জাতীয় বিশ্ববিদ্যালয়ের সিলেবাসভুক্ত আইসিটি বিষয়ক অনলাইন কোর্স
রিডিং ম্যাটেরিয়াল

অনলাইন ইথিক্স, ডিজিটাল ওয়েলবিং ও সাইবার সুরক্ষা

প্রযুক্তিনির্ভর এই যুগে ইন্টারনেট আমাদের দৈনন্দিন জীবনের অবিচ্ছেদ্য অংশ। তবে এই ডিজিটাল জগতকে নিরাপদ ও উপভোগ্য করে তুলতে হলে আমাদের অনলাইন আচরণবিধি (Ethics), শারীরিক ও মানসিক সুস্থতা (Wellbeing) এবং নিরাপত্তা (Security) সম্পর্কে বিস্তারিত জ্ঞান থাকা জরুরি।

১. অনলাইন ইথিক্স (Online Ethics): ডিজিটাল শিষ্টাচার

অনলাইন ইথিক্স হলো ইন্টারনেট ব্যবহারের সময় শালীনতা, সততা, সহানুভূতি এবং দায়িত্বশীল আচরণের একটি নৈতিক নীতিমালা। বাস্তব জীবনে আমরা যেমন শিষ্টাচার মেনে চলি, ডিজিটাল জগতেও ঠিক তেমনি আচরণের প্রয়োজন।

- **একজন আদর্শ ব্যবহারকারীর উদাহরণ:** ভিডিওতে আমরা 'রিমি'র ঘটনা দেখেছি। রিমি সোশ্যাল মিডিয়ায় ভদ্র ভাষায় কথা বলে, অন্যের মতামতকে সম্মান জানায় এবং কোনো তথ্য শেয়ার করার আগে তা সত্য কি না যাচাই করে নেয় । ফলে অনলাইনে সবাই তাকে বিশ্বাস করে। রিমির এই আচরণ প্রমাণ করে যে, অনলাইনে দায়িত্বশীল হলে ডিজিটাল জগত নিরাপদ ও সুন্দর হয়ে ওঠে ।
- **অনলাইন ইথিক্স মেনে চলার সুফল:**
    - ভুয়া তথ্য ও গুজব ছড়ানো কমে যায় ।
    - সাইবার বুলিং বা অনলাইনে হয়রানি রোধ করা সম্ভব হয় ।
    - ডিজিটাল পরিবেশ নিরাপদ হয় এবং ব্যবহারকারীদের মধ্যে পারস্পরিক সম্মান বৃদ্ধি পায় ।

২. ডিজিটাল ওয়েলবিং (Digital Wellbeing): প্রযুক্তির সুস্থ ব্যবহার

প্রযুক্তি ব্যবহারের মাধ্যমে নিজের শারীরিক, মানসিক ও সামাজিক সুস্থতা বজায় রাখাকেই 'ডিজিটাল ওয়েলবিং' বলা হয় । প্রযুক্তির অতিরিক্ত আসক্তি আমাদের জীবনের ভারসাম্য নষ্ট করতে পারে।

- **প্রযুক্তির অতিরিক্ত ব্যবহারের নেতিবাচক প্রভাব:** দীর্ঘক্ষণ স্ক্রিনের দিকে তাকিয়ে থাকা বা অতিরিক্ত ইন্টারনেট ব্যবহারের ফলে চোখে চাপ ও মাথাব্যথা হতে পারে । এছাড়া ঘুমের সমস্যা, মানসিক চাপ, একাকীত্ব তৈরি হওয়া এবং পড়াশোনা বা কাজে মনোযোগ কমে যাওয়ার মতো সমস্যা দেখা দেয় ।
- **ডিজিটাল ওয়েলবিং বজায় রাখার উপায়:**
    - স্ক্রিন টাইম নিয়ন্ত্রণ: সারাদিনে নির্দিষ্ট সময়ের বেশি ডিভাইস ব্যবহার করা থেকে বিরত থাকুন ।
    - ঘুমের আগে বিরতি: ঘুমের আগে মোবাইল ফোন ব্যবহার বন্ধ রাখুন ।
    - সামাজিক যোগাযোগ: ভার্চুয়াল জগতের বাইরে পরিবার ও বন্ধুদের সরাসরি সময় দিন ।
    - ভারসাম্য: অনলাইন এবং অফলাইন জীবনের মধ্যে একটি সঠিক ভারসাম্য বজায় রাখুন ।

