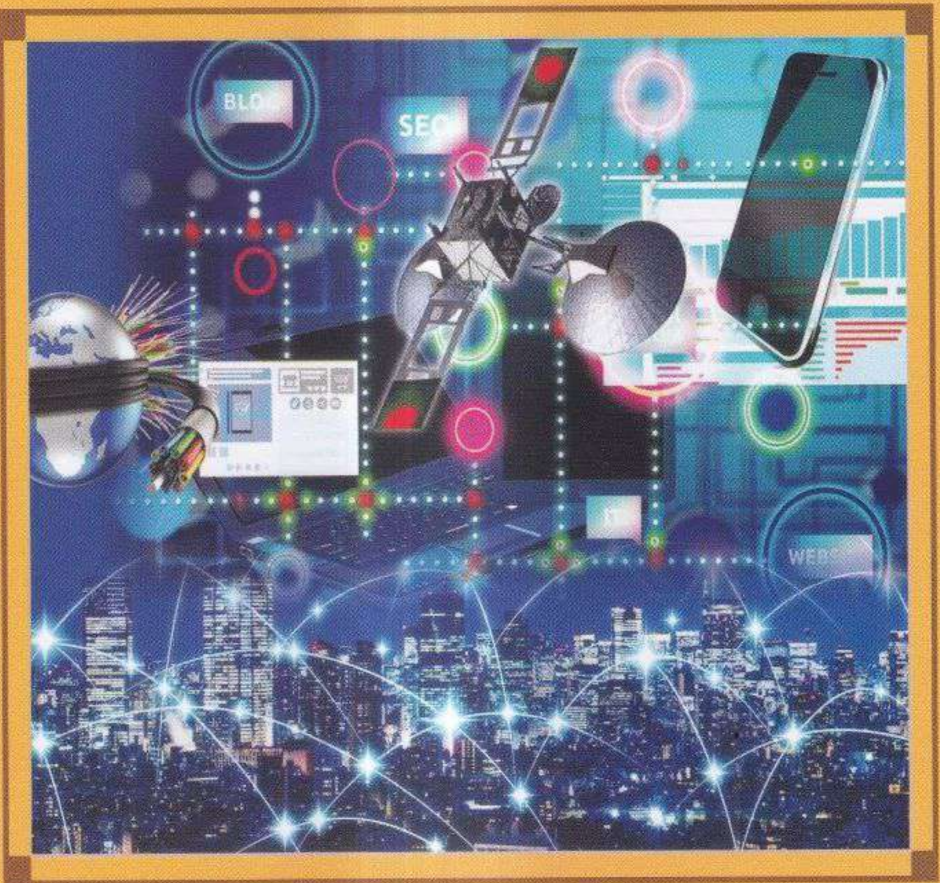
CYBER LAW & CRIMES

With Amendments and Available Rulings

Third Edition



Justice Md. Azizul Haque

Universal Book House

সংক্ষিপ্ত সূচিপত্র

- About Cyber Crime & Law xxxiii
- তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ ৫৭
- সাইবার নিরাপত্তা আইন, ২০২৩ ১৬৩
- ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ ২৪১
- পর্নোগ্রাফি নিয়ন্ত্রণ আইন, ২০১২ ২৫৯
- সরকারি ই-মেইল নীতিমালা ২০১৮ ২৬৭
- জাতীয় তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা, ২০১৮ ২৭৭
- জাতীয় সম্প্রচার নীতিমালা, ২০১৪ ৩৫৯
- জাতীয় অনলাইন গণমাধ্যম নীতিমালা, ২০১৭ (সংশোধিত ২০২০) ৩৬৯
- কেবল টেলিভিশন নেটওয়ার্ক পরিচালনা আইন, ২০০৬ ৩৭৫
- কেবল টেলিভিশন নেটওয়ার্ক পরিচালনা ও লাইসেন্সিং বিধিমালা, ২০১০ ৩৮৩
- আদালত কর্তৃক তথ্য-প্রযুক্তি ব্যবহার আইন, ২০২০ ৩৯৯
- তথ্য অধিকার আইন, ২০০৯ ৪০১
- তথ্য অধিকার (তথ্য প্রাপ্তি সংক্রান্ত) বিধিমালা, ২০০৯ ৪৩৭
- অপরাধ সম্পর্কিত বিষয়ে পারস্পরিক সহায়তা আইন, ২০১২ ৪৪৩
- অপরাধ সম্পর্কিত বিষয়ে পারস্পরিক সহায়তা বিধিমালা, ২০১৩ ৪৫৭
- জাতীয় জরুরি সেবা ৯৯৯ নীতিমালা, ২০২০ ৪৭৩
- তথ্য ও যোগাযোগ প্রযুক্তি (তদন্ত পরিচালনা) বিধিমালা, ২০২২ ৪৮১

সূচীপত্র

About Cyber Crime & Law xxxiii

তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬

প্রথম অধ্যায়
প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম, প্রয়োগ এবং প্রবর্তন ৫৭
২। সংজ্ঞা ৫৮
৩। আইনের প্রাধান্য ৬৩
৪। আইনের অতিরাষ্ট্রিক প্রয়োগ ৬৩

দ্বিতীয় অধ্যায়
ইলেকট্রনিক স্বাক্ষর ও ইলেক্ট্রনিক রেকর্ড

৫। ইলেক্ট্রনিক স্বাক্ষর দ্বারা ইলেক্ট্রনিক রেকর্ড সত্যায়ন ৭২
৬। ইলেক্ট্রনিক রেকর্ডের আইনানুগ স্বীকৃতি ৭২
৭। ইলেক্ট্রনিক স্বাক্ষরের আইনানুগ স্বীকৃতি ৭২
৮। সরকারী অফিস, ইত্যাদিতে ইলেক্ট্রনিক রেকর্ড এবং ইলেক্ট্রনিক স্বাক্ষরের ব্যবহার ৭৩
৯। ইলেক্ট্রনিক রেকর্ড সংরক্ষণ ৭৪
১০। ইলেক্ট্রনিক গেজেট ৭৫
১১। ইলেক্ট্রনিক পদ্ধতিতে দলিল গ্রহণে বাধ্যবাধকতা না থাকা ৭৫
১২। ইলেক্ট্রনিক স্বাক্ষর বিষয়ে বিধি প্রণয়ন ৭৫

তৃতীয় অধ্যায়
ইলেক্ট্রনিক রেকর্ডের স্বীকৃতি, প্রাপ্তি স্বীকার ও প্রেরণ

১৩। স্বীকৃতি ৭৬
১৪। প্রাপ্তি স্বীকার ৭৯
১৫। ইলেক্ট্রনিক রেকর্ড প্রেরণ ও গ্রহণের সময় এবং স্থান ৮০

চতুর্থ অধ্যায়
নিরাপদ ইলেক্ট্রনিক রেকর্ড ও নিরাপদ ইলেক্ট্রনিক স্বাক্ষর

১৬। নিরাপদ ইলেক্ট্রনিক রেকর্ড ৮২
১৭। নিরাপদ ইলেক্ট্রনিক স্বাক্ষর ৮২

পঞ্চম অধ্যায়
নিয়ন্ত্রক ও সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ

