www.jusletter.ch

Gabriel Jaccard

Partie I : L'identité digitale et la création du surhomme 2.0

Cette contribution est la première partie d'une étude qui porte sur le thème de l'identité. Dans ce premier volet, l'auteur aborde les problématiques juridiques liées à l'identité digitale. Le travail expose la législation sur l'identité digitale en Suisse et celle prévue par l'avant-projet de la loi fédérale sur les services d'identification électronique (Loi e-ID). Les problématiques juridiques étudiées portent sur le statut de l'identité digitale ainsi que les différents types de supports sur lesquels elle peut se greffer.

Catégories d'articles : Essais
Domaines juridiques : Informatique et droit ; Protection des données

Proposition de citation : Gabriel Jaccard, Partie I : L'identité digitale et la création du surhomme 2.0, in : Jusletter 30 avril 2018

ISSN 1424-7410, https ://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Table des matières

I. Introduction

[Rz 1] En ce début de 21ème siècle, le héros moderne code sa réalité. En ce sens, les aventuriers de la *Tech*, sont les dignes héritiers des chercheurs d'or arrivés au milieu du 19ème siècle en Californie. Déterminés, et ne partant souvent de rien, ils sont comme eux prêts à bâtir de nouveaux paradigmes au travers de leur seule volonté. Toutefois, si l'imprimerie inventée au 15ème siècle, ou l'IPhone sorti en 2007, visait à apporter un silex de plus à la trousse à outils des Hommes, les projets actuels relèvent d'une toute autre ampleur.

[Rz 2] Notre sujet porte sur l'identité et se scindera en deux volets. Le premier porte sur le thème de l'identité digitale et le second sur l'humanité augmentée. En quoi cela consiste-t-il ? La première notion vise à la création d'un nouveau type d'identité qui délivrera à toute personne une existence véritable au sein des systèmes digitaux. Le deuxième étudiera la problématique de l'humanité augmentée, qui vise à décupler les capacités humaines grâce à tous les moyens, appareils et programmes qui nous entourent ou qui font parties intégrantes de notre personne. A titre d'exemple, on peut prendre les pacemakers intelligents reliés aux numéros des secours ou encore l'utilisation de l'intelligence artificielle pour améliorer la réflexion humaine.

[Rz 3] Ces technologies, prometteuses et controversées, n'arrivent pas sans attiser de houleux débats tant d'un point de vue moral, politique ou juridique, dont les résolutions se révèlent bien différentes en fonction de la culture et des sensibilités vers lesquelles on se tourne. En effet, quel regard porter sur des innovations qui chamboulent à chaque instant un peu plus le cap de l'humanité ? Nous tenterons de poser les bases des éléments de réponse, bien que, nous le verrons, les approches prudentielles ou progressistes se valent facilement face à une multitude de dilemmes Cornéliens et d'incertitudes.

[Rz 4] En effet, les questions que nous aborderons touchent du bout des doigts à ce que Nietzsche appelait la quête du surhomme (*übermensch*). Bien que le concept Nietzschéen ne vise pas l'évolutionnisme en tant que tel, à savoir une création biologique ou artificielle d'un homme supérieur, l'évolution technologique de l'humanité augmentée et de l'identité digitale reproduit à notre sens le chemin intérieur que les Hommes modernes prennent en direction d'une sorte de transcendance. Sur cette terre, plutôt que dans les cieux, certains veulent mettre toute leur volonté à se compléter, à se dépasser, et à exister autrement, afin d'être un peu moins Bête et un peu plus Homme. Cette tension entre l'Homme et le chemin qui le métamorphose en un être supérieur doit être un espoir dans un monde de plus en plus nihiliste ; bien que, à l'image du danseur de corde dans Zarathoustra[1], cette performance ne soit dénuée de risques pour personne.

[Rz 5] Au terme du présent travail, nous exposerons les problématiques légales liées à l'identité digitale (*Infra* nºII). Nous étudierons plus avant les diverses méthodes d'intrication qui existent comme l'implantation, la portabilité et les registres externes.

[Rz 6] Enfin, nous illustrons notre propos tout le long de notre travail avec des scènes de l'une des expressions modernes de la quête du surhomme, celle du film Matrix, soit l'histoire d'un homme qui naît *Anders(on)* (un autre), et qui devient *Neo* (le nouveau).

1 Friedrich Nietzsche, *Also sprach Zarathustra*, N6 s.

II. L'identité digitale

Agent Smith :
It seems that you've been living two lives.

In one life, you're Thomas A. Anderson, program writer for a respectable software company, you have a social security number, you pay your taxes, and you help your landlady carry out her garbage.

The other life is lived in computers, where you go by the hacker alias Neo and are guilty of virtually every computer crime we have a law for.

One of these lives has a future, and one of them does not.

[Rz 7] Dans la première section, nous nous intéressons premièrement à définir et à délimiter l'identité digitale (*Infra* n°1). Puis, nous explorerons le cadre juridique de l'identité digitale (*Infra* n°2), avant d'étudier les divers supports sur lesquels on la retrouve (*Infra* n°3).

1. Définition & délimitations

1.1. L'identité physique & intellectuelle

[Rz 8] La question de l'identité est celle d'une quête intérieure. Les maximes résonnantes comme « *Qui suis-je ?* » ou « *Connais-toi toi-même* » participent au fondement de notre identité et au passage vers la création de la personnalité humaine. C'est un chemin ombragé et délicat, dont le développement mérite toute la considération du droit, qui doit aussi servir à le protéger. Mais le concept de l'identité est difficilement saisissable *in extenso* en quelques aphorismes. Qu'est-ce qui vous définit le plus : une carte d'identité ? Une guitare ? Un casier judiciaire ? L'avis de vos amis ? Un historique internet ? Une photo ? Une bibliographie ? Un parfum ? Un compte Instagram ? Est-

ce que tous ces éléments réunis réussiraient à former le contenu de votre identité ou le reflet de son contour seulement ?

[Rz 9] « *Mais où est donc ce moi, s'il n'est ni dans le corps, ni dans l'âme ?* »[2]. Cette question, est de nature philosophique et il ne nous appartient pas ici d'y répondre. En effet, ce travail ne porte pas sur l'identité humaine physique et intellectuelle d'une personne en tant que telle – par ailleurs indirectement traitée dans son volet juridique au travers de la personnalité aux art. 11 ss du Code civil suisse (CC) et des art. 10 ss de la Constitution fédérale de la Confédération suisse (Cst.) – mais bien plus sur l'une de ses expressions parallèles : « *l'identité digitale* ».

1.2. Les identités légales, digitales et virtuelles

[Rz 10] Grâce à la montée en puissance d'internet, de nouveaux types d'identités fleurissent sous des lexiques divers et dont les contenus se recoupent souvent. Principalement, on les rassemble sous le terme d'identité digitale et d'identité virtuelle[3], ou encore « *numériques* », notamment en France.

[Rz 11] On notera au préalable pour le lecteur que le terme *identité* se réfère aux caractéristiques qui se rapportent à une personne (âge, sexe, nationalité)[4], tandis que *l'authentification* se rapporte à la vérification conforme de cette identité avec celui qui l'allègue (1=Nombre indéfini) et dernièrement la *vérification* consiste à comparer les données fournies avec une donnée référentielle (1=1). Du reste, quant au terme « *système digital* », on doit l'entendre au sens littéral, à savoir « *qui se trouve au bout des doigts* ».

[Rz 12] Dans un premier temps, il nous faut définir *l'identité digitale lato sensu*, soit : « *l'ensemble des données qu'émet, volontairement ou non, une personne physique ou morale*[5] *au sein des systèmes digitaux* »[6]. Ces données forment les traces du passage d'une personne. Selon nous, il convient de distinguer deux sous-catégories au moins, traitées en détail plus bas, à savoir *l'identité digitale stricto sensu* et *l'identité virtuelle*. Ceci posé, notons que l'identité digitale *lato sensu* est trop conséquente pour le cadre de la présente contribution. En effet, celle-ci englobe des notions telles que les données de géolocalisations laissées par les téléphones, les photos de vos vacances sur les réseaux sociaux, etc.

---

2 PascalBlaise, Pensées, *Qu'est-ce que le moi ?*, Laf. 688, Sel. 567.

3 Les sociologues proposent trois dimensions aux identités virtuelles et digitales « L'identité déclarative, qui se réfère aux données saisies par l'utilisateur. L'identité agissante, qui est indirectement renseignée par les activités de l'utilisateur sur la toile. L'identité calculée, qui résulte d'une analyse de l'identité agissante par le système ». GeorgesFanny, L'identité numérique dans le web 2.0, in : Le mensuel de l'université no 27, juin 2008.

4 Par ailleurs, on peut définir l'identité de manière générale : « *Persistence of something, as being definable, recognizable* ». Voir Nick Bostrom, Anders Sandberg, The Future of Identity, 2011 Report, Commissioned by the UK's Government Office for Science, p. 7.

5 N.B. Cette contribution est développée sous l'angle de la personne physique. Cependant, il n'est pas inintéressant de noter que l'identité digitale et virtuelle de la personne morale revêt aussi une grande importance. Par exemple, on peut observer pour l'identité virtuelle que les entreprises actuelles sont très alertes sur la question de leur « e-reputation ». Par ailleurs, on peut remarquer une émergence de la reconnaissance de l'identité des entreprises au sein des canaux technologiques. Par exemple, dans le cadre du droit des marques, l'enregistrement d'une entreprise sur les domaines internet de premier niveau lui donne un droit préférentiel à obtenir ce nom. Concernant l'identité digitale, nous sommes favorables à la création d'une identité digitale propre et indépendante pour les personnes morales dès lors que le droit donne déjà fictivement la personnalité juridique à ces dernières.

6 Voir par exemple la définition du Boston Consulting Group, *The value of our digital identity*, 2012, p. 4. (ci-après « *BCG, p. X* ») : « *the sum of all digital information available* »

[Rz 13] Bien plus, notre intérêt porte sur une de ces sous-sections, soit *l'identité digitale stricto sensu* sous un angle légal, à savoir « *l'ensemble des données formant l'identité d'une personne physique qui lui permettent de s'authentifier authentiquement et de manière légale* ». C'est dans ce sens que nous utiliserons le terme identité digitale tout au long de ce travail.

[Rz 14] En soit, d'une part, il s'agit de prouver que c'est bien *un tel* qui est représenté[7] au travers d'un paquet de données. Et d'autre part, qu'un tiers de confiance a vérifié l'authenticité de ce paquet de données comme étant lié à cette personne, au cours d'un processus juridique établissant une fiction légale équivalente à celle requise pour l'établissement de l'authentification *de visu*. C'est-à-dire en un mot une « *carte d'identité digitale* » équivalente à la présentation de votre carte d'identité physique. Dès lors, pour rentrer dans cette catégorie, peu importe que l'identité digitale revête la garantie d'un degré d'authentification bas ou élevé, pourvu qu'elle soit légalement reconnue[8].

[Rz 15] Dans un deuxième temps, nous pouvons distinguer *l'identité digitale stricto sensu* de l'*identité virtuelle*. En effet, cette dernière ne permet, ni ne s'occupe véritablement, ou suffisamment, d'authentifier l'identité sous-jacente d'une personne. Par conséquent, comme mentionné au paragraphe précédent, le critère essentiel de la qualification d'une identité digitale face à une identité virtuelle est celui de l'identification d'une personne au travers d'un processus légal jugé suffisant.

