SciencesPo

CHAIRE DIGITAL, GOUVERNANCE ET SOUVERAINETÉ

LES ENJEUX PARADOXAUX DE L'IDENTITÉ NUMÉRIQUE RÉGALIENNE

Bénédicte BEVIERE-BOYER

Maître de conférences – HDR en droit privé
Centre de droit privé et droit de la santé de l'Université de Paris

Juin 2022

TABLE DES MATIERES

Résumé analytique

Dans un contexte de dématérialisation croissante des services publics et privés, l'identité numérique connaît un déploiement considérable en matière de contrôles dans les aéroports, de démarches administratives, d'achats en ligne, de gestion et d'utilisation des données de santé.

Elle devrait prendre à l'avenir un essor encore plus important par la dématérialisation des documents d'identité et des titres sécurisés, omniprésents dans toutes les activités humaines *via* le smartphone des personnes. Elle se complète par la mise en place de portefeuilles numériques, permettant de s'identifier numériquement, de stocker et de gérer, sous forme électronique, des données d'identifications (carte d'identité, passeport électroniques, données biométriques), des documents officiels (diplômes, permis de conduire), ainsi que d'autres informations personnelles (Mon Espace santé), l'enjeu étant de faciliter le recours à l'identité numérique à l'occasion de multiples services publics et privés.

L'identité numérique constitue par conséquent un outil stratégique majeur autant pour l'Etat français que pour l'Union européenne. Elle doit faire l'objet d'une attention renforcée et être consolidée compte-tenu de la concurrence des entreprises privées, particulièrement les géants du numérique, mettant en place des identités numérique privées de plus en plus utilisées par le public. Leur développement est d'autant plus préoccupant qu'elles sont associées à des objectifs commerciaux, éloignés des enjeux de l'identité numérique des États membres associés à leur souveraineté, de déploiement des activités européennes, à l'intérêt général et à la protection des citoyens en termes de libertés et de vie privée.

A ce titre, l'identité numérique régalienne doit indiscutablement être consolidée au profit des enjeux d'intérêts publics. Objet d'enjeux paradoxaux, une vigilance s'impose à l'égard des actions qui sont menées en raison des atteintes potentielles aux libertés et à la vie privée.

Introduction

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques », Article 1er de la loi informatique et libertés.

1. **Le développement démultiplié de nouvelles formes d'identités numérique par l'essor des nouvelles techniques d'identification.** L'identité numérique[1] ne cesse de se déployer dans un contexte croissant de dématérialisation des services publics et privés : contrôles dans les aéroports, démarches administratives, achats en ligne, de gestion et d'utilisation des données de santé. Elle devrait prendre à l'avenir un essor encore plus important par la dématérialisation des documents d'identité et des titres sécurisés, omniprésents dans toutes les activités humaines *via* le smartphone des personnes[2]. La période Covid-19 2020-2022 a accéléré son recours et transformé son appréhension[3]. Initialement associée à l'identité civile constituée par l'« *ensemble des éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique (dans la société, au regard de l'état*

[1] Sur le sujet : C. Prebissy-Schall, « La nouvelle carte d'identité électronique comme support nécessaire d'une identité numérique qui tarde à être mise en œuvre… », Le Club des juristes, 9 avril 2021, https://blog.leclubdesjuristes.com/la-nouvelle-carte-didentite-electronique-comme-support-necessaire-dune-identite-numerique-qui-tarde-a-etre-mise-en-oeuvre-par-catherine-prebissy-schnall/; A. Bensoussan Avocats, « L'identité numérique 5.0 », Livre blanc, 03/12/2021, https://www.alain-bensoussan.com/download/livre-blanc-identite-numerique-5-0/ ; J. Eynard, (sous la direction de), « L'identité numérique : quelle définition pour quelle protection », Larcier, 2020 ; E. Caprioli., « Les enjeux de l'identité numérique », L'usine digitale, 20 janvier 2019, électronique et aux services de confiance pour les transactions électroniques , la loi n°2016-1321 du 7 octobre 2016 pour une République numérique ; M. Bardin., « L'identité numérique et le droit : esquisse d'une conciliation difficile », Hermès 80., 2018, n°78, p.273 ; N. Chambardon, « L'identité numérique de la personne humaine : contribution à l'étude du droit fondamental à la protection des données à caractère personnel », Thèse Lyon II, 2018, https://hal.archives-ouvertes.fr/tel-02464483; T. Douville., «Enfin un cadre juridique général pour l'identification électronique ! »., D. 2018., p.676 ; E. Netter., « Numérique et grandes notions du droit privé », Ed Ceprisca Collection essais, Janvier 2019., p. 48 à 159 ; J. Pierre, « Génétique de l'identité numérique – Sources et enjeux des processus associés à l'identité numérique », Les cahiers du numérique 2011/1 (Vol7), p.15-29, https://www.cairn.info/revue-les-cahiers-du-numerique-2011-1-page-15.html;

[2] Pour une illustration permettant de mieux rendre compte de l'intégration croissante de l'identité numérique dans la vie quotidienne des personnes, vidéo Thales, « Dématérialisation des documents d'identité et titres sécurisés : bienvenue dans le monde du Digital ID Wallet », https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/identite/digital-id-wallet

[3] B. Bévière-Boyer, « L'identité civile numérique nationale, une priorité en matière de souveraineté et de protection des citoyens », Actu-Juridique.fr, 23/09/2020, https://www.actu-juridique.fr/ntic-medias-presse/lidentite-civile-numerique-nationale-une-priorite-en-matiere-de-souverainete-et-de-protection-des-citoyens/

civil): nom, prénom, date de naissance, filiation »[4] *par le biais de* la carte d'identité ou encore par le passeport, elle se rapporte désormais plus à l'identité personnelle, unique, personnalisée, singulière, permettant d'identifier une personne physique compte-tenu de ses caractéristiques, de ses attributs spécifiques (empreintes digitales, œil, reconnaissance faciale, ADN), de son jumeau numérique, double virtuel.

2. **L'identité numérique régalienne rattachée au pouvoir exclusif des États**. Les États membres de l'Union européenne ont traditionnellement pour fonction de mettre à disposition différents services et moyens ayant des finalités d'intérêt général et de protection des intérêts particuliers. A ce titre, ils sont chargés de garantir la véracité et la protection des données d'identité pour l'état civil. Disposant de compétences exclusives en matière d'attribution de la nationalité, ils sont souverains en matière d'identité nationale[5], rattachée à la vérification officielle de la qualité des personnes à l'aide de la carte d'identité ou du passeport numérisé. L'identité numérique régalienne dépend ainsi principalement des États en vertu du droit international public. Elle se rattache aussi de plus en plus au droit européen intervenant activement dans le domaine technique aux fins d'harmonisation des moyens d'identification, ce qui renvoie à l'interopérabilité des systèmes numériques des États membres de l'Union européenne (UE). Cette stratégie est destinée non seulement à consolider l'identité numérique des États membres, mais aussi à faciliter la libre circulation des personnes et à fluidifier les transactions des biens et services numériques. Elle se complète par la mise en place de portefeuilles numériques, permettant de s'identifier numériquement, de stocker et de gérer sous forme électronique des données d'identifications (carte d'identité, passeport électroniques, données biométriques), des documents officiels (diplômes, permis de conduire), ainsi que d'autres informations personnelles (Mon Espace santé), l'enjeu étant à la fois de faciliter le recours à l'identité numérique, et le recours à de multiples services publics et privés.

3. **La France, *leader* en matière d'identité numérique.** Ayant pris la mesure de toute l'importance de la transformation numérique destinée à renforcer la souveraineté numérique nationale, la France est à l'origine de plusieurs initiatives en s'affirmant comme leader en matière d'identité numérique. Ont ainsi été déployés le programme interministériel *France Identité numérique*[6],

[4] G. Cornu., Vocabulaire juridique, Association Henri Capitant., Ed Quadridge/Presses universitaires de France., janvier 2001., p.431.
[5] J. Keller, C. Levallois-Barth, « La fragile définition de l'identité européenne par ses valeurs numériques », Revue générale du droit, Chronique du droit de l'Union, 2021, https://www.revuegeneraledudroit.eu/wp-content/uploads/PRGD_2021076_1.pdf
[6] Programme interministériel France Identité numérique, https://france-identite.gouv.fr/

FranceConnect[7], portefeuille d'identités numérique ayant pour objectif de « *sécuriser et simplifier la connexion à plus de 1000 services en ligne* » et la nouvelle carte d'identité électronique (*CNIe*), lancée depuis le 15 mars 2021. Celle-ci, contenant une puce stockant différentes informations, comprend différentes données personnelles telles que les données biométriques, les empreintes digitales et la photographie de la personne concernée[8]. Le décret n°2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique (SGIN)[9], le décret n°2021-279 du 13 mars 2021 portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé « titres électroniques sécurisés » (TES), l'avis n° 2021-2080 du 7 octobre 2021 concernant deux projets de décrets relatifs aux catégories de données devant être conservées en application de l'article L. 34-1 du CPCE et l'article 6 de la loi n° 2004-575 pour la confiance dans l'économie numérique[10], sont venus conforter les dispositifs mis en place. Le « *Contrat stratégique de la filière « industries de sécurité* » » du 29 janvier 2020, comprend aussi un pilier destiné à « *permettre le développement rapide du déploiement et de l'utilisation de l'identité numérique en France*»[11]. Ces initiatives successives constituent des réponses au rapport d'information, déposé le 8 juillet 2020 auprès de l'Assemblée nationale portant sur « *L'identité numérique* », par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis[12],qui avaient mis en exergue toute la nécessité de renforcer le dispositif existant, dans la continuité d'autres textes en lien avec l'identité numérique, notamment, la loi n°2018-493 du 20 juin 2018 relative à la protection des données

[7] France-Connect, https://franceconnect.gouv.fr/

[8] Ministère de l'intérieur, « La nouvelle carte nationale d'identité », 03/05/2021, https://www.interieur.gouv.fr/actualites/actu-du-ministere/nouvelle-carte-nationale-didentite La puce contient: « Les données d'état-civil du titulaire du titre : le nom de famille, les prénoms, la date et le lieu de naissance, le sexe, la taille, la nationalité, le nom dont l'usage est autorisés par la loi ; le domicile ou la résidence de l'intéressé ou, le cas échéant, le lieu où il a fait élection de son domicile dans les conditions prévues à l'article L.264-1 du code de l'action sociale et des familles, et si celui le demande ; la date de délivrance et la date de fin de validité du document, le numéro de la carte, l'image numérisée de la photographie, l'image numérisée des empreintes digitales de deux doigts ».

[9] Ce décret abroge le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ». Il est publié au JORF n°0098 du 27 avril 2022, Texte n°27, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825

[10] L'avis n° 2021-2080 du 7 octobre 2021 concernant deux projets de décrets relatifs aux catégories de données devant être conservées en application de l'article L. 34-1 du CPCE et de l'article 6 de la loi n° 2004-575 pour la confiance dans l'économie numérique, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044315808

[11] Conseil national de l'industrie, « Contrat stratégique de la filière « industries de sécurité » 2020-2022 », 29 janvier 2020, https://www.conseil-national-industrie.gouv.fr/files_cni/files/csf/Securite/dossier-presse-signature-csf-securite-janv-2020.pdf

[12] Assemblée nationale Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique » a été déposé le par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis, https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information

personnelles[13], l'Ordonnance n°2017-1426 du 4 octobre 2017 relative l'identification électronique et aux services de confiance pour les transactions électroniques[14] et la loi n°2016-1321 du 7 octobre 2016 pour une République numérique[15].

