Renforcer les solutions d'identité numérique grâce au RGPD

Dans un contexte de dématérialisation croissante des démarches administratives et de multiplication des services en ligne, la notion d'identité vit des mutations profondes, à mesure qu'émerge l'identité numérique. La maîtrise de ses identités par l'utilisateur et la sécurité de celles-ci sont primordiales pour la protection de la vie privée des personnes et le développement de services numériques de confiance.

L'INTÉRÊT DE L'IDENTITÉ NUMÉRIQUE

Pour une même personne, il peut exister plusieurs identités en fonction du contexte (état civil, vie sociale et professionnelle, services, jeux en lignes, etc.) et du niveau de confiance associé.

Une identité numérique peut reposer sur différents supports : cela peut être un téléphone, une carte à puce ou bien des serveurs lorsqu'elle est totalement dématérialisée. Dans de nombreux pays, et bientôt en France, l'État fournit une carte nationale d'identité numérique qui permet d'étendre au monde numérique la possibilité de prouver des éléments de son état civil du monde physique.

FOCUS

La différence entre carte d'identité biométrique et carte d'identité numérique

La biométrie est un moyen d'authentification comme les mots de passe, la possession d'un smartphone dont le numéro a été enregistré, ou encore une carte bancaire et son code PIN. Elle permet de vérifier le lien entre une identité et son porteur. Elle peut également servir à identifier les personnes.

Un règlement européen voté en juin 2019 oblige les États membres à rendre biométrique leur carte nationale d'identité en intégrant, sur un support sécurisé, une photo et deux empreintes digitales du titulaire. Ainsi celle-ci pourra être utilisée, comme cela est aujourd'hui le cas pour les passeports, pour authentifier le porteur lors des passages aux frontières. Cependant cela ne les rend pas nécessairement « numériques » car 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 belge n'est pas (encore) biométrique mais elle est pourtant numérique depuis 2004. Elle permet ainsi à ses détenteurs de s'authentifier auprès du gouvernement belge et de signer numériquement des documents. Autre exemple, la carte nationale d'identité allemande ne contient des données biométriques qu'à la demande du porteur mais peut, dans tous les cas, être utilisée pour prouver en ligne ses attributs d'identité. Dans un objectif de protection de la vie privée, la carte allemande permet aussi à son détenteur de prouver qu'il est majeur sans indiquer son âge ou sa date de naissance.

LES GRANDS PRINCIPES DE LA CNIL EN MATIÈRE D'IDENTITÉ NUMÉRIQUE

La mise en œuvre d'une solution d'identité numérique comporte nécessairement un traitement de données personnelles. Dès lors, le RGPD est applicable. Compte tenu du développement des solutions d'identités numériques, voici les principaux points de vigilance en matière de protection des données, étant rappelé que ces dispositifs doivent le plus souvent faire l'objet, avant leur déploiement, d'une analyse d'impact sur la protection des données (AIPD) compte tenu des enjeux pour les personnes.

La pluralité des identités numériques

L'identité numérique étant multiple et contextuelle, il est important de permettre aux individus d'avoir plusieurs identités numériques. Ainsi, un individu devrait pouvoir utiliser différentes identités numériques dans différents contextes (par exemple : une identité numérique dite « régalienne », liée à l'état civil et garantie par l'État, pour s'inscrire sur les listes électorales et une identité numérique liée à un pseudonyme choisi par l'utilisateur pour un réseau social).

La proportionnalité de la solution d'identité numérique et l'importance des pseudonymes

L'identification et l'authentification devraient être graduées selon la confiance nécessaire à chaque service en ligne. En effet, il n'est pas nécessaire de sécuriser l'ensemble des cas d'usage de l'identité numérique et il peut être à

la fois plus simple pour les organismes, plus ergonomique pour les utilisateurs et plus protecteur en termes de traitement de données personnelles d'adapter le niveau de sécurité requis aux risques liés à l'usage d'une identité numérique.

En pratique, l'utilisation obligatoire d'une identité régalienne forte (c'est-à-dire l'identité garantie par l'État au plus haut niveau d'assurance) pourrait être limitée à un nombre de cas réduits tandis que les solutions déclaratives et l'utilisation d'un pseudonyme pourraient être privilégiées dès lors qu'il n'y a pas de besoin particulier de fiabilité, sans renoncer à l'impératif de bien sécuriser l'usage de toutes ces identités.

