DOSSIER THÉMATIQUE

L'identité **numérique**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

INTRODUCTION

L'identité, un concept aux multiples visages

La question de l'identité des individus est une composante importante de l'organisation de toute société, car elle permet notamment d'attribuer un statut ou un rôle à chacun dans une organisation collective.

L'identité ne se résume pas à l'état civil ou identité dite « régalienne », tenu en France dans les mairies depuis 1792 et dès le XIVe siècle dans les registres paroissiaux. **Elle renvoie en effet à plusieurs notions en sciences sociales :**

- **l'identité propre en philosophie (ipséité) ou ce qui fait qu'une personne est unique et distincte d'une autre ;**
- **l'identité personnelle, c'est-à-dire à la conscience et la représentation qu'une personne a d'elle-même ;**
- **l'identité sociale, qui peut être multiple et se réfère au groupe, aux catégories sociales dont on possède des attributs.**

Une même personne peut avoir plusieurs identités, car l'identité présentée dépend du contexte dans lequel elle est utilisée (état civil, vie sociale, vie professionnelle, jeux en ligne, etc.) **et de la confiance qui lui est accordée**.

Une distinction peut être faite entre une identité « régalienne », reliée à l'état civil de l'individu et qu'il utiliserait dans ses démarches administratives ou formelles, et une identité « non régalienne », qu'elle soit reliée à un pseudonyme qu'il pourrait utiliser par exemple sur un site de rencontres, ou à un nom et un prénom d'usage (même reconnus par l'État) qu'il pourrait utiliser pour acheter un objet en ligne.

L'identité numérique, ou les identités numériques, ont en effet pour particularité d'opérer un lien numérique entre **différentes formes d'identités** administratives ou caractérisées par les sciences sociales. Il s'agit ici d'un **ensemble d'attributs** tels qu'un pseudonyme, un nom, un prénom, un âge ou un lieu de naissance, associés à une personne physique, qui permet de relier ces données à cette personne.

Les identités numériques d'une personne sont ainsi ses différentes identités immatérielles, qui vont lui permettre d'accéder à des produits et services, principalement numériques.

Le développement des identités numériques s'inscrit pleinement dans la réflexion actuellement menée par **l'État, qui développe et encourage des moyens d'identification électroniques sécurisés**.

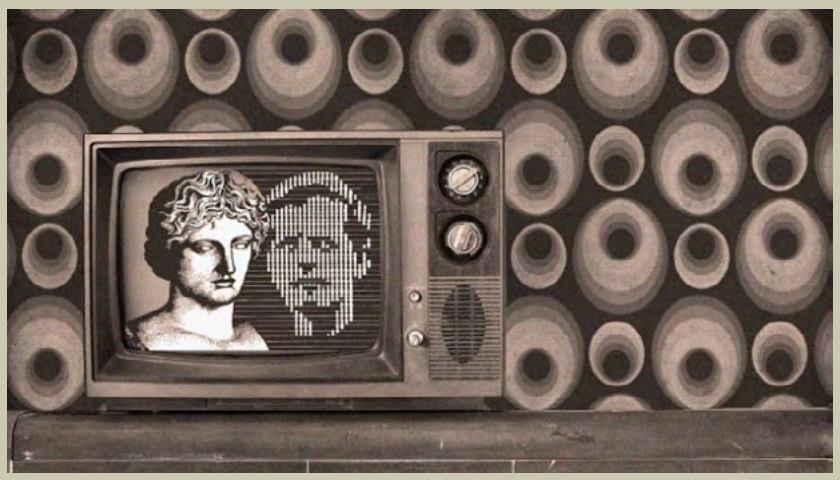
Si l'usage d'identités numériques peut constituer une garantie forte dans le contexte des transactions électroniques, il peut également être perçu comme une **démultiplication des possibilités de surveillance**, notamment par l'analyse des traces que la personne laissera dans l'environnement numérique. En effet, la numérisation massive des existences humaines nécessite d'assurer l'équilibre entre l'identification des personnes et la possibilité, pour elles, d'agir de façon libre et autonome.

Quelques chiffres sur l'identité numérique

13 910 064 utilisateurs se sont connectés sur le seul mois de décembre 2021 sur FranceConnect.

2 954 568 cartes nationales d'identité électroniques ont été créées en 2021.

UN PEU D'HISTOIRE...



En France, le service de la démographie du régime de Vichy avait été chargé en 1940 de constituer un fichier de population, le fichier national d'identification des personnes physiques, qui identifiait chaque personne sur la base d'un identifiant numérique significatif de 13 chiffres. À la Libération, le fichier fut réutilisé pour la (toute nouvelle) sécurité sociale et l'identifiant devint le numéro de sécurité sociale. L'Institut national de la statistique et des études économiques (Insee), invité en 1947 à participer à la remise en ordre des fichiers électoraux, reprit les travaux pour constituer le répertoire d'identification de toutes les personnes nées en France, qui a évolué et qui est plus connu aujourd'hui sous le nom de répertoire national d'identification des personnes physiques (RNIPP).

En mars 1970, ce même institut annonça un projet connu par la suite sous le nom de SAFARI (pour Système automatisé pour les fichiers administratifs et le répertoire des individus) et reposant sur l'informatisation du RNIPP. Ce répertoire national informatique de la population prévoyait d'utiliser le numéro de sécurité sociale (le NIR) comme identifiant unique à chaque individu pour l'ensemble des répertoires et fichiers publics. À la suite de l'annonce du projet SAFARI et des vifs débats relatifs aux enjeux pour la vie privée et les libertés individuelles que celui-ci a soulevés, la loi Informatique et Libertés est votée en 1978.

Cette loi, qui a par la suite connu de nombreuses évolutions, a posé la première pierre d'une sécurité nouvelle pour la protection de la vie privée des citoyens français et a donné naissance à la CNIL, première autorité administrative indépendante créée en France.

L'un des objectifs de la création de la CNIL fut d'éviter, en partie, la mise en place d'un registre national de la population française intégrant l'ensemble de ces informations et, notamment, un identifiant unique et persistant pour l'ensemble des services de l'État.

Aujourd'hui, la CNIL reste un des interlocuteurs incontournables des pouvoirs publics et des acteurs privés pour les accompagner dans leurs questionnements relatifs à l'identité numérique.

DE QUOI PARLE-T-ON ?
L'identité numérique

Dans le contexte de la protection des données, et plus largement dans celui des systèmes informatiques, **l'identité** correspond à un **ensemble d'attributs associés à une personne physique qui permet de la relier à d'autres données**.

Ces **attributs** sont des caractéristiques liées à la personne dans un contexte donné. Ils sont, par essence, variés. Certains sont relativement stables dans le temps, comme les nom, prénom, adresse, empreintes digitales et signature vocale par exemple. D'autres changent souvent, comme la géolocalisation ou la tenue vestimentaire.

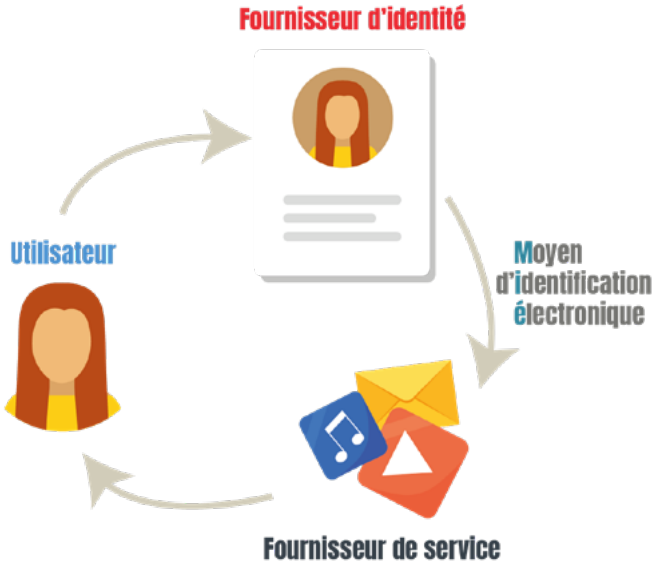
On parle d'**identité numérique** lorsque ces attributs sont enregistrés sous forme numérique, et utilisables en ligne notamment pour interagir avec des systèmes d'information. Une identité numérique repose sur un **moyen d'identification électronique (ou MIE)**, c'est-à-dire sur un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier à un service en ligne. Le MIE peut être une application sur un smartphone, une carte à puce ou encore un compte en ligne.