4. **L'Union européenne, moteur du renforcement de l'identité numérique régalienne.** L'Union européenne, sensible à la nécessité de consolider le Marché Commun Numérique, a déclaré l'identité numérique comme stratégie prioritaire pour la période 2019-2024[16] en ayant pour objectif de faciliter l'interopérabilité des identités numériques des États membres, tout en garantissant des niveaux de sécurité élevés. Suite à ses communications du 19 février 2020 « Façonner l'avenir numérique de l'Europe »[17] et du 9 mars 2021 « Une boussole numérique pour 2020 : l'Europe balise la décennie numérique »[18], elle a initié la révision du règlement *eIDAS* par la proposition de règlement du Parlement européen et du Conseil du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne fiable, applicable autant pour les secteurs publics que privés[19]. Son ambition est forte et exprimée en ces termes : *« La mise en place d'un cadre européen relatif à une identité numérique fondé sur la révision du cadre actuel devrait permettre à au moins 80% des citoyens d'utiliser une solution d'identification numérique pour accéder à des services publics essentiels d'ici à 2030 »*[20]. Cette démarche est à envisager dans un contexte plus global, en lien particulièrement avec le règlement (UE) 2019/1157 du 20 juin 2019 du Parlement européen et du Conseil 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

[13] JORF n°0141 du 21 juin 2018, Texte n°1., https://www.legifrance.gouv.fr/eli/loi/2018/6/20/jusc1732261l/jo/texte

[14] Ordonnance n°2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques, JORF n°0233 du 5 octobre 2017, texte 2, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035720606 ; Dossier législatif : https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000035722616/

[15] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id

[16] Identité numérique européenne, présentation sur le site de la Commission européenne, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr

[17] COM(2020) 67 final, « Façonner l'avenir numérique de l'Europe », 19 février 2020, https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_fr.pdf

[18] COM(2021) 118 final/2, « Boussole numérique 2020 : la voie européenne pour la décennie numérique », https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

[19] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

[20] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

membres de leur famille exerçant leur droit à la libre circulation[21], le règlement (UE) du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications[22], le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)[23], le règlement eIDAS 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[24] et l'article 8 de la Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000 consacrant le « droit à la protection des données personnelles »[25].

5. **L'identité numérique régalienne des États potentiellement concurrencée par les identités numériques privées.** La consolidation de l'identité numérique régalienne des États est d'autant plus justifiée et indispensable que des identités numériques privées sont en plein déploiement par les géants du numérique, les GAFAM américains (*Google*, *Amazon*, *Facebook*, *Apple*, *Microsoft*) et les BATX chinois (*Baidu*, *Alibaba*, *Tencent*, *Xiaomi)*, ainsi que toute autre entreprise se spécialisant dans le secteur de l'identité numérique (fournisseurs de services de communications électroniques, plateformes en ligne) ou détenant des données identitaires (fournisseurs de publicités ciblées). Constitués sans aucune règle contraignante venant les encadrer, grâce à la collecte ininterrompue des données personnelles des internautes (identifiants d'accès à des comptes numériques, recherches sur les moteurs de recherche,

[21] Règlement (UE) 2019/1157 du Parlement européen et du Conseil 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, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R1157

[22] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[23] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*RGPD*) : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679 ; version modifiée : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[24] Règlement eIDAS 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 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=EN ; Pour la présentation du règlement eIDAS (Electronic Identification Ands Trust Services) : ANSSI, « Le règlement EIDAS », https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/#:~:text=Le%20r%C3%A8glement%20eIDAS%20s'applique,march%C3%A9%20de%20la%20confiance%20num%C3%A9rique; T. Douville, JCP E 2017. 1005.

[25] Charte des droits fondamentaux de l'Union européenne ayant consacré le « droit à la protection des données personnelle », 18/12/2000, 2000/C 364/01, https://www.europarl.europa.eu/charter/pdf/text_fr.pdf

traces de navigation, statut, profil, téléchargements, éléments partagés sur les réseaux sociaux), réactualisées, diversifiées et sans cesse enrichies, les « *hubs* d'identité » privées sont potentiellement susceptibles de concurrencer les identités numériques publiques. Leur développement est d'autant plus préoccupant qu'ils sont associés à des objectifs commerciaux, éloignés des enjeux de l'identité numérique des États membres associés à leur souveraineté, à l'intérêt général et à la protection des citoyens en termes de libertés et de vie privée.

6. **L'identité numérique des États membres au centre d'enjeux paradoxaux**. Alors même que l'identité numérique des États membres représente indiscutablement des enjeux publics majeurs en termes de souveraineté et de déploiement des activités européennes, ce qui justifie des actions de consolidation, paradoxalement, les enjeux privés des particuliers peuvent être affectés. Il en est ainsi des dérapages majeurs affectant les libertés et la vie privée, ce qui justifie des actions de contrôles et des sanctions renforcées. A ce titre, l'identité numérique fait l'objet d'enjeux paradoxaux. Par conséquent, si elle doit indiscutablement être renforcée au profit des enjeux publics (I), elle doit néanmoins faire l'objet d'une forte vigilance à l'égard des actions qui sont menées en raison des atteintes potentielles aux libertés et à la vie privée (II).

I – L'identité numérique régalienne renforcée au profit des enjeux publics

7. Le déploiement inédit du numérique, par le développement des services publics en ligne (démarches administratives, transactions, télémédecine, etc.) et des services privés proposés par les entreprises, impose que les identités numériques utilisées soient sécurisées. Cette exigence intervient autant pour les moyens d'authentification, consistant en la vérification d'identité, que pour ceux d'identifications électroniques tendant à établir l'identité des personnes. La sécurité des démarches et des transactions en ligne passe par une stratégie européenne d'affirmation des identités numériques des États membres (A), ainsi que leur consolidation (B).

A – La stratégie européenne d'affirmation des identités numériques des États membres

8. **Les risques de la mise en service d'identités numériques privées et publiques parallèles**. De fait, un « millefeuille » d'identités numériques publiques et privées existe pour une même personne. Les degrés d'identification et d'authentification, plus ou moins solides, constituent un

véritable obstacle à la protection et à la bonne utilisation des services du numérique par les usagers. En effet, certains sites internet recourent à des moyens d'authentification par le biais de profils d'utilisateurs de certaines plateformes numériques, à l'exemple des médias sociaux tels que *Facebook*, *Google* et *Linkedin*. Ce procédé constitue un risque important de divulgation de données personnelles, sans véritable contrôle par les personnes intéressées, au mépris de leur protection[26] alors même qu'elles prennent progressivement l'habitude d'y recourir de par le monde. Les géants du numérique cherchent en effet tous les moyens possibles pour capter la clientèle, limiter la libre concurrence, voire créer de nouvelles dépendances par des situations de monopoles techniques à des fins de valorisation. Ils peuvent même mettre en place des surveillances de masse en vue de contrôler et même d'influencer potentiellement le comportement des utilisateurs[27]. Le risque est d'autant plus accru que les GAFAM collectent de nombreuses autres données des utilisateurs provenant de sources secondaires[28]. Aussi, afin de faire face au déploiement anarchique et non transparent d'identités numériques privées non sécurisées, les États membres ont tout intérêt à déployer leurs identités numériques régaliennes renforçant leur souveraineté numérique (1) qui doit plus que jamais être de confiance et fonctionnelle (2).

1 – Des identités numériques régaliennes renforçant la souveraineté numérique des États

9. La mise à disposition par l'UE de moyens destinés à conforter les identités numériques des États membres.

Les enjeux du renforcement des moyens des identités numériques régaliennes. La proposition de révision du règlement *eIDAS* a pour objet de fournir « *un instrument approprié pour la mise en place de la structure d'interopérabilité nécessaire à la création d'un écosystème d'identité numérique de l'UE, fondé sur des identités juridiques délivrées par les États membres et*

[26] Par exemple, DPC, 15 mars 2022, infligeant une amende de 17 millions d'euros à Meta Platforms (anciennement Facebook) suite à une série de douze notifications de violation de données reçues entre le 7 juin 2018 et le 4 décembre 2018, https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry

[27] Dissenting Statement of Commissioner Rohit Chopra, in re Facebook, Inc., July 24, 2019; https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf ; P. Mouron, "Une amende record de 5 milliards de dollars prononcées par la FTC contre Facebook », Revue européenne des médias et du numérique, IREC, 2019, p.77-79.

[28] CNIL, Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019, https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation

sur la fourniture d'attributs d'identité numérique qualifiés et non qualifiés »[29]. L'enjeu de l'Union européenne est ainsi d'apporter une sorte de « boîte à outils » comprenant des moyens permettant de renforcer les identités régaliennes des États membres (architecture technique, cadre de références, normes communs), afin de remédier à la fragmentation actuelle des identités nationales pas opérationnelles entre les États-membres. Dans cette perspective, les États gardent la mainmise sur leurs identités numériques publiques au profit de leur souveraineté nationale et de la pérennité de leurs choix de politiques stratégiques des critères d'identité des citoyens et des moyens de gestion et de contrôle. Dans ce sens, la France cherche à préserver et à consolider ses moyens d'identités numériques régaliens par le portefeuille d'identités numériques *FranceConnect* et par la nouvelle carte d'identité électronique (CNIe).

La question de l'émergence d'une identité numérique européenne. Alors même que l'Union européenne incite au déploiement d'une identité numérique européenne « *universelle* »[30] au profit de tous les citoyens (qui comprendrait plusieurs éléments tels que la carte d'identité numérique, le passeport vaccinal, le permis de conduire numérique, la déclaration de revenus, etc.), il est possible de s'interroger sur le fait de savoir si l'UE s'en tient uniquement à la fourniture de dispositifs tendant à renforcer les identités numériques régaliennes des États membres ou dépasse ce cadre en préfigurant une identité numérique européenne. Pour sa part, la Commission européenne fait explicitement référence à « l'identité numérique européenne » sur son site en mentionnant « une identité numérique pour tous les européens »[31]. Elle précise par ailleurs, à l'occasion de la proposition de révision du règlement *eIDAS* du 3 juin 2021, que ceci permettrait aux citoyens, « *qui ont recours à une identité numérique européenne qui les représente en ligne et pour les fournisseurs de services en ligne, qui pourront pleinement s'appuyer sur des solutions d'identité numérique et les accepter, indépendamment du lieu où elles auront été délivrées* »[32]. Elle va même plus loin en se référant à des « *portefeuilles européens d'identité*

[29] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

[30] Pour des développements sur le sujet : Assemblée nationale Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique » a été déposé le par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis, https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information

[31] Identité numérique européenne, présentation sur le site de la Commission européenne, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr

[32] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

numérique »[33]. Cette question majeure doit faire l'objet de discussions approfondies par les États membres et par l'Union européenne. Certes, il convient de renforcer la souveraineté numérique européenne, indispensable pour faire face à des grandes puissances numériques telles que les Etats-Unis et la Chine, ainsi qu'aux géants du numériques, mais pour autant, les souverainetés nationales des États membres ne sauraient être sacrifiées. Des équilibrages s'avèrent nécessaires, l'enjeu étant de reconnaître à la fois l'originalité des identités numériques nationales permettant de mettre en exergue les spécificités des États membres, tout en s'orientant vers un contenu de la base *minima* des éléments communs en constituant le socle d'une identité numérique commune de base interopérable : acte de naissance, signature électronique, carte d'identité européenne, carte d'identité électronique nationale, déclaration des revenus, sceau électronique[34], etc.

