European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 133-144
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 10

*L'identification en ligne du citoyen : la reconquête de son pouvoir de certification de l'identité par l'État**

Jessica Eynard
(Associate Professor, University of Toulouse Capitole-Private Law Institute (EA 1920))

ABSTRACT If the State has control over the identification of individuals in the real world, it has yet to conquer this faculty online at a time when the major platforms have developed their own identification tools. Several devices are thus emerging, in which the State plays an active role, directly or indirectly. On the whole, these systems deserve to be encouraged, although particular vigilance is required, at the risk of seeing identity become an ordinary object of the market, through the certification function.

1. *Introduction*

« Aujourd'hui plus que jamais, surtout depuis l'émergence de l'internet ; nous sommes identifiés chaque jour par les forces occultes du marché ; bien plus que par le pouvoir d'État »[1].

Genèse de l'identification[2] - L'histoire prouve que les acteurs de la société civile ont été les premiers à développer des moyens d'identification. D'abord fondée sur des pratiques traditionnelles d'interconnaissance, l'identification s'est peu à peu « professionnalisée » par l'établissement de listes, de tableaux et de registres. A l'origine, la connaissance de ses citoyens par le pouvoir nécessitait l'intervention d'intermédiaires locaux tels que des curés ou des notables. L'ordonnance du 15 août 1539 de François Ier exigeait en ce sens des curés qu'ils procèdent à l'enregistrement des naissances, des mariages et des décès. Petit à petit, l'État a commencé à jouer un rôle croissant dans l'identification des individus. L'adoption du décret du 20 septembre 1792 a abouti à confier aux maires, et donc à des représentants de l'État, le soin d'enregistrer l'état civil de l'ensemble des citoyens. Très rapidement, un écart s'est creusé entre l'identité réelle des personnes et leur identité légale et des solutions ont dû être trouvées pour pallier les déficiences de l'état civil. C'est ainsi qu'un système d'identification anthropométrique a été élaboré par Alphonse Bertillon. Cette même déficience de l'état civil explique aujourd'hui le recours à des identifiants biométriques, notamment dans des pays africains ou encore en Inde, où la fiabilité des registres peut être remise en cause.

L'histoire montre que, si l'État n'a pas été au fondement de l'identification, il s'en est saisi jusqu'à jouer un rôle fondamental tout au long du processus d'identification, que ce soit au moment de l'établissement de l'identité ou à celui de l'apport de la preuve de cette identité. Il n'est pas certain qu'il soit parvenu à tenir ce rôle dans le monde en ligne.

L'État, présent au moment de l'établissement de l'identité - A sa naissance, la personne doit être individualisée. Cela se fait par l'attribution d'une identité au nouveau-né lors de la déclaration de naissance à l'officier de l'état civil. Cette identité renvoie à « ce qui fait qu'une personne est elle-même et non une autre » et, par extension, à « ce qui permet de la reconnaître et de la distinguer des autres »[3]. Elle n'est pas définie par la loi française. Classiquement, elle renvoie à l'« ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalité, filiation, …) »[4]. Si elle individualise, l'identité ne confère pas un statut juridique à la personne, qui est acquis par l'établissement d'actes de l'état civil par un agent public, l'officier d'état civil[5], sous la responsabilité de l'État et le

* Article submitted to double blind peer review.

[1] G. Noiriel (éd.), *L'identification. Genèse d'un travail d'État*, Paris, Belin, 2007, 3.

[2] Sur cette partie, voir G. Noiriel (éd.), *L'identification. Genèse d'un travail d'État.*

[3] G. Cornu, *Vocabulaire juridique*, Association H. Capitant, Paris, PUF, 2020.

[4] *Lexique des termes juridiques*, Paris, Dalloz, 2014-2015.

[5] M. Bruggeman, *État civil et identité : quel(s) rapport(s) ?*, in J. Eynard, *L'identité numérique. Quelle définition pour quelle protection ?*, Bruxelles, Larcier, 2020.

contrôle du Procureur de la République. L'établissement de ces actes est entouré d'un formalisme important (mentions obligatoires, absence d'abréviation ou de date en chiffres, lecture des actes par l'officier qui invite les parties et témoins éventuels à en prendre connaissance[6]) qui s'explique par le fait que ces actes doivent parfaitement refléter la situation réelle de l'individu au moment où ils sont dressés mais également au gré des évolutions affectant l'état de l'individu[7], ce qui se manifeste par des ajouts en bas de page, en marge ou au verso de l'acte[8]. Pour davantage de sécurité, les actes de l'état civil sont soumis au principe de la reliure (pour éviter les fraudes et les pertes) et la tenue du double original. Il résulte de ces précautions que les actes de l'état civil sont considérés comme fiables. Ce faisant, ils sont utilisés pour l'établissement des moyens qui permettront à la personne de s'identifier.

L'État, présent au moment d'apporter la preuve de l'identité – Si l'identité peut se prouver par tous moyens, certains documents sont tout de même privilégiés. Le Conseil d'État observe en ce sens que, « si le principe de liberté de la preuve de l'identité d'une personne est consacré par la tradition républicaine, la création de la carte d'identité en 1955, puis le regroupement des fichiers des cartes d'identité et des passeports dans un fichier unique (le Fichier national de gestion) attestent la prééminence très forte acquise par les documents officiels – étatiques – d'identité dans cette certification »[9]. Les documents dont il s'agit reposent sur l'identité inscrite à l'état civil. Leur obtention nécessite qu'un acte de naissance soit fourni et qu'une vérification de la correspondance entre le document produit et la personne présente soit faite. Cette phase, appelée enrôlement, est particulièrement importante pour s'assurer de la correspondance entre l'identité demandée et l'identité réelle. Par la suite, la personne pourra produire sa carte d'identité ou son passeport pour prouver son identité, sans que la présentation de ces moyens ne devienne systématique[10]. Ce processus met en lumière le rôle joué par l'État puisque ce sont les moyens de preuve de l'identité qu'il produit qui sont utilisés en pratique, que ce soit par le secteur public ou le secteur privé. L'État se présente ainsi comme le garant de l'identité des usagers. Cette tâche semble néanmoins se dérober sous ses pieds lorsque l'identification a lieu en ligne.

