রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ গেজেট

অতিরিক্ত সংখ্যা

কর্তৃপক্ষ কর্তৃক প্রকাশিত

শুক্রবার, এপ্রিল ১০, ২০২৬

বাংলাদেশ জাতীয় সংসদ

ঢাকা, ২৭ চৈত্র, ১৪৩২/১০ এপ্রিল, ২০২৬

সংসদ কর্তৃক গৃহীত নিম্নলিখিত আইনটি ২৭ চৈত্র, ১৪৩২ মোতাবেক ১০ এপ্রিল, ২০২৬ তারিখে রাষ্ট্রপতির সম্মতিলাভ করিয়াছে এবং এতদ্বারা এই আইনটি সর্বসাধারণের অবগতির জন্য প্রকাশ করা যাইতেছে:—

২০২৬ সনের ৮১ নং আইন

সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫ রহিতপূর্বক সাইবার সুরক্ষা নিশ্চিতকরণ এবং সাইবার স্পেসে সংঘটিত অপরাধ শনাক্তকরণ, প্রতিরোধ, দমন ও উক্ত অপরাধের বিচার এবং আনুষঙ্গিক বিষয়ে বিধান প্রণয়নকল্পে প্রণীত আইন

যেহেতু সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫ (২০২৫ সনের ২৫ নং অধ্যাদেশ) রহিতপূর্বক পুনঃপ্রণয়ন করা সমীচীন ও প্রয়োজনীয় ;

সেহেতু এতদ্দ্বারা নিম্নরূপ আইন প্রণয়ন করা হইল :—

প্রথম অধ্যায়

প্রারম্ভিক

১। **সংক্ষিপ্ত শিরোনাম ও প্রবর্তন**।— (১) এই আইন সাইবার সুরক্ষা আইন, ২০২৬ নামে অভিহিত হইবে।

(২) ইহা ২১ মে, ২০২৫ তারিখে কার্যকর হইয়াছে বলিয়া গণ্য হইবে।

মূল্য : টাকা ৪০.০০

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

(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 ইন্টারনেট অফ থিংস (আইওটি) ডিভাইস বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক বা কৃত্রিম বুদ্ধিমত্তা সফটওয়্যার এজেন্ট, লার্জ ল্যাঙ্গুয়েজ 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 ল্যাঙ্গুয়েজ 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 উপ-ধারা (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**" অর্থ 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 থ্রেট ইন্টেলিজেন্স"** অর্থ এমন একটি কর্ম-প্রক্রিয়া বা পদ্ধতি যাহার মাধ্যমে গুরুত্বপূর্ণ তথ্য অবকাঠামোর সাইবার সুরক্ষা, 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 যাহা কোন ব্যক্তি, কৃত্রিম বুদ্ধিমত্তা এজেন্ট, প্রতিষ্ঠান এবং রাষ্ট্রকে এসব হুমকির বিরুদ্ধে প্রতিরোধমূলক ব্যবস্থা গ্রহণ করিতে সহায়তা করে ;

(ঞ) **"জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম (National Cyber Emergency Response Team-NCERT)"** অর্থ সরকার কর্তৃক অনুমোদিত সত্তা যাহা সাইবার আক্রমণ এবং সাইবার সুরক্ষা সংক্রান্ত ঘটনাসমূহ পরীক্ষা-নিরীক্ষা, ফোরকাস্ট ও পর্যালোচনা, সাইবার সুরক্ষা আইন প্রয়োগের কারিগরি জ্ঞান নির্মাণ ও বিস্তারে সহায়তা এবং সাইবার অপরাধের আইনি তদন্তের জন্য সকল ধরনের প্রযুক্তিগত সহায়তা প্রদান করে ;

(ট) **"জাতীয় সাইবার নিরাপত্তা অপারেশন সেন্টার (National Security Operation Center-NSOC)"** অর্থ একটি রাষ্ট্র-সমর্থিত সংস্থা যাহা একটি দেশের জাতীয় পর্যায়ের সাইবার নিরাপত্তা নিশ্চিত করিবার জন্য কাজ করে। এটি জাতীয়ভাবে গুরুত্বপূর্ণ অবকাঠামো (যেমন বিদ্যুৎ, জ্বালানি, স্বাস্থ্যসেবা, ব্যাংকিং, যোগাযোগ ব্যবস্থা) এবং সরকারিডাটা সিস্টেমের সুরক্ষা নিশ্চিত করিতে কেন্দ্রীয় ভূমিকা পালন করে ; জাতীয় সাইবার নিরাপত্তা অপারেশন সেন্টার সাধারণত সাইবার হুমকি শনাক্ত, প্রতিরোধ, মোকাবিলা এবং পরবর্তী পদক্ষেপের জন্য বিশ্লেষণ পরিচালনা করে ; এটি রাষ্ট্রের বিরুদ্ধে সাইবার আক্রমণ, সাইবার সন্ত্রাসবাদ, এবং ক্রিটিক্যাল ইনফ্রাস্ট্রাকচার লক্ষ্য করিয়া পরিচালিত আক্রমণসমূহের প্রতিরোধে সক্রিয় ভূমিকা পালন করে ; পাশাপাশি এটি আন্তর্জাতিক সাইবার নিরাপত্তা অংশীদারদের সহিত সমন্বয় সাধন করে এবং সাইবার নিরাপত্তা সচেতনতা প্রশিক্ষণসহ বিভিন্ন কার্যক্রমে সহায়তা করে ; এছাড়াও, জাতীয় সাইবার নিরাপত্তা অপারেশন সেন্টার একটি নিয়ন্ত্রক সংস্থা হিসেবে কাজ করিতে পারে যাহা দেশের সকল সরকারি ও বেসরকারি সিকিউরিটি অপারেশন সেন্টার এর কার্যক্রম পরিচালনা ও স্বীকৃতি প্রদান করে সঠিক নিয়মাবলি এবং প্রবিধান অনুসরণ নিশ্চিত করে ; জাতীয় সাইবার নিরাপত্তা অপারেশন সেন্টার দেশের সকল সিকিউরিটি অপারেশন সেন্টার 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"** অর্থ কম্পিউটার সিস্টেমের মাধ্যমে সংঘটিত যোগাযোগ সম্পর্কিত যেকোনো কম্পিউটার ডাটা, যাহা যোগাযোগের শৃঙ্খলে অংশ নেওয়া কম্পিউটার সিস্টেম দ্বারা উৎপন্ন হয় বা অনুরূপ কৃত্রিম বুদ্ধিমত্তা সিস্টেম দ্বারা উৎপন্ন হয়, যাহা 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 আইনের উদ্দেশ্য পূরণকল্পে, ইলেকট্রিক্যাল, ইলেকট্রনিক, ডিজিটাল ম্যাগনেটিক, অপটিক্যাল, বায়োমেট্রিক, ইলেকট্রোকেমিক্যাল, ইলেকট্রোমেকানিক্যাল, ওয়্যারলেস বা ইলেকট্রো-ম্যাগনেটিক টেকনোলজি, কৃত্রিম বুদ্ধিমত্তা টেকনোলজি, ব্লকচেইন, লার্জ ল্যাঙ্গুয়েজ মডেল ও 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 এপ্লিকেশন, এ্যালগরিদম, ডাটা ভিত্তিক সিদ্ধান্ত গ্রহণের 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 ল্যাঙ্গুয়েজ 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 আন্তর্জাতিকভাবে স্বীকৃত কমপ্লায়েন্স নিশ্চিত করে, যাহা আইনিভাবে গ্রহণযোগ্য পদ্ধতিতে ডিজিটাল প্রমাণ সংগ্রহ, সংরক্ষণ, বিশ্লেষণ এবং উপস্থাপন করিতে প্রয়োজনীয় কারিগরি সক্ষমতাসহ গঠিত হয় ;

(থ) **"ডিজিটাল শিশু যৌন নিপীড়ন সংক্রান্ত উপাদান"** অর্থ যে কোনো মাধ্যমে, কোনো ডিজিটাল বা ইলেকট্রনিক মাধ্যম ব্যবহার করিয়া তৈরি করা কোনো উপাদান বা উপস্থাপনা যাহা—

(অ) দৃষ্টিগত, শ্রবণযোগ্য, বা পাঠ্যগতভাবে, অথবা অন্যকোনোভাবে, চিত্রিত বা বর্ণনা করে, যাহা বাস্তব বা অনুকৃত (simulated) যৌন সম্পর্কিত স্পষ্ট কার্যকলাপ, অথবা কোনো যৌন অঙ্গ, অথবা যৌন শোষণ বা নির্যাতন, অথবা যৌনসেবা, অথবা শিশুসহ অন্য ব্যক্তির সহিত যৌনতাপূর্ণ যোগাযোগ, অথবা প্রযোজ্য আইন অনুযায়ী সংজ্ঞায়িত যৌন অপরাধ যাহা শিশু আইন, ২০১৩ (২০১৩ সনের ২৪ নং আইন) এর ধারা ২(১৭) ও ৪ এ সংজ্ঞায়িত কোনো শিশুর সম্পর্কিত বা উপস্থিতিতে সংঘটিত হয় ; বা

