Une voie indienne vers la souveraineté des données : L'architecture DEPA

Juin 2026

ISPIRT

Inria FONDATION

Présentation

Depuis 2013, l'Inde a engagé une transformation numérique d'une ampleur et d'une cohérence remarquables. À travers une série de projets — identité numérique avec Aadhaar, paiements instantanés avec UPI, commerce ouvert avec ONDC, consentement et partage de données avec DEPA — elle a construit ce qu'on appelle désormais l'*India Stack*, ou Infrastructures Publiques Numériques. Ces projets ont leurs spécificités, mais ils partagent des caractéristiques profondes : une philosophie du numérique mûrement réfléchie, une rigueur d'exécution certaine, et une ambition constante — construire des protocoles ouverts au service de l'intérêt général, sans sacrifier l'innovation ni la souveraineté.

Les résultats sont notables. UPI a bancarisé plusieurs centaines de millions de personnes en quelques années et génère aujourd'hui plus de transactions électroniques que la Chine et les États-Unis réunis. ONDC a permis à des milliers de petits commerçants d'accéder au commerce numérique sans passer par une plateforme dominante. Ces avancées résultent d'un choix délibéré de construire des infrastructures partagées, interopérables, gouvernées comme des biens communs — un choix dont les limites et les conditions de succès méritent d'être analysées avec soin.

L'Europe a tout intérêt à analyser, à comprendre, et sans doute à s'inspirer de ce mouvement. Ces approches suggèrent qu'il existe une voie entre le modèle américain des grandes plateformes privées et le modèle chinois des

super-applications intégrées : une voie où l'action publique dynamise le marché au lieu de le freiner, où l'interopérabilité limite le verrouillage par les acteurs dominants, et où une certaine souveraineté démocratique sur les données et les règles du jeu peut être préservée. C'est précisément le débat que l'Europe peine encore à trancher.

Le projet DEPA (*Digital Empowerment and Protection Architecture*) s'inscrit dans cette lignée. Initié par le ministère indien de l'Électronique et des Technologies de l'Information (MeitY) et développé par iSPIRT Foundation, il est publié en open source et se veut une ressource évolutive — toute personne ou institution souhaitant y contribuer est invitée à le faire via github.com/iSPIRT/DEPA. Conçu d'abord pour le partage consenti de données financières, DEPA s'étend aujourd'hui à l'entraînement des modèles d'IA — l'un des enjeux les plus aigus de notre époque. Le présent document, issu de la publication originale d'iSPIRT, en présente l'architecture et la philosophie.

La Fondation Inria suit de près ces travaux, et la France a contribué en mettant à disposition un expert technique permanent aux côtés des équipes d'iSPIRT depuis l'automne 2023.

C'est dans ce cadre que la France s'intéresse aux applications franco-indiennes de DEPA, notamment dans le domaine de la santé. Le projet Sada Santé réunit ainsi l'Indian Council of Medical Research (ICMR) soutenu au niveau technique par iSPIRT et, côté français, la Plateforme des Données de Santé (French Health Data Hub) dont l'Inria est membre de la gouvernance. Son ambition est de démontrer qu'un transfert transfrontalier de données,

permettant l'hébergement sécurisé de données médicales sensibles indiennes en France est non seulement possible, mais maîtrisable techniquement et juridiquement. Plus qu'une simple expérimentation, Sada Santé constitue la première traduction opérationnelle des principes portés par DEPA dans un contexte international.

Il apporte une preuve concrète que les différentes régulations nationales de protection des données peuvent être articulées entre elles, au bénéfice de la recherche et des patients. La souveraineté et la coopération internationale ne sont pas contradictoires : Sada Santé montre qu'elles peuvent se renforcer mutuellement.

Si les preuves de concept sont concluantes, Sada Santé a vocation à s'étendre à un cadre Europe-Inde, contribuant ainsi à faire de l'Europe un acteur à part entière de cette nouvelle génération d'infrastructures publiques numériques.

Si ces preuves de concept aboutissent, SadaSanté a vocation à s'étendre à un cadre Europe-Inde — une perspective qui pourrait contribuer à faire de l'Europe un acteur sérieux de cette nouvelle génération d'infrastructures publiques numériques.

Henri Verdier Directeur général, Fondation Inria

Introduction

Pendant la majeure partie de la dernière décennie, chez iSPIRT, nous avons posé une seule et même question à chaque initiative numérique publique que nous avons mise en place ou soutenue : à quoi ressemblerait cette initiative, si elle était conçue non pas comme un produit, mais comme un protocole ? Les réponses à cette question ont façonné l'architecture que l'Inde partage aujourd'hui avec le monde entier, et elles constituent le fondement philosophique des travaux présentés dans ce manuel.

Un protocole se distingue d'un produit sur trois points essentiels. Il est interopérable du fait de sa conception, de sorte qu'aucun acteur ne peut s'approprier la couche qu'il occupe. Il est régi de manière ouverte, de sorte que son évolution relève d'une délibération publique plutôt que d'une décision commerciale. Enfin, il est souverain dans son fonctionnement tout en restant ouvert au niveau de l'interface, de sorte que le pays qui le gère en conserve le contrôle réglementaire, tout en accueillant les contributions de tout développeur souhaitant créer de la valeur par-dessus, et les innovations qui en découlent.
L'Inde a mis ces principes en œuvre à grande échelle. MOSIP, notre infrastructure d'identité numérique, est désormais opérationnelle dans vingt-sept pays. UPI, notre infrastructure de paiement, est en cours de déploiement en France. DEPA est le troisième volet de ce même cadre, consacré cette fois-ci aux données. Il est décrit en détail dans les chapitres qui suivent.

Le discours dominant actuel sur l'intelligence artificielle met l'accent sur le développement des capacités de calcul et

l'entraînement de modèles toujours plus volumineux. Cela ne représente qu'une partie du tableau. L'autre partie, moins visible sur les marchés financiers mais plus déterminante pour l'intérêt général, réside dans l'élaboration des protocoles permettant à l'IA de fonctionner au-delà des frontières institutionnelles, juridictionnelles et nationales. L'Inde s'est engagée dans cette seconde partie du tableau, et nous pensons que l'Europe l'est également.

La DEPA revêt une importance capitale dans ce contexte. La valeur de l'intelligence artificielle au cours de la prochaine décennie ne sera pas créée à partir de données provenant de l'internet public, mais grâce à une collaboration sécurisée et respectueuse de la vie privée sur des données d'entraînement privées. L'infrastructure juridique et technique permettant à un modèle d'apprendre à partir de ces données sans que celles-ci ne quittent jamais leur dépositaire n'existe pas encore en tant que norme mondiale. L'Inde et l'Europe peuvent en construire une ensemble.

Le lecteur découvrira un ensemble de mécanismes : des environnements informatiques confidentiels que même l'opérateur ne peut pas consulter ; des contrats électroniques qui intègrent le droit de la juridiction concernée dans le protocole lui-même ; et des garanties mathématiques de confidentialité qui empêchent la réidentification de tout individu à partir de n'importe quel résultat. Ensemble, ils permettent aux institutions de différents pays d'entraîner des modèles sur les données des unes et des autres sans jamais en transférer la gestion.

La collaboration franco-indienne autour du projet DEPA, et plus particulièrement le projet SadaSanté, constituent les premières manifestations concrètes de cette convergence.

Nous tenons à remercier la Fondation Inria, Henri Verdier, le Health Data Hub, le Conseil indien de la recherche médicale, ainsi que les institutions médicales des deux pays qui se sont engagées de bonne foi dans ce travail. La confiance qu'ils se sont mutuellement accordée est le fondement sur lequel tout le reste repose.

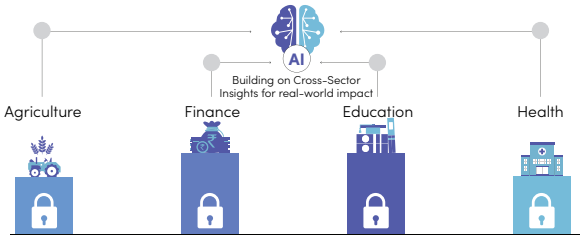
Ce manuel s'inscrit dans ce même esprit. Il ne s'agit pas d'un cahier des charges, mais d' une invitation à construire avec nous.

Sharad Sharma
Co-fondateur, iSPIRT

Résumé

01. Le goulet d'étranglement des données

L'intelligence artificielle repose fondamentalement sur des données d'entraînement massives, diversifiées et de qualité. L'Inde en produit en abondance — dans la santé, la finance, l'éducation, l'agriculture — mais ces données restent largement inaccessibles : risques de vie privée, risques institutionnels, absence de cadres de confiance, analyse coût-bénéfice défavorable. Ce «goulet d'étranglement» n'est pas un problème technique mineur : sans y remédier, l'innovation est freinée, les biais des modèles s'aggravent, et la concentration du marché s'accentue au profit des grands acteurs mondiaux. *DEPA Inférence*, qui encadre le partage consenti de données individuelles via les Agrégateurs de Comptes, a constitué une première réponse importante. Mais elle ne suffit pas pour l'entraînement de l'IA, qui requiert l'agrégation sécurisée de données à grande échelle — un défi fondamentalement différent.

