LIVRE BLANC

L'IDENTITÉ NUMERIQUE 5.0

LEXING

ALAIN BENSOUSSAN AVOCATS

LIVRE BLANC

L'IDENTITÉ NUMERIQUE 5.0

SOMMAIRE

AVANT PROPOS **ALAIN BENSOUSSAN**

A l'heure de la fusion annoncée des mondes réel et virtuel, l'identité numérique est un enjeu qui cristallise toutes les attentions.

L'identification d'une personne constitue, on le sait, le prérequis indispensable, tant d'un point de vue technique que juridique, à la confiance et la sécurisation des transactions électroniques, qu'elles soient échanges de messages, contrats, démarches ou procédures voire même workflow internes.

Garantir la confidentialité et la valeur juridique des échanges numériques en identifiant de manière irrévocable les auteurs des contenus, les expéditeurs, les destinataires et tous les tiers autorisés à chaque étape critique, constitue pour cette raison un défi majeur.

Ceci est d'autant plus vrai que se multiplient les entités autonomes appelées à effectuer des tâches pour lesquelles elles ont été conçues et « mandatées » : robots, intelligences artificielles, objets connectés, etc.

Autant de nouveaux acteurs qu'il est également nécessaire, sur fond de risques de fraude et de cybersécurité, de pouvoir identifier[1].

L'identité numérique, définie par la mission parlementaire Karamanli, Hennion et Mis [2] comme « *la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources* », a été consacrée par la loi d'orientation et de programmation sur la performance de la sécurité intérieure (Loppsi 2) du 14 mars 2011 [3] à travers le nouveau délit d'usurpation d'identité en ligne.
De fait, l'identité numérique doit être réservée à des concepts mis en œuvre dans le monde virtuel, des personnalités virtuelles, dont les avatars sont les premières matérialisations. Par ailleurs, le succès des réseaux sociaux et les formes multiples de l'identité numérique multiplient nécessairement les risques d'utilisation de l'identité d'autrui et ceux sous-jacents pour l'entreprise d'être victime de vols d'informations ou encore de campagnes de désinformation.

Intitulé « L'identité numérique 5.0 » [4], le présent Livre blanc a tout d'abord pour objet de décomplexifier au plan juridique l'actualité foisonnante qui entoure l'identité numérique.

Qu'on en juge :

- Édiction, sous impulsion du législateur européen — notamment avec le Règlement e-IDentity And Signature (eIDAS) de 2014 – de nombreux textes législatifs et réglementaires intégrant une composante d'identification électronique ;
- Lancement par le Gouvernement en 2018 d'une mission interministérielle consacrée au déploiement d'un parcours d'identification numérique sécurisé ;
- Projet d'identité numérique porté par le programme France Identité Numérique ;
- Mise en place de FranceConnect en 2016, fédérateur d'identité, et expérimentation d'ALICEM en 2019, la première solution d'identité numérique régalienne sécurisée ;
- Mise en conformité, dès l'été 2021, de la France au droit européen en dotant ses ressortissants d'une carte nationale d'identité électronique.

Mais il vise aussi et surtout à poser les bases nécessaires à la mise en œuvre d'identités numériques « interopérables et inter-opposables dans un écosystème dont les opérateurs ne sont plus émetteurs mais seulement garants des procédures »[5].

Ici comme ailleurs dans le monde numérique, les questions d'éthique, de confiance, de sécurité et de protection de la vie privée, sont immenses. C'est tout le mérite de ce livre blanc de s'en emparer et d'apporter sa contribution au projet global d'émergence d'une identité universelle et irrévocable supranationale et opposable aux tiers.

Alain Bensoussan
Avocat à la Cour
Alain Bensoussan Avocats Lexing

---

[1] En les dotant notamment d'une personnalité juridique dédiée : V. dans ce sens Alain Bensoussan et Jérémy Bensoussan, IA, robots et droits, Bruylant 2019.
[2] Mission d'information commune à la commission des Lois et à la commission des Affaires économiques de l'Assemblée nationale présidée par Marietta Karamanli (Soc), dont les co-rapporteurs sont Christine Hennion et Jean-Michel Mis (LaREM), dont le rapport a été déposé en juillet 2020.
[3] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
[4] Identité 1.0 : sceaux et bannières
Identité 2.0 : registre des baptêmes puis état civil, dont l'aboutissement est la carte d'identité nationale
Identité 3.0 : révolution numérique : adresse de courriel, compte Google ou Microsoft Live, et tout autre «login ID»
Identité 4.0 : certificats cryptographiques et cartes d'identité numériques, dont l'aboutissement est eIDAS
Identité 5.0 : identité numérique irrévocable et supranationale
[5] Cf. Chapitre 7

AVANT PROPOS **PHILIPPE MOREL**

En France, c'est en 1792 que naît l'état civil. Depuis sa création, la gestion ainsi que le contrôle de l'identité sont sous la responsabilité régalienne de l'Etat.

L'arrivée du numérique perturbe nos visions, en particulier parce l'anonymat y est roi et qu'il n'existe pas de frontières sur internet.

Dès lors, que devient le concept régalien dans un univers numérique ? Quelles sont ces nouvelles territorialités juridiques ? Quid de la souveraineté personnelle et nationale ?

L'arrivée du numérique dans toutes les étapes de notre vie reformule cet acquis historique et nous invite à repenser, voire recréer les composantes culturelles et comportementales à partir desquelles se sont nouées nos valeurs aux fins de préserver notre modèle sociétal. Parfois de façon inconsciente, mais constamment ces valeurs sont contrariées par des comportements numériques nouveaux, en mutation constante et en croissance virale.

C'est une universalité numérique qui perturbe les liens et les valeurs qui nous unissent au point de nous interroger sur les principes de confiance, de respect de la vie privée, du secret des correspondances, du secret des affaires, bref de la nature de notre libre arbitre qui nous oblige à redéfinir ce QUI nous sommes et pour quel projet commun.

Le marketing du marché de la confiance laisse à penser que l'authentification serait suffisante à la protection des droits fondamentaux. De même, certains estiment qu'une signature numérique se substitue à l'identité, ou que des certificats cryptographiques suffiraient à la création d'une identité. Il n'en est juridiquement rien.

Une identité est unique et constante.

Nombre d'affaires d'usurpation d'identité avec des fuites massives de données ont réduit à néant l'idée de confiance que les entreprises ainsi que les citoyens pouvaient accorder aux fournisseurs d'identité publics/privés.

La prolifération de ces affaires conjuguée aux moyens de surveillance généralisée accroît avec force et urgence l'impérieuse nécessité d'établir les moyens d'une solution juridico-technologique au service d'une identité numérique opposable aux tiers dans un environnement supranational et protectrice des droits.

Aucune industrie ne saurait s'exonérer du droit

Alors que les entreprises et les citoyens français ont fait de l'internet un outil de la vie quotidienne, qu'un nombre croissant d'entre eux utilisent les réseaux sociaux, que les services de l'état se dématérialisent à grande vitesse, que l'Union Européenne lance un plan d'investissement Horizon 2030 au sein duquel les « new Tech » sont centrales, que le marché de l'identité numérique est évalué comme étant le plus gros marché du numérique, il est indispensable de fournir à tous les acteurs, personnes physiques et personnes morales, robots et autres automates, une identité universellement reconnue offrant à chacun les moyens juridiques de la protection la plus stricte de la vie privée.

Pourrons-nous faire davantage de business avec moins de confiance ?

Il y va de la liberté de chacun et de nos souverainetés en général.

Philippe Morel
Spécialiste de l'identité numérique,
co-fondateur de Woobe

AVANT PROPOS **BERNARD HAUZEUR**

« Remarquable ! »... C'est ce qui vient à l'esprit quand on lit le dernier rapport d'information de l'Assemblée Nationale sur l'identité numérique[6]. Loin de nous la volonté de plagier ce document public dont nous recommandons la lecture en préambule à celui-ci.

En plus de présenter l'état de l'art de l'identité numérique en France, ce document formule 43 recommandations pour « le déploiement rapide de l'identité numérique » (sic). Ce grand nombre de mesures pose question : si tant de mesures sont nécessaires pour atteindre mon objectif, ne dois-je pas remettre en question soit l'objectif que je m'assigne, soit le chemin que j'emprunte pour l'atteindre ?

- Remettre en question l'objectif ? l'aspiration à une identité numérique fiable, universelle, au service des citoyens et d'un commerce honnête, à l'abri des abus et détournements, autant que des turpitudes permises par les avatars auto-attribués actuels... ce serait nier son existence même. Il n'y a pas de demi-identité !

- Remettre alors en question le chemin ? C'est la proposition de ce document.

Le bateau « identité numérique » prend l'eau de toutes parts. On l'a, il est vrai, assemblé en cours de navigation sur l'océan du virtuel. Faut-il alors considérer que l'on est tellement loin de tout port d'attache qu'il ne nous reste d'autre possibilité que de colmater par tous moyens possibles notre bateau, par l'intérieur, avant d'embarquer des millions de passagers ? Ou peut-on se poser quelque part, et demander à nos architectes navals de concevoir le vaisseau du siècle du virtuel ?

Dans les années 80, alors que l'on commençait tout juste à interconnecter des ordinateurs, il devenait de plus en plus clair qu'il fallait aussi penser à poser des serrures sur les portes ainsi ouvertes : on a inventé la sécurité informatique.

Début des années 90, avec la multiplication des ordinateurs personnels, on a inventé les réseaux locaux, et puis le réseau des réseaux : l'Internet.

De l'interconnexion des ordinateurs, on est passé à la connexion de personnes aux ordinateurs, puis aux personnes entre-elles. On s'est mis à penser que l'on pouvait identifier les personnes avec des certificats cryptographiques comme on le fait pour interconnecter des machines. On est resté focalisé sur les questions de sécurité (déjà tellement mises à mal par un développement trop rapide tous azimuts) en passant totalement à côté de quelque chose de fondamental : le Droit ; et en particulier celui qui touche la personne.

Bien sûr, depuis le milieu des années 90 des voix se sont élevées et on a tenté de rattraper l'histoire en collant du Droit par-dessus ce qui était fait. Résultat : eIDAS[7] qui nous dit : c'est peut-être vous (niveau de sécurité « faible »), probablement vous (« substantiel »), ou presque totalement vous (au niveau « élevé » avec un certificat dit « qualifié »).

A l'obligation de la preuve avec obligation de résultat, on a substitué un risque dans une obligation de moyens. La protection de mon identité est-elle juste une question de moyens économiques ? Puis-je accepter le risque que mon fournisseur d'identité soit hacké et me laisse ensuite sans dédommagements suite à sa banqueroute ? Existe-t-il une alternative qui garantirait le résultat ? On doit au minimum se poser la question.

Comment s'y prendre ? Sans doute en partant de ce qu'on a initialement éclipsé : le Droit.

Les mathématiques enseignent qu'il suffit de quelques axiomes bien pensés pour construire des univers cohérents avec des infinités d'applications possibles. Donc la question est : quels sont les axiomes de l'identité numérique ?

Bernard Hauzeur
Architecte informatique, expert en sécurité et identité numérique, co-fondateur de Woobe

[6] Mission d'information de l'Assemblée sur l'identité numérique, Rapport Ass. Nat. N° 3190, 8 juillet 2020.
[7] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014.

AVANT PROPOS **DINESH UJOODAH**

La récente pandémie a accéléré de manière incroyable la transition numérique et nos usages digitaux. Plus que jamais, nous devons retrouver dans le monde digital et les interactions à distance la confiance que nous avons dans le monde réel pour réaliser les actes et transactions de tous les jours.

A bien y regarder le concept est évident : comment s'assurer à l'heure du digital et de la relation à distance que l'interlocuteur qui est en train de faire une opération sur son appareil préféré, mobile ou internet, est bien celui qu'il prétend être ? Comment assurer à son correspondant la garantie et la confiance nécessaire à l'exécution des opérations. Si ce n'est pas le cas, alors on sent bien que c'est tout le développement et le potentiel de services à distance qui peuvent être remis en cause.

Au-delà des bénéfices en matière de droit, les citoyens équipés d'identité numérique verront de nouveaux parcours digitaux très largement simplifiés car l'accès à la donnée entre des écosystèmes pourra être réalisé en toute confiance grâce à des acteurs liés entre eux par une fédération d'identité se faisant mutuellement confiance.

Assurer la véracité de l'identité numérique est vital ! Elle constitue la clé d'accès à des services de plus en plus essentiels où la confiance est au cœur de la relation : services automatisés d'enrôlement et de vérification d'identité (KYC/KYB), services personnalisés et pertinents de santé, accès à des processus administratifs, notariaux, de succession, d'éducation, de mobilité, authentification forte lors des paiements en ligne, authentification forte et simplifiée lors des paiements en magasin, services de souscription de crédits réalisée en trois authentifications fortes...

L'identité numérique constitue au final la base de notre liberté, notre nouvelle Liberté à l'heure du numérique. Et comment s'assurer que chaque citoyen puisse accéder à son identité numérique gratuitement ?

Nous le touchons bien du doigt maintenant : l'identité numérique est la clé de voûte dans le nouveau monde digital. En poser les fondamentaux en matière de droit est nécessaire, c'est l'ambition de ce Livre Blanc. C'est un des défis majeurs qui est posé. Et si le prochain virus planétaire n'était pas biologique mais numérique ? Et si notre identité dans le monde digital était usurpée ?

C'est dans cet esprit que A3BC (Anything, Anytime, Anywhere Biometric Connections), acteur privé de la French Tech, vient compléter les initiatives de l'État en matière de numérique pour offrir aux entreprises privées et aux particuliers des solutions d'identité numérique universelle et d'authentification forte extrêmement sécurisées en s'appuyant entre autres sur la biométrie, locale ou centralisée, pour en simplifier l'utilisation ainsi que sur des brevets en matière de stockage des données.

Notre plateforme est bien entendu conforme à la réglementation européenne concernant la protection des données issue du RGPD (Règlement Général sur la Protection des Données) et afin de répondre aux enjeux de User-Centric Identity nous entamons maintenant le processus de certification eIDAS (electronic IDentification Authentication and trust Services) en y intégrant entre autres les nouvelles avancées technologiques telles que la blockchain (self-sovereign Identity).

Il faut redonner à chaque individu la maîtrise de ses données personnelles, le contrôle sur leur exploitation, la confiance nécessaire à l'utilisation des services qu'il préfèrera par choix et au final permettre à chacun la maîtrise de sa vie toute entière !

Dinesh Ujoodah
CEO d'A3BC

REMERCIEMENTS

1. Sincères et chaleureux remerciements à Lucien Pauliac, Directeur de SCRIPTUM-Archives, pour son soutien technique. Expert en conservation des moyens de preuve, l'expertise de Lucien nous a été d'une grande aide. Qu'il en soit vivement remercié.

2. Remerciements à Anthony Sitbon, consultant, directeur du département Sécurité du cabinet Alain Bensoussan Avocats Lexing, coordinateur de l'ensemble des moyens techniques et humains requis par la création de cet ouvrage, sans qui rien ne se serait fait.

3. Remerciements aux avocats du cabinet Alain Bensoussan Avocats Lexing intervenus dans la préparation de cet ouvrage :

- Éric Bonnet, avocat, Directeur du département Communication juridique ;

- Isabelle Pottier, avocat, Directrice du département Etudes et publications.

1. PREAMBULE

Ce livre blanc pose les bases nécessaires à la mise en œuvre d'identités numériques « interopérables et inter-opposables dans un écosystème dont les opérateurs ne sont plus émetteurs mais seulement garants des procédures ».

4. L'année 1792 marque la création de l'état civil en France. Depuis, la gestion ainsi que le contrôle de l'identité sont sous la responsabilité régalienne de l'Etat.

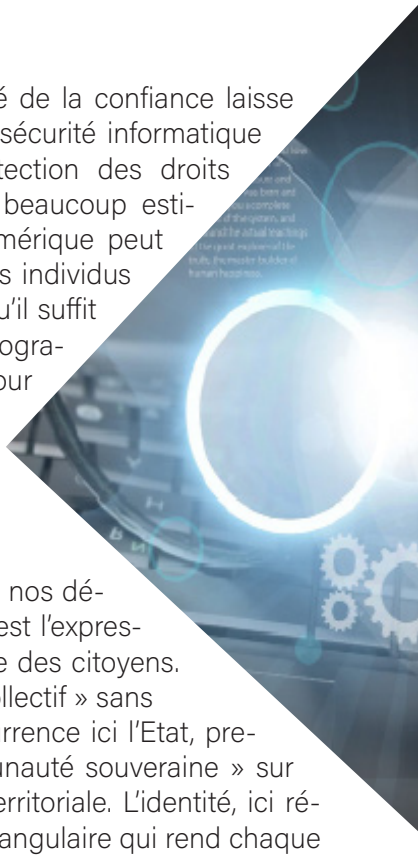
5. Il faudra attendre les années 1990 pour que l'essor inexorable de l'internet remette en question beaucoup de certitudes et d'acquis, par la création d'un nouveau monde, sans frontières, dans lequel l'anonymat est roi et qui se caractérise par l'existence de nouvelles souverainetés, dont les Etats ne sont plus les titulaires, mais qui ont été acquises par les nouveaux acteurs techniques et économiques de l'internet.

6. Le pouvoir des géants de l'Internet est désormais considéré comme plus important que celui de bon nombre d'Etats, rendant obsolète le concept même de pouvoir régalien, et posant en conséquence la question de la délimitation de nouveaux territoires juridiques non géographiques. Ainsi, l'intrusion du numérique dans tous les aspects de notre vie remet en question cet acquis historique que l'on pouvait croire intangible : la vie privée pour les citoyens, le secret des affaires pour les entreprises et la confiance entre tous les acteurs de la société : publics, privés, citoyens.

7. Constamment, et souvent de façon inconsciente, ces valeurs sont contrariées par des comportements numériques nouveaux, en mutation constante, voire incontrôlée, et en croissance virale. La possibilité de vous tracer en tous lieux et de mesurer en permanence vos choix et vos activités en regard d'un « profil », ne sont-ils pas des outils de domination ? Ou juste un outil commercial sympa «on-va-vous-faire-plaisir» ? Ou une question de sécurité nationale ?

8. C'est une universalité numérique qui perturbe les liens et les valeurs qui nous unissent au point de remettre en question notre libre arbitre, et qui nous oblige à redéfinir QUI nous sommes dans ce monde numérique parallèle, et pour quel projet commun.

9. Le marketing du marché de la confiance laisse à penser qu'une meilleure sécurité informatique serait suffisante à la protection des droits fondamentaux. De même beaucoup estiment qu'une signature numérique peut se substituer à l'identité des individus ou des entreprises parce qu'il suffit de relier un certificat cryptographique à une personne pour créer une identité.



10. Or il n'en est juridiquement rien.

11. Retour à la racine : dans nos démocraties, la souveraineté est l'expression de la volonté collective des citoyens. Or il ne peut y avoir de « collectif » sans « communauté », en l'occurrence ici l'Etat, premier exemple de « communauté souveraine » sur une base historiquement territoriale. L'identité, ici régalienne, est alors la pierre angulaire qui rend chaque membre de cette communauté responsable vis-à-vis des autres et du bien collectif, ainsi que de lui garantir le contrôle[8] sur le degré de partage qu'il souhaite entre le personnel et le collectif, grâce au système de Droit auquel cette 'communauté' répond, ou dont cette communauté s'est souverainement dotée.

12. Le monde virtuel a créé des « identités numériques » – c'est un fait[9]. Elles échappent à notre contrôle, planent au-dessus de notre devenir, et ne sont rattachées à RIEN de souverain ni de collectif, si ce n'est les contrats de service des sociétés commerciales étrangères, les GAFAM's[10], gouvernées par des intérêts privés.

13. La question de la souveraineté est la clé de l'identité. Si l'identité n'est pas rattachée à une communauté au sein de laquelle règne un système souverain de droits et d'obligations, alors nous ne sommes pas libres, mais asservis.

[8] ...ou encadrer sévèrement, dans le cas des états autoritaires ! Contrôle personnel = liberté, contrôle par l'état = autorité.
[9] Clairement affirmé et décortiqué par Blandine Mallet-Bricout et Thierry Favario (L'identité, un singulier au pluriel, Dalloz 2015) et (Nicolas Chambardon, L'identité numérique de la personne humaine : contribution à l'étude du droit fondamental à la protection des données à caractère personnel, Thèse de doctorat en Droit public, 27-09-2018).
[10] Google Amazon Facebook Apple Microsoft et toutes les autres par extension comme Tencent, ByteDance, Snap, Uber, Baidu, Alibaba, etc.

Nos 'identités numériques' auprès des GAFAM's n'ont rien de souveraines : elles sont asservies aux lignes de code opaques des applis éditées par ces sociétés et à leurs conditions générales unilatérales.

14. La question de l'identité est étroitement liée à la notion de souveraineté. Souveraineté individuelle et souveraineté collective (communauté). Il n'y a pas de souveraineté Internet : « Les États sont des lieux, l'Internet est un lien. Les souverainetés se définissent dans des espaces physiques délimités, l'Internet est une dimension qui relie tous les territoires sans en être un lui-même ».[11]

15. Le monde numérique a éclaté les frontières des états et les GAFAM's ont pris le contrôle à notre grand dam ! Or, ce sont les états qui sont dépositaires de la souveraineté d'un système de Droit apte à protéger les entreprises et les citoyens sur leur territoire. Les états ne sont pas en position ni ne disposent des moyens de s'imposer comme les « communautés » émettrices d'une « identité »[12] universelle à moins de se transformer en « territoire numérique »[13] ; les GAFAM's les ont largement devancés et se sont attribué ce rôle.

16. Quant aux entreprises industrielles, elles s'en tiennent aujourd'hui à leurs stricts besoins, et donc à des systèmes IAM (Identity & Access Management) composant de leur infrastructure informatique ne permettant la reconnaissance mutuelle que de leurs seuls employés[14]. Elles souscrivent ensuite quelques certificats cryptographiques aux PKI's[15] pour les besoins de sécurisation des échanges avec l'extérieur et d'authentification mutuelle, soit entre systèmes, soit entre personnes soit entre les personnes et les systèmes.

17. Pas de quoi créer une « identité » sur la toile, alors que ces personnes morales – les entreprises – sont rattachées par nature à un système de Droit et forment des communautés naturelles légales émettrices de mandats (contrats d'emploi, représentants) gouvernant une grande partie de notre identité et de notre vie : le travail. De plus, les entreprises ont des moyens et une rapidité d'action que l'état ne peut s'offrir.

18. En fait, Microsoft, Google, Facebook ont montré une voie : celle pour les entreprises de devenir émettrices d'identités numériques[16] ; sauf que, c'est actuellement dans les mains de sociétés dont la finalité est de monnayer nos vies privées ; nous devons permettre aux sociétés qui nous emploient (et pas qu'elles) de devenir émettrices d'identités numériques[17], juridiquement opposables[18], sur une base universelle et souveraine, pour permettre la reconnaissance mutuelle de celles-ci.

19. Cela permettrait à un partenaire d'une société de reconnaître également l'identité assignée par un tiers (qu'il s'agisse d'engager temporairement le consultant d'un tiers, ou de négocier avec un nouveau partenaire), et de disposer des garanties que cette reconnaissance repose sur les bases juridiques nécessaires à la protection légale de ses affaires.

20. Leurs investissements IAM et leur travail de gestion du personnel s'en trouvent revalorisés par une portée hors des murs de l'entreprise qui peut être mise au service des affaires.

21. This.is.me@SomeCompany.com ne serait plus une présomption, mais une source de certitudes.

---

[11] Pierre Bellanger, La souveraineté numérique, Édition Stock, janvier 2014.