[Rz 16] Dans un troisième temps, il convient maintenant de faire quelques remarques sur la nature de *l'identité digitale stricto sensu*, dont la teneur s'applique de même pour l'identité virtuelle et légale *mutatis mutandis*. Tout d'abord, on peut triplement qualifier l'identité digitale de multiple, de fragmentée et de fictive. D'une part fragmentée, car elle peut exister en plusieurs endroits[9]. Multiple, car en effet, bien qu'elle se rapporte à un seul individu, son contenu est potentiellement différent en fonction du registre dans lequel l'information est stockée[10]. Et finalement, l'identité digitale est fictive, car à l'image d'une carte d'identité, elle ne nous représente pas à proprement parler.

[Rz 17] Dernièrement, il nous faut dire un mot en général sur la question des degrés d'authentification. De manière générale, le niveau d'identification et d'authentification tel qu'apporté par l'identité digitale, en comparaison avec celui de l'identité virtuelle, n'est pas nécessaire dans de nombreuses relations juridico-sociales. Tout dépendra de la relation, des exigences du domaine concerné et de la volonté des parties[11]. On rappellera que le droit suisse a pour règle la liberté contractuelle, hormis les cas où une forme spéciale est prescrite.

[Rz 18] Par exemple, dans le cadre des jeux vidéo en ligne, l'authentification requise nécessite principalement la titularité d'un droit d'accès, peu importe son utilisateur. Généralement, il

7 On note qu'il est difficile d'établir l'identité de personnes sur internet précisément car le système ne connecte en soi pas à des *gens* entre eux, mais seulement à des *machines*. Cette particularité qui fait abstraction des personnes avait amené Kim Cameron, Chief Architect of Identity de Microsoft, à parler de « *missing identity layer* ».

8 Voir point II.2.3 ss pour des exemples.

9 Ex. un serveur de banque, la clé cryptographique d'un email, etc.
Voir :https ://www.letemps.ch/opinions/2017/11/16/lidentite-numerique-suisse-estelle-soluble-paranoia
(tous les liens ont été consultés le 16 avril 2018).

10 Les registres conservent généralement l'information de manière centralisée, par exemple sur un serveur informatique unique. A l'inverse la Blockchain propose des modèles de conservation des données dis « *décentralisés* ».

11 Par exemple, l'utilisation d'un mot de passe (plus ou moins difficile), d'un pseudonyme, d'un téléphone, d'un appareil biométrique, d'un titre (ex. une carte de crédit sans contact), d'une donnée personnelle, etc.

s'agira d'un pseudonyme, un mot de passe, et d'avoir acheté le jeu. On pourrait alléguer que l'identité d'une personne est établie dès lors que celle-ci communique ses informations bancaires lors de l'achat, car les intermédiaires financiers ont l'obligation légale d'authentifier leurs clients via des *onboarding procedure*, notamment pour des raisons de lutte contre le blanchiment d'argent. Toutefois, le joueur et l'acheteur ne sont pas forcément identiques. Partant, les activités menées et l'identité requise dans le jeu vidéo relèvent par conséquent d'une identité virtuelle, car même si l'identité du joueur peut être établie avec quasi-certitude via les données du service de paiement, cela n'est pas pour autant l'assurance irréfragable de l'identité d'une personne[12].

[Rz 19] De même, dans le cadre du e-commerce, l'achat d'un livre au travers d'un compte Amazon, en fournissant des données véridiques sur l'acheteur, mais non nécessaires (ex. adresses, noms, prénoms), permet au service d'Amazon de fonctionner correctement. Toutefois, ni le vendeur ni Amazon ne se soucient en réalité de la véritable identité de l'acheteur[13], subjectivement cette dernière ne forme pas une condition essentielle du contrat, bien qu'elle soit objectivement nécessaire à sa conclusion. Dans ce cas là encore, l'identité doit être qualifiée de virtuelle car les données sont probablement véritables et véridiques, mais non-vérifiées et non-requises au sein de la relation juridique *ad hoc*.

2. Aspects juridiques

2.1. L'intérêt juridique de la question

[Rz 20] En préambule, il convient d'expliquer pourquoi la notion d'identité est importante juridiquement. On le verra, celle-ci est cruciale en ce qui concerne le développement de services et d'applications efficaces et sécurisés.

[Rz 21] En premier lieu, l'identité en général est une question de droit public. En effet, il est nécessaire à tout Etat de reconnaître qui sont les citoyens et les étrangers qui forment sa population (art. 38 de la Constitution fédérale [Cst.]). Cette qualification a, par la suite, des conséquences juridiques pour les uns et les autres, leur imposant ainsi des droits (ex. droit de vote) et des obligations (ex. obligations militaires).

[Rz 22] Deuxièmement, l'identité a un intérêt pratique accru dans toute sorte de relations juridiques publiques ou privées. En effet, elle permet alors de reconnaître ou d'accorder clairement la titularité de droits, d'obligations, ainsi que par exemple le droit à la fourniture de services. De plus, ajoutons que le droit des obligations peut prévoir que la conclusion de certains contrats doit avoir lieu *intuitu personae*[14]. Par ailleurs, la connaissance des parties qui concluent le contrat est un élément essentiel (art. 1 de la loi fédérale complétant le Code civil suisse ; CO) de ce dernier.

12 Par exemple, acheter un jeu avec la carte de crédit de qqn d'autre (ses parents, amis, ...).

13 Dans les faits, les données de facturation (ex. carte de crédit) permettraient de se renseigner indirectement auprès de l'intermédiaire financier sur la véritable identité de l'acheteur. Toutefois, l'intérêt du vendeur ne se trouve souvent pas dans l'identité de son débiteur mais bien plus dans l'assurance du versement du paiement de la transaction. C'est pourquoi, l'utilisation d'une autre identité que la sienne – par exemple via la carte de crédit d'un ami, ou encore via un paiement mobile ou carte prépayée, sans qu'une trace de l'identité n'en ressorte – ne change rien à la validité du contrat, et ce malgré la nécessité de connaître les parties dans un contrat selon l'art. 1 de la loi fédérale complétant le Code civil suisse du 30 mars 1911 (CO ; SR 220). En effet, dans la pratique des contrats conclus sur internet, c'est donc le financement que l'on cherche à garantir et pas l'identité de la personne. Cette situation découle du fait qu'aucune solution avancée d'identité digitale n'existe encore.

14 P.ex. le contrat de mandat (art. 393 CO) ou le contrat de travail (art. 319 CO).

Il est en effet utile d'identifier les parties dès lors que certaines restrictions peuvent s'appliquer en lien avec la personnalité de la personne cocontractante, comme sa nationalité[15] ou sa capacité[16]. Pour donner un exemple récent, on peut mentionner en droit anglais le Digital Economy Act 2017, qui prévoit que la mise à disposition de contenus pornographiques à des mineurs est interdite, et met à la charge desdits acteurs de vérifier l'âge de leurs utilisateurs, sous peine de sanction pécuniaire pouvant se chiffrer jusqu'à č 250'000[17].

[Rz 23] Un troisième élément est celui de la sécurité du droit et des citoyens, ceci à une époque où les relations juridiques se meuvent de plus en plus vers des environnements digitaux. En effet, un risque et un intérêt accru existent alors pour les citoyens de voir leurs identités bien gérées et protégées. Des phénomènes comme l'usurpation d'identité et l'accès illicite à des données sensibles présentent aujourd'hui des risques concrets qui peuvent se révéler délétère pour tout un chacun. Un meilleur contrôle de l'identité digitale permettrait un respect accru du droit. Par exemple, les fournisseurs de services, qu'ils soient issus de la cyberadministration ou du commerce en ligne, pourraient dès lors, au moins théoriquement, avoir un moyen fiable et légitime de vérifier que les exigences légales sont respectées, par exemple via la vérification de l'identités de leurs utilisateurs (ex. accéder à un site pour adulte, l'âge de conclusion d'un contrat, etc.)[18]. En outre, notons qu'il est problématique à notre sens que le contrôle des identités digitales ou de leur utilisation, échappent encore largement à leurs utilisateurs[19].

[Rz 24] Quatrièmement, une législation cohérente et bien encadrée permettrait aux corporations privées de proposer aux citoyens l'accès à des services novateurs avec des avantages pratiques conséquents[20]. On affiche ci-dessous un tableau qui montre les domaines auxquels touche l'identité digitale. Tous ceux-ci sont donc susceptibles d'être « *disruptés* », pour employer une expression à la mode. Par conséquent, il serait bénéfique que le droit apporte des solutions pour le développement de l'identité digitale afin de favoriser la création de services et de valeurs[21].

15 P.ex. dans le cadre de l'acquisition d'un bien immobilier par un étranger dans la loi fédérale sur l'acquisition d'immeubles par des personnes à l'étranger du 16 décembre 1983 (LFAIE ; RS 211.412.41).

16 P.ex. lorsque la personne est incapable de discernement (art. 16 ss du Code civil suisse [CC ; RS 210]) ou plus simplement n'a pas la capacité de disposer (art. 12 CC).

17 Voir Digital Economy Act 2017, part III. N.B. Peut-être cela encouragera-t-il une économie de faussaires ou prêteur d'identités en leur fournissant des clients prêts à payer pour garder profil bas ?

18 N.B. Cette idée de vérification des utilisateurs va dans le sens de la mouvance d'une responsabilité pour les acteurs de l'Internet de plus en plus accrue (voir Julien Francey, *La responsabilité délictuelle des fournisseurs d'hébergement et d'accès Internet*, Zurich 2017).

19 Op cit. 6, BCG, p. 4.

20 Voir par exemple les services proposés dans des pays comme l'Estonie (cf. II.2.3.2b).

21 Voir par ailleurs, Op cit. 6, BCG, p. 6 ss.

Proof of Identity Infographic — Australia Post & The Boston Consulting Group: "A Frictionless Future for Identity Management" Dec. 2016

2.2. Des « données »

[Rz 25] D'un point de vue technique, l'identité digitale représente un simple paquet de données, de sorte que la loi sur la protection des données (de la loi fédérale sur la protection des données ; LPD)[22] devrait généralement s'appliquer. La plupart du temps, ces données seront considérées juridiquement comme des données personnelles au sens de l'art. 3 LPD, dès lors qu'elles rendent une personne identifiable. On mentionnera à ce titre, le nom, le prénom, l'adresse, et les données biométriques (not. le système veineux)[23], comme autant d'exemples de données personnelles. Toutefois, notons que les données biométriques changeront de catégorisation après la révision de la LPD et seront alors considérées comme des données sensibles.

[Rz 26] Actuellement, le système juridique ne prévoit pas de protection particulière, outre celle de la LPD, pour les données, qu'elles soient personnelles ou non. Elles ne sont notamment pas susceptibles d'un droit de propriété (*sui generis*) de leur titulaire. Dans un avenir proche, on pourrait néanmoins se poser la question si cela ne devait pas être le cas. Notamment, certaines voix se sont élevées pour conférer un statut particulier aux données personnelles. Par ailleurs, il est de plus en plus évident que certaines autres données peuvent représenter une valeur patrimoniale importante[24]. Au vu de la rapide montée en puissance des discussions sur les données, il n'est ainsi pas exclu que des types propriété ou un statut *sui generis* soient développés concernant les données personnelles touchant à l'identité. Tout du moins ces données pourraient obtenir un statut et une protection juridique encore plus large dans le futur.

22 Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; RS 235.1).

