

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ কর্তৃক প্রস্তুতকৃত ‘সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫’ এর খসড়া অধিকতর পর্যালোচনার নিমিত্ত সর্বসাধারণের মতামত প্রদানের জন্য খসড়া অধ্যাদেশটি ওয়েবসাইটে প্রকাশ করা হয়েছে। খসড়া অধ্যাদেশটির বিষয়ে আগামী ২৮/০২/২০২৫ তারিখের মধ্যে মতামত dg@ncsa.gov.bd অথবা lrf.sec@ictd.gov.bd ই-মেইল যোগে অথবা সচিব, তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ বরাবর পত্রযোগে প্রেরণের জন্য বিশেষভাবে অনুরোধ করা যাচ্ছে। উপদেষ্টা পরিষদ বৈঠকে চূড়ান্ত অনুমোদনের জন্য প্রেরণের পূর্বে প্রাপ্ত মতামতের আলোকে খসড়া অধ্যাদেশটি পুনরায় পরিমার্জন করা হবে।

সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫
(২০২৫ সনের নং অধ্যাদেশ)
[, ২০২৫]

সাইবার নিরাপত্তা আইন, ২০২৩ রহিতক্রমে সাইবার সুরক্ষা নিশ্চিতকরণ এবং সাইবার স্পেসে সংঘটিত অপরাধ শনাক্তকরণ, প্রতিরোধ, দমন ও উক্ত অপরাধের বিচার এবং আনুষঙ্গিক বিষয়ে বিধান প্রণয়নকল্পে প্রণীত অধ্যাদেশ

যেহেতু সাইবার নিরাপত্তা আইন, ২০২৩ রহিতক্রমে সাইবার সুরক্ষা নিশ্চিতকরণ এবং সাইবার স্পেসে সংঘটিত অপরাধ শনাক্তকরণ, প্রতিরোধ, দমন ও উক্ত অপরাধের বিচার এবং আনুষঙ্গিক বিষয়ে বিধান প্রণয়ন করা সমীচীন ও প্রয়োজনীয়; এবং

যেহেতু সংসদ ভাঙ্গিয়া যাওয়া অবস্থায় রহিয়াছে এবং রাষ্ট্রপতির নিকট ইহা সন্তোষজনকভাবে প্রতীয়মান হইয়াছে যে, আশু ব্যবস্থা গ্রহণের জন্য প্রয়োজনীয় পরিস্থিতি বিদ্যমান রহিয়াছে;

সেহেতু গণপ্রজাতন্ত্রী বাংলাদেশের সংবিধানের ৯৩ (১) অনুচ্ছেদে প্রদত্ত ক্ষমতাবলে রাষ্ট্রপতি নিম্নরূপ অধ্যাদেশ প্রণয়ন ও জারি করিলেন: -

প্রথম অধ্যায়

প্রারম্ভিক

১। **সংক্ষিপ্ত শিরোনাম ও প্রবর্তন।**— (১) এই অধ্যাদেশ ‘সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫’ নামে অভিহিত হইবে।

(২) ইহা অবিলম্বে কার্যকর হইবে।

২। **সংজ্ঞার্থ।**— (১) বিষয় বা প্রসঙ্গের পরিপন্থি কোনো কিছু না থাকিলে এই অধ্যাদেশে,

(ক) ‘আপিল ট্রাইব্যুনাল’ অর্থ তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (২০০৬ সনের ৩৯ নং আইন) এর ধারা ৮২ এর অধীন গঠিত সাইবার আপিল ট্রাইব্যুনাল;

(খ) ‘উপাত্ত-ভান্ডার’ অর্থ টেক্সট, ইমেজ, অডিও বা ভিডিও আকারে উপস্থাপিত তথ্য, ডিজিটাল স্বাক্ষর সংযুক্ত বা বিযুক্ত ডিজিটাল ডকুমেন্টস বা ইলেক্ট্রনিক ফাইল, জ্ঞান, ঘটনা, মৌলিক ধারণা বা নির্দেশাবলি, যাহা-

(অ) কোনো কম্পিউটার, ট্যাবলেট, স্মার্টফোন, ডিজিটাল ওয়ারেবলস, বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক বা কৃত্রিম বুদ্ধিমত্তা সফটওয়্যার এজেন্ট, লার্জ ল্যাঞ্জুয়েজ মডেল বা টুল ইত্যাদি দ্বারা আনুষ্ঠানিক পদ্ধতিতে প্রস্তুত করা হইতেছে বা হইয়াছে; এবং

(আ) কোনো কম্পিউটার, ট্যাবলেট, স্মার্টফোন, ডিজিটাল ওয়ারেবলস, বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক বা কৃত্রিম বুদ্ধিমত্তা সফটওয়্যার এজেন্ট, লার্জ ল্যাঞ্জুয়েজ মডেল বা টুল ইত্যাদিতে ব্যবহারের উদ্দেশ্যে প্রস্তুত করা হইয়াছে;

(গ) ‘এজেন্সি’ অর্থ ধারা ৫ এর অধীন গঠিত জাতীয় সাইবার সুরক্ষা এজেন্সি;

(ঘ) ‘কম্পিউটার ইমার্জেন্সি রেসপন্স টিম’ বা ‘কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম’ অর্থ ধারা ৯ এর উপধারা (২) এ বর্ণিত কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম;

(ঙ) ‘কম্পিউটার সিস্টেম’ অর্থ এক বা একাধিক কম্পিউটার বা ডিজিটাল ডিভাইস এর মধ্যে আন্তঃসংযোগকৃত প্রক্রিয়া যাহা এককভাবে বা একে অপরের সহিত সংযুক্ত থাকিয়া তথ্য-উপাত্ত গ্রহণ, প্রেরণ বা সংরক্ষণ করিতে সক্ষম;

(চ) ‘কম্পিউটার ডাটা’ বলিতে যেকোনো তথ্য, উপাত্ত বা ধারণার এমন উপস্থাপনা, যাহা কম্পিউটার সিস্টেমে প্রক্রিয়াকরণের উপযোগী, যাহার মধ্যে এমন প্রোগ্রামও অন্তর্ভুক্ত, যাহা কম্পিউটার সিস্টেমকে কোনো নির্দিষ্ট কার্য সম্পাদনে সক্ষম করিবে;

(ছ) ‘কাউন্সিল’ অর্থ ধারা ১২-এর অধীন গঠিত জাতীয় সাইবার সুরক্ষা কাউন্সিল;

- (জ) ‘**গুরুত্বপূর্ণ তথ্য পরিকাঠামো (Critical Information Infrastructure-CII)**’ অর্থ সরকার কর্তৃক ঘোষিত এইরূপ কোনো বাহ্যিক বা ভার্চুয়াল তথ্য পরিকাঠামো যাহা কোনো তথ্য-উপাত্ত বা কোনো ডিজিটাল বা ইলেকট্রনিক তথ্য নিয়ন্ত্রণ, প্রক্রিয়াকরণ, সঞ্চারণ বা সংরক্ষণ করে এবং যাহা ক্ষতিগ্রস্ত বা সংকটাপন্ন হইলে-
- (অ) জননিরাপত্তা, বা অর্থনৈতিক নিরাপত্তা, বা জনস্বাস্থ্য; এবং
- (আ) জাতীয় নিরাপত্তা বা রাষ্ট্রীয় অখণ্ডতা বা সার্বভৌমত্ব,
- এর উপর ক্ষতিকর প্রভাব পড়িতে পারে;
- (ঝ) ‘**গ্লোবাল স্ট্রেট ইন্টেলিজেন্স**’ অর্থ এমন একটি কর্ম-প্রক্রিয়া বা পদ্ধতি যার মাধ্যমে গুরুত্বপূর্ণ তথ্য অবকাঠামোর সাইবার নিরাপত্তা, অর্থনীতি, স্বাস্থ্য এবং অন্যান্য গুরুত্বপূর্ণ হার্ডওয়্যার ও সফটওয়্যার খাতে বৈশ্বিক হুমকি এবং ঝুঁকির তথ্য ও লগ সংগ্রহ, বিশ্লেষণ এবং রিপোর্ট করা হয়। এর উদ্দেশ্য হলো সঠিক এবং প্রাসঙ্গিক তথ্য রিপোর্ট করা, সাইবার ডিফেন্স ও কৌশল সমাধান প্রস্তাব করা যা ব্যক্তি, কৃষ্টিম বুদ্ধিমত্তা এজেন্ট, প্রতিষ্ঠান এবং রাষ্ট্রকে এসব হুমকির বিরুদ্ধে প্রতিরোধমূলক ব্যবস্থা গ্রহণ করতে সহায়তা করে।
- (ঞ) ‘**জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম (National Cyber Emergency Reponse Team-NCERT)**’ অর্থ একটি সরকার-অনুমোদিত সত্তা যা সাইবার আক্রমণ এবং সাইবার সুরক্ষা সংক্রান্ত ঘটনাগুলি পরীক্ষা-নিরীক্ষা, ফোরকাস্ট ও পর্যালোচনা করে; সাইবার সুরক্ষা আইন প্রয়োগের কারিগরি জ্ঞান নির্মাণ ও বিস্তারে সহায়তা করে এবং সাইবার অপরাধের আইনি তদন্তের জন্য সব ধরনের প্রযুক্তিগত সহায়তা প্রদান করে;
- (ট) ‘**জাতীয় সাইবার নিরাপত্তা অপারেশন সেন্টার (National Security Operation Center-NSOC)**’ অর্থ একটি রাষ্ট্র-সমর্থিত সংস্থা যা একটি দেশের জাতীয় পর্যায়ের সাইবার নিরাপত্তা নিশ্চিত করার জন্য কাজ করে। এটি জাতীয়ভাবে গুরুত্বপূর্ণ অবকাঠামো যেমন বিদ্যুৎ, জ্বালানি, স্বাস্থ্যসেবা, ব্যাংকিং, যোগাযোগ ব্যবস্থা এবং সরকারি ডাটা সিস্টেমের সুরক্ষা নিশ্চিত করতে কেন্দ্রীয় ভূমিকা পালন করে। NSOC সাধারণত সাইবার হুমকি শনাক্ত, প্রতিরোধ, মোকাবিলা, এবং পরবর্তী পদক্ষেপের জন্য বিশ্লেষণ পরিচালনা করে। এটি রাষ্ট্রের বিরুদ্ধে সাইবার আক্রমণ, সাইবার সন্ত্রাসবাদ, এবং ক্রিটিক্যাল ইনফ্রাস্ট্রাকচার লক্ষ্য করে পরিচালিত আক্রমণগুলোর প্রতিরোধে সক্রিয় ভূমিকা পালন করে। পাশাপাশি এটি আন্তর্জাতিক সাইবার নিরাপত্তা অংশীদারদের সাথে সমন্বয় সাধন করে এবং সাইবার নিরাপত্তা সচেতনতা প্রশিক্ষণসহ বিভিন্ন কার্যক্রমে সহায়তা করে। এছাড়াও, NSOC একটি নিয়ন্ত্রক সংস্থা হিসেবে কাজ করতে পারে যা দেশের সকল সরকারি ও বেসরকারি SOC-এর কার্যক্রম পরিচালনা ও স্বীকৃতি প্রদান করে সঠিক নিয়মাবলী এবং প্রবিধান অনুসরণ নিশ্চিত করে। NSOC দেশের সকল SOC-এর মধ্যে সমন্বয় সাধনকারী হিসেবে কাজ করে এবং তাদের কার্যক্রম ও সাফল্য সূচক (Key performance Indicator-KPI) তদারকি করে;
- (ঠ) ‘**ট্রাইব্যুনাল**’ অর্থ তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (২০০৬ সনের ৩৯ নং আইন) এর ধারা ৬৮-এর অধীন গঠিত সাইবার ট্রাইব্যুনাল;
- (ড) ‘**ট্রাফিক ডাটা**’ বলিতে কম্পিউটার সিস্টেমের মাধ্যমে সংঘটিত যোগাযোগ সম্পর্কিত যেকোনো কম্পিউটার ডাটা, যা যোগাযোগের শৃঙ্খলে অংশ নেওয়া কম্পিউটার সিস্টেম দ্বারা উৎপন্ন হয়, বা অনুরূপ কৃত্রিম বুদ্ধিমত্তা সিস্টেম দ্বারা উৎপন্ন এবং যা যোগাযোগের উৎস, গন্তব্য, পথ, সময়, তারিখ, আকার, সময়কাল বা প্রাথমিক সেবার ধরন নির্দেশ করে;
- (ঢ) ‘**ডিজিটাল**’ অর্থ যুগ্ম-সংখ্যা (০ ও ১/বাইনারি) বা ডিজিটভিত্তিক কার্য পদ্ধতি এবং এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, ইলেকট্রনিক্যাল, ইলেকট্রনিক, ডিজিটাল ম্যাগনেটিক, অপটিক্যাল, বায়োমেট্রিক, ইলেকট্রোকেমিক্যাল, ইলেকট্রোমেকানিক্যাল, ওয়্যারলেস বা ইলেকট্রো-ম্যাগনেটিক টেকনোলজি, কৃত্রিম বুদ্ধিমত্তা টেকনোলজি, ব্লকচেইন, লার্জ ল্যাঞ্জুয়েজ মডেল, মেশিন ভিশনও ইহার অন্তর্ভুক্ত হইবে;
- (ণ) ‘**ডিজিটাল ডিভাইস**’ অর্থ কোনো ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক, অপটিক্যাল বা তথ্য প্রক্রিয়াকরণ যন্ত্র বা সিস্টেম, যাহা ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক বা অপটিক্যাল ইমপালস ব্যবহার করিয়া যৌক্তিক, গাণিতিক এবং স্মৃতি কার্যক্রম সম্পন্ন করে, এবং কোনো ডিজিটাল বা কম্পিউটার ডিভাইস সিস্টেম বা কম্পিউটার নেটওয়ার্কের সহিত সংযুক্ত, এবং সকল ইনপুট, আউটপুট, প্রক্রিয়াকরণ, সঞ্চিতি, ডিজিটাল ডিভাইস সফটওয়্যার বা যোগাযোগ সুবিধাদিও ইহার অন্তর্ভুক্ত হইবে; যাহাতে সফটওয়্যার, এপিআই, কোডিং, সফটওয়্যার এনালিসিস, এ্যালগরিদম, ডাটা ভিত্তিক সিদ্ধান্ত নেয়ার প্রক্রিয়া কাজ করে, বা যাহাতে কৃত্রিম বুদ্ধিমত্তার টুল কাজ করে, যাহাতে ওয়েবসাইট বা পোর্টাল চলে, কোয়ান্টাম কম্পিউটিং, ব্লকচেইন কম্পিউটিং, মেশিন লার্নিং, গেইমিং, কম্পিউটার

