ব্যক্তিপরিসর সুরক্ষা: এক দায়বদ্ধ কাঠামোর উপাদানসমূহ

শুভাশিস ব্যানার্জী

ভূমিকা

পুট্টাস্বামী মামলার রায় ঘোষণার পর ভারতবর্ষ যেন হঠাৎ করে ব্যক্তিপরিসর (privacy) পূর্ববর্তী সমাজ থেকে নতুন এক যুগে প্রবেশ করল। দেখা গেল, ডিজিটাল ডেটাবেসে (databases) ব্যক্তিপরিসরের সুরক্ষা ব্যাপারটা গোটা দেশের চিন্তার কারণ হয়ে উঠেছে [১,২,৩]। আসলে আমরা এমন একটা সময়ে দাঁড়িয়ে আছি যখন তথ্যপ্রযুক্তি ব্যবস্থা আমাদের জীবনের ভাঁজে ভাঁজে ঢুকে পড়েছে। ব্যক্তিপরিসর সুরক্ষা আর মসৃন দৈনন্দিন জীবনযাপনের মধ্যেকার দ্বন্দ্ব মোকাবিলা করাই এখন একটা চ্যালেঞ্জ। অনেকের মতে আমরা ব্যক্তিপরিসর পরবর্তী সমাজে বসবাস করছি। এখানে ব্যক্তিপরিসর নিয়ে যে বেঁচে থাকাতে পারব তার কোনো নিশ্চয়তা নেই—'In the post-privacy world, privacy is no longer guaranteed or expected.' [Spivack][৪]। ভারতের সুপ্রিম কোর্ট কিন্তু এই ভাবনাকে মেনে নেয় নি। কোর্ট তার রায়ে ব্যক্তিপরিসরের অধিকারকে অলঙ্ঘনীয় হিসাবে চিহ্নিত করেছে[১]। ব্যক্তিগত তথ্যের স্ব- নিয়ন্ত্রণের অধিকার পুট্টাস্বামী রায়ের অন্যতম গুরুত্বপূর্ণ ভাবনা [৫]। বিচারপতি কল (Kaul) এই অধিকারের বিষয়ে বলতে গিয়ে বলেছেন—ব্যক্তিপরিসরের ধারণাটির মধ্যেই অন্তর্গত রয়েছে ব্যক্তিগত তথ্য উদ্‌ঘাটনের (dissemination) অধিকারটি—'an aspect of privacy [is] the right to control dissemination of personal information.' (অনুচ্ছেদ ৫৩ দ্রষ্টব্য)। এখানে বিচারপতি আরও বলেছেন যে মানুষ সমাজের সঙ্গে যে সীমারেখা টানে, তা শুধুমাত্র শারীরিকই নয়, তা তথ্য-বিষয়কও বটে।[৫]

ডিজিটাল পরিচয়জ্ঞাপক কোনো প্রকল্পের মাধ্যমে লেনদেন (transactions) করলে লেনদেনকারীর ডিজিটাল তথ্য এবং সেই তথ্যের আন্তঃসম্পর্ক-সম্বন্ধীয় একটি সংগ্রহ তৈরি হয়। পরবর্তীকালে, তথ্য আদানপ্রদানের এই পথেই সেই ব্যক্তির ব্যক্তিপরিসরের লঙ্ঘন ঘটতে পারে। তাই, ডিজিটাল ডেটাবেসের পরিপ্রেক্ষিতে

ব্যক্তিপরিসরের কেন্দ্রে রয়েছে তথ্য সুরক্ষা ব্যবস্থা। লেনদেনের ডিজিটাইজেশনের মাধ্যমে দুটি সুবিধা মেলে—ভবিষ্যতে অডিট বা অনুসন্ধানের প্রয়োজনে নির্ভুল নথি সংরক্ষণ (record keeping), এবং ডেটা অ্যানালিটিক্সের (data analytics) মাধ্যমে তথ্যের ব্যবহারযোগ্য নিদর্শন (patterns) আবিষ্কার। এই দ্বিতীয় সুবিধাটির প্রভাব আধুনিককালে যে ক্ষেত্রগুলিতে উল্লেখযোগ্যভাবে পড়েছে সেগুলি হলো ইকনোমেট্রিক বিশ্লেষণ, মহামারীবিজ্ঞান গবেষণা, একটি প্রণালীর কার্যকারণ বিশ্লেষণ আর সুপ্ত বিষয়ের আবিষ্কার (latent topic discovery)। এখানে সুপ্ত বিষয়ের আবিষ্কারের সম্পর্কে দু-একটা কথা বলা যেতে পারে। টপিক আবিষ্কার[৩৯]; সেই বিষয়গুলি শনাক্ত করা যা দস্তাবেজের একটি সংকলনকে (বা তথ্য সংগ্রহকে) সবথেকে ভালোভাবে বর্ণনা করে। নীচে উল্লেখিত উদাহরণগুলি থেকে ব্যাপারটা বোঝা যাবে—

১. হোয়াটস্‌অ্যাপ মেসেজের একটি সংগ্রহ থেকে কোন বিষয়গুলি নিয়ে দেশে বা বিদেশে আলোচনা হচ্ছে তা নির্ধারণ করা।
২. খবরের কাগজের কিছু খবর ও প্রবন্ধ থেকে সাম্প্রতিক গুরুত্বপূর্ণ আলোচনার বিষয়গুলি আবিষ্কার করা।
৩. প্রাথমিক স্বাস্থ্য কেন্দ্রগুলির সার্বজনীন ডিজিটাল হেল্‌থ রেকর্ড থেকে একটি নতুন অজানা ছোয়াঁচে রোগের অস্তিত্ব আবিষ্কার করা।
৪. অগোছালো কিছু তথ্য সংগ্রহ থেকে তথ্যের সূচি খুঁজে বার করা। আমরা সকলেই জানি, এই ইনফর্মেশনের যুগে তথ্যের ভাণ্ডারে এত তথ্য জমা হচ্ছে যে প্রয়োজন মাফিক তার বিন্যাস করা একান্ত জরুরি হয়ে উঠেছে। এখানেই টপিক মডেলের সার্থকতা। তথ্যের বিস্ফোরণের মধ্যে দাঁড়িয়ে টপিক মডেলের সাহায্যে শুধুমাত্র তার উপযুক্ত বিন্যাসই সম্ভব নয়, এই প্রক্রিয়ার মাধ্যমে এইসব অগোছালো তথ্যের ভাণ্ডার থেকে উঠে আসতে পারে অপ্রত্যাশিত সামাজিক চাহিদা বা অজানা ছোয়াঁচে রোগের অস্তিত্ব আবিষ্কারের মতো বিষয়। আগে যেহেতু এগুলি জানা ছিল না, তাই একে বলে সুপ্ত বিষয়ের আবিষ্কার। ওপরের আলোচনা থেকে পরিষ্কার হয় যে কেন উন্নততর সামাজিক নীতি নির্ধারণ, তার স্ট্র্যাটেজি তৈরিতে এবং অসঙ্গতির চিহ্নিতকরণে ও পূর্বাভাস প্রদানে অ্যানালিটিক্সের সাহায্য পাওয়া যেতে পারে[৬]। তবে নথি সংরক্ষণ আর অ্যানালিটিক্স, এই দুইয়ের দ্বারাই ব্যক্তিপরিসর সংকোচনের সম্ভাবনা থেকেই যায়।

