L’identité numérique en quête de son identité juridique

Poullet, Yves

Published in:
L'identité numérique

Publication date:
2020

Document Version
le PDF de l'éditeur

PROPOS CONCLUSIFS L'IDENTITÉ NUMÉRIQUE EN QUÊTE DE SON … IDENTITÉ JURIDIQUE

YVES POULLET

Professeur associé à l'UClille, Professeur émérite à l'Université de Namur,
Coprésident de NADI (UNamur), Membre de l'Académie royale de Belgique

Note liminaire. Tout colloque et, en particulier, celui tenu à Toulouse, a des allures de feu d'artifice et la personne chargée de conclure ce feu d'artifice se découvre bien penaude lorsque, les feux de la fête à peine éteints, elle prend la plume et tente de retracer toutes les pistes ouvertes pendant la journée. Honoré par ce devoir de conclure, merci Mme Eynard de votre confiance, j'ai tenu à le faire à chaud sans attendre les contributions écrites : le temps refroidit le feu des idées exprimées et les impressions alors ressenties. Qu'il soit donc clair que c'est en toute humilité et en m'excusant auprès de chacun des intervenants à la tribune ou dans la salle que je dépose cette modeste contribution. J'ajoute que mon « identité » belge a eu parfois quelques difficultés de suivre les orateurs dans le dédale des textes administratifs d'outre-Quiévrain.

Mon premier devoir est d'exprimer au nom de toutes les personnes présentes nos remerciements. Que les organisateurs de ce colloque, le commanditaire et surtout l'équipe responsable de l'étude qui a servi de base à ce colloque soient félicités pour la hauteur qu'ils ont donnée aux débats animés de ce colloque. Ils ont pleinement démontré tout l'enjeu « politique », au sens le plus noble du terme, d'un thème qui pouvait paraître bien ennuyeux, logé dans les arcanes du droit administratif voire, confronté à la réalité numérique, complexe et incompréhensible pour un juriste. En parcourant et confrontant les diverses approches du droit de l'identité (droit civil, droit administratif, droits de l'homme, droit de la preuve, droit pénal, …), ils ont eu à cœur de montrer combien le numérique modifie le sens de l'identité, hier inscription unique par l'autorité dans une lignée humaine, aujourd'hui instruments multiples aux mains d'opérateurs privés à la fois de recoupement de données au profit de certains et de reconnaissance au sein de réseaux, évoluant dans un monde désincarné. Ce faisant, le débat initié par l'équipe de Toulouse oblige à repenser le rôle de l'État dans son rôle de garant de l'existence juridique des personnes et de créateur de confiance à la fois pour son porteur, ses libertés et pour les tiers. Avec l'ensemble de l'auditoire, nous tenons profondément à remercier l'équipe de Toulouse pour les chemins variés et pertinents empruntés ensemble ce 12 décembre.

La notion d'identité : une notion ambiguë. L'identité oscille entre deux pôles : l'*ipse* et l'*idem.* La première consacre une approche subjective : elle part de l'individu et prétend réunir autour de l'essence de chacun, clé unique de leur interprétation, les différentes manifestations de lui-même. On est proche de la conception kantienne qui voit dans la personne une identité, toujours la même, sous tous les actes qu'elle exerce. À cette conception « endogène » de l'identité, s'oppose une conception « exogène » : celle de l'identité pour autrui. Il s'agit de l'ensemble des attributs qu'autrui nous assigne pour nous distinguer de toute autre personne ou en tout cas de la plupart d'entre eux. Cette distinction s'est révélée importante comme outil de compréhension des tendances actuelles de la notion d'identité et de sa reconnaissance en droit mais également de la façon dont le numérique oblige à repenser la notion d'identité.

Le point de départ du droit de l'identité. La naissance de tout individu fait l'objet d'une reconnaissance par la Société et partant par le Droit qui encadre cette arrivée. À cette reconnaissance, est liée l'attribution de droits. L'identité civile inscrit l'individu dans la société et permet sa reconnaissance univoque ou quasi univoque par chacun ; elle désigne son *idem* juridique. Il s'agit de pouvoir identifier de manière indubitable chaque individu à partir d'un minimum d'attributs qui relient l'individu à quelques données essentielles qui inscrivent la personne dans une lignée : le nom de famille ; le distinguent par un prénom et notent son entrée dans la société des humains : la date de naissance. À ces données minimales dites d'identité civile, le registre d'état civil ajoute d'autres attributs : l'état civil est constitué des éléments qui permettent l'identification d'une personne, tels que le *nom*, le ou les *prénoms*, le *sexe*, la *date* et le *lieu de naissance*, la *filiation*, la *nationalité*, le *domicile*, la situation matrimoniale, la date et le lieu de *décès*. Il est intéressant comme l'ont noté différents intervenants d'y voir s'ajouter l'attribut de « pseudonyme », qui, dans le cadre du droit de l'état civil, semble réserver à des personnages publics ayant acquis leur notoriété sous un nom d'emprunt (Jean Philippe Smets, alias Johnny Halliday). Cette construction publique et volontariste de l'identité civile par l'État est récente : la Révolution française l'impose en 1792. Elle s'explique par l'affaiblissement des solidarités locales, la mobilité croissante des individus et de la puissance ecclésiastique jusqu'alors « attributeur » non neutre de l'identité du moins des chrétiens.

