Executive summary n° 1

Pour la reconnaissance d'un droit à des identités numériques multiples[1]

Juillet 2020

*Claire Levallois-Barth (*claire.levallois@imt.fr)

Coordinatrice de la Chaire VP-IP, Enseignante-chercheure à Télécom Paris

Identité civile, identité réelle, identité personnelle, identité biologique, identité professionnelle, identité régalienne. Ces possibilités d'identités, subies ou souhaitées, témoignent de l'importance d'établir qu'une personne est bien celle qu'elle prétend être ou que nous présumons être. Elles nous confrontent à l'écriture d'une nouvelle structure sociale portée dans les textes juridiques, notamment, au niveau européen, ceux concernant les modalités d'identification des personnes aux frontières, l'identification électronique[i] ou la sécurisation des cartes d'identité des citoyens européens[ii]. Au niveau français, les institutions impliquées dans le débat confirment l'importance des enjeux, qu'il s'agisse de la mission interministérielle sur les solutions d'identité numérique sécurisée[iii], du Conseil national du numérique[iv] ou de l'Assemblée nationale[v].

Parmi les thématiques, on retiendra principalement la question du contrôle par l'utilisateur de ses identités ainsi que la difficulté à formaliser la notion d'identité numérique. En philosophie, une manière d'aborder cette problématique consiste à distinguer l'identité *Idem* et l'identité *Ipse*. « *L'identité* Idem *correspond à un regard porté sur l'individu de l'extérieur, qui le considère comme une somme de caractéristiques stables. L'identité* Ipse *correspond … à l'individu tel qu'il se rapporte à lui-même* »[vi]. Le droit de son côté privilégie une approche objective, la notion d'« identité » pouvant être définie comme « *ce qui fait qu'une personne est elle-même et non une autre ; par extension, ce qui permet de la reconnaître et de la distinguer des autres ; … l'ensemble des caractères qui permettent de l'identifier* »[vii].

L'identité numérique ne correspond pas pour autant à une transposition de l'identité civile dans le cyberespace. L'accroissement exponentiel des types d'attributs permis par la dématérialisation fait ainsi ressortir la nécessité de parler non pas **d'une** identité numérique mais **des** identités numériques (I). Si nos identités sont construites et attribuées par les acteurs publics et privés, il ne faut pas perdre de vue la nécessité d'établir les conditions permettant à la personne d'agir de façon autonome pour qu'elle puisse déterminer elle-même la façon dont elle entend se présenter aux autres (II). La prise en compte de ces deux aspects – qu'on désignera par identité objective et

[1] Résumé de l'article rédigé pour un ouvrage publié aux éditions Larcier *L'identité numérique : quelle définition pour quelle protection ?*, sous la direction de J. Eynard, en décembre 2020.

identité subjective – nous paraît essentielle. Elle doit, selon nous, se traduire par la reconnaissance d'un droit à des identités multiples.

I. Les identités numériques, une notion polysémique

Selon une approche civiliste, l'identité correspond à un regard porté sur l'individu par l'État, en particulier à travers la constatation de l'état civil. Ce regard extérieur considère la personne comme une somme de caractéristiques stables (nom de famille, prénom, filiation, lieu et date de naissance, nationalité et sexe) pour l'identifier sans équivoque dans la continuité[viii]. Il s'agit d'asseoir l'emprise de l'État-nation sur la personne envisagée abstraitement[ix]. Le changement possible de certaines caractéristiques traditionnelles (sexe, nom de famille) conduit à retenir de nouveaux attributs comme un numéro (« *numéro de sécurité sociale* », identifiant unique persistant[x]) ou des éléments fournis par le corps (ADN, iris, main, voix, réseau veineux). Dans cette logique, une photographie faciale et deux empreintes digitales offrant une identification supposée infaillible, renforcent la sécurité des cartes d'identité[xi], des passeports biométriques[xii] ainsi que la quasi-totalité des systèmes d'informations à grande échelle dans le cadre de gestion des frontières et de l'ordre public de l'Union européenne[xiii].