আমরা জানি, ডিজিটাইজেশনের জন্য প্রয়োজন নির্ভুল শনাক্তকরণ। আর এই কারণেই দরকার সূচক বা অনন্য এক পরিচায়কের (unique identifier)। যেমনটা আমরা রেশন কার্ড বা জব কার্ড জাতীয় বিভিন্ন সামাজিক সুরক্ষা প্রকল্পে দেখেছি। এই ধরনের প্রকল্পে, দীর্ঘকালীন ব্যবস্থায় ব্যক্তি পরিচয়ের সূচকের ভিত্তিতে (indexed by an

identity) সংরক্ষিত ডিজিটাল নথির অবৈধ অনুপ্রবিষ্টন বা অ্যাক্সেসের (access) ফলে ব্যক্তিপরিসর লঙ্ঘিত হতে পারে। অ্যানালিটিক্সের কাজে বহু সময়ে বিভিন্ন ক্ষেত্র (domain) থেকে তথ্য জুড়ে-জুড়ে জ্ঞানের সীমাকে প্রসারিত করা হয়[৬]। ক্ষেত্রের সীমারেখার এই অবলুপ্তি ব্যক্তিবিশেষের প্রোফাইল তৈরির কাজে অবৈধভাবে ব্যবহৃত হতে পারে, এবং এর ফলে ব্যক্তির নিজস্ব তথ্যের অধিকারের ধারণাও অমান্য করা হবে। অর্থাৎ, ডেটাবেসের কার্যকর ব্যবহার এবং ব্যক্তিপরিসরের সুরক্ষার মধ্যে আপাতদৃষ্টিতে পরস্পরবিরোধী সম্পর্ক আছে।

এই লেখায় আমরা বোঝার চেষ্টা করব কীভাবে ব্যক্তিপরিসরের সুরক্ষা-সংক্রান্ত পরস্পরবিরোধী এই সম্পর্কের সংগতি সম্ভব হতে পারে। এখানে আমরা শ্রীকৃষ্ণ কমিটির ডেটা সুরক্ষা সংক্রান্ত সুপারিশগুলি নিয়েও আলোচনা করব।[৭] আমাদের মূল বক্তব্য হচ্ছে, যে সমাধান শুধুমাত্র ব্যক্তিপরিসর লঙ্ঘন হলে তার উদ্‌ঘাটন এবং তৎপরবর্তী কালে প্রতিকারমূলক ব্যবস্থায় আগ্রহী, সেই সমাধান অধিকাংশ সময় কার্যকরী হতে পারে না। একই সঙ্গে প্রয়োজন একটি অনলাইন কাঠামোগত ব্যবস্থাপনা বা আর্কিটেকচারাল সমাধান (architectural solution), যা গোড়াতেই ব্যক্তিপরিসর লঙ্ঘনের প্রচেষ্টাকে প্রতিহত করবে[৮]। এদেশের প্রেক্ষিতে একাধিক ঘটনার আলোচনার মাধ্যমে রাঘবন দেখিয়েছেন—কেন ঘটনার পূর্বেই ব্যবস্থা গ্রহণ জরুরি।[৯]

ব্যক্তিপরিসর সংক্রান্ত ব্যাপারে ইদানীং যে গুরুত্ব আরোপিত হচ্ছে, সেটা আমাদের একটা সুযোগ এনে দিয়েছে ভারতে ডিজিটাল পরিষেবার ক্ষেত্রে কার্যকরী প্রোটোকল ডিজাইন (protocol design) নিয়ে নতুন চিন্তা-ভাবনার। আমাদের দেশে মার্কিন যুক্তরাষ্ট্রের তুলনায় ব্যক্তিপরিসর রক্ষায় কঠোরতর ব্যবস্থা দরকার। লন্ডন স্কুল অফ ইকনমিক্স অ্যান্ড পলিটিক্যাল সায়েন্সের[১০] একটি গবেষণায় বেরিয়ে এসেছে যে সেদেশে ব্যক্তি-পরিচয় চুরির ঘটনা অস্বাভাবিক রকম বেশি। এছাড়া সেখানে গুগ্‌ল্‌ এবং ফেসবুকের মতো কর্পোরেট 'প্যানঅপটিকন'-রা মোটামুটিভাবে অবাধে বেড়ে ওঠার সুযোগ পেয়েছে। (জেরেমি বেন্থামের ধারণা অনুযায়ী প্যানঅপটিকন এমন একটা চক্রাকার জেলখানা, যেখানে কেন্দ্রবিন্দুতে অবস্থিত ওয়াচ-টাওয়ার থেকে ইন্সপেক্টর প্রত্যেক বন্দির চলাফেরা দেখতে পায় কিন্তু বন্দিরা ইন্সপেক্টরকে দেখতে পায় না। ডিজিটাল যুগে, যা ডেটাভিত্তিক নজরদারির প্রতীক হিসেবে দেখা চলে)।[১১]

অন্যদিকে, ভারতের প্রয়োজন এমন ব্যবস্থা, যা ইউরোপিয়ান জিডিপিআরের[১২] তুলনায় ইনোভেশনে কম বাধা আনে, কারণ ইউরোপীয় ব্যবস্থা হয়তো যতটা না গণ্ডিবদ্ধ ততটা কার্যকরী নয়। এছাড়া, দেশের বিপুল সংখ্যক অবহেলিত প্রান্তিক মানুষদের কথা মনে রেখে ডিজাইনারদের সচেতন থাকতে হবে যাতে আমাদের ব্যবস্থা ওই মানুষদের সাংস্কৃতিক ক্ষমতার তুলনায় অতিরিক্ত জটিল না হয়ে পড়ে।

২. ডিজিটাল ডেটাবেসে ব্যক্তিপরিসরজনিত ঝুঁকি

ব্যক্তিপরিসরজনিত সুরক্ষার ব্যাপারটা বুঝতে গেলে প্রথমেই জানা দরকার কীভাবে ডিজিটাল ডেটাবেসে ব্যক্তিপরিসরের সুরক্ষায় ঘাটতি আসতে পারে। যে-কোনো ধরনের গণ-ডিজিটাইজেশন প্রক্রিয়াতে নজরদারির ভীতিটা থেকেই যায়, বিশেষভাবে ডিজিটাইজেশন প্রক্রিয়া যদি সরকারের পক্ষ থেকে চালু হয়। সমস্ত ডিজিটাইজেশন প্রক্রিয়াতেই অনন্য ডিজিটাল আইডেনটিটি (unique digital identities) বা পরিচয়ের দরকার। আর একটি সার্বজনীন পরিচয় যদি বহুসংখ্যক ডেটাবেসে ব্যবহৃত হয়, তাহলে এমন একটি পরিকাঠামো তৈরি হয় যার সাহায্যে নাগরিকদের বিভিন্ন ক্রিয়াকর্মের ওপর সর্বগ্রাসী নজরদারি চালানো সম্ভব হয়ে ওঠে। সমাজবিদ ড্রেজ ২০১৬ সালে একটি লেখায় বলেছিলেন যে দেশে যখন অসংখ্য ডেটাবেস আর অনন্য ডিজিটাল আইডেনটিটির মাধ্যমে ব্যাপক নজরদারির একটি পরিকাঠামোর অস্তিত্ব থাকে, তখন নাগরিক এবং রাষ্ট্রের মধ্যেকার ক্ষমতার ভারসাম্যে পরিবর্তন আনতে পারে। এই অবস্থা নাগরিক সমাজের কণ্ঠরোধ ও নাগরিক স্বাধীনতায় ভীতিপ্রদর্শন বাস্তব হয়ে উঠতে পারে। গণ-ডিজিটাইজেশন এবং অনন্য ডিজিটাল আইডেনটিটি প্রক্রিয়াতে সরকারি উদারতার ওপর বিশ্বাস রাখা তাই নিতান্তই বোকামি।[১৩] অনেকেই এই অবস্থাকে চিত্রিত করতে অরওয়েলের 'বিগ ব্রাদার' বা প্যানঅপটিকন জাতীয় 'ক্লিশে' উদাহরণ দিয়েছেন।