Deux remarques à ce stade nous permettront de mieux apprécier la révolution apportée par le numérique à la conception traditionnelle de l'identité civile exposée par Mme Bruggeman. Premièrement, cette identité civile et le registre d'état civil sont sous contrôle exclusif de l'autorité publique qui en assure la publicité et délivre à chaque citoyen capable un document qui prouve son identité : la carte d'identité et le passeport, mais ces documents n'excluent pas la possibilité pour chacun de prouver son identité par tout moyen, nous dit l'article 1 de la loi sur la protection de l'identité(75). Cette preuve d'identité dont la présentation obligatoire était limitée à la seule autorité publique (police, administration communale, douanes, …) et, exceptionnellement, à des acteurs privés habilités à l'exiger au regard des risques

(75) « L'identité d'une personne se prouve par tout moyen » (art. 1 de la loi n° 2012-410 du 27 mars 2012, *JO*, n° 75, 28 mars 2012, p. 5604).

d'usurpation d'identité lié au service offert (ainsi, la banque lors de l'ouverture d'un compte) devient, avec le numérique introduit sur une puce présente dans la carte d'identité, le sésame lisible et exigible légalement ou contractuellement par toute une série d'opérateurs publics et privés. En second lieu, les attributs se réfèrent à une dimension sociétale, réelle de l'individu : « fils (ou fille) de », « né (e) le … » ; le sexe, attributs considérés alors comme intangibles dans le temps. Les principes d'unicité, d'impérativité et d'immutabilité de cette identité sont liés à cette conception.

L'identité face aux droits de l'homme. Mme Hurpy note combien la jurisprudence relative à l'article 8 de la CEDH modifie le principe d'immutabilité de l'identité. Ainsi, l'identité ne désigne plus un contenu stable dans la mesure où l'autonomie des sujets oblige à reconnaître, à la suite des jugements de la Cour strasbourgeoise, la possibilité pour l'individu de changer son identité : son prénom, son nom, son sexe. Même si cette jurisprudence souligne quelques limites que l'intérêt général peut, dans certains cas, imposer à la liberté de l'individu d'une maîtrise de son identité, l'épanouissement personnel du sujet : « se sentir mieux dans sa peau » doit autoriser ces changements. L'*idem* cède à l'*ipse,* dira-t-on.

Dans le même sens et, toujours, dans le cadre de l'article 8, sur lequel se fondent *in fine* les législations en matière de protection des données*,* s'ajoute, à cette première réflexion, la difficulté de concilier la notion de données d'identité et celle de données à caractère personnel. L'article 4 (1) du RGPD définit la donnée à caractère personnel : « données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Cette définition sur laquelle nous reviendrons autorise deux réflexions : la première constate le glissement progressif d'une conception de l'identité, attestation de l'existence d'une personne, à une vision différente à savoir la protection nécessaire de l'identité comme outil de recoupement des données relatives à une personne concernée ; la seconde note le fait que l'identité à protéger n'est plus seulement l'identité juridique ou civile mais également l'identité « physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Ces identités – ou faut-il les qualifier plus proprement de moyens d'identification, autre concept énoncé et donc distingué dans l'article – renvoient ainsi à d'autres données que celles reconnues au départ comme identité civile et reçoivent un statut juridique, celui de la protection particulière que leur consacrent les législations de protection des données à caractère personnel. Il est clair que cette extension se comprend par les risques nouveaux créés par l'outil numérique aux libertés individuelles.

Le numérique et l'identité dans le cadre des réseaux. Sans être exhaustif, relevons quelques points épinglés par les orateurs de la journée. Le réseau numérique met en contact des personnes situées à distance. Il est donc utile de mettre sur pied

des systèmes de reconnaissance d'autrui[76] voire de certains de ses attributs, afin de sécuriser la relation et de répondre par exemple aux questions suivantes sans devoir procéder à des démarches de vérification longues et difficiles auprès de tiers variés : « Parlons-nous à la bonne personne ? », « La personne qui réclame l'accès est-elle autorisée ? Par exemple, est-elle majeure ? ». Il est important de noter que, dans le premier cas, les attributs à vérifier sont différents du seul attribut réclamé dans le second cas, à savoir l'âge de la majorité ? Ainsi, le numérique permet une sélection des attributs de l'identité civile que le moyen de vérification utilisé certifiera.

Dans le cas du besoin d'une vérification plus complète, on souligne que le numérique permet l'identification de l'émetteur mais non nécessairement de découvrir son identité civile. La garantie qu'offre le moyen d'identification n'exige pas nécessairement que soit connue par le tiers l'identité civile de ce dernier. Ainsi, des outils permettront à travers des systèmes complexes de clés et de cryptographie de garantir la qualité individuelle de l'interlocuteur[77]. L'identification certifie l'unicité de la personne, son identité mais non point nécessairement son identité civile. C'est tout l'apport de la signature électronique, qui n'est plus une émanation de la personnalité comme l'était la signature manuscrite mais bien une construction mathématique construite par des logiciels et certifiée par les prestataires de services de certification, qui atteste de l'engagement d'une personne habilitée à le prendre mais sans que le tiers auquel le message est destiné doive nécessairement connaître son identité civile.

Le règlement eIDAS de 2014, décrit par notre collègue M. Caprioli, porte 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. Ce texte distingue bien l'« identification électronique », à savoir « le *processus* consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale[78] » (art. 3.1 du règlement) et les « don-

(76) Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI) (http://enetter.fr/la-personne/chapitre-1-lidentite-numerique/section-1-les-elements-de-lidentite-numerique/i-le-centre-lidentite-stable/#note-16), s'assurer de l'identité d'un interlocuteur peut s'opérer grâce à trois types d'informations. Soit, l'information transmise porte sur « quelque chose que celui qui doit être identifié ou reconnu sait » (un identifiant, un mot de passe, une signature, …), soit « quelque chose qu'il possède » (une carte à puce, une carte magnétique, un téléphone sur lequel est reçu un SMS, …), soit, enfin, « quelque chose qu'il est » (une caractéristique biométrique, comme une empreinte digitale ou une reconnaissance rétinienne).