La question des moyens mis à disposition permettant de renforcer les identités numériques régaliennes. Le déploiement des identités numériques des États membres passe par le choix qualitatif et sécuritaire des moyens techniques mis à disposition, permettant de garantir la sécurité des données, pilier de la légitimité des identités numériques régaliennes. Par exemple, les décisions prises concernant les moyens de stockage sécurisés s'avèrent essentielles tant pour la sécurité des données des internautes utilisateurs, que pour la préservation de la souveraineté numérique des États membres et de l'UE. L'expérience du *Health Data Hub national*, plateforme nationale des données de santé, ayant recours à *Microsoft*, largement critiquée, de même que la remise en cause du *cloud* européen *GaïaX* ayant intégré comme partenaires de nombreux géants du numérique, sont à méditer. Les États membres et l'UE doivent par conséquent apporter des moyens techniques sécuritaires à la hauteur des risques de captation des données des utilisateurs par les autorités administratives américaines compte-tenu du *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) du 23 mars 2018 en vertu duquel les agences d'exécution de la loi, c'est-à-dire les forces de l'ordre, les agences de renseignements, disposent de la faculté d'accéder aux données stockées sur les serveurs des opérateurs télécoms et des fournisseurs de services de *cloud computing* au-delà des frontières. Outre la nécessaire mise en place de dispositifs techniques permettant de consolider l'écosystème d'identités numériques nationales de l'UE, différentes mesures doivent être envisagées afin d'éviter toute dépendance matérielle en cas, notamment, de conflits ou de contraintes dues à la raréfaction de certaines matières premières et de

[33] Commission européenne « La Commission propose une identité numérique fiable et sécurisée pour tous les européens », Communiqué de presse, 3 juin 2021, https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_2663
[34] Ce moyen permet de garantir l'origine et l'intégrité d'un document.

l'énergie. Une approche environnementale doit aussi être engagée lors de tout projet en lien avec l'identité numérique nationale afin de mieux tenir compte des contraintes actuelles et surtout à venir. L'identité numérique doit, en effet, être appréhendée dans un écosystème global tenant compte de multiples contraintes.

La gestion des superpositions d'identité numériques nationales. La superposition d'identités numériques sur le territoire national (L'identité numérique de La Poste, la nouvelle carte d'identité biométrique) peut avoir pour effet de complexifier l'appréhension, par les utilisateurs, de l'identité numérique. Une identité numérique nationale unique, surpassant toute autre identité numérique, sous forme papier et sous forme électronique, aurait l'intérêt de la simplification et aussi de la reconnaissance étatique de la force de l'identité numérique régalienne. Cet enjeu semble d'autant plus légitime pour asseoir l'autorité de l'État sur l'identité numérique des citoyens au niveau national. Reste à savoir s'il serait possible de créer techniquement une fusion entre la carte d'identité biométrique, préfigurant l'identité numérique nationale et l'identité numérique nationale virtuelle. A ceci s'ajouterait la difficulté de la remise en question de l'implication des entreprises ayant déjà investi dans le développement d'identités numériques privées.

10. **Les obstacles potentiels au renforcement des identités régaliennes.** D'importantes opérations de *lobbying* de la part des géants du numérique sont susceptibles de contrarier les objectifs prioritaires de renforcement des identités numériques des États membres, comme cela est le cas déjà à l'égard de nombreux textes européens et nationaux, à l'exemple du RGPD[35]. A ce titre, des procédures de contrôles renforcées et régulières doivent être engagées pour éviter de telles actions intrusives préjudiciables aux intérêts européens et

[35] Sur le sujet : J.-L. Clergerie, « L'influence du lobbying sur les institutions communautaires », *in* Mélanges en hommage à Georges Vandersanden : *Promenades au sein du droit européen*, Bruxelles, Bruylant, 2017, p. 89 ; Vie publique « Le lobbying en France : vers un contrôle accru ? », 15/09/2020, https://www.vie-publique.fr/eclairage/271135-groupes-dinterets-lobbying-vers-un-controle-accru ; GRECO, « Cinquième cycle d'évaluation prévention e la corruption et promotion », 02/12/2019, p. 23 ets. , https://rm.coe.int/cinquieme-cycle-d-evaluation-prevention-de-la-corruption-et-promotion-/16809969fd https://rm.coe.int/cinquieme-cycle-d-evaluation-prevention-de-la-corruption-et-promotion-/16809969fd ; Agence Française anticorruption (AFA), « Plan national pluriannuel de lutte contre la corruption 2020 – 2022 », https://www.agence-francaise-anticorruption.gouv.fr/files/files/Plan%20national%20pluriannuel%202020-2022.pdf
(2) Lobby Control et PDG « *Lobbying Big Tech Google*, *Amazon* et ses amis et leur influence cachée », *Corporate Europe Observatory,* 13/09/2020, https://corporateeurope.org/en/2020/09/big-tech-lobbying
J. Rossi, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel », Thèse Sciences de l'information et de la communication et sciences politique, Université de technologie Compiègne, 2 juillet 2020, p.36, p.93, p.302.

nationaux. Des sanctions dissuasives sont aussi à envisager *via* les CNIL européennes.

11. **Le rôle de veille et de protection des institutions régaliennes à l'égard de l'identité numérique régalienne.** Plusieurs agences, institutions, organismes, tant au niveau européen qu'au niveau national ont un rôle moteur à jouer en ce qui concerne la protection des intérêts européens et nationaux et la mise en place des politiques stratégiques envisagées à l'égard de l'identité numérique régalienne. A ce titre, plusieurs institutions européennes et nationales doivent rester attentives aux obstacles susceptibles de remettre en cause les identités numériques régaliennes pour privilégier la souveraineté européenne et nationale: l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), la direction générale des réseaux de communication, du contenu et des technologies (DG *Connect*), le Comité européen de protection des données (CEPD), l'Agence nationale de sécurité des systèmes d'information (ANSSI)[36], l'Agence nationale des titres sécurisés (ANTS)[37], la direction interministérielle du numérique (DINUM)[38], la Commission nationale de l'informatique et des libertés (CNIL)[39], le Conseil d'État (CE)[40] et le Parlement[41]. Il leur faut soutenir et agir, pour que les identités numériques régaliennes, mises en place par les États membres, soient adaptées aux besoins des citoyens, tout en les protégeant. La souveraineté des identités numériques passe par la sécurisation des données et leur fonctionnalité.

2 – Une identité numérique de confiance et fonctionnelle

12. **La légitimité des identités numériques régaliennes passant par la confiance réciproque des utilisateurs et des services et entreprises y recourant.** La confiance des internautes, des services publics et des entreprises, recourant aux procédés d'identités numériques régaliens mis à disposition par les États membres, suppose la mise en place d'outils solides, efficaces et sécurisés. Les utilisateurs, souhaitant recourir à leur identité numérique publique pour accéder et utiliser à des services publics en ligne

[36] L'ANSSI a pour missions d'informer, de prévenir, d'accompagner les victimes lors de cyberattaques.
[37] L'ANTS intervient notamment à l'égard de la carte nationale d'identité, des passeports, des permis de conduire. Site : https://ants.gouv.fr/ L'ANTS intervient à l'égard des permis de conduire, des cartes grises, des passeports et des cartes d'identité biométriques.
[38] DINUM, https://www.numerique.gouv.fr/dinum/
[39] CNIL, Avis sur l'arrêté du 24 juillet 2015 à l'origine de *FranceConnect* ; Avis n°2018-342 du 18 octobre 2018 sur le projet de décret autorisant la création d'un traitement automatisé permettant de délivrer une identité numérique dénommée « Application de lecture de l'identité d'un citoyen en mobilité » (Alicem).
[40] CE, Décision du 4 novembre 2020 validant l'application Alicem alors qu'un recours en illégalité contre le décret du 13 mai 2919 portant sur la création d'Alicem avait été déposé par La Quadrature du Net.
[41] Le Parlement a, selon l'article 24 de la Constitution, une mission de contrôle de l'action du gouvernement. A ce titre les décisions prises concernant l'identité numérique entre bien dans cette sphère de contrôle.

(administration en ligne, e-justice, e-santé, inscription des enfants dans une crèche municipale, collège, lycée) et à des services privés mis en place par des entreprises, doivent être assurés que leurs données personnelles, constituant des attributs de leur identité numérique régalienne, bénéficient d'une protection renforcée, pour ne pas dire infaillible conformément à l'article 32 du RGPD. Dans cette perspective, la proposition de révision du règlement *eIDAS* du 3 juin 2021 prévoit notamment que « *le nouveau service de confiance qualifié pour la gestion des dispositifs de création de signatures et de cachets électroniques à distance apporterait des avantages considérables du point de vue de la sécurité, de l'uniformité, de la sécurité juridique et des possibilité de choix pour les consommateurs, en ce qui concerne tant la certification des dispositifs de création de signatures qualifiés que les exigences auxquelles doivent satisfaire les prestataires de services de confiance qui gèrent ces dispositifs* »[42]. En parallèle, les administrations, les services, les entreprises, recourant aux identités numériques des utilisateurs, doivent être assurés que les moyens d'authentification et d'identifications électroniques permettent de vérifier et d'établir de manière fiable et sécurisée l'identité des personnes tout en protégeant les données de celles-ci.

13. Une identité numérique simplificatrice en termes de démarches

La facilitation d'utilisation pour les citoyens, gage d'une identité numérique régalienne forte. Du point de vue de l'Union européenne, lors de sa communication « Façonner l'avenir numérique de l'Europe », du 19 février 2020, la Commission a précisé que « Les citoyens devraient avoir la maîtrise de leur identité en ligne, lorsque l'accès à certains services en ligne nécessite une authentification. Une identité électronique publique (eID) universellement reconnue est indispensable pour que les consommateurs puissent accéder à leurs données et utiliser en toute sécurité les produits et services qu'ils recherchent dans devoir recourir pour ce faire à des plateformes tierces et partager inutilement des données personnelles avec celles-ci »[43]. L'objectif est de permettre aux citoyens européens de procéder à des opérations requérant leur identité numérique régalienne quel que soit leur endroit de localisation, grâce à leur portefeuille numérique et à leur faculté de partager certains éléments de leur identité en fonction des opérations envisagées. Il en serait ainsi pour demander soit dans l'État d'origine, soit dans un autre État membre,

[42] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

[43] COM (2020)67 final, 19 fév 2020, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, « Façonner l'avenir numérique en Europe », https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_fr.pdf p.11.

un acte de naissance, utiliser les services publics en ligne, gérer une déclaration fiscale, effectuer une demande de prêt auprès d'une banque, inscrire son enfant dans un collège, un lycée ou une université, utiliser une prescription médicale, louer une chambre d'hôtel, un véhicule, prendre un billet d'avion, etc. Le recours à l'identité numérique européenne pourrait ainsi être appréhendé comme un moyen de simplification des démarches administratives (fiscales), de prises de rendez-vous (services administratifs, médicaux), d'achats de certains biens et services (billets d'avions, de train, chambres d'hôtel). En outre, les citoyens seraient assurés de l'authenticité des moyens (billets, contrat, actes de propriété). Les moyens de conservation seraient ainsi consolidés contre le vol, la détérioration et la falsification.

Du point de vue national, il est encore souvent reproché aux services administratifs de manquer d'ergonomie, de fluidité dans les usages, et plus particulièrement de redemander à plusieurs reprises les mêmes informations pour accomplir une démarche (nom, prénom, adresse, date et lieu naissance…). Des efforts doivent par conséquent être réalisés permettant d'envisager un protocole unifié ou une application numérique donnant les moyens de remédier aux demandes répétitives pour une même démarche. Le portefeuille d'identités numériques *FranceConnect* a justement pour objectif de faciliter l'accès et les formalités auprès de différents services administratifs. En parallèle, il a pour ambition de sécuriser le recours aux identités numériques lors du recours à des services privés proposés par des entreprises. Ces dernières peuvent vérifier de manière plus fluide et sécurisée l'identité de leurs clients. L'enjeu est de faciliter l'échange des documents au profit des transactions commerciales et de contribuer à l'amélioration des moyens de suivi des services mis en place en réduisant les coûts. Ce service de confiance attractif en matière d'efficacité, de sécurité, est ainsi amené à constituer un véritable soutien aux entreprises nationales et européennes au profit du déploiement sécurisé et attractif de l'économie numérique.

