Systèmes nationaux d'information

Aadhaar (Inde) et proposition pour la République du Bénin — avec étude du système de fichiers CP/M

Question 2 : Aadhaar, le système national d'identification de l'Inde

Présentation

Aadhaar (« fondation » en hindi) est le système d'identité numérique géré par l'**UIDAI** (Unique Identification Authority of India), lancé en 2009 et encadré par l'Aadhaar Act de 2016. Chaque résident reçoit un **numéro aléatoire à 12 chiffres**. Plus de 1,3 milliard de personnes sont enregistrées, ce qui en fait la plus grande base d'identité biométrique au monde. Son objectif principal est de permettre à chacun de prouver son identité partout dans le pays, et à l'État de verser les aides sociales directement aux bons bénéficiaires, sans intermédiaires ni doublons.

Les données qui alimentent le système

Catégorie	**Données**	**Rôle**
Démographiques obligatoires	Nom, date de naissance (ou âge), sexe, adresse	Identifier la personne
Démographiques facultatives	Numéro de mobile, e-mail	Authentification par OTP, notifications
Biométriques	Photo du visage, 10 empreintes digitales, 2 scans d'iris	Garantir l'unicité (dédoublonnage) et authentifier
Justificatifs	Preuve d'identité (PoI), preuve d'adresse (PoA), ou attestation d'un « introducteur » pour les personnes sans papiers	Valider les déclarations à l'inscription
Données de transaction	Journaux d'authentification (date, heure, organisme demandeur, résultat)	Traçabilité et audit

Le circuit des données fonctionne ainsi :

1. **À l'inscription**, des agences agréées (banques, postes, administrations) collectent les données démographiques et biométriques. Celles-ci sont chiffrées sur place puis envoyées au **CIDR** (Central Identities Data Repository), le dépôt central.
2. **Le CIDR effectue un dédoublonnage biométrique.** La nouvelle personne est comparée à toutes celles déjà enregistrées. Le numéro n'est attribué que si elle n'existe pas encore.
3. **À l'usage**, un organisme (banque, distribution de rations, opérateur télécom) envoie une requête d'authentification. Le système ne répond que « oui/non », ou renvoie un e-KYC limité si la personne y consent. L'organisme n'accède jamais à la base elle-même.
4. **Les mises à jour** (changement d'adresse, de téléphone) passent par le portail en ligne ou un centre physique.

Aadhaar est aussi la brique centrale de la « trinité JAM » (comptes bancaires Jan Dhan, Aadhaar, Mobile), sur laquelle reposent les transferts directs de prestations (DBT).

Les limites nourrissent la question 3. On observe des exclusions dues aux échecs biométriques (empreintes usées des travailleurs manuels, personnes âgées). Des fuites de données ont eu lieu via des sites tiers. Des risques de surveillance ont été soulevés : en 2018, la Cour suprême indienne (arrêt Puttaswamy) a restreint l'usage d'Aadhaar par les entreprises privées.

Question 3 : S'en inspirer pour un système national au Bénin

Point de départ : ce qui existe déjà

Le Bénin ne part pas de zéro. Le RAVIP (Recensement Administratif à Vocation d'Identification de la Population) a permis d'attribuer à chaque personne un **Numéro Personnel d'Identification (NPI)**, géré par l'**ANIP** (Agence Nationale d'Identification des Personnes). Le pays participe aussi au projet régional WURI, soutenu par la Banque mondiale. Il dispose en outre d'un cadre juridique, le **Code du numérique** (loi n° 2017-20), et d'une autorité de contrôle, l'**APDP** (Autorité de Protection des Données Personnelles).

La bonne proposition n'est donc pas de « copier Aadhaar », mais de faire du NPI le pivot d'un système intégré de services publics : le **Système National d'Identité et de Services (SNIS-Bénin)**.

Proposition : le SNIS-Bénin

1. Le noyau identité (inspiré d'Aadhaar). Le NPI reste l'identifiant unique. Le système y rattache un jeu de données minimal : état civil, photo, empreintes, téléphone. Le dédoublonnage biométrique se fait au niveau central. L'enregistrement des naissances à l'état civil doit être relié directement à l'attribution du NPI, afin que chaque enfant reçoive son numéro dès la naissance.

2. Une couche d'authentification et d'échange. Les administrations (santé via le programme ARCH, éducation, impôts, CNSS) et les acteurs privés agréés (banques, opérateurs mobiles comme MTN, Moov et Celtiis, fournisseurs de mobile money) interrogent le système avec une réponse « oui/non » ou un e-KYC minimal, sur le modèle d'Aadhaar. Chaque administration conserve ses propres données, et elles s'échangent via une plateforme sécurisée plutôt que d'être centralisées dans une base unique. Ce principe s'inspire du X-Road estonien.