La minimisation des données

Un des principes clés du RGPD est le principe de minimisation des données. Il implique de s'assurer de ne traiter que les seules données « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

En conséquence, lors de l'utilisation d'une identité numérique pour l'accès à un service, seules les informations strictement nécessaires aux traitements prévus par ce service devraient lui être communiquées. En pratique, cela consiste à créer ou utiliser des solutions qui donnent accès aux seuls attributs nécessaires, par exemple seulement à un pseudonyme ou seulement au prénom et à l'année de naissance, en fonction de la nature du service utilisé. De nouvelles solutions techniques intégrant la protection de la vie privée dès la conception permettent non seulement de ne donner accès qu'aux attributs nécessaires, mais aussi de répondre à certaines questions en ne donnant que l'information strictement nécessaire (par exemple en répondant par oui ou non à la question « la personne est-elle mineure » plutôt qu'en envoyant tous les attributs de son état civil).

Il s'agit aussi de limiter l'information collectée par le fournisseur d'identité. Par exemple, il est possible de mettre en place des solutions décentralisées, qui ne permettent pas au fournisseur d'identité de savoir à quel service une personne s'est connectée.

En outre, il convient de privilégier les solutions intégrant la protection de la vie privée dès la conception et par défaut.

Soigner l'information délivrée aux personnes

Les traitements d'identité numérique peuvent avoir un impact important sur la vie quotidienne des individus. Dans ce contexte, une vigilance particulière devrait être portée à l'information des personnes concernées sur le traitement de leurs données, que ce soit à l'enrôlement ou au moment de partager certains attributs d'identité.

Le cas particulier de l'usage de la biométrie

Dans certains cas, la biométrie peut être utilisée pour confirmer le lien entre une identité état civil ou « régalienne » et un individu. Elle peut être utilisée lors de la création de l'identité numérique, ou lors de son utilisation. Elle est également utilisée dans certains pays pour compenser l'absence de registres d'état-civil correctement constitués.

Si le recours à la biométrie pour vérifier l'identité d'une personne ou permettre son authentification à un service en ligne peut sembler légitime, ce type de traitement est particulier car il fait intervenir des données sensibles qui bénéficient d'un niveau de protection renforcé. En effet, la donnée traitée est consubstantielle de la personne concernée et ne peut pas être remplacée en cas d'usurpation ou de compromission (un individu peut changer de mot de passe mais ne peut pas changer d'empreintes digitales). Il convient, dès lors, de porter une attention toute particulière aux conditions de licéité d'un tel traitement (art. 9 du RGPD). De manière générale, le stockage sur des supports individuels ou permettant à la personne de garder le contrôle sur leurs données sont plus protecteurs pour les personnes que les dispositifs reposant sur une base centrale de données biométriques.

LES IDENTITÉS NUMÉRIQUES RÉGALIENNES

Les identités numériques régaliennes sont depuis quelques années soumises au règlement européen n°910/2014 du 23 juillet 2014 dit eIDAS. Celui-ci a pour objectif d'accroître la confiance dans les transactions électroniques et l'interopérabilité des systèmes d'identité au sein du marché intérieur. Pour cela il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques à travers l'Europe.

Ce règlement formule notamment des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique pour les échanges entre les organismes du secteur public et les usagers au niveau européen. Il définit trois niveaux de solutions (bas, substantiel et élevé) en fonction du niveau de vérification de l'identité, permettant ainsi de disposer d'un spectre allant d'une vérification préalable succincte à une vérification en profondeur et pouvant faire intervenir des moyens d'authentifications variés (du mot de passe à la carte à puce).

Un niveau « bas » pourra suffire pour s'inscrire à des cours de natation sur le site de la mairie tandis qu'un niveau élevé pourrait être requis pour la déclaration de naissance d'un enfant. La bonne pratique est d'utiliser le niveau le plus faible qui garantisse un niveau de confiance suffisant pour un service donné.