(আ) দৃষ্টিগত, শ্রবণযোগ্য, বা পাঠ্যগতভাবে, অথবা অন্যকোনোভাবে কোনো শিশুকে প্ররোচিত, উত্তেজিত, উৎসাহিত বা নির্দেশিত করে, কোনো বাস্তব বা অনুকৃত (simulated) যৌনতাপূর্ণ কাজে জড়িত হইতে বা পর্যবেক্ষণ করিতে, অথবা কোনো যৌন অঙ্গ প্রদর্শন করিতে, অথবা যৌন শোষণ বা নির্যাতন, অথবা যৌন সেবায় জড়িত হইতে বা সহায়তা করিতে, অথবা শিশুসহ অন্য ব্যক্তির সহিত যৌনতাপূর্ণ যোগাযোগে জড়িত হইতে বা পর্যবেক্ষণ করিতে, অথবা প্রযোজ্য আইনে সংজ্ঞায়িত অন্যান্য যৌন অপরাধে জড়িত হইতে বা সহায়তা করিতে (যাহার মধ্যে রহিয়াছে যৌন সেবার জন্য অর্থ প্রদান বা গ্রহণ করা) অথবা যৌন শোষণের জন্য কোনো শিশুকে নিয়ন্ত্রণ করা, অথবা যৌন উদ্দেশ্যে কোনো শিশুকে প্রলুব্ধ করা ; বা

(ই) দৃষ্টিগত, শ্রবণযোগ্য, বা পাঠ্যগতভাবে, অথবা অন্যকোনোভাবে প্ররোচনা, উত্তেজনা, উৎসাহ, হুমকি বা নির্দেশ প্রদান করিয়া কোনো ব্যক্তি কোনো সাহায্য বা ব্যবস্থার মাধ্যমে কোনো শিশুকে কোনো বাস্তব বা অনুকৃত (simulated) যৌনতাপূর্ণ কাজে জড়িত হইতে বা পর্যবেক্ষণ করিতে, অথবা কোনো যৌন অঙ্গ প্রদর্শন করিতে, অথবা

যৌন শোষণ বা নির্যাতন, অথবা যৌন সেবায় জড়িত হইতে বা সহায়তা করিতে, অথবা শিশুসহ অন্য ব্যক্তির সহিত যৌনতাপূর্ণ যোগাযোগে জড়িত হইতে বা পর্যবেক্ষণ করিতে, অথবা প্রযোজ্য আইন অনুযায়ী সংজ্ঞায়িত অন্যান্য যৌন অপরাধে জড়িত হইতে বা সহায়তা করিতে, যাহার মধ্যে রহিয়াছে যৌন সেবার জন্য অর্থ প্রদান বা গ্রহণ করা, যৌন শোষণের জন্য কোনো শিশুকে নিয়ন্ত্রণ করা, অথবা যৌন উদ্দেশ্যে কোনো শিশুকে প্রলুব্ধ করা :

তবে শর্ত থাকে যে, এই ধরনের উপাদান যৌন উত্তেজনা বা পরিতৃপ্তি সৃষ্টি বা প্ররোচিত করিবার উদ্দেশ্যে তৈরি করা হইয়াছে কিনা তাহা অপ্রাসঙ্গিক বলিয়া বিবেচ্য হইবে :

আরও শর্ত থাকে যে, এই ধরনের যেকোনো উপাদান যাহা স্পষ্টভাবে আইন প্রয়োগের স্বার্থে বা অপরাধ তদন্ত, চিকিৎসা সেবা, বা অনুমোদিত গবেষণা, শিক্ষা, বা গণমাধ্যমের প্রতিবেদনের উদ্দেশ্যে কেবল বৈধ উদ্দেশ্যে তৈরি এবং/অথবা ব্যবহৃত হইয়াছে, তাহা এই সংজ্ঞার আওতাভুক্ত হইবে না ;

(দ) "**পুলিশ অফিসার**" অর্থ সাব-ইন্সপেক্টর পদমর্যাদার নিম্নে নহেন এইরূপ কোনো পুলিশ অফিসার ;

(ধ) "**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 ;

(ন) "**ফৌজদারি কার্যবিধি**" অর্থ Code of Criminal Procedure, 1898 (Act No. V of 1898) ;

(প) '**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 ;

(ফ) '**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 (Cache) হইতে তথ্য-উপাত্ত সরানো, সফটওয়্যার লগ, ট্রেস, রেকর্ড মুছে দেয়া বা সরানো, ক্ষেত্রমত, স্থানান্তর, ব্লক করা, যাহা অনুপ্রবেশ বা হ্যাকিং নামেও অভিহিত হইবে ;

(ব) '**ভৌত অবকাঠামো**' অর্থ সকল ধরনের হার্ডওয়ারভিত্তিক উপাদান ও প্রযুক্তি, যাহা ডিজিটাল নেটওয়ার্ক এবং ভার্চুয়াল পরিবেশের কার্যক্রমকে সমর্থন করে; ডাটা সেন্টার, সার্ভার এবং কম্পিউটার হার্ডওয়ার, নেটওয়ার্কিং অবকাঠামো, ইন্টারনেট এক্সচেঞ্জ পয়েন্ট, ইন্টারনেট অফ থিংস (আইওটি), ওয়াই-ফাই নেটওয়ার্ক, টেলিযোগাযোগ ফোরজি বা ফাইভজিসহ নূতন যোগাযোগ প্রযুক্তি নেটওয়ার্ক, স্যাটেলাইট সিস্টেম, স্যাটেলাইট ইন্টারনেট ও যোগাযোগ টাওয়ার, যোগাযোগ প্রযুক্তিতে ব্যবহৃত বিদ্যুৎ ও জ্বালানি সঞ্চালন ও বিতরণ নেটওয়ার্ক, ভূমিও নদীর তলদেশের ক্যাবল, সাবমেরিন ক্যাবল, ওভারহেড ফাইবার ক্যাবল, অপটিক্যাল সঞ্চালন নেটওয়ার্কও ইহার অন্তর্ভুক্ত হইবে ;

(ভ) '**মহাপরিচালক**' অর্থ এজেন্সির মহাপরিচালক ;

(ম) '**ম্যালওয়্যার**' অর্থ এইরূপ কোনো ডিজিটাল বা ইলেকট্রনিক নির্দেশ, তথ্য-উপাত্ত, প্রোগ্রাম বা অ্যাপ্স যাহা—

(অ) কোনো কম্পিউটার বা ডিজিটাল ডিভাইস কর্তৃক সম্পাদিত কার্যকে পরিবর্তন, বিকৃত, বিনাশ, ক্ষতি বা ক্ষুণ্ন করে বা উহার কার্য-সম্পাদনে বিরূপ প্রভাব বিস্তার করে, বা প্রবেশাধিকারের সীমা বা গভীরতা বাড়ায় ; বা

(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 ;

(য) **"যৌন হয়রানি"** অর্থ–

(অ) সাইবার স্পেসে বারংবার নগ্ন ছবি চাহিবার মাধ্যমে হয়রানি করা, প্রশাসনিক অথবা পেশাগত ক্ষমতার অপব্যবহার করিয়া সাইবার স্পেসে অবৈধ শারীরিক সম্পর্ক স্থাপনের প্রস্তাব দেওয়া ; বা

(আ) সাইবার স্পেসে কোনো ব্যক্তির যৌনাঙ্গের ছবি বা যৌন উদ্দীপক উপাদান বা পর্নোগ্রাফিক উপাদান অনাকাঙ্ক্ষিতভাবে প্রেরণ, কারো অনুমতি ব্যতিরেকে তাহার ছবিকে কোনো প্রযুক্তির সহায়তায় পর্নোগ্রাফিক উপাদানে রূপদান করা বা যৌনকরণ করা ; বা

(ই) সাইবার স্পেসে সম্পর্কের প্রস্তাবে সাড়া প্রদান না করিবার কারণে হমকি প্রদান, প্রলোভন বা হুমকির মাধ্যমে যৌন সম্পর্ক স্থাপনের প্রচেষ্টা ;

(র) **"রিভেঞ্জ পর্ণ"** অর্থ কোনো ব্যক্তির অনুমতি ব্যতিত তাহার ক্ষতিসাধনের উদ্দেশ্যে উক্ত ব্যক্তির অন্তরঙ্গ অথবা ব্যক্তিগত ছবি, ভিডিও অথবা অনুরূপ উপাত্ত যে কোনো প্রকার প্রযুক্তি ব্যবহার করিয়া ছড়াইয়া দেওয়া ;

(ল) **'সাইবার সুরক্ষা'** অর্থে 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 নিশ্চিতকরণসহ উক্তরূপ বিষয়াবলিতে কোন ব্যক্তির পাশাপাশি কৃত্রিম বুদ্ধিমত্তা এজেন্ট বা টুলের এক্সেস বুঝাইবে। নাগরিকদের সার্বক্ষণিক ইন্টারনেট প্রাপ্তির অধিকারও ইহার অন্তর্ভুক্ত হইবে ;

(শ) **"সাইবার স্পেস"** অর্থ আন্তঃসংযোগকৃত সকল ডিজিটাল ডিভাইস এবং ডিজিটাল নেটওয়ার্কসমূহের সকল ফিজিক্যাল এবং ভার্চুয়াল জগত বুঝাইবে (যেমন- 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 যেখানে ডাটা তৈরি, ডাটা মিররিং, অ্যাক্সেস, প্রেরণ, সংরক্ষণ, ব্যবস্থাপনাসহ সকল ধরনের হিউম্যান ও নন-হিউম্যান অনলাইন কর্মকান্ড সংঘটিত হয়) এবং ডিজিটাল ডিভাইস, কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার ডাটা, সিগনালিং ডাটা, ট্রাফিক ডাটা এবং কৃত্রিম বুদ্ধিমত্তা উৎপন্ন ডাটাও উহার অন্তর্ভুক্ত হইবে ;