১৮। নিয়ন্ত্রক ও অন্যান্য কর্মকর্তা, ইত্যাদি ৮৩
১৯। নিয়ন্ত্রকের কার্যাবলী ৮৪
২০। বিদেশী সার্টিফিকেট প্রদানকারী কর্তৃপক্ষকে স্বীকৃতি ৮৬
২১। নিয়ন্ত্রকের সংরক্ষণাধার (repository) হিসাবে দায়িত্ব পালন ৮৭
২২। ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট ইস্যুর জন্য লাইসেন্স ৮৭
২৩। লাইসেন্সের জন্য আবেদন ৮৭
২৪। লাইসেন্স নবায়ন ৮৮
২৫। লাইসেন্স মঞ্জুর বা অগ্রাহ্য করিবার প্রক্রিয়া ৮৮

CONTENTS

About Cyber Crime & Law xxxiii

Information and Communication Technology Act, 2006

CHAPTER I
Preliminary

1. Short title, extent and commencement 57
2. Definitions 58
3. Act to override other laws 63
4. Extra territorial application of the Act 63

CHAPTER II
Electronic Signatures & Electronic Records

5. Certification of electronic record by electronic signature 72
6. Legal recognition of electronic record 72
7. Legal recognition of electronic signatures 72
8. Use of electronic record and electronic signature in Government office, etc. 73
9. Retention of electronic records 74
10. Electronic Gazette 75
11. No obligation on receiving document in electronic form 75
12. Making rules in respect of electronic signature 75

CHAPTER III
Recognition, Acknowledgement and Despatch of Electronic Record

13. Recognition 76
14. Acknowledgement 79
15. Time and place of despatch and receipt of electronic record 80

CHAPTER IV
Secure Electronic Records and Secure Electronic Signatures

16. Secure electronic record 82
17. Secure electronic signature 82

CHAPTER V
Controller and Certificate Issuing Authority

18. Controller and other officers, etc 83
19. Functions of the Controller 84
20. Recognition to foreign certificate issuing authority 86
21. Controller to act as repository 87
22. Licence to issue electronic signature certificate 87
23. Application for licence 87
24. Renewal of licence 88
25. Process for grant or rejection of licence 88

২৬। লাইসেন্স বাতিল বা স্থগিতকরণ ৮৮
২৭। লাইসেন্স বাতিল বা স্থগিতের নোটিশ ৮৯
২৮। ক্ষমতা অর্পণ ৯০
২৯। তদন্তের ক্ষমতা ৯০
৩০। কম্পিউটার এবং উহাতে ধারণকৃত উপাত্তে প্রবেশ ৯০
৩১। কতিপয় বিষয়ে সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ কর্তৃক অনুসরণীয় বিধান ৯১
৩২। সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ কর্তৃক আইন, ইত্যাদির, প্রতিপালন নিশ্চিতকরণ ৯১
৩৩। লাইসেন্স প্রদর্শন ৯২
৩৪। লাইসেন্স সমর্পণ ৯২
৩৫। কতিপয় বিষয় প্রকাশ করা ৯২
৩৬। সার্টিফিকেট ইস্যুকরণ ৯৩
৩৭। সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিশ্চয়তা প্রদান ৯৪
৩৮। ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট বাতিল ৯৫
৩৯। ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট স্থগিতকরণ ৯৬
৪০। বাতিল বা স্থগিতকরণের নোটিশ ৯৭

ষষ্ঠ অধ্যায়
গ্রাহকের দায়িত্বাবলী

৪১। নিরাপত্তা পদ্ধতির প্রয়োগ ৯৭
৪২। ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট গ্রহণ ৯৭
৪৩। সার্টিফিকেট পাইবার ক্ষেত্রে উপস্থাপিত তথ্য সম্পর্কে অনুমান ৯৮
৪৪। গ্রাহকের নিরাপত্তা ব্যবস্থার নিয়ন্ত্রণ ৯৮

সপ্তম অধ্যায়
আইনের বিধান লঙ্ঘন, প্রতিবিধান ও জরিমানা আরোপ, ইত্যাদি

৪৫। নির্দেশ প্রদানে নিয়ন্ত্রকের ক্ষমতা ৯৯
৪৬। জরুরী পরিস্থিতিতে নিয়ন্ত্রকের নির্দেশ প্রদানের ক্ষমতা ৯৯
৪৭। সংরক্ষিত সিস্টেম ঘোষণার ক্ষমতা ১০০
৪৮। ডকুমেন্ট, রিটার্ণ ও রিপোর্ট প্রদানে ব্যর্থতার প্রতিবিধান ১০০
৪৯। তথ্য, বই, ইত্যাদি জমা করিতে ব্যর্থতার প্রতিবিধান ১০০
৫০। হিসাব বই বা রেকর্ড সংরক্ষণে ব্যর্থতার প্রতিবিধান ১০১
৫১। অন্যান্য ক্ষেত্রে জরিমানা ১০১
৫২। সম্ভাব্য লংঘনের ক্ষেত্রে নিয়ন্ত্রকের নিষেধাজ্ঞামূলক আদেশদানের ক্ষমতা ১০১
৫৩। জরিমানা ১০২

অষ্টম অধ্যায়
অপরাধ, তদন্ত, বিচার, দন্ড ইত্যাদি
অংশ-১
অপরাধ ও দণ্ড

৫৪। বিলুপ্ত ১০৩
৫৫। বিলুপ্ত ১০৩
৫৬। বিলুপ্ত ১০৩
৫৭। বিলুপ্ত ১০৩
৫৮। লাইসেন্স সমর্পণে ব্যর্থতা ও উহার দণ্ড ১০৩

26. Revocation and suspension of licence 88
27. Notice of revocation or suspension of licence 89
28. Delegation of Power 90
29. Power of investigation 90
30. Access to computers and data stored in it 90
31. Provisions to be followed by Certificate Issuing Authority in certain matters 91
32. To ensure compliance of Act, etc. by Certificate Issuing Authority 91
33. Display of licence 92
34. Surrender of licence 92
35. Disclosure of certain matters 92
36. To issue certificate 93
37. Assurance of Certificate Issuing Authority 94
38. Revocation of Electronic Signature Certificate 95
39. Suspension of Electronic Signature Certificate 96
40. Notice of revocation or suspension 97

CHAPTER VI

Duties of Subscriber

41. Application of security procedure 97
42. Acceptance of Electronic Signature Certificate 97
43. Presumption about information submitted for obtaining certificate 98
44. Control of safety measure of subscriber 98

CHAPTER VII

Contravention of Provision of act, Remedy and Imposition of Fine, etc.

45. Power of Controller to give directions 99
46. Power of Controller to give directions in emergency 99
47. Power to declare protected system 100
48. Remedy of failure to furnish document, return and report 100
49. Remedy of failure to submit information, book, etc 100
50. Remedy of failure to maintain accounts, book or record 101
51. Fine in other cases 101
52. Power of Controller to issue prohibitory order in case of probable contravention 101
53. Fine 102

CHAPTER VIII

Offence, Investigation, Trial, Punishment, etc.