23 Dominika Blonsky, *Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts*, in : ASR – Abhandlungen zum Schweizerischen Recht Band/Nr. 816, 2015, p. 9 ; Philippe Meier, *Protection des données : fondements, principes généraux et droit privé*, Berne 2011.

24 Gabriel Jaccard, *Smart Contracts and the Role of Law*, in : Jusletter IT 23 novembre 2017, RZ 10 ss.

2.3. Législation actuelle

2.3.1. En Suisse

[Rz 27] Nous séparerons cette section en deux volets, à savoir premièrement la régulation actuelle et future sur l'identité en général (*Infra* let. a) et let. b). Puis deuxièmement, nous donnerons quelques exemples de moyens de reconnaissance digitaux mis en place par la loi (*Infra* let. c) à let. e).

a. Réglementation de l'identité en général

[Rz 28] En tout premier lieu, l'identité des personnes physiques sur le territoire Suisse est régie dans sa continuité par l'ordonnance sur l'état civil (OEC)[25] qui gère les enregistrements et le contenu des informations nécessaires à l'identité. En outre, le droit suisse prévoit une loi fédérale sur les documents d'identité des ressortissants suisses (LDI)[26] et une ordonnance (OLDI)[27] qui mettent en place les règles concernant l'émission des documents officiels d'identité. Par ailleurs, un régime de l'identité spécial s'applique pour l'identité des personnes morales en parallèle, notamment lorsque l'entreprise est active sur les marchés financiers[28]. Enfin, notons que le système de la LDI ne traite pas véritablement la question de l'identité digitale. En effet, outre le fait que les documents d'identité puissent éventuellement être munis d'une puce (art. 2 al. 2bis LDI) contenant une « *identité électronique utilisable à des fins d'authentification, de signature et de cryptage* » (art. 2al. 2quater LDI), le sujet reste largement une *terra nullius*.

[Rz 29] En second lieu, concernant l'identité digitale en particulier, le Conseil fédéral a lancé en 2010 la formule « *SuisseID* »[29] qui sera développée dans le paragraphe suivant. De plus, à l'heure actuelle, notons qu'un avant-projet de « *loi e-ID* » a été mis en consultation. Nous étudierons ce dernier dans la section suivante[30].

[Rz 30] La *SuisseID* a donc été introduite en 2010 avec un succès mitigé[31], notamment au sein du grand public qui ignore encore majoritairement son existence, et pour les entreprises qui ont cherché encore récemment des succédanés à son utilisation[32].

[Rz 31] La SuisseID est régulée au travers de la loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (SCSE) et peut être obtenue auprès de fournisseurs de ce service tels que la Poste sous deux formes : standard et business. Premièrement, la formule standard permet en pratique la vérification élec-

25 Ordonnance sur l'état civil du 28 avril 2004 (OEC ; RS 211.112.2).

26 Loi fédérale sur les documents d'identité des ressortissants suisses du 22 juin 2001 (LDI ; RS 143.1).

27 Ordonnance du DFJP sur les documents d'identité des ressortissants suisses du 16 février 2010 (RS 143.111).

28 En droit suisse, chaque entreprise obtient un numéro d'identification des entreprises (« IDE » ; Loi fédérale sur le numéro d'identification des entreprises du 18 juin 2010, (LIDE ; RS 431.03)). Dans la même veine, les sociétés d'investissements se voient attribuer en outre de l'IDE un « *Legal Entity Identity* » (LEI) sur les marchés, en vertu du droit suisse et de la Directive européenne MIFID II. Cf. https ://www.leiroc.org/lei/how.htm.

29 Cf. https ://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-65745.html

30 Cf. II.2.3.1b)

31 Cf. https ://www.seco.admin.ch/seco/fr/home/Standortfoerderung/KMU-Politik/E-Economy_E-Government/E-Government/suisseid-identitaetsnachweis-und-digitale-signatur.html

32 Par exemple, http ://www.ictjournal.ch/news/2016-12-14/ubs-credit-suisse-et-swisscom-travaillent-a-un-identifiant-digital-partage ; https ://www.letemps.ch/economie/2017/11/21/neuf-entreprises-suisses-sallient-proposer-une-identite-numerique

tronique des informations d'identité telles qu'elles apparaissent sur le passeport (suisse) d'une personne. Son utilisation équivaut à une signature électronique qualifiée, et donc à la signature manuscrite selon l'art. 14 CO[33]. Deuxièmement, la formule business permet, en plus des fonctionnalités de la formule standard, de vérifier l'appartenance à une organisation ou à une entreprise. Enfin, on note que la SuisseID est disponible sur appareil mobile, clé USB, ou carte à puce[34].

[Rz 32] Ensuite brièvement, on peut souligner ici que la législation sur la question de l'identité, du moins celle de l'identité des citoyens suisses, relève d'une prérogative étatique fédérale et pour laquelle les Autorités suisses ont souhaité légiférer de manière extensive, en excluant les acteurs privés[35]. En effet, pour soutenir cette thèse, on note que la LDI prévoit à son art. 1 al. 2 que : « *Les documents d'identité au sens de la présente loi attestent la nationalité suisse et l'identité de leur titulaire* ». De plus, rapportons les propos de la Conseillère fédérale S. Sommaruga qui se prononçait dans l'un de ses discours sur le sujet de l'identité digitale : « *Hierfür braucht es regeln und diese regeln setzt der Staat fest und nicht irgendjemand. Das Möchte ich betonen auch für die digitale Welt ist es der Staat der die existenz einer Person und ihre identitäts Merkmale, wie Name, Geschlecht, oder Geburtstag, prüft und auch bestätigt* »[36].

b. L'avant-projet de la Loi e-ID

[Rz 33] Le Conseil fédéral a annoncé en 2017 la mise en consultation de l'avant-projet de la loi fédérale sur les services d'identification électronique (Loi e-ID), dont l'entrée en vigueur devrait se situer aux alentours de 2020[37]. Au vu des changements importants que cette loi s'apprête à apporter, nous l'étudierons ici. Cependant, le lecteur notera le caractère suspensif de nos propos, dès lors que la teneur définitive du texte qui sera retenu n'est pas encore connue.

[Rz 34] Préalablement, on note que la Loi e-ID se place dans une idée de réponse politico-économique à la question de l'identité digitale. Elle ne vise pas à régler la question de la signature électronique, qui n'est donc pas révisée de concert avec l'avant-projet. L'objectif de la réforme est d'une part, de régler un problème concernant cette identité digitale qui échappe aux Etats, et d'autre part, elle veut permettre l'ouverture des services du e-commerce et de la cyber administration à un plus grand nombre de citoyens suisses. Par ailleurs, ces objectifs pourront être dépassés dans le futur.

[Rz 35] Premièrement, la mise en place de la e-ID s'effectuera via un mécanisme semi-étatique, semi-privé illustré en image ci-dessous[38]. Le système sera composé par un organisme fédéral de reconnaissance qui habilitera des Fournisseurs d'Identité (« FI ») à établir des e-ID pour les

33 https ://www.post.ch/fr/entreprises/index-thematique/suisseid/produits-et-prix/produit-standard-suisseid

34 Cf. https ://www.post.ch/fr/entreprises/index-thematique/suisseid/produits-et-prix/prix

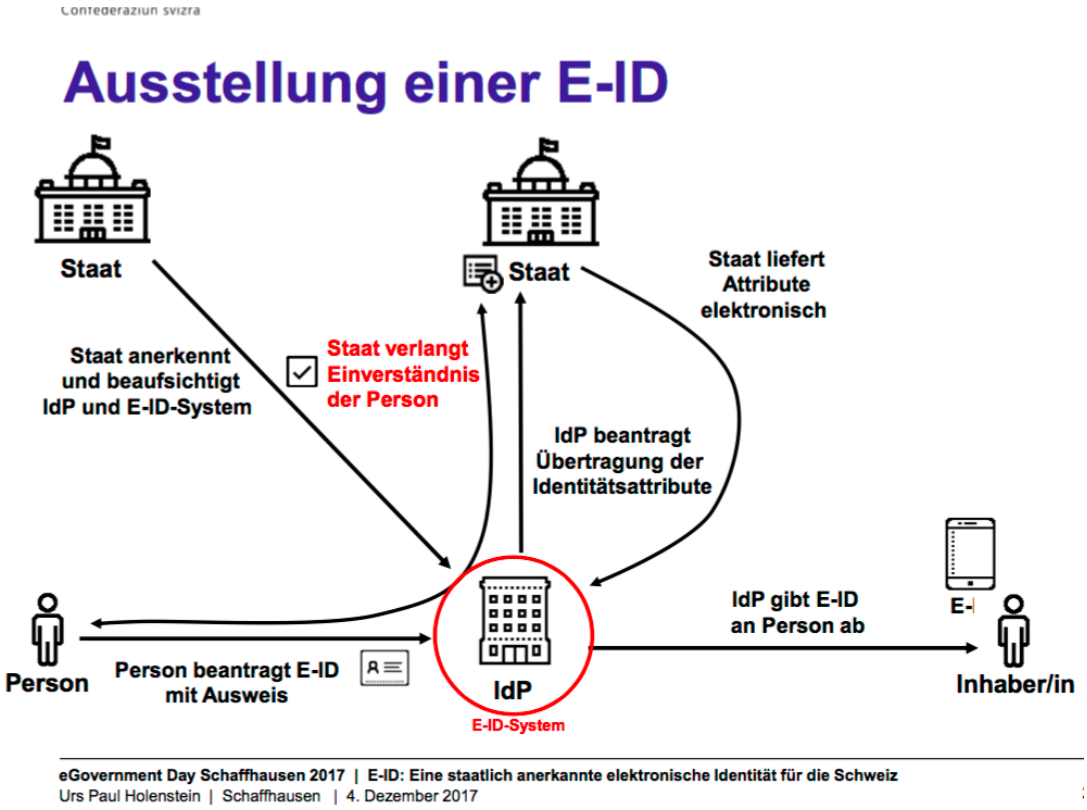
35 Cf. https ://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/e-id.html

36 Voir, Kurzfassung der MK vom 15. November 2017 – BR Sommaruga zur digitalen Identität : https ://www.iso-20022.ch/info-to-go/news/artikel/es-geht-weiter-mit-der-digital-identity-fuer-die-schweiz/ ; Voir aussi Conseil fédéral, *Questions – reponses concernant les e-ID reconnus par l'Etat*, question N3 (Disponible ici : https ://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-11-15.html) (ci-après cité : « *Q&A*, *NX* »), concernant la compétence étatique.

37 On note que certains pays, comme l'Estonie ou la Suède, sont d'ores et déjà très en avance dans ce domaine et pourraient nous servir comme modèle, cf. https ://e-resident.gov.ee/become-an-e-resident/. ; voir II.2.3.2b).

38 En effet, le modèle 100% étatique, comme il a été développé en Allemagne, s'est révélé peu concluant : https ://www.letemps.ch/suisse/2017/11/15/lidentite-numerique-un-chantier

citoyens, et ce à des prix non-prohibitifs[39]. Notons que la question de savoir à qui on devrait laisser la prérogative d'établir des e-ID est sujette à controverse. En effet, certaines voix s'élèvent contre cette incursion de l'Etat dans ce domaine y voyant les prémisses de l'outil d'un Etat « *Big Brother* ». En ce sens, certains estiment qu'une telle prérogative devrait être laissée aux privés, voie au citoyen lui-même (*Self Sovereign Identity*[40]). Dans cette dernière hypothèse, l'idée serait de laisser des registres d'identités digitales, par exemple sur des Blockchain, qui puissent être gérés directement par les citoyens[41].