(ষ) **"সিগনালিং ডাটা"** অর্থে ডিজিটাল ডিভাইস, সার্ভার এবং নেটওয়ার্কের মধ্যকার সংযোগ স্থাপনকালীন বা কানেকশন সেটআপ সম্পর্কিত তথ্য বুঝাইবে;

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

(হ) **"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 ; বা

(ই) এজেন্সি-স্বীকৃত আইএসও বা আইইসি মানের তথ্য ও যোগাযোগ প্রযুক্তি পরীক্ষাগার যাহা সফটওয়্যার টেস্টিং পরীক্ষাগার, সাইবার সিকিউরিটি পেনিট্রেশন টেস্টিং পরীক্ষাগার, সাইবার স্পেসে ব্যবহৃত পণ্যের টেস্টিং, সাইবার সুরক্ষা মূল্যায়ন, সাইবার সুরক্ষা পণ্য বা সেবার সনদ প্রদানকারী, সাইবার সুরক্ষা ব্যবস্থাপনা পদ্ধতি অডিটিং এবং সাইবার সুরক্ষা রিপোর্ট প্রদান করে এবং উক্ত সেবা প্রদানকারী প্রতিষ্ঠান এবং প্রতিষ্ঠান নিয়োজিত সেবা প্রদানকারী প্রযুক্তিবিদ বা অডিটর ; বা

(ঈ) তৃতীয় পক্ষ হিসেবে সেবা প্রদানকারী প্রতিষ্ঠান যারা সাইবার সুরক্ষা পরিচালনা বা পর্যবেক্ষণকারী (সাইবার সিকিউরিটি পরিচালনা কেন্দ্র) এবং প্রতিষ্ঠান নিয়োজিত সেবা প্রদানকারী প্রযুক্তিবিদ বা বিশ্লেষক ; বা

(উ) সাইবার সুরক্ষায় নিয়োজিত ভিএলএসআই বা সেমিকন্ডাক্টর ডিজাইন বা টেস্টিং বা উৎপাদন প্রক্রিয়ায় নিয়োজিত প্রতিষ্ঠান বা সেবা প্রদানকারী প্রতিষ্ঠান এবং প্রতিষ্ঠানে নিয়োজিত সংশ্লিষ্ট সেবা প্রদানকারী পরীক্ষক, নকশাকারী, প্রযুক্তিবিদ ;

(ড়) **'সেক্সটর্শন'** অর্থ এক প্রকার প্রতারণা বা এক্সটর্শন যাহার দ্বারা কোন ব্যক্তির অন্তরঙ্গ অথবা ব্যক্তিগত ছবি, ভিডিও সংরক্ষণ বা সংরক্ষণের দাবি করিবার মাধ্যমে তাহা প্রকাশ করিবার হুমকি প্রদানের মাধ্যমে অর্থ, সুযোগ-সুবিধা লাভ বা শারীরিক সম্পর্ক স্থাপনের চেষ্টা করা।

(২) এই আইনে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞার্থ প্রদান করা হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (২০০৬ সনের ৩৯ নং আইন) এ যে অর্থে ব্যবহৃত হইয়াছে সেই অর্থে প্রযোজ্য হইবে।

৩। **আইনের প্রযোজ্যতা**।—(১) এই আইনের কোনো বিধানের সহিত কোনো আইনের কোনো বিধান অসামঞ্জস্যপূর্ণ হয়, তাহা উক্ত আইনের সংশ্লিষ্ট বিধানের সহিত এই আইনের বিধানটি যতখানি অসামঞ্জস্যপূর্ণ হয় ততখানির ক্ষেত্রে এই আইনের বিধান কার্যকর থাকিবে।

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

৪। **আইনের অতিরাষ্ট্রিক প্রয়োগ**।— (১) যদি বাংলাদেশের কোনো নাগরিক বাংলাদেশের বাহিরে এই আইনের অধীন কোনো অপরাধ সংঘটন করেন যাহা বাংলাদেশে সংঘটন করিলে এই আইনের অধীন দণ্ডযোগ্য হইত, তাহা হইলে এই আইনের 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 আইনের অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে উক্ত ব্যক্তির বিরুদ্ধে এই আইনের বিধানাবলি এইরূপে প্রযোজ্য হইবে যেন উক্ত অপরাধের সম্পূর্ণ প্রক্রিয়া বাংলাদেশেই সংঘটিত হইয়াছে।

(৩) যদি কোনো ব্যক্তি বাংলাদেশের অভ্যন্তর হইতে বাংলাদেশের বাহিরে এই আইনের অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে এই আইনের 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 আইনের 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 সুরক্ষা ও এতদ্‌সংক্রান্ত আইনের বিষয়ে বিশেষজ্ঞ ব্যক্তিদের মধ্য হইতে, যাহাদের সাইবার সুরক্ষা বিষয়ে আন্তর্জাতিকভাবে স্বীকৃত সনদ বা সার্টিফিকেট রহিয়াছে, সরকার কর্তৃক নিযুক্ত হইবেন।

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

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

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

তৃতীয় অধ্যায়

প্রতিরোধমূলক ব্যবস্থাদি

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 সুরক্ষার ক্ষেত্রে হুমকি সৃষ্টি করিলে তিনি উক্ত তথ্য-উপাত্ত অপসারণ, ক্ষেত্রমতো স্থানান্তর বা ব্লক করিবার প্রয়োজনীয় ব্যবস্থা গ্রহণ করিবেন বা প্রযোজ্য ক্ষেত্রে বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশনকে, অতঃপর বিটিআরসি বলিয়া উল্লিখিত, অনুরোধ করিতে পারিবেন।

(২) যদি আইনশৃঙ্খলা রক্ষাকারী বাহিনীর নিকট তথ্য উপাত্ত বিশ্লেষণসাপেক্ষে বিশ্বাস করিবার কারণ থাকে যে, ডিজিটাল বা ইলেকট্রনিক মাধ্যমে প্রকাশিত বা প্রচারিত কোনো তথ্য দেশের অখন্ডতা, নিরাপত্তা, প্রতিরক্ষা,জনশৃঙ্খলা ক্ষুণ্ণ করে, ধর্মীয় বা সাম্প্রদায়িক ঘৃণামূলক বা জাতিগত বিদ্বেষমূলক বক্তব্য যাহা সহিংসতা তৈরিতে উদ্রেগ সৃষ্টি করে বা বিশৃঙ্খলা বা অপরাধমূলক কর্মকান্ডের নির্দেশনা প্রদান করে, তাহা হইলে আইন-শৃঙ্খলা রক্ষাকারী বাহিনী উক্ত তথ্য-উপাত্ত অপসারণ বা ব্লক করিবার জন্য বা, ক্ষেত্রমত স্থানান্তরের জন্য মহাপরিচালকের মাধ্যমে প্রয়োজনীয় ব্যবস্থা গ্রহণ করিবে বা প্রযোজ্য ক্ষেত্রে 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, ক্ষেত্রমত ব্লক করিবার জন্য প্রযুক্তি কোম্পানিকে অনুরোধ এবং অতঃপর উহা সরকারকে অবহিত করিবে এবং কোনো কন্টেন্ট ব্লক করা হইলে স্বচ্ছতার স্বার্থে সরকার সকল ব্লক হওয়া কন্টেন্টের তথ্য জনসম্মুখে প্রকাশ করিবার ব্যবস্থা গ্রহণ করিবে।

(৪) উপ-ধারা (১), (২) ও (৩) এর অধীন তথ্য-উপাত্ত অপসারণ, ক্ষেত্রমত, স্থানান্তর বা ব্লক করিবার ৩ (তিন) দিনের মধ্যে উক্ত বিষয়ে সংশ্লিষ্ট ট্রাইব্যুনালের অনুমতি গ্রহণ করিতে হইবে এবং উল্লিখিত সময়ের মধ্যে অনুমতি গ্রহণ না করিলে বা ট্রাইব্যুনাল অনুমতি প্রদান না করিলে অপসারিত বা, ক্ষেত্রমত, স্থানান্তরিত বা ব্লককৃত তথ্য-উপাত্ত পুনরায় বাধ্যতামূলকভাবে অবমুক্ত করিতে হইবে।

(৫) এই ধারার উদ্দেশ্যপূরণকল্পে, প্রয়োজনীয় অন্যান্য বিষয়াদি বিধি দ্বারা নির্ধারিত হইবে।

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

(২) ধারা ১৫ এর অধীন ঘোষিত কোনো 'গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিজস্ব কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম এবং সিকিউরিটি অপারেশন সেন্টার থাকিবে এবং সকল সিকিউরিটি অপারেশন সেন্টারকে প্রতি ত্রৈমাসিকে তাদের কার্যক্রম ও সাফল্য সূচক রিপোর্ট জাতীয় সাইবার নিরাপত্তা অপারেশন সেন্টার এ জমা প্রদান করিতে হইবে।

(৩) জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইন্সিডেন্ট 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 ইন্সিডেন্ট রেসপন্স টিম, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, সার্বক্ষণিকভাবে দায়িত্ব পালন করিবে, সাইবার ঝুঁকি নির্ণয়, ঝুঁকি অপসারণ এবং ডিজিটাল ফরেনসিক অ্যানালাইসিসের সক্ষমতা নিশ্চিতকরণে এজেন্সি কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম ও সিকিউরিটি অপারেশন সেন্টারসমূহের মধ্যে এজেন্সি সমন্বয় সাধন, পরামর্শ এবং সময় নিয়ন্ত্রিত নির্দেশনা প্রদান করিবে:

তবে শর্ত থাকে যে, কোনো সরকারি, বেসরকারি বা স্বায়ত্বশাসিত সংস্থা বা প্রতিষ্ঠানে সাইবার ইন্সিডেন্ট ঘটিলে উক্ত সংস্থা বা প্রতিষ্ঠান অনতিবিলম্বে এজেন্সির আওতাধীন জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিমকে অবহিত করিবে।

(৫) উপ-ধারা (৪) এর সামগ্রিকতাকে ক্ষুন্ন না করিয়া, জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বা কম্পিউটার ইন্সিডেন্ট 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 আইনের উদ্দেশ্য পূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সমজাতীয় বিদেশি কোনো টিম বা প্রতিষ্ঠানের সহিত তথ্য, লগ এবং ফরেনসিক আদান-প্রদানসহ সার্বিক সহযোগিতামূলক কার্যক্রম গ্রহণ ;

(ঙ) সাইবার সিকিউরিটির গ্লোবাল থ্রেট ইন্টেলিজেন্স এ বাই-লেটারাল তথ্য ও লগ আদান-প্রদানের উদ্যোগ গ্রহণ ;

(চ) এই আইনের উদ্দেশ্য পূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সিকিউরিটি অ্যানালাইসিসের নিমিত্তে ক্লাউডভিত্তিক সাইবার সিকিউরিটি সল্যুউশন (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

(ছ) বিধি দ্বারা নির্ধারিত অন্যান্য কার্য সম্পাদন।

(৬) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম এর প্রযুক্তিগত সক্ষমতা–

(ক) সাইবার নিরাপত্তার প্রশ্নে, সিঙ্গেল পয়েন্ট অফ ফেইলিউর এড়াইতে, কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ নিজেদের সহিত যোগাযোগের সহজলভ্যতা নিশ্চিত করিবে এবং সার্বক্ষণিক যোগাযোগের একাধিক মাধ্যম প্রস্তুত রাখিবে, টিমসমূহ স্পষ্টভাবে নিজেদের যোগাযোগের মাধ্যম অনলাইনে প্রকাশ করিবে এবং যেকোনো পরিবর্তন অংশীদারদের অবগত করিবে ;

(খ) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহের কার্যস্থল এবং সহায়ক তথ্য ব্যবস্থা আবশ্যকভাবে নিরাপদ স্থানে থাকিতে হইবে ;

(গ) কার্যকর ও দক্ষ দায়িত্ব হস্তান্তর নিশ্চিত করিবার জন্য কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ অনুরোধ ব্যবস্থাপনা ও হস্তান্তরের জন্য উপযুক্ত একটি ব্যবস্থা দ্বারা সজ্জিত থাকিবে ;

(ঘ) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহকে, তাদের কার্যক্রমের গোপনীয়তা এবং বিশ্বাসযোগ্যতা নিশ্চিত করিতে হইবে ;

(ঙ) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ নিশ্চিত করিবে যে, তাহাদের সার্বক্ষণিক পর্যাপ্ত সংখ্যক প্রশিক্ষিত লোকবল বিদ্যমান রহিয়াছে ;

(চ) সেবার ধারাবাহিকতা নিশ্চিত করিতে সার্টসমূহ প্রয়োজনাতিরিক্ত ব্যবস্থা এবং কম্পিউটার সিস্টেম প্রস্তুত রাখিতে হইবে ;

ছ) সার্টসমূহ আন্তর্জাতিক সহযোগিতা নেটওয়ার্কে অংশগ্রহণ করিতে পারিবে।

(৭) গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ নিজ নিজ সার্টসমূহের প্রযুক্তিগত সক্ষমতা, জনবল এবং প্রয়োজনীয় অর্থ বরাদ্দ নিশ্চিত করিবে।

(৮) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ নিম্নবর্ণিত দায়িত্ব পালন করিবে:

(ক) জাতীয় পর্যায়ে সাইবার হুমকি, দুর্বলতা এবং ঘটনাবলীর পর্যবেক্ষণ ও বিশ্লেষণ করা এবং, প্রয়োজনে, সংশ্লিষ্ট গুরুত্বপূর্ণ ও অপরিহার্য সংস্থাসমূহের নেটওয়ার্ক ও তথ্য ব্যবস্থার তাৎক্ষণিক পর্যবেক্ষণের জন্য সহায়তা প্রদান করা ;

(খ) সাইবার হুমকি, দুর্বলতা এবং ঘটনাবলী সম্পর্কে সংশ্লিষ্ট গুরুত্বপূর্ণ ও অপরিহার্য সংস্থাসমূহ, নিয়ন্ত্রক কর্তৃপক্ষ এবং অন্যান্য সংশ্লিষ্ট পক্ষকে আগাম সতর্কতা, বিজ্ঞপ্তি, ঘোষণাসহ তাৎক্ষণিক তথ্য প্রদান করা ;

(গ) সাইবার ইন্সিডেন্ট মোকাবিলা করা এবং, প্রয়োজনে, সংশ্লিষ্ট গুরুত্বপূর্ণ ও অপরিহার্য সংস্থাসমূহকে কারিগরি সহায়তা প্রদান করা ;

(ঘ) ফরেনসিক তথ্য সংগ্রহ ও বিশ্লেষণ করা এবং সাইবার নিরাপত্তা সম্পর্কিত নিত্যনৈমিত্তিক ও পরিবর্তনশীল ঝুঁকি ও ঘটনা বিশ্লেষণ এবং পরিস্থিতি সম্পর্কে সচেতনতা বৃদ্ধি করা ;

(ঙ) সংশ্লিষ্ট গুরুত্বপূর্ণ বা অপরিহার্য সংস্থার অনুরোধে তাহাদের নেটওয়ার্ক ও তথ্য ব্যবস্থার সক্রিয় স্ক্যানিং (পরিবীক্ষণ, পরিদর্শন ও নিরীক্ষা) করা, যাহাতে তাৎপর্যপূর্ণ প্রভাব ফেলিবার মতো যেকোনো দুর্বলতা শনাক্ত করা যায় ;

(চ) আন্তর্জাতিক সহযোগিতা নেটওয়ার্কে অংশগ্রহণ করা এবং, প্রয়োজনে, অন্যান্য কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম (CIRT) নেটওয়ার্ক সদস্যদের অনুরোধে পারস্পরিক সহায়তা প্রদান করা এবং, প্রয়োজনে, লগ আদান প্রদানে সাহায্য করা ;

(ছ) জাতীয় সাইবার সুরক্ষা এজেন্সির অনুমতিসাপেক্ষে, কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহের (CIRT) কৌশলগত সহযোগিতা ও তথ্য আদান-প্রদানকে সহায়তা ও সহজতর করিবার লক্ষ্যে একটি সহযোগিতা গ্রুপ প্রতিষ্ঠা করা যাহা সমন্বিতভাবে সাইবার দুর্বলতা উন্মোচনের জন্য সমন্বয়কের ভূমিকা পালন করিবে ;

(জ) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ সংশ্লিষ্ট বেসরকারি খাতের অংশীজনদের সহিত সহযোগিতামূলক সম্পর্ক প্রতিষ্ঠা করিবে এবং তথ্য বিনিময়ে সহায়তা প্রদান করিবে ;

(ঝ) কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ তাহাদের আওতাধীন সংশ্লিষ্ট গুরুত্বপূর্ণ ও অপরিহার্য সংস্থার সক্রিয় উন্মুক্ত নেটওয়ার্ক ও তথ্য ব্যবস্থার স্ক্যানিং পরিচালনা করিতে পারিবে, উক্ত স্ক্যানিং কেবল দুর্বল বা নিরাপত্তাহীনভাবে কনফিগার করা নেটওয়ার্ক ও তথ্য ব্যবস্থা শনাক্ত করিবার জন্য পরিচালিত হইবে এবং সংশ্লিষ্ট সংস্থাসমূহকে অবহিত করিবার উদ্দেশ্যে সম্পাদিত হইবে, এই স্ক্যানিং সংশ্লিষ্ট সংস্থার সেবার কার্যকারিতার উপর কোনো নেতিবাচক প্রভাব ফেলিবে না ;

(ঞ) উপরি-উল্লিখিত দায়িত্বসমূহ পালনকালে, কম্পিউটার ইন্সিডেন্ট রেসপন্স টিমসমূহ ঝুঁকির মাত্রার ভিত্তিতে নির্দিষ্ট কাজকে অগ্রাধিকার প্রদান করিতে পারিবে।

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

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

(২) উপ-ধারা (১) এ যাহা কিছুই থাকুক না কেন, এই আইন 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 আইনের 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 আইনের উদ্দেশ্যপূরণকল্পে, নিম্নবর্ণিত সদস্য সমন্বয়ে জাতীয় সাইবার সুরক্ষা কাউন্সিল গঠিত হইবে, যথাঃ–

(ক) প্রধানমন্ত্রী, গণপ্রজাতন্ত্রী বাংলাদেশ সরকার, যিনি ইহার চেয়ারম্যানও হইবেন ;

(খ) মন্ত্রী, প্রতিমন্ত্রী ও উপমন্ত্রী (যদি থাকে), ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয় ;

(গ) মন্ত্রী, আইন বিচার ও সংসদ বিষয়ক মন্ত্রণালয় ;

(ঘ) 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) সচিব, লেজিসলেটিভ ও সংসদ বিষয়ক বিভাগ ;

(ঠ) ইন্সপেক্টর জেনারেল অব পুলিশ, বাংলাদেশ পুলিশ ;

(ড) চেয়ারম্যান, জাতীয় রাজস্ব বোর্ড ;

