IDEMIA
PUBLIC
SECURITY

Les préconisations d'IDEMIA en lien avec la technologie biométrique dans le domaine de l'identité

De plus en plus fréquemment, les Etats s'appuient sur la biométrie (reconnaissance faciale, de l'iris ou des empreintes digitales) pour sécuriser l'accès à des services publics, en ligne ou en présentiel. La motivation principale des Etats pour mettre en place ce type de système est généralement de réduire le risque de fraude à l'identité (par exemple, dans le cas où un Etat distribue aux fermiers de l'engrais pour leurs plantations, éviter que des personnes non éligibles ne récupèrent l'engrais pour le revendre ensuite aux fermiers).

Le taux d'erreur d'authentification à l'aide de technologies biométriques est considérablement plus faible que celui d'autres techniques, par exemple lorsque la vérification de l'identité d'une personne s'effectue à l'œil nu, sur la base d'une photo présente sur un document d'identité. C'est pour cette raison que la Banque Mondiale ou l'USAID financent les projets de mise en place de registres d'identité biométrique et d'e-ID, notamment en Afrique. Ils permettent d'améliorer l'accès aux services publics et l'inclusion des citoyens.

Certaines précautions doivent être prises lors de la mise en place de systèmes biométriques :

- Au moment de l'établissement des registres (phase d'acquisition des données biométriques), le système peut considérer de manière erronée - mais avec une faible probabilité - qu'une personne existe déjà (« faux doublon »). Dans ce cas, il est d'usage de réaliser une enquête administrative pour écarter le risque de fraude et effectuer un dédoublement biométrique. Une personne ne devrait pas être exclue de l'enregistrement uniquement sur la base de la détection d'un doublon.

- Au moment où la personne souhaite accéder à un service, il est possible qu'elle ne soit pas reconnue, en raison d'un accès réseau dégradé ou pour d'autres raisons techniques. Néanmoins, les technologies d'IDEMIA présentent un taux d'erreur très faible (< 0.5% pour la reconnaissance des empreintes digitales, d'après les dernières évaluations du NIST). Ce taux d'erreur est plus élevé pour les personnes dont les doigts sont très abimés, tout en restant, là encore, très faible. Le groupe démographique n'a quasi aucune incidence sur la performance des algorithmes biométriques d'identification d'IDEMIA et algorithmes d'IDEMIA, qui sont régulièrement évalués comme étant les plus équitables du marché.

Là aussi, IDEMIA recommande de mettre en place une procédure de remédiation pour permettre l'accès d'une autre manière, soit en faisant appel à un autre type de biométrie (authentification par empreinte digitale ou par reconnaissance faciale), soit en revenant à la méthode pré-biométrie (en général, contrôle de l'identité d'une personne par un agent habilité à le faire sur la base d'une photo présente sur un document d'identité).

- La mise en place de ces systèmes ne devrait pas avoir pour effet de priver l'accès à des services publics à une partie de la population sur une base discriminatoire, notamment indirecte.

- L'identification numérique ne devrait pas être l'unique moyen d'accès aux biens et services de base, en particulier lorsqu'un défaut d'accès en raison d'une erreur technique est susceptible de porter atteinte aux droits humains des personnes concernées ou risquerait de leur porter un préjudice vital.

- Enfin, dans la mesure où ces systèmes impliquent la collecte et l'utilisation de données biométriques sensibles, IDEMIA recommande que le déploiement de ces systèmes soit précédé d'une étude d'impact en matière de confidentialité, de protection des données et de droits humains.

IDEMIA met systématiquement en avant ces préconisations auprès de ses clients et travaille activement à les intégrer dans les guides de bonnes pratiques ou recommandations publiées par les groupes de travail auxquels elle participe.