(77) À noter à cet égard la réflexion d'E. Netter à propos de l'utilisation de la cryptographie comme méthode d'identification et d'authentification : « Dans sa fonction d'authentification, le chiffrement n'est donc pas l'adversaire du droit, mais plutôt son auxiliaire. Il permet de procéder aux "contrôles d'identité" en ligne. Il substitue à d'imparfaites "traces numériques", comme l'adresse IP, des mécanismes de nature à susciter une confiance bien plus élevée qu'on traite avec un tel individu, relié à telle identité stable. Il nous paraît fondamental de nous attarder suffisamment sur ces services indispensables rendus au droit par le chiffrement » (E. Netter, *Numérique et grandes notions du droit privé*, n° 40, http://enetter.fr/la-personne/chapitre-1-lidentite-numerique/section-1-les-elements-de-lidentite-numerique/i-le-centre-lidentite-stable/#note-16)).

(78) … voire un « objet » comme le préconise l'article 1 (option b) du *Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance,* en voie d'approbation au sein de la CNUDCI (A CN 9/19/W.G.IV/WP. 157).

nées d'identification personnelle » définies comme un « ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale » (art. 3.3 du règlement). Il s'agit par cette dernière notion de désigner, outre les données d'identité civile définies ci-dessus et conçues comme noyau dur, les données qui permettent aux personnes autorisées (le prestataire de services de certification, le ou les destinataires) de remonter à cette identité civile(79). L'existence du réseau, l'absence de face-à-face, oblige, en effet, à mettre l'accent sur le processus mis en place pour garantir le lien entre le message reçu et l'identité revendiquée et publiée ou non partiellement ou non par le prestataire. Vis-à-vis du destinataire, les données d'identification et les garanties, que présente le système mis en place par le prestataire du service de confiance, garantissent que la personne qui émet le message est bien celle qui est répertoriée comme telle dans les listes du prestataire de services de certification(80). Le destinataire doit avoir accès à ce répertoire à la fin unique de cette vérification(81).

On conçoit dès lors le rôle essentiel du prestataire du service de confiance dans le monde des réseaux. C'est non pas la trace « signature » qui, en tant que telle, garantit l'authenticité d'un document comme c'était le cas dans la signature écrite traditionnelle mais bien le processus mis en place par un tiers qui offre le service de création des moyens d'identification et garantit leur fiabilité lors de la délivrance ainsi que l'accessibilité aux données que ces moyens entendent révéler. Pour ce faire, le prestataire peut être tenu de vérifier, outre l'identité civile de la personne (M. X est bien celui qu'il prétend), d'autres attributs (M. X est bien le CEO de telle entreprise, habilité à signer seule des transactions de plus de tel montant).

On ajoute d'autres vertus au numérique. La cryptographie, en particulier asymétrique à clé publique, permet de réserver au seul destinataire le moyen de la

(79) On notera que la notion de données à caractère personnel du RGPD est plus large encore dans la mesure où sont également visées les données d'individuation qui permettent d'identifier les données relatives à un individu sans que pour autant l'identité civile de cette personne ne soit révélée ni même rechercher (ainsi, le tag RFID placé sur la montre d'un porteur X permet de suivre les déplacements de celui-ci, par exemple dans un supermarché, sans que pour autant le nom de M. X ne soit recherché ni même à la limite utile pour le gérant du magasin qui souhaite connaître les zones d'intérêt de ce porteur).

(80) Tout dépend du niveau de certification que le prestataire du service de confiance entend donner aux moyens d'identification qu'il offre à ses « clients ». Ainsi, l'article 8 du règlement eIDAS définit trois niveaux de garantie. Par exemple, « le niveau de garantie substantiel renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité … ».

(81) Cet égard, l'article 4, b), du *Projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance,* en voie d'approbation au sein de la CNUDCI (A CN 9/19/W.G.IV/WP. 157), qui définit l'identité comme « un ensemble d'attributs se rapportant à un sujet qui permet d'identifier celui-ci (de manière suffisante) (le décrit de façon unique) dans un contexte donné » ; et le justificatif d'identité comme « ensemble des données présentées comme preuve d'une identité déclarée qu'un sujet peut présenter pour permettre de vérifier ou d'authentifier son identité dans un environnement en ligne ».

révélation de l'identité de son émetteur et ainsi soustraire à la connaissance de tous les autres participants au réseau la révélation du contenu du message et l'identité revendiquée. Par ailleurs, je puis souhaiter entrer en relation avec une série d'interlocuteurs différents. Dans ce cas, le numérique me permet de m'identifier de manière plurielle, afin d'interdire les recoupements faciles entre les transactions menées avec des interlocuteurs divers. Si la signature électronique, le moyen d'identification, était unique, la probabilité et donc les dangers d'un tel recoupement seraient à craindre. Le numérique autorise la création et la gestion de plusieurs moyens d'identification, ce qui sans doute ne suffit pas à cloisonner les différentes transactions en fonction des interlocuteurs mais contribue sérieusement à le garantir. L'identification numérique n'est pas unique, elle est fonctionnelle et contextuelle et se conjugue au pluriel. Je puis, par ailleurs, sélectionner les attributs, pas toujours les mêmes, que j'entends révéler au sein d'un réseau et apparaître (m'identifier) sous des identités différentes dans le contexte de tel ou tel réseau. Un professionnel de santé se signalera différemment lorsqu'il s'exprime dans un réseau médical que sur sa page Facebook. Si l'identité civile reste unique, le numérique permet dans le contexte des réseaux une multi-identités ou plutôt un multi-profils et pourrait ouvrir, selon le propos, contesté par certains, de Mme Levallois-Barth, le droit à une multi-identités. La notion de multi-identités est-elle en effet bien compatible avec celle d'identité civile unique, base sur laquelle se conjuguent tous les autres profils dérivés de ce noyau dur ?

