বাংলাদেশ জাতীয় এআই গভর্নেন্স হ্যান্ডবুক

নীতি, আইন, বাস্তবায়ন কাঠামো ও নির্দেশিকা।

National AI Governance in Bangladesh



INCLUSIVE
RESPONSIBLE
SUSTAINABLE
AI FOR
BANGLADESH

Nafiul Ahmad Rafi

শেখার লক্ষ্য

এই অধ্যায় শেষে পাঠক দায়িত্বশীল AI শাসনের নীতিগুলোকে ন্যায্যতা, গোপনীয়তা, নিরাপত্তা, স্বচ্ছতা ও মানবীয় তদারকির বাস্তব সিদ্ধান্তে প্রয়োগ করতে পারবেন।

৪.১ আনুপাতিকতা ও ক্ষতি না করা

আনুপাতিকতার অর্থ হলো—কোনো AI ব্যবস্থা যে লক্ষ্য পূরণের জন্য তৈরি বা কেনা হচ্ছে, তার তুলনায় ব্যবস্থার পরিসর, তথ্য-সংগ্রহ, স্বয়ংক্রিয়তার মাত্রা ও সম্ভাব্য হস্তক্ষেপ যেন প্রয়োজনের বেশি না হয়। প্রথম প্রশ্ন হওয়া উচিত, সমস্যাটি বাস্তব কি না এবং তার একটি নির্দিষ্ট জনস্বার্থমূলক লক্ষ্য আছে কি না। এরপর দেখা দরকার, AI ছাড়া বা কম তথ্য, কম নজরদারি এবং কম জটিল কোনো পদ্ধতিতে একই ফল পাওয়া যায় কি না।

“ক্ষতি না করা” মানে কেবল বড় দুর্ঘটনা ঠেকানো নয়। এর মধ্যে ভুলভাবে সুবিধা থেকে বাদ পড়া, ভুল ব্যক্তিকে সন্দেহভাজন হিসেবে চিহ্নিত করা, ব্যক্তিগত তথ্যের অতিরিক্ত ব্যবহার, বৈষম্য, সেবা বিলম্ব, আর্থিক ক্ষতি, নিরাপত্তা ঝুঁকি এবং পরিবেশের ওপর অযৌক্তিক চাপও পড়ে। সম্ভাব্য ক্ষতির তীব্রতা, সম্ভাবনা, পরিসর, স্থায়িত্ব এবং তা ফিরিয়ে নেওয়া যায় কি না—এসব আগেই মূল্যায়ন করা প্রয়োজন। UNESCO বিশেষভাবে বলে, AI-এর সম্ভাব্য ঝুঁকি ও উপকার বিবেচনা করতে হবে এবং ক্ষতি প্রতিরোধে সতর্কতা অবলম্বন করতে হবে। [1]

বাংলাদেশের সামাজিক সুরক্ষা ভাতা বা অন্য কোনো সরকারি সুবিধার যোগ্যতা যাচাইয়ে AI ব্যবহারের প্রস্তাব বিবেচনা করা হলে, কেবল প্রয়োজনীয় তথ্য নেওয়া উচিত। ভুল তথ্যের কারণে যোগ্য ব্যক্তি বাদ পড়তে পারেন কি না তা পরীক্ষা করতে হবে। সিদ্ধান্তের কারণ জানার, তথ্য সংশোধনের এবং কর্মকর্তার কাছে পুনর্বিবেচনা চাওয়ার পথ থাকতে হবে। এটি নীতিগত নকশার উদাহরণ, কোনো নির্দিষ্ট চালু ব্যবস্থার দাবি নয়।

স্বাস্থ্যসেবায় AI-ভিত্তিক রোগঝুঁকি বা রোগী-অগ্রাধিকার সহায়ক হতে পারে, কিন্তু ব্যবস্থাটি চিকিৎসকের বিবেচনাকে পুরোপুরি প্রতিস্থাপন করবে কি না তা আলাদা প্রশ্ন। জরুরি অবস্থায় ভুল শ্রেণিবিন্যাসের ক্ষতি গুরুতর হতে পারে। তাই স্থানীয় রোগী-জনসংখ্যায় পরীক্ষা, চিকিৎসকের পর্যালোচনা, ব্যর্থ হলে বিকল্প পদ্ধতি এবং ঘটনা-পরবর্তী মূল্যায়ন দরকার।

আইনশৃঙ্খলা বা বায়োমেট্রিক শনাক্তকরণের মতো ব্যবহারে প্রয়োজনীয়তা, বৈধ উদ্দেশ্য, আইনগত ভিত্তি এবং কম-অনুপ্রবেশকারী বিকল্প বিশেষভাবে যাচাই করতে হবে। গণ-নজরদারি বা সামাজিক স্কোরিংয়ের মতো ব্যবস্থা ব্যক্তিস্বাধীনতা ও মর্যাদার ওপর বড় প্রভাব ফেলতে পারে। এমন ব্যবস্থার ক্ষেত্রে কেবল