[12] Très peu d'états dans le monde dotent actuellement leurs citoyens d'une identité 'électronique', qui dans tous les cas ne se rattache à aucune «communauté numérique» identifiée, et ne dispose d'aucun statut juridique propre. C'est juste un moyen technique d'authentification reconnu par un certain nombre de prestataires de services, dont les administrations de l'état. Et comme il s'agit d'un contrat d'adhésion, la qualité ou la faiblesse de ce moyen n'engage que son émetteur, l'état, sauf à prouver la faute de l'utilisateur. Les cartes de crédit émises par les banques tiennent de ce même régime. Rien de bilatéral (je t'identifie, tu m'identifies) ni d'équilibré entre deux partenaires, comme ce doit être le cas pour le commerce.

[13] Par exemple, la Chine pour laquelle un Internet trop ouvert met en danger son système politique et son autorité.

[14] Pire, avec le Cloud, des entreprises de plus en plus nombreuses asservissent leurs systèmes IAM aux applications collaboratives et bureautiques en ligne des mêmes entreprises géantes du numérique. Non seulement celles-ci ont raflé toutes les identifications personnelles, elles sont en train de prendre aussi le contrôle des identités professionnelles, et – cerise sur le gâteau — en se déchargeant au passage des coûts d'administration et de maintenance de ces identités !

[15] Public Key Infrastructures, les opérateurs d'infrastructures à clé publique qui sont les émetteurs des certificats cryptographiques.

[16] Notons aussi que Visa, MasterCard, Amex et autres ont également montré la voie en distribuant des cartes de crédit, succédané d'une identité numérique, avec un système de reconnaissance par des tiers, les banques, mais dans un domaine refermé sur leur business et un seul type de commerce : le paiement.

[17] Très loin de la sous-traitance par l'entreprise de l'émission d'un certificat cryptographique pour chaque employé comme on le verra.

[18] Les GAFAM's n'ont que faire d'une identité «légale». Elles ont seulement besoin de traces monnayables ; l'auto-attribution d'une identité est largement suffisante. Bien à l'abri derrière leurs clauses contractuelles elles ne se sentent pas plus responsables des turpitudes de leurs membres. Pire : une identité numérique forte serait un frein et les impliquerait juridiquement. Leur intérêt est de rester sur des identités numériques faibles, économiquement viables.

2. OBJECTIFS

2.1 Contexte

22. Ce livre blanc propose une base de construction d'identités numériques dans le cadre de communautés souveraines tant à l'échelle d'un État, que d'une société commerciale, ou encore d'un simple groupe d'intérêt.

23. Autant les communautés du monde réel (entreprises, institutions, administrations, associations) que celles du monde virtuel seraient invitées à mettre en œuvre des identités numériques interopérables et inter-opposables dans un écosystème dont les opérateurs ne sont plus émetteurs[19] mais seulement garants des procédures.

24. Cette base de construction réconcilie également la nécessité d'identifier toute entité autonome, agissante et juridiquement imputable : robots, objets connectés, voire des algorithmes dotés d'une intelligence artificielle et aux décisions desquels nous sommes de plus en plus confrontés.

25. Cette identité numérique reconnaît la prééminence des mandats dans l'exécution de toute tâche :

- En commerce, on agit rarement pour son propre compte, mais pour celui de sa société ou de son employeur. Les professions libérales - prenons un médecin - ont tout autant besoin de séparer leur vie familiale de leurs responsabilités médicales.
- On ne peut auto-déclarer son identité ou sa fonction pour en obtenir ensuite des effets de Droit. Il y a toujours un tiers qui confirme vos attributions (comme un directeur des ressources humaines), voire un état civil (un officier ministériel), ou un statut (registre des personnes morales). Vous êtes mandaté dans vos fonctions, et celui qui vous l'attribue doit bien sûr être mandaté pour le faire, au nom de la communauté (institution, personne morale, État) qu'il représente.[20]

- Les mandats sont la clé pour doter nos artefacts intelligents d'une personnalité juridique dûment assortie d'une responsabilité : véhicules, objets connectés, robots, et algorithmes doués d'une autonomie de décision et d'une capacité à agir dans le monde réel ou virtuel.
- Les personnes morales ont une existence juridique avec une identité, mais pas de capacité à agir : elles agissent au travers de leurs représentants, dûment mandatés.
- Les personnes en difficulté physique (handicaps) ou économique (équipements nécessaires) peuvent naturellement mandater un tiers pour agir en leur nom, limité par la portée de son mandat.

26. L'identité d'une personne ne saurait se réduire à sa seule signature que ce soit dans le monde réel ou dans le monde numérique :

- L'identité d'une personne se manifeste dans tous les actes de sa vie courante comme lors de ses démarches administratives, pour marquer son consentement (commande, signature électronique), pour accéder à un service ou un compte, mais aussi à l'occasion d'une publication, lors de l'obtention d'un diplôme ou d'une certification professionnelle, lors de la gestion de la propriété (intellectuelle, industrielle, commerciale), ainsi que pour la bonne marche des affaires tant personnelles qu'en entreprise (acheter, vendre, engager, autoriser, partager, produire, payer, livrer, etc.).
- Pour un robot, il s'agira plus souvent de l'identifier pour lui permettre d'effectuer les tâches pour lesquelles il a été certifié (conduite autonome, prescription médicale, manutention) dans le périmètre d'action (route, ville, soins, entrepôt) pour lequel il est mandaté.

27. L'identité est à la base des mandats, et donc de la capacité à agir (que puis-je faire, dans quel périmètre, au nom de qui), tant des personnes que des artefacts intelligents. Elle touche aussi l'archivage (mes documents, ceux de mes entreprises, la mémoire d'un robot), et la conservation (cadastre, publications, patrimoine, registres publics, traces d'un robot dans les lieux publics).

28. Ce livre blanc est politiquement neutre. Il ne plaide nullement pour l'obligation d'utiliser une identité numérique ou la disparition de l'anonymat sur Internet. Il ne pose ni limite, ni restriction quant aux applications ou exclusions de l'identité numérique proposée.

[19] A la grande différence des PKI / Infrastructures à clés publiques.
[20] Les PKI's ne représentent aucune communauté professionnelle et n'ont donc pas le pouvoir souverain d'attribuer des identités aux membres d'une communauté qu'ils ne représentent pas ; ils doivent changer de rôle et passer d'émetteur à fournisseur des moyens permettant aux délégués des droits de chaque communauté d'exercer leur souveraineté, à commencer par la création d'identités ici numériques.

29. Il propose un écosystème de communautés souveraines, autonomes et libres, tout comme les individus, d'exprimer leurs choix, leurs volontés, et leurs propres règles et limites dans un cadre transnational permettant de viser l'inter-opposabilité juridique.

30. Il laisse autant ouverte la possibilité d'imposer une seule identité régalienne et souveraine à l'échelle de l'État, que d'accepter la multiplication d'identités mutuellement reconnues à l'échelle de communautés souveraines associatives, commerciales, voire même individuelles.

31. Ce livre blanc se base sur le système de Droit romano-civiliste ou Droit Napoléonien par opposition au Droit anglo-saxon ou Common law, et s'attache plus précisément au périmètre européen.

32. Ce livre blanc est technologiquement neutre. Il n'évalue ni ne recommande aucune solution technique, celles-ci étant amenées à évoluer en permanence, mais formule les exigences fonctionnelles et structurelles nécessaires aux effets de Droit.

33. Tout au long de ce document, chaque exigence structurelle ou fonctionnelle découlant de la logique et/ou de principes de Droit sera clairement mise en évidence comme illustré ici par ce symbole : ⚠

2.2 À qui s'adresse ce livre blanc ?

34. Ce livre blanc s'adresse aux professionnels de structures privées ou publiques afin de les aider à résoudre les problèmes que leur posent les contraintes juridico technologiques dans la mise en œuvre d'une solution d'identité sur base numérique, applicable aux relations entre personnes physiques, morales, et les artefacts intelligents (véhicules autonomes, IA, objets connectés) qui prennent une place croissante dans le fonctionnement de la société dans son ensemble.

35. Cet ouvrage se veut pédagogique pour appuyer les études dans ce domaine, et alimenter le débat universitaire, voire normatif.

3. LA NAISSANCE ET L'IDENTITÉ

L'identité numérique est définie par la mission parlementaire Karamanli, Hennion et Mis comme « la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources » (Rapport Ass. Nat. N° 3190, 8 juillet 2020).

36. « L'identité d'une personne peut être vue comme un ensemble de composants grâce auxquels il est établi qu'une personne est bien celle qui se dit ou que l'on présume d'elle ».[21]

37. « L'identité numérique est définie comme un lien technologique entre une entité réelle (personne, organisme ou entreprise) et des entités virtuelles (sa ou ses représentations numériques). Elle permet l'identification de l'individu en ligne ainsi que la mise en relation de celui-ci avec l'ensemble des communautés virtuelles présentes sur le Web[22]. L'identité numérique est non seulement construite par l'entité réelle ou le « Sujet », mais elle est également grandement influencée par le rapport qu'entretient ce dernier à autrui de même qu'à la société[23] »[24].

38. Pour une analyse très complète de toutes les facettes de l'identité en Droit (et son pendant consubstantiel : l'anonymat), renvoyons le lecteur aux actes du colloque sur l'identité organisé par l'Université Lyon 3.[25]

3.1 Que disent nos institutions ?

39. En recherchant sur Internet « identité numérique Europe », vous tombez immédiatement sur le règlement européen « eIDAS »[26]. Ce règlement, adopté en 2014 par le Parlement Européen et le Conseil de l'Union Européenne, est entré en vigueur en France la même année.

40. Il concerne en premier lieu les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union Européenne.

L'objectif de « eIDAS » est d'instaurer un cadre juridique propre à susciter une confiance accrue en matière d'identification électronique et de services de confiance dans les transactions électroniques au sein du marché de l'Union Européenne et ainsi de permettre l'émergence du marché numérique unique.

41. Son objectif étant de créer le socle commun d'interopérabilité que la précédente directive 1999/93/CE sur la signature électronique n'avait pas réussi à créer, il ne remet en question aucune des pratiques existantes qui consistent à attribuer un certificat cryptographique à une personne en guise d'identité. Un certificat cryptographique est la base minimale nécessaire à la création technique d'une signature électronique, une signature = une personne, donc une personne = un certificat.

42. C'est le raisonnement implicite tenu depuis des décennies et par « eIDAS » également. Cette application de la cryptographie est abondamment normalisée, elle est concomitante à l'essor des infrastructures à clés publiques (PKI). « eIDAS » précise dans un règlement d'exécution (2015/1502) la mise en œuvre des technologies afférentes de façon à promouvoir l'interopérabilité, et propose même un logiciel libre. [27]

43. « eIDAS » ne contient aucune définition de l'identité et se limite à l'identité des personnes physiques et morales. Il évoque les attributs d'une identité sans les définir.

44. Le rapport de l'Assemblée Nationale sur l'identité numérique[28] est plus fouillé. Il évoque dans son introduction la multiplicité des définitions, introduit les concepts d'identifiant et d'identité pivot, notamment à la base du projet FranceConnect.

45. Sur le concept même d'identité, le rapport s'en remet à l'histoire, où l'écrit a remplacé le face-à-face, pour aboutir à la création par l'État des registres d'état civil. Ceux-ci ont remplacé les «registres des baptêmes» rendus obligatoires par François 1er.

[21] Serge Guinchard, Gabriel Montagnier, Lexique des termes juridiques, Dalloz 16e éd. juin 2007
[22] Cité par Fanny Georges, « Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 » Réseaux, vol. 2, no 154,2009, pp. 165-193.
[23] Cité par François Perea, « L'identité numérique : de la cité à l'écran. Quelques aspects de la représentation de soi dans l'espace numérique », Les Enjeux de l'information et de la communication, vol. 1, 2010, pp. 144-159.
[24] fr.wikipedia.org
[25] Blandine Mallet-Bricout et Thierry Favario, L'identité, un singulier au pluriel, Dalloz 2015.
[26] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014.
[27] Digital Signature Services DSS https ://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS.
[28] Mission d'information de l'Assemblée sur l'identité numérique, Rapport Ass. Nat. N° 3190, 8 juillet 2020.

C'est la révolution française qui retire la tenue des registres des mains de l'église catholique pour la confier à l'État, et ainsi créer l'identité dite régalienne.

46. On consigne donc dans un livre les informations permettant d'identifier chaque individu : nom, prénom, lieu et date de naissance, identités du père, et de la mère, parfois assorties des professions de ceux-ci, leurs signatures, ainsi que le nom de l'officier d'état civil qui procède à la constatation suivie de sa propre signature. Un numéro de référence est assigné à chaque entrée dans le registre.

47. Aujourd'hui l'information est communiquée électroniquement à l'administration publique par le médecin de la maternité dès l'accouchement. Un numéro national d'identité est assigné.

48. Un nouvel être naît[29] et se voit attribuer une première identité liée à sa personnalité juridique ; c'est aussi simple que cela pour les personnes physiques.

49. Pour les personnes morales, c'est fort semblable : le Greffe enregistre les informations d'identification dans le registre du commerce et des sociétés : nom, forme juridique et régime fiscal, adresse du siège, type d'activité, statuts, représentants.

50. A quelques variantes près, le principe est le même dans toute l'Europe.

51. Pour les robots et autres artefacts intelligents ? Néant ; bien que de très nombreux travaux soient en cours sur le sujet, tant au niveau de l'Europe (ex. euRobotics), que des États, ou de consortiums privés.[30]

3.2 L'identité des artefacts : robots, algorithmes d'IA

52. Notre monde ne se limite plus aux personnes physiques et morales. Les robots sont de plus en plus intelligents et autonomes. Le monde numérique se peuple d'algorithmes d'Intelligence Artificielle qui prennent des décisions qui impactent déjà notre mobilité, nos carrières, notre santé, nos rencontres, voire nos opinions, avec des impacts dans le monde réel. La robohumanité à venir ne peut être écartée de la question de l'identité numérique.

53. L'ouvrage « IA, Robots, et Droit »[31] présente une analyse très complète de la question. Les auteurs constatent que l'idée d'une personnalité juridique des robots est admise même si son statut n'est pas finalisé, ni les registres des « personnes électroniques » mis en œuvre. L'article 3 de la Charte des droits des robots proposée dote le robot d'une personnalité juridique « composée de droits et obligations exercés par son représentant légal ». « Une personne robot possède une identité propre, un numéro d'identification, ainsi qu'un capital dont l'unique objet est de réparer les dommages éventuellement causés par elle »[32]. Cela reste une proposition, mais donne clairement une direction à suivre.

54. Dans le cas des artefacts intelligents (robots, algorithmes) formant des assemblages complexes comme un véhicule autonome, on peut se poser la question du nombre et de la frontière des entités identifiables. En effet, l'opérateur du véhicule peut légitimement sous-traiter la conduite à un logiciel « co-pilote » intelligent[33], maintenu et opéré par une société tierce, et opaque pour l'opérateur du véhicule en propre. Le logiciel « pilote » détecte l'état de la route, les obstacles, leur nature, et informe en continu le robot-véhicule qui lui gère la vitesse, la direction, et le plan de route.

55. Selon leurs intelligences respectives on pourrait assigner 1 ou 2 identités avec leurs responsabilités associées au même titre qu'un pilote et son co-pilote, ou zéro si la volonté est de mettre en avant un opérateur de transport responsable de l'ensemble qui organise avec ses sous-traitants les responsabilités respectives entre le fabricant (défaillance mécanique), la société de maintenance (défaut d'entretien), ou l'éditeur du logiciel de conduite (défaut de navigation).

56. Le monde numérique rend la copie facile, voire nécessaire aux étapes de mise en production, aux sauvegardes, ou encore à la distribution de la charge de traitement des données. Qu'en est-il alors des copies d'un même algorithme IA sur plusieurs environnements ? Y a-t-il plusieurs identités ou une seule ? Et si un pirate détourne une copie pour l'asservir à ses propres desseins ? Est-ce toujours la même entité ?

57. Le Droit traite déjà le cas des personnes kidnappées agissant sous la contrainte, et la multiplication de

[29] Le Droit reconnaît l'existence d'une identité avant la naissance et après la mort, cf. Blandine Mallet-Bricout et Thierry Favario, L'identité, un singulier au pluriel, Dalloz 2015

[30] Un inventaire fouillé de toutes ces initiatives est contenu dans « IA robots et droit » d'Alain Bensoussan et Jérémy Bensoussan paru chez Bruylant, Editions Larcier, collection Théorie et pratique, juillet 2019.

[31] Alain Bensoussan, Jérémy Bensoussan, « IA robots et droit », préc.

[32] « IA robots et droit », annexe 19, préc.

[33] On parle ici d'IA capables de faire face à des situations inédites et dont l'expérience conditionne la réponse. Un GPS même très sophistiqué qui planifie la route reste un composant technique

copies licites d'un même algorithme n'élude pas la question de la responsabilité de chaque « copie » : soit les « copies » sont juste le fait d'une question technique d'architecture interne à une seule entité logique, soit ces copies sont autonomes et, par exemple, dans les mains d'opérateurs différents, et donc forment autant d'entités indépendantes, communicantes, et responsables.

3.3 Que dit le Droit sur l'identité ?

58. Laissons de côté l'identité des débats philosophiques, tout comme celle des nuances ipse ou idem[34], pour nous focaliser sur l'identité la plus réduite telle que strictement nécessaire à la création d'une identité numérique porteuse d'effets juridiques.

3.3.1 Personnalité juridique et identité numérique

59. Le Droit reconnaît l'identité biologique de l'individu, son autonomie physique et mentale, sa capacité à agir[35]. Mais si on élargit le champ des entités à prendre en compte aux personnes morales, robots et IA ainsi que nos avatars numériques, l'aspect de l'identité qui nous intéresse est celui qui confère aux entités ainsi identifiées une personnalité juridique assortie de droits et d'obligations.

60. En pratique, cette identité-là se confond avec l'inscription dans un registre des éléments nécessaires à son identification univoque, et constatant l'existence d'une entité juridiquement responsable de ses actes, assortie d'un patrimoine (propriétaire de toutes natures) comprenant son intégrité physique (mécanique pour les robots), voire son intégrité numérique (algorithmes et métadonnées), ainsi que ses avoirs tant matériels qu'immatériels (renommée, œuvres, habilitations, contrats, capacités, expertise, clientèle, mémoire, connaissances et données numériques[36], capital, etc.).

61. Nous sommes parfaitement conscients du risque de verser dans ce que le professeur Grégoire Loiseau dénonce comme la dérive d'un « techno personnalisme favorisant la colonisation des droits humains au profit d'entités qui n'en sont pas moins totalement dépourvues de sentiment d'identité ou de perception d'elles-mêmes »[37]. Certes, loin de nous la volonté de réduire la personne humaine à une entité « organo-mécanique ». Il ne sera jamais dit ici que le Droit applicable à une personne humaine ne pourra plus prendre en compte bien d'autres facteurs que celui appliqué à un robot. Notre propos n'est fédérateur entre les hommes et les entités non humaines que sur la seule question de l'attribution d'une identité numérique imputable.[38]

62. En dehors de ce champ, rien n'est remis en question ; au contraire, comme expliqué dans le Préambule (chap. 1) il est urgent de redonner à l'humain le contrôle de toutes les manifestations de son identité dans le monde virtuel et d'y instaurer une forme de souveraineté.

3.3.2 Caractéristiques de l'identité numérique

63. Que l'on soit une personne physique ou morale, ou bien un robot, algorithme ou autre artefact intelligent il y a donc une triple caractéristique :

- La constatation par un tiers de l'existence de l'entité visée, à sa naissance ou à sa création,
- L'enregistrement dans un registre des attributs qui caractérisent cette entité en tant que personne unique, et, de façon pragmatique,
- L'assignation d'un identifiant unique dans ce registre.

64. Constatons également que le registre visé est toujours lié à une communauté, en l'occurrence un État dans le cas des identités régaliennes. Mais il existe de nombreuses autres communautés porteuses d'un système d'identification[39] : les sigles des titres (et par extension l'identité de leurs émetteurs) sur les bourses, les codes DUNS, SWIFT ou BIC, les Airline-Codes IATA en 2 à 3 lettres, le numéro d'enrôlement des armées, et même l'identité déclarée de la Légion Etrangère qui apparaît comme un très ancien précurseur dans le monde réel des multiples «identités» que nous nous auto-assignons dans le monde virtuel.

65. ⚠ Il est donc clair que mon identité numérique s'exprimera en pratique au travers d'un identifiant numérique et que celui-ci doit m'être attribué par un tiers

---

[34] « idem » = ce que je suis objectivement / biologiquement ; « ipse » = qui je suis dans ma perception par moi-même et l'image que je renvoie aux autres.
[35] Quid de la volonté ? Les entités artificielles ont-elles une volonté ? Il n'est pas nécessaire de trancher ce débat ici ; la notion de capacité à agir est suffisante au caractère imputable des actes.
[36] Le patrimoine numérique a aujourd'hui autant de sens pour une personne physique que morale, une personne robot ou une IA. La capacité de relier ce patrimoine à une identité dans ce même monde, à savoir numérique, et capable de s'appliquer aux personnes physiques, morales, robots, algorithmes et autres artefacts intelligents revêt une nécessité évidente.
[37] Blandine Mallet-Bricout et Thierry Favario, L'identité, un singulier au pluriel, Dalloz 2015.
[38] Possibilité d'attribuer la responsabilité d'un fait à une personne.
[39] Certes, la plupart ne sont porteurs d'effets juridiques qu'au travers des identités «officielles» auxquels ces systèmes se raccrochent.

lié au registre de la communauté juridique que je rejoins. Idem pour les personnes morales, robots, algorithmes, et autres artefacts intelligents.

66. ⚠ Notons que nous ne pouvons exclure l'inscription d'une même personne dans plusieurs registres[40] de communautés différentes. Or, le droit reconnaît la multiplicité des usages, mais affirme dans le même temps l'unicité de l'identité. Nous ne devons pas éluder que l'identité transcende l'inscription dans un registre.

3.3.3 Identité et communautés numériques

67. En Droit, l'identité est une notion à la fois singulière et plurielle. Singulière par son unicité, plurielle par ses usages : « je » peux à la fois être administrateur d'une société, employé dans une autre, trésorier du club de tennis voisin, père de famille et à ce titre chef du foyer fiscal, membre de l'Amicale Des Bouilleurs De Cru De Montferrand Le Château, ainsi que conducteur d'une camionnette de collecte de denrées alimentaires pour les Restos du Cœur. L'imputabilité variera pour chacune de ces attributions.

68. Il y a donc un seul « je », qui ne change pas, et une infinité de « communautés »[41] au sein desquelles j'exerce des « fonctions » avec des responsabilités associées (on reparlera ci-après de capacité à agir).

69. En Droit : l'identité civile est constante[42] et permanente[43] et plurielle[44] dans ses applications quotidiennes.[45]

70. Dans le monde numérique, il n'y a aucune raison de voir l'Internet comme une seule communauté au sein de laquelle je n'exercerais qu'une seule fonction. On doit donc pouvoir créer autant de communautés « numériques » que désiré, et leur assigner une identité en regard de leur personnalité juridique. Comme les individus, ces communautés «numériques» peuvent avoir une existence dans le monde réel en tant que société commerciale, institut, association, groupement d'intérêt, etc.

71. ⚠ Mon identité numérique doit aussi être permanente, constante, et plurielle dans ses applications. En découlent 2 possibilités :

- Mon identité numérique est liée à un identifiant seulement lié à ma personne, et la fonction que j'exerce à un moment donné dans une communauté particulière n'est reflétée que par le contexte dans lequel j'utilise cet identifiant ;

- Mon identité numérique se décline en autant d'identifiants que j'exerce de fonctions.