৩. সাইবার সুরক্ষা (Cyber Security): নিজেকে নিরাপদ রাখার কৌশল

অনলাইনে ব্যক্তিগত তথ্য, ডিভাইস ও অ্যাকাউন্টকে ভাইরাস, হ্যাকিং ও প্রতারণা থেকে রক্ষা করাই হলো সাইবার সুরক্ষা । বিভিন্ন ধরনের সাইবার হুমকি থেকে বাঁচতে নিচের নির্দেশনাগুলো মেনে চলা জরুরি:

ক. সাধারণ নিরাপত্তা অভ্যাস

নিরাপত্তার প্রথম ধাপ হলো নিজের অ্যাকাউন্ট ও ডিভাইস সুরক্ষিত রাখা।

- শক্তিশালী পাসওয়ার্ড: পাসওয়ার্ড তৈরির সময় অক্ষর, সংখ্যা এবং বিশেষ চিহ্নের (যেমন: @, #, $) সংমিশ্রণ ব্যবহার করুন ।
- টু-ফ্যাক্টর অথেনটিকেশন (২FA): সব ধরনের অ্যাকাউন্টে ২FA চালু রাখুন, যাতে পাসওয়ার্ড জানলেও অন্য কেউ প্রবেশ করতে না পারে ।
- আপডেট ও সুরক্ষা: অপারেটিং সিস্টেম ও অ্যাপ নিয়মিত আপডেট রাখুন এবং বিশ্বস্ত অ্যান্টিভাইরাস ও ফায়ারওয়াল ব্যবহার করুন ।
- ব্যাকআপ: গুরুত্বপূর্ণ ফাইল বা ডেটার নিয়মিত ব্যাকআপ রাখুন ।

খ. ম্যালওয়্যার ও ভাইরাস থেকে সুরক্ষা (Malware/Virus/Trojan)

ক্ষতিকর সফটওয়্যার থেকে বাঁচতে সতর্ক থাকা প্রয়োজন।

- অজানা বা সন্দেহজনক সফটওয়্যার ও অ্যাপ ইনস্টল করা থেকে বিরত থাকুন ।
- সফটওয়্যার ডাউনলোডের সময় শুধুমাত্র অনুমোদিত সোর্স (Authorized Source) ব্যবহার করুন ।
- ফ্রি সফটওয়্যার ডাউনলোডের সময় সতর্ক থাকুন এবং পাইরেটেড সফটওয়্যার ব্যবহার এড়িয়ে চলুন ।
- পেনড্রাইভ বা এক্সটারনাল ডিভাইস কম্পিউটারে যুক্ত করার আগে অবশ্যই স্ক্যান করে নিন ।

গ. ফিশিং ও সোশ্যাল ইঞ্জিনিয়ারিং প্রতিরোধ (Phishing & Social Engineering)

হ্যাকাররা অনেক সময় মানুষের বিশ্বাসকে পুঁজি করে তথ্য হাতিয়ে নেয়।

- গোপনীয়তা রক্ষা: ফোন, ইমেইল বা মেসেজে কাউকে ওটিপি (OTP), পিন (PIN) বা পাসওয়ার্ড দেবেন না ।
- ভয়ভীতি যাচাই: “জরুরি ব্যবস্থা নিন” বা “অ্যাকাউন্ট বন্ধ হয়ে যাবে”—এমন মেসেজ দেখে আতঙ্কিত হয়ে হুট করে বিশ্বাস করবেন না ।
- পরিচয় নিশ্চিতকরণ: ফোনে কেউ ব্যক্তিগত তথ্য চাইলে আগে তার পরিচয় নিশ্চিত হোন এবং ইমেইল আসলে প্রেরকের ঠিকানা ও লিংক ভালোভাবে যাচাই করুন ।