PART-1:

Offence and Punishment

54. [Omitted] 103
55. [Omitted] 103
56. [Omitted] 103
57. [Omitted] 103
58. Failure to surrender licence and its punishment 103

৫৯। নির্দেশ লঙ্ঘন সংক্রান্ত অপরাধ ও উহার দণ্ড ১০৪
৬০। জরুরী পরিস্থিতিতে নিয়ন্ত্রকের নির্দেশ অমান্যে দণ্ড ১০৪
৬১। সংরক্ষিত সিস্টেমে প্রবেশ সংক্রান্ত অপরাধ ও উহার দণ্ড ১০৬
৬২। মিথ্যা প্রতিনিধিত্ব ও তথ্য গোপন সংক্রান্ত অপরাধ ও উহার দণ্ড ১০৬
৬৩। গোপনীয়তা প্রকাশ সংক্রান্ত অপরাধ ও উহার দণ্ড ১০৭
৬৪। ভুয়া (false) ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ সংক্রান্ত অপরাধ ও দণ্ড ১০৮
৬৫। প্রতারণার উদ্দেশ্যে ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ, ইত্যাদি সংক্রান্ত অপরাধ ও উহার দণ্ড ১০৯
৬৬। বিলুপ্ত ১১০
৬৭। কোম্পানী, ইত্যাদি কর্তৃক অপরাধ সংঘটন ১১০

অংশ-২

সাইবার ট্রাইব্যুনাল প্রতিষ্ঠা, অপরাধের তদন্ত, বিচার, আপীল, ইত্যাদি

৬৮। সাইবার ট্রাইব্যুনাল গঠন ১১১
৬৯। সাইবার ট্রাইব্যুনালের বিচার পদ্ধতি ১১২
৭০। ট্রাইব্যুনালের কার্যক্রমে ফৌজদারী কার্যবিধির প্রয়োগ ১১৪
৭১। জামিন সংক্রান্ত বিধান ১২৮
৭২। রায় প্রদানের সময়সীমা ১৩৬
৭৩। ট্রাইব্যুনাল কর্তৃক মামলা নিষ্পত্তির নির্ধারিত সময়সীমা ১৩৬
৭৪। দায়রা আদালত কর্তৃক অপরাধের বিচার ১৩৭
৭৫। দায়রা আদালত কর্তৃক অনুসরণীয় বিচার পদ্ধতি ১৩৭
৭৬। অপরাধ তদন্তের ক্ষমতা, ইত্যাদি ১৩৮
৭৭। বাজেয়াপ্তি ১৪০
৭৮। দণ্ড বা বাজেয়াপ্তকরণ অন্য কোন শাস্তি প্রদানে বাধা না হওয়া ১৪১
৭৯। কতিপয় ক্ষেত্রে নেটওয়ার্ক সেবা প্রদানকারী দায়ী না হওয়া ১৪১
৮০। *** আটক বা গ্রেফতারের ক্ষমতা ১৪২
৮১। তল্লাশী, ইত্যাদির পদ্ধতি ১৪২

অংশ-৩

সাইবার আপীল ট্রাইব্যুনাল গঠন, ইত্যাদি

৮২। সাইবার আপীল ট্রাইব্যুনাল গঠন ১৫৭
৮৩। সাইবার আপীল ট্রাইব্যুনালের এখতিয়ার ও পদ্ধতি ১৫৮
৮৪। সাইবার আপীল ট্রাইব্যুনাল গঠিত না হইবার ক্ষেত্রে আপীল পদ্ধতি ১৫৮

নবম অধ্যায়

বিবিধ

৮৫। জনসেবক ১৫৯
৮৬। সরল বিশ্বাসে কৃত কর্ম রক্ষণ ১৫৯
৮৭। কতিপয় আইনে ব্যবহৃত কতিপয় সংজ্ঞার বর্ধিত অর্থে প্রয়োগ ১৫৯
৮৮। বিধি প্রণয়নের ক্ষমতা ১৬০
৮৯। প্রবিধান প্রণয়নের ক্ষমতা ১৬১
৯০। মূল পাঠ ও ইংরেজীতে পাঠ ১৬২

সাইবার নিরাপত্তা আইন, ২০২৩

প্রথম অধ্যায়
প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ১৬৪
২। সংজ্ঞা ১৬৪
৩। আইনের প্রয়োগ ১৬৮
৪। আইনের অতিরাষ্ট্রিক প্রয়োগ ১৬৮

দ্বিতীয় অধ্যায়
জাতীয় সাইবার নিরাপত্তা এজেন্সি

৫। এজেন্সি গঠন, কার্যালয়, ইত্যাদি ১৭৮
৬। মহাপরিচালক ও পরিচালকগণের নিয়োগ, ইত্যাদি ১৭৮
৭। এজেন্সির জনবল ১৭৯

তৃতীয় অধ্যায়
প্রতিরোধমূলক ব্যবস্থাদি

৮। কতিপয় তথ্য-উপাত্ত অপসারণ বা ব্লক করিবার ক্ষমতা ১৭৯
৯। কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ১৮০
১০। ডিজিটাল ফরেনসিক ল্যাব ১৮১
১১। ডিজিটাল ফরেনসিক ল্যাব এর মান নিয়ন্ত্রণ ১৮২

চতুর্থ অধ্যায়
জাতীয় সাইবার নিরাপত্তা কাউন্সিল

১২। জাতীয় সাইবার নিরাপত্তা কাউন্সিল ১৮২
১৩। কাউন্সিলের ক্ষমতা, ইত্যাদি ১৮৪
১৪। কাউন্সিলের সভা, ইত্যাদি ১৮৪

পঞ্চম অধ্যায়
গুরুত্বপূর্ণ তথ্য পরিকাঠামো

১৫। গুরুত্বপূর্ণ তথ্য পরিকাঠামো ১৮৫
১৬। গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তা পরিবীক্ষণ ও পরিদর্শন ১৮৫

ষষ্ঠ অধ্যায়
অপরাধ ও দণ্ড

১৭। গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে বে-আইনি প্রবেশ, ইত্যাদির দণ্ড ১৮৬
১৮। কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম, ইত্যাদিতে বে-আইনি প্রবেশ ও দণ্ড ১৮৭
১৯। কম্পিউটার, কম্পিউটার সিস্টেম, ইত্যাদির ক্ষতিসাধন ও দণ্ড ১৮৯
২০। কম্পিউটার সোর্স কোড পরিবর্তন সংক্রান্ত অপরাধ ও দণ্ড ১৯২
২১। মুক্তিযুদ্ধ, মুক্তিযুদ্ধের চেতনা, জাতির পিতা বঙ্গবন্ধু শেখ মুজিবুর রহমান, জাতীয় সংগীত বা জাতীয় পতাকা সম্পর্কে বিদ্বেষ, বিভ্রান্তি ও কুৎসামূলক প্রচারণার দণ্ড ১৯৩
২২। ডিজিটাল বা ইলেকট্রনিক জালিয়াতি ১৯৪
২৩। ডিজিটাল বা ইলেকট্রনিক প্রতারণা ১৯৫
২৪। পরিচয় প্রতারণা বা ছদ্মবেশ ধারণ ১৯৭
২৫। আক্রমণাত্মক, মিথ্যা বা ভীতি প্রদর্শক, তথ্য-উপাত্ত প্রেরণ, প্রকাশ, ইত্যাদি ১৯৮