এইডেড ম্যানুফ্যাকচারিং, মেশিন ভিশন, ব্লক চেইন, লার্জ ল্যাঞ্জুয়েজ মডেল, ক্লাউড কম্পিউটিং, ইন্টারনেট অফ থিংস (আইওটি) ইত্যাদি আধুনিক কম্পিউটিং বা সফটওয়্যার বা অ্যাপস কাজ করে;

- (ত) ‘**ডিজিটাল ফরেনসিক ল্যাব**’ অর্থ একটি অনুমোদিত পরীক্ষাগার যাহা জাতীয় আইন, আন্তর্জাতিক মান, সাইবার সুরক্ষার বিভিন্ন প্রোটোকল এবং অন্তর্জাতিকভাবে স্বীকৃত কমপ্লায়েন্স নিশ্চিত করে; যাহা আইনিভাবে গ্রহণযোগ্য পদ্ধতিতে ডিজিটাল প্রমাণ সংগ্রহ, সংরক্ষণ, বিশ্লেষণ এবং উপস্থাপন করিতে প্রয়োজনীয় কারিগরি সক্ষমতাসহ গঠিত হয়;
- (থ) ‘**পুলিশ অফিসার**’ অর্থ সাব-ইন্সপেক্টর পদমর্যাদার নিম্নে নহেন, এইরূপ কোনো পুলিশ অফিসার;
- (দ) ‘**প্রোগ্রাম**’ অর্থ কোনো পাঠযোগ্য মাধ্যমে যন্ত্র সহযোগে শব্দ, সংকেত, পরিলেখ বা অন্য কোনো আকারে প্রকাশিত নির্দেশাবলি, যাহার মাধ্যমে ডিজিটাল ডিভাইস দ্বারা কোনো বিশেষ কার্য-সম্পাদন বা বাস্তবে ফলদায়ক করা যায়;
- (ধ) ‘**ফৌজদারি কার্যবিধি**’ অর্থ Code of Criminal Procedure, 1898 (Act No. V of 1898);
- (ন) ‘**ব্যক্তি**’ অর্থে কোনো ব্যক্তি বা প্রতিষ্ঠান, কোম্পানি, অংশীদারি কারবার, ফার্ম বা অন্য কোনো সংস্থা, ডিজিটাল ডিভাইসের ক্ষেত্রে উহার নিয়ন্ত্রণকারী এবং আইনের মাধ্যমে সৃষ্ট কোনো সত্তা বা কৃত্রিম আইনগত সত্তাও ইহার অন্তর্ভুক্ত হইবে;
- (প) ‘**বে-আইনি প্রবেশ**’ অর্থ কোনো ব্যক্তি বা কর্তৃপক্ষের অনুমতি ব্যতিরেকে বা উক্তরূপ অনুমতির শর্ত লঙ্ঘনক্রমে কোনো কম্পিউটার বা ডিজিটাল ডিভাইস বা ডিজিটাল নেটওয়ার্ক বা ডিজিটাল তথ্য ব্যবস্থায় প্রবেশ, বা উক্তরূপ প্রবেশের মাধ্যমে উক্ত তথ্য ব্যবস্থার কোনো তথ্য-উপাত্তের আদান-প্রদানে বাধা প্রদান বা উহার প্রক্রিয়াকরণ স্থগিত বা ব্যাহত করা বা বন্ধ করা, বা উক্ত তথ্য-উপাত্তের পরিবর্তন বা পরিবর্ধন বা সংযোজন বা বিয়োজন করা অথবা কোনো ডিজিটাল ডিভাইসের মাধ্যমে কোনো তথ্য-উপাত্ত সংগ্রহ; ক্যাশ থেকে তথ্য-উপাত্ত সরানো, সফটওয়্যার লগ, ট্রেস, রেকর্ড মুছে দেয়া বা সরানো, ক্ষেত্রমতো স্থানান্তর, ব্লক করা ইত্যাদি যাহা অনুপ্রবেশ বা হ্যাকিং নামেও অভিহিত হইবে;
- (ফ) ‘**ভৌত অবকাঠামো**’ অর্থ সকল ধরনের হার্ডওয়্যারভিত্তিক উপাদান ও প্রযুক্তি, যা ডিজিটাল নেটওয়ার্ক এবং ভার্চুয়াল পরিবেশের কার্যক্রমকে সমর্থন করে। ডাটা সেন্টার, সার্ভার এবং কম্পিউটার হার্ডওয়্যার, নেটওয়ার্কিং অবকাঠামো, ইন্টারনেট এক্সচেঞ্জ পয়েন্ট, ইন্টারনেট অফ থিংস (আইওটি), ওয়াই-ফাই নেটওয়ার্ক, টেলিযোগাযোগ ফোরজি ফাইভজি সহ নতুন যোগাযোগ প্রযুক্তি নেটওয়ার্ক, স্যাটেলাইট সিস্টেম, স্যাটেলাইট ইন্টারনেট ও যোগাযোগ টাওয়ার, যোগাযোগ প্রযুক্তিতে ব্যবহৃত বিদ্যুৎ ও জ্বালানি সঞ্চালন ও বিতরণ নেটওয়ার্ক, ভূমি-নদী তলদেশের ক্যাবল, সাবমেরিন ক্যাবল, ওভারহেড ফাইবার ক্যাবল, অপ্টিক্যাল সঞ্চালন নেটওয়ার্ক ইহার অন্তর্ভুক্ত হইবে;
- (ব) ‘**মহাপরিচালক**’ অর্থ এজেন্সির মহাপরিচালক;
- (ভ) ‘**ম্যালওয়্যার**’ অর্থ এইরূপ কোনো ডিজিটাল বা ইলেকট্রনিক নির্দেশ, তথ্য-উপাত্ত, প্রোগ্রাম বা অ্যাপস যাহা-
- (অ) কোনো কম্পিউটার বা ডিজিটাল ডিভাইস কর্তৃক সম্পাদিত কার্যকে পরিবর্তন, বিকৃত, বিনাশ, ক্ষতি বা ক্ষুণ্ণ করে বা উহার কার্য-সম্পাদনে বিরূপ প্রভাব বিস্তার করে, বা প্রবেশিবাধিকারের সীমা বা গভীরতা বাড়ায়;
- (আ) নিজেকে (ব্যক্তি, স্বয়ংক্রিয় সফটওয়্যার টুল বা কৃত্রিম বুদ্ধিমত্তা এজেন্ট বা টুল) অন্য কোনো কম্পিউটার বা ডিজিটাল ডিভাইসের সহিত সংযুক্ত করিয়া উক্ত কম্পিউটার বা ডিজিটাল বা ইলেকট্রনিক ডিভাইসের কোনো প্রোগ্রাম, তথ্য-উপাত্ত বা নির্দেশ কার্যকর করিবার বা কোনো কার্য-সম্পাদনের সময় স্বপ্রণোদিতভাবে ক্রিয়াশীল হইয়া উঠে এবং উহার মাধ্যমে উক্ত কম্পিউটার বা ডিজিটাল বা ইলেকট্রনিক ডিভাইসে কোনো ক্ষতিকর পরিবর্তন বা ঘটনা ঘটায়; বা
- (ই) কোনো ডিজিটাল বা ইলেকট্রনিক ডিভাইসের তথ্য চুরি, তথ্য পরিবর্তন ও বিকৃতি, কৃত্রিম বুদ্ধিমত্তা উৎপাদিত তথ্য অনুপ্রবেশ বা উহাতে হিউম্যান বা নন হিউম্যান এআই এজেন্টের মাধ্যমে স্বয়ংক্রিয় প্রবেশের সুযোগ সৃষ্টি করে, বা কোডিং বা এলগরিদম পরিবর্তন করে;
- (ম) ‘**সাইবার সুরক্ষা**’ বলিতে ডিজিটাল ডিভাইস, কম্পিউটার, ট্যাবলেট, স্মার্টফোন, ডিজিটাল ওয়ারেবলস, কম্পিউটার সিস্টেম, কম্পিউটার ডাটা, সিগনালিং ডাটা, ট্রাফিক ডাটা, ডাটাসেন্টার ও ক্লাউডসহ সাইবার স্পেসে ভৌত অবকাঠামোর সুরক্ষার পাশাপাশি ব্যক্তিগত, প্রতিষ্ঠানিক, আর্থিক ও ব্যবসায়িক তথ্যের সুরক্ষা, সরকারি-

বেসরকারি সফটওয়্যার, এপিআই, কোডিং, সফটওয়্যার অ্যালগরিদম, কৃত্রিম বুদ্ধিমত্তা টুল, এবং পোর্টাল বা নেটওয়ার্কে সঠিক ও অনুমোদিত প্রবেশাধিকার সীমায় কেবল অনুমোদিত ব্যক্তিদের দ্বারা সঠিক অ্যাক্সেস নিশ্চিত করা বুঝাইবে। উপরোক্ত বিষয়বলিতে ব্যক্তির পাশাপাশি কৃত্রিম বুদ্ধিমত্তা এজেন্ট বা টুলের এক্সেসও বুঝাইবে। নাগরিকদের সার্বক্ষণিক ইন্টারনেট প্রাপ্তির অধিকারও ইহার অন্তর্ভুক্ত হইবে;

(য) ‘সাইবার স্পেস’ বলিতে আন্তঃসংযোগকৃত সকল ডিজিটাল ডিভাইস এবং ডিজিটাল নেটওয়ার্কগুলোর সকল ফিজিক্যাল এবং ভার্চুয়াল জগত বুঝাইবে, যাহার মধ্যে ইন্টারনেট, টেলিযোগাযোগ ব্যবস্থা, কম্পিউটার নেটওয়ার্ক, কোয়ান্টাম কম্পিউটিং, ব্লকচেইন কম্পিউটিং, মেশিন লার্নিং ও কৃত্রিম বুদ্ধিমত্তা নেটওয়ার্ক, গেইমিং নেটওয়ার্ক, কম্পিউটার এইডেড ম্যানুফ্যাকচারিং, মেশিন ভিশন, ক্লাউড কম্পিউটিং, ইন্টারনেট অফ থিংস, সোশ্যাল মিডিয়া এবং অন্যান্য সকল আধুনিকতম ইলেকট্রনিক ও অপটিক্যাল যোগাযোগ ব্যবস্থা অন্তর্ভুক্ত হইবে; যেখানে ডাটা তৈরি, ডাটা মিররিং, অ্যাক্সেস, প্রেরণ, সংরক্ষণ, ব্যবস্থাপনাসহ সকল ধরনের হিউম্যান ও নন-হিউম্যান অনলাইন কর্মকান্ড সংঘটিত হয়। ডিজিটাল ডিভাইস, কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার ডাটা, সিগনালিং ডাটা, ট্রাফিক ডাটা এবং কৃত্রিম বুদ্ধিমত্তা উৎপন্ন ডাটাও ইহার অন্তর্ভুক্ত হইবে;

(র) ‘সিগনালিং ডাটা’ বলিতে ডিজিটাল ডিভাইস, সার্ভার এবং নেটওয়ার্কের মধ্যকার সংযোগ স্থাপনকালীন বা কানেকশন সেটআপ সম্পর্কিত তথ্য বুঝাইবে;