Concluons ce point, *l'identité dans les réseaux met en évidence le rôle décisif d'un tiers de confiance et des processus offerts de gestion des moyens d'identification de l'identité. Le numérique permet, à côté de l'identité civile et en lien avec cette dernière, la multiplication d'identités (ou « profils ») fonctionnelles, sectorielles ou contextuelles ; il autorise la certification limitée à un attribut ou certains attributs de l'identité ou plus largement de la personne.* Le principe de minimisation énoncé par le RGPD, au-delà, la vie privée et le droit certes relatif à l'anonymat ajoutent, comme le rappelle Mme Bensa, l'obligation de recourir aux technologies d'identification les moins intrusives et emportant le moins de risques pour les personnes concernées. Ainsi, souhaite-t-elle le non-recours aux techniques d'identification biométriques et génétiques lorsque l'identification et l'authentification peuvent se contenter de techniques moins attentatoires à notre vie privée. À cet égard, la légitimité de l'utilisation des techniques de reconnaissance faciale à l'entrée de lycées ou dans des lieux publics est discutable.

Le numérique et les « identités » corporelles ou « attribuées » par les prestataires du réseau. L'exposé de M. Netter évoquait, à partir d'un ouvrage de Damasio, un scénario futuriste où l'identité n'aurait plus de lien avec des données qui inscrivent la personne dans une lignée familiale et donc sociale réelle mais consisteraient en des attributs par ailleurs modifiables conférées par l'autorité sans lien aucun avec la nature humaine. Ainsi, le pouvoir attribuerait à des personnes des numéros matricules qui identifieraient en toute sécurité les individus alors qu'il faut bien reconnaître les faiblesses actuelles de l'identité civile : plusieurs individus pouvant porter les mêmes noms et prénoms. Sans aller jusque-là, reconnaissons que, dans le cadre des réseaux, il est fréquent que soit attribué à l'utilisateur du réseau un numéro d'identification ou qu'un numéro délivré par l'infrastructure soit utilisé. Il

peut s'agir par exemple du numéro de GSM, du numéro IP, du numéro installé par un cookie ou inscrit dans l'objet en possession de l'utilisateur dans le cadre de l'Internet des objets (montre connectée ou implant RFID). L'idée est simple : il s'agit par cette métadonnée de pouvoir suivre les utilisations faites d'un service ou d'un objet voire les déplacements d'une personne afin soit d'optimiser la relation que le prestataire de services sur le réseau (le commerçant en ligne, l'opérateur de la plateforme, le moteur de recherche, le réseau social, …) désire entretenir avec l'utilisateur de son service en le profilant (publicité one-to-one) soit de pouvoir « vendre » à des tiers les données d'utilisation de ses « clients », porteur d'objets connectés. S'agit-il de données d'identité ? Certes non, dans la mesure où elle ne renvoie pas dans la plupart des cas à des données relatives à une personne qui pourrait ainsi être identifiée. L'opérateur d'une plateforme se soucie d'ailleurs peu de savoir quel est le nom de la personne derrière le cookie mais elles constituent par contre indéniablement des données à caractère personnel (voy. en ce sens, l'avis émis sur la notion de données à caractère personnel par le Groupe dit de l'Article 29 de la directive relative à la protection des données à caractère personnel), dans la mesure où elles permettent de connaître une facette de la personnalité de l'utilisateur ou du « client » et donc de prendre vis-à-vis de cet individu X une décision ayant un impact sur ce dernier, par exemple l'envoi d'une publicité *ad hoc*, la fixation d'un tarif, le déni d'un service. Mme Eynard parle ainsi d'« individualisation » des personnes, notion qu'elle distingue de celles d'identification et d'identité. On note que cette individualisation opère au bénéfice des seuls « attributeurs » des métadonnées ou de leurs ayants droit. On note au passage que, par le nombre de données collectées, certains « attributeurs »(82) peuvent ainsi « individualiser » les personnes de manière très précise – et donc dangereuse pour les personnes concernées – par la puissance informationnelle générée à leur profit. Ces métadonnées représentent un risque : celui de réduire la personnalité de quelqu'un à des données désincarnées, dans la mesure où elles sont reprises hors contexte et réduisent un comportement à quelques traces auxquelles est conférée une valeur de vérité et de prédictibilité du comportement de la personne concernée. Le profil d'une personne que permet notamment l'intelligence artificielle « juge » la personne à partir de ces quelques traces qui traitées comme telles se détachent de la personne qui les a émises. Pire, ce profil sert de fondement à des actions vis-à-vis d'elles.

