Unit 4: Addressing Offences: Penalties and Compensation

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Concept of Offences in Cyber Laws
- Commission of Offenses owing to Acts and Omissions of the Controller
- Commission of Offenses owing to Acts and Omissions of the Controller of Certifying Authorities

1.2 INTRODUCTION

The interesting aspect relating to penalties associated with cyber laws is that the provisions addressing them are directed towards penalties towards damage to computer and computer systems as well as towards the process of adjudication. For example, while on one hand, the provisions of the Information Technology Act, 2000 address issues of breach of security or privacy, on the other, it also deals with acts of failing to protect data and privacy. Similarly, the provisions of the Act further address instances wherein the Controller of a Certifying Authority has acted in a manner that is in violation of the provisions of the Act, or had omitted performing

its duties and responsibilities so as to contravene the provisions of the Act. The provisions of the Act and the rules and regulations pertaining to penalties, compensation and adjudication hence have to be read in sync with the essence of cyber laws at large. The Act is governed by the principle ***"He who does not prevent a crime when he can, encourages it."***

1.3 PROVISIONS APPLICABLE TO CERTIFYING AUTHORITIES AND THEIR CONTROLLER

The Information Technology Act, 2000 lays down provisions that give the Controller of Certifying Authorities the power to direct certain necessary measures to be taken to ensure compliance with the provisions of the Act; and any violation by any individual of such direction or order as given by the Controller is deemed to constitute an offence under the Act.

Similarly, suppression of material facts and/or misrepresentation of facts from Certifying Authorities or their Controller for the purposes of obtaining a license or an electronic piece of document is an offence in accordance with the provisions of the Act.[101]

An elaborate understanding with respect to the aforementioned provisions are provided hereinbelow:

i) ***Section 68 – Power of controller to give directions*** *– (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder. (2) Any person who intentionally and knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction or imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both.*[102]

This provision is in turn backed by the ***'Information Technology Security Guidelines'*** and the ***'Security Guidelines for Certifying Authorities'*** issued under the Information Technology (Certifying Authorities) Rules, 2000 which prescribe the security standards which are to be

[101] Offences & Penalties under the IT Act, 2000 <http://www.legalservicesindia.com/article/439/Offences-&-Penalties-under-the-IT-Act,-2000.html>
[102] The Information Technology Act, 2000, s 68(2)

observed by Certifying Authorities and endowing upon them the power to issue directions. While a general interpretation of the provision makes it is evident that the Controller has the power to Certifying Authorities and/or employees thereof, in essence such power can be further extended to apply on subscribers of a digital certificate as well, which can be inferred by a combined reading of ***section 68 with section 18(1) of the Information Technology Act, 2000,*** which states that the Controller shall expressly have the power to resolve any and all conflicts of interests and/or disputes between the subscriber and the respective Certifying Authorities.

Sub-section (2) of the provision goes on to establish that the offence committed by way of non-compliance of the order passed under sub-section (1) shall be a cognizable and non-bailable offence. Since section 27 of the Act allows a Controller to delegate its authorities and responsibilities to a Deputy Controller or an Assistant Controller; accordingly, a non-compliance of the Controller's order by such Deputy Controller or the Assistant Controller shall also fall within the ambit of section 68.

A combined reading of section 68 of the Act with sections 28 and 29 which in turn expressly grant to a Controller the power to investigate contraventions of the Act will clarify that the Certifying Authority has the responsibility to ensure that there is no contravention of the Act in the first place; and of at all the same is conducted by any entity and/or individual, then it will constitute as an offence.

ii) ***Section 71*** *– Penalty for misrepresentation – whoever makes any misrepresentation to or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both.*

In addition to the powers already endowed upon the Certifying Authorities and their Controller through ***section 25 and section 38 of the Act*** to suspend and revoke the license and digital signature certificates, this provision additionally bestows upon the Certifying Authority as well as its Controller the obligation to ensure that applicants who misrepresent information or suppress material information are brought within the ambit of criminal charges.

These two aforementioned provisions of the Act bring to the fore how the intention of the legislature was to address such instances in a criminal light wherein any entity, whether statutory

or otherwise, associated with electronic transactions and/or applications and/or involved any correspondence involving the cyberspace tries to misuse the relevant provisions of law and take advantage thereof.