(লে) ‘সিকিউরিটি অপারেশন সেন্টার (Security Operation Center-SOC)’ অর্থ একটি নির্দিষ্ট সংস্থা বা প্রতিষ্ঠানের ডিজিটাল অবকাঠামো ও সম্পদের নিরাপত্তা নিশ্চিত করার জন্য কাজ করে। এটি সাধারণত প্রতিষ্ঠানের আইটি সিস্টেমের সাইবার হুমকি শনাক্ত করা, প্রতিরোধ করা, ডাটা সুরক্ষা নিশ্চিত করা এবং অননুমোদিত বা ক্ষতিকারক কার্যক্রম সনাক্তকরণ ও প্রতিরোধে সহায়তা করে। SOC প্রতিষ্ঠানের অভ্যন্তরীণ ও বাহ্যিক হুমকি যেমন ফিশিং, ম্যালওয়্যার, র্যানসমওয়্যার, ডাটা লিক, এবং অস্বাভাবিক নেটওয়ার্ক ট্রাফিক নিরীক্ষণ করে। এটি প্রতিষ্ঠানের ধারাবাহিক কার্যক্রম নিশ্চিত করতে, শিল্প মানদণ্ড (industry standard/compliance) অনুসরণ করতে এবং নিরাপত্তা পরিবেশের মান উন্নত করতে কৌশলগত ভূমিকা পালন করে;

(শে) ‘সেবা প্রদানকারী’ অর্থ-

(অ) কোনো ব্যক্তি, সফটওয়্যার নির্মাতা বা এলগরিদম ডেভেলপার বা কৃত্রিম বুদ্ধিমত্তার ভার্চুয়াল এজেন্ট ডেভেলপার যিনি কম্পিউটার বা ডিজিটাল প্রক্রিয়ার মাধ্যমে কোনো ব্যবহারকারীকে যোগাযোগের সামর্থ্য প্রদান করেন; বা

(আ) এইরূপ কোনো ব্যক্তি, সফটওয়্যার নির্মাতা বা এলগরিদম ডেভেলপার বা কৃত্রিম বুদ্ধিমত্তার ভার্চুয়াল এজেন্ট ডেভেলপার, সত্তা বা সংস্থা যিনি বা যাহা উক্ত সার্ভিসের বা উক্ত সার্ভিসের ব্যবহারকারীর পক্ষে কম্পিউটার ডাটা প্রক্রিয়াকরণ বা সংরক্ষণ করেন।

(২) এই অধ্যাদেশে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞার্থ প্রদান করা হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ এ যে অর্থে ব্যবহৃত হইয়াছে সেই অর্থে প্রযোজ্য হইবে।

৩। অধ্যাদেশের প্রযোজ্যতা।— (১) এই অধ্যাদেশের কোনো বিধানের সহিত যদি অন্য কোনো আইনের কোনো বিধান অসামঞ্জস্যপূর্ণ হয়, তাহা হইলে অন্য কোনো আইনের বিধানের সহিত এই অধ্যাদেশের বিধান যতখানি অসামঞ্জস্যপূর্ণ হয় ততখানির ক্ষেত্রে এই অধ্যাদেশের বিধান কার্যকর থাকিবে।

(২) উপধারা (১) এ যাহা কিছু থাকুক না কেন, তথ্য অধিকার সংক্রান্ত বিষয়ের ক্ষেত্রে তথ্য অধিকার আইন, ২০০৯ (২০০৯ সনের ২০নং আইন) এর বিধানাবলি কার্যকর থাকিবে।

৪। অধ্যাদেশের অতিরিক্তিক প্রয়োগ।— (১) যদি বাংলাদেশের কোনো নাগরিক বাংলাদেশের বাহিরে এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটন করেন যাহা বাংলাদেশে সংঘটন করিলে এই অধ্যাদেশের অধীন দণ্ডযোগ্য হইত, তাহা হইলে এই অধ্যাদেশের বিধানাবলি এইরূপে প্রযোজ্য হইবে যেন উক্ত অপরাধটি তিনি বাংলাদেশেই সংঘটন করিয়াছেন।

(২) যদি কোনো ব্যক্তি বাংলাদেশের বাহির হইতে বাংলাদেশে অবস্থিত কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা ডিজিটাল ডিভাইসের সাহায্যে বাংলাদেশের অভ্যন্তরে এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে উক্ত ব্যক্তির বিরুদ্ধে এই অধ্যাদেশের বিধানাবলি এইরূপে প্রযোজ্য হইবে যেন উক্ত অপরাধের সম্পূর্ণ প্রক্রিয়া বাংলাদেশেই সংঘটিত হইয়াছে।

(৩) যদি কোনো ব্যক্তি বাংলাদেশের অভ্যন্তর হইতে বাংলাদেশের বাহিরে এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে এই অধ্যাদেশের বিধানাবলি এইরূপে প্রযোজ্য হইবে যেন উক্ত অপরাধের সম্পূর্ণ প্রক্রিয়া বাংলাদেশেই সংঘটিত হইয়াছে।

দ্বিতীয় অধ্যায় জাতীয় সাইবার সুরক্ষা এজেন্সি

৫। **এজেন্সি গঠন, কার্যালয়, ইত্যাদি।**— (১) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, ১ (এক) জন মহাপরিচালক ও বিধি দ্বারা নির্ধারিতসংখ্যক পরিচালকের সমন্বয়ে জাতীয় সাইবার সুরক্ষা এজেন্সি নামে একটি এজেন্সি গঠন করিবে।

(২) এজেন্সির প্রধান কার্যালয় ঢাকায় থাকিবে, তবে সরকার, প্রয়োজনে, ঢাকার বাহিরে দেশের যে কোনো স্থানে উহার শাখা কার্যালয় স্থাপন করিতে পারিবে।

(৩) এজেন্সি প্রশাসনিকভাবে তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের সংযুক্ত দপ্তর হিসাবে থাকিবে।

(৪) এজেন্সির দায়িত্ব ও কার্যাবলি বিধি দ্বারা নির্ধারিত হইবে।

৬। **মহাপরিচালক ও পরিচালকগণের নিয়োগ, ইত্যাদি।**— (১) মহাপরিচালক ও পরিচালকগণ, কম্পিউটার, ডিজিটাল ডিভাইস, তথ্য প্রযুক্তি বা সাইবার নিরাপত্তা বিষয়ে বিশেষজ্ঞ ব্যক্তিদের মধ্য হইতে, যাহাদের সাইবার নিরাপত্তা বিষয়ে আন্তর্জাতিকভাবে স্বীকৃত সনদ বা সার্টিফিকেট রহিয়াছে, সরকার কর্তৃক নিযুক্ত হইবেন।

(২) মহাপরিচালক ও পরিচালকগণ এজেন্সির সার্বক্ষণিক কর্মচারী হইবে, এবং তাহারা এই অধ্যাদেশ এবং তদধীন প্রণীত বিধির বিধানাবলি সাপেক্ষে, সরকার কর্তৃক নির্দেশিত কার্য-সম্পাদন, চাকরির শর্তাবলি, দায়িত্ব ও কার্যাবলি পালন করিবে।

৭। **এজেন্সির জনবল।**— (১) সরকার কর্তৃক অনুমোদিত সাংগঠনিক কাঠামো অনুযায়ী এজেন্সির প্রয়োজনীয় জনবল থাকিবে।

(২) এজেন্সির জনবলের চাকরির শর্তাবলি বিধি দ্বারা নির্ধারিত হইবে।

তৃতীয় অধ্যায় প্রতিরোধমূলক ব্যবস্থা

৮। **কতিপয় তথ্য-উপাত্ত অপসারণ বা ব্লক করিবার ক্ষমতা।**— (১) মহাপরিচালকের নিজ অধিক্ষেত্রভুক্ত কোনো বিষয়ে ডিজিটাল বা ইলেকট্রনিক মাধ্যমে প্রকাশিত বা প্রচারিত কোনো তথ্য-উপাত্ত সাইবার নিরাপত্তার ক্ষেত্রে হুমকি সৃষ্টি করিলে তিনি উক্ত তথ্য-উপাত্ত অপসারণ, ক্ষেত্রমতো স্থানান্তর বা ব্লক করিবার জন্য বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশনকে, অতঃপর বিটিআরসি বলিয়া উল্লিখিত, বা তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের সংশ্লিষ্ট সংস্থাকে অনুরোধ করিতে পারিবেন।

(২) যদি আইন-শৃঙ্খলা রক্ষাকারী বাহিনীর নিকট তথ্য-উপাত্ত বিশ্লেষণ সাপেক্ষে, বিশ্বাস করিবার কারণ থাকে যে, ডিজিটাল বা ইলেকট্রনিক মাধ্যমে প্রকাশিত বা প্রচারিত কোনো তথ্য-উপাত্ত দেশের বা উহার কোনো অংশের সংহতি, অর্থনৈতিক কর্মকাণ্ড, নিরাপত্তা, প্রতিরক্ষা, ধর্মীয় মূল্যবোধ বা জনশৃঙ্খলা ক্ষুণ্ণ করে, বা জাতিগত বিদ্বেষ ও ঘৃণার সঞ্চার করে, তাহা হইলে আইন-শৃঙ্খলা রক্ষাকারী বাহিনী উক্ত তথ্য-উপাত্ত অপসারণ বা ব্লক করিবার জন্য, বা ক্ষেত্রমতো স্থানান্তরের জন্য মহাপরিচালকের মাধ্যমে বিটিআরসিকে অনুরোধ করিতে পারিবে।

(৩) উপধারা (১) ও (২) এর অধীন কোনো অনুরোধ প্রাপ্ত হইলে বা ট্রাইব্যুনালের আদেশ প্রাপ্ত হইলে বিটিআরসি বা তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের সংশ্লিষ্ট সংস্থা, উপযুক্ত ক্ষেত্রে, উক্ত তথ্য-উপাত্ত অপসারণ বা, ক্ষেত্রমতো ব্লক করিবার জন্য প্রযুক্তি কোম্পানিকে অনুরোধ এবং অতঃপর তৎবিষয়ে সরকারকে অবহিত করিবে। উপধারা (১) ও (২) এর অধীনে কোন কন্টেন্ট ব্লক হইলে স্বচ্ছতার স্বার্থে সরকার সকল ব্লক হওয়া কন্টেন্টের তথ্য জনসম্মুখে প্রকাশ করিবার ব্যবস্থা করিবে।

(৪) এই ধারার উদ্দেশ্যপূরণকল্পে, প্রয়োজনীয় অন্যান্য বিষয় বিধি দ্বারা নির্ধারিত হইবে।

৯। **কম্পিউটার ইমার্জেন্সি রেসপন্স টিম।**— (১) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, এজেন্সির অধীন একটি জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম (NCERT) থাকিবে এবং এজেন্সির অধীন একটি জাতীয় সিকিউরিটি অপারেশন সেন্টার (NSOC) থাকিবে।

(২) ধারা ১৫ এর অধীন ঘোষিত কোনো ‘গুরুত্বপূর্ণ তথ্য পরিকাঠামোর (Critical Information Infrastructure-CII)’ নিজস্ব কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম (CIRT) এবং সিকিউরিটি অপারেশন সেন্টার (SOC) থাকিবে। সকল SOC-কে প্রতি ত্রৈমাসিকে তাদের কার্যক্রম ও KPI রিপোর্ট NSOC-এ জমা দিতে হবে।

(৩) জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইম্পিডেন্ট রেসপন্স টিম সাইবার সুরক্ষা বিষয়ে বিশেষজ্ঞ ব্যক্তি, ডিজিটাল ফরেনসিক বিষয়ে স্বীকৃত সনদধারী বিশেষজ্ঞ এবং প্রয়োজনে, আইন শৃঙ্খলা রক্ষাকারী বাহিনীর সদস্যদের সমন্বয়ে গঠিত হইবে।

(৪) জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইম্পিডেন্ট রেসপন্স টিম, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, সার্বক্ষণিকভাবে দায়িত্ব পালন করিবে। সাইবার ঝুঁকি নির্ণয়, ঝুঁকি অপসারণ এবং ডিজিটাল ফরেনসিক অ্যানালাইসিসের সক্ষমতা নিশ্চিতকরণে এজেন্সি CIRT ও SOC সমূহের মধ্যে এজেন্সি সমন্বয় সাধন, পরামর্শ এবং সময় নিয়ন্ত্রিত নির্দেশনা প্রদান করিবে। যে কোনো স্বায়ত্বশাসিত, সরকারি ও বেসরকারি সংস্থা বা প্রতিষ্ঠানে সাইবার ইম্পিডেন্ট ঘটিলে উক্ত সংস্থা তাৎক্ষণিকভাবে জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম (NCERT) বা এজেন্সিকে অবহিত করিবে।