সূক্ষ্মভাবে দেখলে, অধিকতর ব্যাপ্তিতে রাষ্ট্র এবং রহস্যে ঘেরা, নির্বিকার আর অস্বচ্ছ কিছু আমলাতন্ত্রের কাছে আপন তথ্যের আত্মনিয়ন্ত্রণ খুইয়ে ক্রমাগত আমাদের ব্যক্তিপরিসরে সংকোচন ঘটে চলেছে। অনেক সময়ে সরাসরি অথবা সুনির্দিষ্টভাবে ব্যক্তিপরিসরে আঘাত আসে না, কিন্তু ডেটাবেস থেকে যেমন সহজেই সম্পূর্ণ অথবা আংশিকভাবে ব্যক্তিগত ডেটার প্রতিলিপি (replication) সৃষ্টি সম্ভব, তেমন তার এগ্রিগেশন (aggregation) বা একত্রীকরণ বা বাছাই করা সংমিশ্রণও (selective combination) সম্ভব।[১৪] এটাই অনেকের মধ্যে একটা অনিশ্চয়তার জন্ম দেয়, কে জানে তাদের ব্যক্তিগত তথ্য নিয়ে রাষ্ট্র বা আমলাকুল কি উদ্দেশ্যে তার ব্যবহার করছে। (একত্রীকরণ হলো একজন মানুষ সম্পর্কে আলাদা আলাদা সূত্র থেকে একাধিক তথ্য একত্রিত করে তার সম্পর্কে ধারণা তৈরির পদ্ধতি।) ফ্রান্জ় কাফকার 'দ্য ট্রায়াল' উপন্যাসটির কথা মনে রেখে সোলাভ মনে করেন 'কাফকায়েস্ক' (Kafkaesque) হতে পারে এই অবস্থার সঠিক উপমা। শুধু যে ব্যক্তিগত তথ্য ফাঁস হয়ে যায় এবং অপ্রত্যাশিতভাবে অযাচিত কিছু ব্যক্তি বা সংগঠনের দ্বারা তার ব্যবহার হয় তাই নয়,

এর ফলে বেঠিক প্রোফাইল, ভ্রান্ত মূল্যায়ন এবং এমনসব অপ্রাসঙ্গিক তথ্যের দ্বারা তিনি হয়তো প্রভাবিত হতে পারেন[১৪], যার ওপর তাঁর কোনো নিয়ন্ত্রণ নেই বা হয়তো তিনি সে সম্পর্কে অবগত নন।

আমলাতান্ত্রিক ডিজিটাইজেশনের আরেকটি অন্তরায় হচ্ছে 'ইউজ কেস'[১৫] (use cases)-সংক্রান্ত চিন্তার দৈন্য, অসম্পূর্ণ কেস-বিশ্লেষণ এবং অদক্ষ প্রোগ্রামিং। সফট্ওয়্যার অ্যান্ড সিস্টেম ইঞ্জিনিয়ারিং পাঠে 'ইউজ কেস' বলতে বোঝায় একজন ব্যবহারকারী (কারিগরি ভাষায় 'অ্যাক্টর') এবং সিস্টেমের মধ্যে পারস্পরিক ক্রিয়া-প্রতিক্রিয়া বা তাদের মধ্যেকার কার্যকলাপের বিবরণ। এর ফলে সিস্টেমের উদ্দেশ্য সফলভাবে সম্পাদন করা সম্ভব হয়। আমাদের দৈনন্দিন জীবনযাত্রায় যে সমস্ত ডিজিটাইজেশন প্রক্রিয়ায় ইউজ কেসের ব্যবহার দেখি তার মধ্যে আঙুলের ছাপ দিয়ে পরিচয় প্রমাণ করে রেশন নেওয়া বা আঙুলের ছাপ দিয়ে পরিচয় প্রমাণ করে (KYC) সিম কার্ড নেওয়া বা ব্যাঙ্ক অ্যাকাউন্ট খোলা উল্লেখযোগ্য। গরিব মানুষের টাকা যাতে কেউ লুটে না নিতে পারে, তার জন্য পরিচয়ের প্রমাণ হিসাবে আধার নম্বর দিয়ে জিরো ব্যালান্স ব্যাঙ্ক অ্যাকাউন্ট খুলে জব কার্ডের সঙ্গে তার লিঙ্ক করিয়ে সরাসরি ব্যাঙ্ক ট্রান্সফারের ব্যবস্থা করার পেছনে ইউজ কেস-এর ছায়া যে-কোনো প্রযুক্তিবিদের কাছে প্রতীয়মান। এর ফলে অনেক সময়েই দেখা যায়, কেউ দরকারি কোনো পরিষেবা থেকে বাদ পড়ে গেছেন কারণ তার রেজিস্ট্রেশন বাতিল হয়ে গিয়েছে। এ ব্যাপারে তাঁর কোনো দোষ নেই কিন্তু এর সুরাহা করতে তাকে বিস্তর ছোটাছুটি করতে হচ্ছে। জাতীয় পরিচয়পত্র নেই বলে কেউ হয়তো রেশন তুলতে পারছে না, হাসপাতালে চিকিৎসার সুযোগ থেকে বঞ্চিত হচ্ছে, কেউ-বা স্কুলে ভর্তি হতে পারছে না, কেউ হয়তো নাচের প্রতিযোগিতায় যোগ দিতে পারছে না, কারুর আবার নামের বানান ভুল বা আঙুলের ছাপ মিলছে না বলে সামাজিক সুরক্ষা কর্মসূচির সুবিধা থেকে বঞ্চিত হচ্ছে। এই ধরনের নির্মম ত্রুটি-বিচ্যুতি শুধুমাত্র ব্যক্তিপরিসরেই বিপদ ডেকে আনে না, এর ফলে অনেক সময়ে স্বাধীনতার সঙ্কোচন বা প্রাণের সংশয় ঘটাতে পারে।[৩,১৫]

সর্বশেষে বলা চলে ব্যক্তিপরিসর আর স্বাধীনতার (liberty) ক্ষেত্রে বিপদ বিগ-ডেটা অ্যানালিটিক্স অথবা মেশিন লার্নিং থেকেও আসছে। ও'নিল-এর মতে, যেহেতু বিগ-ডেটা অ্যানালিটিক্স সুবিধাভোগীরা বহুক্ষেত্রেই মুনাফার জন্য সেটা ব্যবহার করেন, তাই তা অনেক সময়ই 'অসাম্যের বৃদ্ধি ঘটায় যেটা গণতন্ত্রের পক্ষে বিপজ্জনক।'[১৬]

তিনি একাধিক উদাহরণ দিয়ে দেখিয়েছেন কীভাবে শিক্ষক-শিক্ষিকাদের মূল্যায়ন আর যোগ্যতা নির্ধারণ থেকে শুরু করে দোষী সাব্যস্ত করা অপরাধীর পুনঃ অপরাধের ঝুঁকি (recidivism risk) নির্ধারণ, ঋণযোগ্যতা (creditworthiness) নির্ধারণ, শিক্ষাপ্রতিষ্ঠান র‍্যাকিং থেকে চাকুরির আবেদনপত্রের স্ক্রিনিং, পুলিশি নজরদারি এবং দণ্ডবিধান, সব কিছুর অ্যালগরিদমে দেখা যাবে অসাম্যের চিত্রটা, যা ধনীদের পালে আরও জোরদার হাওয়া তোলে আর গরিবদের ওপর নামিয়ে আনে দুর্ভোগের খাঁড়া। এই প্রবণতা হয় অ্যালগরিদম বা ডেটা, বা উভয়ের মধ্যেই থাকে। প্রেডিক্টিভ অ্যানালিসিসের এই হতাশজনক পরিণামগুলির সম্মিলিত প্রভাব হল অস্বচ্ছতা আর ক্ষতির ব্যাপক প্রসারণ। অনেক সময়েই অসাম্যকে এরা আরও বাড়িয়ে তোলে।[১৭]

থ্যাচার ও অন্যান্যদের মতে 'যখন অ্যালগরিদমগুলিই সিলেক্ট করে, লিঙ্ক করে, বৃহৎ থেকে আরও বৃহত্তর ডেটা সেটগুলি বিশ্লেষণ করে, তখন তারা আগের দিন যা ছিল ব্যক্তিগত, যে সমস্ত একান্ত মুহূর্তগুলি এতদিন ছিল পরিসংখ্যার নাগালের বাইরে, সেগুলিকে মুনাফার উপাদানে পরিণত করে দেয়।[১৮] একই মতামত ব্যক্ত করেছেন জুবোফও।[১৯]

