RÉPUBLIQUE FRANÇAISE

Vie publique
Au cœur du débat public

Six questions pour comprendre l'identité numérique

Publié le 3 mai 2023
8 minutes
Par : La Rédaction

France identité, e-carte Vitale, FranceConnect... La numérisation croissante de la société, la dématérialisation des démarches administratives et du secteur privé présentent de nombreux enjeux. La protection et la fiabilité de l'identité numérique sont au centre des préoccupations. L'essentiel en six questions.

Qu'est-ce que l'identité numérique ?

L'identité numérique a plusieurs formes. Une définition large désigne l'ensemble des traces laissées par une personne sur internet, notamment :

- l'identité civile (noms, prénom, date de naissance...) de la personne, renseignée lors de démarches administratives en ligne, par exemple ;
- les identifiants, avatars, pseudonymes pour accéder à un compte ou à un service en ligne ;
- les traces laissées en naviguant sur internet ("*cookies*") ;
- les commentaires, photos, vidéos publiés sur les réseaux sociaux ;
- l'adresse IP (numéro d'identification de l'ordinateur) ;
- la géolocalisation (GPS).

Une approche de l'identité numérique, au sens régalien, concerne les identifiants qui permettent à une personne de s'authentifier pour accéder à des services en ligne : l'état civil ou d'autres attributs (numéro de sécurité sociale, par exemple).

Quels sont les risques liés à l'identité numérique ?

Les traces laissées sur internet comprennent des risques liés à la protection des données personnelles et de la vie privée :

- usurpation d'identité : utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses ;
- vols de données personnelles ;
- fraude aux paiements en ligne, en particulier la fraude à la carte bancaire ;
- atteinte à la réputation en ligne (e-réputation)...

Quel est le cadre juridique de l'identité numérique ?

Le cadre légal de l'identité numérique prévoit de protéger les internautes, particuliers et personnes morales. Il comprend essentiellement :

- le règlement général sur la protection des données (RGDP) pour protéger les données personnelles des citoyens de l'Union européenne (UE) : il prévoit par exemple l'obligation, pour les fournisseurs de services, de demander le consentement des personnes avant de recueillir et d'utiliser leurs données ;
- le règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS) qui a pour objectif notamment de permettre aux citoyens d'utiliser leurs propres systèmes nationaux d'identification électronique pour l'accès aux services publics en ligne dans d'autres pays de l'UE ;
- la directive NIS qui prévoit de renforcer la cybersécurité des opérateurs de services essentiels au fonctionnement de l'économie et de la société : grandes entreprises, entreprises de taille intermédiaire et établissements publics ;
- le référentiel général de sécurité (RGS) pour protéger les échanges au sein de l'administration et avec les citoyens ;
- la norme de sécurisation DSP2 pour les paiements en ligne .

Quelles sont les institutions régulatrices de l'identité numérique ?

Plusieurs institutions veillent à la régulation de l'identité numérique et au respect des droits et libertés, notamment :

- la CNIL rend des avis sur des projets de loi (ou décret) concernant la protection des données personnelles et contrôle la bonne application de la règlementation. Elle a, par exemple, sanctionné en 2021 Google et Facebook à hauteur respectivement de 150 millions d'euros et de 60 millions d'euros pour non-respect de la loi concernant la gestion des *cookies* ;

- le Conseil d'État conseille le gouvernement sur le respect des règles, notamment le RGPD, d'un projet de texte. Il est aussi compétent pour juger des recours contre les textes. Par exemple, il a été saisi en 2019 d'un recours en illégalité contre le décret de création d'Alicem (prototype d'application d'identité numérique de l'État sur mobile) qui prévoyait l'activation du compte par reconnaissance faciale (décision du Conseil d'État 432656 de novembre 2020) ;

- le Comité européen de la protection des données (CEPD) assure la cohérence de la mise en œuvre du RGPD entre les différents États membres.

Qu'est-ce que le service public d'identité numérique ?

La mise en place du service numérique France identité doit permettre de garantir son identité officielle et de s'authentifier en ligne avec la même sécurité que la carte d'identité papier. L'usager peut ainsi utiliser plusieurs services publics comme les impôts ou la sécurité sociale. Selon la CNIL, 2 954 568 cartes nationales d'identité électroniques ont été créées en 2021.

Cet outil, basé sur la nouvelle carte d'identité électronique, associe trois éléments :

- la puce de la carte d'identité qui comprend les données d'identité (nom, prénom, date et lieu de naissance, sexe) ;

- le code personnel de la carte ;

- une application pour utiliser son état civil et prouver son identité dans le monde numérique.

L'État encourage les programmes d'identité nationale électronique pour améliorer la confiance dans les échanges et l'accessibilité aux services publics. FranceConnect permet la connexion sécurisée aux services de l'administration avec une identité unique. Près de 14 millions d'utilisateurs se sont

connectés à FranceConnect pour le seul mois de décembre 2021.

La CNIL est favorable à cette "*identité numérique d'État de haut niveau*", qui renforce "*la sécurité des procédures*". Pour l'institution, la généralisation de l'usage de FranceConnect soulève cependant régulièrement la question de l'utilisation proportionnée d'un service d'identité numérique régalien pour des usages de la sphère privée.

Et l'identité numérique européenne ?

La Commission européenne a proposé, le 3 juin 2021, la création d'un système européen de gestion de l'identité : une identité numérique régalienne (e-ID) sécurisée.

Le "*portefeuille européen d'identité numérique* " (PEIN) ou "*European Digital Identity Wallet*" contiendra les identités numériques et attestations fournies aux personnes dans différents pays de l'Union européenne (par exemple, un diplôme d'une université belge, une identité numérique française et un titre de séjour allemand), explique la CNIL.

Le PEIN "*répond à de nombreuses attentes*" de la CNIL en particulier parce que ce portefeuille européen :

- est facultatif et gratuit ;
- respecte la protection des données dès la conception et par défaut "*permettra de rendre interopérables des identités numériques dans tous les États membres et pour des services publics et privés*" (par exemple : accès à un compte bancaire, déclaration d'impôts, inscription à l'université).