3. Les données qui alimenteraient le système béninois :

- l'état civil (naissances, mariages, décès), déclaré par les mairies et les centres de santé ;
- l'enrôlement biométrique fait par l'ANIP et ses points mobiles ;
- les numéros de téléphone vérifiés par les opérateurs, pour les codes OTP ;
- les registres sectoriels : bénéficiaires de l'ARCH, élèves et étudiants, contribuables, assurés sociaux ;
- les journaux d'authentification, pour l'audit.

4. Les adaptations au contexte béninois (tirées des limites d'Aadhaar) :

- **Authentification hors-ligne**, par une carte à QR code signé ou une vérification par USSD. La connexion Internet est irrégulière dans certaines zones rurales, par exemple dans l'Atacora ou l'Alibori.
- **Des alternatives à la biométrie** (OTP, visage, agent vérificateur), pour ne pas exclure les personnes dont les empreintes sont illisibles.

- **Une interface multilingue** (français, fon, yoruba, bariba, dendi…) et des agents de proximité.
- **La protection des données** sous le contrôle de l'APDP : minimisation des données partagées, journal consultable par chaque citoyen (« qui a consulté mes données ? ») et sanctions en cas d'abus.
- **Une dimension régionale**, grâce à l'interopérabilité avec les pays voisins via WURI et la CEDEAO, pour faciliter la libre circulation.

5. Les bénéfices attendus : ciblage des aides sociales et des bourses, lutte contre les fonctionnaires fictifs, ouverture de comptes mobile money pour l'inclusion financière, dossier de santé suivi, et démarches en ligne sur service-public.bj simplifiées.

Bonus : le système de fichiers CP/M (1974)

CP/M (Control Program for Microcomputers) a été créé par Gary Kildall (Digital Research) pour les micro-ordinateurs 8 bits. Il était conçu pour des disquettes 8 pouces d'environ 250 Ko (77 pistes de 26 secteurs de 128 octets).

L'organisation du disque. Les deux premières pistes sont réservées au système : le chargeur de démarrage, le CCP (l'interpréteur de commandes) et le BDOS. Vient ensuite le **répertoire**, qui compte typiquement 64 entrées de 32 octets. Les blocs de données suivent, avec une unité d'allocation de 1 Ko sur une disquette standard.

Un système « plat ». CP/M n'a aucun sous-répertoire. Pour séparer les fichiers, il propose seulement des **zones utilisateur numérotées de 0 à 15**. Les noms suivent le format **8.3**, par exemple RAPPORT.TXT.

La structure d'une entrée de répertoire (32 octets) :

Octet(s)	Contenu
0	Numéro d'utilisateur (0–15) ; la valeur E5h signifie « fichier supprimé »
1–8	Nom du fichier ; les bits de poids fort servent d'attributs
9–11	Extension ; les bits de poids fort codent les attributs lecture seule, système et archive
12	EX, numéro d'extent (partie basse)
13–14	S1, S2 (S2 contient la partie haute du numéro d'extent)
15	RC, nombre d'enregistrements de 128 octets dans cet extent
16–31	Carte d'allocation : 16 numéros de blocs sur 8 bits, ou 8 sur 16 bits pour les grands disques

Les points remarquables :

- **Les extents.** Une entrée décrit au plus 16 Ko. Un fichier plus gros occupe donc plusieurs entrées portant le même nom et des numéros d'extent successifs.
- **Aucune table d'espace libre sur le disque.** Quand un disque est monté, le BDOS parcourt le répertoire et reconstruit en mémoire une table de bits des blocs occupés.

- **Une taille de fichier comptée en enregistrements de 128 octets.** La taille exacte en octets n'est pas connue. Les fichiers texte se terminent donc par le caractère ^Z (1Ah), une convention héritée ensuite par MS-DOS.
- **Une astuce de conception.** Un disque neuf est formaté avec des octets E5h, si bien que toutes les entrées apparaissent d'emblée comme « supprimées », c'est-à-dire libres. Il n'y a pas d'étape d'initialisation du répertoire.
- **Aucun horodatage** dans les premières versions, ni aucune permission par utilisateur.

Le lien avec le sujet. Le répertoire de CP/M est en fait un petit « registre national » de fichiers. Chaque entrée associe un identifiant unique (nom + zone utilisateur) à des métadonnées et à la localisation physique des données. On retrouve les mêmes principes et les mêmes défis que dans un système d'identité national :

1. garantir l'unicité (pas de doublon de nom, comme pas de doublon de NPI) ;
2. gérer la suppression proprement (le marqueur E5h, comme la gestion des décès à l'état civil) ;
3. reconstruire l'état global à partir des entrées (la table de bits, comme les statistiques nationales).

L'absence de sous-répertoires et de permissions dans CP/M montre aussi ce qu'un système national moderne doit ajouter : une hiérarchie des accès et une traçabilité de qui consulte quoi.