[Rz 36] A notre avis, la régulation de l'identité digitale au travers d'une loi suisse e-ID est la meilleure solution. Outre le fait que la compétence de l'identité *stricto sensu* reviendrait à l'Etat[42], l'intérêt public face aux éventuelles dérives est en Suisse à notre sens mieux protégé entre les mains des acteurs étatiques. Cependant, on peut imaginer qu'une partie de la compétence de l'identité *lato sensu*, c'est-à-dire lorsqu'elle n'est pas équivalente au but de la carte d'identité, pourrait revenir à des acteurs privés, notamment dans les supports de l'identité digitale que nous étudierons plus loin (cf. *infra* n°3).

[Rz 37] Deuxièmement, pour ce qu'il en est de sa teneur, la e-ID devrait jouer le rôle d'une sorte de prolongement de la carte d'identité physique. Actuellement, les documents d'identité phy-

39 Probablement des acteurs des télécoms ou la Poste.

40 Cf. https ://medium.com/learning-machine-blog/the-time-for-self-sovereign-identity-is-now-222aab97041b

41 Cf. https ://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/

42 Voir par ailleurs dans ce sens aussi art. 7 règlement du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (eIDAS).

sique contiennent les informations suivantes, à savoir : *nom d'état civil ; prénoms ; sexe ; date de naissance ; lieu d'origine ; nationalité ; taille ; signature ; photographie ; autorité d'établissement ; date d'établissement ; date d'expiration ; numéro et type du document* (art. 2 LDI).

[Rz 38] En comparaison, l'art. 7 al. 1 AP-Loi e-ID prévoit que la e-ID contiendra au minimum : *le numero d'enregistrement de l'e-ID* (soit un numéro individualisant le citoyen) ; *le nom d'état civil ; les prenoms ; la date de naissance*. Cependant, l'art. 7 al. 2 AP-Loi e-ID ajoute que lorsqu'une identification substantielle ou élevée sera requise, la liste des éléments s'étendra : *le sexe ; le lieu de naissance ; l'etat civil ; la nationalite, eventuellement le statut de sejour ; une photographie ; le numero et le type du document d'identite ou du titre de sejour délivré par la Suisse ; une image de la signature*. Enfin, l'art. 7 al. 4 AP-Loi e-ID prévoit que le FI « *peut attribuer d'autres données* »[43] à la e-ID.

[Rz 39] Dans cette optique, on notera ici que la signature électronique ne fait pas partie de la liste des informations contenues dans la e-ID. Cependant, des voix se sont élevées afin que les organismes qui fournissent de telles signatures soient néanmoins reconnus comme équivalents au FI[44]. A défaut, la signature d'un contrat requérant la forme écrite devrait alors nécessiter, par exemple, l'authentification de la e-ID, en sus de l'utilisation d'une signature électronique (art. 14 al. 2bis CO)[45], ce qui serait peu pratique. De même, cette mesure diffère du système estonien qui prévoit le cumul des fonctions de preuve d'identité et de signature[46].

[Rz 40] Troisièmement, la e-ID ne concernera que les personnes physiques, et non les personnes morales, bien que ce point reste encore incertain à l'heure actuelle[47]. Son obtention sera conditionnée à la possession de la nationalité suisse ou d'un permis de séjour valable (art. 3 al. 1 AP-Loi e-ID). Toutefois, concernant les personnes morales, dès lors qu'une personne physique ayant la capacité selon le registre du commerce de représenter une entreprise aura été authentifiée, on pourrait imaginer que cette dernière puisse aussi facilement représenter et s'engager au nom de la personne morale via ce biais.

[Rz 41] Quatrièmement, il est prévu que la e-ID ne soit pas obligatoire : « *L'utilisation de l'e-ID n'est pas une obligation prescrite par l'Etat. Selon le principe de la liberte contractuelle, le prestataire decidera lui-meme s'il veut exiger un e-ID pour l'acces a ses services en ligne* »[48].

[Rz 42] Cet aspect est une faiblesse importante selon nous, car il appert que l'obligation de l'e-ID a été l'un des facteurs majeurs ayant permis son adoption dans des pays phares comme l'Estonie[49]. Par ailleurs, nous pensons que le domaine de l'identité digitale est, comme pour les moteurs de recherches, un domaine technologique ou l'hégémonie d'un fournisseur de service permettrait de maximiser le bénéfice commun et l'efficacité. Dernièrement, la e-ID ne sera pas créée automati-

43 Il a notamment été suggéré par L'UBS d'ajouter a l'art. 7 al. 4 AP : « *[...], en particulier une adresse, un numéro de téléphone ou un numéro de client* ». L'ISSS suggéra de son côté de compléter la liste avec la mention d' « *autres attributs* biométriques » ou de « *paramètres personnels additionnels* » afin d'anticiper sur l'évolution de la numérisation. Voir *Op cit*. 47, *synthèse consultation*, p. 17.

44 *Op cit*. 47, p. 13 s.

45 Peut-être que l'ouverture opérée par l'art. 7 al. 4 AP-Loi de la loi fédérale sur les services d'identification électronique (e-ID) permettra une telle adjonction.

46 Cf. II.2.3.2b)

47 UBS propose de mentionner dans la loi à l'art. 6 qu'une personne peut disposer de plusieurs e-ID. Conseil fédéral, Synthèse des résultats de la procédure de consultation, (lien : https ://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/e-id.html) (ci-après : « *synthèse de consultation, p.X* »), p. 17. A notre sens, les personnes morales devraient pouvoir aussi prétendre à une e-ID.

48 *Op cit*. 36, Q&A, N4.

49 Cf. II.2.3.2b)

quement pour les citoyens[50] bien qu'elle devrait exister de manière unique pour chaque personne physique qu'elle concerne.

[Rz 43] Cinquièmement, l'obtention d'une e-ID sera soumise à des devoirs pour son titulaire. Par exemple, il ne pourra pas la laisser à la disposition de tiers et il devra prendre les mesures nécessaires afin d'éviter toute utilisation abusive (art. 14 AP-Loi e-ID).

[Rz 44] Sixièmement, concernant le degré de garantie d'authentification, l'art. 5 de l'AP-Loi e-ID prévoit qu'il existera trois niveaux (faible/substantiel/élevé)[51] d'e-ID en fonction de leurs degrés de garantie. Les niveaux dépendront des types d'authentification requis. En l'occurrence, les e-ID offriront un degré de garantie faible lorsque le risque d'utilisation abusive ou l'altération de l'identité est faible. Substantiel, lorsqu'il est substantiel. Et élevé lorsqu'il est élevé.

[Rz 45] Septième point, il est intéressant de relever la question de la mise à jour des informations sur les e-ID. Il est important que ces données ne soient pas statiques, c'est pourquoi l'avant-projet prévoit leur révision périodiquement (art. 8 AP-Loi e-ID) en fonction du niveau de garantie qu'elles offrent, à savoir : faible / annuellement, substantiel / trimestriellement, élevé / hebdomadairement.

[Rz 46] Enfin, l'un des éléments essentiels de la e-ID reste la question de l'interopérabilité. En effet, il ressort de l'état des discussions actuelles que la e-ID a pour finalité de pouvoir être utilisée à la fois de manière uniforme à l'intérieur de la Suisse (art. 18 AP-Loi e-ID) mais aussi, au minimum, au sein de l'Europe. Effectivement, une identité digitale qui serait limitée à la Suisse seulement, ou techniquement limitée à un fournisseur d'accès, perdrait nettement de son utilité dès lors qu'internet et le digital en général, eux, n'ont pas de frontières. D'autres questions restent en suspens dans l'avant-projet telle que la question de l'identité digitale pour les binationaux.

[Rz 47] Dernièrement, faisons remarquer que la mise en place de la e-ID ne mettra probablement pas un terme à toutes autres identités digitales, ceci notamment si la e-ID n'est pas obligatoire. En effet, il y aura toujours des personnes ou des entités (ex. banques) qui ne passeront pas par le système d'authentification classiques. Par exemple car elles développeront d'autres standards plus élevés.

c. La signature électronique

[Rz 48] A titre liminaire, on note que la signature électronique se définit comme « *un ensemble de données électroniques qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité* » (art. 2 al. 1. let. a LSCE). Celle-ci peut avoir plusieurs degrés de garantie. De plus, on distingue les signatures électroniques des cachets[52]et les certificats électroniques[53].

i) La signature électronique simple, avancée, réglementée et qualifiée

[Rz 49] Le droit suisse connaît déjà un type d'identité digitale sous la forme des signatures électroniques. Celles-ci ont été mise en place au travers de la loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques

50 *Op cit*. 36, Q&A, N11.

51 Ces trois niveaux sont un parallèle avec la régulation européenne eIDAS.

52 Destinés aux personnes morales.

53 Destinés aux personnes physiques ou morales afin de garantir la provenance des documents.

(SCSE)[54] et son ordonnance (OSCE)[55]. Cette loi vise à mettre en place un procédé technique permettant deux choses. A savoir premièrement de garantir l'authenticité d'un document ou d'un message électronique et deuxièmement, de s'assurer de l'identité de son expéditeur[56]. Par ailleurs, notre législation est largement basée sur le règlement du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (eIDAS).

[Rz 50] Il existe plusieurs types de signatures électroniques et autres certificats qui peuvent être utilisés par les personnes physiques et/ou morales (cf. art. 2 SCSE). Concernant les personnes physiques, on note quatre formes possibles. Nous étudierons ici les formes crescendo en fonction de leur degré de sécurité.

[Rz 51] Premièrement, la *signature électronique simple* consiste en un ensemble de données électroniques qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité (art. 2 al. 1 let. a SCSE). Il s'agira ici d'une forme basique non-qualifiée. Cette forme doit permettre de disposer de l'identité du signataire (non-contrôlée par un tiers), d'assurer l'intégrité du document et permet éventuellement de donner une idée de la volonté de son auteur. On l'utilise par exemple pour des adhésions à des conditions d'utilisation sur les sites. Notez, le paraphe par ordinateur au bas d'un email ou encore la signature photographiée envoyée par email ne rentrent pas dans cette catégorie.

[Rz 52] Deuxièmement, la *signature électronique avancée* (art. 2 al. 1 let. b SCSE) est une signature électronique qui remplit les quatre conditions suivantes : 1. être liée uniquement au titulaire, 2. permettre d'identifier le titulaire (avec un contrôle par un tiers), 3. être créée par des moyens que le titulaire peut garder sous son contrôle exclusif, 4. être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. On l'utilisera par exemple pour signer les P.V. de décisions dans les assemblées générales.

[Rz 53] Troisièmement, la refondation du 1er janvier 2017 de la SCSE a vu naître la *signature électronique réglementée*[57] (art. 2 al. 1 let. c SCSE), qui consiste en une signature électronique avancée créée au moyen d'un dispositif sécurisé de création de signature au sens de l'art. 6 SCSE et fondée sur un certificat réglementé se rapportant à une personne physique et valable au moment de sa création. Elle forme une signature électronique qualifiée « *light* » permettant d'identifier une personne et d'authentifier des documents sans pour autant que cette forme remplisse les exigences de la forme écrite de l'art. 14 al. 1 CO. Elle devrait notamment être utilisée pour signer des emails ou des actes juridiques ne nécessitant pas la forme écrite.