72. Cette deuxième possibilité est beaucoup plus intéressante car elle permet notamment de désigner une personne par la fonction qu'elle exerce au sein d'une communauté[46] et de gérer le cycle de vie propre de cette fonction en toute souveraineté[47]. De plus elle n'exclut pas la première.[48]

3.3.4 Place des identifiants numériques

73. ⚠ Rien ne s'oppose donc à ce que je dispose de plusieurs identifiants numériques auprès de plusieurs registres.

74. ⚠ Comme dans le monde réel, je dois pouvoir garder la possibilité de « naviguer » ou de « m'exprimer » dans le monde numérique sans être systématiquement identifié : je reste libre d'utiliser l'identifiant que je souhaite, ou de ne pas en utiliser.

75. Il n'y a pas de lien de Droit entre un certificat et son utilisateur ; il devient clair qu'un certificat cryptographique ne peut servir d'identité numérique :

- Il n'est ni constant, ni permanent :

  ▪ Je peux perdre mon « identité » /certificat, et entreprendre une démarche pour la récupérer ;
  ▪ Elle devra être renouvelée typiquement tous les 2 ans ;
  ▪ Le cycle de vie d'un certificat cryptographique et celui de mon identité numérique n'ont rien de commun, les associer apparaît comme un non-sens ;

---

[40] Il n'est même pas besoin de se restreindre au cas des personnes disposant de plusieurs nationalités, qui d'entre nous n'a pas à la fois un passeport et une carte d'identité ?
[41] Ce terme est utilisé ici pour désigner à la fois les sociétés – personnes morales, les institutions ou organismes, les associations professionnelles, les ASBL, les groupements d'intérêts, les corps constitués, et toute forme de groupement doté d'une personnalité juridique.
[42] Identique, invariable, à travers tous les moments de son existence (mais pourrait apparaître et disparaître).
[43] Existe sans discontinuer, sans interruption (mais pourrait changer au cours de cette existence continue).
[44] La pluralité de l'identité peut faire référence à des variations de genre ou ethniques, religieuses, culturelles, ou de la nature de l'entité identifiée (humaine, robot, IA). Le sens présent fait référence à l'exercice d'une identité.
[45] Blandine Mallet-Bricout et Thierry Favario, L'identité, un singulier au pluriel, Dalloz 2015
[46] Comme adresser légalement un document au «Directeur de la société XYZ» sans le nommer et hors de tout contexte.
[47] Il y a bien d'autres avantages comme nous le verrons par la suite.
[48] En tant qu'employé de la société W (= fonction FW attribuée par le DRH) je peux me faire membre de deux forums en ligne, ainsi que d'une communauté professionnelle relative à cette fonction, conduisant aux 3 «usages» FWa, FWb, FWc d'une même «identité». Mais je suis aussi trésorier d'un club (= Fclub attribuée par le comité de gestion), et abonné à la SNCF (= F0 = en mon nom propre).

▪ Mon « identité » /certificat a une date d'expiration : non-sens ;
▪ Elle peut être révoquée : un absolu non-sens.

- Un certificat cryptographique est un instrument de sécurité efficace ; c'est une clé, au même titre que la clé de ma voiture, de ma maison, d'un coffre. L'identité n'est pas une clé, ni ne peut être réduite à un problème de sécurité.
- L'autorité de certification émettrice – et tous les opérateurs intermédiaires entre moi et cette dernière – disposent d'un pouvoir de nuisance si le renouvellement de mon certificat échoue à son expiration. Il se pourrait que je ne puisse plus être moi ![49]
- En dehors du champ de la signature électronique, la clé privée associée à mon certificat cryptographique doit être doublée d'un mécanisme de « key escrow », ce qui implique qu'une 'copie de mon identité' est aux mains d'un tiers.
- S'approprier le certificat cryptographique d'une personne, ce n'est pas que s'approprier son identifiant, mais toute sa personne dans le monde numérique.[50]
- Quand les ordinateurs quantiques pourront casser les systèmes de chiffrement à clé publique, ils ne casseront pas que les communications cryptées, mais toutes les identités.

3.3.5 Identité numérique et certificats cryptographiques

76. ⚠ Il est donc impératif et urgent de dissocier l'identité numérique des certificats cryptographiques.

77. Certes, on doit utiliser les certificats cryptographiques, et même abondamment, pour sécuriser toutes les applications de mon identité numérique. Mais mon identité numérique doit pouvoir traverser toute la diversité, le renouvellement, et la multiplication des mécanismes de sécurité nécessaires aujourd'hui dans le monde numérique sans me lier à ces mécanismes.

78. Si mon identité tient à un certificat cryptographique, je n'ai qu'un seul mécanisme pour me protéger, et je ne peux pas multiplier celui-ci sans multiplier mon identité.

79. Il en va de même pour l'identité numérique des personnes morales, des robots, des entités intelligentes.

80. Nous laissons à ce stade deux questions importantes en suspens :

- Comment vais-je détacher cette identité d'un certificat ou tout autre objet cryptographique sans l'exposer aux abus ? Autrement dit : comment puis-je garder le contrôle exclusif de mon identité numérique si elle se réduit à un identifiant ?

- Comment réconcilier le caractère unique de l'identité avec sa pluralité ? Précisément, avec la multiplicité d'usages qualifiés en relation avec les fonctions exercées au sein de différentes communautés ?

▪ Cette question soulève un double défi :
(a) le cloisonnement entre ces usages multiples ; à savoir d'éviter que l'accès à mes documents professionnels, voire pour différents clients potentiellement concurrents, ne se confonde entre eux et avec ceux de ma vie privée ;
(b) le cycle de vie indépendant et entremêlé de chacune des attributions légalement liées à une même identité : je suis nommé administrateur, je suis élu président du club pour 2 ans, je suis employé, je démissionne de ma fonction d'administrateur, je travaille pour un client, je termine ma mission, je deviens directeur, je suis renvoyé, mon mandat expire, etc. On peut déjà remarquer que ceux qui auront légalement l'autorité de me nommer et révoquer dans chacune de ces attributions ne peuvent se confondre avec un seul opérateur de PKI.

●

[49] Certes, on peut argumenter que le certificat m'est délivré par une entreprise dans laquelle j'ai une fonction et qu'il est logique de me retirer cette fonction quand je suis renvoyé. Mais alors, j'aurais autant de certificats que de pluralités à mon identité ! Et puis, lequel de ces certificats serait alors ma véritable identité dans ce qu'elle a d'unique ?
[50] En ce sens que l'on pourra se faire passer pour elle, mais aussi accéder à toutes ses données historiques : son existence numérique.

4. MODÈLE ET DÉFINITIONS

Chaque fois que cela sera nécessaire, nous utiliserons une majuscule pour distinguer un terme défini par notre modèle de ses autres usages. Par exemple, nous avons l'Identification telle que nous la définissons ici, et l'identification dans les usages multiples que ce terme revêt par ailleurs (cf. point 4.4).

81. Une taxonomie est indispensable, et nous avons déjà le matériel nécessaire à l'ébauche d'un modèle.

82. Il y a beaucoup de contraintes juridiques, fonctionnelles, et techniques à énoncer. Plutôt que de tenter un inventaire exhaustif, lui-même précédé d'un abondant catalogue de définitions, il nous apparaît beaucoup plus efficace de proposer un modèle de référence :

- Qui permette de visualiser chaque définition ;
- De localiser et comprendre chaque contrainte ;
- De convertir les principes de Droit en exigences fonctionnelles ;
- Aux spécialistes des technologies de l'information, de disposer d'un modèle conceptuel conforme au Droit, et de le dériver ensuite en modèle logique puis physique pour une mise en œuvre ;
- Ou d'évaluer méthodiquement en quoi un système existant ne serait pas conforme au Droit.

4.1 Ebauche

83. Le plan de départ contient cinq éléments qui s'imposent par eux-mêmes :

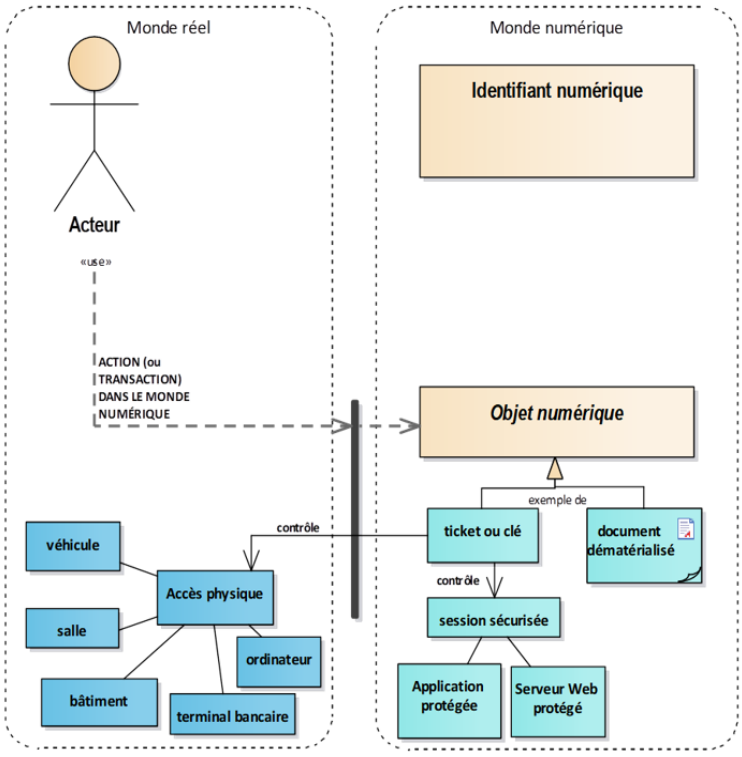
- Le monde réel ;
- Le monde numérique ;
- L'entité du monde réel[51], dotée d'une personnalité juridique ; on peut donc parler de la personne
- L'Identifiant numérique de cette entité/personne, conséquence des discussions qui précèdent ;
- L'Objet dans le monde numérique sur lequel l'entité de départ souhaite porter son action.

84. L'entité du monde réel, celle qui agit sur l'objet numérique, est par définition l'Acteur tel que représenté à la figure ci-contre.

85. L'Objet de son action est très général : il couvre autant la marque de l'identité sur une transaction ou un document, que l'exercice de l'accès à une application ou des données, ainsi que l'exécution d'une opération (calcul, ajout ou modification de données) dans le monde numérique.

L'Objet est donc représenté dans le monde numérique bien que l'action déclenchée puisse avoir des effets dans le monde réel. Les exemples d'objets numériques présentés dans la figure ci-dessous sous l'Objet numérique et leurs artefacts dans le monde réel ne sont aucunement exhaustifs.

86. La barre noire verticale au travers de laquelle s'exerce l'action de l'Acteur sur l'Objet numérique ainsi que le retour éventuel d'effets de l'objet numérique sur le monde réel représente l'Interface homme-machine et/ou l'interface applicatif (clavier, souris, écran, capteurs, moteurs électriques, boutons, interrupteurs, antenne, etc.).

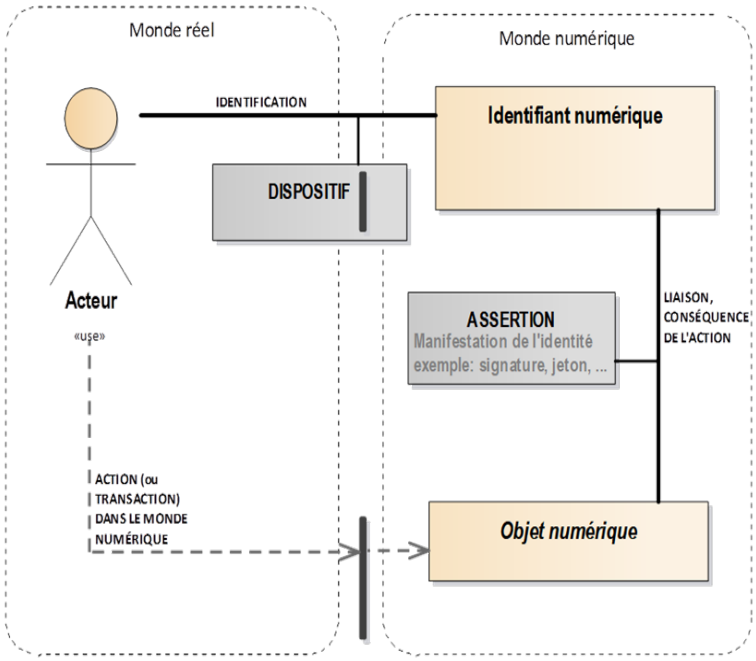


[51] Le cas des entités n'existant que dans le monde numérique sera résolu par la suite.

87. L'Identification désigne alors l'association entre l'Acteur et son Identifiant numérique, telle que représentée par la ligne horizontale du diagramme en figure ci-dessous.

88. Cette association traverse la barrière entre le monde réel et le monde numérique. Elle est par nature éphémère et doit donc obligatoirement s'accompagner d'un Dispositif de support d'une Interface apte à renouveler et re-valider cette liaison entre l'Acteur dans le monde réel et son Identifiant dans le monde numérique, et ceci chaque fois que l'avatar de notre Acteur dans le monde numérique, à savoir son Identifiant, est utilisé.

89. En d'autres termes c'est, par définition, le Dispositif – généralement composé de plusieurs éléments — qui rend un Acteur maître de son Identifiant numérique. Et puisque l'Acteur et l'Identifiant sont dans des mondes différents, il y a forcément une Interface.



90. Sans se prononcer à ce stade sur leurs qualités respectives en regard du Droit, voici 4 exemples

91. Exemple 1 :

- Acteur : moi
- Dispositif : carte à puce et lecteur biométrique
- Identifiant : données numériques scellées dans la carte à puce
- Objet Numérique : un document sur lequel je souhaite apposer ma signature

92. Exemple 2 :

- Acteur : moi
- Dispositif : le clavier de mon ordinateur et le composant logiciel de gestion des accès (par login ID + mot de passe) d'un serveur de courrier électronique
- Identifiant : mon adresse e-mail
- Objet Numérique : l'application de consultation de mon courriel Internet

93. Exemple 3 :

- Acteur : moi
- Dispositif : un terminal de paiement et ma carte bancaire
- Identifiant : mon N° de compte
- Objet Numérique : un ordre de paiement

94. Exemple 4 :

- Acteur : moi
- Dispositif : le clavier de mon ordinateur, mon téléphone mobile équipé d'une application de génération de codes à usage unique, une application web d'authentification à 2 facteurs, et un serveur d'identification distant avec sa base de données d'utilisateurs.
- Identifiant : un numéro d'utilisateur
- Objet Numérique : une assertion SAML[52] qui me donnera accès à un espace de partage de documents dans une application de gestion documentaire.

.

[52] SAML (Security Assertion Markup Language) est une norme éditée par le consortium industriel OASIS qui définit le contenu de messages cryptés permettant à un fournisseur d'identité (IdP – Identity Provider) de transmettre les informations d'autorisation aux fournisseurs de services (SP – Service Provider). Concrètement, lorsqu'un utilisateur U essaye d'accéder à une application A, celle-ci s'adresse en retour à une application X spécialisée dans l'identification (ou seulement l'authentification) des utilisateurs. Si cette dernière constate que votre précédente identification n'est plus active, elle vous redemande de présenter votre mot de passe, ou code généré par votre téléphone mobile, ou des données scellées dans une clé USB ou une carte à puce, ou encore votre image faciale ou empreinte digitale (bref, tout le processus que cette dernière a décidé de mettre en œuvre pour vous identifier/authentifier) et, vérification faite, entreprend de construire un message SAML avec votre identifiant, une indication de la vérification positive, et parfois la liste de vos droits d'accès, le tout scellé par cryptographie entre X et A. L'application d'identification X transmet ce message à l'application A de départ qui valide les propriétés cryptographiques, décode le contenu, et ouvre l'accès demandé à A par l'utilisateur U. Au cas où la précédente identification de U auprès de X était encore active, l'application d'identification X dispense l'utilisateur de tout ce tralala et génère directement le message SAML ad hoc. L'utilisateur a le confort d'accéder directement à A sans être (ré) identifié. S'il essaye ensuite d'accéder à une autre application B, il peut également être dispensé du tralala précité, c'est le système du Single Sign On (SSO).

95. Certes, il existe une infinité de variantes, de standards, de mécanismes, d'objets numériques et de technologies associées. Mais on peut à chaque fois déterminer l'Acteur, le Dispositif, l'Identifiant, et l'Objet numérique ciblé par l'action ou la transaction en question.

96. On comprend immédiatement tous les enjeux et la difficulté de cette liaison Acteur-Identifiant pour qu'elle soit unique, irrévocable, et assure le contrôle exclusif de l'exercice de son Identifiant par l'Acteur, car elle doit traverser la frontière entre le monde physique et le monde numérique, autrement dit entre le matériel et le virtuel.

97. On reviendra sur les contraintes de Droit applicables au chapitre 5, point 5.1 sur le régime de la preuve.

98. On remarque dans le modèle figure § 89 une association verticale : la liaison entre l'Identifiant et l'Objet numérique. Cette liaison exprime, dans le monde numérique la relation indirecte[53] entre l'Acteur et l'Objet de son action.

99. N'existant que dans le monde numérique, cette association s'exprime par une Assertion, à savoir une affirmation numérique[54] de la relation entre l'Identifiant et l'Objet. L'assertion est l'équivalent d'un écrit, ici dans le monde numérique.

100. L'association verticale de ce diagramme incarne la volonté de l'Acteur vis-à-vis de l'Objet numérique à un instant précis, qu'il s'agisse du jeton d'accès à une application sécurisée, de la marque de son consentement sur un document (signature électronique) ou encore de l'émission d'un ordre de paiement (Objet) depuis son compte (Identifiant).

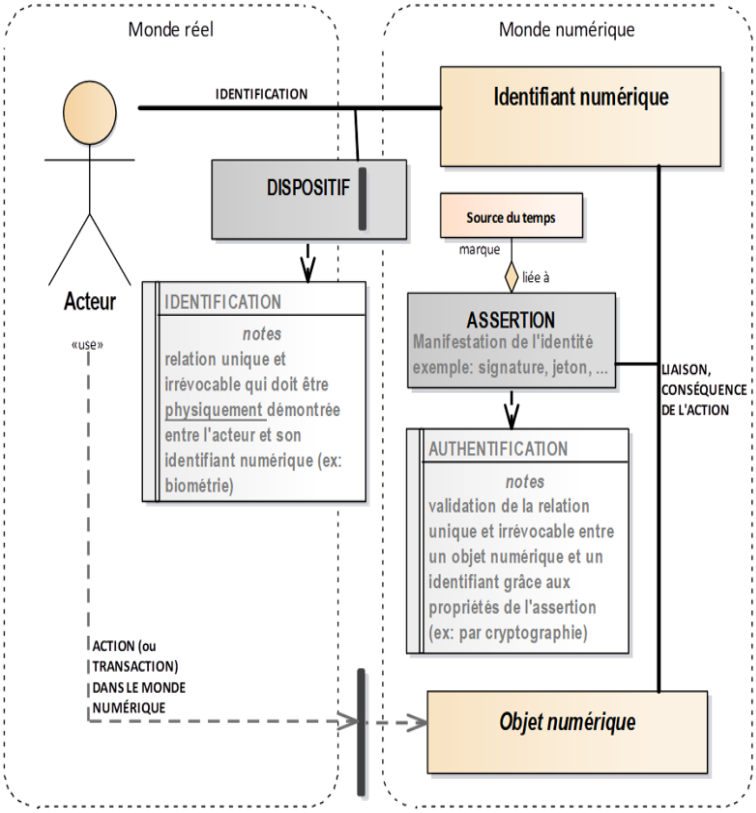
101. Exemples pratiques d'Assertions :

- Un état mémoire éphémère (cookie) tel que le contexte de session[55] entre votre navigateur et l'application Web auprès de laquelle vous vous êtes identifié.
- Une signature électronique conforme au standard « PAdES »[56] sur un document au format PDF tel que prescrit par le règlement d'exécution eIDAS.
- Les informations de validation jointes à l'ordre électronique de paiement émis par le terminal du commerçant à destination de l'opérateur de paiement.
- Les informations de validation de votre identifiant à l'intérieur d'un message SAML, un objet numérique déjà évoqué qui sert de jeton d'accès à une application informatique.

102. A l'instar de l'Identification qui revalide la liaison Acteur–Identifiant à chaque opération (action ou trans'action) exécutée par l'Acteur, l'Authentification est l'opération qui consiste à valider une Assertion.[57]

103. Par une ellipse qui assimile l'identifiant à l'acteur, l'authentification est souvent confondue avec une identification.[58] Si notre Authentification valide bien la liaison entre un Objet et un Identifiant, on comprend clairement avec ce modèle qu'elle ne connaît pas l'Acteur derrière l'Identifiant.

104. On peut donc ici Identifier sans Authentifier, et (hélas dans la plupart des systèmes actuels) Authentifier sans Identifier.



[53] Directe entre l'Identifiant et l'Objet, indirecte (via l'identifiant) entre l'Acteur et l'Objet.
[54] On parle ici de structures de données voire un message électronique structuré désignant ou contenant l'objet numérique, l'identifiant, et généralement une date, le tout scellé le plus souvent grâce à la cryptographie de façon à pouvoir valider à posteriori l'association ainsi «écrite» dans ces données.
[55] On parle souvent de cookies dans le cas des serveurs Web. Ceux-ci sont de petits paquets de données, parfois cryptées, échangées à chaque requête entre votre navigateur Web et l'application en ligne. Ces cookies sont soit « anonymes » (en théorie !) avec le seul but de tracer vos accès répétés au site sur base d'un identifiant généré par le serveur, soit contiennent en plus des données qui véhiculent l'identifiant qui vous a été assigné (login ID) et l'indicateur de votre entrée en session réussie (par ex. avec login ID et mot de passe).
[56] PAdES : PDF Advanced Electronic Signature, un ensemble de standards publiés par l'ETSI (European Telecommunications Standards Institute), voir la documentation « EU eSignature » : https ://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Standards+and+specifications
[57] Attention : ceci est la taxonomie utilisée dans le présent document. Elle est loin de faire universellement école. Pour les variantes de sens, cf. point 4.4.
[58] Cf. point 4.4.

105. Alors que l'on comprend facilement la fragilité de la liaison Acteur-Identifiant qui doit franchir la barrière physique-numérique, il en va tout autrement dans le monde numérique où se trouve entièrement la liaison Identifiant-Objet : les techniques cryptographiques permettent depuis longtemps de construire des Assertions robustes et irrévocables.

106. Cela met-il la partie droite du modèle à l'abri de toute turpitude ?

107. Hélas non : il faut en premier garantir l'autonomie et la pérennité des assertions[59] pour, par exemple, bénéficier juridiquement et dans le temps de l'opposabilité aux tiers. Sauf mesures particulières (comme une « blockchain », mais pas seulement), il reste possible dans le monde numérique d'effacer toute trace d'une assertion si cela sert les intérêts de son auteur et de ses complices éventuels… ou d'invoquer la fabrication d'un faux quand les mécanismes de calcul des Assertions sont faciles à retourner.

108. De plus, la marque du temps compte dans la validité d'une assertion, et les sources de temps utilisées pour fabriquer une assertion sont trop souvent falsifiables, voire sous contrôle direct de l'auteur (comme l'horloge de son ordinateur personnel).