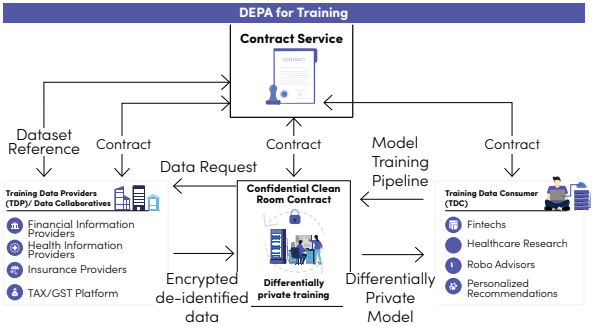


Unlockink India's AI potential requires intra and inter-sectoral collaboration on training data

02. L'architecture *DEPA Entraînement*

DEPA Entraînement est l'Infrastructure Publique Numérique indienne pour l'IA. Elle organise la collaboration entre Fournisseurs de Données d'Entraînement — hôpitaux, banques, organismes publics — et Consommateurs de Données d'Entraînement — startups, chercheurs, régulateurs — au sein d'un écosystème structuré et décentralisé, animé par des Collectifs de Données sectoriels.

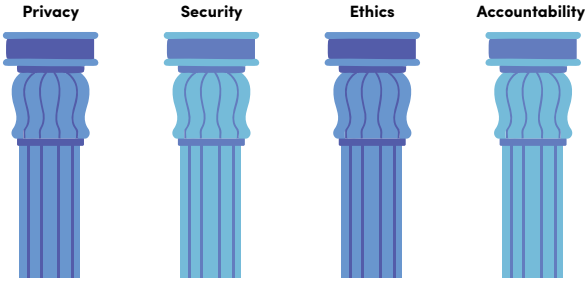
Sa force tient à trois piliers techniques intégrés dès la conception : les contrats électroniques lisibles par machine, qui automatisent l'application des conditions de partage ; les Salles Blanches Confidentielles, environnements d'exécution sécurisés où les données ne sont jamais exposées sous leur forme brute ; et la Confidentialité Différentielle, technique mathématiquement robuste qui garantit qu'aucun individu ne peut être réidentifié à partir des résultats d'un modèle. L'anonymisation traditionnelle ne suffit pas — DEPA le démontre et y répond.



03. Une approche techno-légale de la gouvernance de l'IA

Les réglementations statiques ne peuvent suivre le rythme d'une technologie aussi évolutive que l'IA. DEPA propose une réponse originale : intégrer la conformité dans l'architecture technique elle-même, plutôt que de la laisser à la bonne volonté des acteurs ou à des contrôles manuels. Contrats électroniques, Salles Blanches Confidentielles, Confidentialité Différentielle et architecture Zero Trust forment ensemble un système de responsabilité en boucle fermée — la conformité non comme frein, mais comme moteur de l'innovation.

Ce cadre est conçu pour s'articuler avec les grandes réglementations nationales et internationales — DPDP Act indien, RGPD européen, AI Act — et avec les lois sectorielles comme HIPAA ou Bâle III. Sa gouvernance repose sur un organe multipartite — fournisseurs, consommateurs, société civile, experts — chargé de l'accréditation, de la certification des modèles et du règlement des litiges.



04. Opportunités de marché

En levant l'impasse sur les données d'entraînement, DEPA peut générer une valeur économique considérable. Dans la santé, il ouvre la voie à la médecine de précision, à l'épidémiologie prédictive et à la découverte de médicaments. Dans les services financiers, il permet de construire des modèles de crédit alternatifs pour les 400 millions de personnes et PME aujourd'hui exclues du crédit formel. Dans l'éducation, il rend possible l'apprentissage adaptatif à grande échelle et la reconnaissance portable des compétences.

Au-delà de l'Inde, DEPA ambitionne de devenir un modèle exportable — une Infrastructure Publique Numérique de deuxième génération, conçue non pour les transactions mais pour la confiance, et susceptible d'être adoptée par d'autres nations et consortia internationaux.

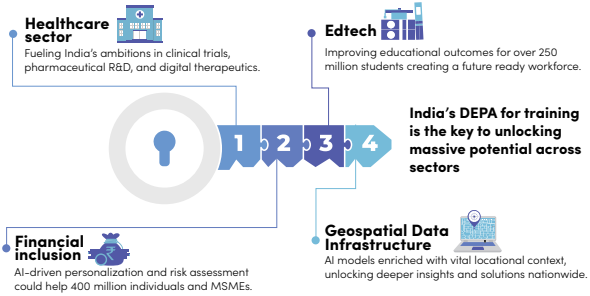


Table des matières

01. Le goulet d'étranglement des données

1.1 Comprendre le rôle crucial des données d'entraînement

L'intelligence artificielle (IA) transforme rapidement les industries, les économies et les sociétés du monde entier. De l'alimentation des moteurs de recommandation et de l'aide au diagnostic médical à l'optimisation des chaînes d'approvisionnement et la conduite de véhicules autonomes, le potentiel de l'IA semble illimité. Cependant, le moteur de cette révolution — le carburant même qui permet aux modèles d'IA d'apprendre, de s'adapter et d'accomplir des tâches complexes — ce sont les données. Plus précisément, l'IA repose fortement sur des données d'entraînement massives, diversifiées et de haute qualité.

Qu'est-ce que les données d'entraînement ?

Il s'agit de la collection organisée d'informations utilisée pour adapter ou optimiser un modèle d'IA. Pour un modèle d'IA, ces données comprennent de nombreux exemples. Dans un contexte supervisé, chaque point de données contient généralement une entrée et la sortie souhaitée, ou une étiquette identifiant la catégorie de ce point de données. Par exemple, entraîner un modèle d'IA à identifier des tumeurs dans des images médicales nécessite de lui présenter des milliers d'images, certaines étiquetées « tumeur détectée » et d'autres « aucune tumeur détectée ». En revanche, dans un contexte non supervisé — par

exemple pour construire un modèle de détection de fraude financière —, le modèle d'IA doit être exposé à des millions de transactions. Celles qui s'écartent de la distribution peuvent être classées comme frauduleuses ou illégitimes.

Il est important de noter qu'une caractéristique cruciale des données d'entraînement, notamment pour la construction de modèles sophistiqués tels que les grands modèles de langage (LLM) ou les systèmes prédictifs complexes, réside dans leur nature agrégée. Bien qu'elles proviennent de points de données individuels (comme une transaction unique, une image médicale spécifique ou le clic d'un utilisateur), leur puissance réside dans les tendances collectives, les corrélations et les propriétés statistiques qui n'émergent que lorsque l'on analyse les données en masse. Un modèle d'IA qui apprend les tendances du marché ne se concentre pas sur l'achat d'une seule personne ; il apprend du comportement d'achat combiné de millions d'individus. De même, un modèle d'IA de diagnostic médical apprend des tendances à partir des dossiers de santé agrégés d'innombrables patients, et non pas seulement de l'historique d'un seul individu.

C'est là que la distinction entre entraînement et inférence devient cruciale. L'inférence en IA désigne le processus d'application d'une intelligence préexistante — c'est-à-dire d'un modèle déjà entraîné — pour effectuer une prédiction ou prendre une décision à partir d'un point de données d'entrée pouvant être reçu individuellement. Un exemple concret est l'utilisation de vos données bancaires personnelles, accessibles via un cadre basé sur le consentement comme celui de l'Account Aggregator de DEPA, pour obtenir (ou non) une offre de prêt pré-approuvée à l'aide d'un modèle de notation de crédit existant. L'entraînement de l'IA, quant

à lui, désigne le processus fondamental de construction de l'intelligence du modèle. Cela nécessite d'alimenter le système avec d'énormes quantités de données, lui permettant ainsi d'apprendre les tendances statistiques, les corrélations et les enseignements tirés de l'information collective — la valeur résidant dans ce vaste panorama statistique constitué par les données agrégées. C'est ainsi que les détails granulaires d'un individu, observés au sein d'une sous-population entière, deviennent significatifs pour le modèle.

En conclusion, l'entraînement vise à construire une intelligence à partir de données agrégées à grande échelle, tandis que l'inférence consiste à appliquer cette intelligence à des entrées ou points de données spécifiques pour la prise de décision. Comprendre cette différence fondamentale et cette complémentarité — le besoin de données agrégées à grande échelle pour l'entraînement, et de données individuelles pour l'inférence — est la première étape pour saisir les défis uniques que *DEPA Entraînement* relève en rendant les données d'entraînement collectives accessibles en toute sécurité à l'innovation.

Les données d'entraînement sont la collection organisée d'informations utilisée pour adapter un modèle d'IA.

1.2 Pourquoi les données d'entraînement les plus précieuses sont-elles typiquement inaccessibles ?

L'Inde se trouve à un tournant singulier. Portée par une numérisation rapide de tous les secteurs, stimulée par des écosystèmes numériques développés en interne, le pays génère des données à une échelle sans précédent. Des dossiers médicaux dans les hôpitaux et cliniques aux

transactions financières transitant par les banques et les FinTechs, en passant par les données éducatives des écoles et des universités, les données agricoles des exploitations et les comportements des consommateurs capturés par les plateformes de commerce électronique, l'Inde est incontestablement un pays « riche en données ».