[Rz 54] Dernièrement, la *signature électronique qualifiée* (art. 2 al. 1 let. e SCSE), soit une signature électronique réglementée fondée sur un certificat qualifié est une forme équivalente à la forme

54 Loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques du 18 mars 2016 (SCSE ; RS 943.03).

55 Ordonnance sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques du 23 novembre 2016 (OSCSE ; RS 943.032).

56 Cf. https ://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/communication-numerique/signature-electronique.html

57 Parallèlement, la loi introduit le cachet électronique règlementé qui représente l'équivalent de la signature électronique règlementée mais pour les personnes morales.

manuscrite selon l'art. 14 al. 2bis CO[58]. De plus, on relève que seuls les fournisseurs reconnus sont habilités à délivrer une telle signature électronique qualifiée (art. 3 SCSE).

[Rz 55] En Suisse, les signatures électroniques sont encore peu usitées en dehors des milieux professionnels, notamment en ce qui concerne l'utilisation au sein de l'activité quotidienne de la population (email, achat, etc.). Par ailleurs, la forme manuscrite est encore souvent légalement requise dans les documents officiels.

ii) La signature électronique « authentique »

[Rz 56] La régulation suisse connaît l'ordonnance sur l'établissement d'actes authentiques électroniques et la légalisation électronique (OAAE)[59]. Cette dernière prévoit une méthode spécifique destinée à reproduire digitalement la forme des actes authentiques ou les légalisations. Ce qui est notamment utile dans le cadre des activités notariales.

[Rz 57] L'OAAE prévoit à son art. 3 que le notaire doit établir les documents selon les cas prévus par le droit. Puis il doit enregistrer lesdits documents dans un format reconnu avec une formule de confirmation, avant de signer le document au moyen de sa signature électronique qualifiée qui contiendra aussi un horodatage électronique qualifié[60]. Enfin, il accompagnera le tout de la preuve qu'il a le droit de dresser des actes authentiques. Les règles et aspects techniques sont réglés par l'OAAE-DFJP[61].

[Rz 58] En pratique, il appert que cette méthode est peu utilisée, les notaires préférant encore la « *simplicité* » du papier.

d. La reconnaissance par vidéo et en ligne

[Rz 59] La reconnaissance en ligne a passablement évolué ces dernières années. Sans pour autant créer une nouvelle e-identité, on note que de nombreux efforts ont été mis en place afin de faciliter l'identification au travers des canaux digitaux. Par exemple, la récente Circulaire 2016/7 Identification par vidéo et en ligne, de la FINMA. En particulier, cette circulaire met en place une méthode d'équivalence entre l'identification *in personam*, et l'identification en ligne ou par vidéo-conférence, et aussi via la méthode TAN.

[Rz 60] Par ailleurs, on note que l'utilisation de la méthode TAN, ainsi que les autres procédés analogues, est considérée comme équivalente à la signature électronique qualifiée, qui est par exemple nécessaire lors de la déclaration de l'ayant-droit économique de valeurs patrimoniales déposées chez l'intermédiaire[62].

---

58 Cf. https ://www.seco.admin.ch/seco/fr/home/Standortfoerderung/KMU-Politik/E-Economy_E-Government/E-Government/suisseid-identitaetsnachweis-und-digitale-signatur.html

59 Ordonnance sur l'acte authentique électronique du 23 septembre 2011 (OAAE ; RS 943.033).

60 A savoir, un horodatage électronique qui est opéré par un fournisseur de services de certification reconnu en vertu de la présente loi et qui est muni d'un cachet électronique réglementé (art. 2 let. e et j de l'ordonnance sur l'établissement d'actes authentiques électroniques et la légalisation électronique ; OAAE ; RS 211.435.1).

61 Ordonnance du DFJP sur l'acte authentique électronique du 25 juin 2013 (OAAE-DFJP ; RS 943.033.1).

62 Circulaire FINMA Identification par vidéo et en ligne, N48.

e. Le e-commerce

[Rz 61] En dernier lieu, nous tenons ici à soulever brièvement le point du e-commerce. En effet, cette pratique exacerbée du 21ème siècle a donné lieu au développement de quelques règles et pratiques pour l'identification et le consentement des parties.

[Rz 62] Selon l'art. 3 al. 1 let. s de la loi fédérale contre la concurrence déloyale (LCD), un marchand sur internet doit obligatoirement indiquer de manière claire et complète son identité et son adresse de contact, y compris son courrier électronique. Cette règle n'impose cependant pas la pareille au consommateur. Par conséquent, le degré de l'identité requis dans le e-commerce tombe la plupart du temps dans la catégorie d'une identité virtuelle car rien ou peu de chose ne permet de véritablement identifier la partie contractante[63], sauf peut-être ses informations bancaires de paiement quand celles-ci lui appartiennent effectivement ou même existent.

[Rz 63] Dernièrement, sauf cas particuliers[64], il n'existe pas dans le e-commerce l'obligation stricte d'identifier les consommateurs dans la plupart des contrats. Ceci dans le but principal de ne pas perturber la bonne marche des affaires.

2.3.2. Dans l'Union européenne

a. Union européenne

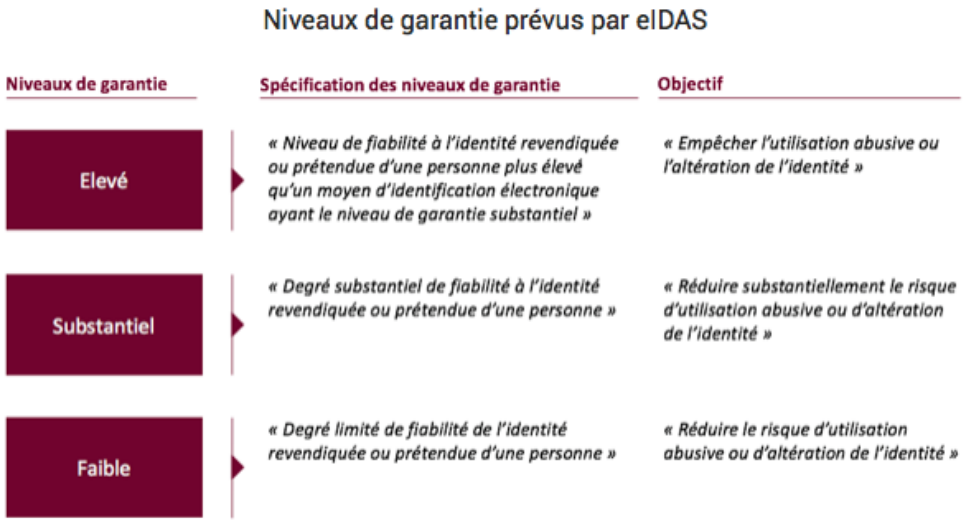
[Rz 64] Au niveau européen, on relève une législation nodale dans le domaine de l'identification, à savoir le Règlement (UE) n°910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/ce, en vigueur depuis le 1er juillet 2016 (eIDAS). Cette pièce maîtresse règle et harmonise la question de l'identité et des signatures électroniques au niveau européen, tout en laissant une marge de manœuvre aux Etats Membres. Le Règlement constitue l'équivalent suisse en Europe de la SCSE et de l'AP loi e-ID.

[Rz 65] En ce qui concerne l'identité digitale en Europe, deux éléments notables doivent être mentionnés[65]. Premièrement, les moyens d'identifications électroniques sont reconnus de manière mutuelle. Par conséquent, l'identité digitale, reconnue dans l'un des pays de l'UE, est valable dans tous les autres. Il s'agit donc d'un « *one stop shop* ». Deuxièmement, le Règlement instaure trois niveaux de garanties des identités digitales (art. 8 eIDAS) exposés ci-dessous :

63 Et ce malgré la théorie générale des contrats (art. 1 CO), qui veut que les parties doivent être clairement identifiées ou identifiables afin que le contrat soit valablement conclu.

64 Sauf cas particuliers, loi fédérale sur les placements collectifs de capitaux (LPCC ; RS 951.31), vente d'immeubles, cession de créance, etc.

65 Cf. http ://eur-lex.europa.eu/legal-content/FR/TXT/ ?uri=LEGISSUM%3A310603_1



[Rz 66] En ce qui concerne la signature électronique, l'eIDAS prévoit trois cas de figure, la signature simple (ou standard), avancée et dernièrement qualifiée (voir art. 3 eIDAS, définitions).

[Rz 67] Premièrement, les signatures simples ne donnent pas de certitude absolue sur l'identité d'un signataire ou de l'intégrité d'un document. L'art. 25 al. 1 eIDAS prévoit simplement que « *la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.* ». Toutefois, les Etats membres ont encore une marge de manœuvre dès lors qu'« *il appartient au droit national de définir l'effet juridique produit par les signatures électroniques, à l'exception de l'exigence prévue dans le présent règlement selon laquelle l'effet juridique d'une signature électronique qualifiée devrait être équivalent à celui d'une signature manuscrite* » (Regeste eIDAS N49).

[Rz 68] Deuxièmement, les signatures avancées (art. 26 eIDAS) permettent de garantir l'identité de la personne du signataire, la date de la signature, et l'intégrité des données. Elles ne sont toutefois pas équivalentes à la forme manuscrite.

[Rz 69] Troisièmement, les signatures qualifiées permettent l'équivalence avec la forme manuscrite (art. 25 al. 2 eIDAS). Dernièrement, on note que l'eIDAS prévoit, de même qu'en droit suisse, l'existence des cachets électroniques (art. 35 eIDAS).

b. Le cas de l'Estonie

[Rz 70] L'Estonie est un pays baltique membre de l'Union européenne. Il est composé de 1.3 million d'habitants et fût fondé en 1991 après l'effondrement de l'URSS. Le PIB nominal était alors d'environ 300 millions CHF, et il est à environ 26 milliards CHF aujourd'hui, preuve du succès croissant et impressionnant de cette jeune nation dynamique.

[Rz 71] Sa réussite, l'Estonie la doit à son pari d'investir dans le digital dès sa création, et d'avoir (re)bâti l'organisation de son Etat sur cette base, avec en tête et pour motivation de subsister face à son puissant voisin la Russie. Ainsi, le pays a été le pionnier, et est le leader actuel, de l'identité digitale. Aujourd'hui, les chiffres sont impressionnants : 98% des Estoniens possèdent une e-ID

Card, 98% des sociétés sont créées en ligne, tandis que 99% des transactions bancaires et 95% des déclarations administratives sont faites en ligne[66].

[Rz 72] Le système de l'identité digitale est divisé en plusieurs parties[67]. Premièrement, l'ID-Card (appelée généralement e-ID), à savoir une carte physique contenant une puce électronique avec l'identité digitale. Deuxièmement, la Mobile-ID qui consiste en une puce contenant l'identité digitale liée à la carte SIM d'un téléphone. Troisièmement, la Smart-ID, qui consiste en une application mobile similaire à la Mobile-ID, mais non-reliée à une quelconque puce. Et dernièrement, on mentionnera pour les non-nationaux, la e-Residency, qui est une identité digitale réservée aux étrangers, résidant physiquement en Estonie ou non.

[Rz 73] Le système fonctionne de la façon suivante. Premièrement, l'identité digitale doit être obtenue auprès d'un fournisseur officiel (en l'occurrence la société SK-ID). Puis, l'utilisateur se voit remettre un code d'identification qui individualise le citoyen, ainsi que deux codes d'accès (PIN1 et PIN2) : un premier lui permettant de s'authentifier et un deuxième lui permettant d'apposer une signature électronique. D'un point de vue juridique, le droit estonien prévoit que cette signature digitale est équivalente à la forme écrite (§80 General Part of the Civil Code Act, RT 2002, 35, 216). De même, du point de vue de l'eIDAS, elle remplit les conditions d'une signature électronique qualifiée.