FranceConnect

Aujourd'hui les solutions d'identité numériques eIDAS sont mises en œuvre grâce à France Connect, qui sert de pont entre des fournisseurs d'identité (les impôts, la Poste, Ameli, Alicem, etc.) et de nombreux services de l'administration en ligne (mairies, renouvellement de permis de conduire, etc.) ou des services

privés ayant un besoin réglementaire de vérifier des attributs d'identité.
S'il faut avoir à l'esprit que l'inaccessibilité de FranceConnect aurait un impact important sur l'accès à de nombreux services publics, cette architecture présente trois principaux avantages :
1 - Les fournisseurs d'identité n'ont pas connaissance des services utilisés par le détenteur de l'identité.
2 - France Connect peut sensibiliser les fournisseurs de service à l'importance d'identifier les attributs strictement nécessaires et suffisants à leur service, et ne leur transférer que ceux-ci.
3 - France Connect ne nécessite pas la mise en œuvre d'un registre de la population dédié à la gestion de l'identité numérique, même si France Connect effectue une vérification auprès du registre national d'identification des personnes physiques.

Il est à noter que FranceConnect centralise les traces techniques de connexion, et que l'utilisateur peut consulter ses traces et vérifier si des accès illégitimes ont eu lieu.

Le premier fournisseur d'identité visant un niveau élevé en France : Alicem

Alicem est une application mobile permettant aux personnes majeures titulaires d'un passeport biométrique ou d'un titre de séjour biométrique de créer une identité numérique pour accéder à des services en ligne tels que l'assurance maladie, la CAF, le site « impots.gouv.fr », etc.
Dans un premier temps, l'identité numérique Alicem ne pourra être utilisée que par l'intermédiaire de FranceConnect. C'est la première solution d'identité numérique développée par l'État qui vise à atteindre le niveau élevé au sens du règlement eIDAS. Une phase expérimentale a été lancée en 2019.
Sollicitée dans le cadre d'une demande d'avis, la CNIL a conseillé au gouvernement de ne pas rendre obligatoire l'utilisation de la reconnaissance faciale pour l'enrôlement. La CNIL a même suggéré d'utiliser des solutions alternatives à la reconnaissance faciale pour vérifier l'identité de la personne :

- Une vérification de l'identité en face à face : déplacement en préfecture, en mairie, auprès d'un service public accueillant du public.
- Une vérification manuelle de la vidéo et de la photographie sur le titre : envoi de la vidéo sur les serveurs de l'ANTS[21] et vérification opérée par un agent.
- Appel vidéo en direct avec un agent de l'ANTS.

À SUIVRE

2021 : année de la carte nationale d'identité numérique ?

En application du règlement européen relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union adopté en juin 2019, le gouvernement prévoit une carte d'identité numérique française pour 2021.
Cette carte serait à la fois une carte d'identité « classique » et le support d'une identité numérique forte portée par l'État.

Alors que les technologies ont beaucoup progressé ces dernières années, y compris pour proposer des systèmes plus protecteurs des données personnelles, la France pourrait être à la pointe de l'identité numérique respectueuse de la vie privée en choisissant une solution limitant au strict nécessaire ce que chaque entité participant à son utilisation obtient comme information, que ce soit à la création ou à l'utilisation d'une telle identité.

La CNIL devra être saisie pour avis des projets de textes qui viendront encadrer le futur dispositif. À ce stade, plusieurs éléments pourraient notamment être pris en compte :

- Certaines **architectures décentralisées** permettent d'éviter une interaction systématique avec le fournisseur d'identité au moment de l'utilisation du service. Comme pour la majorité des utilisations de la carte d'identité dans le monde physique, seul le fournisseur de service et l'utilisateur sont en mesure de savoir que l'identité est utilisée à un moment donné pour un service donné. En outre, lorsqu'une identification de plus haut niveau est requise, ou toutes les X utilisations de l'identité, une vérification que l'identité n'a pas été révoquée peut être mise en œuvre.
- Ces solutions pourraient intégrer, dès la conception, l'utilisation de différents identifiants, pour permettre par exemple **l'utilisation de plusieurs identifiants** sectoriels pour le secteur public.
- Afin de respecter le principe de minimisation des données, la solution choisie pourrait **permettre au fournisseur de service d'indiquer quels sont les attributs dont il a besoin** et assurer que seuls ceux-ci lui soient transmis.
- La solution choisie pourrait intégrer des **technologies de preuve de connaissance** qui permettent, par exemple, d'obtenir uniquement une preuve de majorité de la personne.

21 L'ANTS est l'agence nationale en charge de l'émission des titres d'identité : carte d'identité, passeport ou encore permis de conduire. Elle dépend du ministère de l'Intérieur.