(৫) উপধারা (৪) এর সামগ্রিকতাকে ক্ষুণ্ণ না করিয়া, জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইম্পিডেন্ট রেসপন্স টিম নিম্নবর্ণিত দায়িত্ব পালন করিবে, যথা:-

- (ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামো'র জরুরি নিরাপত্তা নিশ্চিতকরণ;
- (খ) সাইবার বা ডিজিটাল হামলা হইলে এবং সাইবার বা ডিজিটাল নিরাপত্তা বিঘ্নিত হইলে তাৎক্ষণিকভাবে উহা প্রতিকারের প্রয়োজনীয় ব্যবস্থা গ্রহণ;
- (গ) সম্ভাব্য ও আসন্ন সাইবার বা ডিজিটাল হামলা প্রতিরোধের লক্ষ্যে প্রয়োজনীয় উদ্যোগ গ্রহণ;
- (ঘ) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সমধর্মী বিদেশি কোনো টিম বা প্রতিষ্ঠানের সহিত তথ্য, লগ এবং ফরেনসিক আদান-প্রদানসহ সার্বিক সহযোগিতামূলক কার্যক্রম গ্রহণ; সাইবার সিকিউরিটির 'গ্লোবাল গ্রেট ইন্টেলিজেন্স' এ বাই-লেটারাল তথ্য ও লগ আদান-প্রদানের উদ্যোগ গ্রহণ এবং
- (ঙ) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সিকিউরিটি অ্যানালাইসিসের নিমিত্তে ক্লাউডভিত্তিক সাইবার সিকিউরিটি সল্যুশন (যেমন Security Information and Event Management-SIEM, Security Orchestration, Automation, and Response-SOAR, Endpoint Detection and Response-EDR/Extended Detection and Response-XDR, Network Detection and Response-NDR) ইত্যাদি ব্যবহার এবং লগ আদান-প্রদানের উদ্যোগ গ্রহণ; এবং
- (চ) বিধি দ্বারা নির্ধারিত অন্যান্য কার্য সম্পাদন।

(৬) এজেন্সি, জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, কম্পিউটার ইম্পিডেন্ট রেসপন্স টিম এবং জাতীয় সিকিউরিটি অপারেশন সেন্টারের মধ্যে সমন্বয় সাধন ও তত্ত্বাবধান করিবে।

১০। **ডিজিটাল ফরেনসিক ল্যাব।**— (১) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, এজেন্সির নিয়ন্ত্রণ ও তত্ত্বাবধানে, এক বা একাধিক ডিজিটাল ফরেনসিক ল্যাব থাকিবে।

(২) উপধারা (১) এ যাহা কিছুই থাকুক না কেন, এই অধ্যাদেশ প্রবর্তনের পূর্বে কোনো সরকারি কর্তৃপক্ষ বা সংস্থার অধীন কোনো ডিজিটাল ফরেনসিক ল্যাব স্থাপিত হইয়া থাকিলে, ধারা ১১-এর অধীন নির্ধারিত মান অর্জন সাপেক্ষে, এজেন্সি উহাকে স্বীকৃতি প্রদান করিবে এবং সেইক্ষেত্রে উক্ত ল্যাব এই অধ্যাদেশের অধীন স্থাপিত হইয়াছে বলিয়া গণ্য হইবে।

(৩) এজেন্সি ডিজিটাল ফরেনসিক ল্যাবসমূহের মধ্যে সমন্বয় সাধন করিবে।

(৪) ডিজিটাল ফরেনসিক ল্যাব স্থাপন, ব্যবহার, পরিচালনা ও অন্যান্য বিষয়াদি বিধি দ্বারা নির্ধারিত হইবে।

১১। **ডিজিটাল ফরেনসিক ল্যাবের মান নিয়ন্ত্রণ।**—(১) এজেন্সি, বিধি দ্বারা নির্ধারিত মানদণ্ড অনুযায়ী, প্রত্যেক ডিজিটাল ফরেনসিক ল্যাবের গুণগত মান নিশ্চিত করিবে।

(২) উপধারা (১) এর অধীন নির্ধারিত গুণগত মান নিশ্চিত করিবার ক্ষেত্রে, অন্যান্য বিষয়ের মধ্যে, প্রত্যেক ডিজিটাল ফরেনসিক ল্যাব-

- (ক) উপযুক্ত যোগ্যতাসম্পন্ন, স্বীকৃত সার্টিফিকেটধারী, অভিজ্ঞতাসম্পন্ন এবং প্রশিক্ষণপ্রাপ্ত জনবল দ্বারা উহার কার্যক্রম পরিচালনা করিবে;
- (খ) উহার ভৌত অবকাঠামোগত সুযোগ সুবিধা নিশ্চিত করিবে;

- (গ) উহার অধীন সংরক্ষিত তথ্যাদির নিরাপত্তা ও গোপনীয়তা বজায় রাখিবার জন্য প্রয়োজনীয় উদ্যোগ গ্রহণ করিবে;
- (ঘ) ডিজিটাল ফরেনসিক পরীক্ষার কারিগরি মান বজায় রাখিবার লক্ষ্যে মানসম্পন্ন যন্ত্রপাতি, আন্তর্জাতিকভাবে স্বীকৃত সফটওয়্যার বা টুল ব্যবহার করিবে; এবং
- (ঙ) বৈজ্ঞানিক প্রক্রিয়া অনুসরণক্রমে, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, কার্য-সম্পাদন করিবে।

চতুর্থ অধ্যায়
জাতীয় সাইবার সুরক্ষা কাউন্সিল

১২। **জাতীয় সাইবার সুরক্ষা কাউন্সিল।**— (১) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, নিম্নবর্ণিত সদস্য সমন্বয়ে জাতীয় সাইবার সুরক্ষা কাউন্সিল গঠিত হইবে, যথা:

- (ক) প্রধান উপদেষ্টা/প্রধানমন্ত্রী, গণপ্রজাতন্ত্রী বাংলাদেশ সরকার, যিনি ইহার চেয়ারম্যানও হইবেন;
- (খ) উপদেষ্টা/মন্ত্রী, প্রতিমন্ত্রী ও উপমন্ত্রী (যদি থাকে), ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়;
- (গ) উপদেষ্টা/মন্ত্রী, আইন বিচার ও সংসদ বিষয়ক মন্ত্রণালয়;
- (ঘ) প্রধান উপদেষ্টা/প্রধানমন্ত্রীর মুখ্যসচিব;
- (ঙ) গভর্নর, বাংলাদেশ ব্যাংক;
- (চ) সচিব, আইন ও বিচার বিভাগ
- (ছ) সচিব, ডাক ও টেলিযোগাযোগ বিভাগ;
- (জ) সচিব, তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ;
- (ঝ) সচিব, জন নিরাপত্তা বিভাগ;
- (ঞ) পররাষ্ট্র সচিব, পররাষ্ট্র মন্ত্রণালয়;
- (ট) ইন্সপেক্টর জেনারেল অব পুলিশ, বাংলাদেশ পুলিশ;
- (ঠ) চেয়ারম্যান, জাতীয় রাজস্ব বোর্ড;
- (ড) চেয়ারম্যান, বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন;
- (ঢ) মহাপরিচালক, প্রতিরক্ষা গোয়েন্দা মহাপরিদপ্তর;
- (ণ) মহাপরিচালক, জাতীয় নিরাপত্তা গোয়েন্দা সংস্থা;
- (ত) মহাপরিচালক, ন্যাশনাল টেলিকমিউনিকেশন মনিটরিং সেন্টার; এবং
- (থ) মহাপরিচালক, জাতীয় সাইবার সুরক্ষা এজেন্সি।

(২) মহাপরিচালক কাউন্সিলের কার্যসম্পাদনে সাচিবিক সহায়তা প্রদান করিবেন।

(৩) উপধারা (১) এর উদ্দেশ্যপূরণকল্পে কাউন্সিল, চেয়ারম্যানের পরামর্শ গ্রহণক্রমে, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, নির্ধারিত মেয়াদ ও শর্তে, কোনো বিশেষজ্ঞ ব্যক্তিকে বা নাগরিক সমাজের উপযুক্ত প্রতিনিধিকে ইহার সদস্য হিসাবে যে কোনো সময় কো-অপ্ট করিতে পারিবে।

১৩। **কাউন্সিলের ক্ষমতা, ইত্যাদি।**— (১) কাউন্সিল, এই অধ্যাদেশ এবং তদধীন প্রণীত বিধির বিধান বাস্তবায়নকল্পে, এজেন্সিকে প্রয়োজনীয় নির্দেশনা ও পরামর্শ প্রদান করিবে।

(২) কাউন্সিল অন্যান্য বিষয়ের মধ্যে, বিশেষ করিয়া, নিম্নবর্ণিত কার্য-সম্পাদন করিবে, যথা:-

- (ক) সাইবার নিরাপত্তা হুমকির সম্মুখীন হইলে উহা প্রতিকারের জন্য প্রয়োজনীয় দিক-নির্দেশনা প্রদান;
- (খ) সাইবার নিরাপত্তার অবকাঠামোগত উন্নয়ন ও জনবল বৃদ্ধি এবং মানোন্নয়নে পরামর্শ প্রদান;
- (গ) সাইবার নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে আন্তঃপ্রাতিষ্ঠানিক নীতি নির্ধারণ;

- (ঘ) অধ্যাদেশ ও তদধীন প্রণীত বিধির যথাযথ প্রয়োগ নিশ্চিতকরণের লক্ষ্যে প্রয়োজনীয় ব্যবস্থা গ্রহণ; এবং
- (ঙ) বিধি দ্বারা নির্ধারিত অন্য কোনো কার্য সম্পাদন।

১৪। **কাউন্সিলের সভা, ইত্যাদি।**— (১) এই ধারার অন্যান্য বিধান সাপেক্ষে, কাউন্সিল উহার সভার কার্যপদ্ধতি নির্ধারণ করিতে পারিবে।

(২) কাউন্সিলের সভা প্রতি ৩ মাসে অন্তত একবার এবং জরুরি পরিস্থিতিতে যেকোনো সময় উহার চেয়ারম্যান কর্তৃক নির্ধারিত তারিখ, সময় ও স্থানে অনুষ্ঠিত হইবে। কাউন্সিল প্রতি তিন মাসে প্রতিটি ‘গুরুত্বপূর্ণ তথ্য পরিকাঠামো (Critical Information Infrastructure)’ সহ দেশের সকল মন্ত্রণালয়, বিভাগ এবং সরকারি-বেসরকারি সংস্থার সাইবার ঝুঁকি নিরীক্ষণ করা হইবে। এই কাজে সার্ট (CIRT) সাইবার সিকিউরিটি সফটওয়্যার আউটপুট দ্বারা প্রস্তুতকৃত প্রতিবেদন তৈরিতে সাহায্য ও তত্ত্বাবধান করিবে যা কাউন্সিল কর্তৃক মূল্যায়ন করা হইবে।

(৩) চেয়ারম্যান কাউন্সিলের সকল সভায় সভাপতিত্ব করিবেন। চেয়ারম্যানের অনুপস্থিতিতে ডাক টেলিযোগাযোগ ও তথ্য প্রযুক্তি মন্ত্রণালয়ের দায়িত্বপ্রাপ্ত উপদেষ্টা/মন্ত্রী কাউন্সিলের সভায় সভাপতিত্ব করিবেন।

(৪) কাউন্সিলের কোনো কার্য বা কার্যধারা কেবল উক্ত কাউন্সিলের কোনো সদস্য পদে শূন্যতা বা কাউন্সিল গঠনে ত্রুটি থাকিবার কারণে অবৈধ হইবে না এবং তৎসম্পর্কে কোনো প্রশ্নও উত্থাপন করা যাইবে না।

পঞ্চম অধ্যায় গুরুত্বপূর্ণ তথ্য পরিকাঠামো

১৫। **গুরুত্বপূর্ণ তথ্য পরিকাঠামো।**—এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা তথ্য পরিকাঠামোকে গুরুত্বপূর্ণ তথ্য পরিকাঠামো (Critical Information Infrastructure) হিসাবে ঘোষণা করিতে পারিবে এবং প্রতিবছর অন্তত একবার গুরুত্বপূর্ণ তথ্য পরিকাঠামোর তালিকা হালনাগাদ করিবে।

১৬। **গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তা পরিবীক্ষণ, পরিদর্শন ও নিরীক্ষা।**— (১) মহাপরিচালক, এই অধ্যাদেশের বিধানাবলি যথাযথভাবে প্রতিপালিত হইতেছে কি না তাহা নিশ্চিত করিবার জন্য, সময় সময়, কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিবীক্ষণ ও পরিদর্শন করিবেন এবং এতৎসংক্রান্ত প্রতিবেদন কাউন্সিলের নিকট দাখিল করিবেন।