4.2 Modèles emboîtés

109. La valeur juridique d'un acte est liée au régime de la preuve[60]. Le modèle met clairement en évidence la nature et les fragilités de chacune des 2 liaisons nécessaires à un acte juridiquement opposable aux tiers, à savoir dont il est possible d'apporter la preuve indépendamment des affirmations de l'intéressé conformément au principe de Droit : « Nul ne peut se constituer de titre à soi-même ».[61]

110. Cette démonstration peut vite devenir complexe, car notre modèle peut s'emboîter sur plusieurs niveaux comme des poupées russes au travers d'une hiérarchie de Dispositifs. Et c'est très souvent le cas en pratique.

111. Prenons l'exemple des « authentifications à double facteur » (2FA – « Two-Factor Authentication ») de plus en plus répandues.

112. Avec une application ad hoc, votre smartphone se transforme en Dispositif d'identification dont la liaison à l'Acteur n'est garantie que par le caractère personnel de ce téléphone. Au passage, protéger son téléphone avec un PIN code (ou un parcours de points sur l'écran, ou le lecteur d'empreinte digitale intégré) n'est plus une option, même si la robustesse de ces mécanismes est toute relative (piratage technique ou phishing).

113. On a donc un premier Dispositif – avec ses qualités et ses défauts – visant l'activation du téléphone (Objet numérique) par l'Acteur qui le tient en main, et l'Assertion : « j'en suis le propriétaire ».

114. L'Acteur peut alors lancer l'« appli 2FA » (2ème Dispositif) sur son téléphone qui lui demandera de se ré-identifier (autre PIN code? reconnaissance faciale? etc.) avant de lui délivrer un code à usage unique (Assertion : « c'est moi, c'est mon téléphone et c'est maintenant ») permettant à notre Acteur de confirmer (facteur 2 du « 2FA ») un processus d'identification déjà amorcé « en ligne » auprès d'une application Web typiquement avec login ID et mot de passe (facteur 1 du « 2FA ») via un 3ème dispositif, composé de votre navigateur Internet et du sous-système d'identification utilisé par l'application distante qui va authentifier le code unique.

115. Le 3ème Dispositif intègre le 2ème qui lui-même dépend du premier.

116. C'est clairement très complexe. Déjà techniquement, mais encore plus juridiquement. En effet, en cas de fraude ou de simple défaillance, quelles sont les responsabilités du fabricant du téléphone ?… de l'éditeur de l'application 2FA ?… du fournisseur du sous-système d'identification utilisé par l'application distante ?… des opérateurs des réseaux de communication ?… du prestataire de service de l'application que vous avez (ou n'avez pas !) accédé ?… et des hébergeurs de tous les composants impliqués ?

117. La réponse rapide est que tous ces intervenants se déchargent aujourd'hui de toute responsabilité en se rangeant derrière une obligation de moyens et que le règlement eIDAS malgré les espoirs suscités n'a rien pu faire d'autre que de promouvoir l'interopérabilité des « moyens » (les Dispositifs) et sélectionner des standards existants (des « moyens » également) pour la reconnaissance mutuelle des Assertions.

118. ⚠ On comprend déjà que pour fabriquer des preuves, il va falloir revenir à des dispositifs beaucoup plus simples, compacts, et surtout autonomes… sans compromis sur la sécurité.[62]

[59] Cf. Chapitre 5
[60] Cf. Chapitre 5, point 5.1.
[61] Code civil, art. 1363.
[62] Cf. Chapitre 6, points 6.1 et 6.2 sur les Dispositifs compacts et biométriques.

4.3 Composition d'un Identifiant

119. Question importante : l'Identifiant peut-il être quelconque ?

120. Le Droit apporte la réponse.

121. Nous avons déjà évoqué la multiplicité des formes : l'identité est unique en droit, mais multiple en usages. Dans le monde des entreprises l'Acteur agit rarement pour son propre compte. Qu'il soit employé, directeur, administrateur, représentant, agent ou membre d'une profession réglementée (médecin, notaire, avocat, auditeur, etc.), cet Acteur agit au nom d'une entité tierce, le plus souvent personne morale (entreprise, État, organisme), ou communauté professionnelle :

⚠ Nous appelons **Communauté** tout regroupement d'individus (les membres de cette communauté) généralement doté d'une personnalité juridique, mais dans tous les cas rattaché à un système de Droit, ou autrement dit une juridiction. La notion de Communauté désigne ainsi toute forme d'entreprise industrielle, d'institut, d'administration, d'association, ou de groupement d'intérêt ainsi que les entités souveraines comme les États ou des subdivisions de celui-ci comme les régions.

⚠ Nous appelons **Fonction** le rôle – assorti de droits et d'obligations exercé par un membre de cette Communauté au sein de celle-ci et/ou pour le compte de celle-ci, tel qu'il lui a été attribué par un tiers (et non par lui-même) dûment mandaté par cette Communauté.

122. Cette capacité à exercer une Fonction pour le compte d'un tiers prend encore plus de sens lorsque l'entité (l'Acteur) n'est pas une personne physique, mais une personne morale : comme la personne physique, la personne morale dispose de la personnalité juridique ; on peut la poursuivre en justice. On ne peut donc pas interdire à une personne morale d'exister (et donc d'être proprement identifiable et justiciable) dans le monde numérique, mais on ne peut pas non plus laisser son/ses identifiants « flotter » sans contrôle par l'absence de tout dispositif d'identification.

123. Le Droit dit clairement que tous les représentants et mandataires (employé, directeur, etc.) agissant pour le compte d'une personne morale (agissant au travers d'une fonction, d'un mandat, ou de statuts), engagent la responsabilité de cette dernière. C'est donc par le Dispositif d'un de ses représentants ou mandataires que notre personne morale va pouvoir s'identifier, et agir légalement.

124. Le cas des robots est aussi pertinent : ils ont clairement une capacité à agir sur le monde réel, mais qu'en est-il de leur personnalité juridique[63] ?

125. Si ce robot s'identifie comme agissant pour le compte d'un tiers, personne physique ou morale, il hérite alors de la personnalité juridique de ce dernier et devient une entité légalement imputable de ses actes tant dans le monde réel que numérique.

126. Dans ce monde numérique, un algorithme doté d'intelligence artificielle devient justiciable si on le dote d'une identité en tant que mandataire d'une personne physique ou morale, telle qu'une IA autonome qui délivre un diagnostic automatisé pour plusieurs hôpitaux et qui sera assurée tel un médecin.

127. Un véhicule autonome correctement identifié et mandaté par un opérateur de transport rend ce dernier responsable des accidents dudit véhicule.

128. Le Droit permettra d'encadrer sereinement les investigations pour autant que les entités participantes (physique, morale, robot) soient identifiées irrévocablement[64], que leurs actions soient tracées (conservation des assertions / journalisation[65], et que ces identités soient qualifiées comme expliqué ci-après. (167 à 173).

129. La figure § 131 généralise tous les types d'entités identifiables sur base des combinaisons entre personnalité juridique et capacité à agir. Clairement, les objets non-autonomes de la colonne de gauche n'ont besoin d'aucune identification. Ils tombent dans la catégorie des biens mobiliers. Ce sera aussi le cas de la très grande majorité des robots dont l'action est déterministe et invariable en fonction de l'expérience.

130. Le modèle est flexible : si l'on est sensible aux dérives de la « techno-personnalisation »[66] une communauté qui emploie des robots dotés d'une IA pourrait décider de tous les garder dans la catégorie des biens mobiliers, ou au contraire les doter d'une personnalité juridique et d'un identifiant numérique ad hoc, on encore créer une catégorie « à part » dans le cadre du système de Droit dont cette Communauté souveraine se dote, et/ou hérite.

---

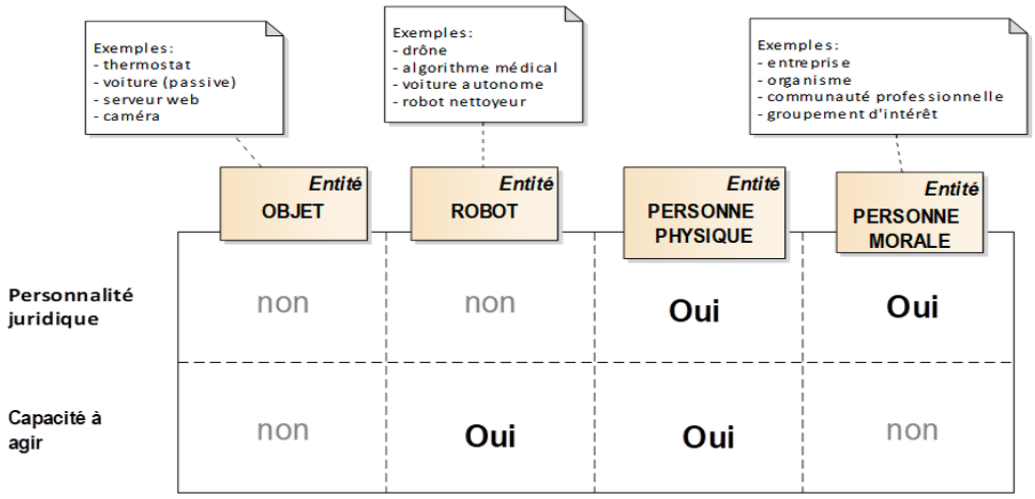
[63] Pour une discussion approfondie de la question : «IA, robots et droits» (Bensoussan & Bensoussan, 2019)

[64] Il ne faudra pas verser dans une multiplication inutile et vide de sens des identifications numériques, comme d'en assigner une à un moteur d'avion, ou la roue d'une voiture. Toute défaillance de ces objets asd'identité : la nature des biens mobiliers est parfaitement encadrée par le Droit et s'applique d'ailleurs aux animaux et actuellement aux robots, pour la grande majorité desquels cela ne pose aucun problème ; seuls les robots dotés d'une IA capables d'une autonomie de décision basée sur leur propre 'expérience' en tant que robots posent la question d'une personnalité juridique tant pour les protéger que les imputer.

[65] Cf. Chapitre 5, point 5.4

[66] Cf. ci-dessus 61

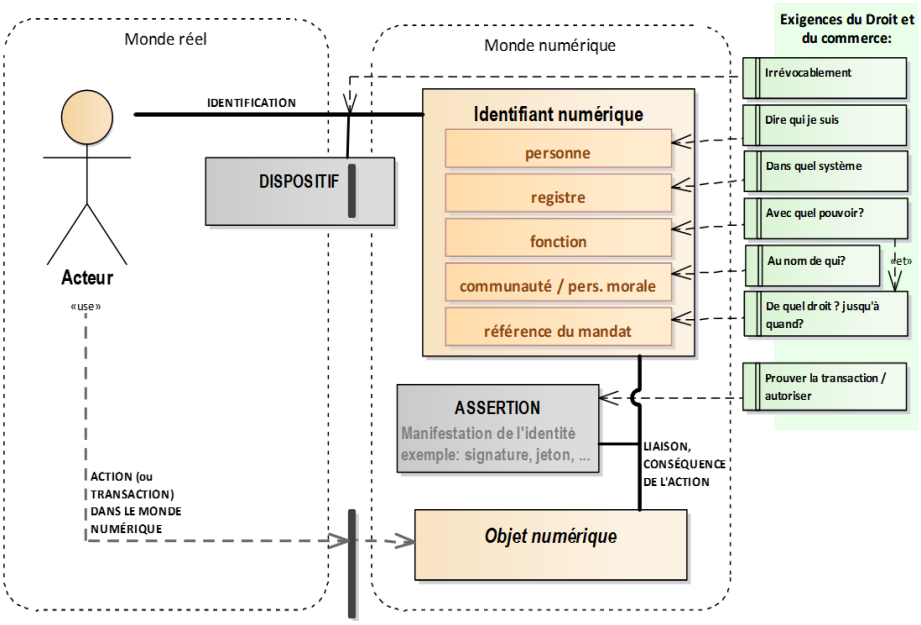
131. Enfin le cas des personnes physiques et morales est évident : leur personnalité juridique intrinsèque appelle à la création d'identifiants numériques capables de porter celle-ci.



132. « Nul ne peut se constituer de titre à soi-même »[67] en conséquence de quoi toute Fonction émane d'un Mandat qui donc attribue une Fonction à une Personne dans le cadre d'une Communauté dont la référence doit faire partie de l'identifiant numérique. En effet :

- Un Mandat a son propre cycle de vie : il a souvent une date limite, il peut être renouvelé, voir abrogé anticipativement.
- Alors que la Fonction est essentiellement un titre, son contenu (prérogatives, limites, droits, obligations) est déterminé par le Mandat. La Fonction peut rester identique dans son assignation, mais évoluer dans son contenu avec le renouvellement des Mandats.
- Alors que les 4 autres éléments de notre identifiant numérique (personne, registre, fonction, communauté) sont essentiellement déclaratifs, c'est le Mandat qui donne à l'ensemble une valeur juridique.
- En réalité, on pourrait se contenter de la seule référence unique à un mandat en guise d'identifiant numérique complet ; mais les exigences d'exploitation, ainsi que la capacité à éviter tout fichier central de données à caractère personnel invite à joindre les 4 premiers éléments à notre identifiant numérique.

133. ⚠ Cet identifiant numérique à 5 éléments est représenté à la figure ci-dessous. Il supporte par construction une identification de la Personne ès qualités.



[67] Cf. ci-dessus 109.

134. A droite de la figure § 133 sont illustrées les exigences qui couvrent tant la composition d'un identifiant numérique que sa relation à l'Acteur (association horizontale) et l'Objet (association verticale) de son action.

135. Que se passe-t-il alors lorsque j'agis en mon nom propre ? Il n'y a pas de mandat ? Si : l'officier d'état civil qui a enrôlé mon identité civile en tant que citoyen d'un pays, avec des droits et des obligations. Certes, on parle ici d'identité numérique : il y aura donc une Communauté (numérique elle aussi qui pourrait être la « France numérique » autant que par exemple un syndicat de Huissiers de Justice) au sein de laquelle ma première identité numérique sera assignée.

136. Supposons que je sois employé au cabinet d'un huissier, ce dernier étant également officier d'état civil pourrait dans le même élan enrôler ma Fonction d'employé à son service en même temps que ma Fonction « en mon nom propre » rattachée à mon identité civile.

137. En revanche, si ma première identité numérique m'est attribuée par le directeur des ressources humaines d'une entreprise industrielle, je pourrais décider d'adjoindre ultérieurement ma Fonction « en mon nom propre » en me rendant chez un enrôleur dûment habilité à confirmer mon identité civile. Ou encore : pourquoi le directeur des ressources humaines ne pourrait-il être habilité à vérifier mon identité civile, ce qui est également dans son intérêt ? Toute identité numérique dans ce modèle dispose de la référence obligatoire à un mandat, la Fonction « en mon nom propre » n'y échappe pas.

138. Un mandat, c'est un document, Objet Numérique, avec au minimum la signature de l'enrôleur (assertion irrévocable de son engagement sur le déroulement de l'enrôlement) et celle de l'enrôlé (assertion irrévocable de son consentement sur la Fonction attribuée), nouant ainsi toutes les exigences juridiques d'une identité ès qualités, et permettant aussi de poursuivre toute fraude à l'identification.

139. Dans la suite de notre appel[68] à découpler les identités numériques des mécanismes de sécurité destinées à les protéger (ex. un certificat cryptographique). Il faut alors comprendre que la sécurité d'une identité numérique doit être attachée au cycle de vie du Mandat, celui-ci étant révocable et renouvelable sans remettre en cause la Fonction de la personne. C'est une évidence !

140. Nous pouvons alors aller encore plus loin en faisant coexister des identités numériques certifiées avec Mandat, avec d'autres non certifiées (et sans recours juridiques) sans Mandat, quitte à les faire certifier ultérieurement. Certes, ces identités numériques seraient aussi protégées avec un niveau de sécurité adéquat, mais à la différence des identités formellement attribuées par Mandat, l'utilisateur prend la responsabilité entière[69] de la sécurité de ses identités auto-attribuées. Celles-ci sont par construction dénuées de tout recours juridique, ne pouvant prouver l'identité réelle des Acteurs.

141. Le champ des possibles devient colossal, et il appartiendra aux Communautés de déterminer souverainement leurs applications et leurs limites.

142. Toutes les exigences juridiques qui suivent[70] viendront renforcer ce modèle.

143. Certes, on pourrait argumenter qu'il suffit d'enfermer cette proposition d'identification numérique dans un certificat cryptographique pour en revenir à la pratique des PKI. Grave erreur ! La multiplicité des fonctions pour une même personne, multipliée par le cycle de vie propre des Fonctions, multipliée par celui des Mandats, viendra télescoper le cycle de vie propre aux certificats cryptographiques pour aboutir à un magma ingérable pour les PKI.

144. La solution développée ci-après est beaucoup plus simple, robuste, et transparente.

4.4 Identifier versus authentifier

145. S'il y a bien deux termes dont la sémantique varie fortement, ce sont ceux-là.

146. Si l'on part d'une définition « stricto sensu »[71] de l'authentification en tant qu'opération qui valide la correspondance entre une observation et une proposition relative à cette observation, l'identification serait la proposition (« cette personne est liée à cet objet numérique »[72]) qui fait l'objet de cette validation. Dans notre modèle, la proposition se réduit à « cet identifiant est lié à cet objet numérique » et le chemin de l'identifiant du monde numérique à l'individu du monde réel (l'Identification de notre modèle) reste hors de portée.

[68] Cf. ci-dessus 76.

[69] Toutefois contraint par les procédures, mécanismes, et polices de sécurité que la Communauté qui accepte ces auto-attributions choisirait de mettre en place dans le cadre de sa souveraineté.

[70] Cf. chapitre 5 sur le Cadre Juridique.

[71] Ce n'est pas celles que l'on trouve dans les dictionnaires. Le Littré ne connaît pas ce mot récent, le Larousse est direct : « Processus par lequel un système informatique s'assure de l'identité d'un utilisateur ». Le Robert empile les définitions : « action d'authentifier » -> « […] reconnaître comme authentique » -> « Qui est véritablement de l'auteur auquel on l'attribue. / Dont l'autorité, la réalité, la vérité ne peut être contestée. / […] ». Le lexique Dalloz s'en tient à la certification conforme des « actes authentiques ».

[72] Ce qui peut être aisément prouvé par de la cryptographie.

147. Pour les auteurs du rapport de l'Assemblée Nationale[73], l'identification n'a lieu que lorsque que l'on remonte à l'identité civile et donc aux registres de l'État. Elle est établie par l'acte d'enrôlement et confère une qualité persistante à l'identifiant ainsi enrôlé, cet identifiant étant précisément ce que les auteurs dénomment l'« identité pivot », à savoir la base de son identité civile : nom, prénoms, date et lieu de naissance, sexe.

148. La maîtrise de la personne sur cet identifiant passe par exemple par la reconnaissance faciale (ALICEM), et lorsque cette dernière est une opération purement locale (le GSM compare l'image de la personne à un masque localement enregistré), on continue à parler d'authentification mais pas d'identification. L'authentification est alors la partie dynamique : apporter la preuve (sic) de son identité numérique lors d'un acte dans le monde numérique grâce à divers moyens dont il est admis que le niveau de sécurité peut varier... ce qui - on notera au passage - se pose en contradiction avec la notion stricte de preuve : une preuve est établie ou pas, sans gradation aucune.

149. Pour d'autres auteurs, toute distinction entre identification et authentification n'a aucun sens : elle entretient la confusion sachant que l'une ne peut aller sans l'autre sauf à introduire le doute. Ce sont deux facettes indissociables d'une seule opération : celle de prouver qui est la personne derrière un acte dématérialisé.

150. Dans cette acception, l'authentification est la mise en œuvre de l'identification. L'identification est la finalité des opérations d'authentification ; les termes sont donc interchangeables selon que l'on veuille mettre en avant les moyens (authentification) ou l'objectif (identification).

151. En ce qui concerne le présent document, aux fins de construire une identité numérique 5.0, nous devons distinguer clairement 2 notions :

- La capacité d'une personne à garder le contrôle exclusif de son identifiant numérique, et donc indiquer irrévocablement que toute trace[74] de son identifiant sur un acte numérique quelconque émane de sa volonté[75], voire de son consentement explicite au moment de l'acte[76] ou en amont de celui-ci, et ne peut donc résulter ni d'un usage accidentel, ni abusif.

Il s'agit d'une opération dynamique qui consiste à prouver la liaison entre la personne et son identifiant numérique à chaque usage de ce dernier (ou en amont d'une série [77]) sur un support numérique.

- La capacité à prouver la liaison entre un identifiant numérique et un objet numérique (document dématérialisé, journal d'activités, transaction, autorisation, certification, propriété intellectuelle, industrielle, ou commerciale sur des avoirs immatériels ou dématérialisés, etc.). Cette preuve doit évidemment être persistante. Sa construction et ses vérifications ultérieures[78] s'exécutent dans le monde numérique avec des moyens qui, par construction, doivent exclure toute falsification et détournement. Cela implique aujourd'hui quasi systématiquement le recours à la cryptographie appliquée.[79]

152. A défaut d'inventer de nouveaux termes, nous parlons d'identification dans le premier cas, et d'authentification dans le second. Cet usage est simple (personne <Identification> identifiant numérique <Authentification> objet/support numérique) et approprié à notre contexte (cf. le modèle proposé). Il est surtout pertinent comme il sera démontré par la suite.

153. En termes simples, Authentifier c'est valider qui on prétend être, Identifier c'est valider qui on est.

154. Les définitions données au § 151 ne sont incompatibles ni avec celles visées aux § 149 et § 150. En effet, si la maîtrise d'une personne sur son identifiant n'est pas sûre, on ne peut parler d'Identification au sens défini au § 151 1°. D'autre part, il ne peut y avoir de preuve que si l'on a répondu aux conditions énumérées au § 151 : Identifier implique de pouvoir (ré)Authentifier à postériori ; Authentifier implique d'avoir Identifié sauf à introduire le doute, et donc invalider l'authentification au sens de § 146 ou § 148.

155. Il est clair que pour démontrer la liaison entre une personne et un objet/support numérique, on ne peut dissocier identification et authentification. C'est pour cela que dans le langage courant on assimile souvent une opération d'authentification à une identification.

---

[73] Mission d'information de l'Assemblée sur l'identité numérique, Rapport Ass. Nat. N° 3190, 8 juillet 2020.
[74] On utilise le terme plus précis d'assertion dans notre modèle, cf. point 4.1.
[75] Dans le cas de traces multiples comme l'historique des sites Web visités par la personne, ou l'historique de son GPS, il faut comprendre la trace comme faisant référence au groupe de traces élémentaires de même nature, et la volonté de la personne par rapport à ce groupe.
[76] Cas de la signature électronique.
[77] Cf. note 75.
[78] Autant de fois que nécessaire à l'exercice des droits et obligations qui découlent de cette liaison.
[79] On ne souhaite pas exclure les microfiches digitales, les disques optiques dans une certaine mesure, ni des technologies futures comme la micro-gravure en 3 dimensions dans des blocs de quartz. Les blockchains sont aussi de la cryptographie appliquée.

156. Identifier sans Authentifier a peu de sens[80], mais Authentifier sans Identifier est hélas l'apanage actuel de l'Internet. L'identité numérique telle qu'utilisée à ce jour est plus souvent le résultat d'une auto déclaration, assortie d'un moyen extrinsèque de démonstration comme un « nom d'usage » doublé d'un mot de passe, et parfois d'une abondance de mesures de sécurité comme l'identification à deux facteurs (2FA).