Pour une même personne, il existe plusieurs identités numériques puisqu'une identité dépend du contexte, mais aussi du niveau de garantie de sa fiabilité (attribut déclaré, choisi ou vérifié avec tel ou tel niveau de vérification).

Une identité numérique permet de créer un certain niveau de confiance numérique pour :

- **l'identification**, qui permet de **distinguer une personne** d'une autre dans une population donnée, par exemple avec l'utilisation d'identifiants nationaux tel que le numéro national étudiant (INE) ;
- **l'authentification**, qui permet à une personne de **prouver que c'est bien une de ses identités**, par exemple en indiquant le mot de passe correspondant à un identifiant ;
- **la preuve d'attributs d'identité**, qui permet de **démontrer des caractéristiques** de son identité (par exemple une nationalité, un statut d'étudiant, un âge ou le fait d'être majeur).

Les données d'identité sont utilisées dans la plupart des systèmes d'information pour gérer au moins les utilisateurs du système, ses administrateurs et les personnes concernées par les traitements de ce système. En particulier, les questions de politique d'habilitation, d'exactitude des données ou d'exercice des droits sont liées à la gestion des identités dans ces traitements. Pour autant, la CNIL ne vise pas ici la question de l'identité numérique dans ces contextes. Elle se focalise sur l'identité numérique utilisée dans le cadre de **schémas d'identification tels que ceux établis par le règlement européen eIDAS ou permettant son usage dans différents systèmes, selon des standards établis.**



Un schéma d'identification permettant à une personne d'utiliser son identité numérique fait intervenir au moins **trois acteurs :**

- un **utilisateur** : une personne physique qui souhaite accéder à un ensemble de services en ligne et hors ligne ;
- un **fournisseur d'identité** : un tiers de confiance qui va mettre à disposition un MIE. Par défaut, c'est lui qui garantit les attributs présentés par l'utilisateur ainsi que le lien entre les attributs et cet utilisateur. Mais il peut aussi s'appuyer sur des **fournisseurs d'attributs** pour ajouter des attributs au MIE en en garantissant la qualité (par exemple, une université pourrait ajouter un attribut « étudiant inscrit » sur un MIE géré par un autre acteur) ;
- un **fournisseur de service** : un opérateur public ou privé qui met à la disposition de l'utilisateur un ensemble de services dont l'accès est conditionné soit à une authentification soit à une preuve d'attribut(s). Chaque MIE fournit un **niveau de garantie** donné en fonction du contexte d'usage, pouvant aller d'une identité déclarative (par exemple, une identité sur un réseau social construite autour d'un pseudonyme ou d'un nom d'usage choisi par l'utilisateur sans vérification) à une identité régalienne, c'est-à-dire garantie par l'État (par exemple l'identité numérique liée à la nouvelle carte nationale d'identité électronique (CNIe)).

QUE DISENT LES TEXTES ?

Les **identités régaliennes** (états civils), sont soumises au règlement européen eIDAS de 2014. L'objectif de ce règlement est, notamment, d'harmoniser les moyens d'identification électronique utilisés dans l'Union européenne, afin qu'un usager dans un État membre puisse accéder aux services publics d'un autre État membre.

Ce règlement définit trois niveaux de garantie (« faible », « substantiel » et « élevé ») pour les identités régaliennes en fonction du niveau de vérification de l'état civil et du niveau d'authentification mis en œuvre.
Le niveau de garantie « faible » correspond à une vérification préalable succincte avec une authentification simple, tandis que le niveau « élevé » garantit une vérification en profondeur (par exemple, par un entretien en face-à-face avec la personne pour la création de son identité) et requiert une authentification forte.
Un niveau « faible » pourra suffire pour déclarer ses impôts, un niveau « substantiel » pour ouvrir un compte en banque en ligne, tandis qu'un niveau « élevé » sera requis pour la déclaration de naissance d'un enfant.

La bonne pratique, au titre de la protection de la vie privée, est d'identifier le besoin de confiance pour le service et de retenir l'utilisation du plus faible niveau d'identification et d'authentification y répondant. Cela permet à la fois de minimiser les données traitées (l'élévation de niveau va généralement de pair avec la quantité de données traitées – y compris sensibles – et leur durée de conservation) et de limiter les conséquences pour les personnes qui seraient victime d'une usurpation d'identité de haut niveau en leur permettant de continuer d'avoir accès aux services pour lesquels cela est acceptable.

ÉTAT DES LIEUX
L'identité numérique aujourd'hui

Identité numérique et preuve numérique d'identité dans le monde physique

L'identité numérique d'une personne sert principalement à accéder à des services dans le monde numérique mais peut aussi, dans certains cas, être utilisée dans le monde physique.

L'exemple de la carte bancaire
Lorsque nous payons avec une carte bancaire, nous prouvons dans le monde physique, par la détention de la carte (avec éventuellement un code PIN), que l'on est bien le détenteur du compte à débiter.

Identité numérique et biométrie

La biométrie regroupe l'ensemble des techniques permettant d'identifier ou d'authentifier automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales : empreintes digitales, réseaux veineux de la paume de la main, reconnaissance vocale, du visage, de l'iris, analyse comportementale telle que la dynamique de frappe au clavier, etc.

Ces caractéristiques ont la particularité d'être uniques et, pour certaines, permanentes. Elles sont en effet inhérentes au corps lui-même et le caractérisent de façon définitive, ce qui signifie qu'elles ne peuvent pas être révoquées par l'individu (à l'inverse d'un mot de passe ou d'un identifiant attribué). Elles peuvent être utilisées pour suivre et identifier un individu, même à son insu. Le caractère sensible de ces données est consacré par l'article 9 du RGPD.

La biométrie utilisée comme un moyen d'authentification l'est au même titre que les mots de passe ou la possession d'une carte à puce. Elle permet de vérifier le lien entre une personne et l'identité qu'elle présente.

La biométrie étant un traitement sensible, la CNIL préconise que **tout MIE l'utilisant propose une alternative équivalente pour accéder aux mêmes services**. Cela permet, d'assurer le **consentement libre** de l'usager. Cette solution alternative pourrait notamment prendre la forme d'un face-à-face (tel qu'un déplacement en préfecture, en mairie, ou auprès d'un autre service public accueillant directement le public).

À SAVOIR

L'utilisation de techniques biométriques au sein d'un titre d'identité n'implique pas forcément qu'il contienne une identité numérique.

Inversement, une identité numérique ne nécessite pas forcément l'utilisation de techniques biométriques.

Depuis juin 2019, l'Union européenne impose d'intégrer des techniques biométriques dans la carte nationale d'identité en stockant, sur un support sécurisé, une photo et deux empreintes digitales du titulaire. Cependant, cela ne rend pas ces cartes d'identité nationales « numériques » pour autant : elles ne peuvent être utilisées que dans le monde physique.

