L'AGENCE GOUVERNEMENTALE DES PAPIERS D'IDENTITÉ SÉCURISE MAL NOS DONNÉES !

COMMUNIQUÉ
PARIS, LE 28 AVRIL 2026

Un exemple frappant parmi plusieurs vols récents au sein des administrations publiques[1].

« Mercredi 15 avril 2026, l'agence nationale des titres sécurisés (ANTS) a détecté un incident de sécurité pouvant impliquer une divulgation de données issues de comptes particuliers et professionnels du portail ants.gouv.fr ».

C'est ainsi que l'ANTS a annoncé que les données de 11 à 12 millions personnes pour obtenir passeport, carte d'identité, permis de conduire ou carte grise ont été volées par des hackers, notamment : identifiant de connexion, civilité, nom, prénoms, adresse électronique, date de naissance, identifiant unique du compte.

L'ANTS affirme avoir informé les personnes concernées par un mail sans qu'aucune démarche ne soit à effectuer. Elle les met cependant en garde contre les tentatives d'hameçonnage (*phishing*) dont elles pourraient être victimes. En somme, rien de plus que les consignes habituelles, régulièrement rappelées par les services de communication du gouvernement !

Pourtant, le 22 septembre 2025, l'ANTS affirmait : *« En tant qu'opérateur du ministère de l'Intérieur manipulant des données sensibles, l'ANTS fait l'objet de mesures de sécurité renforcées et d'une vigilance permanente des services de l'Etat contre toute intrusion, physique ou informatique. »* Dans la foulée, elle se dotait d'une « charte éthique » qui promettait de mettre *« en place les mesures adéquates pour garantir la sécurité des données et des systèmes suivant les exigences qui s'y appliquent »* et de protéger *« les informations sensibles contre toute forme de menace, qu'elle soit interne ou externe. »*

Avec le vol, cette fois confirmé, un signalement a été transmis à la Commission nationale de l'informatique et des libertés (CNIL), ainsi qu'au parquet de Paris qui a confié les investigations à l'Office anti-cybercriminalité. De son côté, le ministre de l'Intérieur a demandé à l'Inspection générale de l'administration d'établir la chaîne de responsabilités.

Lors de la création du fichier baptisé « titres électroniques sécurisés » (TES), la LDH avait alerté sur les dangers inhérents aux bases de données centralisant des informations personnelles et biométriques sur la quasi-totalité de la population française[2].

Depuis, ce qu'on appelait des risques sont devenus des certitudes, notamment avec l'introduction de l'IA pour profiter des vulnérabilités des systèmes. Nos données ne sont pas en sécurité. Leur centralisation accroit les effets de chaque intrusion.

Les politiques publiques de protection de nos données ne peuvent plus se contenter d'être des promesses creuses. Elles doivent passer par le renforcement des mesures de protection tant physique que technique, même si celle-ci ne pourra pas être absolue. Mais surtout, elles impliquent de rompre avec

[1] Parcoursup vient d'annoncer le vol de données de 705 000 dossiers, par l'utilisation du compte d'un agent, en octobre 2025. Outre le peu de sécurisation des comptes des agents, l'absence de transparence interroge, car le risque d'utilisation frauduleuse est évident.
[2] https://www.ldh-france.org/toussaint-2016-retour-du-fichier-gens-honnetes/

une vision axée sur la seule centralisation des données. Mettre les moyens, tant humains, budgétaires que technologiques, dans la protection de nos données est une condition de la survie de nos libertés individuelles et par conséquent, de nos démocraties.