157. Or si l'on peut réduire le risque d'usage abusif d'un compte en ligne, et donc améliorer la qualité de l'authentification, on n'a toujours pas démontré qui était vraiment la personne derrière l'identifiant qu'elle s'est auto-attribué. Pour être recevable et de surcroît opposable aux tiers, l'utilisateur doit être en mesure de prouver son identité selon des moyens intrinsèques sous sa seule maîtrise ; comme il sera expliqué, une identité digne de ce nom[81] doit être irrévocable, ce qui implique la preuve de l'Identification autant que de l'Authentification.

158. L'irrévocabilité implique de conserver les traces à l'abri de toute turpitude, car quoi de technologiquement plus facile dans le monde numérique que d'altérer ou effacer des données ?[82] Cette question sera développée au chapitre 5, point 5.4 sur l'archivage des moyens de preuve.

●

[80] Par exemple, reconnaître un tableau comme étant du Picasso sans être sûr qu'il soit vraiment de lui.
[81] Nul besoin ici de lui ajouter le qualificatif de numérique, c'est universel.
[82] Si les technologies 'blockchain' ont quelque intérêt ici, c'est bien pour journaliser de façon définitive et inaltérable toutes les traces des transactions sans recourir à un tiers de confiance omnipotent.

5. LE CADRE JURIDIQUE

Garantir la confidentialité et la valeur juridique des échanges numériques en identifiant de manière irrévocable les auteurs des contenus, les expéditeurs, les destinataires et tous les tiers autorisés à chaque étape critique, constitue un défi majeur.

159. Aucune industrie ne saurait s'exonérer du droit.

5.1 Le régime de la preuve

5.1.1 Le régime des obligations

160. Code civil :

- Article 1353 : « Celui qui réclame l'exécution d'une obligation doit la prouver. Réciproquement, celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation ».
- Article 1357 : « L'administration judiciaire de la preuve et les contestations qui s'y rapportent sont régies par le code de procédure civile ».

161. Code de procédure civile :

- Article 9 : « Il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention ».
- Article 146 : « Une mesure d'instruction ne peut être ordonnée sur un fait que si la partie qui l'allègue ne dispose pas d'éléments suffisants pour le prouver. En aucun cas une mesure d'instruction ne peut être ordonnée en vue de suppléer la carence de la partie dans l'administration de la preuve ».

162. ⚠ Un problème apparaît avec l'identité numérique qui n'existait pas avec le papier : je suis concerné par la qualité « du bras et du stylo » de l'autre partie. Il ne suffit pas que je sois moi super équipé avec une super Identité numérique et un super Dispositif d'Identification irrévocable ; si la partie d'en face n'utilise qu'un moyen d'Identification faible, ou si plus simplement aucun tiers (aucun Mandat) ne vient confirmer que l'Identifiant numérique utilisé est bien le sien, je ne pourrai rien prouver.

163. ⚠ Le Mandat attaché à mon identité numérique n'est pas une option. Exemple : je signe avec une identité numérique « perso » parce que c'est la seule que j'ai – un document pour mon employeur, qui se désiste en antidatant au jour précédent une lettre de licenciement… là où le Mandat numérique aurait établi sans ambiguïté que j'agissais pour mon employeur, et que si il y avait eu révocation, la date de celle-ci aurait été certifiée par un prestataire tiers d'horodatage.

5.1.2 Le régime de la preuve parfaite

164. Faisant partie des preuves dites « parfaites »[83], la preuve par écrit s'impose au juge, sous réserve de sa conformité avec les textes qui la régissent, notamment :

165. Code civil :

- Article 1363 : « Nul ne peut se constituer de titre à soi-même ».

166. ⚠ Qui se risquera à utiliser une identité numérique seulement protégée par mot de passe ou PIN code dans des transactions importantes ? Soit elle est admise comme présomption irréfragable à titre de preuve, on m'a dérobé ce code, et je ne peux plus me désister ; soit ce n'est pas une preuve (c'est le cas !) et j'en suis également à mes dépens. Et toutes les disputes intermédiaires où je devrais tenter de convaincre que c'était moi, ou pas moi.

167. ⚠ Pas d'identité numérique sans un Mandat (tiers par nature) pour en confirmer l'attribution. Exemple : je m'auto-enrôle avec un super Dispositif. Je pourrais certes démontrer au juge que ce Dispositif est sous mon contrôle pour l'Identité numérique visée, mais qui prouve que je suis seul à avoir ce contrôle ?

168. Code civil :

- Article 1364 : « La preuve d'un acte juridique peut être préconstituée par un écrit en la forme authentique ou sous signature privée ».
- Article 1365 : « L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support ».

[83] Excluant par définition toute présomption..

169. ⚠ Il faut donc s'en tenir aux technologies (notamment cryptographiques) aptes à créer des Assertions infalsifiables et que celles-ci ne puissent disparaître avec le temps (de façon volontaire ou involontaire), à savoir la question de l'archivage, cf. point 5.4.

170. Code civil :

- Article 1366 : « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

171. ⚠ Il faut assurer par tous moyens utiles[84] l'irrévocabilité de la liaison Acteur Identifiant. Les Dispositifs doivent ainsi interdire toute possibilité d'usage par un tiers des identifiants d'un Acteur, même avec la complicité de ce dernier (comme de communiquer son PIN code). Toute centralisation des identifiants et, pire, des moyens de les exercer pose la question de leur usage abusif (potentiellement sans laisser de traces) en cas de violation de la sécurité informatique. Tout serveur central de signature électronique est donc banni.

172. ⚠ L'article réaffirme l'impérieuse nécessité d'assurer la pérennité des supports (assertions et objets numériques associés, cf. point 5.4), et des mécanismes de vérification de l'authenticité de ces supports ; prouver 30 ans plus tard que c'était bien Monsieur M qui avait manifesté son consentement à telle transaction, le contenu de cette transaction devant lui aussi rester intelligible.

173. Code civil :

- Article 1367 : « La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret[85] en Conseil d'Etat ».

174. ⚠ Cet article impose une manifestation explicite du consentement. Il ne saurait être question d'un clic ou de l'enfoncement d'une touche au clavier, mais d'une activité écartant toute confusion, captation inopinée, ou interprétation variable. En d'autres termes, le Dispositif retenu doit exiger un geste explicite et sans ambiguïté, émanant de l'Acteur et excluant toute répétition automatique ou implicite et tout autre intervenant. Ceci exclut clairement les clics autant que les SMS de confirmation.

175. De plus, il ne peut y avoir de consentement sans une facilité équivalente de renoncement comme jugé par la CJUE[86], et désormais clairement indiqué dans un document[87] précisant les termes du RGPD[88]. Le consentement n'est pas donné « en cas de silence, de cases cochées par défaut ou d'inactivité ».

5.2 Protection de la vie privée

176. « La masse de données collectées auprès des internautes (big data) constitue, on le sait, « le pétrole du XXIe siècle » dans la mesure où son exploitation permet de probabiliser – voire d'orienter – le comportement des consommateurs et des clients »[89].

5.2.1 Les données à caractère personnel

177. Selon le RGPD, constitue une donnée à caractère personnel « toute information se rapportant à une personne physique identifiée ou identifiable (…) ; est réputée être une « personne 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, génétique, psychique, économique, culturelle ou sociale »[90]. Cette définition est aussi celle adoptée par la CNIL.[91]

178. La loi Informatique et libertés modifiée reprend les définitions fixées par le RGPD et fait donc sienne celle de la donnée à caractère personnel.[92]

---

[84] Cf. Chapitre 6, point 6.2 sur la biométrie.
[85] Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, faisant référence au règlement eIDAS (UE 910/2014), lui-même suivi d'un règlement d'exécution (UE 2015/1502). Noter que le Décret n° 2010-112 du 2 février 2010 qui impose le RGS (Règlement Général de Sécurité, édité par l'ANSSI) continue à s'appliquer dans les échanges avec l'administration. Les différences sont minimes.
[86] Cour de justice de l'UE, 11 novembre 2020, C-61/19.
[87] Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 = RGPD
[88] Règlement UE 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données.
[89] Pauline Türk et Christian Vallar, La souveraineté numérique : Le concept, les enjeux, Ed. Mar & Martin 2018.
[90] Règl. 2016/679 du 27 04 2016, art. 4.
[91] www.cnil.fr/fr/definition/donnee-personnelle
[92] Loi 78/17 du 06 01 1978 relative à l'informatique, aux fichiers et aux libertés, art. 2.

179. La collecte et l'utilisation de ces données personnelles doivent s'opérer dans le respect des principes énoncés par le RGPD et bientôt, dans le respect de ceux qu'arrêtera le projet de règlement sur la protection des données à caractère personnel dans les communications électroniques, dit « e-privacy »[93], visant à compléter les dispositions du RGPD, actuellement en discussion au niveau européen.

180. L'identification d'une personne physique doit se faire dans le respect le plus strict de la protection de la sécurité et de la confidentialité des données à caractère personnel utilisées à cette fin dans le respect de la vie privée des individus et de leurs droits fondamentaux.

181. Dans le monde numérique, une personne laisse de très nombreuses traces de ses actions, voire de son simple passage. Si l'identité de cette personne doit être sans ambiguïté pour un petit nombre d'opérateurs (fournisseur de services) ou de correspondants de celle-ci aux fins des effets de Droit nécessaires à ses Actions, il est souhaitable qu'elle reste anonyme pour tous les autres intervenants indirectement impliqués (gestionnaires des infrastructures, opérateurs de télécommunication, éditeurs des logiciels intermédiaires, serveurs relais, capteurs de fréquentation, analyse des « clics », fournisseurs de publicité, etc.). La protection de la vie privée sera alors d'autant mieux assurée par l'usage d'identifiants numériques aussi anonymes que possible et sous le contrôle strict de la personne désignée.

182. ⚠ En d'autres termes, nous préconisons l'utilisation d'identifiants dénués de toute signification, en excluant donc un patronyme comme « Dupont », ou même une fonction comme « Directeur » et à plus forte raison tous les usages actuels des adresses de courrier électronique. A ce titre, un champ numérique binaire alloué de façon pseudo-aléatoire[94] est le meilleur identifiant, allié à la capacité de la personne d'utiliser plusieurs identifiants (on revient sur la multiplicité des usages [95]). Ainsi la personne peut entièrement contrôler les informations publiques qu'elle souhaite attacher à chaque identifiant au travers d'un annuaire, ou – selon les besoins en les incluant dans les enveloppes (en clair) ou le contenu (crypté) de ses échanges.

183. ⚠ On pourrait même préconiser le remplacement de moyens implicites d'identification (adresse IP, cookies corrélés par des sites multiples, profilage), par une identification explicite, mais anonyme, sous le contrôle de cette personne. On ne peut nier l'intérêt économique des analyses de marketing, voire même un apport positif à l'optimisation des ressources, ni l'intérêt potentiel pour les utilisateurs d'une personnalisation des services, mais pas à l'insu de la personne concernée.

184. On peut alors voir les Identifiants numériques plus comme des adresses, au même titre qu'un numéro de téléphone. Toutefois la structure exposée dans la figure § 133 avec l'élément désignant le Mandat s'impose ici, ce qui, avec la Fonction associée, en fait un instrument d'identification bien plus pertinent qu'un numéro de téléphone même si ceux-ci, réduits à des numéros, restent anonymes.

5.2.2 L'usurpation d'identité

185. Le fournisseur de l'identité numérique doit protéger chacun contre l'usurpation d'identité. La loi « LOPPSI 2 »[96] sanctionne pénalement l'usurpation d'identité sur internet insérée dans le code pénal à l'article 226-4-1.

186. L'Internet a ceci de particulier que même si l'on peut poursuivre au pénal une usurpation d'identité, les dégâts éventuels en termes d'image ou de réputation peuvent être irréversibles vu l'impraticabilité du droit à l'oubli. Seul le droit au déréférencement est envisageable.

187. ⚠ L'Identité numérique telle que proposée[97] présente plusieurs avantages :

- A partir du moment où l'auto-attribution disparaît «pour tout ce qui compte», que la problématique de l'Identification est correctement traitée en regard des enjeux, et que des tiers mandatés par des communautés (personnes morales) et identifiables (judiciables) sont référencés par les identités attribuées, l'Identité numérique devient, par construction, beaucoup plus robuste.
- Elle instaure un système d'identités multiples et par nature cloisonnées aux communautés au sein desquelles elles ont été attribuées.
- Tout usage abusif ne pourra – par construction – cibler qu'un Mandat particulier, qu'il est possible de révoquer et renouveler.[98]

[93] Proposition de règlement sur la protection des données à caractère personnel dans les communications électroniques (e-privacy), Compromis du 18 septembre 2019.
[94] « Pseudo » aléatoire car il doit rester unique.
[95] Cf. 66 à 71.
[96] Loi 2011-267 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure, JORF du 15 mars 2011.87
[97] Cf. 133, figure § 133
[98] Cf. § 139.

5.2.3 Le secret des affaires et des correspondances

188. Pour un développement de cette question, voir Annexe 1 du présent livre blanc.

189. Il est évident que pour pouvoir ou non autoriser une personne à accéder à une information, il faut en premier lieu identifier cette personne, et donc disposer d'une identité numérique fiable.

190. L'identification proposée qui s'étend à la Fonction d'un individu au sein d'une Communauté vient clairement renforcer la qualité de l'identification nécessaire à la protection des avoirs immatériels des entreprises/personnes morales, elles-mêmes identifiables. De plus elle cloisonne mes fonctions : le cycle de vie d'une fonction A et les droits d'accès associés n'interfère pas sur l'accès aux documents que j'ai dans le cadre d'une fonction B.

5.3 La conclusion des contrats

191. Les articles 1112 à 1171 du Code civil sur la conclusion et la validité des contrats laissent totalement ouvert le champ de leur conclusion par la voie électronique. Le courrier électronique est nommément désigné, sans pour autant faire référence au courriel Internet et laissant ainsi la voie ouverte à tout système de même nature. Or, ces articles ajoutent une exigence supplémentaire à celle, évidente, de la qualité de l'identification des parties au contrat en cours de négociation : la capacité de savoir avec certitude si, et à quel moment, une partie a reçu (ou pas) une information de l'autre partie.

192. A cet égard, rappelons que le modèle proposé ne limite aucunement son champ d'application à la signature d'actes. L'acceptation formelle d'un échange (Objet numérique) peut ainsi être visée par une Assertion (j'accepte – ou je refuse[99] – un échange électronique) entre parties dûment identifiées.

193. Le fait d'introduire la Fonction, assortie d'un Mandat, dans les Identités numériques proposées vient clairement renforcer la qualité juridique des échanges des documents en permettant l'émission, mais aussi l'adressage dans le cadre strict des Mandats des personnes impliquées. La relation contractuelle entre personnes morales au travers de leurs mandataires (représentants, employés, administrateurs) retrouve tout son poids juridique ici aussi dans le monde numérique.

5.4 L'archivage des moyens de preuve

194. Nous avons déjà cité à de multiples reprises[100] la nécessité impérieuse de l'archivage des Assertions.

195. Une analyse très pertinente de la question est proposée par Lucien Pauliac[101]. L'auteur relève la contradiction de l'article 1379 du Code civil qui instaure la notion de «copie fiable» et le décret d'application 2016-1673[102] au sujet de la modification possible de la copie réputée «non modifiable» dans le cas où celle-ci est conservée sous forme électronique et nécessite des renouvellements techniques pour sa conservation dans le temps. La microforme argentique s'impose alors pour 3 raisons :

- La solution est éprouvée, et normalisée par l'AFNOR
- La preuve est ici irréfutable, et non modifiable par nature
- Elle offre une économie nette sur le coût (dépense énergétique, hébergement) de la préservation.

196. L'auteur conclut au sujet de l'archivage électronique : « Partant, établir ou conserver ses actes juridiques par des méthodes dont on sait par avance qu'elles vont susciter la méfiance est contraire aux finalités d'une preuve préconstituée et, d'une certaine manière, déroge aux exigences de l'administration de la preuve. Quand la loi exige que la preuve des actes soit préétablie, c'est bien pour qu'il en résulte des moyens de preuve efficaces, pas une énigme ; c'est bien pour que la résolution des litiges en soit simplifiée, pas le contraire ».

197. Il appartient aux Acteurs d'archiver les Assertions autant que les Objets numériques qui concourent au succès de leurs prétentions, comme il est d'usage de dire en Droit.

198. En fonction de la nature de l'Objet et de l'action captée par l'Assertion (ticket d'accès à une application, consentement quant à l'utilisation de mes données sur un site Web, facture, contrat, titre de propriété), la durée de l'archivage variera de quelques minutes à plusieurs dizaines d'années.

199. Il va de soi que tant pour contrôler l'accès aux archives que d'en connaître les propriétaires, une Identité numérique solide est essentielle.

200. A ce titre, considérant les archives des entreprises, des administrations, et de tous les organismes publics ou privés, la capacité de doter les personnes morales d'une identité numérique, et la capacité d'identifier tous les employés de ces entreprises avec une identité qualifiée par la Fonction exercée au sein de ces collectivités apparaissent comme une nécessité.

[99] Le droit au consentement implique le droit au renoncement.
[100] Cf. § 158, 169, 170.
[101] Lucien Pauliac, Le numérique, l'archivage, et la preuve.
[102] Décret 2016-1673 du 5 décembre 2016, JORF du 6 décembre 2016.

6. MISE EN ŒUVRE

Les solutions numériques de l'identité doivent se conformer au droit strict de la preuve ; preuve de l'identité des acteurs (et non d'une adresse IP) ; preuve du consentement ; preuve de la constitution des conventions. Elles doivent être recevables et opposables en justice et valider irrévocablement le lien de droit d'agir entre acteurs et actions.

6.1 L'autonomie de la preuve

201. Il est un principe général en Droit de la preuve : « une preuve ne se suppose pas, elle s'impose ». En d'autres termes, il ne peut y avoir d'ambiguïté ni de doute résiduel quant à l'observation élevée au rang de preuve. Cette notion en appelle une autre, celle de l'autonomie de la preuve, à savoir que la validité d'une preuve ne peut dépendre d'autres éléments, eux-mêmes non vérifiables.

202. Ainsi, un Dispositif d'Identification simple et compact (voir point 6.2) sera toujours préférable à une chaîne d'Identification complexe comprenant de nombreux sous-systèmes distribués.

203. L'utilisateur dérouté par une cascade de menus, de fenêtres pop-up, de boutons ou liens mal cliqués, de messages éventuels d'erreur de communication, de messages de confirmation tout aussi furtifs ou effacés par un malencontreux rafraichissement de page web, pourra toujours invoquer : « Monsieur le juge, ma volonté a été altérée par la complexité de la machine ».

204. Il n'est même pas besoin d'une possible confusion, toute machinerie programmable, voire en composants distants les uns des autres (un applet Web dans votre navigateur Internet d'une part, la saisie du PIN code par le pilote du clavier, et le calcul de l'Assertion sur l'Objet numérique par le serveur distant) désigne une intelligence intermédiaire capable d'altérer la volonté de l'Acteur, tant par sa défaillance possible, que par une (re)programmation malveillante.

205. Même le multifenêtrage auquel nous sommes tellement habitués sur nos ordinateurs et tablettes, et nos technologies Web dont la composition des pages est par nature fragmentée sur de multiples sources distantes, posent question. Il est très facile de substituer un contenu par un autre via la superposition graphique de fenêtres sans contours ; on ne peut pas non plus garantir qu'une page Web est complète ou intègre, même sans volonté de nuire, à cause d'un incident de communication.

206. « Monsieur le juge, ma volonté a été altérée par la complexité de la machine ».

207. ⚠ En d'autres termes, s'il existe des Dispositifs électroniques :

- Non programmables (figés dans leurs algorithmes),
- Autonomes, en ce qu'ils ne requièrent aucune intervention de systèmes externes à ce Dispositif,
- Sous ma maîtrise, à savoir que le geste[103] ne peut être dissocié du Dispositif utilisé pour libérer l'Identifiant[104] aux fins de créer une nouvelle Assertion,
- Capables de fabriquer une Assertion liant l'identifiant que je choisis avec l'Objet numérique visé par mon action, alors c'est clairement ce type de Dispositif qu'il me faut utiliser.

6.2 Dispositifs compacts et biométriques

208. Nous avons compris que toute la difficulté réside dans le caractère irrévocable de l'Identification telle que définie dans notre modèle[105] :

- Avoir la maîtrise exclusive de mes identifiants
- Aux fins de construire des Assertions liées aux Objets numériques visés par mon action
- Consécutive à l'expression explicite[106] de ma volonté (consentement ou renoncement)[107].

[103] Cf. 174.
[104] Que je choisis parmi ceux qui m'ont été attribués et associés à un Mandat en cours de validité.
[105] Cf. 87.
[106] Ni implicite (actes en série sauf englobant explicitement une telle série), ni accidentel.
[107] Cf. 175.

209. A ce stade, la seule façon actuellement fiable d'impliquer un utilisateur précis du monde réel dans la fabrication autonome[108] d'une Assertion dans le monde numérique est de recourir à la biométrie en combinaison avec un deuxième facteur[109], typiquement un jeton physique amovible comme une clé ou une carte à puce qui enferme les « secrets » nécessaires aux opérations cryptographiques.

210. L'exigence d'autonomie plaide fortement en faveur d'une exécution locale de l'Identification ; à savoir une validation des captations biométriques et la génération des Assertions au sein du Dispositif et sans agent extérieur.

211. Ni la validation à distance à l'aide d'un fichier central de masques biométriques (empreinte digitale, iris, ou faciale par ex.), ni le calcul des Assertions par un serveur central ne sont illégaux. Toutefois, cela pose des questions de sécurité liées à la transmission de ces données au travers d'autres systèmes susceptibles de les intercepter, de les altérer, ou de les rejouer à l'insu de la personne. Le calcul des Assertions par le serveur central aggrave encore plus ces questions. Et quel recours aura la personne quand un tiers (l'hébergeur du système central, l'opérateur des serveurs, le prestataire du réseau) vous empêchera de manifester votre identité à un moment critique à cause d'une indisponibilité passagère ?

212. Tous ces éléments plaident en faveur de dispositifs autonomes, sachant de plus que ces technologies existent.

213. Les techniques biométriques sont en pleine évolution. Il peut s'agir d'empreintes digitales, de reconnaissance faciale, iris, voix, micro-vaisseaux sanguins, champs électriques neuronaux, micro-vibrations physiologiques, et d'autres encore basées sur des implants, voire d'une combinaison de divers moyens. Nous ne discuterons en conséquence ni de la fiabilité, ni du mérite de chacune de ces techniques, ou de leur résistance aux tentatives de falsification. Le taux de faux positifs[110] réalisable actuellement est sous 1/1.000.000 avec, notamment, les empreintes digitales.

214. Une preuve n'est pas un moyen, c'est un résultat : que fait-on du millionième restant ? La réponse est juridique : le fournisseur du dispositif doit s'engager sur une obligation de résultat et non une obligation de moyens. Il couvre le risque résiduel à l'aide d'assurances, tout simplement.

215. Ce n'est pas si différent de ce qui se passe aujourd'hui pour les opérateurs de cartes de crédit sauf que cela ne concerne qu'un seul type d'Objet numérique : l'ordre de paiement. Le dédommagement de la fraude est à la charge des opérateurs si l'utilisateur n'a commis aucune faute. Leur commission comprend une assurance pour couvrir un taux de fraude (environ 0,05%) qui est ici très largement supérieur au 1/1.000.000 atteignable par la biométrie.

216. Il ne faut pas oublier les règles de proportionnalité, licéité, et finalité[111], à savoir la mise en œuvre de moyens proportionnels aux risques, aux enjeux, et conformes à la loi.

217. Ceci confirme encore une nécessité intégrée au modèle, à savoir la pluralité des identifiants, et la flexibilité en conséquence qu'il y aura d'attacher des moyens de reconnaissance proportionnels à l'importance fonctionnelle de chaque identifiant.