L'État, absent an matière d'identification en ligne ? - Le réseau internet n'a pas été conçu pour permettre de déterminer qui est derrière la machine. L'identification concerne la machine elle-même et pas l'utilisateur. Pourtant, avec le développement de l'activité en ligne, le besoin de savoir avec un certain degré de certitude qui est connecté ou qui accède à tel ou tel service est devenu prégnant. Sont alors apparus les identifiants et les mots de passe. La multiplication des comptes, associés à chaque nouveau service a eu un effet pervers. Ces codes d'accès ont pu être oubliés, entraînant l'adoption de mots de passe identiques pour plusieurs sites et peu sécurisés (du type 1234). Certains acteurs ont en outre développé leur propre service d'identification de façon à devenir des intermédiaires permettant à l'internaute de s'identifier auprès d'un éventail de sites.

Cela amène à deux constats : « d'une part, l'utilité directe (des documents officiels) pour certifier son identité lorsqu'elle est demandée par un site internet est toute relative, pour ne pas dire inexistante ; d'autre part, surtout, la fonction de certification de l'identité est aujourd'hui très largement exercée par des plateformes numériques – Facebook à titre principal et Google également – sans intervention aucune de l'État »[11]. Le Conseil

[6] Voir pour les détails : Instruction générale du 29 mars 2002 relative à l'état civil.

[7] M. Bruggeman, *Le contenu de l'acte de naissance*, in C. Neirinck (dir.), *L'État civil dans tous ses états*, Paris, LGDJ, Series Droit et Société. Série Droit, 2008,

[8] Art. 49 du Code civil.

[9] Conseil d'État, *Étude annuelle 2017 Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, Paris, La documentation Française, spécialement 94.

[10] En effet, le principe de proportionnalité doit être appliqué de façon à ce que le moyen d'identification utilisé soit adapté au besoin de sécurité pour accéder au service. La Commission nationale de l'informatique et des libertés (CNIL) précise par exemple que la justification de l'identité « peut intervenir "par tout moyen". Ainsi, il n'est pas nécessaire de joindre une photocopie d'un titre d'identité en cas d'exercice d'un droit dès lors que l'identité de la personne est suffisamment établie (par exemple, par la fourniture d'informations supplémentaires à celles relatives à l'identité, comme un numéro client ou adhérent, etc.) ». Pour cette autorité de contrôle, « le niveau des vérifications à effectuer peut varier en fonction de la nature de la demande, de la sensibilité des informations communiquées et du contexte dans lequel la demande est faite », www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces.

[11] Conseil d'État, *Étude annuelle 2017 Puissance publique et plateformes numériques : accompagner l'«*

d'État parle ici d'« ubérisation » de la fonction de certification de l'identité. L'utilisation des boutons « Se connecter avec Facebook » et « Se connecter avec Google » sont en effet aujourd'hui largement répandus, ce qui participe à la collecte informationnelle sans fin opérée par ces acteurs et, par corrélation, à la remise en cause de droits et libertés fondamentaux. Pourtant, l'importance de pouvoir justifier d'une identité de façon fiable, et donc d'une identité reposant sur des éléments vérifiés et pas seulement déclarés, apparaît clairement quand il s'agit d'accéder à certains services.

Les enjeux de l'identification en ligne – Selon la Fédération de e-commerce et vente à distance, 2,3 milliards de transactions ont été réalisées sur des sites de vente sur internet en 2022, soit une hausse de 6,5% par rapport à l'année précédente[12]. La dématérialisation s'est aussi opérée en dehors du champ commercial, avec une intensification de la réalisation en ligne d'actes de la vie courante. La pandémie a aidé ce mouvement et on a vu par exemple apparaître la possibilité de se faire ausculter par un médecin et d'avoir un diagnostic en ligne. Tous ces actes impliquent de pouvoir identifier son co-contractant. En parallèle, les risques en termes de cybersécurité ont cru. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) considère que la menace cyber « se maintient à un niveau élevé », avec 831 intrusions avérées en 2022. Parmi les risques relevés, l'usurpation d'identité comprise largement comme l'utilisation d'une ou de plusieurs données relatives à une personne par une autre personne qui se fait passer pour elle afin d'obtenir un avantage, se trouve en bonne position. Dans son rapport sur l'usurpation d'identité, l'Agence européenne de la cybersécurité (ENISA) rapporte ainsi que 900 cas internationaux d'usurpation d'identité ou de délits liés à l'identité ont été détectés en 2019[13]. Ce chiffre n'est que la partie émergée de l'iceberg et on peut s'attendre à ce que les nombreuses violations de données, dont certaines sont régulièrement reprises dans les médias, se soldent par des usurpations d'identité à court, moyen ou long terme. Les possibilités d'usurpation permises par l'intelligence artificielle amplifient le phénomène, au moment où l'on s'inquiète du phénomène des « deepfakes ». Ces hypertrucages qui consistent à reproduire une voix ou à modifier un contenu visuel, tout en donnant l'impression d'une piste audio ou vidéo authentique, sont en pleine expansion. D'après les chercheurs de la société Deeptrace, le nombre de ces contenus truqués et volontairement trompeurs trouvés en ligne en 2019 étaient d'environ 15000, contre un peu moins de 8000 vidéos recensées un an auparavant[14]. Les conséquences pour les victimes de ces trucages, et les victimes d'usurpation d'identité plus largement, ne doivent pas être minimisées. Outre le préjudice économique qui peut en résulter, ces personnes se retrouvent souvent dans une situation complexe, leur imposant d'apporter une double preuve : celle de leur identité et celle de leur absence de culpabilité face à une infraction commise sur la base des informations dérobées. Ici, c'est le fait de pouvoir s'identifier avec certitude qui se présente comme essentiel.

