমোদনপ্রাপ্ত বেসরকারি কোন ব্যক্তি বা প্রতিষ্ঠানের কারিগরী দায়িত্বে নিয়োজিত উপযুক্ত প্রতিষ্ঠান হইতে সনদপ্রাপ্ত ব্যক্তিবর্গের নিকট হইতে প্রাপ্ত মতামত বিশেষজ্ঞের মতামত হিসাবে বিবেচিত হইবে এবং উহা আদালতে সাক্ষ্য হিসাবে ব্যবহার করা যাইবে।

৮। দণ্ড:

(১) কোন ব্যক্তি পর্নোগ্রাফি উৎপাদন করিলে বা উৎপাদন করিবার জন্য অংশগ্রহণকারী সংগ্রহ করিয়া চুক্তিপত্র করিলে অথবা কোন নারী, পুরুষ বা শিশুকে অংশগ্রহণ করিতে বাধ্য করিলে অথবা কোন নারী, পুরুষ বা শিশুকে কোন প্রলোভনে অংশগ্রহণ করাইয়া তাহার জ্ঞাতে বা অজ্ঞাতে স্থির চিত্র, ভিডিও চিত্র বা চলচ্চিত্র ধারণ করিলে
*সর্বোচ্চ ৭ (সাত) বৎসর পর্যন্ত সশ্রম কারাদণ্ড এবং ২,০০,০০০ (দুই লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন

(২) কোন ব্যক্তি পর্নোগ্রাফির মাধ্যমে অন্য কোন ব্যক্তির সামাজিক বা ব্যক্তি মর্যাদা হানি করিলে বা ভয়ভীতির মাধ্যমে অর্থ আদায় বা অন্য কোন সুবিধা আদায় বা কোন ব্যক্তির জ্ঞাতে বা অজ্ঞাতে ধারণকৃত কোন পর্নোগ্রাফির মাধ্যমে উক্ত ব্যক্তিকে মানসিক নির্যাতন করিলে
*সর্বোচ্চ ৫ (পাঁচ) বৎসর পর্যন্ত সশ্রম কারাদণ্ড এবং ২,০০,০০০ (দুই লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

(৩) কোন ব্যক্তি ইন্টারনেট বা ওয়েবসাইট বা মোবাইল ফোন বা অন্য কোন ইলেকট্রনিক ডিভাইসের মাধ্যমে পর্নোগ্রাফি সরবরাহ করিলে
*সর্বোচ্চ ৫ (পাঁচ) বৎসর পর্যন্ত সশ্রম কারাদণ্ড এবং ২,০০,০০০ (দুই লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

(৪) কোন ব্যক্তি পর্নোগ্রাফি প্রদর্শনের মাধ্যমে গণউপদ্রব সৃষ্টি করিলে
*সর্বোচ্চ ২ (দুই) বৎসর পর্যন্ত সশ্রম কারাদণ্ড এবং ১,০০,০০০ (এক লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

(৫) কোন ব্যক্তি—
(ক) পর্নোগ্রাফি বিক্রয়, ভাড়া, বিতরণ, সরবরাহ, প্রকাশ্যে প্রদর্শন বা যে কোন প্রকারে প্রচার করিলে অথবা উক্ত সকল বা যে কোন উদ্দেশ্যে প্রস্তুত, উৎপাদন, পরিবহন বা সংরক্ষণ করিলে; অথবা

(খ) কোন পর্নোগ্রাফি প্রাপ্তি স্থান সম্পর্কে কোন প্রকারের বিজ্ঞাপন প্রচার করিলে; অথবা

(গ) এই উপ-ধারার অধীন অপরাধ বলিয়া চিহ্নিত কোন কার্য সংঘটনের উদ্যোগ গ্রহণ করিলে;

*সর্বোচ্চ ২ (দুই) বৎসর সশ্রম কারাদণ্ড এবং ১,০০,০০০ (এক লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

(৬) কোন ব্যক্তি কোন শিশুকে ব্যবহার করিয়া পর্নোগ্রাফি উৎপাদন, বিতরণ, মুদ্রণ ও প্রকাশনা অথবা শিশু পর্নোগ্রাফি বিক্রয়, সরবরাহ বা প্রদর্শন অথবা কোন শিশু পর্নোগ্রাফি বিজ্ঞাপন প্রচার করিলে

*সর্বোচ্চ ১০ (দশ) বৎসর পর্যন্ত সশ্রম কারাদণ্ড এবং ৫,০০,০০০ (পাঁচ লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

(৭) এই আইনের অধীন সংঘটিত কোন অপরাধের সহিত প্রত্যক্ষভাবে জড়িত বা সহায়তাকারী ব্যক্তি প্রত্যেকেই একই দণ্ডে দণ্ডিত হইবেন।