14. Des identités numériques régaliennes interopérables et fonctionnelles

L'enjeu d'éviter une fragmentation des systèmes utilisés rendant impossible l'interopérabilité des identités numériques régaliennes. L'interopérabilité, définie par la proposition de règlement du *Data Act* du 23 février 2022 comme « *la capacité de deux ou plusieurs espaces de données ou réseaux de communication, systèmes, produits, application ou composant à échanger et à utiliser des données afin de remplir leurs fonctions* »[44] renvoie à plusieurs éléments : interopérabilité des données constituant le pilier des

[44] COM (2022)68 final Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data, 23 février 2022, article 2, 19)

identités numériques des États membres, interopérabilité par les spécifications techniques, interopérabilité par le biais des supports et l'interopérabilité entre les pays membres. Tout doit être fait pour éviter la fragmentation des systèmes utilisés qui serait préjudiciable à la libre circulation des citoyens et internautes européens et au libre marché des biens et services numériques européens. La Commission européenne, lorsqu'elle présente l'identité numérique fait état que « *seulement 60% de la population de l'UE, dans 14 États membres, est en mesure d'utiliser sa carte d'identité électronique nationale à l'étranger ; Seuls 14% des fournisseurs de services publics clés dans tous les États membres autorisent l'authentification transfrontalière au moyen d'un système d'identité électronique* »[45]. Des dispositions complémentaires, prévues par la révision du règlement *eIDAS* n°910/2014, ont ainsi pour objectif de renforcer les moyens techniques d'échanges et d'interopérabilité transfrontalière. Est mise en avant l'opportunité de la construction d'une identité harmonisée, uniforme, interopérable, normalisée par une même architecture pour tous les États membres, ce qui suppose la mise place des dispositifs techniques et juridiques communs et homogènes (architecture technique commune, cadres de références et normes communs).

La fonctionnalité des identités numériques régaliennes basée sur l'interopérabilité. La fonctionnalité et l'effectivité des interactions des identités numériques nationales passent obligatoirement par l'interopérabilité des systèmes utilisés. Tout l'enjeu est de mettre en place des moyens techniques pratiques et facilités en matière d'utilisation transfrontières au profit du marché unique et des marchés nationaux. Dans ce sens, la proposition de révision du règlement *eIDAS* du 3 juin 2021 prévoit que « l*es utilisateurs pourraient avoir recours à un écosystème amélioré d'identité électronique et de services de confiance reconnus et acceptés partout dans l'Union* »[46]. Des schémas d'identification électronique communs fortement sécurisés et interopérables devraient permettre d'assurer l'identification électroniques des personnes concernées (moyens d'identification, d'authentification électroniques, signatures électroniques). Il en est de même pour les moyens de transactions électroniques. Différentes mesures doivent par conséquent être prises en termes de spécifications et caractéristiques techniques à l'instar de la révision du règlement *eIDAS*. Dans cette optique, l'Agence nationale des titres sécurisés (ANTS), ayant à « *définir une stratégie de l'identité numérique*

[45] Identité numérique européenne, présentation sur le site de la Commission européenne, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr
[46] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

conforme aux normes européennes du règlement eIDAS »[47], a envisagé une nouvelle version du pilote *Middleware IAS-ECC*. Ce logiciel a pour objectif d'assurer l'interopérabilité des cartes à puce au sein des administrations, en termes d'authentification, de chiffrement de fichiers, de signature de documents, d'accès aux données personnelles du porteur[48].

15. **Une identité numérique régalienne économiquement accessible.** L'attractivité de l'identité numérique régalienne passe indiscutablement par sa mise à disposition gratuite ou à faible coût pour les citoyens. Les États doivent prendre la mesure de l'importance des investissements à réaliser dans ce domaine, qui doivent être chiffrées de manière régulière, compte-tenu de l'obsolescence rapide des moyens numériques utilisés. L'analyse d'impact envisagée lors de la proposition de révision du règlement *eIDAS précise que les « coûts minimaux quantifiables peut être estimés à au moins 3,2 milliards d'euros* [49].

16. **La complexité de l'identité numérique régalienne potentiellement discriminatoire.** La complexité des procédures, en lien avec l'identité numérique des États membres, est susceptible de constituer une cause sévère d'abandon d'une partie non négligeable des citoyens. En effet, les opérations destinées à attester de l'identité numérique les astreignent à mener plusieurs procédures et à apporter différents éléments d'identité afin d'engager les opérations d'inscription, de vérification, de réception de la validation de l'authenticité des moyens d'identité numérique présentés et de l'activation de l'identification. Ces procédures, légitimes, mais compliquées, s'avèrent impossibles à réaliser pour les personnes de tout âge, non adeptes de la connectivité, touchées par l'illettrisme ou l'illectronisme numérique. Elles peuvent être à l'origine d'inégalités d'accès, de stigmatisation, ce qui est d'autant plus discriminatoire dans l'hypothèse d'un service régalien d'identité numérique. Afin de mieux résoudre de telles difficultés, des situations d'accompagnement et de formation doivent être envisagées par les États membres.

[47] ANTS, « Identité numérique », 10 décembre 2021, https://ants.gouv.fr/nos-missions/les-solutions-numeriques/identite-numerique
[48] Pour plus d'explications techniques : Pilote Middleware et téléchargement : https://ants.gouv.fr/nos-missions/les-solutions-numeriques/identite-numerique
[49] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

B – Une identité numérique solide

17. Si l'identité numérique régalienne est attractive et constitue une véritable opportunité pour l'Union européenne, les États membres et les utilisateurs, encore faut-il qu'elle fasse preuve d'une robustesse technique suffisante et hautement sécuritaire permettant d'assurer sa légitimité et sa pérennité. Cette optique est fortement marquée dans la proposition de révision du règlement *eIDAS* du 3 juin 2021 qui marque toute l'importance de « *donner accès à des solutions d'identité électronique hautement sécurisées et fiables* », de « f*aire en sorte que les services publics et privés puissent s'appuyer sur des solutions d'identités numériques fiables et sécurisées* »[50]. La Commission européenne privilégie « *le niveau d'ambition le plus élevé et vise à réglementer la fourniture d'un portefeuille d'identité numérique personnel hautement sécurisé délivré par les États membres* »[51]. A ce titre, l'identification des obstacles au déploiement de l'identité numérique régalienne (1), permet de mieux mesurer le défi d'une régulation robuste et sécuritaire (2).

1 – Le défi d'une identité numérique robuste

18. En dépit des efforts réalisés, les dispositifs techniques actuels, envisagés par les États membres pour l'identité numérique régalienne, restent insuffisants, voire risqués. Il est par conséquent indispensable d'envisager des moyens pour y remédier.

19. **L'appel à des acteurs européens et nationaux pour la conception des identités numériques régaliennes aux fins de soutenir des entreprises et de consolider la souveraineté.** L'Union européenne, et particulièrement la France, sont dotés d'un nombre important d'entreprises spécialisées dans le domaine de l'identité numérique (supports physiques tels que les puces, cartes, jetons, logiciels d'authentifications numériques et de signatures électroniques, activités d'interfaçage, d'enrôlement, de dérivation, de certifications, services de validation d'identité, fournisseurs d'identités ou de services de confiance, etc.). Selon le rapport d'information déposé le 8 juillet 2020 auprès de l'Assemblée nationale portant sur « L'identité numérique », le secteur comprendrait en France 500 entreprises pour un chiffre d'affaires de 1,4 milliards d'euros en 2018. Par ailleurs, le potentiel économique généré par l'identité numérique est conséquent et prometteur : « *Le marché de l'identité numérique devrait représenter 250 millions d'euros d'ici 2024 et plus d'un*

[50] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN
[51] Op. cit, COM (2021) 281 final, la proposition du 3 juin 2021.

milliard d'euros d'ici 2029 »[52]. Il est donc essentiel que l'Union européenne et les États membres privilégient les entreprises européennes et nationales fournisseurs de supports physiques et prestataires de services lorsqu'elles mettent en place leurs moyens techniques destinés à la mise en place et la gestion de l'identité numérique régalienne. Trop souvent, les États ont tendance à privilégier les géants du numérique, les *GAFAM* ou d'autres entreprises américaines puissantes alors qu'il existe d'importantes problématiques rattachées au *Cloud Act* et à la dépendance technique qui pourraient mettre en péril la confiance et la pérennité des identités numériques régaliennes. Ce risque est d'autant plus fort que cette dernière est confortée par une dépendance sociétale des citoyens qui, par manque d'information, de formation ou par confort, peuvent avoir tendance à privilégier les services proposés par les *GAFAM,* alors même qu'il existe pourtant déjà des services alternatifs proposant des options plus fiables en termes de sécurité et plus éthiques. Les entreprises nationales, présentant des garanties suffisantes d'indépendance, n'ayant pas envisagé de partenariats avec les géants du numérique, doivent être privilégiées, d'autant que, selon le rapport d'information déposé le 8 juillet 2020 auprès de l'Assemblée nationale portant sur « L'identité numérique », « *l'arrivée d'une solution régalienne sur le marché de l'identité numérique pourrait stimuler la concurrence et l'innovation, au profit des acteurs français, particulièrement performants dans ce domaines* »[53]. La difficulté est que, parfois, il est objecté que les entreprises européennes et nationales ne disposent pas de la stature technique et technologique des *GAFAM*. A ce titre, des études comparatives devraient être engagées pour vérifier objectivement de telles affirmations. Il est aussi essentiel de privilégier les entreprises nationales et européennes pour renforcer l'économie, les emplois et favoriser le secteur du numérique qui est crucial pour l'avenir. Il est aussi crucial de les inciter à créer des produits réellement adaptés aux citoyens, qui soient faciles d'accès et d'utilisation.

20. **Les critiques portant sur le choix de techniques et de matériaux insuffisamment robustes**. Les exigences de la qualité notamment des techniques, des supports, des *clouds* et des matériaux utilisés doivent faire l'objet d'évaluations préalables permettant de justifier les choix opérés. S'inscrivant dans le cadre du règlement (UE) 2019/1157 du 20 juin 2019 du Parlement européen et du Conseil 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

[52] Assemblée nationale Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique » a été déposé le par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis, https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information
[53] Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique », préc.

libre circulation[54], l'enjeu a été d'harmoniser le niveau de robustesse des cartes nationales d'identité numérique des États membres afin d'éviter les risques de falsification de titres générant des usurpations d'identité et des usages de faux. La nouvelle carte d'identité biométrique française, généralisée sur le territoire national depuis août 2021, constitue un exemple d'amélioration connaissant toutefois des limites. Elle fait l'objet d'importantes critiques, bien qu'elle dispose désormais d'une puce électronique (comprenant les données d'état civil du titulaire de la carte telles que le nom, les prénoms, la date et le lieu de naissance, le sexe, la taille, la nationalité, ainsi que le domicile ou la résidence de l'utilisateur, la date et la délivrance de la carte, la date de validité, le numéro de carte, l'image numérisée de la photographie et les empreintes digitales de deux doigts)[55] et d'un cachet électronique sous la forme d'un code-barres à deux dimensions. Il lui est reproché son niveau insuffisant de sécurité, le titre étant techniquement dépassé et pas à niveau compte-tenu des innovations existantes dans ce domaine[56]. Même les composants électroniques ne sont pas considérés comme en mesure de tenir la durée des dix ans de la carte. De telles failles en termes de robustesse, de fiabilité et de qualité opérationnelle des systèmes techniques utilisés ne sauraient se pérenniser dans le cadre d'une identité numérique nationale.

21. **Le problème des modalités de stockage des données ne présentant pas de garanties suffisantes de sécurité.** Les données personnelles de la nouvelle carte d'identité numérique biométrique sont stockées dans la base centralisée des titres électroniques sécurisés (TES)[57] créé par le décret n°2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, et géré sous la responsabilité du ministère de l'intérieur. Cette base de données centralisées, validée par le Conseil d'état le 18 octobre 2018[58], regroupe de multiples informations telles l'image numérisée du visage et des empreintes digitales, l'image numérisée de la signature, les noms et prénoms, la date et le lieu de naissance, le sexe, la couleur des yeux, la taille, l'adresse postale, l'adresse de messagerie électronique, les coordonnées téléphoniques, etc.