Une carte d'identité « numérique » est une carte d'identité qui contient une identité numérique et qui peut être utilisée pour prouver, en ligne, les attributs d'identité qu'elle contient. Par exemple, la carte nationale d'identité française est biométrique depuis août 2021 et elle peut être numérique depuis que l'application « France Identité », présentée à la CNIL sous le nom « Service de garantie de l'identité numérique » (SGIN), est déployée. À l'inverse, l'ancienne carte nationale d'identité allemande ne contenait des données biométriques qu'à la demande du porteur mais pouvait déjà être utilisée pour prouver en ligne ses attributs d'identité.

Identités numériques dans les secteurs public et privé

Au cours des quinze dernières années, de nombreuses identités numériques ont été créées. Certaines sont issues du secteur public, tandis que d'autres (les plus nombreuses) ont été développées par le secteur privé.

Plusieurs caractéristiques de ces identités sont particulièrement intéressantes : leurs références, leurs attributs et leurs usages.

Quelle est la référence pour établir une identité ?

La référence pour établir une identité peut être une base de données de l'État, tel que le RNIPP pour la carte Vitale ou FranceConnect ou encore la base des « Titres électroniques sécurisés » (TES) pour l'identité « France Identité » issue de la nouvelle CNIe.

Dans le secteur privé, il s'agit souvent d'une identité déclarative, choisie par l'utilisateur, ou d'une identité issue de papiers d'identité. L'adresse courriel ou le numéro de téléphone mobile sont couramment utilisés comme données de référence.

Quels attributs sont considérés ?

Chaque MIE a un ensemble d'attributs qui lui est propre, qui est défini en fonction des usages souhaités par les fournisseurs d'identité qui l'utiliseront.

Pour quels usages une identité est-elle prévue ?

QUELQUES EXEMPLES DANS LE TEMPS (PUBLIC/PRIVÉ)

1996	1998	2008	2012	2013	2015	2020	2020	2021	2021	2022
Blizzard (jeux vidéo)	**Assurance maladie**	**Facebook Connect**	**Apple Wallet**	**Google Identity Services**	**FranceConnect**	**L'Identité Numérique (La Poste)**	**TousAntiCovid**	**e-Carte Vitale (ApCV)**	**Référentiel PVID (ANSSI)**	**France Identité**
RealID et BattleTag (identifiants uniques que les joueurs peuvent transmettre pour rester en contact dans les différents jeux).	État civil, numéro de sécurité sociale.	Nom d'usage, âge, liste d'amis, adresse courriel, etc.	État civil, localisation, carte de paiement, cartes de fidélité, clé de voiture numérique, carte d'étudiants, etc.	Nom d'usage, adresse courriel, etc.	État civil.	État civil.	État civil, état vaccinal ou sanitaire.	État civil, numéro de sécurité sociale.	État civil, photographie.	État civil.

Focus sur l'identité numérique officielle en France

La nouvelle carte nationale d'identité électronique (CNIe), au format « carte bancaire », contient une puce électronique et permet de générer une identité numérique, appelée « France Identité ». Elle a d'abord été délivrée dans deux départements à partir du 16 mars 2021 puis sur tout le territoire depuis le 2 août 2021.

Cette évolution résulte de l'adoption en 2019 du règlement européen visant à renforcer la sécurité des cartes d'identité, applicable aux États membres à partir du 2 août 2021. Il rend notamment obligatoire l'insertion d'un composant électronique sécurisé au sein des cartes d'identité stockant l'image numérisée de la photographie et deux empreintes digitales du détenteur du titre. La CNIe peut, depuis quelques mois, être utilisée pour générer une identité numérique via France Identité.

LA CARTE D'IDENTITÉ ÉLECTRONIQUE (CNIE)

RECTO

Photographie (également au verso)

Signature

- Type de document (carte nationale d'identité)
- Nom
- Prénom
- Sexe
- Date et lieu de naissance
- Nationalité
- Nom d'usage autorisé par la loi
- Numéro de la carte, également appelé numéro du titre (donnée personnelle du titulaire pour la durée de validité de la carte)
- Date d'expiration
- Code de lecture automatique (alternative à la zone de lecture automatique permettant l'accès aux données conservées sur la carte)

VERSO

Cachet électronique (code QR) et composant électronique (puce) comprenant nom, prénom(s), date et lieu de naissance, sexe, taille, nationalité, domicile, dates de délivrance et d'expiration, numéro de la carte, image numérisée du titulaire, images numérisées des empreintes digitales.

- Taille
- Date de délivrance
- Adresse (lieu de résidence ou lieu où la personne a élu domicile)

Zone de lecture automatique
Prénom(s), nom, sexe, nationalité, date de naissance, type de document, État émetteur, numéro du titre et date d'expiration.

L'application France Identité permet à tout titulaire d'une nouvelle carte nationale d'identité et d'un smartphone compatible (c'est-à-dire doté de lecture « sans contact » ou NFC et pouvant télécharger l'application gouvernementale) d'y générer, s'il le souhaite, une identité numérique régalienne.

Le titulaire pourra alors :

- **s'identifier et s'authentifier en ligne de manière sécurisée auprès d'organismes publics ou privés** (fournisseurs de service liés par convention à FranceConnect ou au ministère de l'Intérieur) ;
- **prouver certains attributs** liés à son identité (par exemple l'âge pour l'accès à certains services) ;
- **prendre connaissance des données contenues dans sa CNIe** ;
- **créer des justificatifs d'identité** à utiliser à la place d'une photocopie de la pièce d'identité.

L'AVIS DE LA CNIL

Une telle évolution a été **accueillie de manière favorable par la CNIL** car elle permet :

- la **création d'une identité numérique d'État de haut niveau ;**
- de **renforcer la maîtrise des personnes sur leurs données**, notamment en leur donnant la possibilité de ne divulguer que certaines informations ;
- d'**améliorer la sécurité des procédures**, notamment en supprimant la circulation de photocopies de pièces d'identité lors de l'accomplissement de tous types de démarches ;
- de **faciliter la lutte contre la fraude documentaire** (en 2021, la CNIL a reçu 1 755 demandes d'exercice indirect des droits motivées par une usurpation d'identité, avérée ou non, concernant le fichier des comptes bancaires et assimilés (FICOBA)).

La CNIL insiste cependant sur la nécessité de **ne pas rendre ce moyen d'identification électronique obligatoire.**

LA PAROLE À

Anne-Gaëlle BAUDOIN,

Préfète,
Directrice de l'ANTS,
Directrice du programme
France Identité
Numérique

Quels sont pour vous les enjeux de l'identité numérique ?

L'identité numérique vise à accroître la confiance dans les transactions lors d'interactions électroniques en ligne ou hors-ligne. France Identité, l'application d'identité numérique régalienne, a pour ambition de fournir un service public inclusif et accessible au plus grand nombre.

De quelle manière le moyen d'identification électronique de France Identité s'inscrit-il dans le projet de portefeuille européen prévu par la nouvelle proposition de règlement eIDAS ?

France Identité permet dès à présent aux usagers disposant d'une carte d'identité de nouvelle génération de l'utiliser pour des transactions numériques. L'application est la première brique d'un dispositif plus large et interopérable qui s'inscrit dans le projet de portefeuille européen.

QUELQUES EXEMPLES D'IDENTITÉ NUMÉRIQUE RÉGALIENNE DANS L'UNION EUROPÉENNE

En Estonie, une identité numérique certifiée existe depuis 2002 grâce à une carte nationale d'identité électronique qui est un document d'identité obligatoire. Cette carte contient une puce sécurisée où sont insérés deux certificats, l'un pour l'authentification en ligne, l'autre pour la signature électronique.

À partir de 2007, une solution sur mobile a également été développée par l'État avec les opérateurs télécoms. Ces deux solutions, réalisées en partenariat avec les pouvoirs publics et les acteurs privés, ont fait l'objet d'une notification dans le cadre du règlement eIDAS et permettent une authentification aux niveaux de sécurité « substantiel » et « élevé ».