২৬। অনুমতি ব্যতীত পরিচিতি তথ্য সংগ্রহ, ব্যবহার, ইত্যাদির দণ্ড ২০০
২৭। সাইবার সন্ত্রাসী কার্য সংঘটনের অপরাধ ও দণ্ড ২০১
২৮। ওয়েবসাইট বা কোনো ইলেকট্রনিক বিন্যাসে ধর্মীয় মূল্যবোধ বা অনুভূতিতে আঘাত করে এমন কোনো তথ্য প্রকাশ, সম্প্রচার, ইত্যাদি ২০৩
২৯। মানহানিকর তথ্য প্রকাশ, প্রচার, ইত্যাদি ২০৪
৩০। আইনানুগ কর্তৃত্ব বহির্ভূত ই-ট্রানজেকশনের অপরাধ ও দণ্ড ২০৫
৩১। আইন-শৃঙ্খলার অবনতি ঘটানো, ইত্যাদির অপরাধ ও দণ্ড ২০৬
৩২। হ্যাকিং সংক্রান্ত অপরাধ ও দণ্ড ২০৭
৩৩। অপরাধ সংঘটনের সহায়তা ও উহার দণ্ড ২০৮
৩৪। মিথ্যা মামলা, অভিযোগ দায়ের, ইত্যাদির অপরাধ ও দণ্ড ২০৮
৩৫। কোম্পানি কর্তৃক অপরাধ সংঘটন ২০৯
৩৬। ক্ষতিপূরণের আদেশ দানের ক্ষমতা ২১০
৩৭। সেবা প্রদানকারী দায়ী না হওয়া ২১০

সপ্তম অধ্যায়

অপরাধের তদন্ত ও বিচার

৩৮। তদন্ত, ইত্যাদি ২১০
৩৯। তদন্তের সময়সীমা, ইত্যাদি ২১০
৪০। তদন্তকারী অফিসারের ক্ষমতা ২১১
৪১। পরোয়ানার মাধ্যমে তল্লাশী ও জব্দ ২১২
৪২। পরোয়ানা ব্যতিরেকে তল্লাশি, জব্দ ও গ্রেফতার ২১৩
৪৩। তথ্য সংরক্ষণ ২৩০
৪৪। কম্পিউটারের সাধারণ ব্যবহার ব্যাহত না করা ২৩০
৪৫। তদন্তে সহায়তা ২৩১
৪৬। তদন্তে প্রাপ্ত তথ্যের গোপনীয়তা ২৩১
৪৭। অপরাধ বিচারার্থ গ্রহণ, ইত্যাদি ২৩২
৪৮। অপরাধের বিচার ও আপিল ২৩২
৪৯। ফৌজদারি কার্যবিধির প্রয়োগ ২৩৩
৫০। বিশেষজ্ঞ মতামত গ্রহণ, প্রশিক্ষণ, ইত্যাদি ২৩৩
৫১। মামলা নিষ্পত্তির জন্য নির্ধারিত সময়সীমা ২৩৪
৫২। অপরাধের আমলযোগ্যতা ও জামিনযোগ্যতা ২৩৪
৫৩। বাজেয়াপ্তি ২৩৫

অষ্টম অধ্যায়

আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা

৫৪। আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা ২৩৬

নবম অধ্যায়

বিবিধ

৫৫। ক্ষমতা অর্পণ ২৩৬
৫৬। সাক্ষ্যগত মূল্য ২৩৬
৫৭। অসুবিধা দূরীকরণ ২৩৬
৫৮। বিধি প্রণয়নের ক্ষমতা ২৩৬
৫৯। রহিতকরণ ও হেফাজত ২৩৭
৬০। ইংরেজিতে অনূদিত পাঠ প্রকাশ ২৩৯

ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০

১।	সংক্ষিপ্ত শিরোনাম	২৪১
২।	সংজ্ঞা	২৪১
৩।	ডিজিটাল নিরাপত্তা এজেন্সির ক্ষমতা	২৪১
৪।	ডিজিটাল নিরাপত্তা এজেন্সির দায়িত্ব ও কার্যাবলি	২৪২
৫।	মহাপরিচালকের ক্ষমতা ও দায়িত্ব	২৪৩
৬।	জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিমের দায়িত্ব ও কার্যাবলি	২৪৩
৭।	ডিজিটাল নিরাপত্তা সংক্রান্ত তথ্যপ্রেরণ, ইত্যাদি	২৪৪
৮।	জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এর কার্যালয়	২৪৫
৯।	জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এর সার্বক্ষণিক দায়িত্ব	২৪৫
১০।	তথ্য বিনিময়	২৪৫
১১।	ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা সম্পর্কে ব্যবস্থা গ্রহণ	২৪৫
১২।	গুরুত্বপূর্ণ তথ্য পরিকাঠামোর মূল্যায়ন	২৪৬
১৩।	ডিজিটাল ফরেনসিক ল্যাব স্থাপন	২৪৭
১৪।	ডিজিটাল ফরেনসিক ল্যাব কর্তৃক অনুসরণীয় মানদন্ড	২৪৭
১৫।	সাক্ষ্যের ফরেনসিক বিশ্লেষণ	২৪৮
১৬।	ডিজিটাল ফরেনসিক ল্যাবের জনবল	২৪৮
১৭।	গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনাকারী ব্যক্তি বা প্রতিষ্ঠান কর্তৃক অনুসরণীয় বাধ্যবাধকতা	২৪৮
১৮।	গুরুত্বপূর্ণ তথ্য পরিকাঠামো নিরীক্ষা	২৪৯
১৯।	গুরুত্বপূর্ণ তথ্য পরিকাঠামো চিহ্নিতকরণ, ইত্যাদি	২৫০
২০।	সংশ্লিষ্ট ব্যক্তি বা প্রতিষ্ঠানের সহায়তা গ্রহণ	২৫০
	তফসিল: ডিজিটাল ফরেনসিক পরীক্ষা পদ্ধতিসমূহ	২৫০