[54] Règlement (UE) 2019/1157 du Parlement européen et du Conseil 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, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R1157
[55] Ministère de l'intérieur, « La puce de la nouvelle carte nationale d'identité », 16/03/2021, https://www.interieur.gouv.fr/actualites/actu-du-ministere/nouvelle-carte-nationale-didentite/puce-de-nouvelle-carte-nationale
[56] Pour l'exposé des critiques : S. Smart, « Notre carte d'identité est-elle sécurisée ? », 29 mars 2021, https://www.bsmart.fr/video/4900-smart-tech-partie-29-mars-2021
[57] CNIL, « Le fichier des titres électroniques sécurisés (TES) », 28 mai 2021, https://www.cnil.fr/fr/le-fichier-des-titres-electroniques-securises-tes
[58] CE, 18 octobre 2018, n°404996, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000037507135/

Reste à savoir si cette centralisation, gérée par l'Agence nationale des titres sécurisés (ANTS) est satisfaisante ou risquée en matière de protection des données.

Dès la création du TES, différentes réserves ont été émises, notamment celle du Conseil national du numérique qui, le 7 novembre 2016 a demandé sa suspension en raison des risques de détournement des finalités du fichier et de piratage. Il en a été de même de l'observatoire des libertés et du numérique le 14 novembre 2016. Il a été reproché à la société *Amesys* d'avoir apporté son soutien au pilotage du TES concernant la maîtrise d'ouvrage technique et des systèmes d'information par un contrat de cinq millions d'euros[59]. Pourtant, le 30 mars 2017, ce fichier a été mis en place et continue d'être exploité. Le site de l'Agence nationale des titres sécurisés (ANTS) n'apporte aucune information officielle précise, alors même que le stockage des données d'identité numérique des citoyens français est en cause. La presse mentionne uniquement que le Ministère de l'intérieur a sélectionné, le 10 mai 2021, pour le futur système de gestion de l'identité numérique (SGIN), le groupe français *Atos* (développement des applications permettant aux usagers de s'identifier aux services *via FranceConnect*[60], développement et maintenance du SGIN), *Sopra Steria* (prestations d'assistance dans le pilotage de lot sur les question d'architecture technique, de sécurité, de qualité de l'expérience utilisateur, de mise en œuvre de méthodes agiles dans la conduite de projets) et un groupement composé d'*Idemia* et d'*Idakto* (logiciel permettant la lecture des informations sur les titres d'identité électronique sur lesquelles se fondent l'identité numérique) [61] . Reste à savoir si ces entreprises présentent suffisamment de garanties quand on sait que le SGIN permettra aux usagers de s'identifier à certains services en ligne tel que l'espace numérique de santé (ENS appelé « Mon espace Santé » intégrant le dossier médical partagé DMP) ou pour déposer une plainte. La difficulté est que *Atos* a engagé le 24 avril 2018, avec la société *Google Cloud* un partenariat mondial « *pour fournir des*

[59] Cette société a été poursuivie pour complicité de torture en Libye par la vente de technologies de surveillance des télécommunications présente des garanties suffisantes : A. Fradin, « Amesys file un coup de main à l'agence en charge du fichier monstre », L'Obs avec Rue89, 21 Nov 2016, https://www.nouvelobs.com/rue89/rue89-tech/20161109.RUE4193/amesys-file-un-coup-de-main-a-l-agence-en-charge-du-fichier-monstre.html

[60] France Connect, https://franceconnect.gouv.fr/

[61] Ces différentes informations sont issues de l'article de A. Vitard, « Atis, Sopra Steria, Indemia et Idakto ont été choisis pour le chantier de l'identité numérique, Usine digitale, 19 mai 2021, https://www.usine-digitale.fr/article/atos-sopra-steria-idemia-et-idakto-ont-ete-choisis-pour-le-chantier-de-l-identite-numerique.N1094534 ; Voir aussi E. Marzolf, « Exclusif : l'Intérieur a choisi les prestataires qui développeront son identité numérique », Acteurspublics, 18 mai 2021, https://www.acteurspublics.fr/articles/exclusif-linterieur-a-choisi-les-prestataires-qui-developperont-son-identite-numerique

solutions sécurisées de pointe aux entreprises »[62]. Il en est de même avec *Microsoft*[63] et *Amazon Web Service*[64]. Le choix d'*Atos*, comme acteur prioritaire pour le développement du système de gestion de l'identité numérique nationale pose par conséquent des problèmes de souveraineté nationale majeurs en raison de ses partenariats avec les géants du numérique américain. Cette solution n'apparaît pas satisfaisante en termes de protection des données personnelles des citoyens français, même en dépit de la fusion d'*Atos* avec *Thales* pour former *Athea*, solution européenne de *Big Data* souverain ayant pour objet le « traitement de données massives à destination des États et des opérateurs d'importance vitale »[65]. La sécurité des données sensibles des utilisateurs risque en conséquence d'être altérée, ce qui pourrait remettre en cause leur confiance en cas d'incidents.

La mise en place de modalités d'évaluations plus approfondies s'impose, de même que la mise en place de bonnes pratiques aux fins d'optimiser les choix techniques utilisés. Les instances décisionnelles doivent être davantage responsabilisées en justifiant leurs choix par des procédures transparentes suite à des appels d'offres. Dans ce sens, le service *FranceConnect,* qui permet à l'utilisateur de se connecter à plusieurs services en ligne à l'aide d'un identifiant sécurisé, sorte de laisser-passer unique, a été considéré, le 20 janvier 2020, par l'ANSSI comme présentant un niveau de sécurité « substantiel »[66]. De même, l'identité numérique Alicem (Authentification en ligne certifiée sur Mobile), créé par le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile »[67]. Elle a été considérée par le Ministère de l'intérieur, le 12 février 2020, comme « *la première solution d'identité numérique régalienne sécurisée* »[68]. Il devra en être de même pour le

[62] Atos, « Atos et Google Cloud forment un partenariat mondial », Communiqué de presse 24 avril 2018, https://atos.net/fr/2018/communiques-de-presse_2018_04_24/atos-et-google-cloud-forment-un-partenariat-mondial

[63] Atos, « Atos et Microsoft – Partenaires pour de meilleurs résultats numériques », https://atos.net/en/about-us/partners-and-alliances/microsoft

[64] Atos, « Atos étend sa collaboration avec Amazon Web Servic e, un partenaire Atis OneCloud », 16 novembre 2020, https://atos.net/fr/2020/communiques-de-presse_2020_11_16/atos-etend-sa-collaboration-avec-amazon-web-services-un-partenaire-atos-onecloud

[65] Athea, https://athea.tech/ Il est mentionné sur le site que « *La société développe une plateforme digitale de traitement de données massives pour des clients privés ou publics de secteurs sensibles : défense, renseignement, sécurité intérieure, santé, énergie, transports…* ».

[66] L'article 8 du règlement européen IDAS du 23 juillet 2014 prévoit trois niveaux : faible, substantiel et élevé, lesquels sont précisés dans le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015.

[67] Décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF n°0113 du 16 mai 2019, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038475477/2019-07-22/

[68] Ministère de l'intérieur, « Alicem, la première solution d'identité numérique régalienne sécurisée », 12/02/2020, https://www.interieur.gouv.fr/actualites/actu-du-ministere/alicem-premiere-solution-didentite-numerique-regalienne-securisee

nouveau moyen d'identification électronique dénommé « Service de garantie de l'identité numérique (SGIN) se substituant à Alicem par le décret n°2022-676 du 26 avril 2022[69], De telles exigences d'évaluation des garanties de sécurité sont d'autant plus indispensables compte-tenu de l'expérimentation du téléservice dénommé « *Mon FranceConnect* » (MFC) envisagée par le décret n°2021-1538 du 29 novembre 2021[70] par la direction interministérielle du numérique « *ayant pour objet de mettre à disposition des citoyens un ensemble de données personnelles les concernant et détenues par les administrations* »[71].

22. **Le recours à des opérateurs internes, prestataires et fournisseurs externes certifiés.** Pour la mise en place et la gestion des moyens techniques propres aux identités numériques régaliennes, différents opérateurs internes, fournisseurs et prestataires externes interviennent. La question de leur fiabilité est majeure, l'enjeu étant de pouvoir se reposer sur des prestataires de confiance pour une identité numérique forte et sécurisée. Il existe différentes certifications, labellisations de confiance, mais celles-ci peuvent s'avérer limitées, obsolètes et non assorties de contrôles réguliers et suffisants. L'identité numérique, ou encore les portefeuilles d'identités numériques, doivent être consolidés en termes de fiabilité en se basant sur les prescriptions du Règlement *eIDAS.* La proposition de révision de celui-ci, en date 3 juin 2021, mentionne dans ce sens que « *La conformité des portefeuilles européens d'identité numérique (…) devrait être certifiée par des organismes accrédités par les États membres. Le recours à un schéma de certification, fondé sur la disponibilité des normes convenues d'un commun accord avec les États membres, devrait garantir un niveau élevé de confiance et d'interopérabilité*»[72]. Par conséquent, les schémas européens de certification de cybersécurité doivent répondre au règlement (UE) 2019/881[73]. De même, au niveau national, les prestataires extérieurs doivent répondre à des référentiels de sécurité envisagés par l'ANSSI dans le cadre des prescriptions du règlement européen

[69] Ce décret abroge le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ». Il est publié au JORF n°0098 du 27 avril 2022, Texte n°27, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825

[70] Décret n°2021-1538 du 29 novembre 2021 relatif à l'expérimentation du téléservice dénommé « Mon FranceConnect » (MFC), JORF n°0278 du 30 novembre 2021, Texte 20, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044385101

[71] Les usagers disposent d'un espace en ligne placés sous leur contrôle. Les données concernées sont celles portant sur les données d'état civil des usagers, de même que les informations ou données susceptibles de faire l'objet d'un échange entre administrations.

[72] Op. cit, COM (2021) 281 final, la proposition du 3 juin 2021, (10).

[73] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA) et à la certification de cybersécurité des technologies de l'informations et des communications, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R0881

eIDAS n°910/2014. Il est indispensable de sans cesse renforcer les modalités de contrôle des prestataires extérieurs dits « de confiance ». La publication et la publicité des listes des experts de confiance devraient être mises à jour en fonction de l'effectivité des mesures de sécurité prises par ces prestataires extérieurs et de la qualité de leurs prestations. Ces dernières devraient faire l'objet de vérifications régulières subordonnant le maintien ou non des prestataires de confiance sur les listes publiées. Les organismes responsables des certifications devraient aussi faire l'objet de critères d'éligibilité particulièrement stricts et faire, eux aussi, l'objet de contrôles réguliers par les administrations européennes et nationales tels que le Comité européen de normalisation (CEN), l'Institut européen de normalisation des télécommunications (IENT), l'Organisation internationale de normalisation (ISO), l'Union internationale des télécommunications (UIT).

23. **Des procédures d'évaluation des risques et de notifications en cas de failles en matière de sécurité ou de dysfonctionnement des systèmes utilisés**. Doivent être envisagées des procédures renforcées régulières d'évaluations, d'analyses des risques et, le cas échéant, des notifications en cas d'identification de failles, de dysfonctionnement des systèmes utilisés. Ces procédures devraient être imposées autant aux prestataires internes qu'aux prestataires externes. Là encore, des règles de bonnes pratiques pourraient être préparées. Les notifications devraient être adressées aux différents acteurs ayant un intérêt direct et majeur concernant les systèmes, que ce soient ceux intervenant dans la mise en place de l'identité numérique, de ceux chargés des contrôles. Des procédures transparentes d'alertes devaient aussi être engagées à l'égard des utilisateurs (États, services administratifs, sociétés, particuliers) pour que ceux-ci soient aussi en mesure de prendre, dans les meilleurs délais, des mesures destinées à protéger les données personnelles utilisées. Afin de favoriser la traçabilité et la preuve de ces actions, des techniques, telles que la *blockchain*, pourraient être utilisées pour fixer les attributs constitutifs de l'identité numérique régalienne. Elles pourraient détecter les différentes opérations menées sur celle-ci telles que les procédures d'authentification, les historiques de navigation, l'enjeu étant d'identifier les personnes malveillantes et leurs actions de cyberpiratage, d'usurpation d'identité, d'action en e-réputations et de tout autre abus potentiel.