প্রযুক্তিগত নির্ভুলতা যথেষ্ট যুক্তি নয়। UNESCO-র সুপারিশে সামাজিক স্কোরিং ও ব্যাপক নজরদারি নিয়ে কঠোর উদ্বেগের কথা রয়েছে। [1]

কোনো প্রতিষ্ঠান চালুর আগে অন্তত পাঁচটি প্রশ্ন করবে: লক্ষ্যটি কি সুনির্দিষ্ট ও বৈধ? AI-ই কি উপযুক্ত উপায়? কম-অনুপ্রবেশকারী বিকল্প পরীক্ষা করা হয়েছে কি? কোন গোষ্ঠী কী ধরনের ক্ষতি বহন করতে পারে? ভুল হলে দ্রুত সংশোধন, স্থগিত বা বন্ধ করার ক্ষমতা কার হাতে? উচ্চ-প্রভাবের সিদ্ধান্তে গড় নির্ভুলতা ভালো হলেও স্থানীয় ভাষা, অঞ্চল, প্রতিবন্ধিতা বা লিঙ্গভেদে ফল খারাপ হতে পারে। তাই সামগ্রিক সূচকের পাশাপাশি প্রাসঙ্গিক গোষ্ঠীভিত্তিক পরীক্ষা দরকার। [3]

অতিরিক্ত সতর্কতারও খরচ আছে। দীর্ঘ অনুমোদন বা ব্যয়বহুল মূল্যায়নে প্রয়োজনীয় সেবা বিলম্বিত হতে পারে। কিন্তু ঝুঁকি না মেপে দ্রুত চালু করলে ক্ষতি বড় পরিসরে ছড়াতে পারে। ভারসাম্যের উপায় হলো ঝুঁকিভিত্তিক ধাপ: কম-ঝুঁকির কাজে সহজ যাচাই, মাঝারি ঝুঁকিতে নথিবদ্ধ মূল্যায়ন ও পর্যবেক্ষণ, আর উচ্চ-প্রভাবের কাজে পূর্ণ প্রভাব মূল্যায়ন, মানবীয় পর্যালোচনা এবং প্রয়োজনে স্বাধীন পরীক্ষা।

৪.২ নিরাপত্তা ও সুরক্ষা

এই নীতিতে **নিরাপত্তা** বলতে AI ব্যবস্থার কারণে অনিচ্ছাকৃত ক্ষতি প্রতিরোধ বা কমানো বোঝায়। **সুরক্ষা** বলতে আক্রমণ, অননুমোদিত প্রবেশ, তথ্য ফাঁস, মডেল বা ডেটায় কারসাজি এবং ইচ্ছাকৃত অপব্যবহার থেকে রক্ষা বোঝায়। কোনো ব্যবস্থা শুধু পরীক্ষাগারে ভালো ফল দিলেই নিরাপদ হয় না। বাস্তব ব্যবহারে, পরিবর্তিত তথ্য, ভুল ইনপুট, নতুন সংস্করণ, নেটওয়ার্ক বিচ্ছিন্নতা এবং আক্রমণের পরিস্থিতিও বিবেচনা করতে হয়। UNESCO এবং OECD জীবনচক্রজুড়ে নিরাপত্তা, স্থিতিস্থাপকতা ও ঝুঁকি ব্যবস্থাপনার ওপর জোর দেয়। [1] [2]

ঝুঁকি ব্যবস্থাপনা নকশা থেকেই শুরু হওয়া উচিত। প্রতিষ্ঠানের আগে নির্ধারণ করতে হবে, কী ধরনের ভুল সবচেয়ে ক্ষতিকর, কোন তথ্য বা সেবা আক্রান্ত হতে পারে, কোন ব্যবহারকারীর কাছে ব্যবস্থা পৌঁছাবে এবং কী পরিস্থিতিতে সেটি কাজ বন্ধ করবে। NIST-এর কাঠামোতে “Govern, Map, Measure, Manage”—অর্থাৎ শাসন স্থাপন, প্রেক্ষাপট ও ঝুঁকি বোঝা, ঝুঁকি পরিমাপ এবং তা মোকাবিলা—এই চারটি ধারাবাহিক কাজের মাধ্যমে ঝুঁকি-ব্যবস্থাপনা সাজানো হয়েছে। কাঠামোটি স্বেচ্ছামূলক নির্দেশিকা, বাংলাদেশের আইন নয়। [3]

বাংলাদেশি প্রেক্ষাপটে স্থানীয় ভাষার ইনপুট, বাংলা লিপি, বানানভেদ, আঞ্চলিক উচ্চারণ, নিম্ন-সংযোগ পরিবেশ এবং ব্যবহৃত যন্ত্রের পার্থক্য পরীক্ষা করা জরুরি। একটি বাংলা চ্যাটবটের উত্তর শহুরে, উচ্চশিক্ষিত ব্যবহারকারীর ক্ষেত্রে ভালো হলেও গ্রামীণ বা ভিন্ন উপভাষার ব্যবহারকারীর কাছে ভুল হতে পারে। স্বাস্থ্য বা