ঘ. র‍্যানসমওয়্যার, স্পাইওয়্যার ও অন্যান্য হুমকি থেকে সুরক্ষা

- র‍্যানসমওয়্যার (Ransomware): নিয়মিত গুরুত্বপূর্ণ ফাইলের অফলাইন ব্যাকআপ রাখুন। সন্দেহজনক ইমেইল অ্যাটাচমেন্ট খোলা বা অজানা লিংকে ক্লিক করা এড়িয়ে চলুন ।
- স্পাইওয়্যার ও কি-লগার (Spyware/Keylogger): অজানা অ্যাপ বা ব্রাউজার এক্সটেনশন ইনস্টল করবেন না। পাবলিক কম্পিউটার (যেমন সাইবার ক্যাফে বা লাইব্রেরি) ব্যবহার করে ব্যক্তিগত অ্যাকাউন্টে লগইন করা থেকে বিরত থাকুন এবং নিয়মিত নিজের ডিভাইস স্ক্যান করুন ।
- অ্যাডওয়্যার (Adware): কোনো সফটওয়্যার ইনস্টল করার সময় ‘Custom’ বা ‘Advanced’ অপশন বেছে নিন এবং অপ্রয়োজনীয় টুলবারগুলো আনচেক বা রিমুভ করুন ।

সাইবার অপরাধ থেকে বাঁচার সবচেয়ে বড় হাতিয়ার হলো ‘সচেতনতা’ । আমরা যদি অনলাইন ইথিক্স মেনে চলি, ডিজিটাল ওয়েলবিং নিশ্চিত করি এবং নিজের সাইবার সুরক্ষা নিয়ে সতর্ক থাকি, তবেই ডিজিটাল জগত আমাদের জন্য নিরাপদ ও কল্যাণকর হয়ে উঠবে ।

এছাড়া ডিজিটাল যুগে নিজেকে সুরক্ষিত রাখতে প্রতিটি নাগরিকের 'সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫' এবং 'ব্যক্তিগত উপাত্ত সুরক্ষা অধ্যাদেশ, ২০২৫' সম্পর্কে জানা অত্যন্ত জরুরি। নিচে আপনার জন্য এই দুটি গুরুত্বপূর্ণ অধ্যাদেশের একটি সংক্ষিপ্ত সারসংক্ষেপ তুলে ধরা হলো:

সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫

সাইবার স্পেস বা ইন্টারনেট বর্তমান জীবনের অবিচ্ছেদ্য অংশ। তবে এর অপব্যবহার ব্যক্তিগত জীবন, সমাজ এবং রাষ্ট্রের জন্য বড় হুমকি হতে পারে। **সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫**-এর মূল লক্ষ্য হলো সাইবার স্পেসে সংঘটিত অপরাধ শনাক্তকরণ, প্রতিরোধ ও দমন এবং সাইবার সুরক্ষা নিশ্চিত করা । একজন সচেতন নাগরিক হিসেবে ডিজিটাল মাধ্যমে নিরাপদ থাকতে এবং আইনি জটিলতা এড়াতে এই অধ্যাদেশের বিধানগুলো সম্পর্কে বিস্তারিত জানা অপরিহার্য।

১. সাইবার অপরাধ ও নিষিদ্ধ কর্মকাণ্ডসমূহ

এই অধ্যাদেশে বেশ কিছু ডিজিটাল কর্মকাণ্ডকে সুনির্দিষ্টভাবে অপরাধ হিসেবে চিহ্নিত করা হয়েছে। ডিজিটাল স্পেস ব্যবহারের সময় নিম্নোক্ত বিষয়গুলো থেকে বিরত থাকা বাধ্যতামূলক:

- **বেআইনি প্রবেশ বা হ্যাকিং (Illegal Access & Hacking):** কোনো ব্যক্তি বা কর্তৃপক্ষের অনুমতি ছাড়া কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার নেটওয়ার্ক বা সার্ভারে প্রবেশ করাকে 'বে-আইনি প্রবেশ' বলা হয় । বেআইনিভাবে প্রবেশ করে তথ্য চুরি, বিনাশ, পরিবর্তন বা ক্ষতিসাধন করাকে 'হ্যাকিং' হিসেবে গণ্য করা হয়, যার জন্য কারাদণ্ড ও অর্থদণ্ডের বিধান রয়েছে । এমনকি অপরাধ সংঘটনের উদ্দেশ্যে অনুমতি ছাড়া অন্যের ডিভাইসে প্রবেশে সহায়তা করাও দণ্ডনীয় অপরাধ ।
- **ডিজিটাল মাধ্যমে যৌন হয়রানি ও ব্যক্তিগত গোপনীয়তা লঙ্ঘন:**
    - **অনলাইন হয়রানি ও অশালীন আচরণ:** ডিজিটাল মাধ্যমে কাউকে বারবার অশালীন প্রস্তাব দেওয়া, বিরক্ত করা বা প্রযুক্তির সাহায্যে অনুমতি ছাড়া কারো ছবি বিকৃত করা দণ্ডনীয় অপরাধ ।
    - **ব্যক্তিগত ছবির অপব্যবহার:** কারো ক্ষতি করার উদ্দেশ্যে অনুমতি ছাড়া তার একান্ত ব্যক্তিগত মুহূর্তের ছবি বা ভিডিও ইন্টারনেটে ছড়িয়ে দেওয়া একটি গুরুতর অপরাধ ।
    - ব্ল্যাকমেইলিং ও ভীতি প্রদর্শন: কারো গোপন ছবি বা ভিডিও সংরক্ষণের দাবি করে বা তা প্রকাশের হুমকি দিয়ে অর্থ বা অনৈতিক সুবিধা আদায়ের চেষ্টা করা বা চাপ প্রয়োগ করা কঠোর শাস্তিযোগ্য অপরাধ ।
- **সাইবার বুলিং ও ভীতি প্রদর্শন:** ডিজিটাল মাধ্যমে ইচ্ছাকৃতভাবে কাউকে ব্ল্যাকমেইলিং করা বা ভীতি প্রদর্শন করা অপরাধ। ব্ল্যাকমেইলিং বলতে গোপনীয় তথ্য প্রকাশের ভয় দেখিয়ে কোনো সুবিধা আদায় বা কোনো কাজে বাধ্য করাকে বোঝায় ।
- **ধর্মীয় ও জাতিগত বিদ্বেষমূলক প্রচার:** ইচ্ছাকৃতভাবে ডিজিটাল মাধ্যমে এমন কোনো বক্তব্য বা তথ্য প্রকাশ করা যা ধর্মীয় বা সাম্প্রদায়িক ঘৃণা ছড়ায় অথবা জাতিগত বিদ্বেষ ও সহিংসতা সৃষ্টি করে, তা শাস্তিযোগ্য অপরাধ ।
- **ক্ষতিকর সফটওয়্যার ও ফিশিং (Malware & Phishing):** কোনো কম্পিউটার বা নেটওয়ার্কের ক্ষতি করার উদ্দেশ্যে ম্যালওয়্যার, ভাইরাস বা ক্ষতিকর সফটওয়্যার প্রবেশ করানো অপরাধ । কারো অনুমতি ছাড়া অযাচিত 'ফিশিং' (Phishing) মেইল পাঠানো বা র‍্যানসমওয়্যার (Ransomware) বা সাইবার মুক্তিপণ দাবি করা দণ্ডনীয়।
- **অনলাইন জুয়া (Online Gambling):** সাইবার স্পেস ব্যবহার করে জুয়া খেলার পোর্টাল বা অ্যাপ তৈরি, পরিচালনা, এতে অংশগ্রহণ বা এর প্রচার ও বিজ্ঞাপনে অংশ নেওয়া সম্পূর্ণ নিষিদ্ধ।

২. কৃত্রিম বুদ্ধিমত্তা (AI) ও আধুনিক প্রযুক্তির অপব্যবহার

নতুন অধ্যাদেশে কৃত্রিম বুদ্ধিমত্তার অপব্যবহার রোধে বিশেষ গুরুত্ব দেওয়া হয়েছে:

- **এআই হ্যাকিং:** কৃত্রিম বুদ্ধিমত্তা সফটওয়্যার এজেন্ট বা টুলের মাধ্যমে কোনো সিস্টেমে বেআইনি প্রবেশ বা নতুন ডাটা উৎপাদন করে ক্ষতিসাধন করা অপরাধ হিসেবে গণ্য হবে ।
- **ডিপফেক ও বিকৃতি:** কৃত্রিম বুদ্ধিমত্তা ব্যবহার করে কারো ছবি বা ভিডিও বিকৃত করা বা এডিট করে সম্মানহানি বা যৌন হয়রানি করা কঠোর শাস্তিযোগ্য অপরাধ ।

৩. গুরুত্বপূর্ণ তথ্য পরিকাঠামো (CII) সুরক্ষা

রাষ্ট্রের গুরুত্বপূর্ণ ডিজিটাল সেবা বা অবকাঠামোর সুরক্ষায় বিশেষ সতর্কতা প্রয়োজন:

- সরকার ঘোষিত 'গুরুত্বপূর্ণ তথ্য পরিকাঠামো' (যেমন- ব্যাংক, বিদ্যুৎ, টেলিযোগাযোগ নেটওয়ার্ক)-এর ক্ষতিসাধন বা এতে বেআইনি প্রবেশ সাধারণ হ্যাকিংয়ের চেয়েও গুরুতর অপরাধ ।
- নিত্যপ্রয়োজনীয় দ্রব্য বা সেবা সরবরাহ ব্যবস্থায় ব্যাঘাত ঘটানোর উদ্দেশ্যে সাইবার আক্রমণকে 'সাইবার সন্ত্রাস' হিসেবে গণ্য করা হবে, যার শাস্তি অত্যন্ত কঠোর ।

৪. ভুক্তভোগীদের জন্য আইনি প্রতিকার ও সুরক্ষা

সাইবার অপরাধের শিকার হলে ভুক্তভোগীদের সুরক্ষায় আইনে নিম্নোক্ত ব্যবস্থা রাখা হয়েছে:

- **ক্ষতিকর তথ্য অপসারণ (Content Removal):** যদি ডিজিটাল মাধ্যমে প্রকাশিত কোনো তথ্য সাইবার সুরক্ষার জন্য হুমকি হয় বা হয়রানিমূলক হয়, তবে জাতীয় সাইবার সুরক্ষা এজেন্সির মহাপরিচালক তা অপসারণ বা ব্লক করার ব্যবস্থা নিতে পারেন । আইনশৃঙ্খলা রক্ষাকারী বাহিনীও জননিরাপত্তা বা সাম্প্রদায়িক সম্প্রীতি রক্ষার স্বার্থে আপত্তিকর কন্টেন্ট অপসারণের উদ্যোগ নিতে পারে ।
- **ক্ষতিপূরণ প্রাপ্তি:** সাইবার অপরাধের কারণে কেউ ক্ষতিগ্রস্ত হলে ট্রাইব্যুনাল অপরাধীর কাছ থেকে জরিমানা আদায় করে ক্ষতিগ্রস্ত ব্যক্তিকে ক্ষতিপূরণ প্রদানের আদেশ দিতে পারে ।
- **অভিযোগ দায়ের ও তদন্ত:** সংক্ষুব্ধ ব্যক্তি বা ভুক্তভোগী ট্রাইব্যুনালে মামলা দায়ের করতে পারেন । সুষ্ঠু তদন্তের জন্য পুলিশ বা এজেন্সির সমন্বয়ে যৌথ তদন্ত দল গঠনের সুযোগ রয়েছে । তদন্তকারী অফিসার তদন্তের স্বার্থে ৯০ দিন পর্যন্ত তথ্য সংরক্ষণের নির্দেশ দিতে পারেন ।
- **কারিগরি সহায়তা:** সাইবার আক্রমণ বা ইনসিডেন্ট মোকাবিলার জন্য 'জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম' (CERT) কাজ করবে । এরা সাইবার হুমকি বিশ্লেষণ এবং ডিজিটাল ফরেনসিক সহায়তায় ভূমিকা পালন করে ।