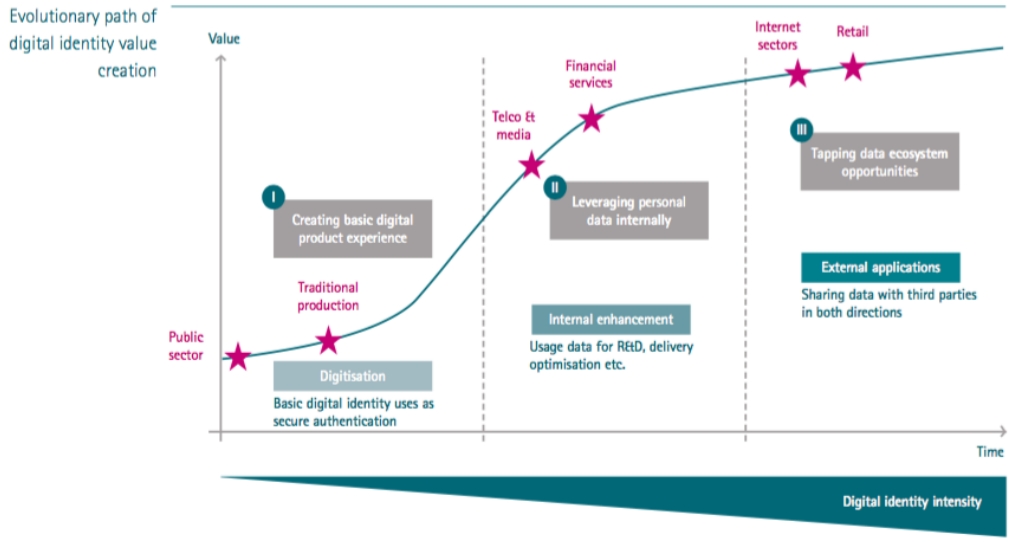
[Rz 74] En comparaison avec nos contrées helvètes, le retard est conséquent. En effet, l'équivalent estonien de l'avant-projet suisse actuel (2017) de la loi e-ID (ID-card et signature digitale – le digital signature Act, qui a été récemment remplacé par le Electronic Identification and Trust Services for Electronic Transactions Act – fût accepté en 1997 par le parlement estonien (entrée en force en 2002)[68]. Grâce à cette e-ID, qui est obligatoire, de nombreux services aussi sûrs qu'efficaces ont pu se construire, motivés tant par des objectifs privés (contrats, sociétés, ...) que publics (vote, gouvernance, santé, taxe, ...).

[Rz 75] Le point d'orgue qui ressort est donc le fait que sans régulation cumulée d'un soutien actif de l'Etat, rien n'aurait été possible. En effet, l'e-ID s'est développé par palier technologique et par incitation répétée mêlée à une éducation des citoyens dans l'utilisation de cette technologie (voir illustration ci-dessous). Ainsi, afin d'inciter la population, l'Etat a dû proposer des réductions, par exemple sur les tickets de bus, ou des avantages (ex. meilleurs temps de réactions de l'administration et une disponibilité 24/7) afin que les citoyens utilisent la e-ID à large échelle.

66 E-estonia guide, https ://e-estonia.com.

67 Cf. https ://e-estonia.com/solutions/e-identity/

68 La Mobile-ID, a été introduite en 2007.



Op cit. 6, BCG, p. 55.

[Rz 76] Bien que le système estonien soit sans aucun doute un exemple à suivre, il n'en demeure pas moins imparfait. Les risques liés à la digitalisation de l'identité sont très grands notamment dans l'éventualité d'une usurpation d'identité, d'un bug, d'une erreur, d'une indisponibilité du service internet[69], ou autre. Nous l'illustrons ici par deux exemples. Premièrement, en 2014, en raison d'une faille potentielle au niveau de la puce électronique, l'Etat fût obligé de rappeler la plupart des ID-Card[70]. Cet événement eût pour effet de paralyser complètement le pays pendant quelques jours, car les gens avait pris pour habitude d'utiliser leur identité digitale pour accéder aux bâtiments de travail ou même pour se connecter sur leur ordinateur. Deuxièmement, fort du savoir qu'aucun système n'est infaillible, il appert en pratique qu'il n'est pas exclu que des personnes proches ou appartenant au cercle restreint, familial notamment, puisse facilement connaître les codes d'accès et de signatures (PIN1 et PIN2) des personnes à risque, c'est-à-dire les jeunes ou les aînés.

69 Par exemple à cause d'une panne d'électricité. Notamment la digitalisation de l'identité pose la question de la consommation d'énergie accrue des nouvelles technologies : http ://www.ictjournal.ch/articles/2017-12-15/faut-il-craindre-un-cyber-blackout

70 Cf. http ://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/

3. Les supports de l'identité digitale

***Morpheus** : This is the construct. It's our loading program. We can load anything from clothing, to equipment, weapons, training simulations, anything we need.*

***Neo** : Right now we're inside a computer program ?*

***Morpheus** : Is it really so hard to believe ? Your clothes are different. The plugs in your arms and head are gone. Your hair has changed. Your appearance now is what we call residual self image. It is the mental projection of your digital self.*

***Neo** : This...this isn't real ?*

***Morpheus** : What is real ? How do you define real ? If you're talking about what you can feel, what you can smell, what you can taste and see, then real is simply electrical signals interpreted by your brain. This is the world that you know.*

[Rz 77] Dans cette section, nous verrons qu'il existe plusieurs types de supports de l'identité digitale. Il pourra s'agir de supports intégrés au corps humain (*infra* n°3.1), des objets à proximité (*infra* n°3.2), et enfin des supports externes (*infra* n°3.3).

3.1. La réunion de l'identité physique et l'identité digitale ou virtuelle

3.1.1. En général

[Rz 78] Notre première catégorie concerne les supports dits « *implantables* » ou sous-cutanés, à savoir ceux qui font fusionner l'identité digitale avec le corps humain. Il s'agit, le plus souvent, de puces électroniques contenant des informations sur l'identité d'une personne, soit d'autres

informations[71], qui lui sont implantées directement sous la peau[72], généralement dans la main ou le bras. Bien que cette pratique reste encore largement marginale chez les êtres humains, on peut noter que le phénomène de l'identification par puce électronique est largement répandu, depuis quelques années pour les animaux de compagnie[73].

[Rz 79] Les puces électroniques peuvent servir diverses fonctions[74]. Par exemple, elles peuvent contenir des données d'identités sur une personne qui lui permettront de s'identifier. Ou encore, la puce peut émettre un signal impersonnel et constant[75] (Near Field Communication, « NFC » ou Radio Frequency Identification « RFID »)[76] qui permettra l'accès à une porte ou à un accès informatique, voire même la validation d'un paiement.

[Rz 80] Toutefois, ce n'est pas parce que l'identité est fusionnée avec le corps que les informations qu'elle contient sont toujours « *véritables* ». Cela s'explique notamment du fait que ce type d'identité digitale est souvent autogérée de manière privée et sans qu'un tiers de confiance (ex. une banque ou un fournisseur d'identités) ne valide son contenu[77]. De plus, les informations nouvelles ne donnent pas lieu obligatoirement à des mises à jour, ce qui rend les puces tendanciellement statiques face aux changements, et ce qui augmente le risques d'informations inexactes.

[Rz 81] Dernièrement, l'insertion d'un tel support implantable est aujourd'hui devenu très facile et ne représente pas de risques importants pour la santé. Il existe même des kits d'implantations « *do it yourself* »[78]. Par conséquent, ce type d'identité se révèle difficilement contrôlable par une autorité publique.

3.1.2. Aspects légaux

[Rz 82] D'un point de vue légal, ce phénomène amène à de multiples questionnements auxquels nous apporterons quelques éléments de réponse. A savoir, premièrement est-ce que l'existence d'une telle identité est compatible avec les identités « officielles », digitales ou non, créées par le gouvernement ? Quelle est la valeur légale de ces identités et comment consent-on via une puce RFID ? Et dernièrement, quelles sont les problématiques liées à l'implantation d'une puce électronique ?

a. Coexistence avec les identités officielles

[Rz 83] La législation sur l'identité en Suisse, a pour objectif de réguler l'identité digitale de manière exclusive. Par conséquent, la mise en place d'une identité digitale équivalente concurrente sur le territoire suisse par un tiers non-autorisé est illégale.

---

71 Par exemple, on pourrait penser à une puce qui contient des données sur la personne : groupe sanguin, allergie,..

72 Cf. http ://www.lemonde.fr/lifestyle/article/2017/10/03/en-suede-des-puces-electroniques-dans-la-peau_5195287_1616922.html

73 Voir la réglementation sous les art. 15a (équidés) et art. 16 (chiens) de l'Ordonnance sur les épizooties du 27 juin 1995 (état le 1er mars 2018) (OFE ; RS 916.401), qui prévoit l'obligation des puces électroniques.

74 Cf. https ://dangerousthings.com

75 Pas de bouton « *off* ».

76 N.B. Il existe une multitude de types de ces puces.

77 Par exemple, les cartes de crédits récentes (depuis 2004) permettent un paiement « *sans contact* », qui en font des titres au porteur. Dès lors elles ne sont garantes d'aucune preuve d'identité.

78 Cf. https ://dangerousthings.com/shop/xnti/

[Rz 84] Cependant, nous ne voyons rien à redire dans l'éventualité où un FI aurait l'idée de prolonger ses services, par exemple en proposant des puces électroniques implantables, dès lors que ces puces respectent la loi sur la protection des données. En particulier sous l'angle de la confidentialité, il faudrait alors impérativement protéger techniquement la puce, notamment si elle rentre dans la catégorie des RFID, par exemple en empêchant leur lecture via un appareil quelconque.

[Rz 85] Deuxièmement, la régulation de la loi suisse n'empêche pas que des multitudes d'identités digitales (p.ex. la e-ID et TAN) puissent coexister, voir même qu'elles se concurrencent (p.ex. e-ID suisse, TAN, e-residency Estonienne)[79]. Tout d'abord car à défaut d'un système d'identité digitale parfaitement interopérable, une multitude d'e-ID devrait nécessairement exister à l'international. En effet, dans cette optique transfrontalière, le contrôle de l'Etat sur l'identité digitale est en vérité totalement illusoire sans coopération intra-étatique. On note toutefois, qu'un certain contrôle pourrait être obtenu par les Autorités. Par exemple, afin d'obtenir un meilleur contrôle sur l'identité digitale, l'Etat pourrait obliger les fournisseurs de services digitaux et internet en Suisse, lorsque la situation l'exige, à authentifier leurs utilisateurs via le système d'e-ID national ou par son équivalence pour les étrangers[80].

[Rz 86] Troisièmement, les identités virtuelles ne font pas partie du champ d'application de la régulation de l'identité digitale. Partant, les puces utilisées pour le Biohacking qui permettent d'ouvrir une porte, de s'authentifier devant une borne, etc. pourront être utilisée légalement et à discrétion sans contrevenir auxdites lois.

b. Valeurs légales des identités & consentement

[Rz 87] Premièrement, comme on l'a mentionné plus haut, les puces d'identité implantées ne pourraient pas pouvoir prétendre ni à un statut ni au fonction d'une identité digitale mais uniquement à celui d'une identité virtuelle. Les raisons principales sont la régulation exclusive du droit suisse et l'absence d'un tiers de confiance reconnu pour valider le contenu de l'information sur l'identité.