24. **Le principe de suivi, de contrôle, d'alerte des systèmes techniques d'identité numérique.** Compte-tenu des innovations techniques incessantes et du déploiement continu des cyberattaques, il importe que les responsables des services techniques d'identité numérique mettent en place en continu différentes procédures de suivis, de contrôles, d'alertes qui soient communes et réellement opérationnelles au niveau de l'Union européenne et des États

membres. Afin de renforcer l'efficacité de ces procédures, des évaluations de conformité internes, basées sur des contrôles réguliers doivent être prévues, de même que le recours à des audits externes de prestataires de services de confiance.

25. ***Les responsabilités*.** Plusieurs responsabilités pourraient être envisagées.

La responsabilité des Etats-membres. Bien que l'Union européenne intervienne de manière croissante sur le sujet de l'identité numérique et des portefeuilles d'identité numérique, actuellement, les États membres demeurent les principaux responsables de leur constitution et de leur gestion. A ce titre, leur responsabilité doit être prioritairement engagée en cas de failles au niveau de la sécurité des données et de l'insuffisante protection des citoyens concernant leurs données personnelles utilisées. Les États membres ont par conséquent tout intérêt à être vigilants quant au choix des services et prestataires auxquels ils recourent.

La responsabilité des prestataires de services extérieurs. Dans le cadre de leurs interventions relatives à l'identité numérique européenne, les prestataires de services, en cas de prestations insuffisamment sécurisées, comportant des failles préjudiciables aux ressortissants des États membres, devraient *a minima* engager leur responsabilité civile destinées à réparer les préjudices. Devraient aussi être envisagées des sanctions dissuasives du point de vue de la responsabilité pénale.

26. **Des couvertures assurantielles à la hauteur des enjeux de l'identité numérique régalienne.** Les États-membres, ainsi que les prestataires des services extérieurs, doivent envisager des couvertures assurantielles obligatoires, suffisantes et conséquentes puisqu'il existe de plus en plus de failles de sécurité concernant les services numériques régaliens, à l'exemple de nombreux établissements publics régulièrement piratés. Compte-tenu de la masse des informations majeures associées aux identités numériques étatiques et aux portefeuilles d'identités numériques, la base centralisée TES (Titres électroniques sécurisés) fera certainement l'objet de convoitises, particulièrement des risques de piratages majeurs, ou associés à des faits de guerres numériques. Le contenu et les limites des couvertures pourraient être envisagés au niveau de l'Union européenne. De tels scénarios doivent faire l'objet d'études approfondies et de mesures à la hauteur des risques de la centralisation des données auprès des fournisseurs de *cloud*. Dans de telles conditions, reste à savoir si les risques relatifs aux prestations d'identité numérique seraient assurables. *A minima*, des plafonds de garantie pourraient

être envisagés. Un plafond spécifique de garantie pourrait aussi être envisagé lorsque l'identité numérique envisagée est régalienne.

2 – Le « challenge » d'une régulation sécuritaire de l'identité numérique

27. **Le respect du RGPD permettant d'assurer la protection des données personnelles des utilisateurs**. Le recours aux différents éléments d'identifications permettant de constituer l'identité numérique sont rattachés au RGPD dans la mesure où il s'agit de données personnelles. Aussi, tout promoteur d'identité numérique, tout responsable de traitement de service numérique rattaché à un portefeuille d'identités numérique, que celui-ci soit public ou privé, doit s'astreindre à respecter les différentes règles afférentes au RGPD. Cette obligation est explicitement rappelée par la proposition de règlement du Parlement européen et du Conseil du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne fiable applicable autant pour les secteurs publics que privés[74]. Ceci suppose le respect des principes de licéité, de loyauté, de transparence, de limitation des finalités, de minimisation des données, de limitation de la conservation, proportionnée au but envisagé et restreinte dans le temps, d'intégrité et de confidentialité. Tout doit être pensé pour sécuriser au mieux les données. Une analyse d'impact sur la protection des données (AIPD) [75] peut être envisagée. Par conséquent, le comité européen de la protection des données (CEPD) doit interagir sur les aspects de la mise en œuvre du RGPD en lien avec l'identité numérique développée par les États membres. Il en est de même, au niveau national, de la Commission nationale de l'informatique et des libertés (CNIL) et du Conseil d'État (CE).

28. **La lutte contre les risques en matière de cybersécurité.** La lutte contre la cybersécurité est mise en exergue par la commission par sa « nouvelle stratégie de cybersécurité de l'UE et nouvelles règles visant à renforcer la résilience des entités critiques physiques et numérique »[76]. Cette-ci intervient notamment dans le cadre du règlement (UE) 2019/881 relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA) et à la certification de cybersécurité des technologies de l'informations et des communications[77].

---

[74] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

[75] CNIL, Outil PIA, 30 juin 2021, https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil ; CNIL Déclaration RU 48 « *FranceConnect* », 16 mars 2022.

[76] Commission européenne « Nouvelle stratégie de cybersécurité de l'UE et nouvelles règles visant à renforcer la résilience des entités critiques physiques et numérique », Communique de presse, 16 décembre 2020, https://ec.europa.eu/commission/presscorner/detail/fr/IP_20_2391

[77] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA) et à la certification de cybersécurité des

Les identités numériques attractives pour les cyberpirates. En raison du développement majeur de la cybercriminalité, l'identité numérique régalienne peut désormais faire l'objet de fraudes, d'usurpations d'identités, d'« Identité d'emprunt », soit par le vol direct des informations personnelles en ligne (numéro de sécurité sociale, vol de copies de documents d'identité), soit par l'achat, notamment, de passeports ou de cartes d'identités mis en vente pour un prix d'environ 600 dollars sur le *Dark Web*[78]. Les cyberpirates cherchent toujours plus à avoir accès de manière illégale aux services financiers (pour une obtention de crédit), aux services publics (santé), à la cryptomonnaie par le biais de l'usurpation de l'identité numérique. Ils peuvent aussi avoir pour objectif de vouloir entacher la réputation d'une personne dans l'intention de lui nuire, en faisant croire qu'elle a commis des actes répréhensibles. La Commission européenne et le Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité ont pris la mesure de toute l'urgence d'agir par le biais notamment, le 16 décembre 2020, de la « Stratégie de cybersécurité de l'Union européenne »[79].

Une centralisation des données des identités numériques discutable en matière de cybersécurité. Si les orientations actuelles prises par les autorités gouvernementales s'orientent vers la centralisation, le risque est que *FranceConnect* notamment soit à la merci de cyberpirates disposant de moyens toujours plus performants leur permettant d'accéder aux codes uniques des utilisateurs. Dans une telle hypothèse, les risques seraient majeurs, autant pour les usagers, que pour les services étatiques et entreprises de services impliqués. Il en serait de même en cas d'une identité numérique régalienne au niveau européen.

La nécessité d'actions renforcées de prévention et de prises en charge en cas d'attaques. Selon l'entreprise *Onfido*, entreprise de vérification et d'authentification en ligne, depuis 2019, la fraude à l'identité numérique aurait augmenté de 44%, touchant autant les particuliers consommateurs, que les entreprises, le taux moyen étant de 5,9% pour 2021[80]. Compte-tenu du développement massif de la cybercriminalité, des actions de prévention nécessitent d'être renforcées, particulièrement par l'ANSSI, l'enjeu étant

technologies de l'informations et des communications, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R0881

[78] R. Pomian-Bonnemaison, « Votre passeport est peut-être en vente sur le dark web », Pressecitron, 02/12/2021, https://www.presse-citron.net/dark-web-cartes-didentite-et-passeports-francais-voles-se-vendent-en-toute-impunite/

[79] Commission européenne, « The EU's Cybersecurity Strategy for the Digital decade", https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[80] Onfido, « Fraude à l'identité : rapport 2022 », 21/12/2021, https://onfido.com/resources/fr/fraude-identite-rapport-2022

d'améliorer la qualité des infrastructures informatiques, ce qui revient à inciter constamment à des mises à jour pour renforcer les sécurisations, de certifier régulièrement les prestataires de confiance en termes de cybersécurité, d'envisager les référentiels de sécurité concernant les moyens d'identification électronique, etc. Il en est de même des actions d'assistance et des expertises en cas de cyber attaques. Concernant la nouvelle carte d'identité numérique, les données contenues dans la puce font l'objet de dispositifs en cryptographie afin d'éviter les falsification et modification des données, une lecture à distance par une radio-identification illicite. Ces mécanismes cryptographiques respectent la norme 9303 de l'Organisation de l'aviation civile internationale (OACI)[81]. En outre, il est indispensable que les différents acteurs prennent conscience des précautions à envisager telles que, par exemple, le changement des codes d'accès, la nécessité de changer régulièrement les supports informatiques.

La mise en place d'évaluations des moyens de cybersécurité. Des moyens d'évaluation peuvent être préconisés tels que, par exemple, un cyberscore indiquant le niveau de sécurité d'une identité numérique utilisée, qu'elle soit publique ou privée. Cette transparence permettrait d'inciter les acteurs de l'identité numérique à toujours perfectionner leur niveau de protection de la plateforme et des autres moyens techniques utilisés. Là encore, des évaluations régulières des cyberscore par des autorités indépendantes devraient être envisagées.

L'anticipation des risques accrus générés par le futur ordinateur quantique. Cette nécessaire prise de conscience d'anticiper et de mieux se préparer aux risques accrus de cybersécurité intervient à plus forte raison avec l'ordinateur quantique disposant de puissances de calculs tellement fortes qu'il serait possible de remettre en cause les codes de sécurité en lien avec les identités numériques régaliennes en peu de temps. Les États doivent incontestablement se préparer à ce nouveau risque majeur qui pourrait conduire à des vols de données sensibles à grande échelle. Des scénarios de sécurisation des données doivent être anticipés comme par exemple des copies des identités numériques sur des systèmes indépendants non connectés ou sur un cloud étatique très sécurisé.

29. **L'importance de la recherche et de l'innovation**. *In fine*, une véritable mobilisation doit être engagée en matière de recherche et d'innovation permettant de générer de nouveaux moyens techniques ayant pour objet de

[81] Ministère de l'intérieur « La puce de la nouvelle carte nationale d'identité », 16/03/2021, https://www.interieur.gouv.fr/actualites/actu-du-ministere/nouvelle-carte-nationale-didentite/puce-de-nouvelle-carte-nationale

répondre aux évolutions techniques liées à l'identité numérique et aux portefeuilles d'identité numérique. L'enjeu doit être de sans cesse améliorer les différents moyens mis en place et de faire face aux multiples risques de la cybersécurité. Le soutien de la recherche publique et privée pourrait à ce titre constituer un vivier dynamique de nouvelles opportunités numériques. Il contribuerait au développement de ce secteur hautement stratégique, offrant de nouvelles perspectives économiques aux *start-up*, aux petites et moyennes entreprises européennes et en termes d'emplois.

II –L'identité numérique régalienne affectant potentiellement les libertés et la vie privée

30. **Une vigilance constante pour une identité numérique respectueuse des libertés et de la vie privée.** Les utilisateurs des identités numériques bénéficient d'un véritable « droit à la protection des données personnelles » consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000 »[82]. A ce titre, les solutions envisagées en termes de protection de la vie privée, en lien avec l'identité numérique régalienne, s'avèrent plus vertueuses que celles développées par les géants du numérique. La proposition de révision du règlement eIDAS précise dans ce sens que « *les solutions d'identité, qui ne relèvent pas du champ d'application du règlement eIDAS, telles que celles proposées par les fournisseurs de médias sociaux et les établissements financiers, suscitent des inquiétudes quant au respect de la vie privée et à la protection des données* »[83]. Pour autant, une importante vigilance s'impose aussi à l'égard des identités numériques et des portefeuilles d'identité numériques déployés par les États membres. Les dérapages émergents (A) mettent en exergue la nécessité de s'assurer que l'identité numérique régalienne privilégie la liberté et la vie privée des utilisateurs (B).