Plan - L'État a indubitablement un rôle à jouer. Ce rôle s'inscrit en particulier dans les politiques européennes enjoignant les États membres à créer des schémas d'identification électronique[15] et à établir une identité numérique pour leurs citoyens[16]. L'objectif visé est de permettre à 80 % des citoyens de l'Union européenne d'utiliser une solution d'identification numérique pour accéder à des services publics essentiels d'ici à 2030[17]. Dans certains cas, l'État peut se révéler être le fournisseur du moyen d'identification en ligne. Dans d'autres cas, il recourt aux services d'opérateurs privés. En cela, il est tantôt un acteur direct (1), tantôt un acteur indirect (2) en matière d'identification en ligne.

ubérisation », 94.

[12] www.fevad.com/bilan-du-e-commerce-en-france-les-francais-ont-depense-pres-de-147-milliards-deuros-sur-internet-en-2022.

[13] ENISA, *L'usurpation d'identité. De janvier 2019 à avril 2020. Paysage des menaces de l'ENISA*, 2020, 2.

[14] www.oracle.com/fr/security/definition-deepfake-risques.html.

[15] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit règlement eIDAS, JOUE, L 257 du 28 août 2014, 74-114.

[16] Proposition de règlement européen modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021, COM(2021) 281 final.

[17] *Ibid*., 2.

2. *L'État, acteur direct en matière d'identification en ligne*

Le règlement eIDAS, adopté en 2014, a confié à chaque État membre le soin d'adopter un ou des schémas(s) d'identification électronique. Ce dernier est un « système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales »[18]. Le moyen d'identification électronique est lui-même défini comme « un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne »[19]. Concrètement, chaque État membre était invité à établir un processus d'identification, permettant la délivrance d'outils, grâce auxquels l'usager pouvait s'identifier en ligne, auprès de services proposés dans l'ensemble de l'Union européenne. Au moment de la publication de la proposition de règlement visant à modifier le règlement eIDAS et à établir un cadre européen relatif à une identité numérique[20], la Commission européenne relevait que seuls 14 États membres avaient notifié au moins un schéma d'identification électronique, de sorte que 59 % des résidents de l'Union européenne avaient en réalité accès à des schémas d'identification électronique fiables et sécurisés par-delà les frontières[21]. La France accuse un certain retard, en ayant notifié un seul schéma, permettant d'atteindre seulement un niveau de garantie substantiel qui plus est[22]. A l'échelon national, plusieurs outils assurant un niveau de garantie élevé ont pourtant été développés, mais sans faire l'objet d'une notification à la Commission européenne. Ainsi en est-il de l'application Alicem qui a été abandonnée avant sa diffusion auprès du public (1.1), et du Service de garantie de l'identité numérique (SGIN) qui vient à peine d'être lancé (1.2).

2.1. *L'échec d'Alicem*

L'application d'« Authentification en ligne certifiée sur mobile » connue sous le nom de Alicem est née avec le décret n° 2019-452 du 13 mai 2019[23]. Ce moyen d'identification électronique devait permettre aux usagers « de s'identifier électroniquement et de s'authentifier auprès d'organismes publics ou privés, au moyen d'un équipement terminal de communications électroniques doté d'un dispositif permettant la lecture sans contact du composant électronique de ces titres, en respectant les dispositions prévues par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 susvisé, notamment les exigences relatives au niveau de garantie requis par le téléservice concerné »[24]. Dit simplement, l'outil Alicem avait été conçu pour permettre aux usagers de s'identifier et de s'authentifier en ligne à l'aide d'un téléphone portable capable de lire la puce électronique présente sur le passeport ou le titre de séjour de l'utilisateur, grâce à une technologie sans contact. Ces modalités ne posaient aucune difficulté. Elles ne permettaient néanmoins pas d'atteindre un niveau de garantie élevé, lequel requiert de respecter des spécifications techniques, des normes et des procédures propres à empêcher l'utilisation abusive ou l'altération de l'identité[25]. Une couche supplémentaire de sécurité avait donc été prévue. L'utilisation de Alicem exigeait au surplus le respect d'un processus de vérification de l'identité incluant un système de reconnaissance faciale dynamique et statique. L'application proposait ainsi des défis à la personne qui devait en valider trois. L'utilisateur se voyait par exemple proposer de cligner des yeux, de tourner la tête à droite, puis à gauche ou encore de sourire. Le but était de s'assurer que l'application était utilisée par une personne vivante et non sa représentation sur une photo ou son cadavre. Puis, une comparaison était faite entre une photographie extraite de la vidéo faite au moment des défis et la photographie présente sur le passeport ou le titre de séjour. Il s'agissait alors d'authentifier

[18] Art. 3, paragraphe 4, du règlement eIDAS.
[19] Art. 3, paragraphe 2 du règlement eIDAS.
[20] Depuis cette date, de nouveaux schémas d'identification électronique ont été notifiés. Il est possible d'en prendre connaissance à l'adresse https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.
[21] Proposition de règlement modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, Exposé des motifs, 2.
[22] Le règlement eIDAS établit une échelle avec trois niveaux de garantie, à savoir les niveaux faible, substantiel et élevé.
[23] Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF n° 0113 du 16 mai 2019.
[24] Art. 1er du décret n° 2019-452 du 13 mai 2019, *op.cit*.
[25] Art. 8, paragraphe 2, point c) du règlement eIDAS.

la personne grâce à une caractéristique biométrique. Alicem et en particulier le recours à la reconnaissance faciale ont fait l'objet de nombreuses critiques. Au-delà de l'émotion qu'il a suscité dans l'opinion publique[26], des arguments juridiques remettant en cause la légalité de ce dispositif ont été soulevés.