[Rz 88] Bien que l'identité digitale implantée ne soit pas légale en tant que document d'identité officiel, on peut imaginer des situations de droit privé où la puce électronique implantée ferait office de titre (art. 965 CO) pour effectuer des paiements (fonction *monétique*) ou autres. On peut notamment penser à une analogie avec la situation actuelle des cartes « *sans contact* » où l'utilisateur accepte d'effectuer des petits paiements sous simple présentation de la puce RFID sur sa carte bancaire[81]. Dans une hypothèse monétique, il faudrait que la puce électronique implantée soit émise par la banque qui serait soumise à une procédure *d'onboarding* et aux normes KYC, anti-

79 En effet, il est imaginable que tout un chacun puisse détenir une multitude d'identités digitales. Ceci notamment car les fournisseurs de services, qu'ils soient ceux de l'Internet ou de la e-ID, sont présents à l'international et que, même interopérable, chaque pays développera sa propre identité digitale. Par ailleurs, les différences entre les réglementations des pays pourraient rendre certaines nationalités plus attrayantes que d'autres, excitant par là le *forum shopping* des nationalités et des statuts de résidents (p.ex. la e-residency estonienne).

80 Par ailleurs, on pourrait se demander quelles seraient les méthodes que pourraient utiliser les autorités suisses pour imposer sur la durée l'utilisation d'une telle e-ID ? Les solutions devront être non-discriminatoires, ce qui pose problème dès lors que ni les étrangers, ni même forcément tous les suisses (dès lors que la e-ID n'est pas obligatoire) y auront accès.

81 Par exemple, (https ://www.mastercard.ch/fr-ch/clients-prives/services-savoir-innovations/innovations/sans-contact.html) les cartes contiennent une puce électronique émettrice d'un signal qui permet le paiement.

blanchiment d'argent visant les intermédiaires financiers[82]. En outre, comme pour la carte sans contact, le client devrait consentir préalablement à cette forme spécifique de passer un contrat. En tout état de cause, nous estimons qu'il ne devrait pas être rendu légalement plus difficile de contracter au travers d'une telle technologie que lorsque le contrat a lieu uniquement dans le cadre du e-commerce[83].

[Rz 89] Deuxièmement, on pourrait imaginer des puces électroniques implantées permettant de signer des documents ou contrats électroniquement, comme celles de la SuisseID[84]. Cette hypothèse pose néanmoins plusieurs problèmes. Tout d'abord, dès lors que la forme légale requise serait celle de la forme écrite, il faudrait impérativement que la puce émette une signature électronique qualifiée. Celle-ci ne pouvant être obtenue qu'exclusivement chez certains fournisseurs reconnus (art. 3 SCSE), il faudrait donc impérativement passer par eux. Ensuite, on peut imaginer qu'une puce électronique RFID émise par une banque soit munie d'un numéro de référence unique qui identifierait son détenteur. De ce fait, cela rendrait son détenteur traçable et cela ferait rentrer les informations concernant l'utilisation de la puce dans la catégorie des données personnelles régulée par la LPD. Enfin, on pourrait se poser la question de savoir si l'utilisation ne devrait pas alors être équivalente à la signature électronique simple ?

[Rz 90] En dernier lieu, le problème majeur des puces électroniques RFID, quelle que soit leur utilisation, est le consentement. En effet, les puces RFID émettent en permanence leur signal, ce qui engendrerait que la réception dudit signal ne représente qu'une preuve de proximité de la puce, mais pas du consentement de son détenteur. D'un point de vue contractuel, cela empêcherait donc de pouvoir déduire du signal un consentement, sauf si ce dernier a été préalablement donné[85]. De plus, cela entraînerait qu'il faille nécessairement prendre des mesures de sécurité, par exemple un mécanisme de stoppage du débit en cas de paiements proches et répétés, ou encore prévoir un moyen de sécurité supplémentaire (p.ex. un code) en cas de paiement d'une somme importante.

[Rz 91] Ensuite, le consentement n'est pas non plus présent lors de la collection des données. Comme le soulignait le Conseil fédéral en 2005 déjà, le risque vis-à-vis de la protection des données est ainsi mis à l'œuvre[86], bien que le Parlement n'a pas jugé nécessaire de mettre en place un registre national des puces RFID en 2008[87]. En Europe, le Règlement sur la protection des données (RGDP[88]) requiert que soit effectué une analyse d'impact sur la protection des données des utilisateurs (art. 35 GDPR) pour les puces RFID et qu'une série de recommandations soient suivies[89].

---

82 A l'inverse, on pourrait imaginer des situations où le système est « *pré payé* », comme dans certains abonnements téléphoniques mobiles.

83 Par exemple, une puce électronique comprenant le nom, le prénom, l'adresse email et avec un moyen de paiement valide.

84 Cf. https ://www.postsuisseid.ch/fr/

85 P.ex. voir conditions générales de VISECA Card services, 2.1 let. e Conditions générales du 1er Juillet 2017 (https ://www.viseca.ch/Viseca/media/content/fr/conditions/conditions-generales-cartes-credit-prepaid.pdf)

86 Cf. https ://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft ?AffairId=20053067

87 Cf. https ://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft ?AffairId=20083323

88 Regulation (eu) 2016/679 of the European parliament and of the council of 27 april 2016.

89 Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification ; http ://rfid-pia-en16571.eu/ressources/documents/

c. L'implantation d'un objet dans le corps

[Rz 92] Nous traitons trois aspects ici. En premier lieu, celui de l'activité de l'implantation d'un objet dans le corps. Deuxièmement, celui de la puce en tant que matériau. Et enfin, le statut légal de cet objet une fois intégré au corps.

[Rz 93] Premier aspect, l'activité de l'implantation. A notre sens, l'implantation en elle-même ne devrait pas être autorisée librement. En effet, bien que cela soit difficilement contrôlable, cette activité doit néanmoins, par exemple pour le canton de Genève, être assimilée via la loi sur la santé genevoise (LS GE)[90] aux pratiques associées du tatouage et du piercing selon l'art. art. 2 al. 2 let. d du règlement genevoise sur les activités pouvant mettre en danger la santé (RAMDS)[91]. En effet, il existe un intérêt public qui exige qu'on ne laisse pas des gens pratiquer seuls ce genre « *d'opérations* » sur eux-mêmes ou sur les autres. En outre, l'implantation d'une puce ne devrait pas pouvoir être imposée, par exemple dans un rapport de travail[92].

[Rz 94] Deuxième aspect, l'implantation entraîne l'application des normes concernant les matériaux implantables dans un corps humain. Premièrement, selon l'Ordonnance sur les denrées alimentaires et les objets usuels de la Ordonnance sur les denrées alimentaires et les objets usuels (ODAIOUs), la puce électronique sera soumise aux exigences spécifiques pour les objets qui rentrent en contact avec la peau, notamment concernant la matière dont elle est constituée (art. 61 ss ODAIOUs). Cette exigence est complétée par l'Ordonnance sur les objets destinés à entrer en contact avec le corps humain (OCCH)[93]. Dernièrement, on note que les puces électroniques, notamment RFID ont donné lieu à plusieurs normes ISO ainsi qu'à des guides de bonnes pratiques utiles à leur implémentation[94]. Dès lors qu'elles respectent toutes ces conditions, en général, les puces électroniques devraient donc être implantables.

[Rz 95] Troisième aspect, on pourrait finalement se demander si une puce, une fois intégrée dans le corps, ne pourrait pas obtenir la qualification de prothèse ou de « *partie intégrante* » (art. 642 CC) du corps humain, ce qui entraînerait une éventuelle perte de sa qualité de chose au sens du droit civil ainsi qu'une assimilation de l'objet à la personnalité de son porteur[95]. Cette qualification demanderait que deux éléments soient réalisés. Premièrement, une liaison d'une intensité particulière et deuxièmement de se situer dans un contexte ou l'objet permet au corps de former (ou reformer) un tout dans une optique cosmétique ou médicale[96]. Il appert que la plupart des puces intégrées dans notre contexte sont liées avec une grande intensité au corps humains, dès lors qu'on ne peut pas les enlever à la façon d'une prothèse ou d'une perruque. Cependant leur fonction ne se place généralement pas à proprement parler dans une optique médicale ou cosmétique. Bien plus, elle relève d'une utilité fonctionnelle ou pratique. Toutefois, l'évolution

90 Loi sur la santé du canton Genève du 7 avril 2006 (LS ; RSG K1.03).

91 Règlement sur les activités pouvant mettre en danger la santé du canton de Genève du 27 juin 2007 (RAMDS ; RSG K3.10.03).

92 Cf. http ://www.lalibre.be/actu/belgique/travailleurs-puces-peeters-s-inquiete-du-respect-de-la-vie-privee-58d2c749cd705cd98e199570

93 RS 817.023.41, de son nom complet : Ordonnance du DFI sur les objets destinés à entrer en contact avec les muqueuses, la peau ou le système pileux et capillaire, et sur les bougies, les allumettes, les briquets et les articles de farces et attrapes du 23 novembre 2005.

94 En Suisse, le SNV (www.snv.ch) et on se réfèrera à la norme SN EN 16571 :2014 ; http ://rfid-pia-en16571.eu/ressources/documents/.

95 Oliver Kälin, *Der Sachbegriff im schweizerischen ZGB*, Diss., Zürcher Studien zum Privatrecht, Band Nr. 174, Zurich 2002, p. 106 ss.

96 *Idem.*

des mœurs et le fait que cette puce permettrait de compléter une partie manquante de l'identité dans le futur, à la différence d'un piercing ou autre, on pourrait être amenés à rediscuter de cette notion. En définitive, nous pensons qu'on ne peut pas, pour l'instant, considérer que les puces électroniques perdent leur qualité de choses, bien que l'idée soit intéressante. Par ailleurs, cette question est juridiquement pertinente dès lors qu'une telle qualification empêcherait probablement la prise de certaines actions à l'encontre du porteur d'une puce illégale, par exemple avec une identité falsifiée.

3.2. L'identité digitale à proximité

3.2.1. En général

[Rz 96] La deuxième catégorie concerne les identités digitales que nous conservons grâce à des objets détenus « *à proximité* » ou « *portables* » (ID-Card, Mobile-ID, ...). L'idée est que la possession d'un appareil externe utilisé en combinaison ou non avec d'autres moyens permettent de s'authentifier dans un système[97]. On peut citer par exemple, les puces de téléphones portables (mobile-ID), ou certaines applications (ex. TAN), ou encore la reconnaissance de l'identité digitale au travers des lecteurs de données biométriques. La plupart du temps, le degré de sécurité qui est créé par l'identification via ce genre d'appareil est plutôt élevé car ce type de support a notamment été développé dans le cadre de la téléphonie mobile et des paiements online. Dernièrement, on peut noter que ce type de technologie d'identification se recoupe souvent avec celle de l'identité sur des registres externes, où l'identité digitale est contenue dans un registre externe et est vérifiée au travers d'une application mobile par exemple.

3.2.2. Aspects légaux

[Rz 97] Similairement à ce qui a été dit plus haut, l'identité digitale devrait là aussi être soumise à la régulation exclusive sur l'identité suisse. Il faut souligner que la réglementation qui s'applique à ce type de support sera des plus diverses en fonction des appareils et des applications prévues. Le degré et le type de régulation dépendra d'une analyse au cas par cas. La plupart du temps, lorsque les intermédiaires ne mettent pas en place des services qui touchent à des activités financières, ils devraient être principalement soumis à des exigences légales en termes techniques (sécurités, matériau etc.) et de protection des données.