Si les données existent et recèlent un tel potentiel, pourquoi la collaboration en matière de données pour l'entraînement de l'IA n'est-elle pas plus développée ? Parce que ces obstacles sont importants et multiformes, et vont bien au-delà des simples difficultés techniques.

1.2.1 Premièrement, les risques liés à la protection de la vie privée constituent une préoccupation majeure. Même si les données sont destinées à une analyse agrégée, les données brutes contiennent souvent des informations personnellement identifiables (IPI) ou des informations sensibles. L'utilisation de vastes jeux de données pour l'entraînement — même en interne au sein d'une organisation ou avec des partenaires de confiance — accroît la surface d'exposition aux violations ou aux utilisations abusives potentielles. Des fuites accidentelles ou des attaques malveillantes pourraient exposer des informations hautement sensibles, entraînant de graves conséquences pour les individus concernés et une atteinte à la réputation du responsable du traitement des données. La loi indienne sur la protection des données personnelles numériques (DPDP Act) de 2023 impose, à juste titre, des obligations strictes en matière de traitement des données personnelles, incitant les institutions à la prudence quant à tout partage susceptible d'entraîner une non-conformité.

1.2.2 Deuxièmement, au-delà de la protection de la vie privée des individus, d'importants risques institutionnels et commerciaux existent. Les entreprises détiennent des informations commercialement sensibles intrinsèques à leurs jeux de données : listes de clients, habitudes de transaction, indicateurs opérationnels, algorithmes propriétaires. L'utilisation de ces données d'entraînement, même expurgées des données personnelles directes, pourrait révéler par inadvertance des secrets commerciaux, de la propriété intellectuelle ou des contenus protégés par des droits d'auteur à des concurrents ou à des tiers. La crainte de perdre un avantage concurrentiel ou de faciliter le vol de propriété intellectuelle l'emporte souvent sur tout bénéfice perçu du partage de données pour l'entraînement de l'IA.

1.2.3 Troisièmement, l'absence de cadres fiables et accessibles aggrave le problème. Comment garantir la sécurité de la collaboration en matière de données ? Qui s'assure que les données ne sont utilisées qu'aux fins convenues ? Comment la conformité est-elle contrôlée et appliquée ? En l'absence de protocoles standardisés et dignes de confiance, d'intermédiaires neutres et d'options financièrement viables, les risques perçus et la complexité du partage semblent souvent insurmontables. Le contexte opérationnel de la conformité pour les données agrégées, en particulier destinées à l'entraînement de l'IA, peut s'avérer déconcertant, laissant les institutions dans l'incertitude quant aux méthodes autorisées et aux responsabilités potentielles.

1.2.4 Enfin, l'analyse coût-bénéfice penche souvent en défaveur de la collaboration en matière de données. Les institutions supportent les coûts et les risques liés à la

préparation, à la sécurisation et au partage des données, tandis que les bénéfices — qui reviennent souvent à des tiers tels que les développeurs de modèles d'IA — peuvent ne pas sembler suffisamment immédiats ou tangibles pour justifier les efforts et les risques engagés. En l'absence d'un retour sur investissement clair ou de moyens d'atténuer efficacement les risques et de rendre le processus fluide et rentable, la position par défaut est souvent de maintenir les données sous clé. L'ensemble de ces facteurs crée un obstacle redoutable, entravant la circulation des données essentielles à l'innovation en IA.

1.3 Une nouvelle approche : au-delà du consentement individuel

Consciente de la nécessité d'une meilleure gouvernance des données, l'Inde a introduit l'Architecture d'Autonomisation et de Protection des Données (*DEPA Inférence*), principalement opérationnalisée via le cadre des Agrégateurs de Comptes (AC) dans le secteur financier. *DEPA Inférence* représente une avancée significative, donnant aux individus le contrôle de leurs données personnelles. Grâce aux gestionnaires de consentement (tels que les AC), les individus peuvent accorder un consentement explicite, granulaire et révocable pour que leurs données (par exemple, relevés bancaires, déclarations fiscales) soient partagées en toute sécurité entre un Fournisseur d'Information Financière (FIF, comme une banque) et un Utilisateur d'Information Financière (UIF), comme un établissement de crédit) à des fins spécifiques, telles que la demande d'un prêt.

DEPA Inférence excelle dans la facilitation du partage sécurisé de données individuelles, en encadrant l'inférence comme une transaction ou un service spécifique réalisé

en échange d'un consentement. Elle permet à une petite entreprise d'utiliser ses données de TPS pour prouver sa solvabilité, ou à un particulier de partager ses avoirs en fonds communs de placement avec un nouveau conseiller financier. Ce modèle fondé sur le consentement, centré sur l'individu, est essentiel pour donner aux utilisateurs les moyens d'agir dans leurs interactions directes avec les prestataires de services.

Cependant, le défi posé par les données d'entraînement en IA requiert une approche différente. Si *DEPA Inférence* gère le flux consenti de données individuelles pour l'inférence (à l'aide d'un modèle existant), elle n'est pas conçue pour traiter l'agrégation respectueuse de la vie privée de données massives et désidentifiées, indispensables à la construction même des modèles d'IA. Les enjeux fondamentaux sont différents.

Prenons l'exemple d'un cas d'usage MarTech (technologie marketing). Dans le cadre de *DEPA Inférence*, un utilisateur peut consentir à ce que son historique d'achats soit partagé depuis le Détaillant A vers le Détaillant B afin de recevoir un coupon de réduction personnalisé. Il s'agit de données individuelles partagées pour une tâche d'inférence spécifique (l'application d'une règle de réduction). Mais que se passe-t-il si les Détaillants A, B et C souhaitent collaborer à la construction d'un modèle d'IA performant capable de prédire les tendances d'achat futures sur l'ensemble du marché ? Ils doivent mutualiser les enseignements tirés de millions de transactions clients sans révéler les identités individuelles, sans porter atteinte à la vie privée, ni divulguer de données de ventes confidentielles. Une simple anonymisation ne suffit pas, en raison des risques de réidentification et de la perte d'utilité

des données. Autrement dit, le consentement individuel via *DEPA Inférence* est impraticable à cette échelle et ne résout pas le problème de risque institutionnel.

Voilà l'écart : *DEPA Inférence* prend en charge le partage consenti de données à des fins individuelles dans le cadre de transactions spécifiques ; elle ne fournit pas le cadre nécessaire à la mise en commun sécurisée et respectueuse de la vie privée des données agrégées requises pour construire des modèles d'IA performants. Cela rend indispensable le cadre *DEPA Entraînement* (*DEPA Training Framework*) — une nouvelle couche conçue spécifiquement pour exploiter la valeur des données agrégées pour l'entraînement des IA, tout en préservant la confidentialité et la sécurité grâce à des technologies avancées et des mécanismes de gouvernance.

1.4 Risques liés à l'inaction

A l'ère de l'innovation en intelligence artificielle, il est impératif pour les économies de relever le défi de l'accès à des ensembles de données nouveaux et complémentaires pour l'entraînement des modèles d'IA. Des jeux de données de grande valeur doivent être rendus disponibles pour un couplage sécurisé et privé, permettant l'entraînement de modèles d'IA sur des jeux de données agrégés et interconnectés, en vue de la résolution de problèmes combinatoires. En l'absence d'un tel cadre, les risques sont considérables.

Premièrement, l'innovation serait étranglée. Sans accès à des jeux de données diversifiés et à grande échelle, les startups indiennes, les chercheurs et même les entreprises établies en dehors des géants technologiques dominants auraient du mal à développer des solutions d'IA de pointe adaptées aux besoins

locaux. Les progrès dans des domaines essentiels tels que la santé, la finance, l'agriculture et le développement durable — qui pourraient être accélérés par l'IA — seraient entravés. Le paradoxe « riche en données, pauvre en IA » s'approfondirait, limitant la croissance économique et le potentiel d'améliorations technologiques des services publics et de la qualité de vie.

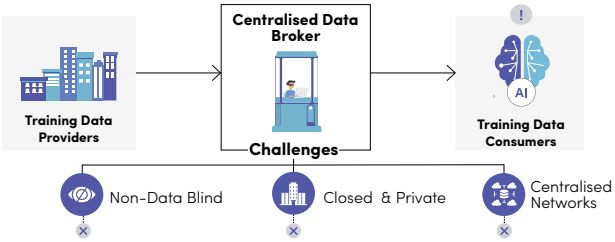
Deuxièmement, le risque de violation de la vie privée et d'utilisation abusive des données augmenterait. En l'absence d'un cadre robuste, sécurisé et digne de confiance, la pression exercée pour accéder aux données pourrait inciter les institutions à recourir à des méthodes ad hoc et non sécurisées, ou à s'appuyer sur des courtiers en données opérant dans des zones grises réglementaires. Cela pourrait accroître la probabilité de violations de données, d'utilisation non autorisée d'informations personnelles et d'érosion de la confiance du public. Des affaires comme celle de Cambridge Analytica rappellent brutalement les conséquences potentielles d'un partage de données dépourvu de garanties et de contrôles adéquats. Elles favorisent également l'émergence d'intermédiaires de données à but lucratif dont les pratiques opaques érodent davantage la confiance et découragent la participation.