(২) এই অধ্যাদেশের আওতায় ঘোষিত গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, প্রতি বৎসর উহার অভ্যন্তরীণ ও বহিঃস্থ পরিকাঠামো নিরীক্ষাপূর্বক একটি নিরীক্ষা প্রতিবেদন কাউন্সিলের নিকট উপস্থাপন করিবে এবং উক্ত প্রতিবেদনের বিষয়বস্তু মহাপরিচালককে অবহিত করিবে।

(৩) মহাপরিচালকের নিকট যদি তথ্য-উপাত্ত বিশ্লেষণ সাপেক্ষে, বিশ্বাস করিবার কারণ থাকে যে, তাঁহার অধিক্ষেত্রভুক্ত কোনো বিষয়ে কোনো ব্যক্তির কার্যক্রম গুরুত্বপূর্ণ তথ্য পরিকাঠামোর জন্য হুমকিস্বরূপ বা ক্ষতিকর, তাহা হইলে তিনি, স্ব-প্রণোদিতভাবে বা কাহারও নিকট হইতে কোনো অভিযোগপ্রাপ্ত হইয়া, উহার অনুসন্ধান করিতে পারিবেন।

(৪) এই ধারার উদ্দেশ্যপূরণকল্পে, নিরাপত্তা পরিবীক্ষণ, পরিদর্শন ও নিরীক্ষা কার্যক্রম সাইবার সুরক্ষা বিষয়ে বিশেষজ্ঞ ব্যক্তি দ্বারা সম্পন্ন করিতে হইবে।

ষষ্ঠ অধ্যায় অপরাধ ও দণ্ড

১৭। **গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে বে-আইনি প্রবেশ বা হ্যাকিং, ইত্যাদির দণ্ড।**— (১) যদি কোনো ব্যক্তি বা সফটওয়্যার ডেভেলপার বা কৃত্রিম বুদ্ধিমত্তা টুলস ব্যবহারকারী ইচ্ছাকৃতভাবে বা জ্ঞাতসারে কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে-

- (ক) বে-আইনি প্রবেশ করেন; বা
- (খ) বে-আইনি প্রবেশের মাধ্যমে কোনো কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম, ইলেকট্রনিক সিস্টেম, সার্ভার, কম্পিউটার নেটওয়ার্ক বা সাইবার স্পেসে বেআইনি প্রবেশ করিয়া তথ্য ভান্ডারের কোনো তথ্য চুরি, বিনাশ, বাতিল, পরিবর্তন বা উহার মূল্য বা উপযোগিতা হ্রাসকরণ, বা কৃত্রিম বুদ্ধিমত্তা এজেন্ট দিয়ে নতুন ডাটা উৎপাদন করেন বা অন্যকোনোভাবে ক্ষতিসাধন করেন, বা কম্পিউটার সোর্স কোড গোপন, ধ্বংস বা

পরিবর্তন করেন, বা অন্য কোনো ব্যক্তির মাধ্যমে উক্ত কোড, প্রোগ্রাম, সিস্টেম বা নেটওয়ার্ক গোপন, ধ্বংস বা পরিবর্তন করিবার চেষ্টা করেন বা উক্ত কাজে সহায়তা করেন, তাহা হইলে উক্ত ব্যক্তির বা ডেভেলপারের বা কৃত্রিম বুদ্ধিমত্তা টুলস্ ব্যবহারকারীর অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর-

(ক) দফা (ক) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৫ (পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ৫০ (পঞ্চাশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন; এবং

(খ) দফা (খ) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৭ (সাত) বৎসর কারাদণ্ডে, বা অনধিক ১ (এক) কোটি টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

১৮। কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম ইত্যাদিতে বে-আইনি প্রবেশ ও দণ্ড।— (১) যদি কোনো ব্যক্তি ইচ্ছাকৃতভাবে—

(ক) কোনো কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্কে বে-আইনি প্রবেশ করেন বা প্রবেশ করিতে সহায়তা করেন; বা

(খ) কোনো কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্কে অপরাধ সংঘটনের উদ্দেশ্যে বে-আইনি প্রবেশ করেন বা প্রবেশ করিতে সহায়তা করেন, বা

(গ) কোনো কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম, ইলেকট্রনিক সিস্টেম, সার্ভার, কম্পিউটার নেটওয়ার্ক বা সাইবার স্পেসে বেআইনি প্রবেশ (হ্যাকিং) করিয়া তথ্য ভান্ডারের কোনো তথ্য চুরি, বিনাশ, বাতিল, পরিবর্তন বা উহার মূল্য বা উপযোগিতা হ্রাসকরণ, অথবা কৃত্রিম বুদ্ধিমত্তা এজেন্ট দিয়ে নতুন ডাটা উৎপাদন করেন বা অন্যকোনোভাবে ক্ষতিসাধন করেন বা উক্ত কাজে সহায়তা করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর-

(ক) দফা (ক) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ১(এক) বছর কারাদণ্ডে, বা অনধিক ১০ (দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন;

(খ) দফা (খ) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ২(দুই) বৎসর কারাদণ্ডে, বা অনধিক ২০ (বিশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

(গ) দফা (গ) এর অধীন কোনো অপরাধ সংঘটন করেন (হ্যাকিং), তাহা হইলে তিনি অনধিক ৫(পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ৫০ (পঞ্চাশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

১৯। কম্পিউটার, কম্পিউটার সিস্টেম ও সাইবার স্পেসের ভৌত অবকাঠামো ইত্যাদির ক্ষতিসাধন ও দণ্ড।— (১) যদি কোনো ব্যক্তি-

(ক) অননুমোদিতভাবে, ক্ষতি সাধনের উদ্দেশ্যে কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা সাইবার স্পেস হইতে কোনো উপাত্ত, উপাত্ত-ভান্ডার, তথ্য বা উহার উদ্ধৃতাংশ সংগ্রহ করেন, বা স্থানান্তরযোগ্য জমাকৃত তথ্য-উপাত্তসহ উক্ত কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কের তথ্য সংগ্রহ করেন বা কোনো উপাত্তের অনুলিপি বা অংশবিশেষ সংগ্রহ করেন;

(খ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক বা সাইবার স্পেসে উদ্দেশ্যমূলকভাবে কোনো ধরনের সংক্রামক, ম্যালওয়্যার বা ক্ষতিকর সফটওয়্যার প্রবেশ করান বা প্রবেশ করানোর চেষ্টা করেন;

(গ) ইচ্ছাকৃতভাবে কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক, উপাত্ত বা কম্পিউটারের উপাত্ত-ভান্ডার, সাইবার স্পেস সংক্রান্ত ভৌত অবকাঠামোর ক্ষতিসাধন করেন, বা ক্ষতিসাধনের চেষ্টা করেন বা উক্ত কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্কে বা সাইবার স্পেসে রক্ষিত অন্য কোনো প্রোগ্রামের ক্ষতি সাধন করেন বা করিবার চেষ্টা করেন;

(ঘ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা সাইবার স্পেসে কোনো বৈধ বা ক্ষমতাপ্রাপ্ত ব্যক্তিকে কোনো উপায়ে প্রবেশ করিতে বাধা সৃষ্টি করেন বা বাধা সৃষ্টির চেষ্টা করেন;

- (ঙ) ইচ্ছাকৃতভাবে প্রেরক বা গ্রাহকের অনুমতি ব্যতীত, কোনো পণ্য বা সেবা বিপণনের উদ্দেশ্যে, স্পাম উৎপাদন বা বাজারজাত করেন বা করিবার চেষ্টা করেন বা অযাচিত ইলেক্ট্রনিক মেইল প্রেরণ করেন; বা
- (চ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্কে বা সাইবার স্পেসে অন্যায়াভাবে হস্তক্ষেপ বা কারসাজি করিয়া কোনো ব্যক্তির সেবা গ্রহণ বা ধার্যকৃত চার্জ অন্যের হিসাবে জমা করেন বা করিবার চেষ্টা করেন,

তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৫ (পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ৫০ (পঞ্চাশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

২০। সাইবার স্পেসে জুয়া খেলার অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি সাইবার স্পেসে জুয়া খেলার নিমিত্ত কোনো পোর্টাল বা অ্যাপস বা ডিভাইস তৈরি করেন বা পরিচালনা করেন বা জুয়া খেলায় অংশগ্রহণ করেন বা খেলায় সহায়তা বা উৎসাহ প্রদান করেন বা উৎসাহ প্রদানের জন্য বিজ্ঞাপনে অংশগ্রহণ করেন তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ২ (দুই) বৎসর কারাদণ্ডে, বা অনধিক ২০ (বিশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

২১। সাইবার স্পেসে জালিয়াতির অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি সাইবার স্পেস ব্যবহার করিয়া জালিয়াতি করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ২ (দুই) বৎসর কারাদণ্ডে, বা অনধিক ২০ (বিশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

ব্যাখ্যা।—এই ধারার উদ্দেশ্যপূরণকল্পে, ‘সাইবার স্পেসে জালিয়াতি’ অর্থ কোনো ব্যক্তি বা কৃত্রিম বুদ্ধিমত্তা এজেন্ট কর্তৃক বিনা অধিকারে বা প্রদত্ত অধিকারের অতিরিক্ত হিসাবে বা অনধিকার চর্চার মাধ্যমে সাইবার স্পেস ব্যবহার করিয়া কোনো কম্পিউটার বা ডিজিটাল ডিভাইসের ইনপুট বা আউটপুট প্রস্তুত, পরিবর্তন, মুছিয়া ফেলা ও লুকাইবার মাধ্যমে অশুদ্ধ ডাটা বা প্রোগ্রাম, তথ্য বা ভ্রান্ত কার্য, তথ্য সিস্টেম, কম্পিউটার বা ডিজিটাল নেটওয়ার্ক পরিচালনা বা ডিজিটাল স্বাক্ষর সংযুক্ত বা বিযুক্ত ডিজিটাল ডকুমেন্টস উৎপাদন বা ইলেক্ট্রনিক ফাইল উৎপাদন বা বিদ্যমান ফাইল পরিবর্তন বা ডিজিটাল মানি বা ইলেক্ট্রনিক মুদ্রা বা ক্রিপ্টোকারেন্সি উৎপাদন বা অন্যের এনআইডিতে নিবন্ধিত সিম ব্যবহার করিয়া মোবাইল ব্যাংকিং পরিচালনা, হস্তি কার্যে নিযুক্তি কিংবা জুয়ার পোর্টাল পরিচালনা করেন।

২২। সাইবার স্পেসে প্রতারণার অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি সাইবার স্পেস ব্যবহার করিয়া প্রতারণা করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৫ (পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ৫০ (পঞ্চাশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

ব্যাখ্যা।—এই ধারার উদ্দেশ্যপূরণকল্পে, ‘সাইবার স্পেসে প্রতারণা’ অর্থ কোনো ব্যক্তি কর্তৃক ইচ্ছাকৃতভাবে বা জ্ঞাতসারে অথবা অনুমতি ব্যতিরেকে কোনো কম্পিউটার প্রোগ্রাম, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক, ডিজিটাল ডিভাইস, ডিজিটাল সিস্টেম, ডিজিটাল নেটওয়ার্কে, ই-কমার্চে বা সামাজিক যোগাযোগ মাধ্যমের কোনো তথ্য পরিবর্তন করা, মুছিয়া ফেলা, নূতন কোনো তথ্যের সংযুক্তি বা বিকৃতি ঘটাইবার মাধ্যমে উহার মূল্য বা উপযোগিতা হ্রাস করা, তাহার নিজের বা অন্য কোনো ব্যক্তির আর্থিক বা অন্য কোন সুবিধা প্রাপ্তির চেষ্টা বা ক্ষতি করিবার চেষ্টা করা বা ছলনার আশ্রয় গ্রহণ করা।

২৩। সাইবার সন্ত্রাসী কার্য সংঘটনের অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি—

- (ক) রাষ্ট্রীয় অখণ্ডতা, নিরাপত্তা ও সার্বভৌমত্ব বিপন্ন করা এবং জনগণ বা উহার কোনো অংশের মধ্যে ভয়ভীতি সঞ্চার করিবার অভিপ্রায়ে কোনো কম্পিউটার বা কম্পিউটার নেটওয়ার্ক বা ইন্টারনেট নেটওয়ার্কে বৈধ প্রবেশে প্রতিবন্ধকতা সৃষ্টি করেন বা বে-আইনি প্রবেশ করেন বা করান;
- (খ) কোনো ডিজিটাল ডিভাইসে এইরূপ দূষণ সৃষ্টি করেন বা ম্যালওয়্যার প্রবেশ করান যাহার ফলে কোনো ব্যক্তির মৃত্যু ঘটে বা গুরুতর জখমপ্রাপ্ত হন বা হওয়ার সম্ভাবনা দেখা দেয়; বা
- (গ) জনসাধারণের নিত্য প্রয়োজনীয় দ্রব্যের সরবরাহ ও সেবা ক্ষতিগ্রস্ত বা ধ্বংসসাধন করেন বা কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর উপর বিরূপ প্রভাব বিস্তার করেন; বা