৫. ডিজিটাল সচেতনতা ও দায়িত্বশীলতা

এই অধ্যাদেশের আওতায় মিথ্যা অভিযোগ দায়ের করাও একটি অপরাধ। অন্য কোনো ব্যক্তির ক্ষতি করার উদ্দেশ্যে মিথ্যা মামলা করলে অভিযোগকারীকেও একই দণ্ডে দণ্ডিত হতে হবে । তাই ডিজিটাল স্পেসে সততা বজায় রাখা এবং প্রমাণের ভিত্তিতে অভিযোগ করা জরুরি।

সুতরাং, সাইবার স্পেসে নিরাপদ থাকার জন্য অনুমতি ছাড়া অন্যের তথ্যে প্রবেশ না করা, অশ্লীলতা ও ঘৃণা ছড়ানো থেকে বিরত থাকা এবং সন্দেহজনক লিংকে ক্লিক না করা অত্যন্ত জরুরি। আইনটি শুধুমাত্র শাস্তি দেওয়ার জন্য নয়, বরং ডিজিটাল জগতকে সকলের জন্য নিরাপদ রাখার উদ্দেশ্যে প্রণীত হয়েছে।

সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫ এর লিংক: http://bdlaws.minlaw.gov.bd/act-1538.html

ব্যক্তিগত উপাত্ত সুরক্ষা অধ্যাদেশ, ২০২৫

বর্তমান ডিজিটাল যুগে মানুষের নাম, পরিচয়, আর্থিক তথ্য বা স্বাস্থ্যগত তথ্য অত্যন্ত মূল্যবান সম্পদ। নতুন এই অধ্যাদেশ অনুযায়ী, একজন ব্যক্তির ব্যক্তিগত উপাত্ত বা তথ্যের মালিক তিনি নিজেই এবং এই তথ্য সুরক্ষিত রাখা একটি আইনি অধিকার। ডিজিটাল সেবা ব্যবহারের সময় নিজের তথ্য সুরক্ষায় নিম্নোক্ত বিষয়গুলো সম্পর্কে স্বচ্ছ ধারণা থাকা আবশ্যক:

১. ব্যক্তিগত উপাত্ত কী এবং এর মালিকানা

- **ব্যক্তিগত উপাত্ত (Personal Data):** কোনো ব্যক্তির নাম, মোবাইল নম্বর, আর্থিক তথ্য, অবস্থান (Location), বায়োমেট্রিক তথ্য বা এমন কোনো তথ্য যা দিয়ে তাকে শনাক্ত করা যায়, তা 'ব্যক্তিগত উপাত্ত' হিসেবে গণ্য হয় ।

- **সংবেদনশীল উপাত্ত (Sensitive Data):** ডিএনএ, আঙুলের ছাপ (Biometric), পাসওয়ার্ড, স্বাস্থ্যগত তথ্য, ধর্মীয় বিশ্বাস, রাজনৈতিক মতাদর্শ বা ব্যাংক অ্যাকাউন্টের তথ্য 'সংবেদনশীল ব্যক্তিগত উপাত্ত' হিসেবে বিবেচিত হয়, যার সুরক্ষায় আইন অত্যন্ত কঠোর।
- **মালিকানা:** কোনো ব্যক্তির ব্যক্তিগত উপাত্তকে তার নিজস্ব মালিকানাধীন সম্পদ হিসেবে গণ্য করা হয়।

২. সম্মতি প্রদান ও তথ্য সংগ্রহ (Consent)

কোনো প্রতিষ্ঠান বা অ্যাপ চাইলেই ব্যবহারকারীর তথ্য নিতে পারবে না। তথ্য সংগ্রহের ক্ষেত্রে কঠোর নিয়ম রয়েছে:

- **সুস্পষ্ট সম্মতি:** সেবা প্রদানকারী বা 'উপাত্ত-জিম্মাদার'কে ব্যবহারকারীর তথ্য নেওয়ার আগে অবশ্যই সুনির্দিষ্ট ও স্পষ্ট সম্মতি নিতে হবে। ব্যবহারকারীকে জানাতে হবে কেন তথ্য নেওয়া হচ্ছে এবং কতদিন তা রাখা হবে।
- **সম্মতি প্রত্যাহার:** ব্যবহারকারী যেকোনো সময় তার দেওয়া সম্মতি প্রত্যাহার করতে পারবেন। সম্মতি তুলে নিলে সেবা প্রদানকারীকে ওই ব্যক্তির তথ্য মুছে ফেলতে হবে।
- **প্রতারণামূলক সম্মতি:** মিথ্যা বলে বা প্রতারণা করে সম্মতি নেওয়া একটি দন্ডনীয় অপরাধ, যার জন্য কারাদন্ড ও অর্থদন্ডের বিধান রয়েছে।