1.4 PENALTIES IN RESPECT OF DAMAGE TO SYSTEMS ASSOCIATED WITH CYBERSPACE

The Information Technology Act, 2000 addresses instances of cyber contraventions through provisions that deal with penalties and/or compensation. Majorly section 43 to section 45 address the aforesaid and in turn list down variable penalties applicable to the respective offenders in accordance with the nature of offence committed.[103] A brief overview of the provisions is provided hereinbelow:

a) ***Section 43*** lists the various instances wherein there could be damage caused to computers or their systems or networks.
b) ***Section 43 A*** deals with an act of failure to protect sensitive data and entails payment of damages by the contravener by way of compensation.
c) ***Section 44*** directs for a penalty to be provided for failure in furnishing information by any person who is required by the Act to provide such information or file any return or maintain books of accounts.
d) ***Section 45*** addresses residuary penalty towards those who violates the rules and regulations made in association with the Act and for the specific contravention of which no penalty has separately been provided.

Section 43 lays down that unauthorized access to computers, an attempt thereof or an assistance thereto are offences under the Act. The ambit of the clause states that such unauthorized access shall cover both physical and virtual access to the computer or its system or network. Such access may be established inter alia if the computer is found to have performed a function as a result of such access. The provision further addresses unauthorized infringement of digital data stored in such computer or its network inter alia through downloading, copying, extracting etc. For the purposes of this provision, downloading, copying and extracting may be differentiated in the following manner –

[103] Penalties and Adjudication in IT ACT 2000 <https://www.pathlegal.in/Penalties-and-Adjudication-in-IT-ACT-2000-blog-1831947>

Downloading	***Copying***	***Extracting***
A file containing digital content being retrieved from a remote computer or network.	A file containing digital content being retrieved from a remote computer or network and then being saved in a storage medium.	A file containing digital content being retrieved from a remote computer or network and then being selectively extracted.

The provision further addresses instances wherein contaminants may be introduced within the computer or its network, and any other attempts that can potentially be made to contaminate data contained in a computer or its network, or destroy, steal, delete, alter the same. Such unauthorized damage to the contents contained in the computer or its computer could be both physical as well as virtual. For the purposes of this provision, physical unauthorized damage and virtual unauthorized damage may be differentiated in the following manner:[104]

Physical Unauthorized Damage	***Virtual Unauthorized Damage***
This could imply changing the configuration of the original software or the original hardware of any computer, computer system or computer network and/or destroying, deleting, altering, modifying in any manner whatsoever the binary files (which shall include but nit be limited to data or other computer programs) available in a computer, computer system or computer network in an unauthorized manner.	This could imply changing the configuration of the original software or the original hardware of any computer, computer system or computer network and/or destroying, deleting, altering, modifying in any manner whatsoever the binary files (which shall include but nit be limited to data or other computer programs) available in a computer, computer system or computer network in an unauthorized manner by way of being remotely connected to such device or network using

[104] Damages or Compensation under IT Act 2000 in India <https://cybercrimelawyer.wordpress.com/2018/04/12/damages-or-compensation-under-it-act-2000-in-india/>

	satellite and/or terrestrial waves and/or microwaves and/or other communication media.

Disruption of a computer or its system or network or denial of access thereto is also considered an offence under this provision. A summary of the sub sections of Section 43 of the Act along with the scope thereof is provided hereunder:

Information Technology Act, 2000	***Scope of Section 43***
Section 43 – Penalty and compensation for damage to computer, computer system, etc. : If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network[105]	The provision majorly addresses all the probable contraventions arising out of unauthorized access to computer, computer system or computer network.
(a) Accesses or secures access to such computer, computer system or computer network or computer resources;	Instances of cracking, hacking, data theft, software piracy etc. will be addressed as a part hereof.
(b) Downloads, copies or extracts data, computer database or information from such computer, computer system or computer network, including information or data stored or held in any removable storage medium;	Instances of digital copying, data theft, violation of privacy will get addressed.

[105] ISACA *State of Cybersecurity: Implications for 2015* <http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf>

(c) Introduces or causes to be introduced any contaminant or computer virus into any computer, computer system or computer network;	Instances of deletion, alteration, destruction, modification of any data stored in a computer would get addressed.
(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;	Instances related to forgery, online fraud, violation of privacy would get addressed.
(e) Disrupts or causes disruption of any computer, computer system or computer network;	Instances such as spamming attacks, denial of service etc. will get addressed.
(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;	Issues related to system interference, misuse of computer devices etc. get covered hereunder.
(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of the Act, rules or regulations made thereunder	Instances of illegal access, misuse of computer devices etc. get covered hereunder.

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network	Online fraud, phishing, identify theft etc. are the instances that could be addressed through this provision.
(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means	Cracking, hacking, data theft, interference into and loss of data, online frauds and forgeries etc. are instances to get covered under this sub-section.
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage	This sub-section could cover instances related to violations of computer programs and software, theft, piracy etc.