En Belgique, dès 2004, une carte d'identité électronique obligatoire a été délivrée à chaque citoyen. En cinq ans, la Belgique est parvenue à doter 100 % de sa population de ce nouvel outil, qui contient une puce intégrant deux certificats : l'un permettant l'authentification en ligne, l'autre permettant l'apposition de la signature électronique de son détenteur.

Ce dispositif a lui aussi été notifié dans le cadre du règlement eIDAS en 2019 pour un niveau de sécurité « élevé ».

En Allemagne, une carte d'identité électronique a été créée en 2010. Si l'utilisation de cette carte est obligatoire, la fonction d'identité numérique régalienne qu'elle offre aux citoyens allemands a été facultative et laissée à la main de l'usager jusqu'en 2017. Depuis, elle bénéficie d'un niveau de sécurité « élevé » et elle est systématique, sauf pour les mineurs de moins de seize ans qui peuvent bénéficier d'un titre ne disposant pas de cette fonctionnalité.

La solution allemande a fait l'objet d'une notification dans le cadre du règlement eIDAS en 2017 pour un niveau de sécurité « élevé ».

La notification consiste en la reconnaissance mutuelle d'un schéma d'identification électronique d'un État membre par les autres États membres.
Cette identité numérique peut alors être utilisée dans toute l'Union européenne.

LES ENJEUX
Sécurité et respect des droits fondamentaux

Permettre la pluralité des identités, le pseudonymat et les noms d'usage

Chacun devrait pouvoir utiliser différentes identités numériques selon les contextes.

Par exemple, un individu pourrait avoir une identité numérique régalienne pour s'inscrire sur les listes électorales et une autre identité numérique liée à un pseudonyme qu'il aurait choisi pour un réseau social.

QUE DISENT LES TEXTES ?

L'avis sur les réseaux sociaux en ligne, adopté le 12 juin 2009 par le G29 (aujourd'hui Comité européen de la protection des données), prévoit que les utilisateurs puissent y utiliser un pseudonyme.
L'article 5 du règlement européen eIDAS prévoit, quant à lui, la possibilité d'utiliser des pseudonymes dans les transactions électroniques.

Il est habituel en France d'utiliser des noms d'usage, qu'il s'agisse d'un nom obtenu par mariage ou du nom d'un parent, ou encore d'utiliser un autre prénom que son premier prénom. Il est tout aussi habituel d'utiliser des pseudonymes ou des noms d'artiste dans différents milieux.

La pluralité des identités est aussi un moyen que chacun peut utiliser pour séparer les différents aspects de sa vie. Ce n'est plus seulement une question de sécurité des données, face par exemple aux risques d'usurpation, il s'agit aussi d'une question **d'une question de possibilité laissée à chacun d'avoir plusieurs identités**, plus ou moins complètes, par contexte d'usage, et non reliées entre elles.

Enfin, les niveaux d'**identification et d'authentification devraient être choisis selon le niveau de confiance nécessaire et suffisant pour chaque service en ligne**. En effet, il n'est pas nécessaire d'utiliser le plus haut niveau d'identification et d'authentification pour l'ensemble des cas d'usage de l'identité numérique. Il est plus simple pour les organismes, plus ergonomique pour les utilisateurs et plus protecteur des données personnelles d'**adapter le niveau d'exigence requis aux risques liés à l'usage d'une identité numérique**.

> *À l'heure où les individus multiplient leur utilisation des outils numériques, il est indispensable que ce qui est habituellement permis dans le* ***monde physique*** *le soit également dans le* ***monde numérique****.*

En pratique, l'utilisation obligatoire d'une identité régalienne forte liée à un nom de naissance et à un premier prénom (c'est-à-dire une identité garantie par l'État au plus haut niveau de confiance) doit être limitée à un nombre de cas réduit, tandis que les solutions permettant l'utilisation de noms d'usage, d'identités déclaratives ou de pseudonymes devraient être privilégiées dès que possible.

Protéger l'anonymat et le pseudonymat

Toutes nos interactions reposent sur des infrastructures numériques (web, réseaux mobiles, etc.), laissent des traces numériques (adresse IP, géolocalisation, etc.) et matérialisent nos relations avec d'autres personnes ; autant d'éléments qui peuvent être utilisés pour nous identifier. Rester anonyme en ligne suppose ainsi d'utiliser de nombreuses techniques, qui vont bien au-delà de la seule utilisation d'un nom d'emprunt ou d'un pseudonyme. La protection de l'anonymat en ligne nécessite, par exemple, d'utiliser un ordinateur dédié, des outils spécifiques masquant l'adresse IP de connexion, ainsi des comptes également dédiés et non reliables à la personne. Au quotidien, il est donc **très difficile de se « cacher » en ligne, de ne pas être tracé ou de ne pas voir ses données être collectées**.

Pour les organismes, la capacité à identifier les utilisateurs peut toutefois constituer un avantage, soit en termes de relation client (cas des « univers authentifiés » ou « loggés »), soit pour assurer la sécurité du service et simplifier la détection de certaines menaces, soit pour se conformer à des obligations réglementaires (obligations de connaissance du client - *Know your customer* ou *KYC* en anglais - dans le domaine bancaire).

Bien que l'anonymat parfait soit difficile sur internet, il est important de permettre aux personnes, dans certaines situations, de naviguer en ligne de manière discrète, comme cela est également possible dans de nombreux actes de la vie physique courante, sauf circonstances particulières (l'« anonymat » sur internet est donc plutôt du pseudonymat et peut être

levé, par exemple à la demande d'un juge lors d'un litige relatif à la publication en ligne d'un contenu haineux sur un réseau social).

Le risque **d'imposer une obligation de déclaration d'identité pour naviguer pourrait avoir des effets néfastes sur la liberté d'expression**. Par exemple, la loi sud-coréenne de 2007 imposant une vérification de l'identité régalienne de la personne souhaitant utiliser un pseudonyme avant de pouvoir publier des commentaires sur les principales plateformes en ligne locales a été retoquée en 2012 par la Cour Constitutionnelle pour ses conséquences sur la liberté d'expression (phénomène d'auto-censure, exode vers des plateformes étrangères).

Éviter la mise en place d'un moyen d'identification unique pour tous les usages en ligne

La CNIL plébiscite depuis de nombreuses années la pluralité des solutions d'identité numérique afin d'éviter tout problème de centralisation de l'information et de concentration des risques par le biais d'un canal exclusif : une telle centralisation augmente les risques d'attaque et leurs impacts sur la société en cas de compromission.

Elle soulève également des inquiétudes quant au suivi des individus. En effet, un tel service générerait lui-même le risque d'établissement d'un identifiant unique et de constitution d'un fichier de population, voire d'un suivi des activités numériques de la population.

À titre d'exemple, l'identité numérique régalienne générée à l'aide du dispositif « Service de garantie de l'identité numérique » déployée par « France Identité » adossée à la CNIe constitue un service optionnel mis à la disposition des usagers. Les usagers conservent alors la possibilité :

- de recourir à d'autres dispositifs d'authentification électronique (pour les niveaux faible et substantiel) ;
- d'entrer en contact avec les organismes publics ou privés par des voies autres qu'électroniques (par exemple, la possibilité de se rendre sur place aux guichets).

DÉFINITIONS

Vérifier l'identité d'un individu revient à vérifier l'un ou plusieurs de ses attributs identifiants (nom, prénom, adresse, nom, âge, taille, sexe, etc.).

La DIVULGATION SÉLECTIVE D'ATTRIBUTS est une opération permettant de ne révéler que les données d'identité nécessaires à un usage précis.