সরকারি ই-মেইল নীতিমালা ২০১৮

১.০ ভূমিকা ২৬৭
২.০ সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ২৬৮
৩.০ উদ্দেশ্যসমূহ (Objectives) ২৬৮
৪.০ পরিধি (Scope) ২৬৮
৫.০ ঐচ্ছিকভাবে (Optionally) সরকারি ই-মেইল সেবা ব্যবহার ২৬৮
৬.০ ই-মেইল ডোমেইন ও নামকরণ ২৬৯
৭.০ পাসওয়ার্ড এবং গোপনীয়তা ২৬৯
৮.০ ই-মেইল একাউন্ট ব্যবস্থাপনা ২৬৯
৯.০ গোপনীয়তা রক্ষা ২৬৯
১০.০ ই-মেইল সেবার নিরাপত্তা রক্ষা ২৭০
১০.১ ই-মেইল সেবার নিরাপত্তা ২৭০
১০.২ সরকারি ই-মেইল সেবা ব্যবহারকারীগণ কর্তৃক অনুসরণীয় কার্যক্রম ২৭০
১১.০ সেবা সহায়তা (Support Services) ২৭০
১২.০ বাস্তবায়নকারী সংস্থার ভূমিকা ও দায়িত্ব ২৭০
১৩.০ ই-মেইল ব্যবহারকারী প্রতিষ্ঠানে (User Organization) ভূমিকা ও দায়িত্ব ২৭২
১৩.২ নীতিমালা প্রচার (Policy Dissemination) ২৭২
১৪.০ ই-মেইল ব্যবহারকারীর (User) দায়িত্ব ২৭২
১৪.১ ই-মেইল সেবার যথাযথ ব্যবহার নিশ্চিতকরণ ২৭২
১৪.২ সরকারি ই-মেইল সেবা ব্যবহারে পরিহারযোগ্য বিষয়াবলি ২৭৩
১৫.০ ই-মেইল পরিচালনাকারী কর্মকর্তা (E-mail Admin Officer) বা ফোকাল পয়েন্ট কর্মকর্তার ভূমিকা ও দায়িত্ব ২৭৩
১৬.০ ই-মেইলের সূক্ষ্ম নিরীক্ষণ (Scrutiny) ও রিলিজ লগস (Release Logs) ২৭৩
১৭.০ নিরাপত্তাজনিত ঘটনা (Security Incident) ব্যবস্থাপনা প্রক্রিয়া ২৭৩
১৮.০০ মেধাসম্প (Intellectual Property) ২৭৪
১৯.০ ই-মেইল সেবার হিসাব নিরীক্ষা (Audit) ২৭৪
২০.০ নীতিমালা পর্যালোচনা (Review) ২৭৪
২১.০ সংযুক্তি-ক : আদ্যক্ষর এবং সংক্ষেপণ ২৭৪
২২.০ সংযুক্তি-খ : শব্দকোষ (Glossary) ২৭৪

জাতীয় তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা, ২০১৮

অধ্যায়-১

সংক্ষিপ্ত শিরোনাম, প্রবর্তন ও সংজ্ঞা

১.১. সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ২৭৭
১.২. সংজ্ঞা বিষয় বা প্রসঙ্গের পরিপন্থী কিছু না থাকলে এ নীতিমালায় ২৭৭

অধ্যায়-২

রূপকল্প ও উদ্দেশ্য

২.১. রূপকল্প (Vision) ২৭৮
২.২. উদ্দেশ্যসমূহ (Objectives) ২৭৯

অধ্যায়-৩

কৌশলগত বিষয়বস্তু

৩.১ ডিজিটাল সরকার (Digital Government) ২৭৯

চতুর্থ অধ্যায়

বিজ্ঞাপন সম্প্রচার

৪.১ রাজনৈতিক এবং ধর্মীয় বক্তব্য ৩৬৩
৪.২ পণ্য, পণ্যের মান এবং ভোক্তা অধিকার সংরক্ষণ ৩৬৩
৪.৩ মহান মুক্তিযুদ্ধ, ভাষা এবং সংস্কৃতি ৩৬৪
৪.৪ শিশু এবং নারীর অধিকার ৩৬৪
৪.৫ বিবিধ ৩৬৪

পঞ্চম অধ্যায়

সম্প্রচারের ক্ষেত্রে অন্যান্য বিবেচ্য বিষয় ৩৬৫

ষষ্ঠ অধ্যায়

সম্প্রচার কমিশন

৬.১ সম্প্রচার কমিশন গঠন ৩৬৬
৬.২ অভিযোগ ও নিষ্পত্তি ৩৬৭

জাতীয় অনলাইন গণমাধ্যম নীতিমালা, ২০১৭ ৩৬৯

কেবল টেলিভিশন নেটওয়ার্ক পরিচালনা আইন, ২০০৬

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ৩৭৫
২। সংজ্ঞা ৩৭৫
৩। চ্যানেল ডাউন লিংক, বিপণন, ইত্যাদি ৩৭৬
৪। লাইসেন্স ৩৭৬
৫। লাইসেন্স প্রদান পদ্ধতি ৩৭৭
৬। লাইসেন্স নামঞ্জুর সংক্রান্ত আপীল ৩৭৭
৭। লাইসেন্সের মেয়াদ ও শর্তাবলী ৩৭৭
৮। লাইসেন্স প্রদানে অনুসরণীয় নীতি ৩৭৮
৯। কতিপয় ব্যক্তির ক্ষেত্রে লাইসেন্স প্রদানের বাধা-নিষেধ ৩৭৮
১০। লাইসেন্সিং কর্তৃপক্ষের ক্ষমতা ৩৭৮
১১। লাইসেন্স স্থগিত বা বাতিলকরণ ৩৭৮
১২। পরামর্শক কমিটি ৩৭৯
১৩। ফ্রিকোয়েন্সী বরাদ্দ সম্পর্কিত লাইসেন্স গ্রহণ, ইত্যাদি ৩৭৯
১৪। লাইসেন্সের ডুপ্লিকেট বা অনুলিপি প্রদান ৩৭৯
১৫। অনুমোদিত চ্যানেল সঞ্চালন বা সম্প্রচার স্থগিতকরণ, ইত্যাদি ৩৭৯
১৬। সরকারী ও বেসরকারী চ্যানেল সঞ্চালন ৩৭৯
১৭। গ্রাহক সেবা ৩৭৯
১৮। গ্রাহকদের অভিযোগ গ্রহণ ও নিষ্পত্তি ৩৮০
১৯। সম্প্রচার বা সঞ্চালনের ক্ষেত্রে বাধা-নিষেধ ৩৮০
২০। জনস্বার্থে কেবল টেলিভিশন নেটওয়ার্কের কার্যক্রম নিষিদ্ধকরণের ক্ষমতা ৩৮১
২১। সেবাপ্রদানকারী কর্তৃক রেজিস্টার সংরক্ষণ ৩৮১
২২। চ্যানেলের মূল্য পরিশোধ, ইত্যাদি ৩৮১
২৩। আটককৃত যন্ত্রপাতির বাজেয়াপ্তকরণ, ইত্যাদি ৩৮১
২৪। ক্ষমতা অর্পণ ৩৮১
২৫। অন্যান্য সংস্থার অনুমোদন গ্রহণ ৩৮১

২৬। অপরাধের অ-আমলযোগ্যতা ও জামিনযোগ্যতা ৩৮১
২৭। কোম্পানী কর্তৃক অপরাধ সংঘটন ৩৮১
২৮। শাস্তি ৩৮১
২৯। অপরাধের বিচার ৩৮২
৩০। অর্থদণ্ড আরোপের ক্ষেত্রে ম্যাজিস্ট্রেটের বিশেষ ক্ষমতা ৩৮২
৩১। সরল বিশ্বাসে কৃত কাজকর্ম রক্ষণ ৩৮২
৩২। অন্যান্য আইনের প্রয়োগ ৩৮২
৩৩। অন্যান্য আইনের উপর প্রাধান্য ৩৮২
৩৫। বিধি প্রণয়নের ক্ষমতা ৩৮২
৩৬। আইনের ইংরেজী অনুবাদ প্রকাশ ৩৮২