৩. সাধারণ নাগরিকদের অধিকার (Rights of Data Subject)

ডিজিটাল সেবায় নিজের তথ্যের ওপর ব্যবহারকারীর পূর্ণ নিয়ন্ত্রণ থাকবে:

- **তথ্য জানার ও ফেরত পাওয়ার অধিকার:** কোনো কোম্পানি ব্যবহারকারীর কী কী তথ্য জমা রেখেছে, তা জানার এবং সেই তথ্যের কপি ফেরত পাওয়ার অধিকার ব্যবহারকারীর রয়েছে।
- **তথ্য সংশোধন:** যদি কোনো সেবায় ব্যবহারকারীর ভুল তথ্য সংরক্ষিত থাকে, তবে তিনি তা সংশোধন বা হালনাগাদ করার দাবি করতে পারেন।
- **তথ্য মুছে ফেলার অধিকার (Right to Erasure):** সেবা নেওয়া শেষ হলে বা প্রয়োজন ফুরিয়ে গেলে ব্যবহারকারী তার সমস্ত তথ্য মুছে ফেলার জন্য কোম্পানিকে নির্দেশ দিতে পারেন।
- **তথ্য স্থানান্তর (Portability):** ব্যবহারকারী চাইলে তার তথ্য এক সেবা প্রদানকারীর কাছ থেকে অন্য সেবা প্রদানকারীর কাছে স্থানান্তর করার ব্যবস্থা করতে পারেন।

৪. শিশুদের (১৮ বছরের নিচে) তথ্যের বিশেষ সুরক্ষা

শিশুদের ডিজিটাল নিরাপত্তা নিশ্চিত করতে আইনে বিশেষ বিধান রাখা হয়েছে:

- **অভিভাবকের সম্মতি:** ১৮ বছরের কম বয়সী কোনো শিশুর তথ্য সংগ্রহ করতে হলে অবশ্যই তার বাবা-মা বা আইনগত অভিভাবকের সম্মতি নিতে হবে।
- **ট্র্যাকিং ও প্রোফাইলিং নিষিদ্ধ:** শিশুদের আচরণ পর্যবেক্ষণ করা, ট্র্যাকিং করা বা তাদের টার্গেট করে বিজ্ঞাপন প্রচার করা (Targeted Advertisement) সম্পূর্ণ নিষিদ্ধ।
- **কঠোর শাস্তি:** শিশুদের তথ্য অবৈধভাবে সংগ্রহ বা ব্যবহার করলে কারাদন্ড ও অর্থদন্ডের বিধান রাখা হয়েছে।

৫. সেবা প্রদানকারী বা কোম্পানির দায়বদ্ধতা

যারা তথ্য সংগ্রহ করবেন (যেমন- ফেসবুক, গুগল, ব্যাংক, ই-কমার্স), তাদের কিছু দায়িত্ব পালন করতে হবে:

- **নিরাপত্তা নিশ্চিতকরণ:** ব্যক্তিগত উপাত্ত হ্যাকিং বা চুরি হওয়া থেকে বাঁচাতে কোম্পানিকে শক্তিশালী কারিগরি নিরাপত্তা (যেমন- এনক্রিপশন) নিশ্চিত করতে হবে।

- **তথ্য ফাঁস হলে জানানো (Data Breach):** যদি কখনো হ্যাকাররা তথ্য চুরি করে বা তথ্যের নিরাপত্তা বিঘ্নিত হয়, তবে কোম্পানিকে দ্রুত কর্তৃপক্ষ এবং ব্যবহারকারীকে জানাতে হবে ।
- **তথ্য ব্যবহারের সীমা:** যে উদ্দেশ্যে তথ্য নেওয়া হয়েছে (যেমন- পণ্য ডেলিভারি), তার বাইরে অন্য কোনো কাজে (যেমন- বিজ্ঞাপন দেখানো বা অন্যের কাছে বিক্রি করা) সেই তথ্য ব্যবহার করা যাবে না ।