এই সমস্ত বিপদগুলি থাকা সত্ত্বেও, ডিজিটাইজেশন এবং অ্যানালিটিক্স যে প্রভূত সুবিধার প্রতিশ্রুতি বহন করে তাতে এগুলিকে অস্বীকার করার কোনো অবকাশ নেই। প্রশ্নটা হলো সুরক্ষিত ও ঠিকঠাকভাবে আমরা কীভাবে এর সুবিধা উপলব্ধ করতে পারি। অরওয়েলের 'বিগ ব্রাদার' আর 'কাফকায়েস্ক' যুক্তির অবতারণা নিশ্চয় চিন্তার উদ্রেক করে, কিন্তু এর মানে এই নয় যে ডিজিটাইজেশন-ভিত্তিক পরিচয় ব্যবস্থা চালু হলে ব্যক্তিপরিসর সুরক্ষা অসম্ভব হবে। যদিও ও'নিল স্পষ্টভাবেই বলেছেন যে 'আমাদের হাতে প্রযুক্তি রয়েছে! আমরা যদি এই ব্যাপারে অঙ্গীকারবদ্ধ হই, তাহলে আমরা বিগ ডেটা ব্যবহার করে সমতা এবং ন্যায় প্রতিষ্ঠার লক্ষ্যে এগিয়ে যেতে পারি'[১৬], তবু অনেক সময়েই প্রেডিক্টিভ অ্যালগরিদম নিয়ে তাঁর কাজের এমন ব্যাখ্যা হাজির করা হয় যেন তিনি কোনোভাবেই এর প্রয়োগে রাজি নন। কয়েকটা নিকৃষ্ট মানের প্রেডিক্টিভ অ্যানালিসিসের ভিত্তিতে এমন সিদ্ধান্তে পৌঁছানো কিন্তু হতাশাবাদী চিন্তারই পরিচয় বহন করে।

৩. রাষ্ট্রের বৈধ স্বার্থ

এই নিয়ে দ্বিধা থাকা উচিত নয় যে ব্যক্তিসুরক্ষার নীতি রাষ্ট্র এবং অত্যাবশ্যক পরিষেবা প্রদানকারী আমলাতন্ত্রের (যেমন ব্যাঙ্কিং বা বিমা) ক্ষেত্রে এবং অত্যাবশ্যক নয় এমন অন্যান্য বেসরকারি পরিষেবা প্রদানকারীদের ক্ষেত্রে যেখানে অংশগ্রহণ স্বেচ্ছাকৃত, এই দুই স্থানে সমভাবে প্রযোজ্য হতে পারে না । প্রথম ক্ষেত্রে রাষ্ট্রের ডিজিটাইজেশনের লক্ষ্যই হলো অনুবর্তিতা (compliance) সুনিশ্চিত করা, যেমন আয়কর আইনের লক্ষ্য সাধনে বা স্বাস্থ্য-সংক্রান্ত রেকর্ডের মতো সার্বজনীন ব্যবস্থার ইলেক্ট্রনিক নথির জন্য।

এই সমস্ত ক্ষেত্রে রাষ্ট্র তার বৈধ স্বার্থের বিষয়টা দ্ব্যর্থহীনভাবে প্রতিষ্ঠা করার এবং উপযুক্ত আইন তৈরির পরেই ডিজিটাইজেশন বাধ্যতামূলক করতে পারে।[১,৫]

এইসব আইনকে অবশ্যই হতে হবে আনুপাতিক (proportional), যুক্তিযুক্ত (reasonable) এবং খেয়ালিপনা (arbitrariness) বিবর্জিত। এখানে সম্মতির ব্যাপারটা গৌণ কিন্তু তথ্য সংগ্রহের ক্ষেত্র ও প্রয়োজনের সীমানা নির্ধারণ (purpose limitation) হবে অতীব গুরুত্বপূর্ণ নীতি। এটাও মনে রাখতে হবে যে শুধুমাত্র আইন করে দিলেই রাষ্ট্র এবং তার আমলাতন্ত্র ব্যক্তিপরিসর রক্ষার দায়ভাগ থেকে মুক্তি পাবে না, এবং পূর্ববর্তী অংশে বর্ণিত সমস্ত বিপদের আশঙ্কা নিরসন করার দায়িত্ব তাদের থেকেই যাবে।[২] তবে এই নীতি রাষ্ট্র কতটা অনুধাবন করতে সক্ষম, তা প্রশ্ন সাপেক্ষ।

বাস্তবে, দুর্বল সুরক্ষা মানদণ্ড গ্রহণের কারণে, অধিকাংশ অতিবিশাল জন-পরিষেবামূলক ব্যবস্থাগুলি যেমন, জাতীয় পরিচয় ব্যবস্থা [২০,১০,৩,৬,৪০], স্বাস্থ্যপঞ্জী[২১, ২২,২৩], জাতীয় নাগরিক ও ভোটার পঞ্জী[২৪,২৫,২৬], গণ ঋণ পঞ্জী[২৭,২৮], আয়[২৯] ও কর পঞ্জী[৩০] ইত্যাদি পঞ্জীগুলি ব্যক্তিপরিসর এবং ন্যায্যতার বিচারে যেমন সংশয়াতীত হয়ে উঠতে পারে নি, তেমনি সেগুলি চালু করার ক্ষেত্রেও নানান অসুবিধার সম্মুখীন হয়েছে।

যখনই সরকারের পক্ষ থেকে বৃহৎ জাতীয়-ডেটা সমন্বয়কারী প্রোজেক্ট শুরু করার চিন্তা এসেছে, তখনই সুরক্ষার রক্ষাকবচ নিয়ে উদ্বেগের ধুকপুকানি শুরু হয়েছে। মনে রাখতে হবে, এই ধরনের প্রোজেক্ট কী ভয়ঙ্কর রকম নজরদারি ব্যবস্থা কায়েম করতে সক্ষম। অনেক সময়ে এই ধরনের প্রোজেক্ট বাতিল হয়েছে শুধুমাত্র এই কারণে যে সেগুলি এ-জাতীয় বিপদের আশঙ্কা দূর করতে পারেনি[২১,২২,৩১]। ভারতেও, হালে কল্যাণমূলক প্রকল্প জনগণের কাছে পৌঁছে দেবার জন্য যে নতুন সরকারি ডেটাবেস এবং ডিজিটাল পরিকাঠামো তৈরি হয়েছে, সেগুলিকে ঘিরে সন্দেহ ও উদ্বেগ দানা বেধেঁছে[৩,৬,৪১]।

৪. ব্যক্তিপরিসর সুরক্ষার প্রচলিত ব্যবস্থাগুলির বিশ্লেষণ

ডিজিটাল ডাটাবেসে ব্যক্তিপরিসর সুরক্ষার আইনি প্রচেষ্টাগুলি মূলত আগাম নোটিশ দিয়ে এবং সম্মতিভিত্তিক সংগ্রহ (collection), উদ্দেশ্য (purpose) এবং স্টোরেজ সীমাবদ্ধতা, স্ব-ব্যবস্থাপনা[৩৩] , স্বচ্ছতা, নিয়ন্ত্রণ (regulation), প্রয়োগ (enforcement) ও জবাবদিহিতার (accountability) উপর ভিত্তি করে তৈরি হয়[৭,১০,৩২]। এই ব্যবস্থাগুলি কোথাও তেমন কার্যকর হয়নি। অন্য দিকে কম্পিউটার সায়েন্সের শৈলীগুলি, যা সাধারণত এনক্রিপশন এবং অ্যানোনিমাইজেশনের উপর নির্ভর করে, অনেক সময়ই ব্যক্তিপরিসর আর গোপনীয়তার মধ্যে পার্থক্য করে না, আর 'কাফকায়েস্ক'; সমস্যাগুলিকে মোটামুটি উপেক্ষাই করে। এখানে আমরা সেটাই বোঝার চেষ্টা করব।

৪.১ ব্যক্তিপরিসরের স্ব-ব্যবস্থাপনা (Privacy Self-Management)[৩৩]