কেবল টেলিভিশন নেটওয়ার্ক পরিচালনা ও লাইসেন্সিং বিধিমালা, ২০১০

প্রথম অধ্যায়
সূচনা

১। সংক্ষিপ্ত শিরোনাম ৩৮৩
২। সংজ্ঞা ৩৮৩

দ্বিতীয় অধ্যায়
লাইসেন্স প্রদান, ইত্যাদি

৩। লাইসেন্স প্রদান, ইত্যাদি ৩৮৪
৪। লাইসেন্সের ডুপ্লিকেট বা অনুলিপি প্রদান ৩৮৫
৫। লাইসেন্সের মেয়াদ ও লাইসেন্স নবায়ন ৩৮৬
৬। লাইসেন্স স্থগিত বা বাতিলকরণ ৩৮৬
৭। গ্রাহক সেবা, ইত্যাদি ৩৮৬
৮। সেবাপ্রদানকারী কর্তৃক রেজিস্টার সংরক্ষণ ৩৮৬
৯। সম্প্রচার বা সঞ্চালনের ক্ষেত্রে বাধা-নিষেধ ৩৮৬

তৃতীয় অধ্যায়
পরামর্শক কমিটি, ইত্যাদি

১০। পরামর্শক কমিটি গঠন, ইত্যাদি ৩৮৭
১১। দায়িত্ব ও কার্যাবলী ৩৮৭
১২। কমিটির সভা ৩৮৭
১৩। কমিটির সিদ্ধান্ত বাস্তবায়ন ৩৮৮
১৪। সভার ব্যয়, ইত্যাদি ৩৮৮

চতুর্থ অধ্যায়
শাস্তি, ইত্যাদি

১৫। শাস্তি, দণ্ড, ইত্যাদি ৩৮৮
তফসিল-১ ৩৯৫
তফসিল-২ ৩৯৬
তফসিল-৩ ৩৯৭
তফসিল-৪ ৩৯৮
তফসিল-৫ ৩৯৮

আদালত কর্তৃক তথ্য-প্রযুক্তি ব্যবহার আইন, ২০২০ ৩৯৯

তথ্য অধিকার আইন, ২০০৯

প্রথম অধ্যায়

প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ৪০২

২। সংজ্ঞা ৪০২

৩। আইনের প্রাধান্য ৪০৫

দ্বিতীয় অধ্যায়

তথ্য অধিকার, তথ্য সংরক্ষণ, প্রকাশ ও প্রাপ্তি

৪। তথ্য অধিকার ৪০৫

৫। তথ্য সংরক্ষণ ৪০৫

৬। তথ্য প্রকাশ ৪০৬

৭। কতিপয় তথ্য প্রকাশ বা প্রদান বাধ্যতামূলক নয় ৪০৭

৮। তথ্য প্রাপ্তির অনুরোধ ৪১০

৯। তথ্য প্রদান পদ্ধতি ৪১১

তৃতীয় অধ্যায়

দায়িত্বপ্রাপ্ত কর্মকর্তা

১০। দায়িত্বপ্রাপ্ত কর্মকর্তা ৪১৩

চতুর্থ অধ্যায়

তথ্য কমিশন প্রতিষ্ঠা, ইত্যাদি

১১। তথ্য কমিশন প্রতিষ্ঠা ৪১৪

১২। তথ্য কমিশন গঠন ৪১৫

১৩। তথ্য কমিশনের ক্ষমতা ও কার্যাবলী ৪১৫

১৪। বাছাই কমিটি ৪১৯

১৫। প্রধান তথ্য কমিশনার ও তথ্য কমিশনারগণের নিয়োগ, মেয়াদ, পদত্যাগ, ইত্যাদি ৪২০

১৬। প্রধান তথ্য কমিশনার ও তথ্য কমিশনারগণের অপসারণ ৪২২

১৭। তথ্য কমিশনারগণের পদমর্যাদা, পারিশ্রমিক ও সুবিধাদি ৪২২

১৮। তথ্য কমিশনের সভা ৪২২

পঞ্চম অধ্যায়

তথ্য কমিশনের আর্থিক বিষয়াদি

১৯। তথ্য কমিশন তহবিল ৪২৩

২০। বাজেট ৪২৪

২১। তথ্য কমিশনের আর্থিক স্বাধীনতা ৪২৪

২২। হিসাব রক্ষণ ও নিরীক্ষা ৪২৪

ষষ্ঠ অধ্যায়

তথ্য কমিশনের কর্মকর্তা ও কর্মচারী

২৩। তথ্য কমিশনের সচিব এবং অন্যান্য কর্মকর্তা ও কর্মচারী ৪২৫

তথ্য অধিকার (তথ্য প্রাপ্তি সংক্রান্ত) বিধিমালা, ২০০৯

১। সংক্ষিপ্ত শিরোনাম ৪৩৭
২। সংজ্ঞা ৪৩৭
৩। তথ্য প্রাপ্তির অনুরোধের আবেদনপত্র গ্রহণ ও প্রাপ্তি স্বীকার ৪৩৭
৪। তথ্য প্রদান, ইত্যাদি ৪৩৮
৫। তথ্য সরবরাহে অপরাগতা ৪৩৮
৬। আপীল আবেদন, ইত্যাদি ৪৩৮
৭। ইন্টারনেটসহ ডিজিটাল পদ্ধতির মাধ্যমে তথ্য প্রাপ্তি ৪৩৯
৮। তথ্য প্রাপ্তির অনুরোধ ফি এবং তথ্যের মূল্য নির্ধারণ, ইত্যাদি ৪৩৯
তফসিল ৪৩৯

অপরাধ সম্পর্কিত বিষয়ে পারস্পরিক সহায়তা আইন, ২০১২

অধ্যায়-১

প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ৪৪৩
২। সংজ্ঞা ৪৪৩

অধ্যায় -২

কেন্দ্রীয় কর্তৃপক্ষ

৩। কেন্দ্রীয় কর্তৃপক্ষ ৪৪৪
৪। কেন্দ্রীয় কর্তৃপক্ষের ক্ষমতা ও দায়িত্ব ৪৪৪
৫। উপদেষ্টা বোর্ড ৪৪৫
৬। উপদেষ্টা বোর্ডের কার্যপদ্ধতি ৪৪৫
৭। সিদ্ধান্তের চূড়ান্ততা ৪৪৬

অধ্যায়-৩

সহায়তা প্রদান এবং সহায়তার জন্য অনুরোধ

অংশ-১

সাধারণ বিধানাবলী

৮। সহায়তার পরিধি ৪৪৬
৯। সহায়তার অনুরোধ প্রেরণ ও গ্রহণ ৪৪৭
১০। সহায়তার অনুরোধ প্রত্যাখ্যান বা স্থগিত রাখা ৪৪৭
১১। অনুরোধ কার্যকরকরণ ৪৪৭
১২। অন্য আইনে সহায়তা প্রদান ৪৪৮
১৩। গোপনীয়তা প্রকাশ না করা ৪৪৮