৬. অপরাধ ও শাস্তি

আইন লঙ্ঘন করলে কঠোর শাস্তির ব্যবস্থা রয়েছে:

- **অনুমতি ছাড়া তথ্য ব্যবহার:** সম্মতি ছাড়া কারো তথ্য ব্যবহার, শেয়ার বা বিক্রি করলে ৫ বছর পর্যন্ত জেল বা ১০ লক্ষ টাকা জরিমানা হতে পারে ।
- **সংবেদনশীল তথ্যের অপব্যবহার:** স্বাস্থ্য বা বায়োমেট্রিক তথ্যের মতো সংবেদনশীল তথ্য অবৈধভাবে প্রক্রিয়া করলে ৭ বছর পর্যন্ত জেল বা ২০ লক্ষ টাকা জরিমানা হতে পারে ।
- **হ্যাকিং বা তথ্যে হস্তক্ষেপ:** অনুমতি ছাড়া কারো ডিভাইসে ঢুকে তথ্য নেওয়া বা তথ্যের প্রবাহে বাধা দিলে ৫ বছর পর্যন্ত কারাদণ্ড হতে পারে ।
- **ক্ষতিপূরণ:** তথ্যের অধিকার লঙ্ঘিত হলে ভুক্তভোগী ব্যক্তি জরিমানার অর্থের পাশাপাশি আলাদাভাবে ক্ষতিপূরণ দাবি করতে পারেন ।

নতুন এই অধ্যাদেশ অনুযায়ী, ইন্টারনেটে বা ডিজিটাল মাধ্যমে বিচরণকারী প্রতিটি ব্যক্তি তার নিজের তথ্যের একচ্ছত্র মালিক। অপ্রয়োজনীয় বা সন্দেহজনক ক্ষেত্রে সম্মতি না দেওয়া, নিয়মিত নিজের তথ্যের খোঁজ রাখা এবং অধিকার লঙ্ঘিত হলে কর্তৃপক্ষের কাছে অভিযোগ দায়ের করার মাধ্যমে ডিজিটাল সুরক্ষা নিশ্চিত করা সম্ভব ।

ব্যক্তিগত উপাত্ত সুরক্ষা অধ্যাদেশ, ২০২৫ এর লিংক: http://bdlaws.minlaw.gov.bd/act-1574.html

এই পাঠ থেকে আমরা যা জানলাম:

- অনলাইন ইথিক্স: ডিজিটাল জগতে শালীনতা ও দায়িত্বশীল আচরণ
- ডিজিটাল ওয়েলবিং: প্রযুক্তির সুস্থ ব্যবহার এবং শারীরিক ও মানসিক সুস্থতা বজায় রাখা
- সাইবার সুরক্ষার মূল অভ্যাস: পাসওয়ার্ড সুরক্ষা, ২FA ব্যবহার এবং নিয়মিত আপডেট
- ম্যালওয়্যার ও ভাইরাস থেকে সুরক্ষা: ক্ষতিকর সফটওয়্যার এবং সন্দেহজনক ফাইল এড়িয়ে চলা
- ফিশিং ও সোশ্যাল ইঞ্জিনিয়ারিং প্রতিরোধ: প্রতারণামূলক ইমেইল ও মেসেজ থেকে সতর্ক থাকা
- র‍্যানসমওয়্যার, স্পাইওয়্যার ও অ্যাডওয়্যার থেকে রক্ষা: আধুনিক সাইবার হুমকি মোকাবিলা
- সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫: সাইবার অপরাধ শনাক্তকরণ, প্রতিরোধ ও শাস্তির আইনি কাঠামো
- ব্যক্তিগত উপাত্ত সুরক্ষা অধ্যাদেশ, ২০২৫: নাগরিকদের তথ্যের মালিকানা এবং গোপনীয়তার অধিকার সংরক্ষণ