218. On peut aussi combiner l'utilisation d'Identifiants numériques sans Mandat attaché[112], à savoir auto-attribués et protégés par exemple par mot de passe ; On comprend qu'un identifiant structuré[113] n'est pas sans intérêt pour gérer mes données personnelles associées à cet identifiant.

219. Si l'on souhaite intégrer dans notre modèle des entités artificielles comme des robots ou IA, les Dispositifs d'Identification devront passer par des caractéristiques physiques scellées et inaltérables, telle une puce hardware inamovible et indispensable à la mise en route des processeurs. De tels dispositifs existent déjà.

6.3 Avec ou sans fichier central

220. Une donnée à caractère personnel est « toute information permettant directement ou indirectement d'identifier une personne »[114]. Peu importe que ces informations soient confidentielles ou publiques.

221. Pour que ces données ne soient plus considérées comme personnelles[115], elles doivent être rendues anonymes de manière à rendre irréversible toute identification de la personne concernée. S'il est possible par

[108] Cf. 207.
[109] Il y a maximum 3 facteurs : (1) ce que je suis (biométrie), (2) ce que je possède (carte à puce ou jeton physique), (3) ce que sais : un PIN code par exemple.
[110] Reconnaissance positive de la personne supposée, alors qu'il s'agit de quelqu'un d'autre.
[111] Cf. RGPD, art. 5 et 6 ; Loi Informatique et libertés, art. 4 et 5.
[112] Cf. 139.
[113] Tel que décrit au 133.
[114] Définition Cnil, https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi
[115] Nuance subtile : la législation ne régit pas la question de la propriété des données personnelles.

recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers (adresse IP, cookies), d'identifier une personne, les données sont toujours considérées comme personnelles.

222. Dans les conditions d'un respect strict de l'usage des données personnelles, il est impératif que tout moyen tendant à produire une identité numérique devra garantir à celui qui s'identifie la maîtrise des données personnelles associées à cette identité (ex : « signé par Mr X, délégué commercial de la société Y »). A nouveau, des dispositifs autonomes peuvent assurer cette fonction autant que le recours à un fichier central d'identités. La question de l'autonomie [116] se double d'une question de protection des données personnelles qui va exactement dans le même sens. Et cette deuxième question ne se limite pas aux données de l'identité : le calcul des Assertions par un serveur central brasse encore plus de données personnelles concernant qui fait quoi avec qui et/ou au nom de qui à quel moment.

223. ⚠ En conséquence, choisir son dispositif avec ou sans l'usage d'un fichier central de données à caractère personnel est important car la construction d'un serveur ou fichier central de données à caractère personnel n'est pas nécessaire à la mise en place d'une Identité numérique telle que celle proposée ici. Les données de l'identité (biométrie, état civil complet, liste de toutes les attributions de la personne) peuvent rester au sein des Dispositifs, les identifiants sont numériques, et les utilisateurs gardent le contrôle complet des informations publiques éventuellement liées à ces identifiants au travers des annuaires associés aux Registres déjà cités.

224. Aucune disposition du RGPD n'interdit la conservation des données biométriques de façon centralisée sur un serveur dédié accessible à distance dans un data center de tiers (cloud), sous réserve des garanties de sécurité appropriées pour faire face aux risques.

225. Par conséquent, l'importance qu'il y a de choisir entre l'utilisation ou non d'un fichier centralisé (et par voie de conséquence toute génération centralisée des Assertions) doit dépendre du cas d'usage :

- Lorsque la personne avec laquelle une transaction est réalisée se confond avec l'opérateur des serveurs centraux ;

- En cas de contrat d'adhésion, à savoir que la Personne à laquelle vous devez démontrer votre identité est aussi celle qui a mis les moyens de cette identification à votre disposition.

226. Le paiement électronique (par carte de crédit ou banque en ligne) en est la parfaite illustration. L'organisme de débit ou crédit me délivre des moyens de m'identifier qu'il a déterminés de façon unilatérale (d'où ce contrat dit d'adhésion) comme étant adéquats pour les services qu'il m'offre. Lorsque je paie un commerçant, c'est à cet organisme que j'adresse mon ordre de paiement. Le commerçant reçoit la preuve du paiement via son propre opérateur de paiement, et n'a pas besoin de m'identifier[117]. S'agissant d'un contrat d'adhésion, tout dysfonctionnement du système ou même fraude qui ne me soit pas imputable est à charge de l'opérateur et donne lieu au remboursement.

227. L'utilisation de moyens d'identification régaliens (mis à disposition par l'État) vis-à-vis de l'administration de ce même État est un autre exemple d'adhésion.

228. ⚠ Par contre, s'agissant de mettre en place une identité numérique universelle opposable à toute personne sans relation aucune avec mon fournisseur de moyens d'Identification, ni moi avec celui de la partie opposée, nous sommes dans un contexte bien différent où les opérateurs concernés n'ont aucune relation ni avec l'Objet de la transaction, ni systématiquement avec la partie opposée. Il faut alors impérativement être fabricant de preuves (cf. Chapitre 5, point 5.1), interopérable (cf. point 6.4) et inter-opposable (cf. Chapitre 7, point 7.2)

6.4 Interopérable

229. L'interopérabilité est une nécessité légale évidente. L'Europe, dans ses règlements dont le RGPD et eIDAS, les organismes de standardisation, et les organismes des Nations Unies comme la CNUDCI, imposent qu'il ne peut y avoir de solution liée à un fournisseur de services ou de matériel particulier. Une solution d'identité numérique ne peut imposer ni Android, ni iOS, ni dépendre d'un fournisseur particulier, donc fonctionner dans tous les pays et sur tous les réseaux, et être juridiquement recevable dans tous les états. La concurrence est la règle ; elle passe forcément par des standards concernant les structures de données échangées et les interfaces entre composants de la solution.

230. ⚠ Dans notre écosystème de Communautés souveraines cela englobe la nécessité pour une communauté de reconnaître l'identité assignée par une autre Communauté / sous un autre registre, et notamment de pouvoir enrôler les Fonctions d'une personne au sein d'une Communauté sur base d'identités déjà attribuées par ailleurs.

[116] Cf. 210.

[117] Pas pour le paiement en propre, peut-être bien pour les services que j'achète, mais alors très probablement pas sur base de mon « identité bancaire ».

231. Le développement complet de ces questions et l'inventaire des données/interfaces à standardiser sont très avancés mais sortent du cadre du présent livre blanc. Ces questions feront l'objet de spécifications ultérieures.

6.5 Cas d'usage : contractualisation

232. L'identité numérique se doit de créer les conditions permettant de produire la sécurité juridique des transactions dématérialisées, littérales et autres, échangées entre une ou plusieurs personnes physiques ou morales ainsi qu'entre objets communicants. Le service produit par cette solution se doit d'être interopérable (indépendant des systèmes opérants), inter-opposable (juridiquement recevable dans 193 états membre de l'ONU), pérenne (constante dans le temps) et supranational (pas de frontières sur internet).

233. On notera que le mode opératoire évoqué ici se passe de tout fichier central.

234. Le système s'articule sur un enchaînement insécable de fonctions issues d'une cinématique fonctionnelle expliquée ci-dessous dans l'hypothèse d'un Dispositif formé :

- D'une carte à puce porteuse des identifiants de l'utilisateur, des clés de chiffrement nécessaires à la sécurité, et des attributs de son identité ;
- D'un lecteur d'empreintes digitales dont la validation est une opération locale[118] entre des données protégées de la carte et le lecteur d'empreintes.

235. L'enchaînement systématique et indéfectible de ces points constitue les éléments de preuve nécessaires et suffisants à l'élaboration d'une relation contractuelle opposable aux tiers, en vue de la formation d'un contrat ou de l'expression d'une obligation de quelque nature que ce soit

6.5.1 Identification irrévocable du signataire/expéditeur du document

236. Maîtrise – Sous le contrôle matériel, moral et juridique du porteur de la carte.

- L'une des premières conditions nécessaires à la réalisation de la démonstration de la preuve de l'identité dans un environnement numérique est que l'acteur ait la maîtrise pleine et entière de son moyen physio-technologique d'identification. Ainsi un Dispositif local, compact, et non reprogrammable est par nature non vulnérable à la prise en main par autrui, restant sous le contrôle exclusif de l'Acteur souhaitant s'identifier.

237. Autonomie – Faculté de se déterminer par soi-même.

- L'une des complexités de l'espace virtuel numérique est la faculté de dissocier plusieurs actions sans en maîtriser le contrôle. Si toutes les opérations se déroulent sur mon ordinateur, comment avoir l'assurance que c'est bien l'action que je perçois qui se déroule réellement sur mon ordinateur.
- Dans le cadre du Dispositif illustré ici, on peut résumer l'autonomie par « la carte lit le doigt et le doigt lit la carte » ; s'exprime ici un impératif technologique garantissant que l'action d'appairage entre la volonté de l'Acteur et la capacité du Dispositif à lier cette particularité physique se déroule sans intervention externe possible.

238. L'autonomie garantit l'insécabilité des actions probatoires à la démonstration de « qui je suis ? ».

239. Qualité – Être formellement habilité dans un acte juridique.

- Au-delà de la validation de son identité, l'acteur doit être en mesure d'indiquer à quel titre il est habilité pour agir. Il est nécessaire que l'identité soit juridiquement qualifiée par la Fonction dont l'identifié peut se prévaloir, par exemple : directeur de la société X, trésorier de l'association Y.

240. Capacité – Aptitude à jouir de certains droits et à les exercer.

- En complément, l'acteur doit être en mesure de valider les capacités à agir que sa Qualité lui confère.

241. Corollaire – Distinction du signataire de l'expéditeur.

- Les dispositifs destinés à valider une identité numérique doivent être en mesure de distinguer le signataire d'un courrier de l'expéditeur de celui-ci, ceci afin de préserver les droits et la capacité de chacun à agir. Les droits du destinataire ainsi averti n'en seront que plus affermis.

[118] Qualifiée de « Full Matching on Card ».

6.5.2 Création d'un lien indéfectible entre le consentement du signataire et l'objet du consentement

242. Consentement – Je suis libre de consentir ou de renoncer ; je signe ce que je vois, et je vois ce que je signe.

- Comme déjà évoqué, l'une des complexités de l'espace virtuel est la faculté de dissocier plusieurs actions sans en centraliser le contrôle. Sur son ordinateur, croyant signer un document « A », l'Acteur signe un document « B », même juste par la confusion du fenêtrage sans qu'il y ait eu malversation. Dans le cas des interfaces Web, ce qui est vu résulte souvent de l'assemblage de nombreux « morceaux de page » provenant de sources différentes, et des erreurs de communication peuvent en altérer l'affichage sans pour autant être visibles.
- A défaut le consentement entaché de doute ne pourra être garanti et sera donc susceptible de contestation.

243. Lien de causalité – Garantie matérielle de la chose signée.

- Se pose ici la question du lien de causalité entre l'Acteur et l'Action. Le Dispositif générant l'identité numérique de l'Acteur devra, sans défaillance possible et avec obligation de résultat, assurer qu'il existe un lien biunivoque et indéfectible entre l'acteur et l'action, sans possibilité d'usurpation ni de copiage.

244. Intégrité – Incorruptibilité du document garantie.

- Dès lors que l'acteur identifié irrévocablement, ayant consenti à une action, dont le lien de causalité sera définitivement acquis, le résultat des fonctions précitées devra être définitivement encapsulé et encrypté dans un acte total (document final), original, unique.
- Il s'agit ici de garantir les modalités techniques nécessaires à rendre l'action précitée immuable dans le temps et l'espace. Cryptée ou non, la forme originale du document devra être garantie indépendamment des évolutions (mise à jour) des applications destinées à lire ledit document.

245. Confidentialité – Seules les parties signataires ont accès au contenu de la convention.

- Dans le respect stricto sensu de la protection du secret des affaires ainsi que du secret des correspondances, il est impératif que les communications formées depuis un système d'identification et de consentement (signature) doivent garantir la plus ferme confidentialité et protéger les co-contractants de toute dispersion de l'information ainsi échangée.

6.5.3 Signature électronique irrévocable

246. Irrévocabilité – La signature électronique doit être irrévocable pour être opposable aux tiers.

- Pour être opposable aux tiers, le consentement (signature) né de l'identité de l'auteur, devra être qualifiable d'irrévocable. Par conséquent, le système fournissant ce service devra être en mesure de démontrer tant l'enchaînement des fonctions énoncées mais aussi en démontrer l'insécabilité.

247. Supranationalité – Il n'y a pas de frontières sur Internet.

- Pour satisfaire à cette qualité, le service « identité-signature » devra être conforme aux contraintes légales imposées par la CNUDCI[119] en cette matière. Dès lors, le service rendu sera recevable en opposabilité dans les 193 pays signataires.

248. Pseudonymisation La signature électronique ne nécessite pas de mettre en place un fichier central des données à caractère personnel.

- Par construction, le système décrit ici n'en a pas besoin. Le système intermédiaire d'échange peut valider les opérations à l'aide de « zero knowledge proofs » (ZKP) ou preuves à divulgation nulle de connaissance. Il s'agit de protocoles permettant à un acteur de prouver qu'une situation est réelle sans avoir à révéler les informations relatives à cette dernière.[120]

249. Unicité – La signature n'est pas reproductible. Chaque signature est unique et différente.

- Aux fins de garantir l'originalité de chaque action consentie, la marque du consentement sous sa forme électronique devra être unique et exclusive à chaque action. Il en va de la qualité intrinsèque du consentement lié à une action précise, qualité essentielle quant à la démonstration de la preuve, mais également de la sécurité des actes consentis en interdisant alors la duplication et/ou l'interception de toutes formes de consentement.

---

[119] Loi type de la CNUDCI sur les signatures électroniques (Juillet 2001) : 35 pays signataires
Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (New York, 2005) : 27 pays signataires

[120] Guillaume Chanut, « Les zero-knowledge proofs (ZKP) : principe et applications », Cryptoast.fr le 25 juillet 2020.

250. Non corruptibilité – La signature électronique doit être chiffrée.

- L'ensemble des fonctions composantes du service « identité – consentement – contrat » devront être protégées par des moyens cryptographiques garantissant la sécurité de bout en bout des échanges ainsi réalisés.

251. Multi signature – La signature électronique doit permettre la signature multiple du même document par plusieurs signataires.

- La faculté de satisfaire à une capacité de multi-signataires est une nécessité, notamment en termes d'actes contractuels. De plus, chaque participant doit pouvoir exercer sa capacité sans aucune interférence avec les autres.
Or, notons que le standard actuel de signature (PAdES)[121] sur les documents PDF/A (PDF Archive) impose une stricte séquence de signatures « empilées » sur une copie unique, qui :

- (a) soit est centralisée et soulève alors les questions de fichier central et d'autonomie (serveur distant programmable),
- (b) soit circule entre les participants ouvrant la porte à l'obstruction ou la rétention aux dépens des signataires suivants.

252. Opposabilité – La signature électronique doit être opposable aux tiers et juridiquement recevable dans les 193 États membres de l'ONU.

- L'opposabilité aux tiers (le premier « tiers » est le juge) sera acquise à la condition que l'acte soit parfait, c'est-à-dire que les parties prenantes soient irrévocablement identifiées, les consentements avertis et incontestables, et que les conditions générales sous lesquelles la convention est formée soient conformes aux dispositions édictées par la CNUDCI en ce qui concerne la supranationalité.

6.5.4 Création d'un document original

253. Intervention d'un tiers – « nul ne peut se constituer de preuve à soi-même »[122].

- Selon le principe de la qualité extrinsèque de la formation des moyens de preuve, il est acquis que dans un espace numérique où les moyens de fabrication de documents et de signatures sont accessibles à tous sans laisser de traces, l'intervention d'un tiers aux fins de garantir la qualité juridique des conventions formées en ligne et/ou l'échange d'informations sous toutes formes est nécessaire à la formation des conventions.

254. Précisons que les techniques actuelles (notamment le « zero knowledge proofs[123] ») permettent de garantir cette qualité sans avoir à connaître le contenu ni identifier les intervenants d'une transaction numérique.

255. Journalisation de l'échange – Horodatage en temps universel.

- Eu égard à la portée mondiale de la transmission des informations, du caractère « sans frontière » de l'espace numérique, il sera de convention, que pour être opposable, l'horodatage devra se faire sur la base du temps universel.

256. Validation du signataire/expéditeur – Droit à agir.

- Outre l'identité du signataire, le système produisant le consentement (signature) devra être en mesure d'indiquer quels sont les droits à agir des parties prenantes aux conventions, ceci afin de garantir et de protéger les co-contractants quant à la nature et le quantum des engagements auxquels ils consentent mutuellement.

257. Original/Unique – Le service produisant « identité-consentement » devra être en mesure de garantir l'originalité du document produit, et ce tout au long de son existence.

- L'internet est par nature un système favorisant la copie de l'information. Il faut donc mettre en place un concept de document original « logique » indépendamment de la copie des supports de celui-ci plutôt que de lutter contre la copie numérique toujours possible, même avec des « coffres-forts » électroniques.

258. Intégrité – Garantir l'incorruptibilité du document par une solution de chiffrement.

- L'intégrité des documents (informations) échangés devra être garantie par des solutions de cryptage nécessaires et suffisantes à produire un original unique et d'en assurer l'unicité dans le temps.

6.5.5 Identification irrévocable du destinataire

259. Les conditions de maitrise, d'autonomie, de qualité pour agir et de capacité à agir du destinataire sont les mêmes que celles détaillées au point 6.5.1 concernant le signataire expéditeur.

---

[121] Le format PAdES (PDF Advanced Electronic Signature) est le format des signatures électroniques incluses dans les documents PDF.
[122] Cf. Clémence Mouly-Guillemaud, « La sentence « nul ne peut se constituer de preuve à soi-même » ou le droit de la preuve à l'épreuve de l'unilatéralisme », Revue trimestrielle de droit civil (RTD Civ.), Dalloz, 2007, pp.253 hal-02196195.
[123] Cf. § 248

260. Corollaire – Distinction du destinataire et du récepteur.

6.5.6 Livraison conforme du document

261. Intégrité – Conformité à l'original précité.[124]

262. Livraison non intrusive – Le document est quérable.

- Considérant que l'espace numérique d'un ordinateur/PDA est un espace privé, toutes les formes imposées de délivrance de l'information pourraient être qualifiées de violation de domicile. De plus, la capacité d'acceptation doit être proportionnelle et réciproque à la capacité de refus pour être valide (on peut refuser un recommandé). Le prestataire de messagerie doit alors :

- S'assurer que le destinataire peut refuser la délivrance d'un courrier électronique,
- Garantir que les courriels sont quérables et non portables.

263. Confidentialité – Seul le destinataire peut lire le document

- Le service doit assurer au destinataire la plus extrême confidentialité des courriers reçus.

267. La figure ci-dessous et les explications afférentes sont tirées de la documentation disponible sur le portail Partenaires de franceconnect.gouv.fr.

6.6 Cas d'usage : paiement

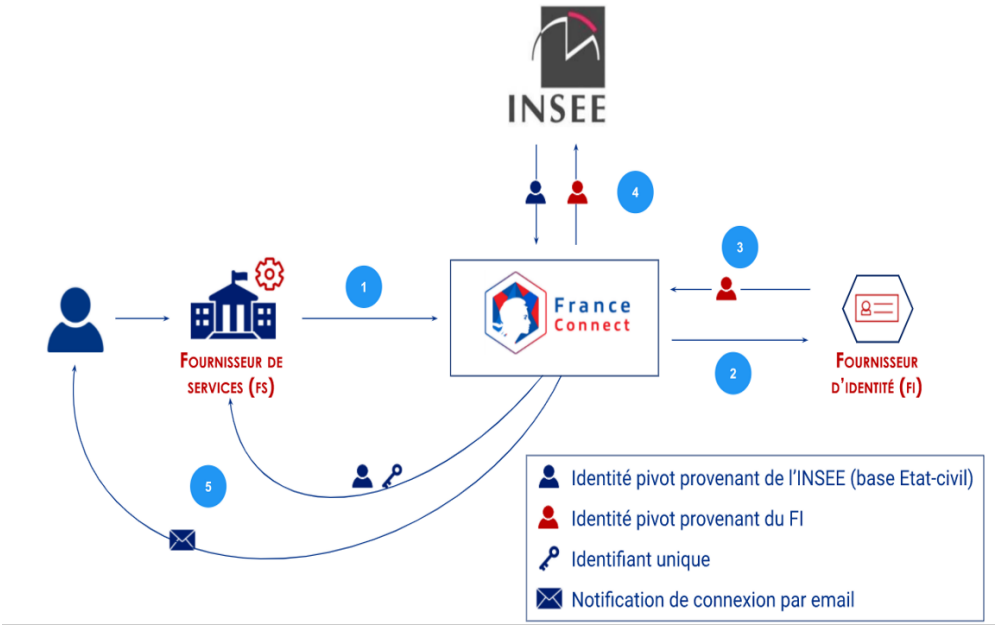
264. La lettre de change - Avec une identité irrévocable et à peu de choses près le même enchaînement de fonctions que celui qui vient d'être décrit, on peut réinventer la lettre de change et de manière plus générale tous les effets de commerce.

6.7 Dispositif FranceConnect

265. FranceConnect est un dispositif conçu par l'État pour faciliter et sécuriser les démarches en ligne.

6.7.1 FranceConnect

266. Le système FranceConnect est un système fédérateur entre fournisseurs de services (FS) et fournisseurs d'identité (FI) pour l'identité régalienne, également dénommée « identité pivot » : nom, prénoms, date et lieu de naissance, sexe, et en option un alias et une adresse courriel.



(1) Le fournisseur de service (FS) demande au Tiers de confiance (TC) de lui renvoyer tout ou partie des données personnelles de l'usager (identité pivot) conformément à l'habilitation.
(2) L'usager sélectionne un fournisseur d'identité (FI) et s'identifie en utilisant les identifiants de son compte chez le FI.
(3) Le FI renvoie à FranceConnect l'identité pivot de l'usager (nom, prénom(s), date et lieu de naissance, sexe), le nom d'usage s'il est connu du FI, ainsi que l'email de contact (l'email pouvant différer suivant le FI choisi par l'usager).
(4) FranceConnect demande validation de l'identité pivot à l'INSEE, qui la redresse en cas de faible écart. FranceConnect génère un identifiant unique de l'usager, spécifique au FS.
(5) FranceConnect retourne l'identité pivot et l'identifiant unique au FS. L'usager est connecté au service et informé par mail.

[124] Cf. point 6.5.4.

268. Son avantage déclaré est d'isoler les fournisseurs de services et les fournisseurs d'identité, selon le principe que les fournisseurs d'identité ne savent pas à quel service l'utilisateur demande d'accéder, et que le fournisseur de services ne connaît pas les données personnelles d'identité utilisées pour authentifier (selon leur définition) l'utilisateur.

269. FranceConnect est surtout – de notre point de vue – un système technique qui permet à l'État français de confirmer l'identité régalienne d'une personne tout en se déchargeant de la gestion de l'identification autant que de l'exploitation des services, avec à la clé une économie d'efforts et de moyens substantielle pour tous les acteurs.

270. En effet, un fournisseur de service (FS) se voit en mesure d'accepter un nouvel utilisateur sans avoir à passer par toutes les procédures de délivrance d'une identification suffisamment sécurisée à celui-ci ; il obtient de plus, la garantie de traiter une identité régalienne officielle, sans responsabilité sur la qualité de l'Identification ad hoc (à part d'exiger un niveau de sécurité minimal, par exemple « substantiel » ou « élevé », tel que réglementé par eIDAS).