Le second point est plus important encore. De plus en plus, à l'identité civile réduite à quelques attributs est substituée l'identité biométrique(83) ou génétique dont nous a parlé Mme Debaets. Un cheveu tombé sur un coin de table révèle bien mieux

(82) … dans la mesure où ils offrent une panoplie de services (voy. par exemple, Google qui offrent outre Google Search Engine, Google Street ou Maps, Double Click, Android, …) ou simplement que les services qu'ils offrent de manière quasi monopolistique sont des services de première nécessité dans le cadre d'une société de l'information, par exemple Facebook et son réseau social.

(83) La biométrie, définie comme l'« étude statistique des dimensions et de la croissance des êtres vivants » (Dictionnaire Larousse), vise « l'ensemble des techniques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales (empreintes digitales, réseaux veineux de la paume de la main, reconnaissance vocale, de visage, de l'iris, analyse comportementale telle que la dynamique de frappe au clavier, etc.) » (CNIL, « Biométrie à disposition de particuliers : quels sont les principes à respecter ? », 10 avril 2018, https://www.cnil.fr/fr/biometrie-disposition-de-particuliers-quels-sont-les-principesrespecter).

que tout autre indice le coupable d'une infraction, nous diront les services d'enquête policière. Dans le cadre des réseaux, c'est en tout cas le fondement du procédé Alicem qui utilise un système de reconnaissance faciale(84), la relation avec un individu est bien mieux certifiée que par tout autre moyen d'identification. La reconnaissance faciale que la carte d'identité électronique européenne pourrait permettre en reprenant la digitalisation d'une photo et des empreintes digitales certifie bien mieux que le nom et le prénom l'identité d'une personne et autorise dès maintenant la police sur le terrain à identifier les manifestants déjà fichés ou à ficher dans les bases de données policières ou judiciaires. On sait que l'utilisation d'outils biométriques est déjà largement le fait des entreprises privées au-delà des utilisations de plus en plus nombreuses autorisées par la loi. Les exposés de Mme Debaets et les interventions de plusieurs participants mettent en évidence les dangers de « réductionnisme »(85) (et donc d'erreurs) que représentent les données biométriques de même que les risques, en particulier de sécurité, associés à leurs utilisations. Deux considérations militent contre l'utilisation de données biométriques comme moyen d'identification de l'individu : la première est la possibilité de dégradation lors du processus de digitalisation de l'empreinte biométrique ; la seconde plus importante est le fait, relevé par Mme Eynard, de l'impossibilité de modifier la trace que laisse l'empreinte biométrique : si le vol d'un mot de passe ou d'un code secret, se répare facilement par l'attribution ou le choix d'un nouvel identifiant, ce n'est point le cas de la donnée biométrique attachée au corps de l'individu et donc « attribut » irrévocable.

Concluons ce point. *Le numérique autorise de nouveaux moyens d'identification, soit qu'ils soient attribués par celui-là même qui fournit le service, qu'il s'agisse d'un prestataire privé ou public, soit qu'ils soient dérivés d'éléments corporels de l'individu. Dans les deux cas, on notera le réductionnisme opéré, qui consiste à donner à une trace de l'action de l'individu ou de l'individu lui-même une signification, celle de représenter son identité et/ou de pouvoir lui attribuer toutes les actions ou comportements liés ou « reliables » à cette trace. On note que dans tous ces cas, il ne s'agit pas de définir une identité* erga omnes *mais plutôt pour les opérateurs privés qui délivrent de tels moyens d'identification de se réserver les avantages de cette identification pour des finalités propres à leurs activités.*

Quels rôles de l'État et du Droit face à l'identité numérique ? Au vu des considérations qui précèdent, les rôles de l'État peuvent être de divers ordres. Le premier est traditionnel : il concerne l'attribution, la gestion et la certification de l'identité civile, de même que la production des divers documents et registres d'état civil.

(84) Ce projet a été développé par l'Agence nationale des titres sécurisés (ANTS). Il permet à une personne de s'identifier et de s'authentifier dans le but d'accéder à des services en ligne grâce à un smartphone et un passeport électronique.

(85) Et ceci pas simplement parce que les données biométriques sont réduites à un « gabarit ». Les données biométriques enregistrées (reconnaissance faciale, empreinte digitale, reconnaissance de l'iris, etc.) sont analysées par un logiciel qui trace les points essentiels de ces données. Le logiciel transformera ensuite les données représentées par ces points essentiels en un code informatique appelé « gabarit ». C'est ce gabarit, qui comme on le comprend est le résultat d'une triple réduction : données réelles du visage vers, premier temps, image de ces données, vers, deuxième temps, traduction de cette image en points essentiels, enfin, vers, troisième temps, traduction de ces points en un code appelé « gabarit ».

Le deuxième est le rôle que l'État doit jouer en ce qui concerne la mise sur pied pour ses propres services administratifs de moyens d'identification électronique. Les questions des libertés, en particulier de la protection des données, et de la non-discrimination dans l'usage et le design des nouveaux moyens d'identification et des services auxquels ils donnent accès doivent ensuite être évoquées. Le quatrième concerne le rôle que l'État doit jouer tantôt vis-à-vis des prestataires privés de services en ce qui concerne la certification d'attributs particuliers, tantôt vis-à-vis de prestataires de confiance en ce qui concerne la délivrance et la gestion des moyens de confiance. Le cinquième concerne la protection pénale de l'identité peu importe sa nature civile ou autre. Enfin, on terminera par quelques réflexions supplémentaires relatives à la collaboration entre l'autorité publique et les prestataires ou opérateurs privés dans le cadre de la mise sur pied et du fonctionnement des systèmes d'identification numérique.