- (ঘ) ইচ্ছাকৃতভাবে বা জ্ঞাতসারে কোনো কম্পিউটার, কম্পিউটার নেটওয়ার্ক, ইন্টারনেট নেটওয়ার্ক, সংরক্ষিত কোনো তথ্য-উপাত্ত বা কম্পিউটার ডাটাবেইজে প্রবেশ বা অনুপ্রবেশ করেন বা এইরূপ কোনো সংরক্ষিত তথ্য-উপাত্ত বা কম্পিউটার ডাটাবেইজে প্রবেশ করেন যাহা বৈদেশিক কোনো রাষ্ট্রের সহিত বন্ধুত্বপূর্ণ সম্পর্ক বা জনশৃঙ্খলা পরিপন্থি কোনো কাজে ব্যবহৃত হইতে পারে অথবা বৈদেশিক কোনো রাষ্ট্র বা কোনো ব্যক্তি বা গোষ্ঠীর সুবিধার্থে ব্যবহার করা হইতে পারে; বা
- (ঙ) প্রতারণা করিবার বা ঠকাইবার উদ্দেশ্যে নিজের পরিচয় গোপন করিয়া বা অপর কোনো ব্যক্তির পরিচয় ধারণ করেন বা কাহারো জাতীয় পরিচয় পত্র বিকৃত করেন বা অন্য কোনো ব্যক্তির ব্যক্তিগত কোনো তথ্য নিজের বলিয়া প্রদর্শনপূর্বক দফা (ক), (খ), (গ) ও (ঘ) এর কোনো কার্য সংঘটন করেন,

তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে সাইবার সন্ত্রাস অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ১০ (দশ) বৎসর কারাদণ্ডে, বা অনধিক ১ (এক) কোটি টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

২৪। আইনানুগ কর্তৃত্ব বহির্ভূত ই-ট্রানজেকশনের অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি—

- (ক) কোনো ব্যাংক, বিমা বা অন্য কোনো আর্থিক প্রতিষ্ঠান বা মোবাইল আর্থিক সেবা প্রদানকারী প্রতিষ্ঠান হইতে কোনো ডিজিটাল বা ইলেকট্রনিক মাধ্যম ব্যবহার করিয়া আইনানুগ কর্তৃত্ব ব্যতিরেকে ই-ট্রানজেকশন করেন; বা
- (খ) সরকার বা বাংলাদেশ ব্যাংক কর্তৃক, সময় সময়, জারিকৃত কোনো ই-ট্রানজেকশনকে অবৈধ ঘোষণা করা সত্ত্বেও ই-ট্রানজেকশন করেন,

তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ১ (এক) বৎসর কারাদণ্ড এবং অনধিক ১০ (দশ) লক্ষ টাকা অর্থদণ্ডে দণ্ডিত হইবেন।

ব্যাখ্যা।—এই ধারার উদ্দেশ্যপূরণকল্পে, ‘ই-ট্রানজেকশন’ অর্থ কোনো ব্যক্তি কর্তৃক তাহার তহবিল স্থানান্তরের জন্য কোনো ব্যাংক, আর্থিক প্রতিষ্ঠান অথবা ডিজিটাল বা ইলেকট্রনিক মাধ্যমে কোনো সুনির্দিষ্ট হিসাব নম্বরে অর্থ জমা প্রদান বা উত্তোলন বা উত্তোলন করিবার জন্য প্রদত্ত নির্দেশনা, আদেশ বা কর্তৃত্বপূর্ণ আইনানুগ আর্থিক লেনদেন এবং কোনো ডিজিটাল বা ইলেকট্রনিক মাধ্যমে অর্থ স্থানান্তর।

২৫। যৌন হয়রানি, ব্ল্যাকমেইলিং বা অন্ত্রীল বিষয়বস্তু প্রকাশ সংক্রান্ত অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি ওয়েবসাইট বা অন্য কোনো ডিজিটাল বা ইলেকট্রনিক মাধ্যমে ইচ্ছাকৃতভাবে বা জ্ঞাতসারে অন্য কোনো ব্যক্তিকে যৌন হয়রানি বা রিভেঞ্জ পর্ন দিয়ে ব্ল্যাকমেইল করিবার অভিপ্রায়ে সৃষ্ট কোনো তথ্য, অন্ত্রীল ভিডিও চিত্র, অডিও ভিজ্যুয়াল চিত্র, স্থির চিত্র, গ্রাফিকস বা অন্য কোনো উপায়ে ধারণকৃত, এডিটকৃত, কৃত্রিম বুদ্ধিমত্তা দ্বারা নির্মিত অথবা এডিটকৃত ও প্রদর্শনযোগ্য এইরূপ কোনো তথ্য-উপাত্ত প্রেরণ, প্রকাশ বা প্রচার করেন, বা প্রেরণ, প্রকাশ বা প্রচার করার হুমকি প্রদান করেন, যাহা ক্ষতিকর বা ভীতি প্রদর্শক; তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ২ (দুই) বৎসর কারাদণ্ডে, বা অনধিক ১০ (দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

(৩) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন অপরাধ, কোনো নারী বা অনূর্ধ্ব ১৮ (আঠারো) বৎসরের কোনো শিশুর বিরুদ্ধে সংঘটন করেন, তাহা হইলে তিনি অনধিক ৩ (তিন) বৎসর কারাদণ্ডে, বা অনধিক ২০ (বিশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

ব্যাখ্যা।— এই ধারার উদ্দেশ্যপূরণকল্পে, ‘ব্ল্যাকমেইলিং’ বলিতে এমন হুমকি বা ভীতি প্রদর্শন বোঝাইবে, যাহার মাধ্যমে কোনো ব্যক্তি অন্য ব্যক্তিকে তার গোপনীয় তথ্য প্রকাশের বা ক্ষতি করার ভয় দেখাইয়া বেআইনি সুবিধা, সেবা বা চাহিত কোনো কার্য সম্পাদনে বাধ্য করে।

২৬। সাইবার স্পেসে ধর্মীয় বা জাতিগত বিষয়ে ঘৃণা ও বিদ্বেষমূলক তথ্য প্রকাশ ইত্যাদির অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি বা গোষ্ঠী ইচ্ছাকৃতভাবে বা জ্ঞাতসারে বা ছদ্ম পরিচয়ে নিজের বা অন্যের আইডিতে অবৈধ প্রবেশ করিয়া কোনো ধর্ম বা এর অনুসারীদের

প্রতি ঘণ্টা, বিদ্রোহ বা উস্কানিমূলক কোনো কিছু সাইবার স্পেসে প্রকাশ বা প্রচার করেন বা করান, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ২(দুই) বৎসর কারাদণ্ডে, বা অনধিক ১০ (দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

২৭। অপরাধ সংঘটনে সহায়তা ও উহার দণ্ড।— (১) যদি কোনো ব্যক্তি এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটনে সহায়তা করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি মূল অপরাধটির জন্য যে দণ্ড নির্ধারিত রহিয়াছে, সেই দণ্ডেই দণ্ডিত হইবেন।

২৮। মিথ্যা মামলা, অভিযোগ দায়ের, ইত্যাদির অপরাধ ও দণ্ড।— (১) যদি কোনো ব্যক্তি অন্য কোনো ব্যক্তির ক্ষতিসাধনের অভিপ্রায়ে উক্ত ব্যক্তির বিরুদ্ধে এই অধ্যাদেশের অন্য কোনো ধারার অধীন মামলা বা অভিযোগ দায়ের করিবার জন্য ন্যায্য বা আইনানুগ কারণ না জানিয়াও মামলা বা অভিযোগ দায়ের করেন বা করান, তাহা হইলে উহা হইবে একটি অপরাধ এবং তজ্জন্য মামলা বা অভিযোগ দায়েরকারী ব্যক্তি এবং যিনি অভিযোগ দায়ের করাইয়াছেন উক্ত ব্যক্তি মূল অপরাধটির জন্য যে দণ্ড নির্ধারিত রহিয়াছে সেই দণ্ডে দণ্ডিত হইবেন।

(২) কোনো ব্যক্তি যদি উপধারা (১) এর অধীন এই অধ্যাদেশের একাধিক ধারায় কোনো মামলা বা অভিযোগ করেন, তাহা হইলে উক্ত ধারায় বর্ণিত অপরাধসমূহের মধ্যে মূল অপরাধের জন্য যাহার দণ্ডের পরিমাণ বেশি হয় উহাই দণ্ডের পরিমাণ হিসাবে নির্ধারণ করা যাইবে।

(৩) ট্রাইব্যুনাল ক্ষতিগ্রস্ত ব্যক্তি বা তাহার কর্তৃক ক্ষমতাপ্রাপ্ত ব্যক্তির লিখিত অভিযোগের ভিত্তিতে বা স্বপ্নোদিত হয়ে উপধারা (১) এর অধীন সংঘটিত অপরাধের অভিযোগ গ্রহণ ও মামলার বিচার করিতে পারিবে।

২৯। কোম্পানি কর্তৃক অপরাধ সংঘটন।— (১) কোনো কোম্পানি কর্তৃক এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটনের ক্ষেত্রে, উক্ত অপরাধের সহিত প্রত্যক্ষ সংশ্লিষ্টতা রহিয়াছে কোম্পানির এইরূপ প্রত্যেক মালিক, প্রধান নির্বাহী, পরিচালক, ম্যানেজার, সচিব, অংশীদার বা অন্য কোনো কর্মকর্তা বা কর্মচারী বা প্রতিনিধি উক্ত অপরাধ সংঘটন করিয়াছেন বলিয়া গণ্য হইবেন, যদি না তিনি প্রমাণ করিতে সক্ষম হন যে, উক্ত অপরাধ তাহার অজ্ঞাতসারে হইয়াছে বা উক্ত অপরাধ রোধ করিবার জন্য তিনি যথাসাধ্য চেষ্টা করিয়াছেন।

(২) উপধারা (১) এ উল্লিখিত কোম্পানি আইনগত ব্যক্তিসত্তা বিশিষ্ট সংস্থা হইলে, উক্ত ব্যক্তিকে অভিযুক্ত ও দোষী সাব্যস্ত করা ছাড়াও উক্ত কোম্পানিকে আলাদাভাবে একই কার্যধারায় অভিযুক্ত ও দোষী সাব্যস্ত করা যাইবে, তবে উহার উপর সংশ্লিষ্ট বিধান মোতাবেক কেবল অর্থদণ্ড আরোপযোগ্য হইবে।

ব্যাখ্যা।—এই ধারার উদ্দেশ্যপূরণকল্পে,-

(ক) 'কোম্পানি' অর্থে কোনো বাণিজ্যিক প্রতিষ্ঠান, অংশীদারি কারবার, সমিতি, সংঘ বা সংগঠনও অন্তর্ভুক্ত হইবে;

(খ) বাণিজ্যিক প্রতিষ্ঠানের ক্ষেত্রে, 'পরিচালক' অর্থে উহার কোনো অংশীদার বা পরিচালনা বোর্ডের সদস্যও অন্তর্ভুক্ত হইবে।

৩০। ক্ষতিপূরণের আদেশ দানের ক্ষমতা।— কোনো ব্যক্তি এই অধ্যাদেশের অধীন কোনো অপরাধ করিলে, ট্রাইব্যুনাল সৃষ্ট ক্ষতির সমতুল্য অর্থ বা তদ্বিবেচনায় উপযুক্ত পরিমাণ অর্থ ট্রাইব্যুনাল কর্তৃক আরোপিত জরিমানা হইতে বা জরিমানার অতিরিক্ত অর্থ ক্ষতিপূরণ হিসাবে ক্ষতিগ্রস্ত ব্যক্তি বা প্রতিষ্ঠানকে প্রদানের জন্য আদেশ দিতে পারিবে।

সপ্তম অধ্যায় অপরাধের তদন্ত ও বিচার

৩১। তদন্ত, ইত্যাদি।— (১) পুলিশ অফিসার বা এই অধ্যায়ে তদন্তকারী অফিসার বলিয়া উল্লিখিত ব্যক্তি এই অধ্যাদেশের অধীন সংঘটিত কোনো অপরাধ তদন্ত করিবেন।

(২) উপধারা (১) এ যাহা কিছুই থাকুক না কেন, কোনো মামলার প্রারম্ভ বা তদন্তের যেকোনো পর্যায়ে যদি প্রতীয়মান হয় যে, উক্ত মামলার সুষ্ঠু তদন্তের জন্য একটি তদন্ত দল গঠন করা প্রয়োজন, তাহা হইলে ট্রাইব্যুনাল তদন্তকারী সংস্থা, আইনশৃঙ্খলা রক্ষাকারী বাহিনী এবং এজেন্সির সমন্বয়ে একটি যৌথ তদন্ত দল গঠন করিতে পারিবে।