271. Le fournisseur d'identité (FI) offre à chaque nouvel utilisateur l'accès potentiel à tous les fournisseurs de services (FS) « FranceConnect » ; il délivre des moyens d'identification certifiés eIDAS sans avoir à s'inquiéter de la nature ni de la valeur des services qui seront utilisés, donc sans responsabilité sur les dommages éventuels d'un abus. Enfin, l'utilisateur est aussi bénéficiaire : il ne doit s'enregistrer qu'une seule fois pour avoir accès à tous les services « FranceConnectés ».

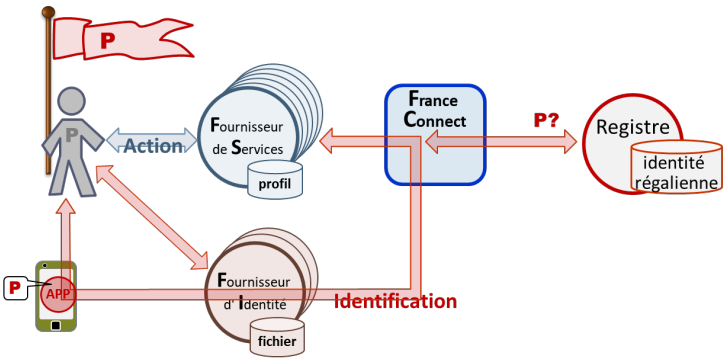
272. FranceConnect est basé sur les standards d'authentification « Open ID Connect » et « OAuth 2.0 »[125] qui ont été conçus pour permettre à des opérateurs de service Web (FS) de partager des identifiants déjà enregistrés auprès d'un autre opérateur (FI souvent FS lui aussi).

273. Ne vous est-il pas déjà arrivé de vous connecter à un fournisseur de service – achats, photos, blogs, presse, forum, hébergement – qui accepte désormais vos identifiants Google ou Facebook ? De prime abord une simplification sympathique, mais le traçage de vos activités n'en est que plus efficace. Pire, comme cela a déjà été évoqué en préambule, les géants du cloud (rôle FS uniquement) peuvent avec ce système offrir un accès à leurs services en ligne sur la base des identifiants internes à l'entreprise (dans le rôle FI). Tout en étant rémunérées pour leurs services bureautiques, elles peuvent ainsi observer l'activité interne de chaque entreprise cliente.

274. Dans l'architecture originale, « Open ID Connect » et « OAuth 2.0 » sont conçus pour connecter directement FS et FI dans une architecture N-à-N entièrement maillée. FranceConnect a très intelligemment étendu ces standards pour se poser en intermédiaire fédérateur dans une architecture en étoile N-à-1-à-N de façon à garder son rôle de dépositaire des identités régaliennes.

275. On peut parler d'une approche défensive de la souveraineté de l'État face à la déferlante numérique[126]. La répartition des rôles résulte ici plus d'une vision technique et pragmatique que juridique ; elle est illustrée à la figure ci-dessous. La bannière qui flotte au-dessus de la tête de notre utilisateur représente l'identité numérique qu'il peut exercer.

276. Dans cette figure, un téléphone mobile fait partie du Dispositif d'Identification utilisé. Les fournisseurs d'identité peuvent bien sûr proposer d'autres moyens dans le cadre des certifications eIDAS[127] ou Référentiel Général de Sécurité applicable aux administrations[128] sous la supervision de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).[129]



[125] OpenID Connect est une couche d'identification complémentaire au protocole OAuth 2.0. Il permet aux clients de vérifier l'identité de l'utilisateur final sur la base de l'authentification effectuée par un serveur d'autorisation, ainsi que d'obtenir des informations de profil de base sur l'utilisateur final. Informations sur https://openid.net/connect/.
[126] Cf. chapitre 7.
[127] Certifications prévues par le Règlement « eIDAS » n° 910/2014 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.
[128] Certifications prévues par le référentiel général de sécurité (RGS) visant à normaliser les échanges de l'administration, aux termes de l'Ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[129] Pour plus d'information, https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/

6.7.2 Communautés souveraines

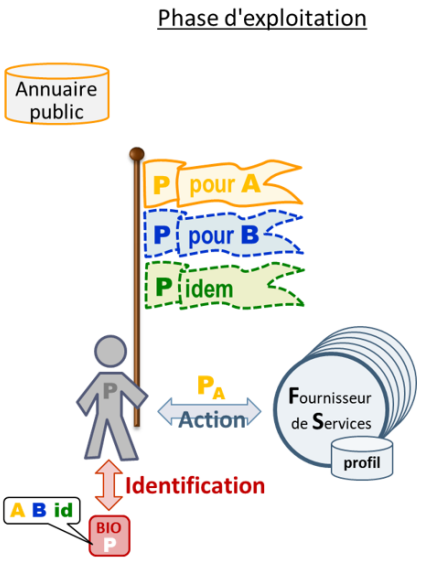
277. L'approche juridique de l'Identité numérique que nous proposons aboutit à une répartition des rôles bien différente, et – nous pensons – bien plus universelle. Cette répartition est illustrée en figure ci-contre : le schéma est très simple puisque les diverses Identités numériques – toutes validées – ont été stockées dans le Dispositif, avec l'accord de son propriétaire[130] et la confirmation d'un enrôleur de la Communauté en question. Le Dispositif devant être par construction sous le contrôle exclusif de son propriétaire, celui-ci est alors entièrement autonome pour faire valoir l'identité qu'il choisit d'exercer.

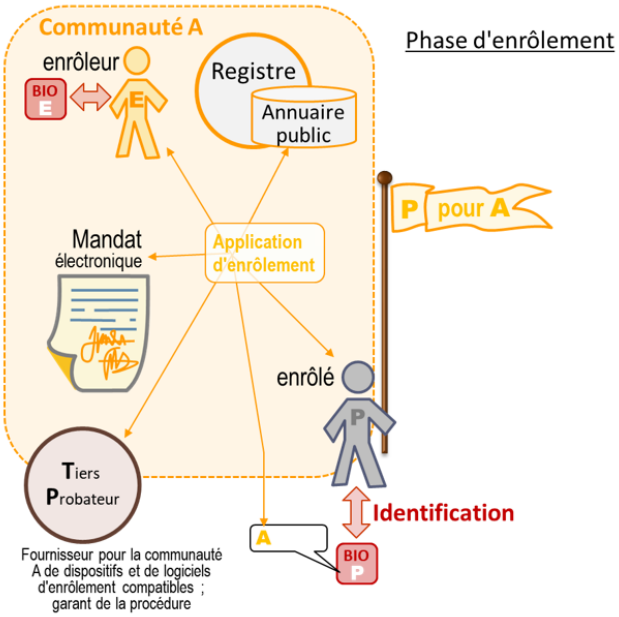
278. ⚠ Cette autonomie d'identification (sans interaction avec un système central) vient s'ajouter à l'autonomie de la preuve[131]. En effet, aucun système tiers ne peut venir entraver la volonté de s'identifier de l'utilisateur, ni s'y substituer.

279. La phase initiale d'enrôlement est illustrée figure ci-contre pour une seule des identités numériques de notre utilisateur. Cette opération ne se déroule qu'à la création d'une attribution (une Fonction dans une Communauté), voire de l'identité « idem » / en nom propre, et n'est répétée qu'en cas de perte d'éléments du Dispositif d'Identification, comme par exemple une carte à puce, ou de mise à jour des masques de capture biométrique (pour éviter toute substitution de la personne).

280. Le « Tiers Probateur » remplace ici le fournisseur d'identité (FI). Son rôle étant bien différent d'un FI, la dénomination « Tiers Probateur » indique clairement que cette entité n'est là que pour fournir aux Communautés, et en particulier les personnes légalement mandatées par ces Communautés pour enrôler les membres (exemple : le directeur des ressources humaines dans une entreprise), les moyens interopérables nécessaires à l'enrôlement – sans pouvoir interférer dans celui-ci autrement qu'en tant que garant de la procédure, ce qui signifie aussi sans capter aucune donnée personnelle de la personne enrôlée.

281. ⚠ Etant donné l'exigence de découplage entre l'identité et les propriétés de sécurité[132], le renouvellement périodique des variables de sécurité (clés cryptographiques, certificats, etc., tous les 2 ans en moyenne) n'exige aucune opération compliquée : l'application de l'utilisateur gérant le Dispositif constatant le terme proche des variables de sécurité sollicitera simplement l'accord de l'utilisateur pour la mise à jour. Cet accord est explicite, car pour satisfaire à la maîtrise exclusive du Dispositif par l'utilisateur, il ne peut y avoir de changement interne à celui-ci sans son consentement.





282. Il y aurait beaucoup d'explications supplémentaires à formuler concernant les phases d'enrôlement et d'exploitation, mais cela sort du cadre du présent livre blanc. Les spécifications nécessaires feront l'objet d'un document de spécification complémentaire à ce livre blanc.

283. L'approche proposée n'est pas incompatible avec FranceConnect. Les Communautés peuvent devenir Fournisseurs d'Identités (FI) dans l'architecture FranceConnect par l'entremise des Tiers Probateurs. Ceux-ci sont aptes à valider la sécurité d'une identification (précisément, d'une Identification Numérique grâce à la référence du Mandat) sans pour autant pouvoir identifier les personnes.[133]

[130] Cf. point 6.2.
[131] Cf. point 6.1.
[132] Cf. ci-dessus 76.
[133] Cette affirmation peut paraître contradictoire ; elle se fonde sur une technique certes moins connue mais pourtant bien rodée de la cryptographie : les « zero knowledge proofs » (ZKP). Sur cette notion cf. point 6.5.3.

7. DÉPLOIEMENT

L'expression « souveraineté numérique » qui se diffuse progressivement a été popularisée par Pierre Bellanger, qui multiplie les interventions médiatiques à partir de 2008, avant de publier La souveraineté numérique en 2014 (éditions Stock).

7.1 Créer un écosystème de communautés souveraines

7.1.1 Souveraineté numérique

284. L'intrusion dans toutes les activités de la vie sociale et économique d'une informatique en réseau aux mains de quelques sociétés privées dont les bénéfices rivalisent avec le PIB de nombreux pays développés remet en question la souveraineté des états.

285. Même si on ne partage pas toutes les prédictions du président directeur général et fondateur de Skyrock, Pierre Bellanger[134] concernant la dépendance à venir des personnes, des entreprises et des états, à une informatique en réseau (le « résogiciel »[135]) aux mains de quelques sociétés privées (les GAFAM's[136]) majoritairement américaines, on ne peut pas nier que ce mouvement est en marche.

286. Le concept classique de souveraineté a été posé par Jean Bodin au XVIe siècle « pour permettre au roi de se dégager à la fois des seigneurs féodaux et du pouvoir de l'église »[137]. Le concept renvoie aujourd'hui au pouvoir légitime de l'État (élu ou autoritaire) à gouverner un territoire et une population sans ingérence de puissances extérieures aux fins de conserver la maîtrise de son destin.

287. « Rares sont les domaines dans lesquels l'exercice des compétences de l'État n'est pas conditionné désormais par sa dépendance aux réseaux numériques et à ceux qui les gouvernent : politiques monétaires et fiscales, défense, systèmes sociaux, politique industrielle, systèmes de santé, énergie, culture, éducation, information et communication, transport, et même conservation des archives ».[138]

288. Cette souveraineté numérique, qui qualifie tant le problème que les réponses à y apporter, peut être vue à différents niveaux [139] :

1. « Revendiquée par les états, la souveraineté numérique n'est cependant pas conçue de la même façon par tous : selon une conception autoritaire et offensive, elle fonde le droit pour l'État de reprendre le contrôle des espaces numériques pour y appliquer ses lois et y promouvoir ses intérêts ; selon une conception plus libérale et défensive, elle fonde le droit pour l'État de protéger ses citoyens contre les politiques de surveillance et d'exploitation conduites dans le cyberespace par des entités mues par leurs intérêts propres ».

2. « Mais la souveraineté numérique, ce peut être aussi la souveraineté collectivement revendiquée par des groupes d'utilisateurs du numérique, voire par des communautés d'internautes plus ou moins organisées qui revendiquent d'être associées à la détermination des règles applicables et de participer à l'organisation de la protection de leurs données sur les réseaux. Reconnaître [ce] droit pour les communautés [...] conduit d'une certaine façon à transposer au monde numérique la réflexion classique sur la formation des sociétés civiles et le passage aux sociétés politiques ».

3. « La souveraineté numérique c'est aussi celle de l'individu sous l'angle de sa capacité à s'autodéterminer, à commander pour lui-même, à maîtriser ses données ».

289. La notion est donc appréhendée de façon très diverse qu'il s'agisse de prolonger la souveraineté des États ou d'imaginer de nouvelles formes de souveraineté non étatiques. Elle reçoit des acceptions juridiques, économiques, techniques ou fonctionnelles, et se conçoit à de nombreux niveaux : individuel,

[134] Pierre Bellanger, La souveraineté numérique, Paris, Ed. Stock 2014.
[135] Sur la définition et la mission du résogiciel, voir https://pierrebellanger.skyrock.com/tags/cNtC2lXjcUw-resogiciel.html
[136] Google, Amazon, Facebook, Apple, Microsoft, et toutes les autres par extension comme Tencent, ByteDance, Snap, Uber, Baidu, Alibaba, etc.
[137] Pauline Türk et Christian Vallar, La souveraineté numérique: Le concept, les enjeux, Ed. Mar & Martin, 2018.
[138] Pauline Türk et Christian Vallar, préc.
[139] Pauline Türk et Christian Vallar, préc.

collectif (communauté d'utilisateurs), national (conservation des archives publiques sur un « cloud souverain » par exemple), européen (protection des données personnelles), ou même international (gouvernance des réseaux).

290. Plutôt que d'associer au monde numérique une nouvelle forme de souveraineté, Karim Benyekhlef voit surtout une mise en « concurrence des souverainetés » amplifiée par l'Internet, et capable de redessiner les contours[140].

291. ⚠ C'est ce modèle qui s'impose en pratique, car il n'exclut aucun mécanisme de Droit pour peu que l'on puisse identifier la personne en rapport à une (ou des) collectivité(s) au sein de laquelle ou pour laquelle l'individu exerce son activité. Cette collectivité commence avec l'unité de sa propre personne jusqu'à l'échelle planétaire en passant par les entreprises, groupes d'intérêts, les états, et les unions (ex. Europe), chaque niveau disposant d'une forme de souveraineté, emboitées les unes dans les autres[141] et interagissant entre elles.

292. L'émergence d'un droit international de l'Internet, voire d'une constitution numérique universelle ne viendrait en rien bouleverser notre modèle, juste ajouter un niveau de plus auquel il faudra se référer pour déterminer le droit applicable à partir du moment où on connaît l'individu et son Mandat (de quel droit – sans faire de jeu de mots – peut-il exercer sa Fonction). On peut même imaginer que le monde virtuel viendrait interposer/superposer ses propres collectivités numériques transnationales à celles des entreprises et des états, avec un niveau de règles juridiques ad hoc.

293.. ⚠ Une identité numérique ne peut donc se concevoir en dehors d'une communauté, mais elle peut se rattacher à plusieurs communautés, l'individu ayant à chaque fois une attribution dans chacune des communautés, d'où le modèle (indivisible) de l'Identifiant numérique : <registre> + <communauté> + <identifiant personnel> + <fonction / attribution > + < mandat / capacité à agir>.

294. ⚠ Dans notre système[142] fondé sur les droits de l'homme et la liberté, l'individu est souverain dans sa décision de rejoindre des Communautés, et celles-ci sont souveraines vis-à-vis des systèmes de Droit dans lesquels elles choisissent de s'inscrire. Elles sont aussi souveraines en tant qu'entités protégées de l'ingérence potentielle d'autres entités auxquelles elles n'ont pas choisi d'adhérer.

7.1.2 Approche juridique : la souveraineté nationale

295. La souveraineté nationale est le principe selon lequel la souveraineté appartient à la nation qui est une entité collective abstraite, unique et indivisible. Les Etats souverains prennent des engagements et assurent ainsi mutuellement la sauvegarde de leur souveraineté et de leurs intérêts par de nombreux accords bilatéraux ou multilatéraux.

296. Identifier irrévocablement chaque citoyen composant une nation, tout en sauvegardant chacun des droits fondamentaux, c'est créer les dispositions nécessaires à la préservation d'une souverainement nationale, voire à l'échelle des unions[143], sur une base juridique solide et partagée.

7.1.3 Approche politique et économique : la souveraineté des opérateurs économiques

297. Selon cette approche de nature politique et économique, la souveraineté numérique serait celle des opérateurs économiques qui disposent de facto du pouvoir d'imposer des règles.

298. Quelques multinationales (GAFAM's) exercent aujourd'hui un véritable pouvoir de commandement et de réglementation dans le cyberespace. Elles fixent ainsi les conditions générales d'utilisation de services en ligne devenus indispensables, développent les algorithmes, décident de supprimer des contenus, de fermer le profil d'un utilisateur, de conserver ou de vendre les données personnelles dont elles assurent le stockage, etc.

299. Certaines créent leurs propres monnaies virtuelles (Bitcoin, projet Libra), et se dotent de leurs propres services juridiques de règlement des différends. D'autres bâtissent des projets de sociétés fondées sur le progrès technologique, où elles auraient vocation à rendre des services équivalents, voire supérieurs à ceux des États, ainsi remplacés.

---

[140] Karim Benyekhlef, L'Internet : un reflet de la concurrence des souverainetés, Lex Electronica, vol. 8, n° 1, automne 2002

[141] Par exemple dans l'entreprise, le contrat de travail et le règlement d'ordre intérieur viennent s'ajouter aux conventions collectives puis au droit applicable à l'entreprise, celui-ci étant déterminé par le secteur industriel auquel l'entreprise appartient, le territoire (potentiellement numérique) sur lequel elle exerce son activité et enfin sa nationalité (l'état).

[142] Système de Droit romano-civiliste ou Droit Napoléonien par opposition au Droit anglo-saxon ou common law.

[143] La Cour de Justice de l'Union Européenne a frappé un grand coup le 16 juillet 2020 en invalidant avec effet immédiat le « Privacy Shield » qui encadrait les échanges de données entre les Etats-Unis et l'Europe (CJUE arrêt C 311/18 dit Schrems II). La CJUE a ainsi envoyé un message à la fois aux autorités américaines qui peuvent se servir du « Cloud Act » pour accéder aux données de toutes les personnes surveillées, américaines ou non américaines et ce quel que soit le lieu de stockage de ces données tant que ces personnes sont clientes d'une société américaine… Mais également directement aux GAFAM qui collectent allégrement toutes les données personnelles de leurs clients.

300. ⚠ Grâce à l'identité numérique proposée nous pourrions fortement remettre de l'ordre dans cette anarchie, en épargnant notamment à l'utilisateur d'un site Web d'approuver à chaque fois une liasse de conditions d'utilisation opaques dont la finalité première est de capter un maximum de données personnelles le concernant et dont la masse de conditions légales n'est que contre-publicité à l'encontre des institutions européennes qui cherchent en réalité à protéger sa vie privée.

301. En effet, l'entreprise (la Communauté) au sein de laquelle la personne exerce une Fonction qui l'amène à utiliser un service Web peut prédéterminer les règles de confidentialité applicables, épargnant à son employé toute erreur en même temps que de s'assurer le niveau de protection qu'elle a choisi (en tant que personne morale) de ses actifs incorporels.

302. Le même employé peut, le soir même, utiliser le même service Web et cette fois – dûment identifié par son identité personnelle et non plus professionnelle - décider de profiter du service personnalisé grâce à un partage de son agenda « personnel » (son identité personnelle ne lui permettant par exemple, pas d'accéder son agenda « professionnel »). Voire, il peut aussi rejoindre une communauté « je-refuse-tout-traçage » purement virtuelle et s'identifier par ce biais pour profiter de la protection ad hoc de ses données personnelles sans avoir à éplucher les conditions d'utilisation du fournisseur de service.

7.1.4 Approche libérale : la souveraineté numérique des utilisateurs

303. Une troisième approche s'avère possible, plus libérale et individualiste : il s'agirait d'une souveraineté numérique des utilisateurs. Inspirée des fondements de la souveraineté populaire selon laquelle les citoyens sont la source de tout pouvoir, elle correspond au droit des personnes à s'autodéterminer.

304. Les utilisateurs peuvent effectuer des choix, exprimer des préférences, se détourner de certaines applications, peser dans des forums dédiés à la normalisation technique (par exemple le W3C, organisme de standardisation à but non lucratif, chargé de promouvoir la compatibilité des technologies du World Wide Web telles que HTML, XHTML, XML, etc.), ou plus simplement en tant que consommateurs.

305. Le pouvoir envisagé ici peut être exercé collectivement, dans le cadre de communautés d'utilisateurs (forums de développeurs SW transnationaux), dans le cadre d'une Fonction pour une entreprise ou à titre individuel[144].

306. La notion de souveraineté numérique ne se limite donc pas à la stricte perspective juridique classique, attachée au pouvoir des États. Elle renvoie dans son acception la plus large, au pouvoir de commandement et au droit à l'autodétermination dans un monde numérique. Qui fixe les règles ? Sur quel fondement et avec quelle légitimité ? À qui obéit-on, et avec quelles garanties ? Répondre à ces questions, c'est comprendre qui est souverain sur les réseaux et comment s'exprime cette souveraineté.

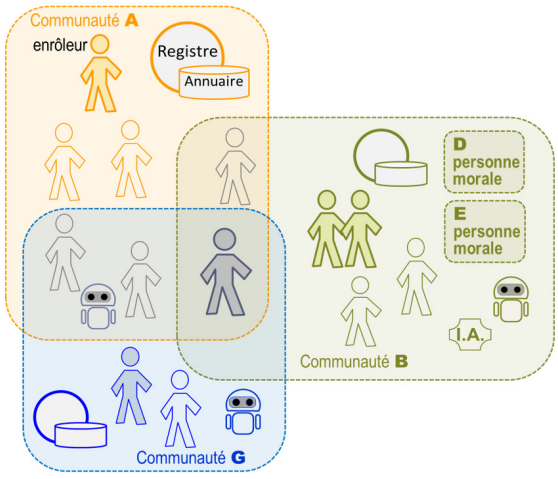
307. ⚠ Comment revendiquer une souveraineté de quelque nature qu'elle soit sans posséder une identité numérique irrévocable, recevable en droit (mandatée), et supranationale ?

7.1.5 Un écosystème de souverainetés communautaires concurrentes

308. Pour rappel, les Communautés de notre modèle sont les entreprises privées, les associations professionnelles, les instituts et organismes publics, l'État, voir des communautés purement virtuelles et potentiellement transnationales. L'État lui-même en fonction de sa taille et de son organisation administrative peut opter pour une méga communauté régalienne ou une sous-division en communautés départementales, provinciales, ou régionales.

309. Les Communautés étant le plus généralement des personnes morales, celles-ci auront non seulement une identité numérique propre (exercée au travers de leurs représentants légaux – mandatés dans ce rôle, une personne morale n'ayant pas de capacité à agir en propre), mais peuvent également prendre Fonction dans d'autres communautés.

310. L'intégration éventuelle de robots et d'IA dans le modèle devient toute aussi facile que celle des personnes physiques et morales (Figure ci-dessous).



[144] Il se traduit concrètement par des droits et garanties en cours de consécration tels le droit à la protection des données personnelles, à la portabilité des données, à l'oubli ou au déréférencement, qui pourraient être inclus dans un droit plus général à « l'autodétermination informationnelle » selon l'approche allemande, Pauline Türk, « Le droit à l'autodétermination informationnelle », Revue Politeia, 2017, n° 31.