L'État comme certificateur de l'identité civile et d'autres attributs. C'est le rôle traditionnel de l'État et chacun lors de la conférence entend bien le lui conserver. L'identité civile reste le socle sur lequel se construisent nombre d'autres identifiants et constituent en définitive le dernier recours qui puisse garantir l'existence d'un individu. Le fait que lié à cette identité civile, l'État tienne un registre où il ajoutera d'autres attributs qu'il se devra de valider (adresse, profession, état civil, composition de la famille, etc.). L'État se devra d'attester ces attributs, y compris électroniquement à la demande du citoyen lui-même, détenteur de ces attributs voire à la demande d'un tiers, auxquels le cas échéant il imposera, notamment pour protéger les citoyens, la vérification auprès de ses services.

L'État comme gestionnaire de l'identité électronique comme moyen de communication avec les citoyens. L'administration peut offrir aux citoyens des services accessibles voire les exécuter électroniquement. On s'en réjouira dans la mesure où l'utilisation du numérique rend l'administration plus accessible, efficace et représente pour le citoyen une plus-value. Les débats de la journée ont longuement présenté les diverses réalisations de l'État français en la matière, qu'il s'agisse de FranceConnect (exposé de M. Douville), système présenté souvent comme un fédérateur d'identités mais à considérer plutôt comme une plateforme où diverses administrations voire opérateurs privés,(86) dits fournisseurs d'identité, peuvent obtenir vérification de l'identité d'un citoyen par l'interrogation opérée par la plateforme auprès du RNIPP (frère jumeau du registre de l'état civil) et ainsi délivrer les moyens d'identification et d'authentification propres à leurs services électroniques ; qu'il s'agisse du projet PreNIUM, présenté par M. Pichon, qui repose sur un outil classique, la carte nationale d'identité, laquelle se fonde sur l'acte de naissance et donc les registres de l'état civil. La délivrance du moyen d'identification et d'authentification nécessite ici une reconnaissance *face to face* à l'administration communale. Enfin, Alicem, système déjà présenté, permet une authentification réservée aux détenteurs de mobiles fonctionnant avec le système ANDROID et est fondé sur la reconnaissance

(86) Il s'agit d'opérateurs privés agissant dans le cadre d'une mission publique : « les personnes morales de droit privé qui proposent des services en ligne dont l'usage nécessite, conformément à des dispositions législatives ou réglementaires, la vérification de l'identité de leurs utilisateurs ou de celle de certains de leurs attributs et uniquement pour les services qui nécessitent cette vérification ».

faciale. Les intervenants ont souligné le retard pris par la France en la matière vu l'absence d'un système de registre nationale et d'identification électronique unique pour l'administration publique. Ce retard est, sans nul doute, dû au traumatisme qui a suivi la révélation des dangers du système SAFARI d'un RNIPP et les craintes de l'octroi d'un numéro unique d'identification à chaque citoyen. Reste à savoir si cette multiplication coûteuse et complexe des identités administratives tant pour l'État que pour le citoyen ne sacrifie pas trop aux exigences des libertés individuelles au regard de l'intérêt général et qu'un meilleur compromis ne soit à envisager. Cette réflexion nous amène au troisième rôle de l'État, celui de défenseur des libertés individuelles et de l'égalité des citoyens.

L'État, défenseur des libertés et de l'égalité des citoyens. À l'État revient l'obligation de veiller vis-à-vis de ses propres outils de gestion de l'identité des citoyens au respect des libertés individuelles et de l'égalité et d'être un modèle à suivre par l'ensemble des systèmes mis en place par le privé. Cette préoccupation de l'égalité des citoyens est à souligner à l'heure du « All Digital » de l'administration publique. De plus en plus, les citoyens sont invités de manière pressante à utiliser la voie électronique désormais privilégiée pour l'accès aux services de l'administration(87). Cette digitalisation tous azimuts soulève une difficulté croissante pour certaines catégories de population d'accéder à l'administration(88).

Qu'en est-il de l'application du RGPD par l'administration ? L'exposé de M. Netter invite à quelques considérations à ce propos. L'article 5 du RGPD énonce les principes de base applicables à tout traitement considérés *a priori* comme des balises nécessaires à la protection de nos libertés, de notre dignité et à la prévention de risques de discrimination. Le traitement des données d'identification doit poursuivre une finalité légitime, c'est-à-dire reposer sur un fondement légal, avoir un contenu proportionné à la finalité poursuivie, qui doit être jugée nécessaire dans un État démocratique. Pour l'administration, le traitement doit reposer sur l'exécution de missions légales d'intérêt général. Que le consentement puisse servir comme fondement légal d'un traitement par l'administration n'est acceptable que si ce consentement est prévu par la loi et respecte les conditions prévues par le RGPD pour son expression. À ce premier principe, s'ajoutent ceux de proportionnalité et de minimisation. Il s'agit comme le note l'exposé de Mme Séruga-Cau : ne traiter que les seules données ou attributs nécessaires à la poursuite du but légitime et celui de sécurité de l'accès et de la gestion des données d'identité et des moyens mis en place pour l'identification et l'authentification. S'y ajoute un dernier principe, celui de non-suffisance, particulièrement bienvenu à l'heure des systèmes experts et d'intelligence artificielle. Il s'entend de l'interdiction de fonder une décision vis-à-vis d'un individu sur la seule base d'un traitement informatique. À cet égard, on note les risques pour la vie privée

(87) Déclaration fiscale en ligne, accès au dossier pension, déclaration de naissance, etc. À l'origine de cette digitalisation des relations entre citoyens et administrations, la volonté de diminuer les coûts pour l'administration et de meilleure efficacité pour le citoyen.