Troisièmement, la situation actuelle risque d'entraîner une concentration du marché et de désavantager les acteurs locaux. Les grandes multinationales technologiques disposent souvent des ressources, de l'expertise technique et des vastes bases de données utilisateurs nécessaires au développement de modèles d'IA sophistiqués. Elles peuvent naviguer plus facilement dans les ambiguïtés réglementaires et supporter les risques liés à l'agrégation des données plus aisément que les petites entreprises ou startups indiennes. Il en résulte un terrain de jeu inégal, ou l'innovation se concentre entre les

mains de quelques acteurs mondiaux, risquant de marginaliser les innovateurs indiens et de rendre l'économie dépendante des plateformes d'IA étrangères. L'Inde possède un atout stratégique majeur dans sa vaste production de données ; il est donc d'intérêt national de l'exploiter de manière responsable pour gagner du terrain, de manière nouvelle et impactante, dans la course mondiale à l'IA.

A ces problèmes structurels s'ajoutent des vulnérabilités persistantes en matière de protection de la vie privée et des conflits non résolus en matière de propriété intellectuelle qui, collectivement, créent une impasse des données, maintenant des informations précieuses enfermées dans des silos.

En conclusion, l'inaction n'est pas une position neutre ; elle contribue activement à l'accroissement des risques et à la disparition des opportunités. Mettre en place un cadre comme *DEPA Entraînement* ne se limite pas à faciliter l'accès à l'IA ; il s'agit d'atténuer ces risques considérables, de construire une IPN fiable et décentralisée afin de permettre à l'Inde d'exploiter pleinement le potentiel des données pour une innovation inclusive, une compétitivité économique accrue et le bien-être de ses citoyens, tout en respectant des normes rigoureuses en matière de protection de la vie privée.



The current data architecture is broken

02. DEPA Entraînement — Aperçu de l'architecture

2.1 Un cadre pour une collaboration de confiance

Ce chapitre décrit en détail l'architecture de *DEPA Entraînement*. *DEPA Entraînement* est notre Infrastructure Publique Numérique (IPN) pour l'IA : un écosystème structuré et axé sur la protection de la vie privée, conçu pour faciliter un entraînement sécurisé, privé, conforme et éthique des modèles d'IA. Il étend la philosophie de *DEPA Inférence* — qui avait permis le partage de données individuelles basé sur le consentement pour l'inférence — au défi plus complexe que représente l'utilisation collective des données pour l'entraînement des modèles d'IA. L'architecture est une application des principes fondamentaux DEPA ADEPTS — Accountability, Discoverability, Explainability, Predictability, Teachability, Safety — au contexte spécifique de l'apprentissage automatique à partir de données agrégées.

Au cœur de *DEPA Entraînement* se trouve une architecture fédérée et décentralisée. Elle rompt avec les accords bilatéraux opaques et les risques liés aux courtiers de données centralisés, en établissant un espace de collaboration régulé entre fournisseurs de données et développeurs de modèles d'IA, animé par une gamme de participants facilitateurs (fournisseurs de services cloud, fournisseurs de modèles, organismes de certification, etc.). Cette collaboration est encadrée par une gouvernance sectorielle et des technologies de protection de la vie

privée mises en œuvre via des Plateformes Collaboratives de Données, garantissant la confidentialité et la conformité tout au long du cycle de vie de l'IA. Grâce à l'intégration d'Environnements d'Exécution de Confiance (EEC) et de la Confidentialité Différentielle, le cadre permet à de multiples acteurs de contribuer et d'utiliser des données agrégées anonymisées de manière responsable, sans exposition ni transfert direct des données brutes.

Ce qui suit est une description détaillée de la structure et du flux de fonctionnement de *DEPA Entraînement*. Nous décrirons les rôles et les responsabilités de ses principaux acteurs, des institutions fournissant les données aux innovateurs qui les utilisent, en passant par les nouveaux fournisseurs de services technologiques facilitateurs et les organes de gouvernance qui supervisent leurs interactions. Nous aborderons ensuite les composants techniques sous-jacents qui appliquent les politiques, garantissent la traçabilité et assurent une protection de bout en bout des données. Ce cadre techno-légal établit un modèle de développement de l'IA fondé sur la confiance par le droit, la confiance par la conception et la confiance par la technologie.

2.2 Les acteurs clés de l'écosystème DEPA

DEPA Entraînement est composé de participants distincts mais interdépendants, chacun ayant un rôle défini. Cette séparation structurée des tâches apporte clarté, responsabilité et audibilité à un processus qui a historiquement manqué de transparence.

Personnes Concernées (Data Principals)

Au fondement même de l'écosystème se trouvent les Personnes Concernées — les individus ou entités auxquels les données appartiennent initialement. Bien qu'ils n'interagissent pas directement avec le réseau d'entraînement, leurs droits constituent le socle sur lequel repose l'ensemble de l'architecture. Leurs données sont gérées conformément aux réglementations juridiques qui imposent la limitation des finalités et des garanties de confidentialité, et leurs intérêts sont protégés par une structure de gouvernance d'Organisme d'Autorégulation (OAR) qui met en œuvre des technologies de pointe — contrats électroniques, informatique confidentielle et confidentialité différentielle — à cette fin.

Collectifs de Données (Data Collectives)

Pour combler le fossé entre les personnes concernées et le réseau d'innovation en IA des modélisateurs, une nouvelle catégorie d'acteurs émerge : les Collectifs de Données. Ces institutions intermédiaires, qui peuvent être des coopératives, des associations sectorielles ou des consortiums de recherche, travaillent avec les communautés pour agréger, standardiser et organiser les données provenant de sources multiples. Elles jouent un rôle essentiel dans la synchronisation des flux de données fragmentés en vue d'un traitement ultérieur et peuvent être chargées d'obtenir le consentement primaire le cas échéant. Cette approche par couches permet au réseau de monter en échelle et d'intégrer des données issues de sources souvent sous-représentées et complémentaires dans le développement traditionnel de l'IA.

Fournisseurs de Données d'Entraînement (FDE)

Les Fournisseurs de Données d'Entraînement sont les gardiens formels des données au sein de l'écosystème DEPA. Ce sont des institutions chargées de collecter, gérer et préparer les jeux de données destinés à l'entraînement de l'IA. Leur rôle va au-delà de la simple conservation ; elles doivent appliquer des transformations préservant la confidentialité et s'assurer que les jeux de données répondent aux exigences techniques et réglementaires strictes en matière de désidentification. Les FDE peuvent provenir de tous les secteurs et peuvent inclure, sans s'y limiter :

- Les hôpitaux et les prestataires de soins de santé, qui fournissent des dossiers patients anonymisés pour la modélisation prédictive de la santé ;
- Les établissements financiers, qui partagent des données transactionnelles désidentifiées pour améliorer la détection des fraudes ou les modèles de risque de crédit ;
- Les organismes publics et les opérateurs de villes intelligentes, qui mettent à disposition des flux de données pour la planification urbaine et l'optimisation du trafic ;
- Les entreprises pharmaceutiques, qui partagent des données avec des entreprises plus petites dans le cadre d'initiatives de découverte et de réorientation de médicaments.

Les FDE sont enregistrés auprès du registre central et sont liés par ses normes de gouvernance, appliquées via les contrats électroniques.

Consommateurs de Données d'Entraînement (CDE)

Les Consommateurs de Données d'Entraînement sont les innovateurs qui accèdent à ces jeux de données pour développer, affiner ou évaluer des modèles d'IA. Les CDE doivent opérer dans le strict respect des limites de finalité et de conduite éthique définies dans leurs accords de partage de données avec les Collectifs de Données — qui fédèrent les jeux de données d'un secteur donné provenant de plusieurs FDE — ou directement avec des FDE individuels. Le réseau vise à stimuler l'innovation au sein d'un large spectre de CDE, notamment :

- Les institutions de recherche universitaires et à but non lucratif, qui développent des modèles open source pour le bien commun ;
- Les startups et les entreprises, souvent avides de données mais aux ressources limitées, qui construisent des solutions commerciales basées sur l'IA ;
- Les organismes de réglementation qui cherchent à tester l'équité, la sécurité et l'exactitude de systèmes d'IA tiers dans des domaines sensibles.

Tout entraînement de modèles par les CDE doit se dérouler au sein de Salles Blanches Confidentielles approuvées, et les modèles résultants sont soumis à validation.

2.3 Confidentialité et sécurité intégrées dès la conception

L'intégrité du Cadre de Formation DEPA repose sur un socle technologique où la sécurité et la confidentialité sont intégrées dans l'architecture elle-même. Cette approche de « sécurité dès la conception » est essentielle pour instaurer

la confiance institutionnelle et publique nécessaire à la collaboration à grande échelle sur les données. Deux piliers en particulier constituent les fondements des garanties techniques de DEPA : l'application rigoureuse de la Confidentialité Différentielle et la mise en œuvre exhaustive d'un Cadre de Sécurité dit Zero Trust.

2.3.1 Pourquoi l'« anonymisation » traditionnelle ne suffit pas pour l'entraînement des modèles d'IA

Une suggestion courante pour surmonter les obstacles à la collaboration en matière de données est l' « anonymisation » — c'est-à-dire simplement supprimer les identifiants directs tels que les noms, adresses ou numéros d'identification uniques. L'idée est qu'une fois les données personnelles supprimées, les données deviennent non-personnelles et peuvent être utilisées librement pour l'entraînement, sans risque pour la vie privée. Malheureusement, pour la génération de données d'entraînement robustes pour l'IA, cette approche est souvent une simplification excessive et dangereuse — un mythe qui ne prend pas en compte la complexité des données modernes.