(ঢ) চেয়ারম্যান, বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন ;

(ণ) মহাপরিচালক, প্রতিরক্ষা গোয়েন্দা মহাপরিদপ্তর ;

(ত) মহাপরিচালক, জাতীয় নিরাপত্তা গোয়েন্দা সংস্থা ;

(থ) মহাপরিচালক, ন্যাশনাল টেলিকমিউনিকেশন মনিটরিং সেন্টার ;

(দ) মহাপরিচালক, জাতীয় সাইবার সুরক্ষা এজেন্সি ;

(ধ) প্রধান বিচারপতি কর্তৃক মনোনীত সুপ্রিমকোর্টের একজন অবসরপ্রাপ্ত বিচারক ;

(ন) চেয়ারম্যান, জাতীয় মানবাধিকার কমিশন ;

(প) সচিব, তথ্য কমিশন ;

(ফ) হেড অব বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট (বিএফআইইউ) ; এবং

(ব) সরকার কর্তৃক মনোনীত তথ্য-প্রযুক্তি বা মানবাধিকার বিষয়ক ২ (দুই) জন বেসরকারি পর্যায়ের বিশেষজ্ঞ।

(২) মহাপরিচালক কাউন্সিলের কার্যসম্পাদনে সাচিবিক সহায়তা প্রদান করিবেন।

১৩। **কাউন্সিলের ক্ষমতা, ইত্যাদি।**— (১) কাউন্সিল, এই আইন 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 হুমকি দেখা দিলে 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) এই আইন 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 (তিন) মাসে অন্তত একবার এবং জরুরি পরিস্থিতিতে যেকোনো সময় উহার চেয়ারম্যান কর্তৃক নির্ধারিত তারিখ, সময় ও স্থানে অনুষ্ঠিত হইবে।

(৩) কাউন্সিল প্রতি ৩ (তিন) মাসে প্রত্যেকটি গুরুত্বপূর্ণ তথ্য পরিকাঠামোসহ দেশের সকল মন্ত্রণালয়, বিভাগ এবং সরকারি-বেসরকারি সংস্থার সাইবার ঝুঁকি নিরীক্ষণ করাইবে এবং এই কাজে কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম সাইবার সিকিউরিটি সফটওয়্যার আউটপুট দ্বারা প্রস্তুতকৃত প্রতিবেদন তৈরিতে সাহায্য ও তত্ত্বাবধান করিবে যাহা কাউন্সিল কর্তৃক মূল্যায়ন করা হইবে।

(৪) কাউন্সিল জনস্বার্থ সংশ্লিষ্ট সিদ্ধান্তসমূহ প্রেস বিজ্ঞপ্তির মাধ্যমে সকলকে অবহিত করিবে এবং সংশ্লিষ্ট মন্ত্রণালয়, বিভাগ, দপ্তর, সংস্থা এবং গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ওয়েবসাইটসমূহের সাইবার সুরক্ষা সংক্রান্ত বিশ্লেষণমূলক প্রতিবেদন প্রকাশ করিবে।

(৫) চেয়ারম্যান কাউন্সিলের সকল সভায় সভাপতিত্ব করিবেন, তবে চেয়ারম্যানের অনুপস্থিতিতে ডাক, টেলিযোগাযোগ ও তথ্য প্রযুক্তি মন্ত্রণালয়ের দায়িত্বপ্রাপ্ত মন্ত্রী কাউন্সিলের সভায় সভাপতিত্ব করিবেন।

(৬) কাউন্সিলের কোনো কার্য বা কার্যধারা কেবল উক্ত কাউন্সিলের কোনো সদস্যপদে 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 আইনের উদ্দেশ্য পূরণকল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা তথ্য পরিকাঠামোকে গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসাবে ঘোষণা করিতে পারিবে এবং প্রত্যেক বৎসর অন্তত একবার গুরুত্বপূর্ণ তথ্য পরিকাঠামোর তালিকা হালনাগাদ করিবে।

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

(২) এই আইনের আওতায় ঘোষিত গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, প্রত্যেক 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, তাহার 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 উদ্দেশ্য পূরণকল্পে, নিরাপত্তা পরিবীক্ষণ, পরিদর্শন ও নিরীক্ষা কার্যক্রম সাইবার সুরক্ষা বিষয়ে বিশেষজ্ঞ ব্যক্তি দ্বারা সম্পন্ন করিতে হইবে।

(৫) গুরুত্বপূর্ণ তথ্য পরিকাঠামো এর সংজ্ঞা ও অন্তর্ভুক্তির শর্তসমূহ সর্বশেষ হালনাগাদকৃত সংশ্লিষ্ট গাইডলাইন অনুসারে নির্ধারিত হইবে।

(৬) বাংলাদেশে বলবৎযোগ্য মান অবকাঠামো মোতাবেক এজেন্সি কর্তৃক স্বীকৃত সংশ্লিষ্ট আন্তর্জাতিক মান নিয়ন্ত্রণ (স্ট্যান্ডার্ডাইজেশন) সংস্থা বা ইন্ডাস্ট্রিয়াল ইন্টারনেট কনসোর্টিয়াম মানের তথ্য ও যোগাযোগ প্রযুক্তি পরীক্ষাগার বা সনদধারি প্রতিষ্ঠান দ্বারা নিরাপত্তা নিরীক্ষা কার্যক্রম সম্পন্ন করা যাইবে।

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 টুলস্ 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 দ্বারা নূতন ডাটা উৎপাদন করেন বা অন্য কোনোভাবে 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 বে-আইনি প্রবেশ (হ্যাকিং) করিয়া তথ্য ভান্ডারের কোনো তথ্য চুরি, বিনাশ, বাতিল, পরিবর্তন বা উহার মূল্য বা উপযোগিতা হ্রাসকরণ, অথবা কৃত্রিম বুদ্ধিমত্তা এজেন্ট এর মাধ্যমে নূতন ডাটা উৎপাদন করেন বা অন্য কোনোভাবে 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) বৎসর 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, বা

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

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

(ঙ) ক্ষতিসাধনের উদ্দেশ্যে ইচ্ছাকৃতভাবে প্রাপক বা গ্রাহকের অনুমতি ব্যতীত অযাচিত ইলেক্ট্রনিক ফিশিং (Phishing) মেইল বা র‍্যানসামওয়্যার মেইল (সাইবার মুক্তিপণ) প্রেরণ করেন, বা

(চ) কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্কে বা সাইবার স্পেসে অন্যায়ভাবে 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 উপ-ধারা (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 দন্ড।**— (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 এবং প্রত্যক্ষ ও পরোক্ষভাবে প্রচার বা বিজ্ঞাপিত করেন তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপ-ধারা (১) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ২ (দুই) বৎসর কারাদণ্ডে, বা অনধিক ১ (এক) কোটি 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 উপ-ধারা (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 উদ্দেশ্য পূরণকল্পে, '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 স্বাক্ষরবিহীন ডিজিটাল ডকুমেন্টস উৎপাদন বা ইলেক্ট্রনিক ফাইল উৎপাদন বা বিদ্যমান ফাইল পরিবর্তন বা ডিজিটাল মানি বা ইলেক্ট্রনিক মুদ্রা বা ক্রিপ্টোকারেন্সি উৎপাদন বা অন্যের জাতীয় পরিচয়পত্রে নিবন্ধিত সিম ব্যবহার করিয়া মোবাইল ব্যাংকিং পরিচালনা, হুন্ডি কার্যে নিযুক্তি কিংবা জুয়ার পোর্টাল পরিচালনা করা।

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 উদ্দেশ্য পূরণকল্পে, '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-কমার্সে 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 করেন 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, বা

(খ) কোনো ডিজিটাল ডিভাইসে এইরূপ উদ্দেশ্যমূলক ক্ষতিকর পরিবর্তন সাধন করেন বা ম্যালওয়্যার প্রবেশ করান যাহার ফলে কোনো ব্যক্তির মৃত্যু ঘটে বা গুরুতর জখমপ্রাপ্ত হন বা হইবার সম্ভাবনা দেখা দেয়, বা

(গ) যদি কোনো ব্যক্তি কম্পিউটার সিস্টেম বা সার্ভার আক্রমণের মাধ্যমে নিত্য প্রয়োজনীয় দ্রব্য বা সেবার সরবরাহ ব্যবস্থায় ব্যাঘাত ঘটান, বা ক্ষতিসাধন করেন, অথবা উক্ত সেবাসমূহের সহায়ক কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্ষতি সাধন করেন, বা ইচ্ছাকৃতভাবে বিরূপ প্রভাব ফেলেন, 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, তবে বৃহত্তর জনস্বার্থে কোনো হুইসেলব্লোয়ার অনুরূপ কাজ করিলে তাহা এই আইনের আওতাভুক্ত হইবে না, বা

(ঙ) প্রতারণা করিবার বা ঠকাইবার উদ্দেশ্যে নিজের পরিচয় গোপন করেন বা অপর কোনো ব্যক্তির পরিচয় ধারণ করেন বা কাহারো জাতীয় পরিচয়পত্র বিকৃত করেন বা অন্য কোনো ব্যক্তির ব্যক্তিগত কোনো তথ্য নিজের বলিয়া প্রদর্শনপূর্বক দফা (ক), (খ), (গ) ও (ঘ) এর অধীন কোনো কার্য সংঘটন করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে সাইবার সন্ত্রাস অপরাধ।