Monsieur X achète des billets d'entrée à la piscine municipale. Il n'a besoin que de prouver sa commune de résidence à la personne au guichet pour bénéficier du tarif réduit.

La divulgation sélective d'attributs est déjà réalisable dans le monde physique. Par exemple, le fait de cacher ses informations sur son titre d'identité à l'aide de sa main pour ne laisser que visible son nom de famille est une divulgation sélective d'attribut.

La PREUVE À DIVULGATION NULLE DE CONNAISSANCE est une technique cryptographique. Elle permet à une partie de prouver qu'elle connaît la réponse à une question sans révéler d'autres informations que cette preuve.

Sur la base d'une identité comprenant un attribut « date de naissance », il est possible de construire une preuve mathématique de la réponse (oui/non) à une question comme : « avez-vous plus de 22 ans ? » sans révéler l'âge de la personne ni sa date de naissance.

La divulgation sélective d'attributs et la preuve à divulgation nulle de connaissance sont des solutions qui permettent le respect du principe de minimisation des données qui sont traitées. **Elles participent à intégrer la vie privée dès la conception dans les solutions utilisant des MIE**.

LA PAROLE À

Heung Youl YOUM,

Commissaire à l'autorité de protection des données de Corée du Sud (PIPC), Université de Soonchunhyang

La Corée du Sud a mis à l'essai et ensuite révoqué une législation sur l'usage d'un système de vérification d'identité pour commenter des contenus sur Internet, pourriez-vous partager votre expérience avec la CNIL ?

Il faut distinguer le « Internet Real Name System » et le « Internet Restricted Identity Verification System ». Le premier nécessite le nom réel de l'utilisateur lorsqu'il poste un commentaire sur Internet. À l'inverse, le second nécessite que l'utilisateur utilise son pseudonyme ou son identifiant après une vérification d'identité lorsqu'il ou elle laisse un commentaire sur un forum internet exploité par un fournisseur de service à partir d'une certaine taille de ce dernier. Le « Internet Restricted Identity Verification System » a été créé en 2007 pour prévenir les dommages causés par la divulgation sans discernement de données d'identité personnelles et les agressions en ligne. Il a été abrogé en 2012 lorsque la Cour Constitutionnelle de Corée du Sud l'a déclaré inconstitutionnel notamment en ce qu'il restreignait la liberté d'expression des internautes et leur droit à l'auto-détermination informationnelle.

De quelle manière le gouvernement coréen va-t-il inclure le respect de la vie privée au sein de la nouvelle identité numérique qu'il développe et qui est basée sur la blockchain ?

L'autorité de protection des données de Corée du Sud (PIPC) considère que l'un des sujets principaux concernant les services basés sur la blockchain est l'absence de possibilité de destruction des données. Les personnes ne peuvent plus faire valoir leur droit à l'oubli. Pour résoudre ces questions, la PIPC recommande ainsi aux services utilisant une blockchain de choisir une mise en œuvre qui ne stocke pas de donnée sur la chaîne de blocs elle-même (les données peuvent être stockées hors chaîne ou sur une chaîne latérale).

Par ailleurs, notre règlementation en protection des données a été amendée en juillet 2022 pour reconnaître que les données à caractère personnel sur une chaîne de blocs peuvent être considérées comme détruites lorsqu'il est impossible d'identifier la personne concernée (en utilisant des techniques d'anonymisation).

Enfin, la PIPC entretient une coopération étroite avec le Ministère des sciences et des nouvelles technologies et le Ministère de l'Intérieur et de la Sécurité pour s'assurer que les aspects relatifs à la vie privée sont considérés au sein des systèmes d'identité et d'authentification basés sur une blockchain.

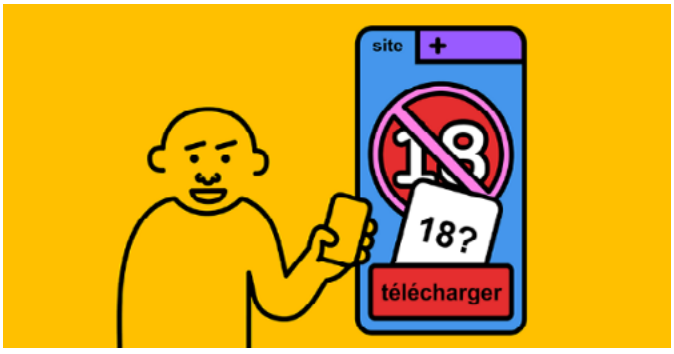
Divulguer le minimum d'information

La CNIL incite les acteurs du numérique à **privilégier les solutions intégrant la protection de la vie privée dès la conception** (ou *privacy by design* en anglais), une obligation prévue par le RGPD.

Cela permet de prendre en compte au plus tôt, dès la définition de l'architecture des solutions les exigences de protection de données, par exemple en ne transférant que les informations strictement nécessaires. Il existe ainsi des solutions pour dévoiler uniquement l'identité d'une personne sans sa date de naissance, voire certifier qu'une personne est majeure sans dévoiler ni son âge ni son état civil. Ces solutions apparaissent en outre conformes au **principe de minimisation des données**, également prévu par le RGPD, car elles permettent de n'utiliser que les seules données dont le fournisseur de service a besoin.

De manière constante, la CNIL a toujours encouragé la mise en œuvre de ces solutions.

L'exemple de la vérification de l'âge



L'un des attributs les plus couramment vérifié est l'âge, notamment pour la preuve de majorité. En effet, plusieurs offres de produits ou de services y sont conditionnées.

Dans sa position publiée en juillet 2022, la CNIL a indiqué qu'elle estimait préférable de recourir à des dispositifs consistant en la fourniture d'une preuve de la majorité d'âge sans information identifiante supplémentaire.

Elle rappelle toutefois qu'il est possible d'utiliser la carte bancaire qui permet, dans la plupart des cas, de protéger les plus jeunes de contenus qui ne leur sont pas destinés y compris lorsque leur accès est gratuit. Lorsqu'un système repose sur l'utilisation d'une carte bancaire pour vérifier un âge, la solution technique déployée doit être opérée par des tiers présentant un niveau de sécurité et de fiabilité suffisant pour éviter les violations de données et garantir **la prise en compte des risques additionnels engendrés par leur utilisation**.

Attention : l'opération de vérification de l'âge des individus peut potentiellement amener à traiter des données de mineurs, qui sont spécifiquement protégés par la loi.

EN SAVOIR PLUS

- Contrôle de l'âge sur les sites web : la CNIL invite à développer des solutions plus efficaces et respectueuses de la vie privée, 26 juillet 2022, cnil.fr
- La CNIL publie 8 recommandations pour renforcer la protection des mineurs en ligne, 9 juin 2022, cnil.fr

L'exemple du passe sanitaire

Pour lutter contre l'épidémie de COVID-19, le passe sanitaire consiste en la présentation numérique, notamment via l'application TousAntiCovid ou papier, d'une preuve sanitaire (c'est-à-dire : vaccination, test PCR, ou preuve de rétablissement).

Pour rappel, le passe sanitaire français utilise le même support technique que le passe sanitaire européen prévu par le règlement sur le « COVID certificate » prévoyant, entre autres, un ensemble de données minimal et l'absence de base centralisée.

Un dispositif visant à ne vérifier qu'un résultat de conformité (« valide » ou « non valide ») réduit considérablement les données accessibles aux personnes habilitées à vérifier le statut des personnes concernées, notamment en n'indiquant pas si elle a été vaccinée, a fait un test ou s'est rétablie d'une infection antérieure à la COVID-19, conformément au principe de minimisation des données.

À cet égard, **le principe de minimisation impose une limitation des données accessibles en fonction du contexte d'utilisation**.