Le problème fondamental réside dans le risque d'identification. Des décennies de recherche ont montré que même des données expurgées de leurs identifiants directs peuvent souvent être réidentifiées en les croisant avec d'autres jeux de données disponibles. Des informations apparemment anodines (telles que la date de naissance, le code postal et le sexe ; ou une combinaison d'horodatages et de lieux de transactions) peuvent, une fois combinées, constituer une « empreinte digitale » unique identifiant un individu. A mesure que les jeux de données s'agrandissent et se diversifient, et que les données auxiliaires (issues

des registres publics, des réseaux sociaux, des courtiers en données) deviennent plus facilement accessibles, la possibilité d'identifier des individus au sein de jeux de données supposément « anonymisés » augmente considérablement. La combinaison de seulement deux ou trois jeux de données modérément anonymisés peut accroître ce risque de manière exponentielle, révélant potentiellement des informations sensibles sur des personnes que l'on croyait protégées.

De plus, le processus d'anonymisation rigoureuse nécessaire pour réduire significativement le risque d'identification compromet souvent l'utilité des données pour l'entraînement des IA. Des techniques telles que le k-anonymat, la l-diversité ou l'ajout d'un « bruit » statistique important impliquent la suppression ou la généralisation de points de données. Si cela renforce la confidentialité, cela peut déformer les tendances et corrélations sous-jacentes dont les modèles d'IA ont besoin pour apprendre efficacement. Des données excessivement anonymisées peuvent empêcher l'identification, mais engendrer des modèles d'IA peu performants, imprécis ou biaisés. Il existe une alternative fondamentale : anonymiser de manière excessive et perdre en utilité ; préserver l'utilité et s'exposer au risque d'identification.

Les techniques d'anonymisation traditionnelles ont souvent été développées lorsque les jeux de données étaient plus petits et la puissance de calcul limitée. Elles sont fréquemment inadaptées aux jeux de données massifs et multidimensionnels requis par l'IA moderne et aux techniques sophistiquées utilisées pour les analyser. Se fier uniquement à la suppression des identifiants directs procure un faux sentiment de sécurité et ne permet pas de

résoudre les problématiques de confidentialité complexes inhérentes au partage de données pour l'entraînement de modèles d'IA sophistiques. Une approche plus élaborée est clairement nécessaire.

2.3.2 Mécanismes de Confidentialité Différentielle

DEPA répond à ce défi par la Confidentialité Différentielle, une technique mathématiquement robuste qui permet de tirer des enseignements des tendances agrégées tout en rendant statistiquement improbable l'inférence d'informations sur un individu particulier.

Plutôt que de simplement supprimer les identifiants, cette méthode introduit un bruit statistique soigneusement calibré dans les réponses aux requêtes ou les sorties du modèle. Ainsi, l'inclusion ou l'exclusion des données d'une personne a un effet négligeable sur le résultat final, rompant ainsi le lien entre l'analyse globale et la contribution individuelle. Ceci est crucial dans des domaines à forts enjeux tels que la santé, où les dossiers patients désidentifiés peuvent être utilisés pour entraîner des modèles de diagnostic sans compromettre la confidentialité des patients.

Au sein de DEPA, la mise en œuvre de la confidentialité différentielle est encadrée et auditée. Les budgets de confidentialité — qui limitent la perte cumulative de confidentialité due aux requêtes répétées — sont définis et surveillés de manière transparente, permettant un compromis entre la maîtrise de la confidentialité et la précision analytique, adapté au profil de risque de chaque secteur.

2.3.3 Cadre de Sécurité dit Zero Trust

La sécurité au niveau des données est complétée par une posture de sécurité réseau régie par un Cadre de Sécurité dit Zero Trust. Ce modèle abandonne la notion obsolète de réseau interne de confiance et repose sur le principe « ne jamais faire confiance, toujours vérifier ». Chaque interaction au sein de l'écosystème DEPA est considérée comme potentiellement hostile et doit être explicitement authentifiée et autorisée. Concrètement, cela signifie :

- Vérification stricte : chaque demande d'accès aux données, quelle que soit son origine, est soumise à une vérification rigoureuse de l'identité, du rôle et de la conformité aux politiques avant que l'accès ne soit accordé.
- Chiffrement généralisé : les données sont protégées à toutes les étapes — au repos, en transit et pendant le traitement — par des protocoles de chiffrement obligatoires conformes aux normes de l'industrie.
- Audit continu : les modèles d'IA et l'infrastructure SBC font l'objet d'audits de sécurité réguliers afin de détecter les vulnérabilités et d'appliquer les politiques d'accès.
- Surveillance en temps réel : les journaux d'accès sont tenus à jour en temps réel, et toute activité anormale — telle qu'une tentative d'accès non autorisée — déclenche automatiquement une alerte et une enquête.

Ce contrôle continu, associé à des contrats et des jeux de données signés cryptographiquement, crée un système de responsabilisation en boucle fermée. Ensemble, la Confidentialité Différentielle et l'architecture Zero Trust garantissent que l'entraînement de l'IA au sein de DEPA est accéléré tout en se déroulant dans le respect des cadres

juridiques et éthiques, et d'une manière fondamentalement sécurisée dès la conception.

2.3.4 Environnements d'Exécution de Confiance / Salles Blanches Confidentielles (SBC)

Les Salles Blanches Confidentielles constituent la pierre angulaire technologique de l'infrastructure de protection de la vie privée de DEPA. Ce sont des environnements de calcul spécialisés à haute assurance où les modèles d'IA peuvent être entraînés sur des données sensibles et anonymisées sans jamais exposer les données brutes aux CDE ni à d'autres systèmes externes. Cela élimine la nécessite de transférer ou d'exposer des données brutes, minimisant ainsi le risque de violations ou d'utilisation non autorisée. Les principales garanties intégrées aux SBC comprennent :

- L'exécution de tous les calculs au sein d'Environnements d'Exécution de Confiance (EEC) — des enclaves matérielles sécurisées qui empêchent les fuites ou les altérations de données pendant le traitement ;
- L'application d'algorithmes de confidentialité tels que la Confidentialité Différentielle, afin de garantir que les motifs individuels ne puissent pas être déduits des résultats du modèle ;
- La prise en charge de techniques avancées telles que l'Apprentissage Fédéré et le Calcul Multipartite Sécurise (MPC), qui permettent un entraînement collaboratif à travers différents silos de données sans les regrouper.

Les fournisseurs de SBC doivent être accrédités, garantissant ainsi qu'ils respectent des normes rigoureuses en matière de sécurité et de confidentialité.

2.4 Mise en œuvre opérationnelle de DEPA Entraînement

2.4.1 Flux de fonctionnement

DEPA Entraînement fonctionne selon un flux rigoureusement orchestré qui garantit la sécurité, la conformité et la traçabilité à chaque étape. Ce processus transforme des données brutes distribuées en modèles d'IA éthiques et certifiés, régis par des règles claires et des garanties techniques.

Étape 1 : Enregistrement et chiffrement des données. Le processus débute lorsqu'un Fournisseur de Données d'Entraînement (FDE) enregistre officiellement un jeu de données auprès du réseau DEPA — directement via des services de catalogue auto-hébergés, ou via un Agent de Découverte de Données ou un Collectif de Données — une action supervisée par un organe de gouvernance. Avant toute utilisation, les données doivent être préparées et cataloguées. Durant cette étape, les jeux de données sont anonymisés et chiffrés afin de supprimer les informations permettant d'identifier des personnes. Chaque jeu de données se voit attribuer des métadonnées structurées décrivant son origine, sa sensibilité et ses restrictions d'accès, et est marqué cryptographiquement ou par filigrane afin de garantir une traçabilité de bout en bout. Ce jeu de données enregistré et protégé est désormais accessible aux consommateurs autorisés via le cadre DEPA.

Étape 2 : Demande de données et validation du contrat. Ensuite, un Consommateur de Données d'Entraînement (CDE) soumet une demande d'accès à un ou plusieurs jeux de données pour un cas d'usage spécifique. Cette demande

n'est pas une simple requête ; il s'agit d'une proposition formelle validée par le Système de Gestion des Contrats Électroniques DEPA. Le système vérifie automatiquement la demande du CDE par rapport aux politiques de partage des données définies par le Collectif de Données ou le FDE, ainsi qu'aux règles de gouvernance. Cette application automatisée des conditions contractuelles garantit que les données ne sont accessibles qu'aux parties autorisées et à des fins légitimement enregistrées.

Étape 3 : Entraînement sécurisé des modèles dans des Salles Blanches Confidentielles. Après validation, l'agrégation et l'analyse des données sont effectuées exclusivement au sein d'une Salle Blanche Confidentielle certifiée (SBC). La conception de la SBC impose une politique stricte de non-exposition des données brutes. Grâce à des Environnements d'Exécution de Confiance (EEC) matériels, les données restent chiffrées et isolées, même pendant leur traitement. Dans cet environnement sécurisé, des techniques de Confidentialité Différentielle sont appliquées de manière systématique afin d'empêcher le modèle d'apprendre ou de révéler des informations propres à un individu. Toutes les activités au sein de la SBC sont consignées de manière immuable à des fins d'audit, garantissant ainsi que le processus est à la fois sécurisé et transparent.