ডিজিটাইজেশানে স্বেচ্ছাকৃত অংশগ্রহণের ক্ষেত্রে ব্যক্তিপরিসর সুরক্ষার জন্য সাধারণত নোটিশ, কনসেন্ট এবং অপ্ট-ইন ও অপ্ট-আউটের উপর নির্ভর করা হয়। কিন্তু, শ্রীকৃষ্ণ কমিটির[৭] মতে একদিকে বিকল্প ব্যবস্থার অভাব, অন্যদিকে অত্যধিক তথ্যের জন্য নোটিশ এবং কনসেন্ট ব্যবস্থা বেশিরভাগ সময়ই কার্যকরী হয় না, যার সাধারণ পরিণাম হলো গতানুগতিক ভাবে 'I Agree' ক্লিক করে দেওয়া। সচরাচরভাবে এটাকে তথ্যের অতিরিক্ত বোঝা বা 'ইনফর্মেশন ওভারলোড' এবং সম্মতি অবসাদ বা 'কনসেন্ট ফ্যাটিগ' বলা হয়। তথ্যের পরিমাণ ও জটিলতা কনসেন্টের নীতিকে অযৌক্তিক করে ফেলেছে। মূলত এই কারণে শ্রীকৃষ্ণ কমিটি কনসেন্টের বদলে একটি দায়িত্ব এবং অধিকার-নির্ভর নীতি প্রণয়নের প্রস্তাব রেখেছে। এতে ব্যক্তি সুরক্ষার দায়িত্ব এবং দায়বদ্ধতার গুরুত্বপূর্ণ খানিকটা অংশ ব্যবহারকারী ব্যক্তির থেকে ডেটা নিয়ন্ত্রণকারীর কাছে স্থানান্তরিত হয়ে যাবে। এটা অবশ্যই একটা প্রয়োজনীয় পদক্ষেপ হতে পারে, তবে এর জন্য একটি শক্তিশালী নিয়ন্ত্রক (regulatory) কাঠামো তৈরি হওয়া অতি আবশ্যক। কিন্তু ব্যক্তিপরিসর সুরক্ষা এবং তার উল্লঙ্ঘন শনাক্তকরণের কী পদ্ধতি হতে পারে, তা নিয়ে এখনো প্রশ্ন থেকেই যায়।

কনসেন্টের সার্থকতা নিয়ে প্রশ্ন থাকা সত্ত্বেও, যখনই কোনো বৈধ রাষ্ট্রস্বার্থ (লেজিটিমেট স্টেট ইন্টারেস্ট) ব্যতীত, উদ্দেশ্য বিস্তারের (পারপাস এক্সটেনশন) সম্ভাবনা থাকবে, তখন নোটিশ এবং কনসেন্টব্যবস্থা অবশ্যই প্রয়োজন। কিন্তু উদ্দেশ্য বিস্তারের প্রকৃত কারণ শনাক্তকরণ এবং রাষ্ট্র কর্তৃক তার স্বীকৃতিটাই সমস্যাযুক্ত হয়ে দেখা দেয়।

৪.২ ব্যাখ্যাপ্রাপ্তির অধিকার

আর্টিফিসিয়াল ইন্টেলিজেন্সের অ্যালগরিদমগুলি থেকে অনেক সময়ই ন্যায় বিবর্জিত বৈষম্যমূলক পরিণাম পাওয়া যায়, যার প্রতিকার হিসাবে ইউরোপিয়ান জিডিপিআর[২২] 'রাইট টু এক্সপ্লানেশনের'[৪২] প্রস্তাব দিয়েছে। কিন্তু এই মেশিন লার্নিং অ্যালগরিদমগুলির কাজের শৈলী অনেক সময়ই 'ব্ল্যাক-বক্স' প্রকৃতির, যার জন্য পরিণামের সঠিক কারণ নির্ধারণ করা অসম্ভব হয়ে পড়ে, আর ব্যাখ্যাগুলি বেশিরভাগ সময়ই অকেজো ও অর্থহীন হয়ে যায়। তা ছাড়াও মেশিন-লার্নিং-এর বিরূপ ফলাফলগুলি অধিকাংশ সময়ই 'কাফকায়েস্ক'খ; ধাঁচের, যে কারণে সবসময়ে তাৎক্ষণিক ক্ষতির অনুমান করা সম্ভব হয় না। ফলস্বরূপ অনেক সময় ব্যাখ্যা চাওয়াটাই মুশকিল হয়ে পড়ে।

৪.৩ নিয়ন্ত্রণ ও প্রয়োগ

ব্যক্তিপরিসরের মান (privacy standards) চালু করা আর জবাবদিহিতা (accountability) স্থির করার জন্য শ্রীকৃষ্ণ কমিটি[৭] একটি শক্তিশালী নিয়ন্ত্রক কাঠামো তৈরির প্রস্তাব রেখেছে। কাঠামোটি বর্তমানে প্রচলিত স্ব-নিয়ন্ত্রণ থেকে শুরু করে আরও কড়া 'কমান্ড অ্যান্ড কন্ট্রোল' পর্যন্ত হতে পারে, কমিটি যদিও মাঝামাঝি সহ-নিয়ন্ত্রণের পক্ষে। কিন্তু এই প্রস্তাবটি ধরে নিচ্ছে যে ব্যক্তিপরিসর উল্লঙ্ঘন সব সময় শনাক্ত করা সম্ভব। প্রস্তাবটি সমস্যাযুক্ত, কারণ ব্যক্তিপরিসর উল্লঙ্ঘনের কার্যকারণজনিত (causal effects) প্রভাব নির্দিষ্ট করা অধিকাংশ সময়ই কঠিন, বিশেষত যদি সেটা 'কাফকায়েস্ক'; ধরনের হয়। তাই ব্যক্তিপরিসর উল্লঙ্ঘন নির্ধারণ করাও কঠিন। উদাহরণস্বরূপ, এটা নিশ্চিত ভাবে জানা অসম্ভব যে অবৈধ ভাবে দেখা মেডিকেল রেকর্ডজনিত বৈষম্যের কারণে কেউ চাকরি হারিয়েছে, নাকি যে কারণ সরকারিভাবে দেখানো হয়েছে সেটাই সত্যি। আসলে ব্যাক্তিপরিসর নিয়ন্ত্রণ আর বাস্তব অবস্থা, এই দুইয়ের মধ্যেকার সম্পর্ক কখনোই সরলরৈখিক নয়।

৪.৪ এনক্রিপশন

পর্যাপ্ত শক্তিসম্পন্ন সিমেট্রিক বা 'পাবলিক কি'[৪৩] (symmetric or public key) ব্যবহার করে ক্রিপ্টোগ্রাফিক ডেটা এনক্রিপশন স্টোরেজ বা আদানপ্রদান (in storage or transit) ডেটার গোপনীয়তা সুরক্ষার জন্য একটি সফল ও জনপ্রিয় পদ্ধতি। কিন্তু এর জন্য 'কি'-গুলিকে নিরাপদে রাখা আবশ্যক। এনক্রিপশনের জন্য অভ্যন্তরীণ আক্রমণ (ইনসাইডার অ্যাট্যাক) একটা বড়ো ঝুঁকি, বিশেষত কি-গুলিও যদি ওই একই ডেটা কন্ট্রোলার কর্তৃপক্ষের হেফাজতে থাকে। কি-গুলি যদি বা নিরাপদে রাখা যায়, ডিক্রিপশনের সময় ওগুলিকে কম্পিউটারের মেমোরিতে আনা যেহেতু আবশ্যক, তখন ওগুলি বেহাত হতেই পারে। আপোষিত (compromised) অপারেটিং সিস্টেম বা হাইপারভাইসার (hypervisor) সফ্‌টওয়্যার থেকে 'কি' ফাঁস হওয়ার সম্ভাবনার জন্য, বিশেষত অভ্যন্তরীণ আক্রমণের দ্বারা, এনক্রিপশনের উপর পুরোপুরি নির্ভর করা সম্ভব নয়। তাছাড়া এনক্রিপশনের লক্ষ্য শুধু ডেটার গোপনীয়তার উপর, তাই 'কাফকায়েস্ক'; ব্যক্তিপরিসর উল্লঙ্ঘন বন্ধ করার জন্য এনক্রিপশন তেমন কার্যকর নয়।