[Rz 98] Le deuxième aspect légal, similairement à ce qui a été dit plus haut, porte sur les aspects contractuels. En effet, on peut se demander à quelles conditions un utilisateur consent au travers d'un mécanisme d'authentification RFID[98] ? En général, l'utilisateur consent à la mise en place du système sous cette forme dans le contrat, puis son identité est vérifiée et considérée valable lors de l'installation du système (ex. réception d'un code par la poste, vérification par email, etc.).

---

97 N.B. Le système classique des cartes de compte bancaire prévoit deux étapes afin d'identifier un client : 1. La possession d'un titre (la carte bancaire) et 2. L'entrée d'un code PIN établi selon une procédure sécurisée. Voir Op.cit. 23, Blonsky, p. 11 s.

98 Cf. plus haut II.3.1.2b). N.B. Un grand magasin américain développe actuellement le concept de supermarché sans caisse ni employé. Le supermarché est truffé de capteur et le consommateur est identifié par son téléphone et débité à la sortie. Tout le contrat n'est alors que « *donnée* », et le consentement a alors lieu par acte concluant : https ://www.letemps.ch/economie/2016/12/06/amazon-teste-supermarche-futur-caisse-employe

[Rz 99] Le troisième élément que nous souhaitons pointer est celui des appareils permettant une bioreconnaissance, comme *Biowatch*[99]. Cette entreprise propose un service très innovant de bracelet de montre qui scanne les veines (données biométrique) afin d'authentifier son porteur. A l'heure actuelle, la plupart des fonctions proposées ne dépassent pas le cadre de l'identité virtuelle (ouverture de porte, déverrouillage de téléphone, allumage voiture, ...). Toutefois, les puces pourraient aussi permettre d'effectuer des petits paiements, ce qui les feraient entrer dans la catégorie de l'identité digitale, dès lors que les services financiers ont une obligation de vérifier l'identité de leurs clients.

[Rz 100] D'une part, nous estimons que ce moyen d'identification est plutôt sûr. D'autre part, comme vu plus haut, le scanning ne donne pas une preuve de consentement élevée. Par conséquent, lorsqu'un paiement d'une certaine valeur ou la passation d'un contrat ne requérant pas la forme écrite est imaginé, il faudrait alors premièrement s'assurer du consentement préalable du client et deuxièmement doubler certaines opérations d'un code PIN (ou d'une application ou autre[100]) afin de s'assurer dudit consentement. Par ailleurs, ce genre de technologie de scanning des veines présente un intérêt juridique important. Notamment, car elle permet de créer une donnée-preuve supplémentaire qui peut ensuite servir de justificatif de la passation d'un contrat oral ou simplement de paiement. Enfin, en comparaison avec un implant sous-cutané, nous pensons que ce genre de système est potentiellement plus en phase avec les mœurs de notre temps en vue d'une adoption par le grand public.

3.3. L'identité digitale sur des registres externes

3.3.1. En général

[Rz 101] Le troisième cas d'application concerne l'identité stockée sur des registres externes, par exemple les SSI (« *Self-Sovereign Identity* »).

[Rz 102] En Suisse, il existe plusieurs projets intéressants dans ce domaine, comme par exemple dans le canton de Schaffhouse, celui de la start-up Procivis[101] ou un autre à Zoug. Ce dernier vise à mettre en place une identité digitale sur la Blockchain Ethereum pour les habitants du canton[102]. Cette identité digitale zougoise permet ainsi aux citoyens d'accéder à une cyberadministration, d'emprunter des vélos ou des livres, de se parquer, et autres. L'identité des habitants est vérifiée par un agent étatique puis stockée sur la Blockchain Ethereum. Enfin, lorsque le citoyen souhaite s'authentifier, il utilise une application mobile et entre un code personnel afin d'accéder à son identité digitale.

3.3.2. Aspects légaux

[Rz 103] La valeur légale d'une identité digitale telle que celle proposée par les cantons de Zoug ou Schaffhouse revêt au moins la qualité d'une identité digitale, dès lors qu'elle est mise en place

99 Cf. http ://www.biowatch.ch/web/ ; en lien avec la note de bas de page n°97, on remarque que cette entreprise souhaite dématérialiser le processus. Ainsi, la perte de la carte ou l'oubli du code PIN n'a plus d'incidence. Les conditions de reconnaissance sont alors : 1. La personne autorisée (ou ses veines) 2. L'appareil Biowatch.

100 P.ex. confirmation du paiement via une application mobile.

101 Cf. http ://procivis.ch/2017/12/04/procivis-and-the-canton-of-schaffhausen-present-eid-solution-at-the-egovernment-day-schaffhausen/

102 Cf. http ://www.stadtzug.ch/de/bevoelkerung/dienste/digitaleid/

par le canton lui-même au travers d'une décision. De plus, on estime que l'on peut considérer ce niveau de garantie comme élevé. Dans ce contexte, on peut déplorer en revanche que la question de la signature électronique n'ait pas été traitée de pair afin que le projet soit encore plus utile. Par ailleurs, on peut se demander si la question de l'identité digitale des citoyens, tant qu'elle sera régulée par l'AP loi e-ID, n'est pas une prérogative fédérale qui exclut la compétence cantonale (art. 38 Constitution (Cst.)). A notre sens, cela devrait être le cas.

[Rz 104] Par ailleurs, on pourrait se demander si le fait d'entreposer l'identité des citoyens sur une Blockchains telle qu'Ethereum est raisonnable au niveau de la sécurité. En effet, l'utilisation de Blockchain publiques et « *internationales* » engendrent que, de fait, ces données personnelles sont disponibles dans un réseau et sortent du territoire (*outsourcing*, art. 6 LPD) vers des pays potentiellement avec une protection des données non-équivalente. De plus, un éventuel changement dans le consensus ou dans le protocole de la Blockchain, événement impossible à prévoir d'avance, fait peser un risque à notre sens intolérable, au vu du type de donnée traitées.

[Rz 105] Dernièrement, un mot sur les SSI. Ce type d'identité doit, à notre sens, être considérée comme une identité virtuelle. En effet, bien qu'elles peuvent représenter un intérêt pratique important, le fait que les informations ne sont pas vérifiées par un tiers de confiance étatique ou désigné par l'Etat rend leur niveau de garantie inexistant. Toutefois, ces solutions ont de l'avenir car la multiplication des identités virtuelles est devenue encombrante et peu pratique pour tout un chacun et l'on gagnerait à utiliser une identité virtuelle unique avec un bon niveau de protection pour, par exemple l'utilisation de Facebook, inscription newsletter, etc.

3.4. La protection des données en particulier

***Agent Smith** : You are going to help us Mr. Anderson.*

Whether you want it, or not.

[Rz 106] Dans ce passage, nous souhaitons insister brièvement sur la question de la protection des données et des quelques défis que pose la généralisation des identités digitales ou virtuelles.

[Rz 107] Premièrement, l'identité digitale forme soit des données personnelles, voire des données sensibles qui doivent être protégées efficacement par ceux qui les traitent (art. 7 LPD). Des exigences techniques élevées en terme de sécurité devraient alors s'appliquer au vu de la sensibilité des données en jeu.

[Rz 108] Deuxièmement, l'intimité que l'*homo digitalis* partage avec la technologie, l'hyperconnectivité et le développement de l'IOT font des téléphones et des supports que l'identité digitale forment, de très bons moyens de tracer des individus et d'établir des profils de personnalités (art. 3 let. d LPD) au détriment de la confidentialité. Dans ce sens, on rappellera que le consentement reste la pierre angulaire d'un traitement de donnée licite, tant au niveau de la LPD suisse que du RGDP européen. Dès lors, l'utilisation des « *traces* » de l'identité digitale, notamment à des fins commerciales devraient être prohibée dans les cas où elle n'est pas reconnaissable.

[Rz 109] Troisièmement, on peut relever la problématique de la communication transfrontière des données et de la sous-traitance. A notre sens, il conviendrait que les données propres à l'e-ID ne soient pas entreposées dans des registres à l'étranger, la question de l'identité des citoyens touchant à la défense nationale. Par exemple, on pourrait penser à utiliser nos bunkers de montagnes désaffectés comme lieu de stockage potentiel ?

[Rz 110] Quatrièmement, on note que dans le projet de révision de la LPD, les données biométriques[103] ainsi que les données génétiques seront désormais considérées comme des données sensibles[104]. Dès lors, des projets permettant une bioreconnaissance (p.ex. Biowatch) devront appliquer des normes plus élevées que pour de simples données personnelles.

[Rz 111] Dernièrement, concernant la responsabilité en cas de manquement du maître du fichier. On notera que la LPD prévoit des sanctions pénales (l'amende) en cas de révélations de données personnelles. Par ailleurs, le RGDP prévoit à son art. 83 un régime de sanction administrative dissuasif en la matière. Enfin, on note que l'AP loi e-ID pose des règles de responsabilités se basant sur le Code des obligations pour les FI et l'exploitant d'un service utilisateur, tandis que celle du service d'identité et de l'organisme de reconnaissance sont régies par une loi spéciale (art. 24 AP Loi e-ID).

103 Les données biométriques peuvent être définies comme : « *Die Biometrie im engeren Sinne widmet sich der Entwicklung und Anwendung von Verfahren, die eine automatisierte Überprüfung der behahupteten Identität von Personen (Verifizierung) oder die Findung der Identität von Menschen (Identifizierung)* » Op.cit. 23 Blonsky, p. 6. Pour les critères permettant de les qualifier comme telles, voir p. 7.

104 Cf. https ://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html

III. Conclusion

Morpheus : *What do you see. Business men, teachers, lawyers, carpenters. The very minds of the people we are trying to save. But until we do, these people are still a part of that system, and that makes them our enemy.*
You have to understand, most of these people are not ready to be unplugged. And many of them are so inert, so hopelessly dependent on the system that they will fight to protect it.

Were you listening to me Neo, or were you looking at the woman in the red dress ?

[Rz 112] En conclusion, l'usage accru des systèmes digitaux durant les siècles à venir engendrera nécessairement la création d'identités digitales élaborées et consubstantielles à notre personne. Dans le monde de demain, l'*Homo digitalis*, qu'il soit avocat ou charpentier, sera relié et connecté à un système. Dans un sens, ce système le fera exister d'une manière qui le dépasse, il sera dans la position d'un surhomme qui s'ignore dans une optique Nietzschéenne.

[Rz 113] Dans ce premier volet, nous avons pu souligner l'importance du développement de l'identité digitale. En plus de permettre tout une gamme de nouveaux services, cette notion permettra à tout un chacun d'exister de manière plus complète, autant physiquement et digitalement, et pour reprendre un concept du film Matrix : « *des deux côtés du téléphone* ».

[Rz 114] Enfin pour conclure, nous dirons que l'implémentation de n'importe quelles technologies dépendra le plus souvent de la politique et des régulations mises en place. En une phrase, nous pensons que la technologie doit être au service de l'homme et de la société. Mais si l'identité digitale contribuera à ce que l'*homo digitalis* existe, il convient cependant de rester prudent. Tel qu'illustré par la scène « *The woman in the red dress* », ne laissons pas les tentations de l'identité digitale nous distraire de notre raison, et devenir un système qui pourrait se changer en notre ennemi.

Gabriel Jaccard, Doctorant en droit à l'Université de Genève