অংশ-২

সহায়তার সুনির্দিষ্ট পদ্ধতি সংক্রান্ত

১৪। অনুসন্ধানের জন্য বিবৃতি ও সাক্ষ্য উপস্থাপন ৪৪৮
১৫। বাংলাদেশের আদালত কর্তৃক সাক্ষ্য (testimony) গ্রহণ ৪৪৮
১৬। সাক্ষ্য বা বিবৃতি গ্রহণ সম্পর্কিত বিশেষ বিধানাবলী ৪৪৯

১৭। কোন ব্যক্তি, সত্তা (entity) বা বস্তু সনাক্তকরণ ৪৪৯
১৮। ভিডিও কনফারেন্সিং প্রযুক্তির ব্যবহার ৪৪৯
১৯। তল্লাশি এবং আটক ৪৫০
২০। বাংলাদেশে আটক রহিয়াছে এমন ব্যক্তিকে হস্তান্তর ৪৫০
২১। ট্রানজিটকালীন কোন ব্যক্তির হেফাজত ৪৫০

অংশ-৩

ফ্রিজিং ও আটক এবং বাজেয়াপ্তকরণের অনুরোধ

২২। ফ্রিজিং বা আটকের আদেশ ৪৫১
২৩। বিদেশী আদালতের রায় বলবৎকরণ ৪৫১
২৪। তৃতীয় পক্ষের অধিকার ৪৫১
২৫। অপরাধের মাধ্যমে অর্জিত সম্পত্তির বিলি-বন্দেজ ৪৫২

অংশ-৪

সরকারী দপ্তরের দলিল বা তথ্যাদি সরবরাহ

২৬। সরকারী দপ্তরের দলিল বা তথ্যাদি সরবরাহ ৪৫২
২৭। ফৌজদারী কার্যধারার সূচনা ৪৫২

অংশ-৫

কম্পিউটার সিস্টেম এবং কম্পিউটার ড্যাটা সংক্রান্ত সহযোগিতা

২৮। কম্পিউটার ড্যাটা সংরক্ষণ ৪৫২
২৯। সংরক্ষিত কম্পিউটার ড্যাটা উপস্থাপন ৪৫২
৩০। কম্পিউটার ড্যাটা তল্লাশি এবং আটক ৪৫২

অধ্যায়-৪

বাংলাদেশ কর্তৃক সহায়তার অনুরোধ

৩১। বাংলাদেশ কর্তৃক সহায়তার অনুরোধ ৪৫৩
৩২। নিরাপত্তা হেফাজতে স্থানান্তরিত ব্যক্তি সম্পর্কিত বিশেষ বিধান ৪৫৩
৩৩। সহায়তার অনুরোধ অনুসারে বাংলাদেশে অবস্থানকারী ব্যক্তির প্রতি নিরাপদ আচরণ ৪৫৩
৩৪। সহায়তার অনুরোধের প্রেক্ষিতে প্রাপ্ত সাক্ষ্য ব্যবহারের সীমাবদ্ধতা ৪৫৪

অধ্যায়-৫

বিবিধ

৩৫। ব্যয় ৪৫৪
৩৬। সাক্ষ্য হিসাবে গ্রহণযোগ্যতা ৪৫৪
৩৭। অনুরোধের ভাষা ৪৫৪
৩৮। বিধি প্রণয়নের ক্ষমতা ৪৫৪
৩৯। জটিলতা নিরসনে সরকারের ক্ষমতা ৪৫৫
৪০। ইংরেজীতে অনূদিত পাঠ প্রকাশ ৪৫৫
৪১। রহিতকরণ ৪৫৫

1. Concept of Cybercrime: Cybercrime is a concept that has different definitions. The United Nations has not provided for a universally accepted definition of cybercrime. Literally, cybercrime pertains to a crime related to the cyberspace, computers, networks and the internet. In general, cybercrimes may be categorized under the following areas:

(a) computers and networks as tools for criminal activity which includes spamming, email bombing and defamation, hate speech and violation of copyright laws;

(b) computers and networks as targets of criminal activity such as unauthorized access, data theft, computer hacking, denial of service, and attacks using malicious code;

(c) computers and networks as place of criminal activity such as financial fraud;

(d) computers and networks as new facilitators for older crimes such as online child pornography, online gambling, phishing, espionage and terrorism. See *Subramanian & Sedita, 2006, p. 40 referred in Jurisdiction in Cybercrimes : A Comparative Study by DR. ADEL AZZAM SAQF AL HAIT.*

In the cyber-world, there are no definite territories or boundaries. The entire world is just a simple click away. This makes the prosecution of cybercrime exponentially difficult for local law enforcement. While domestic police, prosecutors and courts can only operate within their particular territorial jurisdiction, criminal activity and behavior recognizes no borders. It is therefore imperative for states to develop legal tools to deal with cases where one or more of the location of the crime, the accused, evidence, or criminal proceeds is in another country. See *Laura Barnett, 2008, p. 1 referred in Jurisdiction in Cybercrimes : A Comparative Study by DR. ADEL AZZAM SAQF AL HAIT.*

2. Cyber Crimes, Meaning of: According to Black's Law Dictionary "cyber crime is a crime involving the use of computer, such as sabotaging or stealing electronically stored data".

Cyber crimes committed against persons include various crimes like transmission of child pornography, harassment of any one with the use of a computer such as e-mail. See *2013 Cri LJ, Journal Section, at page 97.*

Cyber crime is the use of computers and other electronic devices and internet by criminals to execute fraud and other crimes against companies, consumers and other individuals. It is a broad term which is used to describe criminal activity committed on computers or on the internet. See *2013 Cri LJ, Journal Section, at page 97.*

Cyber crimes are criminal activities carried out by means of computers or internet. See *Oxford Law Dictionary, Oxford University Press, 2nd Ed. (Revised), 2005.*

Cyber Crimes are crimes committed in electronic mediums where *mens rea* is not a requirement. The Cambridge Dictionary defines Cyber Crimes as crimes committed with the use of computers or relate to computers especially through the Internet. The Cyber Crime is an

unlawful act wherein computer is either a tool or a target or both. Cyber Crime is a generic term, which refers to all criminal activities done using the medium of computers, internet cyber space and the World Wide Web. Cyber Crimes are crimes that occur in the digital place, which is the aggregation of the transaction space within each of the connected computers and the virtual spaces arising out of the connection. In short the Cyber Crimes can be defined as offences or contradictions under any law committed with the use of electronic documents. See *2007 Cri LJ, Journal Section, at page 135.*

The concept of Cyber crime is not different from that of conventional crime. Both include act or omission that causes breach of law. A Cyber crime or offence denotes a thing made punishable by the Cyberlaw.

The interment and computer can be used both in positive way and negative way. The use of them in negative way may have destructive impact on societies. Therefore, Cyber crime is a huge threat against different organizations and people i.e. the users whose computers are connected with the internet and also mobile technology.