৪.৫ অ্যানোনিমাইজেশন

অ্যানোনিমাইজেশন হচ্ছে ডাটাবেস রূপান্তরের একটি প্রযুক্তি, যার থেকে কারো আসল পরিচয় খুঁজে বের করা বা ট্রেস ব্যাক বা উৎস খোঁজা কঠিন হয়ে যায়। সাধারণত ডেটা প্রদর্শন করার আগে অ্যানোনিমাইজেশনের জন্য ব্যক্তিগত শনাক্তকারীগুলিকে হঠিয়ে দেওয়া হয় আর ডেটাতে বিভিন্ন প্রকারের দূষণ (নয়েজ) ঢালা হয়। কিন্তু প্রায় এক দশকের গবেষণা প্রমাণ করেছে যে অ্যানোনিমাইজেশন প্রকৃতপক্ষে মোটেই কাজ করে না। এক ব্যক্তি-সংক্রান্ত বিভিন্ন উৎস থেকে জোগাড় করা মামুলি তথ্য, যা কিনা আলাদা আলাদা ভাবে সম্পূর্ণ নিরীহ, তা কিন্তু একসঙ্গে মিলে ব্যক্তিটিকে সম্পূর্ণভাবে উন্মোচিত করে ফেলে[৩৫]। একাধিক তাত্ত্বিক গবেষণা এটাই প্রমাণ করেছে যে প্রকৃত অর্থে অ্যানোনিমাইজেশন অসম্ভব, যদি না এতটাই দূষণ মেশানো হয় যে ডেটার উপযোগিতাই শেষ হয়ে যায়[৩৫,৩৬]। কম্পিউটার সায়েন্স লিটারেচারে সোশ্যাল নেটওয়ার্ক ডেটা, লোকেশন ডেটা, লেখন শৈলী, ব্রাউজিং হিস্ট্রি ইত্যাদি থেকে অ্যানোনিমাইজেশন ভঙ্গের প্রচুর উদাহরণ আছে[৩৬,৩৭,৩৮,৩৯]।

সাধারণভাবে, যদি আক্রমণকারীর কাছে পর্যাপ্ত সহায়ক তথ্যের অনুপ্রবিষ্টনের সুযোগ থাকে তাহলে অ্যানোনিমাইজেশন ভঙ্গের বিরুদ্ধে কোনো নিশ্চয়তা দেওয়া সম্ভব হয় না[৪৪]। এই বিবেচনায় ব্যক্তিপরিসর সুরক্ষার জন্য একটি সম্পূর্ণ কাঠামোগত (আর্কিটেকচারাল) সমাধানের প্রয়োজন।

৫. একটি কাঠামোগত সমাধানের উপাদানসমূহ

কোনও ব্যক্তির ব্যক্তিপরিসর সুরক্ষার মূল উপায় হচ্ছে অপ্রয়োজনে তার পরিচয় প্রকাশ হওয়া থেকে রক্ষা করা, তার অজান্তে তাকে অননুমোদিত প্রোফাইলিং থেকে আড়াল করা এবং তার ডেটা অ্যাক্সেসের সমস্ত ফলাফল সম্পর্কে তাকে অবহিত করা। আমাদের মতে এই উদ্দেশ্যগুলি অর্জনের জন্য ডিজিটাল ডেটাবেসে নিম্নলিখিত কাঠামোগত বৈশিষ্ট্যগুলি অত্যন্ত গুরুত্বপূর্ণ।

৫.১ ভার্চুয়াল আইডেন্টিটি দ্বারা ব্যক্তিপরিসর সুরক্ষা

বিবিধ প্রয়োগক্ষেত্রে (applications) এবং সম্মুখমুখী ডেটাবেসগুলিব. (frontend databases) জন্য একটাই ব্যক্তিগত ডিজিটাল আইডেনটিটির ব্যবহার, ব্যক্তিপরিসর সুরক্ষার দৃষ্টিকোণ থেকে খুবই ঝুঁকিপূর্ণ। পৃথক প্রয়োগক্ষেত্রের জন্য পৃথক পৃথক পরিচয় ব্যবহার করা অনেক বেশি নিরাপদ, যার ফলে পৃথক প্রয়োগক্ষেত্রগুলির মধ্যে ব্যক্তিটির পারস্পরিক সম্পর্ক খুঁজে বের করা কঠিন হয়ে যায়। ক্রিপ্টোগ্রাফিকভাবে এই পৃথক পরিচয়গুলি একটি মাস্টার ডিজিটাল আইডেনটিটি বা পরিচয় থেকে সৃষ্টি করা যেতে পারে[৪৫]। এই ভার্চুয়াল পরিচয়গুলি থেকে অজ্ঞাত শংসাপত্রও (অ্যানোনিমাস ক্রেডেনশিয়াল) তৈরি হতে পারে, যাতে প্রমাণীকরণের (authentication) সময় তথ্য বিনিময় যথা সম্ভব কম হয়।

উদাহরণ হিসাবে ভাবা যায়, বিমানযাত্রার জন্য মিউনিসিলিটি থেকে কেউ একজন

অজ্ঞাত শংসাপত্র ও না-দেখা স্বাক্ষর (ব্লাইন্ড সিগনেচার)[৪৬] দিয়ে একটি কোভিড ভ্যাক্সিন-সংক্রান্ত শংসাপত্র নিয়ে তারপর অন্য একটি ভার্চুয়াল পরিচয়কে ব্যবহার করে বিমানসেবা কোম্পানির কাছে জমা দিতে সক্ষম হচ্ছেন। প্রদত্ত একটি স্বাক্ষর করা দলিলকে (সার্টিফিকেট) সেই ব্যক্তিরই অন্য একটি ভার্চুয়াল পরিচয়ের জন্যে রূপান্তরিত করা যেতে পারে। এতে করে দলিল প্রদানকারী প্রথম কর্তৃপক্ষ জানতে পারবে না কোথায় দলিলটি ব্যবহার করা হলো, এবং দ্বিতীয় কর্তৃপক্ষ—যাকে দলিলটি দেওয়া হলো—জানতে পারবে না ব্যক্তিটির আসল পরিচয়। এই আন-লিঙ্কেবিলিটি (un-linkability) ও আন-ট্রেসেবিলিটি (un-traceability) এমন ভাবেও করা যেতে পারে, যা প্রয়োজনে অনুমোদন থাকলে ভাঙাও যেতে পারে। এই রকম অনুমোদন কানুনি বা বৈধ বিশ্লেষণের প্রয়োজনে দেওয়া যেতে পারে।

একই কর্তৃপক্ষের সঙ্গেও বার বার লেনদেন করার জন্য ভিন্ন ভিন্ন ভার্চুয়াল পরিচয়ও (ওয়ান-টাইম ক্রেডেনশিয়াল) ব্যবহার করা যেতে পারে। এতে সংশ্লিষ্ট কর্তৃপক্ষের পক্ষে ব্যক্তিটির উপর বিভিন্ন সময়ের তথ্য একত্র করা কঠিন হয়ে যায়। এছাড়াও, ব্যক্তিপরিসর সুরক্ষার জন্য সম্মুখমুখী ডেটাবেসে অথবা কোনো ওয়েবপেজে নাম এবং ঠিকানার মতো কোনও দুর্বল শনাক্তকারী (weak identifier) ব্যবহার না করাও আবশ্যক। এই সব ক্ষেত্রে শুধু ভার্চুয়াল পরিচয়ই ব্যবহার করা উচিত।

এইসব সুরক্ষা নিশ্চিত করতে সাধারণ মানুষের জন্য ভার্চুয়াল পরিচয় উৎপন্ন করার নিরাপদ, সহজ এবং ব্যবহারযোগ্য পদ্ধতি সৃষ্টি করা অতি আবশ্যক।

৫.২ অনুমোদন, অ্যাক্সেস নিয়ন্ত্রণ এবং উদ্দেশ্য নিয়ন্ত্রণের জন্য অনলাইন নিয়ন্ত্রক কাঠামো

ব্যক্তিপরিসর লঙ্ঘন রোধ করতে নিয়ামক কর্তৃপক্ষের (রেগুলেটর) প্রয়োজন শুধু তত্ত্বাবধান করার জন্য নয়, ডেটা সুরক্ষা কাঠামোতে নিয়ামক কর্তৃপক্ষের সক্রিয় অনলাইন উপস্থিতিও জরুরি। অভিযোগের প্রতিকার করা ছাড়াও, তাদের আরও দুটি প্রধান ভূমিকা পালনের দায়িত্ব থাকা উচিত।