A – Les dérapages émergents de l'identité numérique régalienne

31. **Les risques paradoxaux de l'identité numérique régalienne.** Alors même que l'identité numérique des États est censée faciliter le recours des citoyens au Marché Unique numérique, tout en renforçant leur protection, et qu'elle est

[82] Charte des droits fondamentaux de l'Union européenne ayant consacré le « droit à la protection des données personnelle », 18/12/2000, 2000/C 364/01, https://www.europarl.europa.eu/charter/pdf/text_fr.pdf ; Se référer aussi à l'article 53 de cette Charte soumettant le droit de l'UE au droit de la CEDH.
[83] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

soutenue par le forum économique mondial[84], force est de constater que d'importants risques émergent par la mise en place accrue de procédés de surveillances et de profilages (1). Une telle situation présente potentiellement des risques de l'apparition progressive d'un crédit social régalien restrictif des libertés (2).

1 – La collecte centralisée des données identifiantes, source de potentiels dérapages

32. **La collecte centralisée et massive des données par les portefeuilles d'identité numérique, potentiellement source de dérapages.** Au niveau national, alors même que, dans le passé, le Conseil constitutionnel, par la décision n°2012-652 DC avait censuré, le 22 mars 2012, l'article 5 de la loi relative à la protection d'identité, tenant notamment « à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation pour non-respect de la vie privée », désormais, par le biais de *FranceConnect* et de *FranceConnect+,* les utilisateurs disposent de la faculté de pouvoir accéder et gérer leur compte fiscal (déclaration impôt sur le revenu, paiement des impôts en ligne), d'engager des démarches en lien avec la citoyenneté (demande de passeport, de carte nationale d'identité, changement d'adresse, casier judiciaire, inscription sur les listes électorales, procuration, espace administration pénitentiaire), de gérer leur santé (couverture maladie universelle – complémentaire, et *MonEspaceSanté* comprenant le dossier médical partagé, la démarche de pré-hospitalisation de l'*AP-HP, la* demande d'une carte européenne d'assurance maladie). Il leur est aussi possible de gérer les différentes formalités relatives à leur famille (déclarer une naissance, consulter un livret scolaire, accéder au portail des allocations familiales), de même que leur activité (simuler leurs droits sociaux, accéder au Pôle emploi, disposer d'attestations de paiement d'indemnités journalières), ainsi que leur retraite (droits, Agirc-Arcco, l'assurance retraite). En outre, ils disposent de la faculté d'accéder à des fournisseurs d'énergie (ENGIE particuliers, ENEDIS), de gérer leurs transports (télépoints : consultation du solde des points du permis de conduire, la déclaration de cession d'un véhicule, demande de certificat d'immatriculation d'un véhicule d'occasion immatriculé en France), d'accéder aux services douaniers DALIA, ainsi qu'à certaines banques et assurances (ouverture d'un compte bancaire) et à leur signature électronique « qualifiée ».

[84] Forum économique mondial, C. Léong, « 5 raisons de participer aux écosystèmes d'identité numérique », 26 nov 2021, https://www.weforum.org/agenda/archive/digital-identity

De manière consécutive, les autorités publiques, gestionnaires des portefeuilles d'identités numériques, disposent de manière centralisée, et à grande échelle, de données personnelles, sensibles, multiples, et diversifiées des citoyens utilisateurs. Par exemple, *FranceConnect* disposerait déjà de plus de 35 millions d'utilisateurs. Le croisement des données peut potentiellement permettre aux États de mieux connaître les moyens financiers de leurs ressortissants (revenus, propriétés, placements financiers), de même que certains éléments liés à leur vie privée et professionnelle (déplacements professionnels et touristiques, consommations alimentaires et énergétiques, éléments de la vie familiale, sexuelle, état de santé, voire même opinions religieuses, philosophiques et politiques) [85] . Cette centralisation est préoccupante en raison des moyens techniques associés à l'intelligence artificielle, permettant de les exploiter, avec des desseins parfois en décalage avec l'intérêt général ou la protection des libertés publiques. Cette situation pourrait ouvrir la voie à de potentiels dérapages d'autorités publiques malintentionnées en termes de surveillances injustifiées et de manipulations individuelles et de masses dans le cadre d'un État incité à la surveillance lors de sa gouvernance. Cette inquiétude est d'autant plus justifiée par l'accessibilité des données des identités numériques régaliennes ouverte à un nombre élargi d'acteurs publics. En France, nombre d'agents disposent, en effet, de la possibilité d'accéder au fichier des titres électroniques sécurisés (TES). La CNIL mentionne à cet égard « *des agents désignés et habilités du ministère de l'Intérieur, du ministère des Affaires étrangères, des préfectures et des sous-préfectures, ainsi que des agents diplomatiques et consulaires, en charge des cartes d'identité ou des passeports, des agents des communes désignés et habilités par le maire ; pour certains passeports (« passeport de mission ») des agents désignés et habilité du ministère de la Défense ; des agents de l'Agence nationale des titres sécurisés chargés de la mise en œuvre du droitement, individuellement désignés et dûment habilités par leur directeur* ». D'autres services de l'État peuvent également y accéder dans l'exercice de leurs missions tels que « *la police nationale, la gendarmerie nationale, le DGSI et la DGSE, dans le cadre de missions de prévention et de répression des atteintes aux intérêts de la Nation et des actes de terrorisme ; la police, la gendarmerie et la douane pour le contrôle de l'identité des personnes (par exemple la police aux frontières) ; la police judiciaire dans le cadre de collaborations avec INTERPOL et avec les États appliquant le système Schengen II (SIS II)* »[86]. La multiplicité et la variété de ces acteurs publics, disposant de possibilités d'accès

[85] D. J. Solove, "*Access and Aggregation: Privacy, Public Records, and the Constitution*", *Minnesota Law Review,* Vol. 86, 1137, 2002, disponible sur SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=283924
[86] CNIL, « Le fichier des titres électroniques sécurisés (TES) », 28 mai 2021, https://www.cnil.fr/fr/le-fichier-des-titres-electroniques-securises-tes

aux données, augmentent les risques de dérives potentielles. A ce titre, il est crucial d'établir des contrôles réguliers de leurs activités par des moyens indépendants et autonomes, assortis, le cas échéant, de sanctions dissuasives en cas d'abus. Doivent aussi envisagés des rapports annuels mis à la disposition du Parlement et des citoyens.

2 – Les moyens inquiétants de la collecte exponentielle des données identifiantes

33. **Une nécessaire vigilance face à la démultiplication des moyens d'identifications numériques.** La collecte des données personnelles intervient principalement par les portefeuilles d'identités numériques, mais aussi par la mise en place de nouveaux moyens tels que la reconnaissance faciale ou encore les QR codes, les objets connectés, les monnaies virtuelles, la *Smart City*, qui contribuent à la création de nouvelles formes d'identifications numériques. A ce titre, des précautions s'imposent.

34. **La reconnaissance faciale, moyen controversé de l'extension de l'identification numérique**. La reconnaissance faciale [87] , procédé d'identification biométrique, permettant d'identifier le visage d'une personne grâce à une image ou à une vidéo, tend à se démultiplier avec des objectifs d'authentification et d'identification des personnes. Elle devient un moyen de contrôle et de surveillance des personnes individuelles et des masses par les États (collectivités, villes, aires de transport, écoles, cantines scolaires [88] , minorités telles que les Ouïghours en Chine[89]). Elle est appréhendée comme un outil de sécurisation et de paix sociale face aux multiples risques terroristes,

[87] Sur le sujet : T. Christakis, K. Bannelier, Cl. Castelluccia, D. Le Métayer, Projet de recherche universitaire MAPFRE, 6 rapports sur l'utilisation de la reconnaissance faciale dans les espaces publics en Europe, MW Grenoble Alpes, AI Régulation.com, 16 mai 2022, https://ai-regulation.com/; Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) Didier Baichère, « La reconnaissance faciale », note n°14, juillet 2019, https://www2.assemblee-nationale.fr/content/download/82754/922439/version/1/file/Note+Scientifique+-+Reconnaissance+Faciale+-+VF+19072019.pdf ; C. Castellucia, D. Le Metayer, « Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode », Rapport de recherche INRIA Grenoble Rhône-Alpes, 2019, https://hal.inria.fr/hal-02373093/document ; International, Biometrics & Indentity Association (IBIA), « NIST Report on Facial Recognition : A Game Changer » 2020, https://www.ibia.org/download/datasets/5124/NIST%20Report%20on%20Facial%20Recognition-%20A%20Game%20Changer.pdf

[88] TA Marseille, n°1901249 La Quadrature du Net, 27 février 2020, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf Cette affaire porte sur une expérimentation de contrôle d'accès par comparaison faciale et de suivi de trajectoire dans une école. La délibération du Conseil régional de Provence-Alpes-Côte d'Azur du 14 déc est annulée en tant qu'elle a « lancé l'expérimentation du dispositif de contrôle d'accès virtuel » dans deux lycées de Nice.

[89] Y. Yang, M. Murgia, « Une fuite de données révèle que la Chine suit près de 2,6 millions de personnes au Xinjiang », Financial Times, 17 fév 2019, https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812

insurrectionnels, et aussi pour faire face à des comportements délictueux et criminels (actions de préventions, identification des présumés coupables lors des enquêtes). Les entreprises, qui y ont aussi recours, l'appréhendent comme un moyen offert à leurs clients de passer commande sur un écran et de payer. Elle est aussi un moyen de surveillance contre le vol. La jonction entre la reconnaissance faciale et l'identification numérique, bien que justifiée *a priori* par des finalités de sécurisation et de protection, peut, si elle est mal circonscrite, porter atteinte gravement aux libertés individuelles et instituer des surveillances personnelles et de masse. Dans ce sens, le rapport d'information n°627 (2021-2022) de Messieurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain portant sur « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance »[90] du 10 mai 2022, ainsi que le rapport d'information portant sur « L'identité numérique », déposé par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis le 8 juillet 2020 auprès de l'Assemblée nationale, ont consacré d'important développements sur ce sujet[91]. L'identité numérique directe par *Alicem, désormais remplacée par le moyen d'identification électronique* « Service de garantie de l'identité numérique (SGIN) par le biais du décret n°2022-676 du 26 avril 2022[92], et l'identité numérique indirecte par l'usage de systèmes de reconnaissances faciales telles que *Clearview AI,* permettent de mieux prendre conscience de l'importante vigilance qui s'impose dans ce domaine sensible.

Le traitement d'identité numérique par la reconnaissance faciale Alicem initialement mis en application en dépit des fortes réserves de la CNIL. Au niveau national, le décret n°2019-452 du 13 mai 2019, désormais abrogé *par l*e décret n°2022-676 du 26 avril 2022, avait autorisé la création d'un moyen d'identification électronique dénommé « *Authentification en ligne certifiée sur*

[90] Sénat, Rapport d'information n°627 (2021-2022) de Messieurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain portant sur « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », fait au nom de la commission des lois, déposé le 10 mai 2022, http://www.senat.fr/rap/r21-627/r21-627.html Ce rapport est ambivalent puisque s'il condamne la reconnaissance facile au nom du rejet d'une société de surveillance, paradoxalement, il préconise un test pendant trois ans de la reconnaissance faciale (recommandation n°7) et l'indentification des « ressorts d'une meilleure acceptabilité de cette technologie (recommandation n°1). Présentation *You Tube* in Romain David, « Reconnaissance faciale : le Sénat plaide pour une loi d'expérimentation », Public Sénat, 10 mai 2022, https://www.publicsenat.fr/article/societe/info-public-senat-reconnaissance-faciale-le-senat-plaide-pour-une-loi-d

[91] Assemblée nationale Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique », préc.

