

RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION : PRATIQUES ACTUELLES EN ESTONIE, EN INDE ET EN AUTRICHE

SOMMAIRE

id4d.worldbank.org



VUE D'ENSEMBLE

Si les systèmes d'identification numérique peuvent être un facteur de transformation dans de nombreux domaines, ils posent également - comme tout système qui recueille, utilise et conserve des données personnelles - des problèmes de protection de la vie privée et des données¹. Comme le soulignent les *Principes généraux sur l'identification*², la protection des données personnelles dans les systèmes d'identification numérique nécessite non seulement un cadre juridique complet, mais également **une approche visant à assurer le respect de la vie privée et la sécurité dès la conception (PbD)**³ qui :

1. **Met en place des systèmes proactifs – et non réactifs** – qui jouent un rôle préventif ;
2. **Considère le respect de la vie privée comme la norme par défaut**, au lieu de nécessiter une action positive ;
3. **Intègre le respect de la vie privée dans la conception technique** dès le départ plutôt qu'à un stade ultérieur ;
4. **Considère le respect de la vie privée comme une solution qui profite à tous** (« gagnant-gagnant ») et non comme un jeu à somme nulle (« soit/soit ») ;
5. **Assure la sécurité de bout en bout**, dans un souci de protection pendant le cycle de vie complet ;
6. **Garantit visibilité et transparence**, grâce à des systèmes ouverts et responsables ; et
7. **Maintient un système axé sur l'utilisateur**, le but étant d'assurer la confidentialité des données personnelles.

Afin de comprendre les pratiques PbD actuellement en place dans les systèmes d'identification numérique, un rapport récemment publié dans le cadre de l'initiative ID4D examine différents moyens de contrôle juridique, opérationnel et technique utilisés en Estonie, en Inde et en Autriche⁴.

ESTONIE – Exemple de pratique PbD : le Portail des citoyens

En Estonie, le Portail des citoyens (eesti.ee) offre aux utilisateurs divers outils pour contrôler leurs données. Premièrement, il permet aux utilisateurs de voir qui a accédé à leurs données grâce à l'écran de contrôle de l'utilisation des données personnelles⁵ qui affiche toutes les opérations contenant des données personnelles. Un utilisateur peut vérifier sur ces registres si ses données ont été utilisées sans autorisation et contester tout accès non autorisé. Deuxièmement, le portail permet aux utilisateurs de contrôler quelles données sont communiquées, et à qui. Dans le cas des services de santé, par exemple, les patients peuvent accéder à leurs dossiers médicaux électroniques sur le Portail des patients en ligne et choisir quelles données communiquer aux prestataires de service après avoir authentifié leur identité grâce à leur identifiant numérique.

INDE – Exemple de pratique PbD : Identité virtuelle et tokenisation

Le système d'identification Aadhaar offre de nombreux moyens de protection de la vie privée, notamment : a) une identité virtuelle ; b) la tokenisation en aval. Le service d'identification virtuelle utilise la tokenisation en amont pour permettre aux utilisateurs d'empêcher les prestataires de service de voir leur numéro Aadhaar (un numéro unique à 12 chiffres) en créant au hasard un numéro d'identification virtuelle à 16 chiffres. Une fois que l'utilisateur a créé un identifiant virtuel, il peut communiquer ce numéro à 16 chiffres au lieu de son numéro Aadhaar aux fins d'authentification. Un aspect essentiel pour renforcer le respect de la vie privée est le fait que l'identifiant virtuel est temporaire et révocable. Par ailleurs, UIDAI (Unique Identification Authority of India) utilise un système de tokenisation en aval pour régler la question du stockage des numéros Aadhaar dans les bases de données des prestataires de service. Par conséquent, lorsqu'un utilisateur communique son numéro Aadhaar ou son identifiant virtuel à un prestataire de service aux fins d'authentification, le système utilise une fonction de hachage cryptographique pour générer un token alphanumérique à 72 caractères propres à ce prestataire qui est enregistré à la place du numéro Aadhaar complet à 12 chiffres. Étant donné que différents services reçoivent différents tokens pour la même personne, il est impossible d'établir un lien entre les données de différentes bases de données.

1. <https://id4d.worldbank.org/research> ou <http://documents.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf>

2. <https://id4d.worldbank.org/principles>

3. D'abord conceptualisé par Ann Cavoukian comme "Privacy by Design" ou PbD. Voir Cavoukian, Ann. 2011. Privacy by Design. https://iab.org/wp-content/uploads/2011/03/fred_carter.pdf

4. <https://id4d.worldbank.org/research> ou <http://documents.worldbank.org/curated/en/546691543847931842/pdf/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria.pdf>

5. <https://github.com/e-gov/AJ>

AUTRICHE - Exemple de pratique PbD : Identifiants propres à chaque secteur

L'Autriche a pris diverses mesures pour réduire la possibilité d'établir un lien entre différentes bases de données. Au lieu d'enregistrer l'identifiant numérique à 12 chiffres (numéro CRR) sur la carte d'identité virtuelle des citoyens autrichiens, le système enregistre le « SourcePIN » — un identifiant unique créé au moyen d'une rigoureuse méthode de cryptage du numéro CRR. Les données figurant sur la carte d'identité virtuelle portent la signature numérique de l'autorité chargée d'enregistrer les nouveaux SourcePIN et sont protégées par un numéro d'identification personnel (code PIN). En outre, la loi sur l'administration en ligne stipule que différents identifiants doivent être utilisés pour chacun des 26 secteurs de l'administration publique. Un identifiant personnel propre à chaque secteur (ssPIN) est créé à partir du SourcePIN en utilisant un algorithme de dérivation à sens unique qui permet de calculer un PIN propre à chaque secteur à partir du SourcePIN.

Les autorités publiques peuvent utiliser le ssPIN pour rechercher les données d'un citoyen stockées dans le même secteur, par exemple si elles ont besoin d'accéder aux données d'un citoyen ou de les utiliser pour pré-remplir des formulaires.

D'autres exemples de pratiques PbD dans chacun des trois pays susmentionnés sont brièvement décrits ci-dessous. Pour en savoir plus sur les pratiques PbD, veuillez consulter complet sur la question et le Guide⁶ du praticien de l'ID4D⁶ sur le site Web de l'initiative ID4D.

EXEMPLES DE PRATIQUES DE RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION À TRAVERS LE MONDE



Collecte de données limitée	Limitation de l'objet	Tokenisation
 Seulement quatre champs obligatoires pour les données démographiques  Principe de ne recueillir les données qu'« une seule fois »	 Échange de données via X Road avec l'autorisation de l'Autorité centrale  Données biométriques chiffrées sur l'appareil pour l'accès	 Identifiant d'utilisateur unique associé de manière cryptographique à une clé numérique empêchant les possibilités de connexion entre différentes bases de données 
Sécurité	Consentement	Anonymisation
 Signature numérique et chiffrage des données pour assurer l'intégrité et la sécurité, chiffrement de bout en bout de données stockées ou en transit.  	 Consentement de l'utilisateur au partage de données obtenu via l'authentification  	 Pseudonymisation et anonymisation des données personnelles 
Portail de transparence	Responsabilité	Minimisation des données
 Possibilité pour les utilisateurs de visualiser et actualiser les données personnelles et l' historique des transactions sur le portail 	 Registres de transactions inviolables signés numériquement et horodatés 	 Numéro d'identification inintelligent et aléatoire 
		Accès aux données limité
		 Données biométriques chiffrées sur un appareil limitant l'accès  Possibilité de verrouiller les données biométriques lorsqu'elles ne sont pas utilisées

6. <https://id4d.worldbank.org/guide>