Étape 4 : Validation du modèle et détection des biais. Une fois entraîné, un modèle doit subir un processus de validation rigoureux et indépendant. Cette évaluation est multidimensionnelle et couvre à la fois les :

- Audits de biais et d'équité : le modèle est testé afin de s'assurer qu'il ne produit pas de résultats discriminatoires ni n'amplifie les inégalités historiques ;

- Tests de sécurité et de robustesse : le modèle est évalué afin de détecter les vulnérabilités aux attaques adversaires ou aux fuites de données potentielles ;
- Tests de sécurité à grande échelle : pour les applications à haut risque, les modèles subissent des tests supplémentaires, notamment la modélisation de systèmes adaptatifs complexes et des tests adversariaux en boîte noire ;
- Exploitabilité algorithmique : la logique du modèle est évaluée afin de garantir que ses décisions puissent être interprétées et expliquées dans des contextes juridiques et pratiques.

Seuls les modèles qui réussissent cet audit complet reçoivent une certification réglementaire.

Étape 5 : Déploiement certifié et surveillance continue. La certification obtenue, le CDE peut déployer le modèle d'IA à des fins publiques ou commerciales. Toutefois, la supervision ne s'arrête pas au déploiement. Le cadre DEPA impose une surveillance continue afin de garantir une conformité et une sécurité permanentes. Cela inclut la tenue de registres d'équité et de sécurité pour des examens périodiques, ainsi que la garantie d'une traçabilité complète depuis les résultats du modèle jusqu'aux données et contrats utilisés pour son entraînement. Cette dernière étape assure la confiance et la responsabilité à long terme pour tous les systèmes d'IA développés au sein de l'écosystème DEPA.

2.4.2 Modèle économique et commercial

Les Plateformes Collaboratives de Données DEPA (*Data Collabs*) servent de nœuds centraux réunissant différents acteurs du marché sur une plateforme commune.

Orientées vers les besoins métiers et sectoriels, elles sont conçues comme des acteurs commerciaux. Leur objectif est de briser les silos et d'apporter consensus, efficience et impact mesurable à la tâche de partage des données et, par conséquent, à la construction de modèles d'IA sûrs et responsables.

Le modèle commercial des *Data Collabs* consiste à fournir des services et des outils écosystémiques essentiels, notamment :

- Des outils et services généraux (enregistrement, authentification, curation pour la découverte) ;
- Des outils et services relatifs aux données (schémas standards, protocole de chiffrement-déchiffrement, protocole d'échange) ;
- Des outils et services spécifiques au domaine (contrats électroniques).

Des incitations sont intégrées pour tous les autres acteurs et facilitateurs de l'écosystème. Via la plateforme, les fournisseurs de données (FDE) peuvent valoriser leurs référentiels de données en entrant dans un modèle de partage des bénéfices selon lequel, par exemple, les hôpitaux qui partagent des données peuvent bénéficier d'un accès prioritaire aux modèles issus de ces données pour améliorer les résultats cliniques et les soins aux patients.

Pour les modélisateurs de données, les avancées en matière d'innovation découlent directement de l'accès à des données plus volumineuses et de meilleure qualité. D'autres acteurs, tels que les fournisseurs de services technologiques (fournisseurs de calcul, fournisseurs de modèles), peuvent aligner, affiner et positionner leurs produits et services en fonction des besoins émergents du secteur de l'innovation en données et en IA.

03. L'approche techno-légale de DEPA : un ré-encadrement réglementaire

3.1 Un nouveau modèle de gouvernance de l'IA

L'IA est une technologie complexe et en constante évolution. Les réglementations statiques et verticales, appliquées via des contrôles manuels ou des audits, sont mal adaptées au rythme de cette technologie numérique. Elles risquent de constituer un goulot d'étranglement pour l'innovation d'un part, et de constituer d'autre part, des garanties inefficaces en raison des difficultés d'application. Là où DEPA Inférence a su tirer parti d'un organisme de réglementation centralisé comme Sahamati pour orchestrer l'écosystème des Agrégateurs de Comptes, *DEPA Entraînement* fait face à des défis plus importants. Il doit permettre le partage de données multipartite tout en garantissant que l'utilisation des données s'inscrit dans le respect de dispositions de sécurité et de confidentialité prédéfinies. L'utilisation équitable et transparente des données est tout aussi importante pour une innovation responsable en matière d'IA. *DEPA Entraînement* est donc conçu selon les principes ADEPTS , avec les idéaux fondamentaux d'actionnement autonome, de responsabilité, d'évaluation, de désambiguïsation de l'intention, de personnalisation et confidentialité, de Transparence et de Sécurité pro active dans le cadre dès la conception et opérationnalisés via l'approche novatrice de gouvernance techno-légale.

3.2 Intégrer la conformité via un cadre techno-légal

La force du cadre *DEPA Entraînement* réside dans sa capacité à fusionner les principes juridiques avec leur application technologique. La conformité n'est pas laissée à la bonne volonté de l'écosystème ; elle est intégrée dans l'architecture même du système. Ce cadre va au-delà de la simple politique pour opérationnaliser la confiance via un système techno-légal cohérent qui offre à la fois des garanties de processus robustes et des garanties informatiques vérifiables.

Cette approche de « conformité par conception » offre un ensemble direct et concret de solutions au déficit d'application, garantissant que la protection de la vie privée et les considérations éthiques sont préservées non seulement par les politiques, mais également par la conception et la technologie.

Les garanties informatiques de DEPA assurent l'application technique rigoureuse de ses principes fondamentaux. La garantie principale est l'utilisation obligatoire des Salles Blanches Confidentielles (SBC) pour tout entraînement de modèle d'IA. Grâce à des Environnements d'Exécution de Confiance (EEC) basés sur le matériel, les SBC créent une enclave sécurisée où les données sensibles et anonymisées peuvent être traitées sans jamais être exposées sous leur forme brute. Il s'agit d'une solution architecturale qui s'oppose principiellement aux risques de violations de données et d'utilisation non autorisée, qui applique les principes de « protection de la vie privée par conception » et de « minimisation des données » au niveau matériel.

La Confidentialité Différentielle vient compléter la sécurité des SBC. Cette technique mathématiquement robuste fournit une garantie d'anonymat vérifiable, palliant ainsi la lacune critique des méthodes d'anonymisation traditionnelles. En introduisant un bruit statistique précisément calibré, la Confidentialité Différentielle rend statistiquement improbable l'inférence d'informations sur un individu à partir des résultats d'un modèle. Ensemble, ces garanties de processus et de calcul créent un système de responsabilité en boucle fermée. Dans ce modèle, la conformité n'est pas un frein à l'innovation ; elle en est le moteur.

En résumé, la gouvernance est mise en œuvre via un ensemble de mécanismes techniques :

- Contrats électroniques : ces accords lisibles par machine automatisent l'application des conditions de partage des données, des limitations de final ité et des droits d'utilisation, créant ainsi une chaîne de responsabilité transparente et vérifiable ;
- Salles Blanches Confidentielles : en tant qu'environnement obligatoire pour tout entraînement de modèle, les SBC empêchent technologiquement l'exposition des données brutes, imposant par défaut la minimisation des données ;
- Confidentialité Différentielle : cette technique offre une garantie mathématique d'anonymat, assurant que les résultats du modèle ne peuvent être utilisés pour identifier des individus, s'alignant ainsi sur les principes fondamentaux du droit de la protection des données.
- Sécurité Zero Trust : l'architecture fonctionne selon le principe « ne jamais faire confiance, toujours vérifier », chaque interaction nécessitant une authentification et une autorisation cryptographiques, le tout étant enregistré dans des journaux d'audit immuables.

Ce cadre est conçu pour s'aligner sur les principales réglementations nationales et internationales, notamment la loi indienne sur la Protection des Données Personnelles Numériques (DPDP Act) de 2023, le Règlement Général sur la Protection des Données (RGPD) de l'UE et la loi européenne sur l'IA, ainsi que d'autres cadres internationaux de gestion des risques. Il prend également en compte les lois sectorielles telles que la loi HIPAA dans le secteur de la santé ou Bâle III dans le secteur financier.

3.3 Une architecture de surveillance collaborative

DEPA Entraînement requiert un organe de gouvernance agile, chargé de garantir l'intégrité et la responsabilité de l'écosystème. Il doit à la fois assurer l'intendance des politiques et l'administration technique, en veillant à ce que chaque participant évolue dans un cadre juridique, éthique et procédural harmonisé. Sa structure se doit d'être une rupture délibérée avec le contrôle centralisé, conçue plutôt comme un consortium constitué par les participants de l'écosystème eux-mêmes, intégrant différentes voix critiques, telles que :

- Les Fournisseurs de Données d'Entraînement (FDE) ;
- Les Consommateurs de Données d'Entraînement (CDE) ;
- Les Collectifs de Données ;
- Les Fournisseurs de Services Technologiques (FST) ;
- Les experts sectoriels ;
- Les représentants de la société civile.