On observe ainsi, dans la prise en compte des éléments contribuant à caractériser un individu, un élargissement des attributs considérés. Cet élargissement entend concourir contribuer à mieux identifier une personne – pour des raisons de sécurité et pour établir un climat de confiance lors de l'utilisation des services publics et privés en ligne – mais aussi à l'individualiser davantage à partir d'éléments extrêmement variables. La jurisprudence découlant du délit d'usurpation d'identité d'un tiers[xiv] sanctionne notamment la création de faux compte *Facebook*, sous le nom et le prénom d'un tiers, comprenant des photographies personnelles[xv].

Autour d'un noyau dur des attributs considérés comme les plus stables, l'identité numérique d'une personne peut être perçue comme la conjonction de nombreuses données personnelles[xvi], disséminées dans le monde virtuel ou réel. Nul besoin de s'enquérir du nom de la dite personne. La technologie permet désormais de *« lui attribuer certaines décisions dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son **identité au sens étroit du terme »***[xvii]. Il importe donc de considérer l'impact de l'usage d'une agrégation d'informations sur la personne[xviii] susceptible de tracer, de distinguer (et donc de traiter différemment) une personne parmi d'autres[xix].

Le choix de ces d'éléments et leur mise en valeur peuvent être décidés volontairement par la personne, dans ce qu'elle perçoit comme la caractérisant. À côté de cette **identité numérique personnelle**, l'individualisation peut être initiée par les acteurs privés[xx] non pas via quelques profils types mais, à l'heure de « l'Intelligence Artificielle », d'une modélisation des comportements humains à partir de données individuellement a-signifiantes[xxi]. Apparaît une nouvelle sorte d'identité, l'**identité numérique algorithmique.** Cette identité calculée se situe dans un mouvement général de réification de l'individu et propose une vision nécessairement partielle, déformée de celui-ci. Elle se distingue de l'**identité numérique régalienne**, définie comme l'adaptation de l'état civil à l'ère numérique, basée sur quelques critères estimés stables (nom et prénom, identifiant univoque persistant dans le temps, données biométriques).

Cependant, cette conception des identités numériques qui tend à transformer l'être humain en un objet statique, nous interroge. Doit-on laisser aux seuls acteurs privés et à l'État le soin de la

déterminer ? Qu'en est-il de nos individualités, de la possibilité de nous construire de notre propre initiative et enfin d'échapper au confinement algorithmique ?

II. L'autonomie de la personne dans la détermination de ses identités numériques

L'identité numérique doit aussi être entendue comme la possibilité pour une personne de se « *projeter* » en choisissant les éléments qu'elle souhaite voir représentés et reconnus. Cette *ipse* correspond à une identité comme ouverture active vers les autres et la société.

La reconnaissance du droit pour chacun d'établir les éléments de son identité se fonde sur une interprétation du droit au respect de la vie privée reconnu par l'article 8 de la Convention européenne des droits de l'Homme[xxii]. La notion de « *vie privée* » est ainsi une notion fonctionnelle, voire extensive. À cet égard, « *l'article 8 protège un droit à l'identité et à l'épanouissement personnel et celui de nouer et de développer des relations avec ses semblables et le monde extérieur* »[xxiii]. À cet épanouissement contribue l'établissement des détails de son identité physique et sociale d'être humain, le droit d'un individu à de telles informations étant essentiel du fait de leurs incidences sur la formation de la personnalité[xxiv].