প্রথম ভূমিকাটি হওয়া উচিত আইনি অনুমোদনের বা সম্মতির ভিত্তিতে স্পষ্টভাবে নির্ধারণ করা যে কে কোন ডেটা কী উদ্দেশ্যে অ্যাক্সেস করতে পারবে। উদ্দেশ্য নিয়ন্ত্রণ (purpose limitation) এই জাতীয় অনুমোদনের একটি গুরুত্বপূর্ণ উপাদান হওয়া প্রয়োজন, এবং সমস্ত ক্ষেত্রে উদ্দেশ্য বিস্তৃতির আবেদন এবং সম্মতি পুনর্নবীকরণ ব্যবস্থাগুলি বিশদভাবে বিবেচনা করাও নিয়ামকের অন্যতম প্রধান দায়িত্ব হওয়া উচিত। ব্যক্তিগত ডেটাতে এ-জাতীয় অ্যাক্সেসের অধিকারগুলি কেবল পরিচালনা, তদন্ত এবং নিরীক্ষণের উদ্দেশ্যেই নয়, ডেটা মাইনিংয়ের অ্যালগরিদমিক অ্যাক্সেস দেওয়ার জন্যও বিবেচিত হওয়া অতি প্রয়োজন। অ্যালগরিদম ডিজাইনের ন্যায্যতা (fairness) নির্ণয়ের প্রয়াসে সাম্প্রতিক কালে প্রচুর অগ্রগতি সত্ত্বেও, ন্যায্যতার গ্যারান্টি সর্বদা সম্ভব হয় না[৪০]। অতএব অ্যালগরিদমগুলির ন্যায্যতা নির্ধারণ এবং ব্যবহারের ক্ষেত্রে সেগুলির হাতে কলমে যাচাই-বাছাই অপরিহার্য।

স্থিতিশীল বিধি এবং অনলাইন সম্মতির কাঠামো অনুসারে অ্যাক্সেসের অধিকারগুলি স্পষ্টভাবে সংজ্ঞায়িত এবং ডিজিটালি কোড করার পরে, নিয়ামকের দ্বিতীয় গুরুত্বপূর্ণ ভূমিকাটি হওয়া উচিত এটা নিশ্চিত করা যে কেবলমাত্র নিরীক্ষিত, প্রাক্-অনুমোদিত এবং ডিজিটালি স্বাক্ষরিত কম্পিউটার প্রোগ্রামের মাধ্যমেই ডেটা অ্যাক্সেস করা যেতে পারে। এর জন্য অ্যাক্সেসের অনলাইনে প্রমাণীকরণ ও অনুমোদনের যাচাইকরণের ব্যবস্থা থাকা আবশ্যক। অ্যাক্সেস প্রোগ্রামগুলির সততা প্রমাণের মাধ্যমে নিয়ন্ত্রকদের এটাও নিশ্চিত করতে হবে যে অ্যাক্সেস-করা ডেটা কেবলমাত্র অনুমোদিত উদ্দেশ্যেই ব্যবহৃত হচ্ছে। এর জন্য প্রোগ্রামগুলিকে নিরীক্ষা, অনুমোদন এবং ডিজিটালি স্বাক্ষর করা আবশ্যিক হওয়া দরকার, যাতে চালু অবস্থায় প্রোগ্রামগুলিকে বদলানো না যেতে পারে। কাঠামোতে এটা নিশ্চিত করতে হবে যে ডেটা নিয়ামক এবং ডেটা কন্ট্রোলার কেউই যেন একক ভাবে ডেটা অ্যাক্সেস না করতে পারে এবং উভয়েই যেন সমস্ত অ্যাক্সেসের হিসাব রাখে যাতে পরবর্তী নিরীক্ষা সম্ভব হয়। পরিশেষে, স্বচ্ছতার স্বার্থে, ব্যক্তিগত তথ্য অ্যাক্সেসের সমস্ত ফলাফল সর্বদা স্বয়ংক্রিয়ভাবে ব্যক্তিগত চ্যানেলের মাধ্যমে সংশ্লিষ্ট ব্যক্তিদের কাছে পৌঁছে দিতে হবে।

এই জাতীয় অনলাইন নিয়ন্ত্রক ক্রিয়াকলাপগুলিকে উপলব্ধ করার জন্য প্রযুক্তিগুলি তৈরি করতে হবে বিদ্যমান কম্পিউটার বিজ্ঞানভিত্তিক কৌশলগুলির উপর নির্ভর করে[৬]। এর জন্য প্রয়োজন একটি কার্যকরী ও অধিকার-ভিত্তিক ডেটা সুরক্ষা আইন গঠনের। সর্বোপরি, কার্যকরী নিয়ন্ত্রক ক্ষমতা গড়ার ইচ্ছাশক্তিও থাকতে হবে।

৬. উপসংহার

ডিজিটাল ডেটাবেসে ব্যক্তিপরিসর সুরক্ষা এটা দাবি করে না যে ডেটা সংগ্রহ, সংরক্ষণ বা ব্যবহার অনুচিত, তবে এমন নিশ্চয়তা থাকা উচিত যে ডেটা কেবলমাত্র অনুমোদিত এবং বৈধ উদ্দেশেই ব্যবহার করা যেতে পারে। আমাদের যুক্তি হচ্ছে যে ব্যক্তিপরিসর লঙ্ঘন শনাক্তকরণের ভিত্তিতে শুধুমাত্র একটি নিষ্ক্রিয় নিয়ামক কাঠামো এবং কনসেন্ট, উদ্দেশ্য নিয়ন্ত্রণ এবং স্বচ্ছতার নীতিগুলির ভিত্তিতে প্রচলিত পদ্ধতিগুলির সফল হওয়ার সম্ভাবনা কম। এই মানক পদক্ষেপগুলি ছাড়াও এখানে অনুমোদনের অনলাইন বৈধতা নির্ধারণ এবং অ্যাক্সেস নিয়ন্ত্রণের ভিত্তিতে একটি আর্কিটেকচারাল সমাধানেরও পক্ষে প্রস্তাব রাখা হয়েছে।