En particulier, la base juridique retenue pour fonder le traitement de données personnelles sous-jacent à l'identification a été questionnée. Classiquement, le consentement ne constitue une base juridique appropriée au sens de l'article 6 du RGPD que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées et si, dans ce dernier cas, elle ne subit aucun préjudice du fait de son refus[27]. Pour cette raison, le consentement ne peut être présumé avoir été donné librement dans certaines situations. Tel est le cas du consentement donné par un salarié pour un traitement mis en œuvre par son employeur ou du consentement donné par un administré à un traitement géré par une autorité publique quand les circonstances rendent improbables le recueil d'un consentement libre[28]. Comme il prenait appui sur le consentement, la validité du dispositif Alicem a pu donc légitimement être interrogée[29]. En réalité, le consentement était utilisé à double titre : d'une part, en tant que base de licéité du traitement et d'autre part, en tant qu'exception à l'interdiction de traiter des données sensibles[30]. Dans les deux cas, le recours au consentement peut faire l'objet de réserves[31]. Concernant tout d'abord la base légale du traitement, la base naturelle en matière de traitement public, à savoir la nécessité du traitement pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable, aurait dû être préférée. Dans le même sens, le choix du consentement pour justifier le traitement de données sensibles paraît étonnant quand, parmi les exceptions permettant de déroger à l'interdiction d'un tel traitement, on trouve la nécessité du traitement pour un motif d'intérêt public important. Le Comité consultatif de la Convention 108 considère en outre que « le consentement ne devrait pas être le fondement juridique utilisé pour la reconnaissance faciale effectuée par les autorités publiques compte tenu du déséquilibre des pouvoirs entre les personnes concernées et ces autorités »[32]. Le choix du consentement dans ces cadres, a certainement été motivé par le fait qu'il apparaît moins contraignant à mettre en œuvre que les fondements classiques. Il évite en effet de devoir justifier de la nécessité du traitement pour un motif d'intérêt public important (dérogation pour traiter des données sensibles) ou de sa nécessité pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable (base légale du traitement). En ce sens, la question de la légitimité du consentement comme fondement au traitement de données en vue d'identification reste en suspens.

Le Conseil d'État, saisi du point de savoir si le dispositif Alicem était légal, n'a pas répondu à cette question. Dans un arrêt du 4 novembre 2020[33], il s'est interrogé sur la liberté du consentement, en faisant complètement abstraction de la question de la légitimité du consentement qui aurait dû être préalable. Il décide de valider le moyen d'identification Alicem en considérant que la liberté du consentement est préservée dans la mesure où l'usager peut accéder à l'ensemble

[26] Parmi les nombreux articles de journaux, il est possible de se reporter à www.laquadrature.net/2019/07/17/la-quadrature-du-net-attaque-lapplication-alicem-contre-la-generalisation-de-la-reconnaissance-faciale ; www.numerama.com/politique/559511-alicem-tout-comprendre-au-dispositif-de-reconnaissance-faciale-controverse-du-gouvernement.html ; www.lesnumeriques.com/vie-du-net/alicem-pourquoi-le-systeme-de-reconnaissance-faciale-de-l-etat-suscite-la-controverse-a142589.html ; https://actu.fr/societe/alicem-pourquoi-lapplication-gouvernement-base-reconnaissance-faciale-fait-polemique_29820368.html.

[27] Considérant n° 42 du RGPD et Comité européen de la protection des données, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) n° 2016/679, 4 mai 2020, n° 3.

[28] Considérant n° 43 du RGPD.

[29] E. Debaets, *A propos des dérives actuelles du consentement en matière de protection des données - Le Conseil d'État et Alicem, in Actualité juridique de droit administratif AJDA*, 2021, n° 6, 346.

[30] Pour rappel, aux termes de l'article 9 du RGPD, les données biométriques sont qualifiées de données sensibles dès lors qu'elles servent à l'identification. Leur traitement est donc par principe interdit mais de nombreuses exceptions existent.

[31] J. Eynard, *RGPD et « empouvoirement » individuel : promesse tenue ou espoir déçu ?*, in *Revue des affaires européennes*, 2021, n° 1, juillet 2021, 15.

[32] Comité consultatif Convention 108, *Lignes directrices sur la reconnaissance faciale*, 28 janvier 2021, T-PD(2020)03rev4, 5.

[33] Conseil d'État, 10ème et 9ème chambre réunies, 4 novembre 2020, La Quadrature du net, n° 432656.

des services à distance sans nécessairement passer par l'application litigieuse et le recueil de gabarits de reconnaissance faciale[34]. Ce faisant, il omet que les alternatives en question ne permettent pas d'atteindre un niveau de garantie élevé. Pour les services requérant ce niveau de garantie, l'utilisateur se trouvait *de facto* en théorie contraint d'utiliser Alicem, à moins de se déplacer en personne.

Outre les difficultés liées au consentement, le respect du principe de proportionnalité était remis en cause. Le dispositif conçu se révélait en effet particulièrement intrusif, en raison notamment de l'inclusion de technologies biométriques. Ces technologies imposent le recueil d'informations biologiques ou comportementales considérées comme quasi uniques pour constituer des gabarits qui permettront l'identification et l'authentification. Le principe de proportionnalité, décliné en un principe de subsidiarité, impose donc de les éviter autant que possible. La Commission nationale de l'informatique et des libertés (CNIL) est allé dans ce sens dans sa délibération du 18 octobre 2018. Pour elle, « la mise en œuvre du traitement projeté doit être subordonnée au développement de solutions alternatives au recours à la biométrie, telle qu'utilisée pour vérifier l'exactitude de l'identité alléguée par la personne créant son compte, et ainsi s'assurer de la liberté effective du consentement des personnes concernées au traitement de leurs données biométriques au moment de l'activation de leur compte ALICEM »[35]. Une censure du dispositif Alicem sur le fondement d'une atteinte au principe de proportionnalité aurait donc été possible. Le Conseil d'État décide du contraire en considérant « que le recours au traitement de données biométriques (…) [devait] être regardé comme exigé par la finalité de ce traitement »[36]. Ce faisant, l'utilisation de données biométriques est considérée comme proportionnée pour atteindre l'objectif d'identification/authentification escompté.