৯। কতিপয় ক্ষেত্রে আইনের অপ্রযোজ্যতা:

ধর্মীয় উদ্দেশ্যে সংরক্ষিত বা ব্যবহৃত কোন পুস্তক, লেখা, অঙ্কন বা চিত্র, অথবা যে কোন ধর্মীয় উপাসনালয় বা উহার অভ্যন্তরে বা প্রতিমাসমূহ পরিবর্তনের জন্য ব্যবহৃত অথবা যে কোন যানবাহনের উপরে খোদাইকৃত, মিনাকৃত, চিত্রিত বা প্রকারান্তরে প্রতিচিত্রিত অথবা কোন ধর্মীয় উদ্দেশ্যে সংরক্ষিত কল্পমূর্তি বা স্বাভাবিক শিল্পকর্মের ক্ষেত্রে এই আইনের বিধানাবলী প্রযোজ্য হইবে না।

১০। অপরাধের আমলযোগ্যতা:

এই আইনের অধীন সংঘটিত অপরাধ আমলযোগ্য (Cognizable) এবং অ-জামিনযোগ্য (Non-bailable) হইবে।

১১। বিচার পদ্ধতি:

এই আইনের অধীন সংঘটিত অপরাধের বিচার ফৌজদারী কার্যবিধিতে বর্ণিত পদ্ধতি অনুযায়ী হইবেঃ
তবে শর্ত থাকে যে, সরকার, সরকারি গেজেট প্রজ্ঞাপন দ্বারা, কোন বিশেষ আদালত বা ট্রাইব্যুনালকে এই আইনের অধীন সংঘটিত অপরাধের বিচার করিবার ক্ষমতা অর্পণ করিতে পারিবে।

১২। আপিল:

এই আইনের অধীন কোন আদালত বা ক্ষেত্রমত, ট্রাইব্যুনাল কর্তৃক প্রদত্ত কোন রায় বা আদেশ দ্বারা সংক্ষুব্ধ কোন ব্যক্তি উক্ত রায় বা আদেশ প্রদানের তারিখ হইতে ৩০(ত্রিশ) দিনের মধ্যে এখতিয়ারসম্পন্ন আদালতে আপিল করিতে পারিবে

১৩। মিথ্যা মামলা, অভিযোগ দায়ের ইত্যাদির দণ্ড:

(১) এই আইনের অধীন ক্ষমতাপ্রাপ্ত কোন ব্যক্তি, কর্মকর্তা বা কর্তৃপক্ষ কোন ব্যক্তির ক্ষতিসাধনের অভিপ্রায়ে এই আইনের কোন ধারার অধীন মামলা বা অভিযোগ দায়েরের কোন ন্যায্য বা আইনানুগ কারণ নাই জানিয়াও মিথ্যা বা হয়রানিমূলক মামলা বা অভিযোগ দায়ের করিলে

*সর্বোচ্চ ২(দুই) বৎসর সশ্রম কারাদণ্ড এবং ১,০০,০০০ (এক লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

(২) এই আইনের অধীন দায়েরকৃত কোন মামলায় আদালত বা ক্ষেত্রমত, ট্রাইব্যুনাল শুনানি ও বিচারান্তে যদি কোন অভিযুক্ত ব্যক্তিকে খালাস প্রদান করে এবং আদালত যদি এই মর্মে অভিমত ব্যক্ত করে যে, উক্ত অভিযুক্ত ব্যক্তির বিরুদ্ধে আনীত অভিযোগ মিথ্যা, ভিত্তিহীন ও হয়রানিমূলক, তাহা হইলে মামলা দায়েরকারী ব্যক্তি অপরাধ করিয়াছেন বলিয়া গণ্য হইবেন *সর্বোচ্চ ২(দুই) বৎসর সশ্রম কারাদণ্ড এবং ১,০০,০০০ (এক লক্ষ) টাকা পর্যন্ত অর্থদণ্ডে দণ্ডিত হইবেন।

১৪। বিধি প্রণয়নের ক্ষমতা:

এই আইনের উদ্দেশ্য পূরণকল্পে সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, বিধি প্রণয়ন করিতে পারিবে।

১৫। আইনের ইংরেজিতে অনূদিত পাঠ:

(১) এই আইন প্রবর্তনের পর সরকার, যথাশীঘ্র সম্ভব, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের বাংলা পাঠের ইংরেজীতে অনূদিত একটি নির্ভরযোগ্য পাঠ (Authentic English Text) প্রকাশ করিবে।

(২) বাংলা পাঠ এবং ইংরেজি পাঠের মধ্যে বিরোধের ক্ষেত্রে বাংলা পাঠ প্রাধান্য পাইবে।