(২) যদি কোনো ব্যক্তি উপ-ধারা (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 উদ্দেশ্য পূরণকল্পে, '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 অশ্লীল বিষয়বস্তু প্রকাশ সংক্রান্ত অপরাধ ও দণ্ড**।— (১) যদি কোনো ব্যক্তি ওয়েবসাইট বা অন্য কোনো ডিজিটাল বা ইলেকট্রনিক মাধ্যমে ইচ্ছাকৃতভাবে বা জ্ঞাতসারে অন্য কোনো ব্যক্তিকে ব্ল্যাকমেইলিং, বা যৌন হয়রানি, বা রিভেঞ্জ পর্ন, বা ডিজিটাল শিশু যৌন নিপীড়ন সংক্রান্ত উপাদান (চাইল্ড সেক্সুয়াল অ্যাবিউজ ম্যাটেরিয়াল) বা সেক্সটর্শন করিবার অভিপ্রায়ে সৃষ্ট, বা প্রাপ্ত, বা সংরক্ষিত কোনো তথ্য, 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 উপ-ধারা (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 উপ-ধারা (১) এর অধীন অপরাধ, কোনো নারী বা অনূর্ধ্ব ১৮ (আঠারো) বৎসরের কোনো শিশুর বিরুদ্ধে সংঘটন করেন, তাহা হইলে তিনি অনধিক ৫ (পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ২০ (বিশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

ব্যাখ্যা।—এই ধারার উদ্দেশ্য পূরণকল্পে, 'ব্ল্যাকমেইলিং' অর্থ এমন হুমকি বা ভীতি প্রদর্শনকে বুঝাইবে, যাহার মাধ্যমে কোনো ব্যক্তি অন্য ব্যক্তিকে তাহার গোপনীয় তথ্য প্রকাশের বা ক্ষতি করিবার ভয় দেখাইয়া বেআইনি সুবিধা, সেবা বা চাহিত কোনো কার্য সম্পাদনে বাধ্য করে।

২৬। **সাইবার স্পেসে ধর্মীয় বা জাতিগত বিষয়ে সহিংসতা, ঘৃণা ও বিদ্বেষমূলক তথ্য প্রকাশ ইত্যাদির অপরাধ ও দণ্ড।**— (১) যদি কোনো ব্যক্তি ইচ্ছাকৃতভাবে বা জ্ঞাতসারে বা ছদ্ম পরিচয়ে নিজের বা অন্যের আইডিতে অবৈধ প্রবেশ করিয়া এমন কোনো কিছু সাইবার স্পেসে প্রকাশ বা প্রচার করেন বা করান, যাহা ধর্মীয় বা সাম্প্রদায়িক ঘৃণামূলক বা জাতিগত বিদ্বেষমূলক বক্তব্য এবং যাহা সহিংসতা তৈরি বা উদ্বেগ সৃষ্টি করে বা বিশৃঙ্খলা বা অপরাধমূলক কর্মকাণ্ডের নির্দেশনা করে, তাহা হইলে অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপ-ধারা (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 আইনের 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 দন্ড।**— (১) যদি কোনো ব্যক্তি অন্য কোনো ব্যক্তির ক্ষতিসাধনের অভিপ্রায়ে উক্ত ব্যক্তির বিরুদ্ধে এই আইনের 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) যদি কোনো ব্যক্তি এই আইনের অধীন একাধিক ধারায় মিথ্যা মামলা বা অভিযোগ দায়ের করেন, তাহা হইলে উক্ত ধারাসমূহে বর্ণিত অপরাধসমূহের মধ্যে মূল অপরাধের জন্য নির্ধারিত দণ্ডের মধ্যে যাহার পরিমাণ বেশি হয় উহাকেই দণ্ডের পরিমাণ হিসাবে নির্ধারণ করা যাইবে।

(৩) ট্রাইব্যুনাল ক্ষতিগ্রস্ত ব্যক্তি বা তদ্‌কর্তৃক ক্ষমতাপ্রাপ্ত ব্যক্তির লিখিত অভিযোগের ভিত্তিতে বা স্বপ্রণোদিত হইয়া এই ধারার অধীন সংঘটিত কোনো অপরাধের অভিযোগ গ্রহণ ও মামলার বিচার করিতে পারিবে।

২৯। **কোম্পানি কর্তৃক অপরাধ সংঘটন**।— (১) কোনো কোম্পানি কর্তৃক এই আইনের 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) উপ-ধারা (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 আইনের 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 প্রদান করিতে পারিবে।

সপ্তম অধ্যায়
অপরাধের তদন্ত ও বিচার

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

(২) উপ-ধারা (১) এ যাহা কিছুই থাকুক না কেন, কোনো মামলার প্রারম্ভে 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 ধারা ২১, ২৫ ও ২৬ এ বর্ণিত অপরাধের অভিযোগে মামলা দায়ের হইলে, মামলা দায়েরের ২৪ (চব্বিশ) ঘণ্টার মধ্যে উক্ত মামলার নথি ও প্রযোজ্য ক্ষেত্রে আটককৃত ব্যক্তিকে সংশ্লিষ্ট আমলী আদালতের ম্যাজিস্ট্রেটের নিকট উপস্থাপন করিতে হইবে।

(৪) উপ-ধারা (৩) এর অধীনে নথি প্রাপ্তির ২৪ (চব্বিশ) ঘণ্টার মধ্যে আমলী ম্যাজিস্ট্রেট উক্ত অপরাধের অভিযোগসহ নথি এবং পারিপার্শ্বিক সকল বিষয় বিবেচনা করিয়া এবং সরাসরি সংক্ষুব্ধ ব্যক্তি কিংবা তাহার 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 প্রযোজ্য ক্ষেত্রে আটক ব্যক্তিকে তাৎক্ষণিক মুক্তির আদেশ প্রদান করিবেন।

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) উপ-ধারা (১) এর অধীন তদন্তকারী অফিসার কোনো তদন্ত কার্য প্রযুক্তিগত সীমাবদ্ধতার কারণে সম্পন্ন করিতে ব্যর্থ হইলে ট্রাইব্যুনাল তদন্তের সময়সীমা, যুক্তিসংগত সময় পর্যন্ত, বৃদ্ধি করিতে পারিবে।

৩৩। **তদন্তকারী অফিসারের ক্ষমতা**।— (১) এই আইনের 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 লওয়া ;

(খ) কোনো ব্যক্তি বা সংস্থার নিকট হইতে তথ্য প্রবাহের তথ্য-উপাত্ত সংগ্রহের লক্ষ্যে প্রয়োজনীয় উদ্যোগ গ্রহণ ; এবং

(গ) এই আইনের উদ্দেশ্য পূরণকল্পে ও মামলা তদন্তের স্বার্থে, প্রয়োজনীয় অন্যান্য কার্য সম্পাদন।

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

(৩) এই আইনের অধীন তদন্ত পরিচালনাকালে তদন্তের স্বার্থে মহাপরিচালক তদ্‌কর্তৃক নিযুক্ত সাইবার সুরক্ষা বিষয়ে আন্তর্জাতিক মানের সনদধারী বিশেষজ্ঞ ব্যক্তিকে তদন্তের আলামত সংগ্রহ অথবা তদন্ত পরিচালনায় তদন্তকারী অফিসারকে সহায়তা প্রদানের জন্য নিযুক্ত করিতে পারিবেন।

(৪) তদন্তকারী অফিসার এই আইনের অধীনে কোনো অপরাধ তদন্তের ক্ষেত্রে জব্দকৃত বা তাহার 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 আইনের অধীন কোনো অপরাধ সংঘটিত হইয়াছে বা সংঘটিত হইবার সম্ভাবনা রহিয়াছে, বা

(খ) এই আইনের অধীন সংঘটিত অপরাধ সংক্রান্ত 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, ক্ষেত্রমত, চিফ জুডিসিয়াল ম্যাজিস্ট্রেট বা চিফ মেট্রোপলিটন ম্যাজিস্ট্রেটের নিকট আবেদনের মাধ্যমে তল্লাশি পরোয়ানা সংগ্রহ করিয়া নিম্নবর্ণিত কার্য সম্পাদন করিতে পারিবেন, যথা :—

(অ) কোনো সেবা প্রদানকারীর দখলে থাকা কোনো তথ্য-প্রবাহের 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 পরোয়ানা ব্যতিরেকে তল্লাশি, জব্দ 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 দুষ্প্রাপ্য হইবার বা করিবার সম্ভাবনা থাকে, তাহা হইলে পুলিশ অফিসার কারণ লিপিবদ্ধ করিয়া, নিম্নবর্ণিত কার্য সম্পাদন করিতে পারিবেন, যথা:—

(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 আইনের অধীন কোনো অপরাধ করিয়াছেন বা করিতেছেন বলিয়া সন্দেহ হইলে উক্ত ব্যক্তিকে গ্রেফতার।

(২) উপ-ধারা (১) এর অধীন তল্লাশি সম্পন্ন করিবার পর পুলিশ অফিসার তল্লাশি পরিচালনার প্রতিবেদন ট্রাইব্যুনালের নিকট অনতিবিলম্বে দাখিল করিবেন।

(৩) উপ-ধারা (১) এর অধীন কোনো ব্যক্তিকে গ্রেফতার করিবার পর পুলিশ অফিসার সংবিধানের ৩৩ অনুচ্ছেদ অনুযায়ী উক্ত ব্যক্তিকে অনতিবিলম্বে বা যাতায়াতের সময় ব্যতীত অনধিক ২৪ (চব্বিশ) ঘন্টার মধ্যে নিকটস্থ ম্যাজিস্ট্রেট বা ট্রাইব্যুনালে হাজির করিবেন।