Si les contrôles aux frontières pouvaient justifier un accès à l'intégralité des données contenues dans le passe sanitaire, les contrôles réalisés dans le cadre des activités (restauration, cinéma, etc.) ne devaient se limiter qu'aux données d'identification et au résultat de validité du passe.

Pour respecter la minimisation des données, **le ministère en charge de la santé a mis en œuvre une solution de lecture et d'affichage sélectifs des données** à la place d'une divulgation sélective : le contrôle aux frontières et la lecture en restaurant s'effectuaient avec différentes versions de l'application TousAntiCovid Verif mais n'affichaient pas les mêmes données.

EN SAVOIR PLUS

- Les avis de la CNIL sur les dispositifs de lutte contre la COVID-19, cnil.fr

Centralisation ou décentralisation : qui doit conserver les données ?

La prise en compte de **la protection des données dès la conception** peut aussi avoir une incidence sur le **type d'architecture utilisée**. Les solutions d'identification et d'authentification se présentent sous une variété de formes allant de la centralisation totale, où un serveur central (par exemple : en utilisant un compte en ligne) est non seulement la référence mais aussi nécessaire à toute identification ou authentification, à des solutions plus décentralisées pour lesquelles l'identification peut se faire indépendamment d'une base centrale (par exemple lorsqu'on prouve son identité en magasin avec une pièce d'identité).

Le principal avantage de l'architecture centralisée est qu'elle permet d'avoir une base de données toujours à jour et donc d'éviter l'utilisation d'un moyen d'identification électronique révoqué. En contrepartie, le serveur a accès à l'ensemble des informations, et notamment qui accède à quoi et quand, et est une cible unique qui concentre les attaques.

Le principal avantage de l'architecture décentralisée est de pouvoir garantir la libre utilisation du moyen d'identification électronique sans surveillance systématique possible. La gestion de moyens d'identification volés, perdus ou périmés, et donc leur révocation, doit être réalisée par un mécanisme dédié. Une solution courante est la mise en œuvre de « listes de révocations », régulièrement récupérées par les services qui vérifient les identités, par exemple tous les jours ou toutes les semaines. Dans ce cas, une identité révoquée pourrait être utilisée quelques jours (en fonction de la fréquence de mise à jour) avant d'être définitivement inutilisable.

Au-delà de l'identité numérique, la CNIL a encore rappelé récemment, dans le cadre de l'examen du traitement DOCVERIF, l'importance de sécuriser les titres d'identité eux-mêmes (notamment les titres régaliens), y compris avec une puce électronique, plutôt que de constituer des fichiers centralisés pour lutter contre la fraude.

Les solutions permettant une utilisation avec une simple interaction entre l'utilisateur, son MIE et le fournisseur de service, sans interaction avec un autre serveur, sont donc les plus protectrices de la vie privée, mais elles sont encore rares.

Lorsque le modèle centralisé est considéré comme nécessaire, toutes les mesures pour limiter la connaissance de chacune des parties au minimum de données requises doivent être mises en œuvre. Par exemple, dans le cadre du téléservice FranceConnect, les données d'état civil sont conservées par le fournisseur d'identité sans qu'il ne sache à quels services l'utilisateur se connecte. FranceConnect conserve les jetons d'accès aux services et les traces mais sous forme pseudonymisée, ce qui est davantage protecteur de la vie privée.

Privilégier une gestion décentralisée des attributs via des API

FranceConnect propose à des « fournisseurs de données » de mettre à disposition d'autres administrations, via son service, des attributs (par exemple : le statut étudiant ou le revenu fiscal de référence). Ce projet, dénommé « API FranceConnectées », permet de garantir l'exactitude des données car elles sont fournies par l'administration d'origine mais également le respect du principe de minimisation en permettant de garantir qu'un demandeur n'accède qu'aux seules données dont il a besoin et en évitant des copies de bases de données complètes.

DÉFINITIONS

Une API (*application programming interface* ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

Enfin, ce type de fonctionnalité, fondé sur des API, permet de garantir une transparence et un contrôle renforcé pour les utilisateurs, contrepartie nécessaire à l'automatisation de certains flux dans le cadre du programme d'échanges d'informations entre administrations nommé « Dites-le-nous une fois ».

En Belgique, cette logique a été poussée au niveau réglementaire en introduisant la notion de « sources de données authentiques », seules habilitées à produire et fournir certaines données ; les administrations utilisatrices ayant de plus l'interdiction d'en constituer des copies intégrales.

En France, la Direction interministérielle du numérique (DINUM) a également proposé un service expérimental dénommé « Mon FranceConnect » permettant de générer, de manière décentralisée, des informations attachées à une identité FranceConnect. Ces développements, qui maintiennent une approche décentralisée sous le contrôle de l'utilisateur, semblent contribuer à la fourniture de services plus développés, tout en protégeant les données des individus des risques liés à la centralisation.

Il serait souhaitable que ce type d'initiatives se développe au niveau européen dans le cadre du portefeuille européen d'identité numérique (PEIN) (voir page 18).

S'assurer du maintien d'alternatives physiques

Afin de lutter contre la **fracture numérique**, la CNIL rappelle de manière constante l'obligation pour le secteur public d'assurer un accès égal aux services publics, quelles que soient les capacités, connaissances et ressources de chacun en matière numérique.

Ainsi, le déploiement de dispositifs d'identification ou d'authentification numérique ne doit pas mener à la disparition **des alternatives physiques** lorsque celles-ci existent, afin que l'accessibilité des personnes aux services concernés ne soient pas conditionnée uniquement par l'usage de ces dispositifs numériques.

Le Conseil d'État, dans une décision en date du 27 novembre 2019, considère que le code des relations entre le public et l'administration crée, par principe, **un droit et non une obligation pour les usagers de saisir l'administration par voie électronique**.

La CNIL recommande d'appliquer le principe du maintien d'alternative physique de façon générale au moins dans le cadre non professionnel ; celui-ci étant obligatoire pour l'accès à des services publics.

À titre d'exemple, dans le cadre de la mise en œuvre du dispositif TousAntiCovid (TAC), la CNIL a rappelé la nécessité de **garantir la mise à disposition des justificatifs certifiés (avec le code QR) en format papier pour assurer l'inclusion de chacun dans le dispositif**, y compris ceux qui étaient les moins rompus à l'outil numérique et ceux qui ne souhaitaient pas utiliser l'application gouvernementale TAC.

LA PAROLE À

Claire HEDON,

Défenseure des Droits

Quels sont pour vous les enjeux de l'identité numérique ?

L'identité numérique permet de simplifier et de sécuriser les démarches en ligne. Cet objectif ne sera cependant atteint que si le dispositif retenu n'exclut pas les personnes les plus en difficulté avec le numérique, si l'accessibilité des dispositifs concernés est assurée pour les personnes en situation de handicap et si les données personnelles « sensibles » sont protégées par un niveau de garantie substantiel.

Quelles sont les préconisations du Défenseur des droits pour veiller à l'inclusion de chacun au sein des dispositifs d'identité numérique ?

Afin de permettre un égal accès de toutes et tous aux services publics, l'identité numérique doit être facultative et gratuite, une alternative à cette dernière devant toujours être offerte. L'identité numérique doit venir renforcer l'effectivité des droits des usagers et ne pas pénaliser l'usager de bonne foi, dans le cadre d'actions de lutte contre la fraude. Sa mise en œuvre doit enfin s'accompagner d'une formation au numérique de tous et toutes.

Les problématiques liées à l'usage d'un MIE personnel dans la vie professionnelle

Certaines situations nécessitent d'identifier les individus au sein de la sphère professionnelle (par exemple : vérifier l'identité d'un professionnel de santé pour qu'il puisse se connecter aux systèmes d'information des établissements de santé dans le but d'accéder aux données médicales d'un patient).