La construction de l'identité par la personne qui en recherche les composantes s'explique par la revendication de mettre en adéquation ces composantes avec l'identité vécue, ressentie. Elle constitue une condition de développement de nos personnalités, du respect de nos dignités « *étant entendu que la dignité s'étend au sens kantien, c'est-à-dire comme exigence vis-à-vis de son action de considérer autrui comme but, et non comme moyen* »[xxv]. Ainsi, la **Cour européenne des droits de l'Homme** ne comprend pas le droit au respect de la vie privée **uniquement comme la protection de l'intimité** de la personne à l'abri du regard des tiers mais aussi comme une ouverture vers l'extérieur permettant d'*« entretenir des rapports avec d'autres êtres humains* » et, plus largement, comme le droit à l'autonomie personnelle[xxvi].

Il appartient donc à notre société démocratique d'assurer la possibilité de nous permettre d'agir sur la construction de notre identité future mais aussi de faire disparaître certains aspects du passé[xxvii]. L'enjeu porte sur le respect du libre arbitre informationnel de chacun. Il ne s'agit pas d'un cas d'école comme en témoigne la politique du « nom réel », pratiquée notamment par *Facebook* et qui a conduit le réseau à supprimer les comptes de transgenres, *drag queens*, homosexuels, natifs américains, dissidents politiques.

Toute la difficulté est alors de maintenir une forme de contrôle dans un environnement numérique où l'individu en dispose de moins en moins. Assurer à la personne une certaine maîtrise sur ses identités implique de s'intéresser aux contextes dans lesquels elle exprime sa personnalité. Nous ne partageons pas les mêmes informations, nous ne construisons pas notre relation de la même manière dans un milieu familial, professionnel, amical ou ludique. Cette assertion est confirmée par le sondage réalisé par la Chaire Valeurs et Politiques des Informations Personnelles en avril 2019 avec Médiamétrie[xxviii].

De nombreux acteurs semblent cependant aller à l'encontre de cette exigence **d'identités en contexte**. Des entreprises du numérique investissent des secteurs d'activités autrefois séparés (culture, information, finance, assurances…). La même identité « privée » est utilisée pour effectuer des achats en ligne, participer à un forum politique ou dans un contexte professionnel. L'identité

Google, quasi-indispensable pour se connecter à des milliers de services tiers, *Facebook Connect*, *Apple ID* ou *Azure AD* participent également à ce mouvement d'enfermement de la personne dans leurs écosystèmes respectifs. Une seconde tendance concerne l'unification des identités numériques régaliennes et privées. En Estonie, depuis 2002, la carte d'identité électronique sert à la fois de carte nationale d'identité et de moyens d'identification en ligne auprès de services publics et privés[xxix]. Cette propension lourde à la fusion de contextes *a priori* étrangers est accentuée par l'amélioration du niveau de sécurité des identités « privées », proposées pour l'instant par peu d'acteurs[xxx].

***

De tels choix ne peuvent être opérés à l'abri du contrôle démocratique par accumulation d'initiatives ponctuelles. Afin de ne pas subir les effets d'une identification univoque généralisée par quelque acteur que ce soit, il s'agit de renforcer l'effectivité au droit au respect de la vie privée en reconnaissant **un nouveau droit subjectif, le droit à des identités numériques multiples**, dont l'exercice garantirait le développement personnel. Ce droit comprendrait la possibilité de ne pas dévoiler sa véritable identité et de ne pas subir de représentation forcée. Il permettrait de préserver une certaine forme d'anonymat. On objectera, au mouvement de défiance de la classe politique[xxxi], qu'il s'agit d'un anonymat relatif, l'autorité compétente pouvant toujours adresser une demande de levée d'identité au fournisseur d'accès à Internet et remonter à l'origine d'un message.

Si l'utilisation de l'identité numérique régalienne ne doit être imposée que dans les situations nécessaires afin d'éviter une traçabilité permanente, les identités alternatives peuvent, si besoin, dériver de l'identité stable à la condition que l'individu puisse définir la granularité des détails qu'il souhaite projeter. Enfin, le droit à la multi-identités revêt un caractère relatif : comme tout droit, il doit s'entendre comme une pondération des intérêts en présence, entre le besoin légitime de tout individu de se présenter comme il l'entend, la protection de l'intérêt des tiers et de l'intérêt général par le recours à une identité régalienne.