DEPA Entraînement a conçu cette composition multipartite de l'organe de supervision afin de garantir que les politiques

de gouvernance de tout cadre DEPA restent ancrées dans la réalité pratique et reflètent un équilibre des intérêts. Elle vise à promouvoir la co-appropriation et un sentiment partagé de responsabilité, où les règles du jeu sont établies par ceux qui les respectent.

Cet organe de surveillance constituerait le point d'ancrage d'un ensemble complet de responsabilités couvrant l'intégralité du cycle de vie de l'entraînement en IA :

- Enregistrement des participants et gestion des identités : maintien d'un registre central de tous les participants à l'écosystème DEPA, incluant l'enregistrement et la vérification formels de l'identité des FDE, des CDE et des fournisseurs de SBC, et émission des identifiants cryptographiques nécessaires à leur interaction sécurisée au sein du réseau ;

- Accréditation et certification : accréditation des principaux fournisseurs d'infrastructure et certification des modèles d'IA. Les Salles Blanches Confidentielles doivent être certifiées conformes aux normes de sécurité et de confidentialité prescrites avant de pouvoir opérer au sein du réseau. De plus, les modèles d'IA entraînés doivent être vérifiés comme « aptes à l'emploi », y compris leur conformité aux normes d'équité, d'atténuation des biais et de sécurité des données, avant d'être déployés ;

- Gestion de l'infrastructure des contrats électroniques : le système de contrats électroniques constitue l'épine dorsale opérationnelle du réseau DEPA. La chaîne contractuelle est liée à la « Chaîne de Provenance IA », un registre distribué qui fournit un enregistrement immuable des opérations de traitement de données effectuées dans le cadre d'accords contractuels signés. Cela garantit la traçabilité, la vérifiabilité et la responsabilité complètes des termes contractuels ;

- Audit et contrôle de la conformité : l'audit des modèles d'IA et des processus d'entraînement est essentiel pour garantir le respect des principes de DEPA. Cela inclut le pouvoir de suspendre ou de révoquer les activités non conformes, constituant ainsi un mécanisme d'application indispensable au maintien de l'intégrité de l'écosystème ;
- Règlement des litiges : en cas de différends entre participants — tels que des désaccords sur l'utilisation des données, des manquements contractuels ou des préoccupations éthiques — des mécanismes formels de médiation et d'arbitrage devront être définis, garantissant un règlement équitable et efficace.

En intégrant ces fonctions réglementaires dans le substrat technique du système DEPA, DEPA Entraînement demeure léger, décentralisé et juridiquement résilient.

3.4 Feuille de route pour la mise en œuvre

La réussite de l'adoption de ce cadre de gouvernance ambitieux requiert une approche structurée et progressive. Pour passer du projet à un écosystème opérationnel, la feuille de route suivante est proposée :

- Mise en place de projets pilotes : la phase initiale est axée sur l'établissement de *Data Collabs* pilotés dans quelques secteurs à fort impact tels que la finance et la santé. Cela permettra d'affiner les protocoles de gouvernance dans des conditions réelles ;
- Mise en place de bacs à sable réglementaires : en parallèle, des bacs à sable réglementaires seront créés pour permettre aux développeurs et aux institutions de

former, tester et valider des modèles d'IA sur des jeux de données DEPA dans un environnement de conformité contrôlé ;

- Promotion de cadres de gouvernance transfrontaliers : les *Data Collabs* s'efforceront activement d'établir des accords bilatéraux et multilatéraux pour faciliter la collaboration et la recherche internationales sécurisées en matière de données, en assurant l'interopérabilité avec les normes mondiales ;
- Lancement de programmes de sensibilisation et de renforcement des capacités : un effort concerté sera déployé pour sensibiliser les développeurs, les institutions et les décideurs politiques aux principes et pratiques du cadre DEPA via des campagnes et des ateliers ciblés ;
- Élaboration de modèles d'incitation durables : afin d'encourager la participation à long terme des fournisseurs de données, le cadre explorera des structures d'incitation viables, telles que des modèles de redevances ou de droits d'accès, qui récompensent les contributions à l'écosystème des données.

Grâce à ce déploiement volontaire et collaboratif, le cadre règlementaire de *DEPA Entraînement* peut s'établir comme une base robuste, évolutive et digne de confiance pour l'avenir de l'IA en Inde — une base qui démocratise l'accès aux données tout en promouvant une innovation éthique et responsable sur la scène mondiale.

04. Opportunités de marché d'une économie maîtrisant les données

4.1 Quantifier le coût de l'impasse sur les données d'entraînement

Les silos de données — des référentiels d'informations isolés de l'architecture économique d'ensemble — engendrent des coûts colossaux. A l'échelle mondiale, cette fragmentation se traduit par des milliers de milliards de dollars de revenus et de productivité non réalisés. Ce problème est particulièrement aigu en Inde, où l'immense empreinte numérique de sa population demeure largement inaccessible à l'innovation nationale, créant ainsi un déficit de données critique pour les startups, les chercheurs et les décideurs politiques.

Le problème technique des silos de données engendre directement le problème économique de l'asymétrie d'information. Cette situation — où une partie à une transaction dispose d'informations plus nombreuses ou de meilleure qualité que l'autre — est un facteur déterminant de défaillance du marché dans les économies en développement. Sur le marché du crédit indien, cette asymétrie se manifeste par un déficit de crédit persistant et massif pour les micros, petites et moyennes entreprises (MPME). Faute de données fiables sur les nouveaux emprunteurs ou les emprunteurs de petite taille, les prêteurs privilégient rationnellement les entités établies disposant d'un long historique de crédit. Un comité d'experts constitué

par la Reserve Bank of India (RBI) a estimé ce déficit de crédit pour les MPME entre 20 et 25 billions de roupies. Il ne s'agit pas d'une simple statistique financière ; c'est un frein majeur à l'entrepreneuriat, à la création d'emplois et à une croissance économique inclusive.

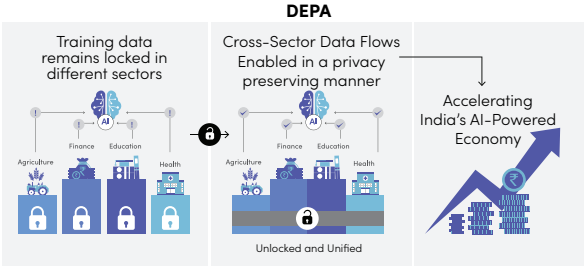
L'Infrastructure Publique Numérique (IPN) indienne existante a déjà démontré sa capacité à corriger de telles défaillances du marché. L'interface de paiement unifié (UPI) et Aadhaar ont considérablement réduit les coûts de transaction et l'asymétrie d'information, permettant en quelques années seulement un niveau d'inclusion financière qui aurait autrement nécessité près de cinq décennies. Ceci constitue un précédent puissant. En établissant des voies sécurisées et interopérables pour le partage de données agrégées et désidentifiées, le cadre *DEPA Entraînement* agit comme une IPN ciblée pour résoudre l'asymétrie d'information au cœur de l'impasse des données d'entraînement, libérant ainsi le potentiel économique de l'ensemble de l'économie.

4.2 La position stratégique de l'Inde dans l'économie mondiale de l'IA

L'économie mondiale de l'IA devrait ajouter plus de 15 000 milliards de dollars au PIB mondial d'ici 2030, une transformation alimentée par la fluidité des données. L'Inde, avec plus d'un milliard d'internautes et un ensemble avancé d'IPN, est idéalement positionnée pour capter une part significative de cette valeur. Les projections indiquent que l'économie numérique indienne atteindra 1 000 milliards de dollars d'ici 2030, l'IA à elle seule pouvant contribuer à hauteur de 500 milliards de dollars au PIB national. Toutefois, pour concrétiser ce potentiel, il est indispensable d'aller au-delà de la simple numérisation. La prochaine vague de croissance

sera portée par la capacité à exploiter les données de manière fiable, sécurisée et créatrice de valeur. La véritable puissance des données ne se révèle pas dans l'isolement, mais dans leur intégration. C'est là que la synergie entre *DEPA Entraînement* et les infrastructures nationales complémentaires telles que l'Infrastructure de Données Géospatiales (IDG) devient stratégiquement vitale.

L'IDG fournit un catalogue unifié de jeux de données spatiales de haute qualité — des couches d'occupation des sols aux réseaux de transport, en passant par l'imagerie satellite — via des API ouvertes. En permettant aux modèles d'IA d'être enrichis de ce contexte de localisation précis, en plus des données sectorielles, via le cadre sécurisé DEPA, un effet multiplicateur est créé. L'intégration de données sectorielles à une couche géospatiale génère des gains d'efficacité importants et ouvre la voie à de nouvelles formes de création de valeur. Un modèle d'IA entraîné sur des données de santé peut identifier des motifs de maladies ; un modèle d'IA entraîné sur des données de santé combinées aux données de l'IDG peut prédire la propagation géographique d'une épidémie et orienter l'allocation des ressources avec une précision pointue. Cette capacité à créer des modèles sophistiqués et contextuels est au cœur de l'opportunité stratégique de l'Inde.



Data Empowerment and Protection Architecture allows for data collaboration
Empowering AI with Richter, Combined Insights

4.3 Analyse sectorielle approfondie

Le cadre *DEPA Entraînement* est la clé pour créer une valeur tangible dans les secteurs les plus critiques de l'Inde. L'analyse suivante explore les opportunités de marchés spécifiques et les obstacles systémiques que le cadre vise à surmonter.