La CNIL recommande l'usage d'une identité numérique professionnelle distincte de l'identité numérique utilisée à titre d'usager de services publics ou privés. Ainsi, par exemple, l'utilisation dans un contexte professionnel d'une identité numérique basée sur le téléservice FranceConnect ou sur des identifiants FacebookConnect (services à destination des individus en leur qualité d'usagers d'un service public et d'un service privé) interroge sur les risques de confusion possible entre vie personnelle et vie professionnelle.

Si la CNIL recommande, de manière constante, **une étanchéité nette entre les données traitées par le MIE et celles traitées par le fournisseur de service en question, elle recommande également de ne pas utiliser un MIE personnel dans la sphère professionnelle.**

FOCUS

L'usage de l'identité régalienne dans le secteur privé

Le fédérateur d'identité FranceConnect

En France, la gestion de l'identité numérique pour des services publics en ligne repose principalement sur **le service FranceConnect, utilisé par plus de 40 millions de personnes**. Ce dispositif, qui repose sur un **mécanisme de fédération d'identités**, permet de centraliser l'accès à tous les services d'administration en ligne ainsi qu'à certains services privés ayant un besoin réglementaire de vérifier des attributs d'identité.

FranceConnect a pour objectifs de :

- simplifier les démarches et formalités administratives effectuées par le public et en assurer la traçabilité et le suivi ;
- sécuriser le mécanisme d'échange d'informations entre autorités administratives via les API ;
- simplifier l'accès du public aux services en ligne proposés par d'autres entités, notamment privées, qui y sont autorisées ;
- permettre au public l'accès à des téléservices d'autres États membres dans le cadre de l'interopérabilité prévue par le règlement eIDAS.

FranceConnect n'est pas un service obligatoire ; il s'agit d'un téléservice facultatif, tel que le précise son texte de création[1].

En pratique, chaque service a la possibilité de prévoir un mécanisme d'identification propre, mais **FranceConnect vise à simplifier la gestion des identités**. À titre d'exemple, la récupération des certificats de vaccination a pu s'appuyer sur FranceConnect.

L'architecture de FranceConnect présente trois principaux avantages :

- les fournisseurs d'identité n'ont pas connaissance des services utilisés par le détenteur de l'identité. FranceConnect permet de créer une séparation étanche entre fournisseur d'identité et fournisseur de service en ligne ;
- Le système peut sensibiliser les fournisseurs de service à l'importance d'identifier les attributs strictement nécessaires et suffisants à leur service et de ne leur transférer que ceux-ci ;
- Enfin, il ne nécessite pas la mise en œuvre d'un nouveau registre de la population dédié à la gestion de l'identité numérique, car il effectue une vérification auprès du RNIPP déjà existant.

Si FranceConnect centralise l'historique d'utilisation (ensemble des connexions et échanges de données) et permet à l'utilisateur de consulter ses traces et vérifier si des accès légitimes ont eu lieu, **cette conservation n'est pas sans risque puisqu'il s'agit de données personnelles**, qui peuvent révéler des informations sensibles. La généralisation de l'usage de FranceConnect pour se connecter à divers sites soulève

> Depuis 1978, la mise en place d'un identifiant unique et persistant, comme dans le cadre du projet SAFARI, a été refusée. Cependant, la création d'un identifiant technique associé à chaque citoyen à partir de son état civil a toutefois déjà été acceptée, mais sans qu'il soit possible de retrouver celui-ci à partir de ce seul identifiant : c'est le cas dans le cadre de FranceConnect. **Cet identifiant technique sert à conserver les clés d'authentification pour l'accès aux services en ligne accessibles via FranceConnect, et donc à des services de divers secteurs, tout en ne les liant pas à un compte où à des éléments d'identité davantage identifiants**.
>
> Son usage est strictement encadré : cet identifiant ne doit pas sortir du cœur informatique de FranceConnect (il ne peut être utilisé par les différents ministères dans leurs traitements, comme le sont les 10 identifiants sectoriels tel que le NIR, le numéro fiscal, etc.) et les différents services accessibles par FranceConnect ne peuvent y avoir accès. En effet, les services n'ont accès qu'à une clé d'authentification et aux attributs d'identité nécessaires à leur traitement.

1 Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », legifrance.fr

régulièrement la question de l'utilisation proportionnée d'un service d'identité numérique régalien pour des usages de la sphère privée. À ce jour, **un nombre limité de services du secteur privé sont habilités à utiliser France Connect** c'est notamment le cas des services en ligne dont l'usage nécessite, conformément à un texte règlementaire la vérification de l'identité de leurs utilisateurs.

Enfin, seules les personnes inscrites au RNIPP et dont l'identité dite « pivot » pour FranceConnect (nom, prénoms, sexe, date et lieu de naissances) est unique dans celui-ci peuvent utiliser un compte FranceConnect. À ce jour, plusieurs milliers de personnes inscrites au RNIPP n'ont pas une identité pivot unique auprès de FranceConnect et ne peuvent donc pas utiliser ce service[2]. Pour préserver un égal accès aux services et éviter que des personnes soient exclues de ceux-ci, il est conseillé aux fournisseurs de services de proposer une alternative numérique non basée sur FranceConnect.

Le rôle croissant des identités privées

En France, un lien étroit unit l'État et l'identité de ses citoyens. Considérée par certains comme un privilège de l'État (notamment en raison de l'octroi par l'État de l'état civil à ses administrés), l'identification des personnes est aujourd'hui un service de plus en plus proposé par les entreprises privées et notamment par les principaux fournisseurs de services numériques en ligne (Google, Apple, Facebook, Amazon ou Microsoft), dont les services d'identité numérique sont utilisés par la majorité de la population sur de multiples sites.

En particulier, Google incite à la création d'un compte Google pour les utilisateurs d'Android (75 % du marché des smartphones) et de Chrome (60 % du marché des navigateurs), et à la fourniture d'informations complémentaires destinées à augmenter le niveau de confiance, comme le numéro de téléphone mobile (parfois présenté comme nécessaire pour des raisons de sécurité).

Le développement de ces services d'identification, qui ne sont aujourd'hui pas reconnus au titre des schémas d'identification eIDAS au sein de l'Union européenne, peuvent soulever des questions légitimes de souveraineté, de sécurité et de protection des données personnelles.

LA PAROLE À

Alain MARTIN,

Président de FIDO Alliance Europe, Directeur du Conseil et des Relations Industrielles chez Thalès

Quels sont pour vous les enjeux de l'identité numérique ?

La dématérialisation des documents papier de façon accessible à tous. Les smartphones, supports privilégiés aujourd'hui, ne sont pas une solution pour tous et toutes. La souveraineté. Le plus souvent, les services de cloud, comme les smartphones, ne sont pas européens. Il est important de travailler sur des standards ouverts et des mécanismes pour apporter des garanties et de la confiance. Assurer la sécurité et la protection des données. Les solutions doivent être économes en données et, pour nous, reposer sur de l'authentification forte.

FIDO Alliance est un standard utilisé dans de multiples produits. Comment ce standard permet-il la coexistence de multiples fournisseurs ?

FIDO est un standard ouvert qui est conçu pour l'authentification. Les services utilisant FIDO acceptent un protocole sans considération de qui le met en œuvre. Votre matériel « FIDO » remplace vos mots de passe pour l'authentification, avec une clé différente pour chaque service. Votre ordinateur ou votre clé USB devient votre moyen d'authentification tout en garantissant une séparation entre les sites. Cela simplifie et sécurise les accès indépendamment de l'identification.