(৩) তবে, ২১, ২৫ ও ২৬ ধারায় অপরাধের অভিযোগে মামলা দায়ের হইলে মামলা দায়েরের ২৪ ঘণ্টার মধ্যে উক্ত মামলার নথি ও আটককৃত ব্যক্তিকে সংশ্লিষ্ট আমলী আদালতের ম্যাজিস্ট্রেটের নিকট উপস্থাপন করিতে হইবে।

(৪) উপধারা (৩) এর অধীনে নথিপ্রাপ্তির ২৪ ঘণ্টার মধ্যে আমলী ম্যাজিস্ট্রেট উক্ত অপরাধের অভিযোগসহ নথি এবং পারিপার্শ্বিক সকল বিষয় বিবেচনা করিয়া এবং সরাসরি সংশ্লিষ্ট ব্যক্তি কিংবা তার আইনজীবীর বক্তব্য (যদি থাকে) শ্রবণ করিয়া অভিযোগের ভিত্তি থাকিলে অভিযোগটির বিষয়ে তদন্তের নির্দেশ প্রদান করিবেন এবং অভিযোগের ভিত্তি না থাকিলে কারণ লিপিবদ্ধ করিয়া অভিযোগটি খারিজ করিয়া দিবেন এবং আটক ব্যক্তিকে তাৎক্ষণিক মুক্তির আদেশ দিবেন।

৩২। তদন্তের সময়সীমা, ইত্যাদি।— (১) তদন্তকারী অফিসার—

- (ক) কোনো অপরাধ তদন্তের দায়িত্ব প্রাপ্তির তারিখ হইতে ৯০ (নব্বই) দিনের মধ্যে তদন্ত কার্য সম্পন্ন করিবেন;
- (খ) দফা (ক) এর অধীন নির্ধারিত সময়ের মধ্যে তদন্ত কার্য সম্পন্ন করিতে ব্যর্থ হইলে তিনি, তাহার নিয়ন্ত্রণকারী অফিসারের অনুমোদনসাপেক্ষে, তদন্তের সময়সীমা অতিরিক্ত ১৫ (পনেরো) দিন বৃদ্ধি করিতে পারিবেন;
- (গ) দফা (খ) এর অধীন নির্ধারিত সময়ের মধ্যে কোনো তদন্ত কার্য সম্পন্ন করিতে ব্যর্থ হইলে তিনি উহার কারণ লিপিবদ্ধ করিয়া বিষয়টি প্রতিবেদন আকারে ট্রাইব্যুনালকে অবহিত করিবেন এবং ট্রাইব্যুনালের অনুমতিক্রমে, পরবর্তী ৩০ (ত্রিশ) দিনের মধ্যে তদন্ত কার্যক্রম সম্পন্ন করিবেন।

(২) উপধারা (১)-এর অধীন তদন্তকারী অফিসার কোনো তদন্ত কার্য সম্পন্ন করিতে ব্যর্থ হইলে ট্রাইব্যুনাল তদন্তের সময়সীমা, যুক্তিসংগত সময় পর্যন্ত, বৃদ্ধি করিতে পারিবে।

৩৩। তদন্তকারী অফিসারের ক্ষমতা।— (১) এই অধ্যাদেশের অধীন কোনো অপরাধ তদন্তের ক্ষেত্রে তদন্তকারী অফিসারের নিম্নবর্ণিত ক্ষমতা থাকিবে, যথা:

- (ক) কম্পিউটার, কম্পিউটার প্রোগ্রাম, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা কোনো ডিজিটাল ডিভাইস, ডিজিটাল সিস্টেম, ডিজিটাল নেটওয়ার্ক বা কোনো প্রোগ্রাম, তথ্য-উপাত্ত যাহা কোনো কম্পিউটার বা কম্প্যাক্ট ডিস্ক বা রিমুভেবল ড্রাইভ বা অন্য কোনো উপায়ে সংরক্ষণ করা হইয়াছে তাহা নিজের নিয়ন্ত্রণে নেওয়া;
- (খ) কোনো ব্যক্তি বা সংস্থার নিকট হইতে তথ্য প্রবাহের (traffic data) তথ্য-উপাত্ত সংগ্রহের লক্ষ্যে প্রয়োজনীয় উদ্যোগ গ্রহণ; এবং
- (গ) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, প্রয়োজনীয় অন্যান্য কার্য সম্পাদন।

(২) এই অধ্যাদেশের অধীন তদন্ত পরিচালনাকালে তদন্তকারী অফিসার কোনো অপরাধের তদন্তের স্বার্থে যে কোনো বিশেষজ্ঞ ব্যক্তি বা বিশেষায়িত প্রতিষ্ঠানের বা আইসিটি কর্মকর্তার সহায়তা গ্রহণ করিতে পারিবেন।

(৩) তদন্তকারী অফিসার এই অধ্যাদেশের অধীনে কোনো অপরাধ তদন্তের ক্ষেত্রে জন্মকৃত বা তার নিয়ন্ত্রণাধীন আলামত বিষয়ে সংশ্লিষ্ট আদালতকে অনতিবিলম্বে অবহিত করিবেন।

৩৪। পরোয়ানার মাধ্যমে তল্লাশি ও জব্দ।— যদি কোনো পুলিশ অফিসারের এইরূপ বিশ্বাস করিবার কারণ থাকে যে,-

- (ক) এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটিত হইয়াছে বা সংঘটিত হইবার সম্ভাবনা রহিয়াছে; বা
- (খ) এই অধ্যাদেশের অধীন সংঘটিত অপরাধসংক্রান্ত কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক, তথ্য-উপাত্ত বা এতৎসংক্রান্ত সাক্ষ্য প্রমাণ কোনো স্থানে বা ব্যক্তির নিকট রক্ষিত রহিয়াছে,

তাহা হইলে, তিনি, অনুরূপ বিশ্বাসের কারণ লিপিবদ্ধ করিয়া, ট্রাইব্যুনাল বা, ক্ষেত্রমতো, চিফ জুডিসিয়াল ম্যাজিস্ট্রেট বা চিফ মেট্রোপলিটন ম্যাজিস্ট্রেটের নিকট আবেদনের মাধ্যমে তল্লাশি পরোয়ানা সংগ্রহ করিয়া নিম্নবর্ণিত কার্য সম্পাদন করিতে পারিবেন,

- (অ) কোনো সেবা প্রদানকারীর দখলে থাকা কোনো তথ্য-প্রবাহের (traffic data) তথ্য-উপাত্ত হস্তগতকরণ;
- (আ) যোগাযোগের যে কোনো পর্যায়ে গ্রাহক তথ্য এবং তথ্যপ্রবাহের তথ্য-উপাত্তসহ যে কোনো তারবার্তা বা ইলেকট্রনিক যোগাযোগে প্রতিবন্ধকতা সৃষ্টিকরণ।

৩৫। বেআইনি প্রবেশ বা অনুপ্রবেশ বা হ্যাকিং এর ক্ষেত্রে পরয়োজনা ব্যতিরেকে তল্লাশি, জন্ম ও গ্রেফতার।— (১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে সাইবার হামলা কিংবা কম্পিউটার, কম্পিউটার সিস্টেম, ডিজিটাল ডিভাইস ইত্যাদিতে বেআইনি প্রবেশ বা অনুপ্রবেশ বা হ্যাকিং এর মাধ্যমে মুছিয়া ফেলা, পরিবর্তন, নষ্ট হওয়া, সাক্ষ্য প্রমাণাদি হারানো বা অন্য কোনো উপায়ে দুস্প্রাপ্য হইবার বা করিবার সম্ভাবনা রহিয়াছে, তাহা হইলে পুলিশ অফিসার কারণ লিপিবদ্ধ করিয়া, নিম্নবর্ণিত কার্য সম্পাদন করিতে পারিবেন,

- (ক) উক্ত স্থানে প্রবেশ করিয়া তল্লাশি এবং প্রবেশে বাধাপ্রাপ্ত হইলে ফৌজদারি কার্যবিধি অনুযায়ী প্রয়োজনীয় ব্যবস্থা গ্রহণ;
- (খ) উক্ত স্থানে তল্লাশিকালে প্রাপ্ত অপরাধ সংঘটনে ব্যবহার্য কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক, তথ্য-উপাত্ত বা অন্যান্য সরঞ্জামাদি এবং অপরাধ প্রমাণে সহায়ক কোনো দলিল জব্দকরণ;
- (গ) উক্ত স্থানে উপস্থিত যে-কোনো ব্যক্তির দেহ তল্লাশি;
- (ঘ) উক্ত স্থানে উপস্থিত কোনো ব্যক্তি এই অধ্যাদেশের অধীন কোনো অপরাধ করিয়াছেন বা করিতেছেন বলিয়া সন্দেহ হইলে উক্ত ব্যক্তিকে গ্রেফতার।

(২) উপধারা (১) এর অধীন তল্লাশি সম্পন্ন করিবার পর পুলিশ অফিসার তল্লাশি পরিচালনার প্রতিবেদন ট্রাইব্যুনালের নিকট দাখিল করিবেন।

(৩) উপধারা (১) এর অধীন কোনো ব্যক্তিকে গ্রেফতার করিবার পর পুলিশ অফিসার উক্ত ব্যক্তিকে অনতিবিলম্বে নিকটস্থ ম্যাজিস্ট্রেট বা ট্রাইব্যুনালে উপস্থাপন করিবেন।

৩৬। তথ্য সংরক্ষণ।— (১) মহাপরিচালক, স্থায়ী বিবেচনায়, বা তদন্তকারী অফিসারের আবেদনের পরিপ্রেক্ষিতে, যদি এইরূপে বিশ্বাস করেন যে, কম্পিউটার বা কম্পিউটার সিস্টেমে সংরক্ষিত কোনো তথ্য-উপাত্ত এই অধ্যাদেশের অধীন তদন্তের স্বার্থে সংরক্ষণ করা প্রয়োজন এবং এইরূপ তথ্য-উপাত্ত নষ্ট, ক্ষয়, পরিবর্তন অথবা দুস্প্রাপ্য করিয়া দেওয়ার সম্ভাবনা রহিয়াছে, তাহা হইলে উক্ত কম্পিউটার বা কম্পিউটার সিস্টেমের দায়িত্বে থাকা ব্যক্তি বা প্রতিষ্ঠানকে উক্তরূপ তথ্য-উপাত্ত ৯০ (নব্বই) দিন পর্যন্ত সংরক্ষণের জন্য নির্দেশ প্রদান করিতে পারিবেন।

(২) ট্রাইব্যুনাল, আবেদনের পরিপ্রেক্ষিতে, উক্ত তথ্য-উপাত্ত সংরক্ষণের মেয়াদ বর্ধিত করিতে পারিবে, তবে তাহা সর্বমোট ১৮০ (একশত আশি) দিনের অধিক হইবে না।

৩৭। কম্পিউটারের সাধারণ ব্যবহার ব্যাহত না করা।— (১) তদন্তকারী অফিসার এইরূপভাবে তদন্ত পরিচালনা করিবেন যেন কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা ইহার কোনো অংশের বৈধ ব্যবহার ব্যাহত না হয়।

(২) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা ইহার কোনো অংশ জব্দ করা যাইবে, যদি-

- (ক) সংশ্লিষ্ট কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা ইহার কোনো অংশে প্রবেশ করা সম্ভব না হয়;
- (খ) সংশ্লিষ্ট কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক বা ইহার কোনো অংশ অপরাধ প্রতিরোধ করিবার জন্য বা চলমান অপরাধ রোধ করিবার জন্য জব্দ না করিলে তথ্য-উপাত্ত নষ্ট, ক্ষয়, পরিবর্তন বা দুস্প্রাপ্য হইবার সম্ভাবনা থাকে।

৩৮। তদন্তে সহায়তা।— এই অধ্যাদেশের অধীন তদন্ত পরিচালনাকালে তদন্তকারী অফিসার কোনো ব্যক্তি বা সত্তা বা সেবা প্রদানকারীকে তথ্য প্রদান বা তদন্তে সহায়তার জন্য অনুরোধ করিতে পারিবেন এবং উক্তরূপে কোনো অনুরোধ করা হইলে সংশ্লিষ্ট ব্যক্তি, সত্তা বা সেবা প্রদানকারী তথ্য প্রদানসহ প্রয়োজনীয় সহায়তা প্রদান করিতে বাধ্য থাকিবেন।

৩৯। তদন্তে প্রাপ্ত তথ্যের গোপনীয়তা।— (১) তদন্তের স্বার্থে কোনো ব্যক্তি, সত্তা বা সেবা প্রদানকারী কোনো তথ্য প্রদান বা প্রকাশ করিলে উক্ত ব্যক্তি, সত্তা বা সেবা প্রদানকারীর বিরুদ্ধে দেওয়ানি বা ফৌজদারি আইনে অভিযোগ দায়ের করা যাইবে না।