Malgré cette décision positive du Conseil d'État, Alicem n'a jamais été déployé de sorte que ce moyen d'identification n'a jamais pu être utilisé en France par l'usager ou les fournisseurs de services. En réalité, Alicem a toujours été conçu comme un test, comme une première brique vers un dispositif qui, lui, serait largement diffusé. Ce dispositif prend le nom de Service de garantie de l'identité numérique (SGIN).

2.2. *La naissance du Service de garantie de l'identité numérique*

Le décret n° 2022-676 du 26 avril 2022[37] donne naissance au SGIN en même temps qu'il met fin à Alicem. En pratique, il crée un traitement de données à caractère personnel mis en œuvre par deux responsables conjoints étatiques, à savoir le ministre de l'intérieur (secrétariat général) et l'Agence nationale des titres sécurisés (ANTS). Ce traitement a vocation à permettre aux titulaires d'une carte nationale d'identité comportant un composant électronique d'utiliser une application téléchargée sur un téléphone portable pour s'identifier et s'authentifier électroniquement auprès d'organismes publics et privés. S'identifier en ligne nécessite par conséquent de posséder un téléphone doté de la technologie de lecture sans contact mais surtout l'utilisateur doit être titulaire d'une carte d'identité électronique alors que celle-ci n'est délivrée en France que depuis le 2 août 2022. Cette temporalité présente en réalité un avantage puisqu'il permet au dispositif « SGIN » de ne pas reposer sur un mécanisme de reconnaissance faciale à distance. Comme il prend appui sur une carte nationale d'identité dont la délivrance n'est qu'à ses débuts, le nouveau système utilise le processus d'identification et d'enrôlement mis en œuvre pour la création de la carte nationale d'identité. Ainsi, « il bénéficie des mesures mises en place pour celles-ci, et donc du contrôle visuel de l'identité du demandeur par un agent de l'État sur la base des documents fournis pour la demande, ainsi qu'une comparaison d'empreintes entre le demandeur et les données inclues dans son titre

[34] *Ibid.*

[35] CNIL, Délibération n° 2018-342 du 18 octobre 2018 portant avis sur un projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité » (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile.

[36] Conseil d'État, *La Quadrature du net*, *op. cit.*, considérant n° 8.

[37] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF n° 0098 du 27 avril 2022.

biométrique »[38]. Le nouveau schéma d'identification mis en place profite du face-à-face nécessaire à l'établissement de la carte nationale d'identité pour atteindre le niveau de garantie élevé, alors que le dispositif Alicem avait suppléé ce face-à-face par le mécanisme de reconnaissance faciale.

Le traitement mis en oeuvre inclut des données permettant l'identification de l'usager telles que son nom ou son prénom, des données permettant l'identification du titre détenu par l'usager (numéro du titre, date de délivrance, …), des données relatives à l'historique des transactions réalisées par l'usager, dans la limite d'un nombre maximal de transactions déterminé par les responsables de traitement (destinataire des données d'identification personnelle de l'usager, catégorie de la transaction, statut de la transaction, …) ainsi que l'identifiant du téléphone portable.

Conformément à la logique sous-jacente au RGPD et au cadre légal entourant l'identité numérique, le fonctionnement du SGIN repose sur l'idée suivant laquelle la personne concernée doit conserver la maîtrise des informations qui la concernent. Cela se voit à plusieurs égards. Tout d'abord, le système permet à l'utilisateur d'établir des attestations de façon à ce que celles-ci n'intègrent que les seules informations utiles au service destinataire, conformément au principe de minimisation. Ensuite, l'architecture retenue implique une conservation des données par l'utilisateur ou, sous son contrôle. Un double stockage est prévu. D'une part, l'utilisateur conserve l'ensemble des informations dans son équipement terminal. D'autre part, les responsables du traitement stockent les données, à l'exception de celles relatives aux transactions, dans un serveur qu'ils gèrent. L'inutilité dans le cadre de la gestion du moyen d'identification opérée par les organes de l'État justifie que ces informations ne soient pas stockées au niveau national et restent en local, pour répondre aux besoins pratiques de l'utilisateur. De nouveau, le principe de minimisation est respecté. La conservation des données de journalisation mérite ici d'être mentionnée. D'une durée de trois ans, cette conservation s'opère dans le serveur des responsables du traitement mais les données ne peuvent être consultées que par certaines personnes et selon des modalités précises. D'une part, seuls les agents des services des responsables du traitement sécurisés chargés de la maîtrise d'ouvrage et de la maîtrise d'œuvre du traitement de données personnelles mis en œuvre dans le contexte du SGIN, individuellement désignés et spécialement habilités par leur directeur, peuvent les consulter. D'autre part, cette consultation ne peut se faire qu'à la demande de l'usager ou, en cas de litige, après l'en avoir informé[39]. Ce faisant, la personne reste au centre du dispositif mis en place, quand bien même une simple information peut suffire à l'évincer.

L'étude du fonctionnement du SGIN sous l'angle du RGPD conduit globalement à saluer le dispositif mis en œuvre. Les droits des personnes sont préservés[40]. L'accès aux données est restreint à certains acteurs. avec l'obligation pour les responsables du traitement de publier une liste des fournisseurs de téléservices qui pourraient accéder aux données par convention[41]. Les durées de conservation sont échelonnées en fonction des situations. Par principe, elle est d'au plus 5 ans à compter de la dernière vérification d'identité de l'usager du moyen d'identification électronique. Cette durée est néanmoins revue à la baisse dans plusieurs cas : soit la personne exerce son droit d'opposition en désinstallant par exemple l'application et les données doivent être effacées du serveur des responsables du traitement dès la désinstallation, soit la personne ne mène pas à son terme la création du moyen d'identification électronique auquel cas les données doivent être effacées de l'ensemble des supports à l'issue d'un délai de 2 mois, soit la personne n'utilise pas le moyen d'identification électronique pendant 2 ans et les données doivent être automatiquement supprimées[42]. Cette dernière situation implique qu'un mécanisme d'effacement automatique ait été prévu au moment de la conception du dispositif, en application du principe de *privacy by design*.