৩৬। **তথ্য সংরক্ষণ**।—(১) তথ্য-উপাত্ত বিশ্লেষণ সাপেক্ষে, বা তদন্তকারী অফিসারের আবেদনের পরিপ্রেক্ষিতে, যদি মহাপরিচালকের নিকট এইরূপে প্রতীয়মান হয় যে, কম্পিউটার বা কম্পিউটার সিস্টেমে সংরক্ষিত কোনো তথ্য-উপাত্ত এই আইনের অধীন তদন্তের স্বার্থে সংরক্ষণ করা প্রয়োজন এবং এইরূপ তথ্য-উপাত্ত নষ্ট, ধ্বংস, পরিবর্তন অথবা দুষ্প্রাপ্য 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 উহার কোনো অংশ অপরাধ প্রতিরোধ করিবার জন্য বা চলমান অপরাধ রোধ করিবার জন্য জব্দ না করিলে তথ্য-উপাত্ত নষ্ট, ধ্বংস, পরিবর্তন বা দুষ্প্রাপ্য হইবার সম্ভাবনা থাকে।

৩৮। **তদন্তে সহায়তা**।— এই আইনের 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 আইনের অধীন তদন্তের সহিত সংশ্লিষ্ট সকল ব্যক্তি, সত্তা বা সেবা প্রদানকারীর তদন্ত সংশ্লিষ্ট তথ্যাদির গোপনীয়তা রক্ষা করিবেন।

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

(৪) উপ-ধারা (১) এর আওতায় তদন্তের স্বার্থে প্রকাশিত তথ্য বা উপাত্তের তালিকা উক্ত ব্যক্তি, সত্তা বা সেবা প্রদানকারীকে ষাণ্মাষিক ভিত্তিতে জাতীয় সাইবার সুরক্ষা কাউন্সিলে জমা প্রদান করিতে হইবে।

৪০। **মামলা দায়ের ও অপরাধ বিচারার্থ গ্রহণ, ইত্যাদি**।— (১) কোনো সংক্ষুব্ধ ব্যক্তি সরাসরি বা তদ্‌কর্তৃক লিখিতভাবে ক্ষমতাপ্রাপ্ত ব্যক্তি বা আইনশৃংখলা রক্ষাকারী বাহিনীর সদস্য ব্যতীত কেহ এই আইনের অধীন মামলা দায়ের করিতে পারিবে না।

(২) সংক্ষুব্ধ ব্যক্তি সরাসরি বা তদ্‌কর্তৃক লিখিতভাবে 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, তবে ট্রাইব্যুনাল অভিযোগকারীকে পরীক্ষা করিয়া সন্তুষ্ট না হইলে অভিযোগটি সরাসরি নাকচ করিবে।

(৩) ট্রাইব্যুনাল তাহার এখতিয়ারের মধ্যে এই আইনের কোনো অপরাধ সংঘটনের কোনো তথ্য প্রাপ্ত হইলে তাহা অনুসন্ধানের জন্য সংশ্লিষ্ট পুলিশকে নির্দেশ প্রদান করিতে পারিবে এবং পুলিশ প্রতিবেদনের ভিত্তিতে পরবর্তী কার্যক্রম গ্রহণ করিতে পারিবে।

(৪) ফৌজদারি কার্যবিধিতে যাহা কিছুই থাকুক না কেন, পুলিশ অফিসারের বা, ক্ষেত্রমত, যৌথ তদন্ত দলের লিখিত প্রতিবেদন ব্যতীত ট্রাইব্যুনাল কোনো অপরাধ বিচারার্থে গ্রহণ (cognizance) করিবে না।

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

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

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

৪২। **ফৌজদারি কার্যবিধি, Evidence Act ও তথ্য ও যোগাযোগ প্রযুক্তি আইনের প্রয়োগ।**— (১) এই আইনে ভিন্নরূপ কোনো বিধান না থাকিলে, উহার অধীন কার্যক্রম গ্রহণের ক্ষেত্রে ফৌজদারি কার্যবিধি, ১৮৯৮, Evidence Act, 1872 এবং তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ এর বিধানাবলি প্রযোজ্য হইবে।

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

৪৩। **সাক্ষ্যগত মূল্য।**—Evidence Act, 1872 বা অন্য কোনো আইনে ভিন্নতর যাহা কিছুই থাকুক না কেন, এই আইনের অধীন প্রাপ্ত বা সংগৃহীত কোনো ফরেনসিক প্রমাণ বিচার কার্যক্রমে সাক্ষ্য হিসাবে গণ্য হইবে এবং ডিজিটাল ফরেনসিক ল্যাবে প্রস্তুতকৃত ডিজিটাল ফরেনসিক এভিডেন্স সংরক্ষণ বাধ্যতামূলক হইবে।

৪৪। **বিশেষজ্ঞ মতামত গ্রহণ, প্রশিক্ষণ, ইত্যাদি**।— (১) ট্রাইব্যুনাল বা আপীল 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 আইন 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 আইনের অধীন কোনো মামলার অভিযোগ গঠনের তারিখ হইতে ১৮০ (একশত আশি) কার্যদিবসের মধ্যে মামলা নিষ্পত্তি করিবেন।

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

(৩) উপ-ধারা (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**।— (১) এই আইনের ধারা ১৭, ধারা ১৮ এর উপ-ধারা (১) এর দফা (গ), ধারা ১৯, ২০, ২১, ২২, ২৩ ও ২৫ এ উল্লিখিত অপরাধসমূহ আমলযোগ্য এবং অন্যান্য ধারায় বর্ণিত অপরাধসমূহ অ-আমলযোগ্য হইবে।

(২) ধারা ১৭, ধারা ১৮ এর উপ-ধারা (১) এর দফা (গ), ধারা ১৯, ২২ ও ২৩ এ উল্লিখিত অপরাধসমূহ অ-জামিনযোগ্য হইবে এবং ধারা ১৮ এর উপ-ধারা (১) এর দফা (ক) ও (খ), ধারা ২০, ২১, ২৪, ২৫ ও ২৬ এ উল্লিখিত অপরাধসমূহ জামিনযোগ্য হইবে।

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

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

(২) উপ-ধারা (১) এ যাহা কিছুই থাকুক না কেন, যদি ট্রাইব্যুনাল এই মর্মে সন্তুষ্ট হয়, যে সাইবার উপকরণ বা বস্তু সম্পর্কে বা সহযোগে উক্ত অপরাধ সংঘটিত হইয়াছে উহা যে ব্যক্তির দখল বা নিয়ন্ত্রণে পাওয়া গিয়াছে তিনি উক্ত উপকরণ সংশ্লিষ্ট অপরাধ সংঘটনের জন্য দায়ী নহেন, তাহা হইলে উক্ত সাইবার উপকরণ বা বস্তু বাজেয়াপ্তযোগ্য হইবে না।

(৩) উপ-ধারা (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, যদি কোনো অপরাধ সংঘটনের জন্য কোনো সরকারি বা সংবিধিবদ্ধ সংস্থার সাইবার উপকরণ বা যন্ত্রপাতি ব্যবহার করা হয়, তাহা হইলে উহা বাজেয়াপ্তযোগ্য হইবে না।

ব্যাখ্যা।——"সাইবার উপকরণ" অর্থে কম্পিউটার, কম্পিউটার সিস্টেম এবং ফ্লপি ডিস্ক, কমপ্যাক্ট ডিস্ক, টেপ ড্রাইভ বা অন্য কোনো আনুষঙ্গিক কম্পিউটার উপকরণও উহার অন্তর্ভুক্ত হইবে।

অষ্টম অধ্যায়
আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা

৪৮। **আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা**।— (১) এই আইনের অধীন সংঘটিত কোনো অপরাধের তদন্ত ও বিচারের ক্ষেত্রে, আঞ্চলিক ও আন্তর্জাতিক সহযোগিতা প্রয়োজন হইলে, অপরাধ সম্পর্কিত বিষয়ে পারস্পরিক সহায়তা আইন, ২০১২ (২০১২ সনের ৪ নং আইন) এর বিধানাবলি প্রযোজ্য হইবে।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ আঞ্চলিক ও আন্তর্জাতিক সাইবার নিরাপত্তা সংশ্লিষ্ট বিষয়ে জড়িত হইলে প্রতিরোধমূলক, তত্ত্বাবধানমূলক এবং সমাধানমূলক কার্যক্রম গ্রহণ ও তদারকির জন্য জাতীয় সাইবার সুরক্ষা এজেন্সি উপযুক্ত কর্তৃপক্ষ হিসাবে বিবেচিত হইবে।

(৩) জাতীয় ও আন্তর্জাতিক উভয় ক্ষেত্রে সাইবার সংক্রান্ত যেকোনো বিষয়ে যোগাযোগ, সমাধান কিংবা মধ্যস্থতার জন্য প্রতিটি গুরুত্বপূর্ণ তথ্য পরিকাঠামো ফোকাল পয়েন্ট হিসাবে বিকল্পসহ একজন প্রতিনিধি মনোনীত করিবে এবং উক্ত ফোকাল পয়েন্ট জাতীয় সাইবার সুরক্ষা এজেন্সির মাধ্যমে জাতীয় এবং আন্তর্জাতিক পর্যায়ে আন্তঃখাত সহযোগিতা নিশ্চিত করিবে, জাতীয় সাইবার সুরক্ষা এজেন্সি সকল ফোকাল পয়েন্টগণের যোগাযোগের মাধ্যমসহ একটি তালিকা অনলাইনে প্রকাশ করিবে।