(২) এই অধ্যাদেশের অধীন তদন্তের সহিত সংশ্লিষ্ট সকল ব্যক্তি, সত্তা বা সেবা প্রদানকারীর তদন্ত সংশ্লিষ্ট তথ্যাদির গোপনীয়তা রক্ষা করিবেন।

(৩) যদি কোনো ব্যক্তি উপধারা (১) ও (২) এর বিধান লঙ্ঘন করেন, তাহা হইলে অনুরূপ লঙ্ঘন হইবে একটি অপরাধ এবং উক্ত অপরাধের জন্য তিনি অনধিক ২ (দুই) বৎসর কারাদণ্ডে বা অনধিক ১ (এক) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

৪০। মামলা দায়ের ও অপরাধ বিচারার্থ গ্রহণ, ইত্যাদি।— (১) সংক্ষুব্ধ ব্যক্তি সরাসরি বা তাহার কর্তৃক লিখিত ক্ষমতাপ্রাপ্ত ব্যক্তি বা আইনশৃংখলা রক্ষাকারী বাহিনীর সদস্য ব্যতীত অন্য কেউ অত্র অধ্যাদেশের অধীন মামলা দায়ের করিতে পারিবে না।

(২) সংক্ষুব্ধ ব্যক্তি সরাসরি বা তাহার কর্তৃক লিখিত ক্ষমতাপ্রাপ্ত ব্যক্তি থানায় কোনো অপরাধের অভিযোগ গ্রহণের অনুরোধ করিয়া ব্যর্থ হইয়াছেন মর্মে হলফনামা সহকারে ট্রাইব্যুনালের নিকট লিখিত নালিশ দাখিল করিলে, ট্রাইব্যুনাল অভিযোগকারীকে পরীক্ষা করিয়া সন্তুষ্ট হইলে অভিযোগটি তদন্তের জন্য পুলিশ অফিসারকে নির্দেশ প্রদান করিবে। ট্রাইব্যুনাল অভিযোগকারীকে পরীক্ষা করিয়া সন্তুষ্ট না হইলে অভিযোগটি সরাসরি নাকচ করিবে।

(৩) ট্রাইব্যুনাল তাহার এখতিয়ারের মধ্যে অত্র অধ্যাদেশের কোনো অপরাধ সংঘটনের কোনো তথ্য প্রাপ্ত হইলে তা অনুসন্ধানের জন্য পুলিশকে নির্দেশ প্রদান করিতে পারিবে এবং পুলিশ রিপোর্টের ভিত্তিতে পরবর্তী কার্যক্রম গ্রহণ করিতে পারিবে।

(৪) ফৌজদারি কার্যবিধিতে যাহা কিছুই থাকুক না কেন, পুলিশ অফিসারের লিখিত রিপোর্ট ব্যতীত ট্রাইব্যুনাল কোনো অপরাধ বিচারার্থ গ্রহণ (cognizance) করিবে না।

(৫) ট্রাইব্যুনাল এই অধ্যাদেশের অধীন অপরাধের বিচারকালে দায়রা আদালতে বিচারের জন্য ফৌজদারি কার্যবিধির অধ্যায় ২৩ এ বর্ণিত পদ্ধতি, এই অধ্যাদেশের বিধানাবলির সহিত সংগতিপূর্ণ হওয়া সাপেক্ষে, অনুসরণ করিবে।

৪১। অপরাধের বিচার ও আপিল।— (১) আপাতত বলবৎ অন্য কোনো আইনে যাহা কিছুই থাকুক না কেন, এই অধ্যাদেশের অধীন সংঘটিত অপরাধসমূহ কেবল ট্রাইব্যুনাল কর্তৃক বিচার্য হইবে।

(২) কোনো ব্যক্তি ট্রাইব্যুনাল কর্তৃক প্রদত্ত রায়ে সংক্ষুব্ধ হইলে তিনি আপিল ট্রাইব্যুনালে আপিল দায়ের করিতে পারিবেন।

৪২। ফৌজদারি কার্যবিধি, সাক্ষ্য আইন ও তথ্য ও যোগাযোগ প্রযুক্তি আইনের প্রয়োগ।— (১) এই অধ্যাদেশে ভিন্নরূপ কোনো বিধান না থাকিলে, ফৌজদারি কার্যবিধি, ১৮৯৮ (১৮৯৮ সনের ৫ নং আইন) (Code of Criminal Procedure, 1898), Evidence (Amendment) Act, 2022 (Act No. 20 of 2022) এবং তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (২০০৬ সনের ৩৯ নং আইন)-এর বিধানাবলি প্রযোজ্য হইবে।

(২) ট্রাইব্যুনাল ফৌজদারি কার্যবিধির অধীন আদি এখতিয়ার প্রয়োগকারী দায়রা আদালতের সকল ক্ষমতা প্রয়োগ করিতে পারিবে।

৪৩। সাক্ষ্যগত মূল্য।— Evidence (Amendment) Act, 2022 (Act No. 20 of 2022) বা অন্য কোনো আইনে ভিন্নতর যাহা কিছুই থাকুক না কেন, এই অধ্যাদেশের অধীন প্রাপ্ত বা সংগৃহীত কোনো ফরেনসিক প্রমাণ বিচার কার্যক্রমে সাক্ষ্য হিসাবে গণ্য হইবে।

৪৪। বিশেষজ্ঞ মতামত গ্রহণ, প্রশিক্ষণ, ইত্যাদি।— (১) ট্রাইব্যুনাল বা আপিল ট্রাইব্যুনাল, বিচারকার্য পরিচালনাকালে, কম্পিউটার বিজ্ঞান, ডিজিটাল ফরেনসিক, ইলেকট্রনিক যোগাযোগ, ডাটা সুরক্ষাসহ অন্যান্য বিষয়ে অভিজ্ঞ কোনো ব্যক্তির মতামত গ্রহণ করিতে পারিবে।

(২) সরকার বা এজেন্সি এই অধ্যাদেশ বাস্তবায়নের সহিত সংশ্লিষ্ট সকল ব্যক্তিকে, প্রয়োজনে, কম্পিউটার বিজ্ঞান, ডিজিটাল ফরেনসিক, ইলেকট্রনিক যোগাযোগ, ডাটা সুরক্ষাসহ অন্যান্য প্রয়োজনীয় বিষয়ে বিশেষায়িত প্রশিক্ষণ প্রদান করিতে পারিবে।

৪৫। মামলা নিষ্পত্তির জন্য নির্ধারিত সময়সীমা।— (১) ট্রাইব্যুনালের বিচারক এই অধ্যাদেশের অধীন কোনো মামলার অভিযোগ গঠনের তারিখ হইতে ১৮০ (একশত আশি) কার্য দিবসের মধ্যে মামলা নিষ্পত্তি করিবেন।

(২) ট্রাইব্যুনালের বিচারক উপধারা (১)-এর অধীন নির্ধারিত সময়ের মধ্যে কোনো মামলা নিষ্পত্তি করিতে ব্যর্থ হইলে, তিনি উহার কারণ লিপিবদ্ধ করিয়া উক্ত সময়সীমা সর্বোচ্চ ৯০ (নব্বই) কার্যদিবস বৃদ্ধি করিতে পারিবেন।

(৩) উপধারা (২) এর অধীন নির্ধারিত সময়ের মধ্যে ট্রাইব্যুনালের বিচারক কোনো মামলা নিষ্পত্তি করিতে ব্যর্থ হইলে, তিনি উহার কারণ লিপিবদ্ধ করিয়া বিষয়টি প্রতিবেদন আকারে হাইকোর্ট বিভাগকে অবহিত করিয়া মামলার কার্যক্রম পরিচালনা অব্যাহত রাখিতে পারিবেন।

৪৬। অপরাধের আমলযোগ্যতা, জামিনযোগ্যতা ও আপোসযোগ্যতা ইত্যাদি।— এই অধ্যাদেশের —

(ক) ধারা ১৭, ধারা ১৮ এর উপধারা (১)-এর দফা (গ), ধারা ১৯, ২০, ২১, ২২, ২৩, ২৫ এ উল্লিখিত অপরাধসমূহ আমলযোগ্য হইবে;

(খ) ধারা ১৭, ধারা ১৮ এর উপধারা (১)-এর দফা (গ), ধারা ১৯, ২২ এ উল্লিখিত অপরাধসমূহ অ-জামিনযোগ্য হইবে; এবং ধারা ১৮ এর উপধারা (১)-এর দফা (ক), (খ), ধারা ২০, ২১, ২৪, ২৫ ও ২৬ এ উল্লিখিত অপরাধসমূহ জামিনযোগ্য হইবে;

(গ) ধারা ১৮ এর উপধারা (১) এর দফা (ক), (খ), ১৯, ২১, ২২, ২৪ ও ২৫ এ উল্লিখিত অপরাধসমূহ আদালতের সম্মতিসাপেক্ষে আপোসযোগ্য হইবে।

৪৭। বাজেয়াপ্তি।— (১) এই অধ্যাদেশের অধীন কোনো অপরাধ সংঘটিত হইলে, যে সাইবার উপকরণ বা বস্তু সম্পর্কে বা সহযোগে উক্ত অপরাধ সংঘটিত হইয়াছে সেইগুলি ট্রাইব্যুনালের আদেশানুসারে বাজেয়াপ্তযোগ্য হইবে।

(২) উপধারা (১) এ যাহা কিছুই থাকুক না কেন, যদি ট্রাইব্যুনাল এই মর্মে সন্তুষ্ট হয় যে, যে ব্যক্তির দখল বা নিয়ন্ত্রণে পাওয়া গিয়াছে তিনি উক্ত উপকরণ সংশ্লিষ্ট অপরাধ সংঘটনের জন্য দায়ী নহেন, তাহা হইলে উক্ত সাইবার উপকরণ বাজেয়াপ্তযোগ্য হইবে না।

(৩) উপধারা (১) এর অধীন বাজেয়াপ্তযোগ্য কোনো সাইবার উপকরণের সহিত যদি কোনো বৈধ সাইবার উপকরণ পাওয়া যায়, তাহা হইলে সেইগুলিও বাজেয়াপ্তযোগ্য হইবে।

(৪) এই ধারার অন্যান্য বিধানে যাহা কিছুই থাকুক না কেন, কোনো অপরাধ সংঘটনের জন্য যদি কোনো সরকারি বা সংবিধিবদ্ধ সংস্থার সাইবার উপকরণ বা যন্ত্রপাতি ব্যবহার করা হয়, তাহা হইলে উহা বাজেয়াপ্তযোগ্য হইবে না।

ব্যাখ্যা: সাইবার উপকরণ বলিতে কম্পিউটার, কম্পিউটার সিস্টেম, ফ্লপি ডিস্ক, কমপ্যাক্ট ডিস্ক, টেপ ড্রাইভ বা অন্য কোনো আনুষঙ্গিক কম্পিউটার উপকরণ অন্তর্ভুক্ত হইবে।

অষ্টম অধ্যায় আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা

৪৮। আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা।— এই অধ্যাদেশের অধীন সংঘটিত কোনো অপরাধের তদন্ত ও বিচারের ক্ষেত্রে, আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা প্রয়োজন হইলে, ‘অপরাধ-সম্পর্কিত বিষয়ে পারস্পরিক সহায়তা আইন, ২০১২’ (২০১২ সনের ৪নং আইন) এর বিধানাবলি প্রযোজ্য হইবে।

নবম অধ্যায় বিবিধ

৪৯। বিধি প্রণয়নের ক্ষমতা।—(১) এই অধ্যাদেশের উদ্দেশ্যপূরণকল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, প্রয়োজনীয় সংখ্যক বিধি প্রণয়ন করিতে পারিবে।

(২) উপধারা (১) এর সামগ্রিকতাকে ক্ষুণ্ণ না করিয়া, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, অন্যান্য বিষয়ের মধ্যে, বিশেষ করিয়া নিম্নবর্ণিত সকল বা যে কোনো বিষয়ে বিধি প্রণয়ন করিতে পারিবে, যথা:—

- (ক) ডিজিটাল ফরেনসিক ল্যাব প্রতিষ্ঠা;
- (খ) মহাপরিচালক কর্তৃক ডিজিটাল ফরেনসিক ল্যাব তত্ত্বাবধান;
- (গ) ট্রাফিক ডাটা বা তথ্য পর্যালোচনা এবং উহা সংগ্রহ ও সংরক্ষণ পদ্ধতি;
- (ঘ) হস্তক্ষেপ, পর্যালোচনা বা ডিক্রিপশন পদ্ধতি এবং সুরক্ষা;
- (ঙ) সংকটাপন্ন তথ্য পরিকাঠামোর নিরাপত্তা;
- (চ) সাইবার সুরক্ষার ক্ষেত্রে আঞ্চলিক ও আন্তর্জাতিক সহযোগিতার পদ্ধতি;
- (ছ) ইমার্জেন্সি রেসপন্স টিম গঠন, পরিচালনা ও অন্যান্য টিমের দলের সহিত সমন্বয়সাধন;