[38] CNIL, Délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », 2, paragraphe 7.

[39] Art. 5 du décret n° 2022-676 du 26 avril 2022.
[40] Art. 6 du décret n° 2022-676 du 26 avril 2022.
[41] Art. 3 II du décret n° 2022-676 du 26 avril 2022.
[42] Art. 4 du décret n° 2022-676 du 26 avril 2022.

La description ainsi faite du dispositif étatique en-cours de déploiement permet de comprendre pourquoi la CNIL a accueilli « très favorablement » le projet[43]. Le SGIN vient combler un manque : celui d'une identité numérique régalienne de niveau élevé et respectueuse de la vie privée des utilisateurs. Par son biais, l'État joue à nouveau son rôle de certificateur de l'identité des citoyens, quel que soit le monde, réel ou en ligne, envisagé. Le déploiement du SGIN doit dès lors être encouragé et son positionnement par rapport à d'autres initiatives dans lesquelles l'État joue un rôle indirect, précisé.

3. *L'État, acteur indirect an matière d'identification en ligne*

Selon toute vraisemblance, le futur verra naître un éventail de dispositifs d'identification électronique, lesquels seront mis à la disposition des personnes qui choisiront quel(s) dispositif(s) privilégier pour quel(s) usage(s). Ces moyens d'identification seront délivrés par des opérateurs privés sans que l'État ne soit jamais bien loin. Dans certains cas, il désignera lui-même les opérateurs en charge de fournir le moyen d'identification (3.1) ; dans d'autres cas, il aura recours à des tiers de confiance certifiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) (3.2).

3.1. *Le portefeuille européen d'identité numérique fourni par des opérateurs privés mandatés*

La proposition de règlement européen modifiant le règlement eIDAS et établissant un cadre relatif à une identité numérique[44] crée un nouveau moyen d'identification, dénommé portefeuille européen d'identité numérique. Il s'agit d'un produit et d'un service « qui permettent à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service […]; et de créer des signatures et cachets électroniques qualifiés »[45]. Cet outil, censé garantir à toutes les personnes physiques et morales dans l'Union un accès sécurisé, fiable et continu à des services publics et privés transfrontaliers, devra en principe être délivré par chaque État membre dans un délai de 12 mois à compter de l'entrée en vigueur du nouveau règlement[46]. Pour le texte, l'État est donc l'acteur qui délivre le nouveau moyen d'identification. Ce principe est néanmoins vite affaibli par l'article 6 bis, deuxième paragraphe, qui dispose que le portefeuille est délivré soit par un État membre, soit sur mandat d'un État membre, soit indépendamment d'un État membre mais avec une reconnaissance par ce dernier du portefeuille délivré. Si l'État demeure le premier acteur visé, on constate que son rôle s'étiole au fur et à mesure des possibilités. Il est alors permis de s'interroger sur les critères qui seront appliqués pour octroyer un mandat ou pour reconnaître un portefeuille délivré par un organisme tiers.

Sur ce point, la proposition de règlement livre quelques pistes. Elle indique que le portefeuille doit être délivré en application « d'un schéma d'identification électronique notifié, conçu selon des normes techniques communes, et à la suite d'une évaluation obligatoire de la conformité et d'une certification volontaire au sein du cadre européen de certification de cybersécurité, tel qu'établi par le règlement sur la cybersécurité »[47]. L'organisme qui délivre le portefeuille, qu'il soit mandaté ou non, devra dès lors être en mesure de prouver qu'il a suivi un schéma d'identification électronique qui, d'une part, a été conçu selon des normes techniques communes[48] permettant d'atteindre un niveau de garantie élevé et qui, d'autre part, a fait l'objet d'une notification auprès de la Commission européenne. Au surplus, il lui faudra présenter une évaluation de la conformité ainsi qu'une certification de

[43] CNIL, Délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », 3, paragraphe 13.

[44] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021, COM(2021) 281 final.

[45] *Ibid*., 26.

[46] Nouvel Art. 6 bis 1. Introduit par la proposition de règlement, *ibid.* Ce délai est passé à 24 mois dans l'accord de principe obtenu en juillet 2023 (art. 6a 1.)

[47] Exposé des motifs, *Ibid*., 11.

[48] *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework*, 26 janvier 2023.

cybersécurité. L'article 6 quater de la proposition vise en réalité une triple certification : celle du portefeuille en lui-même, celle liée à la cybersécurité du portefeuille et celle liée au traitement des données personnelles via le portefeuille[49]. En pratique, des procédures seront nécessaires pour que l'ensemble de ces garanties soit mis en œuvre et contrôlé. La Commission européenne prévoit en ce sens un délai de six mois à compter de l'entrée en vigueur du règlement à venir pour dresser une liste des normes de certification des portefeuilles qui seront délivrés[50]. Selon un schéma classique, des organismes seront accrédités pour procéder à la certification, si bien que des critères spécifiques devront être dégagés pour évaluer ces organismes évaluateurs et leur octroyer une accréditation[51]. On peut finalement s'attendre à ce que deux référentiels voient le jour : l'un, pour les prestataires désireux de délivrer le portefeuille et l'autre, pour les entités désireuses de certifier les portefeuilles. Pour des questions d'harmonisation, c'est la Commission européenne qui établira ces documents et non l'État membre.