2 Cette situation se produit car l'identité pivot utilisée par FranceConnect peut correspondre à plusieurs personnes (homonymes complets de même sexe nés le même jour au même endroit). Ce cas est rare mais se produit notamment dans les régions ayant peu de maternité et où il est habituel de n'avoir qu'un prénom tiré du calendrier ou pour les personnes nées à l'étranger où, dans certains cas, la capitale est utilisée comme lieu de naissance pour tous les ressortissants. Le RNIPP comporte d'autres éléments qui permettent de distinguer de manière unique ces personnes (dont le numéro d'ordre de naissance) mais qui ne sont pas utilisés par FranceConnect.

PERSPECTIVES

L'avenir de l'identité numérique européenne

La gestion de l'identité à portée de main : focus sur le smartphone

Historiquement, l'identité numérique avait pour support soit une carte d'identité électronique (comme en Belgique ou en Allemagne) soit un compte (par exemple : impots.gouv.fr ou laposte.fr).

Le **smartphone** (ou ordiphone en français) s'impose en outil majeur pour le développement de l'identité numérique. Il s'agit à la fois du moyen principal d'accès à Internet pour 41 % de la population (« Ordinateur et accès à Internet : les inégalités d'équipement persistent selon le niveau de vie », étude Insee, 2021) et d'un facteur d'authentification en tant que matériel détenu par un individu (ou un foyer).

De nombreux MIE utilisent, en effet, une application sur smartphone comme **support d'identité numérique. Et souvent, elle permet en plus d'etre utilisée comme support d'attestation d'attributs dans le monde physique** (par exemple, pour les attestations de majorité générées par l'application France Identité et utilisables dans le monde physique).

Le smartphone est aussi un des supports étudiés pour le futur portefeuille européen d'identité numérique (PEIN).

Le PEIN, portefeuille européen d'identité numérique : quelles précautions ?

Le 3 juin 2021, une **proposition de refonte du règlement eIDAS** a été présentée par la Commission Européenne. Cette proposition vise notamment à créer un système européen de gestion de l'identité, c'est-à-dire à mettre en place à l'échelle européenne un cadre pour une identité numérique régalienne (e-ID) sécurisée.

Parmi ses objectifs affichés figure la création d'un « portefeuille européen d'identité numérique » (PEIN) ou « *European Digital Identity Wallet* ». Celui-ci pourra contenir 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).

Le PEIN permettrait aux citoyens, résidents et entreprises de l'Union européenne de :

- **prouver leur(s) identité(s) ;**
- **stocker leurs données ;**
- **gérer leurs données et documents officiels au format électronique** (par exemple : leur permis de conduire, des prescriptions médicales ou des diplômes) pour accéder à des services en ligne ou fournir des attestations diverses (telles que sur l'âge).

Le dispositif qui y est proposé répond à de nombreuses attentes de la CNIL :

- l'adoption du portefeuille européen par les personnes sera **facultative**, et sa délivrance **gratuite** ;
- il inclut des mécanismes de **divulgation sélective d'attributs** ;
- la gestion du portefeuille est laissée au porteur ;
- les attestations et justificatifs seront le résultat de traitements respectant les approches de protection des données dès la conception et par défaut
- il 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, demande de prêt, déclaration d'impôts, inscription à l'université) – aujourd'hui, seulement 60 % de la population de l'UE, dans 14 États membres, est en mesure d'utiliser sa carte d'identité électronique nationale à l'étranger.

EN SAVOIR PLUS

- Proposition de règlement du Parlement européen et du Conseil eIDAS (disponible en français), op.europa.eu

Les risques d'un identifiant unique et persistant

Depuis 2018, le règlement eIDAS permet la mise en place de plusieurs identifiants par personne ainsi que leur renouvellement. La personne est alors reconnaissable (si besoin) d'après son identité pivot composée de six attributs d'identité (nom, prénoms, date de naissance, lieu de naissance, etc.). L'un des objectifs affichés de la proposition de refonte du règlement eIDAS est de mettre en place un identifiant unique et persistant par pays et par personne.

Ce type d'identifiant est déjà utilisé dans plusieurs pays européens et peut constituer un élément clé pour faciliter l'interconnexion des systèmes nationaux de gestion de l'identité numérique européens. Il facilite en effet la réconciliation de comptes et l'identification unique des personnes, en lieu et place des attributs d'identité utilisés aujourd'hui et qui peuvent conduire à des erreurs ou des homonymies.

Pour l'instant, l'Union européenne n'a pas décidé si cet identifiant sera un identifiant « technique » d'interconnexion des systèmes, qui ne serait connu que par les nœuds de connexion européens (à l'image de l'identifiant technique interne de FranceConnect), ou un identifiant qui serait utilisé dans les démarches par l'utilisateur, et donc fourni à tous les fournisseurs d'identité et de services.

La création d'un identifiant dit « unique » et « persistant » pour chaque citoyen au sein de l'Union européenne pose des questions en termes de préservation des libertés publiques. Un usage élargi, permettant par exemple une utilisation de cet identifiant dans de nombreux pays et de nombreux secteurs, n'apparaît pas souhaitable, principalement pour trois raisons :

- cela engendrerait un risque de profilage permanent de la population ;
- cela faciliterait, voire inciterait à, l'interconnexion de fichiers ;
- cela faciliterait le suivi systématique des citoyens dans tous les aspects de leur vie.

De plus, la compromission de ce type d'identifiant, à l'image des données biométriques irrévocables, pourrait avoir des conséquences importantes sur les personnes concernées si cela conduisait à un blocage d'accès à des démarches ou à de lourdes procédures pour bénéficier d'un nouvel identifiant.

Si, dans son avis, le Contrôleur européen à la protection des données (EDPS) salue les efforts déployés pour renforcer la confiance et l'intégrité des solutions d'identification envisagées, il relève que l'identifiant unique et persistant est une nouvelle catégorie de données qui n'est pas sans risque pour les droits et les libertés des personnes. Dans certains États membres, les identifiants uniques ont été jugés inconstitutionnels par le passé, comme ce fut le cas en Allemagne. Par conséquent, l'EDPS recommande d'explorer des alternatives.

Le Contrôleur européen souligne les garanties attendues pour limiter les conséquences de la mise en place d'un tel identifiant dans le règlement :

- si l'obligation se limite au fait qu'un tel identifiant doit exister sur le plan technique pour assurer l'interopérabilité entre systèmes nationaux d'identité. Dans le cas français,, il conviendra par exemple de vérifier si un identifiant déjà existant pourra répondre à cette obligation ou s'il s'agira d'un nouvel identifiant spécifique ;
- si l'obligation vise à étendre les usages d'un identifiant déjà existant pour le cas français, voire à constituer un registre européen, les implications en termes de protection des données semblent très importantes. "Dans le cas français, cela concernerait par exemple le NIR, l'identifiant technique FranceConnect ou tout autre identifiant du même type".

À RETENIR

La gestion de l'identité dans les démarches publiques et privées est une question ancienne. Les évolutions techniques ont permis le développement d'identités numériques dont le cadre légal est en évolution, tant au niveau français qu'européen.

Si la CNIL accueille favorablement ces évolutions, qui sont porteuses de protections pour la vie privée, elle appelle toutefois au respect de grands principes essentiels :

- une protection de la pluralité des identités ;
- une gestion fine des attributs et du niveau de confiance en fonction du contexte ;
- une vigilance sur l'accès de toutes les personnes aux services publics ;
- une gestion des données supplémentaires (attributs) fondée sur des API et des sources authentiques, notamment dans le secteur public ;
- la limitation des risques liés à des infrastructures centralisées ou à la mise en place d'identifiants persistants, notamment s'ils doivent etre utilisés au quotidien.

Commission nationale
de l'informatique et des libertés
3, place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

Février 2023

www.cnil.fr
linc.cnil.fr