According to Paran Daggal, Advocate, Supreme Court of India and a specialist on Cyber Law, "Any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cyber crime."

However, Cyber crime can be defined as a crime against individual or organization committed by means of computer.

3. First Cyber Crime: The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus which is thought to be 'the' earliest form of a computer has been around since 3500 B.C in India, Japan and China. The era of modern computers however began with the analytical engine of Charles Babbage. See *Ian J Loyd Information Technology Law, 3rd Ed Butterworths, London, 2000.*

4. Specialized Crimes: Cyber Crimes are the latest and most specialized evil having its origin in the computers. A new generation of crime has developed with the advent of computers and internet. Computers hacking, software piracy, spooling, telecommunication frauds, e-mail bombing, pornography, Industrial espionage, spreading Trojans, viruses and aims of threatening e-mails, e-mail frauds, salami attacks, denial of service attack, logic bombs, internet time thefts, web hacking, cyber defamation, cyber stalking. Computer vandalism, cyber terrorism, distribution of pirated software are some of the forms of Cyber Crimes. See *2007 Cri LJ, Journal Section, at page 135.*

5. Crime is international in nature: The jurisdictional criteria is a not fundamental aspect that poses serious difficulties, as the nature of the internet is such that geographical and political boundaries are irrelevant. A person of criminal nature with the access of Internet might

তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬
The Information and Communication Technology Act, 2006

[Self Translated English Version]

তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬

(২০০৬ সনের ৩৯ নং আইন)

বাংলাদেশ জাতীয় সংসদ

ঢাকা, ২৩শে আশ্বিন, ১৪১৩/৮ই অক্টোবর, ২০০৬

সংসদ কর্তৃক গৃহীত নিম্নলিখিত আইনটি ২৩শে আশ্বিন, ১৪১৩ মোতাবেক ৮ই অক্টোবর, ২০০৬ তারিখে রাষ্ট্রপতির সম্মতি লাভ করিয়াছে এবং এতদ্বারা এই আইনটি সর্বসাধারণের অবগতির জন্য প্রকাশ করা যাইতেছেঃ-

তথ্য ও যোগাযোগ প্রযুক্তির আইনগত বৈধতা ও নিরাপত্তা প্রদান এবং আনুষঙ্গিক বিষয়াদি সম্পর্কে বিধান প্রণয়নকল্পে প্রণীত আইন

যেহেতু তথ্য ও যোগাযোগ প্রযুক্তির আইনগত বৈধতা ও নিরাপত্তা প্রদান এবং আনুষঙ্গিক বিষয়াদি সম্পর্কে বিধান প্রণয়ন করা সমীচীন ও প্রয়োজনীয়;

সেহেতু এতদ্দ্বারা নিম্নরূপ আইন করা হইলঃ-

প্রথম অধ্যায়
প্রারম্ভিক

১। **সংক্ষিপ্ত শিরোনাম, প্রয়োগ এবং প্রবর্তন।**- (১) এই আইন তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ নামে অভিহিত হইবে।

Information and Communication Technology Act, 2006

(Act No. 39 of 2006)

BANGLADESH PARLIAMENT

Dhaka 23 Ashwin, 1413/ 8 October, 2006

The following Act passed by the Parliament received the assent of the President on 23 Ashwin, 1813 corresponding to 8 October, 2006 and is hereby published for general information:-

An Act to make provisions for legal validity and security of Information and Communication Technology and matters ancillary thereto

WHEREAS it is expedient and necessary to make provisions for legal validity and security of information and communication technology and for matters ancillary thereto;

Therefore, it is enacted as follows:-

CHAPTER I
Preliminary

1. Short Title, extent and commencement.- (1) This Act may be called the Information and Communication Technonogy Act, 2006.

(২) সমগ্র বাংলাদেশে ইহার প্রয়োগ হইবে।

(৩) ইহা অবিলম্বে কার্যকর হইবে।

২। সংজ্ঞা।– বিষয় বা প্রসঙ্গের পরিপন্থি কিছু না থাকিলে, এই আইনে–

(১) **"ইলেক্ট্রনিক স্বাক্ষর"** অর্থ ইলেক্ট্রনিক আকারে কোন উপাত্ত, যাহা–

(ক) অন্য কোন ইলেক্ট্রনিক উপাত্তের সহিত সরাসরি বা যৌক্তিকভাবে সংযুক্ত; এবং

(খ) কোন ইলেক্ট্রনিক স্বাক্ষরের প্রমাণীকরণ নিম্নবর্ণিত শর্তাদি পূরণক্রমে সম্পন্ন হয়–

(অ) যাহা স্বাক্ষরদাতার সহিত অনন্যরূপে সংযুক্ত হয়;

(আ) যাহা স্বাক্ষরদাতাকে শনাক্তকরণে সক্ষম হয়;

(ই) স্বাক্ষরদাতার নিয়ন্ত্রণ বজায় থাকে এমন নিরাপদ পন্থায় যাহার সৃষ্টি হয়; এবং

(ঈ) সংযুক্ত উপাত্তের সহিত উহা এমনভাবে সম্পর্কিত যে, পরবর্তীতে উক্ত উপাত্তে কোন পরিবর্তন শনাক্তকরণে সক্ষম হয়;

(২) **"ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট"** অর্থ ধারা ৩৬ এর অধীন ইস্যুকৃত কোন সার্টিফিকেট;

(৩) **"ইলেকট্রনিক"** অর্থ ইলেকট্রিক্যাল, ডিজিটাল, ম্যাগনেটিক, অয়্যারলেস, অপটিক্যাল, ইলেকট্রোম্যাগনেটিক বা তুলনীয় সক্ষমতা রহিয়াছে এইরূপ কোন প্রযুক্তি;

(৪) **"ইলেক্ট্রনিক উপাত্ত বিনিময় (electronic data inter-change)"** অর্থ তথ্য সংগঠিত করিবার উদ্দেশ্যে একটি স্বীকৃত মানদণ্ড অনুসরণক্রমে কোন উপাত্ত এক কম্পিউটার হইতে অন্য কম্পিউটারে ইলেক্ট্রনিক উপায়ে স্থানান্তর;

(2) It shall extend to the whole of Bangladesh.

(3) It shall come into force at once.

2. Definitions.– In this Act, unless there is anything repugnant in the subject or context–

(1) **"electronic signature"** means a data in electronic form, which —

(a) is connected with any other electronic data directly or logically; and

(b) is done on satisfying the following conditions for authentication of the electronic signature –

(i) which is otherwise connected with the signatory;

(ii) which is capable to identify the signatory;

(iii) which is created in such secure manner as being under the control of the signatory ; and

(iv) which is related with the connected data in such manner as is capable to identify any alteration made in such data afterward;

(2) **"Electronic Signature Certificate"** means a certificate issued under section 36;

(3) **"electronic"** means electrical, digital, magnetic, wireless, optical, electromagnetic or any such technology having comparable capability;

(4) **"electronic data interchange"** means transfer of data from one computer to another computer by means of electronical way by following a recognised standard for the purpose of organizing information ;