Sur le papier, le schéma ainsi établi, fondé sur une triple certification de l'architecture, de la sécurité et des données personnelles devrait permettre au portefeuille d'être un moyen d'identification fiable et respectueux des droits et libertés des individus. Ceci est d'autant plus vrai que la proposition de règlement organise l'obligation pour un ensemble d'acteurs d'accepter le portefeuille comme moyen d'identification. L'article 12 ter issu de la proposition de règlement vise en ce sens les très grandes plateformes en ligne[52] ainsi que les parties utilisatrices privées qui, conformément au droit national, au droit de l'Union ou à une obligation contractuelle, exige une authentification forte de l'utilisateur, « y compris dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications »[53]. L'obligation faite aux très grandes plateformes d'accepter le portefeuille comme moyen d'identification est aussi symptomatique de la volonté de reprendre la main sur la fonction d'identification, au détriment des outils développés par les sociétés Facebook, Google (Alphabet), … La protection des droits et libertés fondamentaux assurée par le portefeuille passe par ailleurs par l'exigence de cloisonner les données. L'article 6 bis, paragraphe 7, issu de la proposition de règlement dispose à cet égard que « les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue ». De cette façon, les données d'identité ne sont pas reliées à l'historique des services, des transactions, des demandes formulées par l'utilisateur. Une étanchéité est mise en œuvre qui permet à la personne de préserver sa vie privée. Cette étanchéité interroge néanmoins.

Dans la pratique en effet, la vigilance s'impose. Si imperméabilité entre les données d'identité et les données d'utilisation du portefeuille il y a, comment le fournisseur du portefeuille se rémunère-t-il alors que la délivrance de cet outil est gratuite pour la personne[54] ? La volonté de faire supporter cette charge financière par les fournisseurs de services qui demandent aux utilisateurs de s'identifier est-elle tenable économiquement ? Si la réponse est négative, le modèle économique ne repose-t-il pas finalement sur l'exploitation des données d'utilisation du portefeuille ? Ces questions sont légitimes quand l'article 6 bis, paragraphe 7, issu de la proposition de règlement prévoit que « l'entité qui délivre le portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille qui ne sont pas nécessaires à la fourniture des services qui y sont attachés » et qu'elle « ne combine pas des données d'identification personnelle et

[49] On notera que la certification liée au traitement de données personnelles semble avoir été allégée au fur et à mesure des débats. Là où la proposition de règlement utilisait les termes « shall be certified », le dernier accord politique utilise « may be certified ». Voir l'article 6c 3) de l'accord obtenu en juillet 2023.

[50] Art. 6 quater, paragraphe 4, de la proposition de règlement.

[51] *Ibid*., art 6 quater, paragraphes 3 et 6.

[52] Telles que définies par l'article 35 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *JOUE* L 227/1 du 27 octobre 2022. Ce règlement est également appelé le *Digital Services Act* ou DSA.

[53] Art. 12 paragraphe 2 de la proposition de règlement.

[54] Art. 6 *bis*, paragraphe 6 de la proposition de règlement.

d'autres données à caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique avec des données à caractère personnel provenant de tout autre service offert par cette entité ou de services tiers qui ne sont pas nécessaires à la fourniture des services attachés au portefeuille, à moins que l'utilisateur n'en ait fait expressément la demande ». En effet, la première partie de phrase laisse entendre que le fournisseur du portefeuille peut collecter des informations relatives à l'utilisation de portefeuille dès lors qu'elles sont nécessaires pour fournir les services attachés au portefeuille. Quels sont ces services dont il est fait mention ? En l'état, l'expression paraît si large qu'elle laisse penser que le fournisseur peut collecter un nombre important d'informations. Quant à la seconde partie de la phrase, elle pose un principe d'interdiction qui va dans le sens d'une protection forte des droits et libertés, pour affaiblir ce principe en prévoyant la possibilité de recueillir le consentement de la personne pour procéder à la combinaison des données. Pour terminer, que penser de l'identifiant unique et persistant qui doit être stocké dans le portefeuille[55] ? Les garanties posées qui consistent à permettre un changement d'identifiant à la demande de l'utilisateur et à prendre des mesures techniques et organisationnelles pour assurer un niveau élevé de protection des données à caractère personnel utilisées pour l'appariement des enregistrements et pour empêcher le profilage des utilisateurs sont-elles suffisantes ? Certes, le dernier accord de principe obtenu en juillet 2023 ne reprend pas cette idée d'identifiant unique mais il enjoint les États membres à garantir sans équivoque la concordance des identités des personnes physiques utilisant des moyens d'identification notifiés ou des portefeuilles d'identité numérique européens. La question est alors celle de savoir comment garantir cette concordance dans le respect des droits et libertés fondamentaux.

Ces interrogations laissent présager de difficultés à venir. Elles s'ajoutent à celle de l'articulation du portefeuille fourni par les organismes privés avec les outils d'identification d'ores et déjà délivrés par les États. Dans le cadre du portefeuille, les intérêts économiques en jeu sont forts, ce qui crée une inquiétude quant à l'implication des entités privées. Cette inquiétude ne semble pas si forte quand l'État recourt à des tiers de confiance certifiés comme le sont les prestataires de vérification d'identité à distance.

3.2. *L'intervention d'opérateurs privés de confiance*

En l'absence de face-à-face en mairie, l'identité doit pouvoir être vérifiée de façon fiable. Pour y parvenir, l'État recourt à des tiers dits de confiance, qui portent le nom de prestataires de vérification d'identité à distance (PVID). Ce sentiment de confiance naît de la mise en œuvre d'un cadre protecteur, dans lequel des garanties sont prévues en amont et en aval de la certification comme PVID. Reste à déterminer si ces garanties sont suffisantes.

La certification comme PVID impose, pour le candidat, de suivre une procédure d'évaluation[56] consistant à déterminer si le candidat remplit les conditions fixées dans le référentiel d'exigences établis par l'ANSSI pour le service spécifique de vérification d'identité à distance[57]. Ce document décrit les modalités de mise en oeuvre d'un service de vérification d'identité, lequel requiert une vidéo du visage de l'utilisateur ainsi que, en fonction des cas, soit une vidéo du titre d'identité présenté par l'utilisateur, soit les données d'identification relatives à l'utilisateur stockées dans le composant de sécurité du titre d'identité présenté par l'utilisateur, y compris la photographie du visage de l'utilisateur[58]. Sur la base de ces données, le prestataire doit veiller, à l'aide de traitements automatisés et humains, à ce que le titre d'identité présenté par l'utilisateur soit authentique et à ce que l'utilisateur soit le légitime détenteur du titre d'identité. Pour ce faire, une détection du caractère « vivant » de l'utilisateur présent sur la vidéo doit être effectuée. De même, une comparaison a lieu entre son visage extrait de la vidéo avec soit une photographie de son visage extrait de la

[55] Art. 11 bis de la proposition de règlement.