সরকারি সেবার ক্ষেত্রে এমন ব্যর্থতার পরিণতি কেবল প্রযুক্তিগত ত্রুটি নয়; তা মানুষের সেবা পাওয়ার সুযোগে প্রভাব ফেলতে পারে।

সাইবার নিরাপত্তায় সরবরাহকারী, ক্লাউড সেবা, API, লগ, অ্যাকাউন্ট ও মডেল আপডেট—সবই বিবেচ্য। ডেটা বা মডেলকে বিষিয়ে দেওয়া, অননুমোদিতভাবে তথ্য বের করা, prompt injection, পরিচয় ছদ্মবেশ, সেবা অচল করে দেওয়া এবং AI-উৎপন্ন কনটেন্ট দিয়ে অপব্যবহার—এসব সম্ভাব্য ঝুঁকি পরীক্ষা করা উচিত। সংবেদনশীল তথ্য ব্যবহৃত হলে প্রবেশাধিকার সীমিত করা, এনক্রিপশন, লগিং এবং ঘটনার প্রতিক্রিয়া নির্ধারণ করা প্রয়োজন।

নিরাপদ ব্যর্থতা-ব্যবস্থা বিশেষ গুরুত্বপূর্ণ। মডেলের আত্মবিশ্বাস কম হলে, তথ্য অসম্পূর্ণ হলে বা নিরাপত্তা ঘটনা ঘটলে ব্যবস্থা যেন ভুলভাবে নিশ্চিত সিদ্ধান্ত না দেয়। প্রয়োজনমতো সেবা সীমিত, স্থগিত বা মানুষের কাছে হস্তান্তর করতে হবে। কোনো সরকারি ক্রয় বা সেবায় AI-ভিত্তিক সংকেতের কারণে দরদাতা, নাগরিক বা গ্রাহককে স্বয়ংক্রিয়ভাবে বাদ দেওয়া ঝুঁকিপূর্ণ হতে পারে। মানবীয় যাচাই ও অভিযোগের পথ থাকা উচিত।

পর্যবেক্ষণে ত্রুটি, আক্রমণ, অনাকাঙ্ক্ষিত ব্যবহার, গোষ্ঠীভিত্তিক ভুল এবং অভিযোগের ধারা দেখা দরকার। AI-ব্যবস্থা, তথ্য, নির্দেশনা বা সরবরাহকারী বদলালে আগের পরীক্ষার ফল যথেষ্ট নাও হতে পারে। তাই সংস্করণ-নিয়ন্ত্রণ, ঘটনা-নথি, সংশোধনের দায়িত্ব এবং অবসান-পদ্ধতি আগেই নির্ধারণ করতে হবে।

৪.৩ গোপনীয়তা ও তথ্য সুরক্ষা

গোপনীয়তার নীতি AI ব্যবস্থার পুরো জীবনচক্রে ব্যক্তির তথ্য, পরিচয়, যোগাযোগ ও ব্যক্তিগত পরিসর রক্ষার কথা বলে। তথ্য সংগ্রহ, পরিষ্কার, প্রশিক্ষণ, পরীক্ষণ, ব্যবহার, ভাগাভাগি, সংরক্ষণ এবং মুছে ফেলা—প্রতিটি ধাপে এই নীতি প্রযোজ্য। শুরুতেই নির্ধারণ করতে হবে, কী উদ্দেশ্যে কোন তথ্য প্রয়োজন এবং একই উদ্দেশ্য কম তথ্য দিয়ে অর্জন করা যায় কি না। উদ্দেশ্য বদলালে পূর্বের অনুমোদন বা নোটিশ যথেষ্ট কি না নতুন করে যাচাই করা দরকার। [1]

তথ্য সুরক্ষার ব্যবহারিক উপায়গুলোর মধ্যে রয়েছে তথ্য-ন্যূনতমকরণ, উদ্দেশ্য-সীমা, ভূমিকা-ভিত্তিক প্রবেশাধিকার, নির্দিষ্ট সংরক্ষণকাল, নিরাপদ স্থানান্তর, ছদ্মনামকরণ এবং তথ্য মুছে ফেলার কার্যকর প্রক্রিয়া। নাম মুছে ফেললেই তথ্য পুরোপুরি অজ্ঞাত হয়ে যায় না। বিরল বৈশিষ্ট্য, অন্য উৎসের তথ্য বা AI ব্যবস্থার উত্তর মিলিয়ে ব্যক্তি পুনরায় শনাক্ত হওয়ার ঝুঁকি থাকতে পারে।

বাংলাদেশে সরকারি ভাতা, স্বাস্থ্যসেবা, শিক্ষার্থী-সহায়তা, ব্যাংকিং বা মোবাইল আর্থিক সেবার তথ্য সংবেদনশীল হতে পারে। একটি প্রতিষ্ঠানের কাছে তথ্য থাকলেই তা অন্য উদ্দেশ্যে ব্যবহার করা যাবে—এমন নয়। শিক্ষার্থীর কথোপকথনকে অপ্রয়োজনে মডেল প্রশিক্ষণে নেওয়া, রোগীর তথ্য দীর্ঘদিন রাখা বা