(88) *Cf.* à cet égard, le Rapport du défenseur des droits de la République française de 2017, l'étude CREDOC et celle d'EMMAUS, qui dénoncent également la question du langage utilisé par ces sites web de l'administration et leur complexité d'utilisation qui écartent de leur usage ceux qui en ont le plus besoin.

et l'autonomie des citoyens d'une politique dite de « *Benevolent e-government* », Sur la base de croisements de données à caractère personnel détenues par diverses administrations permis par des numéros ou des données d'identification communs, l'administration repère les personnes susceptibles de fraude sociale ou fiscale ou, plus positivement, celles ayant droit à telle prestation sans qu'il n'y ait eu déclaration d'intérêt de la part du citoyen(89).

Cette défense des libertés et de l'égalité doit également être présente dans le cadre du contrôle des systèmes mis en place par le secteur privé. C'est, en ce qui concerne les libertés, tout le contrôle des interconnexions de fichiers facilité par l'utilisation d'identifiants communs sur la base des principes de protection des données, celui de l'utilisation de données d'identification biométrique dont l'article 9 limite sévèrement l'utilisation ; en ce qui concerne l'égalité, la dénonciation de discriminations opérées sur la base de profils générés à partir de données dont la corrélation est possible à partir de métadonnées attribuées par le prestataire de services. Le rôle de l'État ne s'arrête pas là : il porte également sur le contrôle des tiers de confiance et des moyens d'identification qu'ils proposent. Il serait également utile, comme le relevaient deux intervenants de s'interroger sur la façon dont les systèmes d'identification mis en place par l'autorité publique, y compris les registres d'état civil et les moyens d'identification, devraient pouvoir être utilisés dans une proportion plus importante par les entreprises privées ou les associations privées dans leurs relations avec leurs « clients » et l'administration(90). Nous reviendrons sur ce point.

Le contrôle des tiers de confiance et des services qu'ils offrent. L'exposé de M. Caprioli et surtout celui de Mme Anderson mettent en relief le rôle important joué par le règlement européen eIDAS et le projet de convention CNUDCI. Ces deux textes assignent à l'État un rôle important en la matière : celui, précisément, de créer la confiance dans ces tiers intermédiaires qui certifieront l'émetteur d'un message, son destinataire, ses qualités, l'envoi et la réception et la date de leur envoi ou de leur réception voire, enfin, son contenu. L'article 17 du règlement européen énonce à cet égard : « Les États membres désignent un organe de contrôle établi sur leur territoire ou, d'un commun accord avec un autre État membre, un organe de contrôle établi dans cet autre État membre. Cet organe est chargé des tâches de contrôle dans l'État membre qui a procédé à la désignation. Les organes de contrôle sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour l'exercice de leurs tâches ». Mme Anderson nous décrit la façon dont l'organe en charge de ce contrôle au plan français, l'Agence nationale de la Sécurité des systèmes d'information (ANSSI), travaille en collaboration avec des experts européens comme réclamé par l'article 18 du règlement, en particulier sur le respect des règles de sécurité présentes à la fois dans les services offerts, en particulier dans la définition des moyens d'identification, leur

(89) Dans ce dernier cas, l'administration les contacte systématiquement afin de leur offrir le bénéfice d'une prestation (ex. la fourniture de mazout de chauffage, ou l'octroi d'une réduction de redevance pour le ramassage des déchets), sans qu'il n'y ait eu déclaration d'intérêt de la part du citoyen.
(90) Faut-il y voir une nouvelle fonction de FranceConnect qui pourrait ainsi contrôler les usages qui seraient faits des moyens d'identification recourant à l'identité civile et aux registres d'état civil ?

attribution et la gestion de la sécurité de leur usage(91). La question des obligations des tiers de confiance en cas de « brèches » ou failles de sécurité se pose tant vis-à-vis du règlement que du RGPD, comme le note M. Caprioli.

Au-delà, il est demandé à l'État de veiller au respect des trois principes fondamentaux qui entourent la reconnaissance des moyens électroniques d'identification et d'authentification, qu'ils soient publics ou privés, à savoir le principe de neutralité, de non-discrimination et d'équivalence fonctionnelle.

Le droit pénal et l'usurpation d'identité. Mme Monteil nous livre quelques réflexions sur l'impact que le droit pénal, en particulier l'article 226.4.1(92), peut avoir sur la protection des identités qu'elles soient civile ou autres : l'utilisation du nom ou du pseudonyme d'un tiers dans le cadre d'un réseau social pour émettre un message injurieux ou dommageable en l'attribuant à autrui ; l'envoi de messages sous une fausse identité afin d'obtenir un versement d'argent sur la base de soi-disant offres de produits ou services ; l'utilisation d'une clé ou d'un mot de passe dérobés afin de signer un message ou d'accéder à une base de données réservée. L'évocation du cas de Martin Guerre dont un sosie prit la place, sosie finalement démasqué à la suite de la révélation de la perte d'un membre de Martin Guerre sur le champ de bataille permet à l'oratrice de souligner la différence entre l'usurpation d'identité traditionnelle qui avait une dimension corporelle et celle désormais consacrée par le Code pénal où l'usurpation constitue dans l'accès et l'usage de données d'identification dans un contexte où ces données prennent sens même si la qualité et la sécurité de ce moyen en tant qu'identifiant peuvent manquer cruellement. Par ailleurs, un arrêt rendu par la Cour d'appel de Dijon le 16 mars 2017 reconnaît coupable d'usurpation d'identité, un individu qui avait utilisé la photographie d'une femme sur un site de rencontres, s'est servi de son pseudonyme et avait conversé avec des internautes sous couvert de ce pseudonyme : « en l'espèce, dit la Cour, il y a bien manipulation en accolant sciemment sur une page internet la photographie de la plaignante à des propos qu'elle n'a jamais tenus et sous une identité numérique qui n'est pas la sienne ». En d'autres termes, les juges d'appel considèrent donc, bien au-delà du concept d'identité civile, que le profil créé à l'aide d'une photographie et d'un pseudonyme relève de la qualification d'identité numérique. Le numérique oblige-t-il, au regard des manipulations qu'il permet, à élargir la notion d'identité bien au-delà de celle civile ? Le libellé de l'article 226.4.1 du Code pénal, qui précisément a été modifié sur ce point, invite cependant – et c'est le propos de Mme Monteil – à distinguer l'usurpation d'identité de « l'usage d'une ou plusieurs données de toute nature permettant de l'identifier en