[56] ANSSI, *Processus de qualification d'un service, version 1.0*, 6 janvier 2017, www.ssi.gouv.fr/uploads/2014/11/qual_serv_process-processus-de-qualification-d-un-service.pdf.

[57] ANSSI, *Prestataire de vérification d'identité à distance. Référentiel d'exigences*, Version 1.1, 1er mars 2021, www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf.

[58] *Ibid*., 12 et 13.

vidéo du titre d'identité, soit la photographie de l'utilisateur extraite du composant de sécurité du titre d'identité. Les technologies de reconnaissance faciale sont ainsi mobilisées[59], de façon à pouvoir atteindre un niveau suffisant de fiabilité et bien qu'elles fassent l'objet de controverses. Ceci explique que le prestataire doive respecter un ensemble de garanties propres à assurer la fiabilité du service fourni mais aussi la confidentialité et l'intégrité des données traitées.

En application du référentiel établi par l'ANSSI, le PVID est notamment tenu d'exigences générales, d'obligations en termes d'appréciation et de traitement des risques, du devoir de prendre les mesures techniques et organisationnelles appropriées pour protéger l'information. L'article IV 1. établit par exemple une liste de dix exigences générales, portant sur la qualité de personne morale du prestataire, sur son obligation de souscrire une assurance professionnelle, sur l'apport d'une preuve suffisante attestant que les modalités de son fonctionnement ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du commanditaire ou de provoquer des conflits d'intérêts, … Une attention particulière est également portée au personnel recruté, avec l'obligation de s'assurer de la véracité des *curriculum vitae* fournis et d'organiser des moyens de sensibilisation aux risques spécifiques rencontrés par certains employés. Un nombre suffisant de personnes doit être recruté, des sessions de formation doivent être organisées et les compétences, être régulièrement évaluées. Dans sa mission, le prestataire doit pouvoir estimer les risques. Il lui est par exemple demandé de prévoir un plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité. Il est par ailleurs tenu d'élaborer et de tenir à jour une politique de vérification d'identité à distance. Le règlement général sur la protection des données (RGPD)[60] s'applique en outre à lui. En réponse à la jurisprudence de l'Union européenne[61], il est intéressant d'observer l'obligation faite au prestataire d'héberger les données relatives au service de vérification d'identité à distance au sein du territoire de l'Union européenne ainsi que d'exploiter et d'administrer ce service depuis ce territoire.

Bref, le prestataire est enfermé dans un ensemble de règles, fixées par l'État par l'intermédiaire de l'ANSSI, et relatives au service fourni mais aussi au prestataire lui-même (son organisation, les qualités qu'il doit présenter, …), qui limitent mais n'estompent pas l'inquiétude qu'un tel service de vérification d'identité peut susciter en termes d'atteinte aux droits et libertés fondamentaux. A ce jour, trois acteurs seulement ont été certifiés par l'ANSSI et seuls sept services sont à l'étude[62]. Ces derniers relèvent en outre tous d'un niveau de garantie substantiel. Aucun prestataire ne semble donc pouvoir être en mesure d'assurer un niveau de garantie élevé à court terme, sauf à supposer qu'un prestataire disposant d'un tel service n'a pas souhaité apparaître sur la liste publiée par l'ANSSI[63].

4. *Conclusions*

En conclusion, il faut observer le cheminement opéré en matière d'identification électronique à distance, avec, on peut l'espérer, une perte de vitesse des grandes plateformes, au profit de l'État, mais aussi d'entités privées certifiées, notamment par l'ANSSI. L'avenir dira lequel de ces deux acteurs, public ou privé, parvient à s'imposer en matière de certification d'identité en ligne. Si, à ce jour, l'État français semble avoir pris un peu d'avance[64] en proposant le seul moyen

[59] On notera qu'un opérateur humain peut également intervenir pour valider le caractère vivant de l'utilisateur et procéder à la comparaison demandée.

[60] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L 119, 4 mai 2016, 1-88.

[61] Notamment l'arrêt de la CJUE du 16 juillet 2020 (affaire C-311/18, Data Protection Commissioner/Maximillian Schrems et Facebook Ireland), dit Schrems II, dans lequel la Cour invalide la décision d'exécution de la Commission européenne ayant considéré les principes du Privacy Shield comme adéquats et, ce faisant, autorisant les transferts de données personnelles vers les États-Unis sous certaines conditions.

[62] https://www.ssi.gouv.fr/entreprise/produits-certifies/prestataires-de-verification-didentite-a-distance-pvid.

[63] Le site de l'ANSSI indique en effet que « seuls apparaissent les projets de certification que les prestataires ont accepté de rendre publiques ».

[64] A l'échelle européenne, l'État français semble plutôt être en retard, au moment où plusieurs États membres ont déjà notifié un ou plusieurs schémas d'identification électronique de niveau élevé à la Commission européenne. Sur ce point, voir https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNIT

d'identification assurant un niveau de garantie élevé, la vigilance reste de mise. Le recours à des acteurs privés ne peut s'opérer qu'au prix de contrôles réguliers, visant à s'assurer de la confidentialité des données traitées, du niveau de sécurité atteint et du respect des droits et libertés fondamentaux. L'État doit encore ici jouer un rôle important, sous peine de perdre la maîtrise de l'identification en ligne de ses citoyens et de laisser cette fonction aux acteurs du marché, dont la survie dépend d'une bonne santé économique. L'identité, même lorsqu'elle est traitée sous l'angle de la certification, ne peut être appréhendée comme un objet ordinaire car, au-delà de l'instrument de police qu'elle représente, l'identité relève de l'intimité de ce que nous sommes depuis notre naissance. L'État doit en être le garant.

Y/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.