En somme, deux points de vue doivent être conciliés : l'identité numérique objective qui est établie par les autorités ou acteurs extérieurs et l'identité numérique subjective, davantage déterminée par nos choix. En ce sens, le RGPD n'est qu'une brique de protection à laquelle d'autres briques doivent être ajoutées. Il y a potentiellement urgence, car si le droit ne s'accommode pas aux changements accélérés de notre époque, il sera conduit à entériner les solutions technologiques déjà déployées[xxxii].

---

[i] Règlement (UE) 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, JOUE L 257/73 du 28 août 2014 (Règlement eIDAS), https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR.

[ii] Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation, JOEU L 188/67 du 12 juillet 2019 (Règlement Cartes d'identité), https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R1157. Concrètement, la France doit faire évoluer sa carte d'identité nationale pour août 2021.

[iii] Lettre de mission de Valérie Peneau signée le 5 janvier 2018 par le ministre de l'Intérieur, Gérard Collomb, la Garde des Sceaux, Nicole Belloubet, et le secrétaire d'État au Numérique, Mounir Mahjoubi, https://www.interieur.gouv.fr/Archives/Archives-ministres-de-l-Interieur/Archives-Gerard-Collomb-mai-2017-

octobre-2018/Communiques-du-ministre/Mise-en-place-de-solutions-d-identite-numerique-securisee-lancement-d-un-programme.

[iv] Conseil National du Numérique, Identités numériques. Clés de voûte de la citoyenneté numérique, Rapport Juin 2020, https://cnnumerique.fr/files/uploads/2020/2020.06_rapport_cnnum_idnum_web.pdf.

[v] Rapport d'information déposé en application de l'article 145 du règlement par la mission d'information commune sur l'identité numérique et présenté par Mme Marietta Karamanli, présidente, Mme Christine Hennion et M. Jean-Michel Mis, rapporteurs, députés enregistré à la présidence de l'Assemblée nationale le 8 juillet 2020, http://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information.pdf.

[vi] A. Khatchatourov, « Les régimes numériques de gestion des identités : de l'exercice de la *privacy* à la modulation de soi », *in Identités numériques en tension : entre autonomie et contrôle*, A. Khatchatourov en collaboration avec P.-A. Chardel, A. Feenberg et G. Peries, Londres, ISTE Editions, 2019, p. 34.

[vii] G. Cornu (G.) (dir.), *Vocabulaire juridique*, 8e éd., Paris, P.U.F., « Quadrige », 2007, p. 463.

[viii] « *Une continuité ininterrompue entre le premier et le dernier stade du développement de ce que nous tenons pour le même individu … : ainsi disons-nous du chêne qu'il est le même, du gland à l'arbre entièrement développé* ». Paul Ricœur, Soi-même comme un autre, 1990, éd. Le seuil, p. 142.

[ix] Dans ce sens, J. Rochfeld, *Les grandes notions du droit privé*, PUF, 2013, 2e édition, p. 40.

[x] Le règlement (UE) eIDAS et son règlement d'exécution 2015/1501 imposent au côté des éléments classiques que sont le(s) « *nom(s) de famille actuel(s) », le(s) « prénom(s) actuel(s) » et la date de naissance, la création par chaque État membre d'un « identifiant unique… qui soit aussi persistant que possible dans le temps* ». Ces quatre éléments constituent un ensemble minimal de données d'identification personnelle qui doit représenter « *de manière univoque* » la personne, permettant ainsi d'établir son identité. C'est bien ici la continuité de l'individualisation que l'on cherche à atteindre. Annexe du règlement d'exécution (UE) n° 2015/1501 de la Commission européenne du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, §8 du règlement eIDAS précité, JOUE L 235/1 du 9 sept. 2015.

[xi] Art. 3-5 du règlement Cartes d'identité, précité.