(৪) এজেন্সি প্রত্যেকটি গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কার্যাবলির যেকোনো পরিবর্তনের বিষয়ে সংশ্লিষ্ট ফোকাল পয়েন্টকে দ্রুত অবহিত করিবে।

নবম অধ্যায়

বিবিধ

৪৯। **বিধি প্রণয়নের ক্ষমতা।**—(১) এই আইনের উদ্দেশ্য পূরণকল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, প্রয়োজনীয় সংখ্যক বিধি প্রণয়ন করিতে পারিবে।

(২) উপ-ধারা (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 সহিত সমন্বয়সাধন ;

(জ) ক্লাউড কম্পিউটিং বা মেটাডাটা সম্পর্কিত ডিজিটাল ফরেনসিক সংক্রান্ত বিষয়াদি ; এবং

(ঝ) গ্লোবাল থ্রেট ইন্টেলিজেন্স এ দ্বিপাক্ষিক তথ্য ও লগ আদান-প্রদান।

৫০। **২০২৩ সনের ৩৯ নং আইনের রহিতকরণ ও হেফাজত।**—(১) সাইবার নিরাপত্তা আইন, ২০২৩ (২০২৩ সনের ৩৯ নং আইন), অতঃপর উক্ত আইন বলিয়া উল্লিখিত, এতদ্দ্বারা রহিত করা হইল।

(২) উক্তরূপ রহিতকরণের অব্যবহিত পূর্বে উক্ত আইনের ধারা ১৭, ১৮, ১৯, ২০, ২২, ২৩, ৩০, ৩২, ৩৫ এবং উক্ত ধারাসমূহে বর্ণিত অপরাধ সংঘটনে সহায়তার অপরাধের অনিষ্পন্ন মামলাসমূহ সংশ্লিষ্ট ট্রাইব্যুনালে এবং অনুরূপ মামলায় প্রদত্ত আদেশ, রায় বা দণ্ডের বিরুদ্ধে আপিল সংশ্লিষ্ট আপিল ট্রাইব্যুনালে এইরূপে পরিচালিত ও নিষ্পত্তি হইবে যেন উক্ত আইন রহিত হয় নাই।

(৩) উপ-ধারা (২) এ উল্লিখিত উক্ত আইনের ধারাসমূহের অধীন যে সকল মামলার রিপোর্ট বা অভিযোগ করা হইয়াছে বা তৎপরিপ্রেক্ষিতে চার্জশিট দাখিল করা হইয়াছে বা মামলা তদন্তাধীন রহিয়াছে, সেই সকল মামলা সংশ্লিষ্ট ট্রাইব্যুনালে বিচারাধীন মামলা বলিয়া গণ্য হইবে।

(৪) উক্ত আইন রহিত হইবার সঙ্গে সঙ্গে, উক্তরূপ রহিতকরণের অব্যবহিত পূর্বে, উক্ত আইনের ধারা ২১, ২৪, ২৫, ২৬, ২৭, ২৮, ২৯, ৩১, ৩৪ এবং উক্ত ধারাসমূহে বর্ণিত অপরাধ সংঘটনে সহায়তার অপরাধে কোনো আদালত বা ট্রাইব্যুনালে নিষ্পন্নাধীন কোনো মামলা বা অন্যান্য কার্যধারা অথবা কোনো পুলিশ অফিসার বা অন্য কোনো কর্তৃপক্ষের নিকট তদন্তাধীন মামলা বা কার্যক্রম বাতিল হইবে এবং উহাদের বিষয়ে আর কোনো কার্যক্রম গ্রহণ করা যাইবে না এবং উক্ত ধারাসমূহের অধীন কোনো আদালত বা ট্রাইব্যুনাল কর্তৃক প্রদত্ত দণ্ড ও জরিমানা বাতিল বলিয়া গণ্য হইবে।

(৫) উক্ত আইন দ্বারা রহিতকৃত ডিজিটাল নিরাপত্তা আইন, ২০১৮ (২০১৮ সনের ৪৬ নং আইন) এর ২১, ২৪, ২৫, ২৬, ২৭, ২৮, ২৯, ৩১ ধারাসমূহে বর্ণিত অপরাধ সংঘটন ও সহায়তার অপরাধে কোনো আদালত বা ট্রাইব্যুনালে নিষ্পন্নাধীন কোনো মামলা বা অন্যান্য কার্যধারা অথবা কোনো পুলিশ অফিসার বা অন্য কোনো কর্তৃপক্ষের নিকট তদন্তাধীন মামলা বা কার্যক্রম বাতিল হইবে এবং উহাদের বিষয়ে আর কোনো কার্যক্রম গ্রহণ করা যাইবে না এবং উক্ত ধারাসমূহের অধীন কোনো আদালত বা ট্রাইব্যুনাল কর্তৃক প্রদত্ত দণ্ড ও জরিমানা বাতিল বলিয়া গণ্য হইবে।

(৬) উপ-ধারা (১) এর অধীন রহিতকরণ সত্ত্বেও, উক্ত আইন ও অধ্যাদেশের অধীন—

(ক) গঠিত সাইবার নিরাপত্তা এজেন্সির সকল স্থাবর ও অস্থাবর সম্পত্তি, দলিল-দস্তাবেজ ও দায়-দেনা, যদি থাকে, জাতীয় সাইবার সুরক্ষা এজেন্সির নিকট ন্যস্ত হইবে ;

(খ) প্রণীত বিধিমালা, জারীকৃত আদেশ, নির্দেশ, প্রজ্ঞাপন বা গাইডলাইন বা কৃত, সূচিত বা গৃহীত কোনো ব্যবস্থা এই আইনের বিধানাবলির সহিত সামঞ্জস্যপূর্ণ হওয়া সাপেক্ষে, এই আইনের অধীন রহিত না হওয়া পর্যন্ত, বলবৎ থাকিবে, এবং উহা এই আইনের অধীন প্রণীত, জারীকৃত, কৃত, সূচিত বা গৃহীত হইয়াছে বলিয়া গণ্য হইবে ;

(গ) সাইবার সুরক্ষা এজেন্সির মহাপরিচালক এবং পরিচালকগণসহ সকল কর্মকর্তা-কর্মচারী জাতীয় সাইবার সুরক্ষা এজেন্সির মহাপরিচালক, পরিচালক এবং কর্মকর্তা-কর্মচারী হিসাবে গণ্য হইবেন, এবং তাহারা যে শর্তে জাতীয় সাইবার সুরক্ষা এজেন্সিতে নিয়োগকৃত বা কর্মরত ছিলেন সেই একই শর্তে জাতীয় সাইবার সুরক্ষা এজেন্সিতে নিয়োগকৃত বা কর্মরত রহিয়াছেন বলিয়া গণ্য হইবেন ;

(ঘ) গঠিত জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এবং কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এই আইনের অধীন গঠিত জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এবং কম্পিউটার ইমার্জেন্সি রেসপন্স টিম বলিয়া গণ্য হইবে ;

(ঙ) স্থাপিত ডিজিটাল ফরেনসিক ল্যাব এই আইনের অধীন স্থাপিত ডিজিটাল ফরেনসিক ল্যাব বলিয়া গণ্য হইবে ;

(চ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো বলিয়া ঘোষিত কম্পিউটার সিস্টেম, নেটওয়ার্ক বা তথ্য পরিকাঠামো এই আইনের অধীন ঘোষিত গুরুত্বপূর্ণ তথ্য পরিকাঠামো বলিয়া গণ্য হইবে।

(ছ) উক্ত অধ্যাদেশ এর অধীন কৃত কোন কার্য বা গৃহীত কোন ব্যবস্থা এই আইনের অধীন কৃত বা গৃহীত হইয়াছে বলিয়া গণ্য হইবে।

৫১। **রহিতকরণ ও হেফাজত**।—(১) সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫ (২০২৫ সনের ২৫ নং অধ্যাদেশ) এবং সাইবার সুরক্ষা (সংশোধন) অধ্যাদেশ, ২০২৫ (২০২৫ সনের ৫৪ নং অধ্যাদেশ) অতঃপর উক্ত অধ্যাদেশসমূহ বলিয়া উল্লিখিত, এতদ্দ্বারা রহিত করা হইল।

(২) উপ-ধারা (১) এর অধীন রহিতকরণ সত্ত্বেও, উক্ত অধ্যাদেশসমূহের অধীন কৃত কোনো কার্য, গৃহীত কোনো ব্যবস্থা বা সূচিত কোনো কার্যধারা এই আইনের অধীন কৃত, গৃহীত বা সূচিত হইয়াছে বলিয়া গণ্য হইবে।

৫২। **ইংরেজিতে অনূদিত পাঠ প্রকাশ**।—(১) এই আইন প্রবর্তনের পর সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের ইংরেজিতে অনূদিত একটি নির্ভরযোগ্য পাঠ (Authentic English Text) প্রকাশ করিতে পারিবে।

(২) এই আইন ও ইংরেজি পাঠের মধ্যে বিরোধের ক্ষেত্রে এই আইন প্রাধান্য পাইবে।

ব্যারিস্টার মোঃ গোলাম সরওয়ার ভূঁইয়া
সচিব।

মোহাম্মদ আবু ইউসুফ, উপপরিচালক (উপসচিব), বাংলাদেশ সরকারী মুদ্রণালয়, তেজগাঁও, ঢাকা কর্তৃক মুদ্রিত।
মোঃ নজরুল ইসলাম, উপপরিচালক (উপসচিব), বাংলাদেশ ফরম ও প্রকাশনা অফিস, তেজগাঁও,
ঢাকা কর্তৃক প্রকাশিত। website: www.bgpress.gov.bd