(91) « Les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents » (art. 19 du règl.).

(92) L'article 226.4.1 énonce : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende ».

vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ».

La collaboration public – privés. La coexistence des moyens d'identification régaliens, c'est-à-dire mis en place par les autorités publiques et des moyens d'identification non régaliens constitue un fait incontestable et mérite quelques remarques. L'émission des moyens d'identification non régaliens peut, pour des raisons de qualité évidentes, s'appuyer sur les registres d'identité civile, conçue comme noyau dur et garantie de l'identité de chacun. Il est nécessaire de prévoir ainsi des accords entre ces intermédiaires de confiance et l'autorité publique qui garantissent le respect de la finalité de la transmission et la mise à jour périodique si nécessaire des attributs. À l'inverse, la mise sur pied des systèmes régaliens d'identification ou de certification d'attributs ne peut s'envisager qu'avec l'aide de sous-traitants privés. Ici également, on sera attentif à la rédaction de cahiers des charges qui astreignent les prestataires privés à respecter strictement le RGPD ainsi que le règlement eIDAS ou l'article L. 102 CPCE et qui permettent aux pouvoirs publics d'avoir la pleine maîtrise du système. L'exposé introductif de M. Guinamant, représentant du ministère de l'Intérieur(93), mettait en évidence ce risque de voir les autorités publiques perdre leur souveraineté, notamment dans cette bataille de l'identification numérique et en particulier vis-à-vis d'acteurs omniprésents comme les GAFAM.

À l'appui de ces dires, plusieurs exposés et interventions ont souligné l'entrée en jeu d'acteurs privés, déjà présents dans le cadre de systèmes d'identité régaliens. Dans le cas de FranceConnect, on a noté la possibilité donnée à certains prestataires privés de jouer le rôle de fournisseur d'identité, certes dans le cadre des autorisations légales mais qui ne demandent qu'à s'élargir. Le système PReNIUM permet l'accès d'opérateurs privés sans que soient précisés exactement à quelles données et pour quel usage cet accès sera autorisé. L'analyse du système mis en place dans le cadre du système Alicem a suscité nombre de commentaires sur le rôle des pouvoirs privés dans la mise en place des moyens d'authentification et d'identification. Dans ce cas particulier, ce moyen de signature mis au point par les pouvoirs publics n'a pu se concevoir sans un accord avec Google dans la mesure où il nécessite l'accès à la puce qui gère le système ANDROID et l'emplacement du « calibre » sur cette dernière.

Plaider pour une meilleure collaboration entre l'État, garant de l'identité civile et les entreprises privées, les banques et les entreprises qui revendiquent de manière légitime l'accès électronique et facile aux données du registre de l'état civil nous semble nécessaire. Ces entreprises, dans le seule mesure de la légitimité de leur demande, doivent pouvoir disposer de telles données d'identification. L'État jouerait à plein alors son rôle de garantie à la fois première et ultime de l'identité de chacun … et de son évolution dans les limites permises par la loi. Il ne s'agit pas de faire de telles données des données publiques accessibles à tous, de permettre à chacun de pouvoir lire et recopier les données d'identification présentes sur la carte mais au contraire, pour l'État, après avis de la CNIL de définir avec précision les personnes et les usages autorisés des supports des moyens d'identification et d'authentification régaliens.

(93) Le ministère de l'Intérieur était par ailleurs le commanditaire de l'étude confiée à l'équipe de Mme Eynard : *L'identité à l'épreuve du numérique*, à paraître.

C'est ainsi que doit se concevoir le rôle de l'État, ultime certificateur de l'identité des citoyens(94), et « digne » de confiance parce que mettant en place les moyens techniques organisationnels et juridiques du respect des libertés de ces derniers.

(94) C'est ainsi que dans le cadre de FranceConnect, l'interrogation du RNIPP est le fait du téléservice lui-même géré par la DINSIC devenue DINUM, donc par l'État. On note que c'était l'objet même de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité (*JO*, n° 0075, 28 mars 2012), qui « a pour objet de garantir une fiabilité maximale aux passeports et aux cartes nationales d'identité, afin de lutter contre les délits liés à l'usurpation d'identité et à la fraude documentaire. Elle propose de sécuriser la procédure de délivrance de ces titres et de sécuriser les transactions, en introduisant une carte d'identité où figureront les informations biométriques du titulaire, soit sa photographie et ses empreintes digitales numérisées ».