[xii] Art. 1 §2 du règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JOUE L 385/1 du 29.12.2004, modifié par le règlement (CE) n° 444/2009 du Parlement européen et du Conseil du 28 mai 2009, JOUE L 142 du 6 juin 2009.

[xiii] Afin de faciliter principalement l'identification des citoyens non européens qui franchissent ou envisagent de franchir les frontières de l'Union, deux règlements européens adoptés le 20 mai 2019 établissent les conditions d'interopérabilité des systèmes d'information dans les domaines, d'une part, des frontières et des visas (Règlement 2019/8174) et, d'autre part, de la coopération policière et judiciaire, l'asile et l'immigration (Règlement 2019/8185). Pas moins de huit systèmes d'information sont concernés : le système d'information Schengen (SIS), le système d'information sur les visas (VIS), le système Eurodac, la base de données d'Interpol sur les documents de voyage volés et perdus (SLTD) et les données d'Europol ainsi que trois nouveaux systèmes : le système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS) et le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN). Tous, sauf ETIAS, stockent des empreintes digitales et contiendront à terme l'image faciale. Le SIS comprend également l'empreinte palmaire.

[xiv] Plus précisément, l'article 226-4-1 du code pénal introduit par la loi du 14 mars 2011 dispose : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende* ». Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite « LOPPSI 2 »), JORF 15 mars 2011, p. 4582.

[xv] TGI, 17e ch. correctionnelle, jugement du 24 mars 2015, V. P. et F. Z. / A. S. et K. G, https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-17e-chambre-correctionnelle-jugement-du-24-mars-2015/.

[xvi] Cette notion est définie par le Règlement Général sur la Protection des Données (RGPD) comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », la personne « identifiable » est entendue comme celle *« qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, … ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ». Art. 4-1 du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L 119 du 4.5.2016, p. 1, ci-après RGPD.

[xvii] Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 15.

[xviii] Créées notamment par les réseaux, les objets connectés, les logiciels de reconnaissance faciale.

[xix] Dans ce sens, Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel telle qu'actualisée par le Protocole d'amendement STCE n°223 adopté le 18 mai 2018 (Convention 108 plus), point 18 du rapport explicatif qui précise : « *Cette individualisation pourrait se faire, par exemple, en se référant à la personne spécifiquement ou à partir … d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un appareil ou un ensemble d'appareils (ordinateur, téléphone portable, appareil photo, console de jeux, etc.)* ».

[xx] La publicité comportementale, par exemple, singularise l'utilisateur à l'aide d'une empreinte numérique unique stockée à distance, sur le serveur de l'opérateur. Cette empreinte (ou *fingerprinting*) est calculée notamment à partir des différentes polices de caractères installées et utilisées par son navigateur, des connexions réseaux ou de l'empreinte sonore de son ordinateur. Si *a priori* ces informations utilisées seules paraissent anodines, il est très peu probable que deux ordinateurs aient la même liste de polices.

[xxi] Comme le souligne Antoinette Rouvroy, « *ainsi ne sommes-nous bien souvent même plus identifiables comme auteurs ni émetteurs des données « qui comptent » et qui nous gouvernement : les « données brutes », lesquelles sont de fait soigneusement nettoyées des traces de leur contexte originaire et toute signification singulière … Il en résulte que, contrairement à l'intuition majoritaire, nous n'avons peut-être jamais été, dans nos singularités respectives, moins significativement visibles dans l'univers numérique …Nous ne faisons plus « autorité » en tant qu'individus, pour rendre compte de nous-mêmes face au profilage algorithmique … Ce qui est réel n'importe pas* ». A. Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », Étude annuelle du Conseil d'État « Le numérique et les droits fondamentaux », Paris, 2014, p. 3, https://works.bepress.com/antoinette_rouvroy/55/.

[xxii] Art. 8-1 de la Convention européenne des droits de l'Homme selon lequel « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

[xxiii] CEDH, aff. *Bensaid c. Royaume-Uni,* n° 44599/88*,* 6 févr. 2001, §47.