Santé et sciences du vivant : des données fragmentées à la santé publique de précision

Le secteur de la santé indien, dont le marché est projeté à 638 milliards de dollars d'ici 2025, se trouve à un tournant critique. Il se caractérise par la coexistence de poches d'excellence de niveau mondial et d'une fragmentation systémique. Cette fragmentation engendre des coûts directs et quantifiables. Bien qu'une étude exhaustive spécifique à l'Inde soit encore en attente, les données internationales suggèrent que la fragmentation des soins peut quasiment doubler les coûts de santé. Dans le contexte indien, un rapport de NITI Aayog estime que la réduction de la fragmentation du système de santé pourrait éviter à 1,5 million de ménages de basculer chaque année dans la pauvreté en raison de dépenses de santé catastrophiques. Le cadre DEPA Entraînement offre une voie permettant de dépasser l'amélioration des diagnostics individuels pour créer une intelligence prédictive à l'échelle de la population. En permettant un accès sécurisé à des données de santé agrégées à grande échelle, il ouvre de nouvelles perspectives dans les domaines suivants :

- Médecine de précision et génomique : le patrimoine génétique de la population indienne est unique. L'entraînement de modèles d'IA sur des données génomiques agrégées à l'échelle panindienne peut mener au développement de modèles de Score de Risque

Polygénique (SRP) adaptés à la population indienne, permettant des stratégies de prévention des maladies personnalisées à grande échelle ;

- Épidémiologie prédictive : l'IA excelle dans l'identification de tendances au sein de données complexes, ce qui en fait un outil puissant pour la création de systèmes d'alerte précoce aux épidémies. *DEPA Entraînement* fournit le mécanisme permettant de connecter des flux de données disparates provenant de plateformes telles que le portail Nikshay (https://nikshay.in/) pour la gestion de la tuberculose et la plateforme de télémédecine eSanjeevani (https://stg.esanjeevani.in), créant ainsi un véritable système national d'intelligence sanitaire prédictive ;
- Découverte et développement de médicaments : ce cadre peut accélérer le développement de nouveaux médicaments et la réutilisation de médicaments existants pour les maladies répandues en Inde, en permettant aux chercheurs d'entraîner des modèles d'IA sur une combinaison riche de données d'essais cliniques, de données réelles de patients et d'informations génomiques.

La faisabilité technique de cette vision a été démontrée. Le projet pionnier Penn Médicine/Intel (https://download.intel.com/newsroom/archive/2025/en-us-2022-12-05-intel-and-penn-medicine-announce-results-of-largest-medical-federated-learning-study.pdf), une fédération de 71 institutions internationales, a eu recours à l'Apprentissage Fédéré au sein d'une Salle Blanche Confidentielle pour entraîner un modèle d'IA supérieur pour la détection des tumeurs cérébrales sans partager les données brutes des patients. Le modèle collaboratif a atteint plus de 99% de la précision d'un modèle hypothétique entraîné sur des don-

nées centralisées. Ce cas démontre que la confidentialité peut être préservée avec une perte de performance négligeable, mais il souligne également que les obstacles les plus importants sont d'ordre non-technique. Le succès de l'OAR de DEPA pour le secteur de la santé dépendra de sa capacité à apporter la clarté juridique et de gouvernance nécessaire pour favoriser la confiance et la participation.

Services financiers : faciliter l'accès au crédit et atténuer les risques

Le secteur des services financiers indien a réalisé d'énormes progrès en matière d'inclusion numérique. Pourtant, on estime que 400 millions de personnes et un grand nombre de PME restent en dehors de l'écosystème de crédit formel. Le goulet d'étranglement des données d'entraînement en est l'une des causes profondes. Le cadre *DEPA Entraînement* vise à lever cette impasse en permettant l'utilisation sécurisée et agrégée de « données alternatives », ouvrant ainsi l'accès au crédit aux populations mal desservies.

Les modèles traditionnels de notation de crédit excluent de fait les personnes sans historique de prêt formel. Les données alternatives — telles que les données transactionnelles issues des déclarations de TPS et des plateformes de commerce électronique, l'historique des paiements de factures de services publics et les données de la chaîne d'approvisionnement — fournissent de précieux indicateurs de santé financière et de capacité de remboursement. En permettant aux prêteurs et aux innovateurs FinTech d'entraîner des modèles d'IA sur des versions agrégées et désidentifiées de ces jeux de données, DEPA peut contribuer à créer des scores de crédit pour des millions d'Indiens « invisibles pour le crédit ».
Cette mesure s'attaque directement à la cause profonde

du déficit de crédit aux PME — estimée entre 20 et 25 milliards de roupies : l'asymétrie d'information. En créant un mécanisme fiable de mutualisation et d'analyse des données transactionnelles agrégées, le cadre réduit le risque perçu associé aux nouveaux emprunteurs et aux emprunteurs de petite taille, permettant ainsi aux prêteurs d'élargir le marché du crédit. Cela stimulerait non seulement la croissance du secteur des PME, qui contribue à près d'un tiers du PIB indien, mais renforcerait également la stabilité des établissements de crédit en leur ouvrant un vaste nouveau marché.

Le défi ne réside pas seulement dans un manque de volonté, mais dans des frictions systémiques. Les récentes mesures réglementaires de la RBI (Reserve Bank of India) à l'encontre de grandes banques pour des défaillances de leur infrastructure informatique mettent en lumière un problème fondamental : nombre d'établissements historiques sont alourdis par des systèmes patrimoniaux obsolètes, techniquement incapables de prendre en charge des échanges de données modernes et sécurisés. *DEPA Entraînement* offre un contournement essentiel à ce problème, en créant un ensemble de canaux standardisés et sécurisés permettant la circulation des données agrégées et en autorisant l'innovation à progresser sans être retenue en otage par la dette technologique des établissements individuels.

Éducation et formation professionnelle : bâtir une main-d'œuvre prête pour l'avenir

Alors que l'Inde s'engage dans la Quatrième Révolution Industrielle, la qualité de son capital humain sera son atout le plus critique. Le secteur de l'éducation et de la formation

professionnelle, dont la valeur devrait dépasser 29 milliards de dollars d'ici 2030, est confronté à la mission de préparer 250 millions d'étudiants à un avenir où les compétences — et non les seuls diplômes — seront la monnaie de l'emploi. Le cadre *DEPA Entraînement* peut servir d'infrastructure de données fondamentale pour permettre cette transition.

- Apprentissage adaptatif à grande échelle : les systèmes d'apprentissage adaptatif basés sur l'IA peuvent personnaliser l'enseignement en fonction des besoins individuels des élèves — une méthode dont des études ont montré qu'elle améliore les résultats aux tests de 30% en moyenne. Cependant, l'entraînement de ces systèmes nécessite de vastes jeux de données diversifiés sur les performances des apprenants, actuellement cloisonnés au sein des établissements. DEPA peut libérer ces données, permettant ainsi le développement de plateformes d'apprentissage personnalisé efficaces à l'échelle nationale ;

- Le dividende du « Passeport de Compétences » : une lacune critique du système actuel est la signalisation inefficace des compétences entre éducation et emploi. Les « passeports de compétences » portables et vérifiables, ou Dossiers d'Apprentissage et d'Emploi (DAE), constituent une solution fondée sur les données. En créant un système fiable et interopérable d'enregistrement et de partage des qualifications vérifiées, DEPA peut améliorer l'efficacité du marché du travail. De manière cruciale, DEPA peut se combiner aux registres numériques nationaux les plus récents, tels que la Banque Académique de Crédits (BAC) déployée dans le cadre de la Politique Nationale d'Éducation de 2020, afin de servir de compte bancaire vivant pour les acquis académiques. Les solutions peuvent être personnalisées pour aider les employeurs à prendre

des décisions de recrutement plus précises et fondées sur les données, tandis que les travailleurs bénéficient d'un dossier complet concernant leur formation continue, améliorant ainsi leur mobilité professionnelle. Ceci est particulièrement crucial pour promouvoir l'équité, car cela permet aux individus d'obtenir une reconnaissance officielle des compétences acquises par des voies non-traditionnelles.

L'expérience d'autres grands pays fédérés montre que la mise en place d'un tel cadre national de données est autant un défi politique et organisationnel que technique. Le succès de l'OAR de DEPA pour l'éducation dépendra de sa capacité à dégager un consensus sur des normes de données communes, à combler les silos organisationnels entre les différents ministères et gouvernements des États, et à établir un cadre de gouvernance qui utilise des outils technologiques pour instaurer et maintenir la confiance du public tout en accélérant l'innovation en IA à grande échelle.

En définitive, *DEPA Entraînement* devrait être perçu comme bien plus qu'un simple cadre de référence. C'est la prochaine grande contribution de l'Inde aux biens communs mondiaux : une Infrastructure Publique Numérique de deuxième génération conçue non pas seulement pour les transactions, mais pour la confiance. S'appuyant sur le succès avéré de l'India Stack, DEPA propose un modèle évolutif, interopérable et reproductible pouvant être adopté par des nations et des consortia du monde entier. Il fournit le chaînon manquant qui relie les principes d'une IA digne de confiance à leur réalité pratique et applicable.


ISPIRT
Inria
FONDATION