Section 43A addresses all instances of violation of the Act arising and accruing from negligence on part of the data processor or controller. This provision is proactive in nature and aims at protecting personal data and information. The provision further identifies body corporates as 'data processors and controllers for possessing, dealing with and/or handling sensitive data, as the case may be. As opposed to the provisions of section 43, section 43A is specifically addressed towards body corporates. The provision further goes on to warrant that in the event

there is a violation of such sensitive and/or personal data invoking the contents of this section, such violation shall entail payment of compensation.[106]

Section 44 of the Act addresses a range of offences thereby imposing a range of penalties on the contravener of such provision in the following manner:

Section 44	***Authority***	***Applicability***	***Penalty Amount***
Clause (a)	Controller or the Certifying Authority	Subscribers, Auditors, Computer Resource Incharge, etc.	Not exceeding Rs. 1,50,000/- (Rupees One Lakh and Fifty Thousand only) for each such failure.
Clause (b)	Controller, any government agency, statutory authority	Subscribers, Auditors, Computer Resource Incharge, etc.	Not exceeding Rs. 5,000/- (Rupees Five Thousand only) for each day during such continuing failure.
Clause (c)	Controller, any government agency, statutory authority	Certifying Authority, Computer Resource Incharge, etc.	Not exceeding Rs. 10,000/- (Rupees Ten Thousand only) for each day during such continuing failure

Section 45 is in essence effective against all contraventions for which no separate penalty has been provided.[107] Therefore, unless an offence is carefully judged and categorized under sections

[106] National Institute of Standards Technology *Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.*
<http://dx.doi.org/10.6028/NIST.SP.800-30r1>

43, 43A or 44, it will by default invoke section 45. A summary of the penalties associated with the provisions is provided hereunder:[108]

Contraventions under the Act	***Penalty Amount***
Section 43 – Penalty and compensation for damage to computers and computer systems	i) Less than Rs. 5,00,00,000/- (Rupees Five Crores only) before the adjudicating officer ii) More than Rs. 5,00,00,000/- (Rupees Five Crores only) before the competent civil court.
Section 44 – Penalty for failure to furnish information, return, etc.	i) Less than Rs. 1,50,000/- (Rupees One Lakh and Fifty Thousand only) for each such failure. ii) Not exceeding Rs. 5,000/- (Rupees Five Thousand only) for each day during such continuing failure. iii) Not exceeding Rs. 10,000/- (Rupees Ten Thousand only) for each day during such continuing failure
Section 45 – Residuary Penalty	Not exceeding Rs. 25,000/- (Rupees Twenty Five Thousand only).

1.5 LET'S SUM UP

In this chapter, we have studied the concept of offences in cyber law along with those provisions that are applicable to Certifying Authorities and their Controller. Finally, we have ended the discussion with the penalties in respect of damage to systems associated with cyberspace.

[107] <http://www.meity.gov.in/content/information-technology-act-2000>
[108] The Gazette of India, The Information and Technology Act, 2000, no. 27 of 2000, The Ministry of Law, Justice and Company Affairs, Part II, New Delhi

1.6 FURTHER READING

- Zenithresearch.org.in (2019), http://zenithresearch.org.in/images/stories/pdf/2012/May/ZIJBEMR/13_ZIBEMR_VOL2_ISSUE5_MAY2012.pdf (last visited Nov 22, 2019).
- Indian - Computer Emergency Response Team, Cert-in.org.in (2019), https://www.cert-in.org.in (last visited Nov 22, 2019).

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the powers of the controller to give directions?**

As per Section 68 of the Act, The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder. (2) Any person who intentionally and knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction or imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both.

2. **What is the punishment for misrepresentation?**

As per Section 71 of the Act, whoever makes any misrepresentation to or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both.

3. **Give a brief overview of the provisions with respect to damages to systems associated with cyberspace?**

a) Section 43 lists the various instances wherein there could be damage caused to computers or their systems or networks.

b) Section 43 A deals with an act of failure to protect sensitive data and entails payment of damages by the contravener by way of compensation.

c) Section 44 directs for a penalty to be provided for failure in furnishing information by any person who is required by the Act to provide such information or file any return or maintain books of accounts.

d) Section 45 addresses residuary penalty towards those who violates the rules and regulations made in association with the Act and for the specific contravention of which no penalty has separately been provided.

1.7 ACTIVITY

Discuss the powers of the investigating machinery under the Information Technology Act, 2000. (1000 words)