[xxiv] CEDH, aff. *Mikulić c. Croatie*, n° 53176/99, 7 fév. 2002, §54, CEDH 2002-I. Également *Odièvre c. France* [GC], n° 42326/98, § 29, CEDH 2003-III qui se réfère à « *l'intérêt vital, protégé par la Convention, à obtenir des informations nécessaires à la découverte de la vérité concernant un aspect important de son identité personnelle* ».

[xxv] Y. Poullet, *La vie privée à l'heure de la société du numérique*, 2018, Larcier, CRIDS, p. 76.

[xxvi] Dans ce sens, CEDH, aff. *Pretty c. Royaume-Uni*, n° 2346/02, 29 avr. 2002, CEDH 2002-III, §61 à propos d'une demande de suicide assisté : « *La Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8* ».

[xxvii] À cet égard, l'article 17 Droit à l'effacement (« droit à l'oubli ») du RGPD, précité, apporte une réponse partielle en instaurant le nouveau droit à l'effacement également appelé droit à l'oubli

[xxviii] Chaire Valeurs et Politiques des Informations Personnelles de l'Institut Mines-Télécom, Deuxième étude sur les données personnelles – synthèse de résultats, avr. 2019, https://cvpip.wp.imt.fr/2019/09/26/31-octobre-2019-18e-rencontre-deuxieme-enquete-cvpip-mediametrie/.

- Sur les forums, blogs ou sites d'actualité, 8% des internautes recourent à une identité alternative, 75% à un pseudonyme,
- Sur les sites d'achat en ligne, 90% se servent de leur « véritable » nom et prénom,
- Dans le cadre des réseaux sociaux, les faux noms et prénoms ou les pseudonymes sont utilisés par 47% des répondants dans un réseau non professionnel et 29 % dans un réseau professionnel.

[xxix] Paiement des impôts, consultations médicales et achats de médicaments sur ordonnance, votes, accès aux transports en commun, suivi des résultats scolaires des enfants à l'école, demande de subvention agricole …..

[xxx] Pour l'instant, l'offre des fournisseurs d'identités porte essentiellement sur le niveau de garantie eIDAS « faible». Par exemple, à la date du 4 juin 2020, l'utilisateur du fédérateur d'identités France Connect peut choisir parmi six offres s'il souhaite bénéficier d'une garantie « faible » (impots.gouv.fr, ameli.fr, L'identité Numérique La Poste, MobileConectetmoi, msa.fr et Alicem). Cependant, il n'a pas d'autre possibilité que d'utiliser L'Identité Numérique de La Poste pour obtenir une garantie de niveau « substantiel ».

[xxxi] 2e grand débat national, 18 janv. 2019, « Emmanuel Macron avance à découvert sur la levée de l'anonymat sur la toile », Zdnet, 24 janv. 2019, https://www.zdnet.fr/actualites/emmanuel-macron-avance-a-decouvert-sur-la-levee-de-l-anonymat-sur-la-toile-39879737.htm.

[xxxii] Un exemple nous est fourni dans le cadre du renforcement de la sécurité des cartes d'identité des citoyens. Le Contrôleur européen à la protection des données relève qu'il n'est pas possible de retenir la technologie qui stocke et compare des points caractéristiques extraits des empreintes digitales (technologie 1), alors que cette technologie est plus à même de limiter le risque d'usurpation d'identité en cas de violation de données. Pour des raisons d'interopérabilité des systèmes nationaux déjà déployés, la solution qui stocke et compare l'ensemble des images d'empreintes digitales doit être retenue (technologie 2) car s'il est impossible pour un État qui a déjà déployé la solution 1 d'obtenir une image d'empreintes digitales à partir des points caractéristiques de la solution 2. Avis 7/2018 du CEPD sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents du 10 août 2018, §§ 45 à 48, https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_fr.pdf.