তথ্যসূত্র

1. The Puttaswamy judgment, 2017. K S Puttaswamy v Union of India (2017): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 24 August, 2017. URL https://www.scobserver.in/ court-case/ fundamental-right-to-privacy. [Accessed January 9, 2018].
2. The Puttaswamy judgment, 2017. K S Puttaswamy v Union of India (2018): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 26 September, 2018. URL https://www.scobserver. in/court-case/ constitutionality-of-aadhaar-act. [Accessed December 9, 2019].
3. Reetika Khera. Dissent on Aadhaar: Big Data Meets Big Brother. Orient BlackSwan, 2019. ISBN 9789352875429. Edited volume.
4. Nova Spivack. The Post-Privacy World, 2013. URL https://www.wired.com/ insights/2013/07/the-post-privacy-world/. [Accessed January 9, 2018].
5. Gautam Bhatia. The Supreme Court's Right to Privacy Judgment. Economic and Political Weekly, Vol. 52 (Issue No. 44), 04 2017.
6. Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma. Privacy and Security of Aadhaar: A Computer Science Perspective. Economic and Political Weekly, Vol. 52 (Issue No. 37), 16, 2017.
7. B. N. Srikrishna, Aruna Sundararajan, Ajay Bhushan Pandey, Ajay Kumar, Rajat Moona, Gulshan Rai, Rishikesha Krishnan, Arghya Sengupta, and Rama Vedashree. White Paper of the Committee of Experts on a Data Protection Framework for India, 2017. URL http://meity.gov.in/writereaddata/ files/ whitepaperondataprotectioninindia171127finalv2.pdf. [Online; Accessed January 9, 2018]
8. Daniel J. Solove. The Digital Person: Technology And Privacy In The Information Age. New York University Press, New York, NY, USA, 2004. ISBN 0814798462.
9. Malavika Raghavan. Before The Horse Bolts, January 2018. URL https:/ /www.thinkpragati. com/think/brainstorm/3180/before-the-horse-bolts/.
10. The London School of Economics and Political Science. The Identity Project: An assessment of the UK Identity Cards Bill and its implications. http://eprints.lse.ac.uk/29117/, June 2005.
11. Thomas McMullan. What does the panopticon mean in the age of digital surveillance?https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance- jeremy-bentham, July 2015.
12. The European Parliament and the Council of European Union. Regulation (EU) no 2016/679, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=celex% 3A32016R0679.
13. Jean Drèze. The Aadhaar coup. http://www.thehindu.com/opinion/lead/jean-drezeon- aadhaar-mass-surveillance-data-collection/article8352912.ece, 2016. [Online; posted 15- March-2016].
14. Nicholas Confessore. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, 2018. URL https://www.nytimes.com/2018/04/04/us/ politics/cambridge- analytica-scandal-fallout.html. [Online; posted 04-April-2018].
15. Subhashis Banerjee. A Welfare Test for Aadhaar, 2017. URL http:// indianexpress.com/ article/opinion/columns/a-welfare-test-for-aadhaar-upa-nda-aadhaarcard-4921582/. [Online; posted 4-November-2017].
16. Cathy O'Neil. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group, New York, NY, USA, 2016. ISBN: 0553418815, 9780553418811.
17. Virginia Eubanks. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, Inc., USA, 2018. ISBN: 1250074312.
18. Jim Thatcher, David O'Sullivan, and Dillon Mahmoudi. Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data. Environment and Planning D: Society and Space, 34(6):990-1006, 2016. doi:10.1177/0263775816633195.URLhttps://doi.org/10.1177/ 0263775816633195.
19. Shoshana Zuboff. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. 1st edition, 2018. ISBN 1610395697.
20. Unique Identification Authority of India. Aadhaar. https://uidai.gov.in, 2020. [Accessed May 31, 2020].
21. James Temperton. NHS care.data scheme closed after years of controversy. https://www.wired.co. uk/article/care-data-nhs-england-closed, 2016. [Online July 6, 2016].
22. Robert N. Charette. Australians Say No Thanks to Electronic Health Records. https://spectrum.ieee.org/riskfactor/computing/it/australians-choosingto-optout-of- controversial-my-health-record-system, 2018. [Online July 27, 2018].
23. Siddarth Shrikanth and Benjamin Parkin. India plan to merge ID with health records raises privacy worries. https://www.ft.com/content/4fbb2334-a864-11e9-984c-fac8325aaa04, July 2019. [Online; posted 17-July-2019].
24. Kim Zetter. Voter Privacy Is Gone - Get Over It. https://www.wired.com/ 2008/01/voterprivacy-i/, 2008. [Online January 31, 2008].
25. Purnima S. Tripathi. Concerns over linking Aadhaar to voter ID and social media accounts. https:// frontline.thehindu.com/the-nation/article 29407553 .ece, September 2019. [Online; posted 27-Septeber-2019].
26. Monica Pal. Are citizens compromising their privacy when registering to vote? https://gcn.com/ articles/2018/12/11/voting-data-privacy.aspx, 2018. [Online; posted December 11, 2018]

1269, Republic and Canton of Geneva, Switzerland, 2017. International World Wide Web Conferences Steering Committee. ISBN 978-1-4503-4913-0. doi: 10.1145/3038912.3052714. URL https://doi.org/10.1145/3038912.3052714.

38. Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen, and Vincent D Blondel. Unique in the´ Crowd: The privacy bounds of human mobility. Scientific Reports, 3, 2013.
39. Arvind Narayanan, Elaine Shi, and Benjamin I. P. Rubinstein. Link Prediction by De- anonymization: How We Won the Kaggle Social Network Challenge. https://arxiv.org/pdf/1102.4374.pdf, 2011.
40. Jon M. Kleinberg, Sendhil Mullainathan, and Manish Raghavan. Inherent trade-offs in the fair determination of risk scores. CoRR, abs/1609.05807, 2016. URL http://arxiv.org/abs/1609.05807.
41. Subhashis Banerjee and Subodh Sharma. Privacy concerns with Aadhaar. Commun. ACM, 62(11):80, October 2019. ISSN 0001-0782. doi: 10.1145/3353770. URL https://doi.org/10.1145/3353770.
42. Andrew D Selbst and Julia Powles. Meaningful information and the right to explanation. International Data Privacy Law, 7(4):233-242, 2017. doi: 10.1093/idpl/ipx022. URL http://dx.doi.org/10. 1093/idpl/ipx022.
43. Gustavus J. Simmons. Symmetric and asymmetric encryption. ACM Comput. Surv., 11(4):305-330, December 1979. ISSN 0360-0300. doi: 10.1145/356789.356793. URL http://doi.acm.org/10.
44. Cynthia Dwork. Differential Privacy. In Proceedings of the 33rd International Conference on Au- tomata, Languages and Programming - Volume Part II, ICALP'06, pages 1-12, Berlin, Heidelberg, 2006. Springer-Verlag. ISBN 3-540-35907-9, 978-3-540-35907-4. doi: 10.1007/11787006 1. URL http://dx.doi.org/10.1007/11787006 1.
45. David Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Commun. ACM, 28(10):1030-1044, October 1985. ISSN 0001-0782. doi: 10.1145/4372.4373. URL http://doi.acm.org/10.1145/4372.4373.
46. David Chaum. Blind Signatures for Untraceable Payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, Advances in Cryptology, pages 199-203, Boston, MA, 1983. Springer US. ISBN 9781-4757-0602-4.

27. epic.org. Equifax Data Breach. https://epic.org/privacy/data-breach/equifax/, 2019. [Online accessed 3-November-2019].
28. Beni Chugh and Malavika Raghavan. The RBI's proposed Public Credit Registry and its implications for the credit reporting system in India. https://www.dvara.com/blog/2019/06/18/therbis-proposed-public-credit-registry-and-its- implications-for-thecredit-reporting-system-in-india/, 2019. [Online posted 18-June-2019].
29. Yle Uutiset. Launch of Incomes Register dogged by data security concerns. https://yle.fi/uutiset/osasto/news/launch_of_incomes_register_dogged_by_data_security_conc erns/10576057, 2018. [Online posted 30 December-2018].
30. Kimberly Houser and Debra Sanders. The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know it? Vanderbilt Journal of Entertainment & Technology Law, 19(4), April 2017. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2943002.
31. GOV.UK Press Release. National identity register destroyed as government consigns ID card scheme to history. https://www.gov.uk/government/news/national-identity-registerdestroyed-as-government-consigns-id-card-scheme-to-history, 2011. [Online posted 10-February-2011].
32. The Planning Commission: Government of India. Report of the group of experts on privacy chaired by Justice A P shah. http://planning commission .nic.in/reports/genrep/repprivacy. pdf, December 2011.
33. Daniel J. Solove. Privacy Self-management and the Consent Dilemma. Harvard Law Review, 126(1880), 2012. URL https://papers.ssrn.com/sol3/papers.cfm?abstractid=2171018.
34. Arvind Narayanan and Vitaly Shmatikov. Robust De-anonymization of Large Sparse Datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, SP '08, pages 111-125, Washington, DC, USA, 2008. IEEE Computer Society. ISBN 978-0-7695-3168-7. doi: 10.1109/SP.2008.33. URL https://doi.org/10.1109/SP.2008.33.
35. Anupam Datta, Divya Sharma, and Arunesh Sinha. Provable De-anonymization of Large Datasets with Sparse Dimensions. In Pierpaolo Degano and Joshua D. Guttman, editors, Principles of Security and Trust, pages 229-248, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-28641-4.
36. A. Narayanan, H. Paskov, N. Z. Gong, J. Bethencourt, E. Stefanov, E. C. R. Shin, and D. Song. On the Feasibility of Internet-Scale Author Identification. In 2012 IEEE Symposium on Security and Privacy, pages 300-314, May 2012. doi: 10.1109/SP.2012.46.
37. Jessica Su, Ansh Shukla, Sharad Goel, and Arvind Narayanan. De-anonymizing Web Browsing Data with Social Networks. In Proceedings of the 26th International Conference on World Wide Web, WWW '17, pages 1261-