7.2 Supranationalité et inter-opposabilité

311. L'usage croissant des Nouvelles Technologies de l'Information et des Communications (NTIC) a structurellement modifié les conditions juridiques de la démonstration de l'identité des internautes. En effet, les fournisseurs de ces technologies et des services y afférents ont laissé croitre l'usage des avatars et se sont satisfaits d'auto déclarations d'identité, souvent multiples et variées pour un seul et même individu. Il est désormais constant que cette situation est devenue intenable et s'avère contraire aux intérêts tant des fournisseurs que des usagers.

312. Pour pallier ce qui précède, et bien que la démonstration de la preuve de son identité soit clairement explicitée ci-dessus (régime de la preuve parfaite), se pose désormais la question de la territorialité du droit applicable. En effet, pourquoi le droit de tel pays prévaudrait-il sur celui de tel autre ? C'est l'ONU qui, au sein de la Commission de Nations Unies pour le Développement du Commerce International (CNUDCI), a posé les conditions d'acceptabilité du droit applicable en imposant le principe juridique de la supra nationalité. Ce principe fut accepté par les 193 pays composant l'ONU en 2005.

313. Par supranationalité, nous comprendrons qu'il s'agit du caractère de ce qui est placé au-dessus des institutions nationales, et dès lors, leur est opposable en droit.

314. C'est dans ce cadre supra national que la CNUDCI énonce 4 dispositions nécessaires :

- Il est essentiel que la personne souhaitant manifester la preuve de son identité ait la maîtrise pleine et entière de son moyen d'identification. Dès lors cet impératif exclut de facto toutes les solutions pouvant être manœuvrées volontairement ou non par toutes personnes pouvant prendre le contrôle directement ou indirectement du moyen de démonstration de la preuve : complicité de l'éditeur de logiciel, piratage, prise de contrôle à distance des outils électroniques par les opérateurs d'une infrastructure, ou simplement l'asservissement d'un serveur central de signature !;

- L'Interopérabilité impose, par définition, à chaque solution d'être compatible avec l'ensemble des systèmes en activité ; ceci s'entendant pour les logiciels, les cartes à puces, les périphériques de tout genre ;

- L'inter-opposabilité est la capacité pour toutes solutions d'identification de se conformer aux dispositions juridiques énoncées par la CNUDCI et être dès lors, recevables en justice devant les juridictions composant l'ONU ;

- La pérennité est la capacité à garantir dans le temps tant les services de démonstration de l'identité que les éléments constitutifs de la preuve.

7.3 Pour une identité numérique universelle

315. Nous avons vu précédemment qu'un document sur support papier ou sur un support numérique dispose d'une même valeur juridique dès lors qu'il respecte les mêmes règles de droit.
En l'espèce, s'agissant de l'identité numérique, nous avons constaté que le droit qui s'impose est celui de la preuve parfaite dans un environnement d'analyse de droit stricte ; autrement dit, toutes interprétations et/ou présomptions seront de nul effet.

316. La neutralité technologique est alors essentielle. La justice ne se focalisera sur les enchaînements techniques qui satisfont à la démonstration de la preuve que secondairement ; le principal étant de s'assurer que les grands principes de droit constitutifs des moyens de démonstration de la preuve de l'identité sont satisfactoires au dit régime de la preuve.

317. Il est constant que les lois et autres règlements successifs qui légifèrent quant à la formation de la démonstration de l'identité numérique énoncent des droits et des obligations des personnes de façon générique, sans égard aux moyens technologiques par lesquels s'accomplissent les activités visées. La loi est désintéressée du cadre technologique spécifique mis en place. La loi ne spécifie pas la technologie qui doit être usitée pour la réalisation et le maintien de l'intégrité des documents et l'établissement d'un lien de droit avec un document. De cette sorte, dans un souci de neutralité, elle n'avantage ni ne désavantage l'utilisation d'une technologie au détriment d'une autre.

318. La neutralité technologique signifie que la loi ne doit pas faire de discrimination entre les diverses techniques. La loi ne doit pas privilégier l'utilisation d'une technologie au détriment d'une autre. Autrement dit, la loi donne à toutes les techniques la même reconnaissance juridique en s'appuyant sur des conditions n'emportant pas l'obligation d'agir selon des normes ou standards particuliers.

319. Il importe de comprendre que la neutralité s'applique tant à la distinction entre papier et support numérique qu'à la distinction entre les technologies elles-mêmes. C'est l'universalité technologique.

320. Il n'y a pas de frontière sur internet. Dès lors se pose la question de la territorialité juridique opposable en justice en cas de litige. C'est alors que le droit supranational intervient au secours des difficultés de compétence territoriale. Comme évoqué, c'est l'ONU, et plus précisément la CNUDCI, qui a posé les conditions d'acceptabilité du droit applicable en imposant le principe juridique de la supra nationalité.

321. Cette même commission a soulevé la question du contrôle monopolistique par un État de l'identité. Elle a conclu que, s'agissant de l'identité numérique, aucun État ne devra en posséder le monopole, laissant ainsi au marché le choix et la compétition dans les offres de service.

322. Un second pas vers une universalité de l'identité numérique était franchi, c'est l'universalité géographique.

323. Dans un même esprit d'universalité, à considérer que l'identité numérique irrévocable soit acquise, son usage devra s'imposer pour tous les services numériques en ligne, considérant l'interopérabilité autant que l'inter-opposabilité. Il s'agit de l'universalité d'usage.

324. ⚠ Le modèle de référence proposé est à ce titre neutre sur tous ces plans et donc propre au support d'une identité universelle. Les spécifications de mise en œuvre (dont la publication sort du cadre du présent livre blanc) restent tout aussi neutres quand elles s'en tiennent aux interfaces nécessaires à l'interopérabilité : structure de l'Identifiant, interfaces des Dispositifs, structures des Assertions.

7.4 Faciliter la Cybersécurité

325. Wikipédia propose une définition pratique : la cybersécurité est définie comme « l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non-répudiation) ».

326. Si on entre un peu plus dans le détail, on pourrait compléter cette définition par les différents contextes dans lesquels la sécurité est appliquée. On peut par exemple parler de :
- Sécurité du réseau qui comprend les politiques et les pratiques adoptées pour contrôler les flux de données à l'intérieur du réseau et aux points d'accès, éviter les engorgements (attaques « denial of service ») et protéger sa configuration de façon à éviter les détournements d'adresses ou de noms de machines.
- Sécurité des applications qui vise à protéger les logiciels, les appareils et les objets connectés.
- Sécurité des informations qui veille à garantir l'intégrité, la confidentialité et la disponibilité des données en transit ou au repos dans un système d'information.

327. La cybersécurité s'adapte au fur et à mesure de l'évolution des cybermenaces. Avec la crise sanitaire liée à la COVID19, le niveau des attaques informatiques a littéralement explosé à travers toute la planète, profitant des connexions à distance d'ordinateurs personnels via des réseaux domestiques peu sécurisés, ainsi que d'une facilité de phishing via des annonces liées à la COVID19 pour lesquelles tout le monde est concerné. Les crypto-monnaies, dont l'échange est anonyme, ont rendu très populaires les attaques de chiffrement / déchiffrement contre rançon. L'exfiltration de données personnelles ou sensibles revendues sur le « dark web » est devenue un marché très lucratif pour les pirates.

328. Il n'est de surcroît plus nécessaire d'être un expert pointu en informatique, des outils de piratage prêts à l'emploi peuvent être achetés, régulièrement mis à jour pour intégrer les dernières failles informatiques exploitables, ou sous forme de cheval de Troie en lien avec une campagne de phishing.

329. Les risques ne sont plus individuels : ils peuvent couler une entreprise, voire causer des dommages à un État entier (perturbations des infrastructures de distribution d'électricité, ou d'eau, attaque des marchés financiers, attaque des réseaux de communication, perturbation de la gestion du trafic air / rail / routes, systèmes de santé, etc.), ou même, venir perturber l'exercice de la démocratie[145] (diffusion d'informations manipulées, influences et incitations, altération des élections).

330. Dans tout ce contexte, ce n'est pas l'absence d''identité' qui pose problème, mais le caractère non fiable de celle-ci. La faculté de se faire passer pour un autre est à la base de la très grande majorité des attaques, qu'il s'agisse de prendre l'identité d'une personne (source d'un courriel ou d'un publipostage), d'une entreprise (phishing, escroqueries, logiciels frauduleux), ou plus techniquement d'un système à l'origine d'une attaque (adresses IP), ou encore l'identité d'un site web (noms de domaines).

[145] « Des utilisateurs de Facebook « manipulés » pour une expérience psychologique », Lemonde.fr, 30 juin 2014 et William Audureau, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », Lemonde.fr, 22 mars 2018.

331. ⚠ L'identité numérique proposée permet d'identifier tant les personnes, que les entreprises (personnes morales) et les systèmes ou objets connectés, et de connaître pour ces derniers le mandant, personne physique ou morale judiciable. La fiabilité de ces identités est alors la clé d'une réduction potentielle considérable des attaques informatiques.

332. En effet, il ne sera pas nécessaire de connaître personnellement son interlocuteur (personne, entreprise, ou système) si l'on sait avec certitude que ce dernier ne peut échapper à ses responsabilités. L'inconnu peut être digne de confiance si on acquiert la certitude qu'il est imputable, parce que l'identité qui sera donnée est irrévocable.

7.4.1 Cas du courrier électronique

333. Il est désolant que ce vecteur de communication (e-mail, tweets, clavardage, forums, etc.), si simple d'emploi, si vulgaire d'usage, premier moyen d'échange d'information et outil de lien social, soit devenu, grâce à l'anonymat électronique, le terrain privilégié des cybercriminels : il est temps de repenser le droit et de créer les moyens d'identification des acteurs œuvrant sur les réseaux.

334. Que serait devenu le réseau routier sans plaque d'immatriculation ? Le chaos. Il suffit d'une brève expérience au sein d'une équipe de support informatique en charge des passerelles de courrier électronique d'une grande entreprise pour s'en rendre compte : le chaos résulte de l'anonymat, et celui-ci prend sa source dans les carences des protocoles Internet ad hoc[146] dont la conception – remarquable par la simplicité de sa mise en œuvre – n'a pas du tout anticipé les questions de détournement de ces protocoles dans une volonté de nuire ou même seulement de profit.

335. Le filtrage des courriels devient très simple : tout ce qui ne relève pas d'une Identification certaine passe à la poubelle ; nul besoin de connaître son correspondant, nul besoin de filtrer les noms, ni de gérer des listes noires, tout courriel devient 'opposable' par nature et donc imputable en dommages et intérêts.

336. Pourquoi devrait-on accepter de régresser avec les tracts électroniques qui envahissent nos boîtes aux lettres, une majorité de ceux-ci étant de plus malveillants ? 60% du courriel entrant dans les passerelles de messagerie électronique des entreprises est indésirable ; 95% de ceux-ci, voire plus, sont rejetés par les filtres anti-spam avant même d'atteindre leur destinataire, mais il en restera toujours pour passer à travers les filtres, notamment ceux qui empruntent l'identité — actuellement «invérifiable» — de vos correspondants

7.4.2 Identité + Sécurité = Sûreté

337. L'identité numérique opposable en droit, supranationale, garante de la protection totale des données personnelles, est une nécessité absolue dont l'industrie numérique ne saurait s'exonérer plus avant.

●

[146] ESMTP et consorts.

8. BIBLIOGRAPHIE

Bernard Benhamou (coord.), Internet des objets et souveraineté numérique: perspectives industrielles et enjeux de régulation, Institut de la souveraineté numérique-Afnic, 2021

P. Bellanger, La souveraineté numérique, Stock 2014

A.Bensoussan, V. Bensoussan Brulé et J. Bensoussan., Jurisprudence Données personnelles - Décisions tendances 2018-2020Lexing Editions, 2021

A. Bensoussan, Informatique et libertés, Editions Francis Lefebvre, 3e éd., 2020

A. Bensoussan et J. Bensoussan, IA, Robots et Droit, Bruylant, 2019

A. Bensoussan, A. (direction), Informatique Télécoms Internet, Editions Francis Lefebvre, 6e éd., 2017

K. Benyekhlef, L'Internet : un reflet de la concurrence des souverainetés, lex-electronica.org, Éd., 2002

N. Chambardon, L'identité numérique de la personne humaine. Université Lyon 2, Ecole doctorale de droit, 2018 https://hal.archives-ouvertes.fr/tel-02464483/document

M. Karamanli, C. Hennion et J.-M. Mis, Rapport d'information N°3190, par la mission d'information sur l'identité numérique. Assemblée Nationale, 2020

B. Mallet-Bricout et T. Favario, L'identité, un singulier au pluriel, Dalloz, 3, Éd., 2015

G. Montagnier, R. Guillien et S. Guinchard, Lexique des termes juridiques, Dalloz, 16 e éd., 2007.

L. Pauliac, Signature électronique : naissance du « faux faux » et du « faux conforme », 2017 https://www.linkedin.com/pulse/signature-%C3%A9lectronique-naissance-du-faux-et-conforme-lucien-pauliac/

L. Pauliac, Le numérique, l'archivage, et la preuve. https://www.scriptum-archives.fr/pauliac.html

P. Türk et C. Vallar, La souveraineté numérique : le concept, les enjeux, Ed. Mar & Martin, 2018.

9. ANNEXES

ANNEXE 1 : LE SECRET DES AFFAIRES ET DES CORRESPONDANCES

1. Le secret des affaires et des correspondances

A condition que les dispositions relatives à la démonstration de l'identité d'une personne physique ou morale satisfassent aux conditions ci-dessus énoncées (preuve parfaite, protection des données, supranationalité), l'identification est de nature à satisfaire aux conditions de la sauvegarde du secret des affaires ainsi que celui des correspondances en identifiant les auteurs desdites informations ainsi que les accédants aux informations, et ce, de façon irrévocable.

2. Définition du secret des affaires

L'article L. 151-1 du Code de commerce pose trois critères pour définir le secret des affaires.

Une information est protégée par le secret des affaires si les critères cumulatifs suivants sont remplis :

- Elle n'est pas généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leurs secteurs d'activités ;
- Elle revêt une valeur commerciale effective ou potentielle qui résulte de son caractère secret ;
- Elle fait l'objet de mesures de protection raisonnables pour demeurer secrète, compte tenu des circonstances.

Sont susceptibles de constituer un secret d'affaires : un savoir-faire, une connaissance technologique ou technique ou bien encore des données commerciales. L'information n'est protégée qu'à la condition d'être détenue de manière légitime ou d'avoir été obtenue de manière licite..

3. La protection judiciaire du secret des affaires

Une personne qui porte atteinte au secret des affaires engage sa responsabilité civile. Le délai de prescription est le même qu'en droit commun, soit de 5 ans.

4. Le secret des correspondances

La correspondance est un échange oral ou écrit entre plusieurs personnes.
Juridiquement elle est par essence considérée comme étant de nature privée. Par principe, il est interdit de la rendre publique. Ce principe vise le « secret des correspondances » et trouve son application dans des textes qui font référence à la protection de la vie privée. Ainsi, il est protégé par l'article 9 du Code civil qui dispose « chacun a droit au respect de sa vie privée », ou par l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales qui vise le respect à la vie privée et familiale.
Ainsi, toute transmission, y compris sous forme de messages électroniques est strictement restreinte à leurs destinataires. La loi réprime sévèrement tout manquement au secret de la correspondance. La jurisprudence a cependant pu considérer qu'il existe des degrés de confidentialité dont l'appréciation relève du pouvoir souverain des juges.
Le Code pénal (article 226-15) réprime le fait, commis de mauvaise foi :

- d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance ;
- d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

Le cas échéant, la violation du secret est punie des peines maximales de trois ans d'emprisonnement et de 45 000 euros d'amende.

ANNEXE 2 : L'E-RÉPUTATION

Quand une entreprise n'a pas mis en œuvre les mesures de sécurité techniques suffisantes, un vol de données peut avoir des conséquences juridiques importantes depuis la mise en œuvre du Règlement Général de Protection de Données (RGPD)

Ce Règlement prévoit en effet que la CNIL peut prononcer en France des sanctions financières pouvant s'élever à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial.

La CNIL a ainsi prononcé plusieurs sanctions financières à l'encontre de sociétés en raison de manquements avérés quant à leurs obligations de sécurité sur les données personnelles de leurs clients [147].

Par exemple en décembre 2018, une société de transport de personnes avec chauffeur (VTC) a été condamnée à une amende de 400 000 euros suite au vol des données de 57 millions de ses utilisateurs. La plateforme avait pourtant été informée d'une première attaque l'année précédente et avait accepté de payer aux pirates la somme de 100 000 euros afin qu'ils ne révèlent pas cette faille à leurs utilisateurs et qu'ils suppriment les données dérobées.

Raté... La même attaque s'étant reproduite quelques mois plus tard, la CNIL a justement reproché à la société de n'avoir pas pris les mesures de sécurité suffisantes pour protéger les données personnelles de ses clients.

Quelles ont été les failles de sécurité exploitées par les pirates dans cette affaire ?

La CNIL a détaillé dans sa décision les modalités de l'attaque.

L'attaque trouve son origine sur la plateforme collaborative GitHub, plateforme de travail privée utilisée par les ingénieurs logiciels de la société de VTC et sur laquelle leurs identifiants étaient stockés en clair. Le nom d'utilisateur était ainsi composé de leur email personnel, accompagné d'un mot de passe individuel.

Les attaquants ont ainsi utilisé ces identifiants pour se connecter à la plateforme GitHub sur laquelle ils ont trouvé une clé d'accès en clair permettant d'accéder à la plateforme d'hébergement sur laquelle étaient stockées les données à caractère personnel des utilisateurs de la société de VTC. Cette clé a également permis aux attaquants d'accéder aux bases de données de la société et ainsi de dérober les données personnelles de millions d'utilisateurs.

La formation restreinte de la CNIL relève que l'accès aurait dû être encadré par des règles de sécurité adéquates, tant au regard des mesures d'authentification que des retraits d'habilitation des anciens ingénieurs, actions non mises en place par la société de transport de VTC.

Enfin, la formation restreinte de la CNIL considère que la sécurisation de la connexion aux serveurs « Amazon Web Services S3 » constitue une précaution élémentaire et qu'un filtrage des adresses IP aurait permis d'éviter ces connexions illicites.

Plus récemment, la CNIL a prononcé une sanction financière contre une société de gestion immobilière. Ainsi en mai 2019[148], la société est condamnée à une amende de 400 000 euros pour ne pas avoir sécurisé les données personnelles de ses clients. Cette sanction faisait suite à un contrôle du site web de la société dans lequel des documents contenant les données personnelles des candidats à la location d'appartement étaient librement accessibles, sans authentification préalable pour tous les visiteurs du site. Il suffisait pour cela de modifier légèrement l'adresse URL affichée dans leur navigateur.

[147] Pour une analyse, Cf. A.Bensoussan, V. Bensoussan Brulé et J. Bensoussan, Jurisprudence Données personnelles - Décisions tendances 2018-2020, Lexing Editions, 2021.

[148] Cnil 28 mai 2019, Délib. SAN-2019-005, confirmée par CE 4 novembre 2020, req. n° 433311

On peut également citer des affaires de piratage étrangères et qui ont eu un effet dévastateur sur la sécurité des données personnelles allant même jusqu'à provoquer des suicides. Par exemple le piratage du site de rencontres « Ashley Madison » qui a eu lieu en 2015 aux Etats-Unis.

Dans cette affaire la base de données de 37 millions de clients de ce sulfureux site contenant les noms, les adresses mails et même les préférences sexuelles des utilisateurs ont été divulgués sur internet, les utilisateurs ayant eu à subir de nombreuses tentatives de chantages poussant notamment un pasteur au suicide.

Après enquête des autorités de protection de la vie privée australiennes et canadiennes, il s'est avéré que le système de sécurité et de confidentialité de ce site n'était pas à la hauteur. On citera par exemple une absence des mises à jour de sécurité des différentes bases de données, une absence de mesures de détections d'attaques informatiques et des sauvegardes de données conservées ad vitam aeternam par l'éditeur de ce site même dans les cas où le membre a supprimé son compte...

Autre piratage retentissant, la compagnie d'assurance américaine « Anthem » s'est fait dérober fin 2015 ses informations personnelles (noms, pseudonymes, login et mots de passe et peut être des données bancaires et ou médicales) de 80 millions de ses clients. Les pirates ont alors utilisé ces données pour tester les login / mots de passe sur d'autres services d'authentification et pour organiser des campagnes de phishing.

L'ensemble de ces affaires démontre bien que le couple d'authentification Login / Mot de passe si robuste soit-il ne suffit plus à assurer une totale sécurité numérique des internautes.

Ainsi, même quand les internautes choisissent des mots de passe complexes en respectant les normes de robustesse notamment recommandées par la CNIL (8 caractères au minimum, utilisation de lettres majuscules et minuscules et de caractères spéciaux, durée de validité de 6 mois maximum), les données peuvent être directement volées sur les serveurs des entreprises.

Impression : Imprimerie Bialec SAS
23 All. des Grands Pâquis,
54180 Heillecourt

Décembre 2021

Crédit image
Fotolia - Adobe Stock

LEXING
ALAIN BENSOUSSAN AVOCATS

Lexing Alain Bensoussan Avocats
58, boulevard Gouvion-Saint-Cyr
75017 Paris France
Tél : +33(1) 82 73 05 05
Fax : +33(1) 82 73 05 06
Mob. : +33(6) 74 48 13 25 / +33(6) 74 17 60 04
www.alain-bensoussan.com

A³BC

Plaidoyer pour une IDENTITÉ NUMÉRIQUE

Le Livre Blanc sur l'identité numérique 5.0 propose une base de construction d'identités numériques dans le cadre de communautés souveraines tant à l'échelle d'un État que d'une société commerciale, ou encore d'un simple groupe d'intérêt.

Il se veut un plaidoyer pour une identité numérique :

- apte à assurer « une circulation de l'information opposable en justice », permettant autant de faire valoir ses droits que de se protéger des abus, sans pour autant échapper à ses obligations ;

- apte à garantir la protection de la vie privée, en cela que tout usage de l'identité en liaison avec une information numérique découlera de sa volonté en toute souveraineté ;

- apte à protéger ses actifs incorporels, en cela qu'il n'y aura – si il le décide – plus de flou quant au propriétaire de ses données et leur partage éventuel ;

- apte à défendre la démocratie en séparant clairement les informations dont la source est identifiée (et responsable) des informations anonymes voire altérées, détournées, ou inventées ;

- apte à identifier tous les acteurs de la vie économique et sociale : personnes physiques, personnes morales, mais également robots autonomes et «créatures» du monde numérique (IA avec laquelle on interagit déjà) et qui ne peuvent donc échapper à leurs responsabilités.

- apte à instaurer un système de confiance numérique par et au service des entreprises, dotant tous les acteurs publics/privés de la capacité de reconnaissance mutuelle, créatrice de la confiance indispensable au bon déroulement des affaires.

Alain Bensoussan,
Avocat à la Cour d'appel de Paris,
Alain Bensoussan Avocats Lexing

Philippe Morel,
Spécialiste de l'identité numérique,
co-fondateur de Woobe

Bernard Hauzeur,
Architecte informatique, expert en sécurité et
identité numérique, co-fondateur de Woobe

Dinesh Ujoodah,
CEO d'A3BC

Anthony Sitbon,
Consultant, Directeur du département Sécurité,
Alain Bensoussan Avocats Lexing

Frédéric Forster,
Avocat, Directeur du pôle Télécoms,
Alain Bensoussan Avocats Lexing