[92] Ce décret abroge le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ». Il est publié au JORF n°0098 du 27 avril 2022, Texte n°27, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825

mobile » (Alicem)[93]. Ce traitement automatisé, sous l'égide du ministère de l'Intérieur, permettant de délivrer une identique numérique Alicem, avait pour finalité de permettre aux personnes, titulaires d'un passeport biométrique ou d'un titre de séjour électronique, comportant un composant électronique, de se créer, à partir de celui-ci, une identité numérique sur leur application mobile de leur téléphone disposant d'un système d'exploitation « Android » et de la technologie sans contact. Tout l'enjeu de la reconnaissance faciale ainsi utilisée était de leur permettre de s'identifier et de s'authentifier auprès des fournisseurs de services en ligne *via* « *FranceConnect* ». Cette initiative s'était révélée exceptionnelle puisque l'article 9 posait l'interdiction de principe de traitement de ce type de données avant d'en définir les exceptions. Nonobstant les réserves émises lors de la délibération n°2018-342 du 18 octobre 2018 sur le projet de décret[94], la CNIL avait considéré le risque élevé pour les droits et les libertés des personnes physiques en mentionnant que *« le consentement au traitement des données biométrique ne peut être regardée comme libre et étant susceptible de lever l'interdiction posée par l'article 9.1 du RGPD* », *« la nécessité de recourir à un dispositif biométrique pour vérifier l'identité d'une personne, dans le but d'atteindre le niveau élevé de l'identité numérique, au sens du règlement e-IDAS, n'a pas été établie, compte tenu notamment de la possibilité de recourir à des dispositifs alternatifs de vérificati*on». En soulignant les risques potentiels, l'association de défense des personnes dans l'espace numérique « La Quadrature du net »[95] avait engagé le 15 juillet 2019 une action aux fins d'annulation du décret du 13 mai 2019[96]. Le Conseil d'État, le 4 novembre 2020, avait néanmoins rejeté la demande d'annulation du décret de la création Alicem pour excès de pouvoir[97], ce traitement automatisé d'identité numérique, continuant de fonctionner, invitait à la prudence et à la vigilance compte-tenu des réserves importantes qui étaient émises. Il n'a pas finalement été pérennisé puisqu'il a été remplacé par un autre système.

---

[93] JORF n°0113 du 16 mai 2019, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038475477/#:~:text=D%C3%A9cr%C3%A8te%20%3A-,Chapitre%20Ier%20%3A%20Dispositions%20autorisant%20la%20cr%C3%A9ation%20d'un%20traitement%20de,)%20(Articles%201%20%C3%A0%2014)

[94] La CNIL a rendu un avis sur le projet de décret autorisant Alicem par la délibération n°2018-342 du 18 octobre 2018, JO, 16 mai 2019, texte 81, Différentes réserves ont été émises, https://www.legifrance.gouv.fr/download/pdf?id=JQDkiVqbiPoVpbHfpdweSZcrPSXYo-T8chbNahjpRk0=

[95] La Quadrature du Net, https://www.laquadrature.net/nous/

[96] La Quadrature du Net, « La Quadrature du net attaque l'application Alicem contre la généralisation de la reconnaissance faciale », 17 juillet 2019, https://www.laquadrature.net/2019/07/17/la-quadrature-du-net-attaque-lapplication-alicem-contre-la-generalisation-de-la-reconnaissance-faciale/ ; Requête introductive d'instance du 15 juillet 2019 : https://www.laquadrature.net/wp-content/uploads/sites/8/2019/07/1084951458_DECR_ALICEM_REQ.pdf

[97] CE, n°432656, 4 novembre 2020, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-11-04/432656; https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2020-11-04/432656?download_pdf

Le traitement d'identité numérique par reconnaissance faciale via Alicem désormais remplacé par le service de garantie de l'identité numérique (SGIN). Le traitement d'identité numérique par reconnaissance faciale Alicem a finalement été abrogé *par l*e décret n°2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique (SGIN). Une nouvelle application permet aux titulaires d'une carte d'identité électronique, disponible sur le territoire national depuis le 2 août 2021, de disposer d'un moyen d'identification électronique sans qu'il soit question de biométrie et de reconnaissance faciale. Les usagers ont ainsi la possibilité facultative[98] de recourir à l'identification électronique aux fins de de leur identification et authentification auprès de fournisseurs en ligne publics ou privés auxquels ils recourent, grâce à leur téléphone portable doté d'une technologie de lecture sans contact[99] leur permettant de pouvoir lire le composant électronique de leur carte nationale d'identité[100] et d'une application mobile compatible. Le contenu de ce décret a été accueilli favorablement par la CNIL[101] par le biais de la délibération n°2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile »[102] et par la délibération n°2022-011 du 10 février 2022 portant avis sur un projet de décret dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » [103], avec toutefois des

[98] Le sommaire du décret précise explicitement que « La création du moyen d'identification électronique et non utilisation relèvent de l'unique volonté des usagers ».
[99] Technologie puce NCF intégrée aux smartphones, permettant la communication en champ proche permettant le scan de la carte d'identité biométrique dans l'applications et de lire la carte d'identité électronique. Cette puce est déjà utilisée dans le cadre des paiements mobiles.
[100] Ce sera étendu par la suite aux passeports.
[101] Pour la présentation des deux délibérations de la CNIL portant sur le contenu du décret : J-M Manach, « Qualifié d'aboutissement d'échanges nourris avec le ministère » de l'Intérieur, la CNIL « accueille très favorablement le nouveau « Service de garantie de l'identité numérique (SGIN) qui fait suite à l'application mobile Alicem de reconnaissance faciale biométrique ainsi qu'au « fichier des gens honnêtes », NextInpact, 28 avril 2022, https://www.nextinpact.com/article/69022/identite-numerique-cnil-approuve-successeur-dalicem
[102] CNIL, Délibération n°2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'une moyen d'identification électronique dénommé "Service de garantie de l'identité numérique » et abrogeant le décret n°2019 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », https://france-identite.gouv.fr/assets/files/CNIL-D%C3%A9lib%C3%A9ration-2021-151_SGIN-France-Identit%C3%A9-1.pdf
[103] CNIL, Délibération n°2022-011 du 10 février 2022 portant avis sur un projet de décret dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne

demandes de précisions complémentaires. Le fait même que la Cnil ait fait un bon accueil à cette nouvelle modalité est rassurant. Il convient toutefois de rester vigilant puisque des régimes dérogatoires sont maintenus, notamment concernant le dispositif de rapprochement par photographies dans le cadre du traitement des antécédents judiciaires ou encore des actions menées par les aéronefs en vue d'assurer la sécurité civile suite au décret n°2022-712 du 27 avril 2022 portant application des articles L.242-1 et suivants du code de la sécurité intérieure et relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs des acteurs de la sécurité civile[104].

L'affaire Clearview AI illustrant une prise de conscience collective des risques de la reconnaissance faciale permettant l'identification numérique. La société *Clearview AI* a collecté, *via* un moteur de recherche biométrique, des données personnelles de photographies et de vidéos accessibles sur internet à partir des images des sites *web* et des réseaux sociaux, sans consentement des personnes concernées, ni même le respect de la base légale imposée par l'article 6 du RGPD, le traitement de données étant par conséquent illicite et sans laisser la possibilité pour les personnes concernées de pouvoir accéder leurs données[105] et demander leur effacement. Cette société, valorisée à 130 millions de dollars, ayant construit sa base des données comprenant plus de 10 milliards d'images dans le monde, affirme qu'elle pourrait, atteindre 100 milliards de photographies de visages dans sa base de données d'ici un an[106], ce qui lui permettrait de rendre *« presque tout le monde (…) identifiable* ». La société commercialise l'accès à cette base d'images principalement aux forces de police du monde entier. Elle établit un véritable système de surveillance, permettant aux forces de l'ordre d'identifier, dans le cadre d'enquêtes, les auteurs de vols à l'étalage, de fraudes par carte de crédit, d'agressions, de destructions, de viols d'enfants[107], de meurtres, ce

certifiée sur mobile », https://france-identite.gouv.fr/assets/files/CNIL-D%C3%A9lib%C3%A9ration-2022-011_SGIN-France-Identit%C3%A9-2.pdf Ce second avis intervient uniquement sur la désignation des responsables de traitement, l'étendue de la responsabilité de traitement de l'administration, ainsi que d'autres modifications du décret.

[104] Décret n°2022-712 du 27 avril 2022 portant application des articles L.242-1 et suivants du code de la sécurité intérieure et relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs des acteurs de la sécurité civile, JORF n°0099 du 28 avril 2022, Texte n°21, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045683289

[105] Articles 12, 15 et 17 du RGPD.

[106] D. Harwell, « La société de reconnaissance faciale Clearview AI indique aux investisseurs qu'elle cherche une expansion massive au-delà de l'application de la loi », The Washington Post, 16 fév 2022, https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/

[107] A. Leparmentier, « Clearview, la start-up new-yorkaise de reconnonnaissance facile qui a aspire vos photos", Le Monde, 11 janvier 2022, https://www.lemonde.fr/pixels/article/2022/01/11/clearview-ai-le-big-brother-qui-a-aspire-toutes-vos-photos_6108951_4408996.html Cet article fait état de l'arrestation du pédocriminel argentin Andres Viola par la police fédérale grâce au recoursà Clearwiew IA.

qui peut avoir pour effet de faciliter les arrestations. Elle a aussi récemment autorisé l'accès, grâce à son moteur de recherche de reconnaissance faciale, à titre gratuit, au ministère ukrainien de la défense de pouvoir repérer les assaillants russes et d'identifier les morts au combat[108]. De même, certaines sociétés privées y ont progressivement recours alors même que cette faculté est critiquée. Progressivement, une véritable prise de conscience s'est mise en place concernant les risques de surveillances de masse généralisées et les atteintes aux libertés individuelles compte-tenu des possibilités offertes par la société *Clearview AI* en matière de reconnaissance faciale.

Les CNIL française[109] et australienne[110] ont mis cette société en demeure de cesser la réutilisation de photographies accessibles sur internet. La CNIL italienne l'a sanctionné en mars 2022 par une amende de 20 millions d'euros et en lui imposant la suppression de toutes les données des personnes localisées en Italie et l'arrêt immédiat de toute collecte et traitement des données par l'intermédiaire du système de reconnaissance faciale[111]. La CNIL du Royaume-Uni, l'Information Commissionner's Officle (ICO), le 23 mai 2022, lui a infligé une amende de 7,5 millions de livres sterling, soit l'équivalent de 8,85 millions d'euros et lui a aussi ordonné la suppression des données britanniques[112].. La CNIL suédoise a, au surplus, condamné la police pour avoir utilisé illégalement les photographies des citoyens par une amende de 250 000 euros[113]. La police canadienne a officiellement annoncé la fin du recours au service de

[108] P. Daveet, J. Datin, « Exclusif : l'Ukraine a commencé à utiliser la reconnaissance faciale de Clearview AI pendant la guerre », Reuters, 14 mars 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

[109] CNIL, « Reconnaissance faciale : la CNIL met en demeure Clearview AI de cesser la réutilisation de photographies accessibles sur son site internet », 16 décembre 2021, https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de ; Décision n°MED-2021-134 du 26 novembre 2021 mettant en demeure la société Clearview AI, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044499030?init=true&page=1&query=CLEARVIEW&searchField=ALL&tab_selection=all

[110] Office of the Australien Information Commissioner (OAIC), « Clearwiew AI a violé la vie privée des australiens", 2 novembre 2021, https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy

[111] Garante per la protezione del date personali (GPDP), « reconnaissance facile : la GPDP inflige une amende de 20 millions d'euros à Clearview. L'utilisation de données biométriques et la surveillance des italiens sont interdites », Communiqué de presse, 9 mars 2022, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323

[112] ICO, « ICO inflige une amende de plus de 7,5 millions de livres sterling à la société de base de données de reconnaissance facile Clearview AI Inc et ordonne la suppression des données britanniques », 23 mai 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/ ; https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/

[113] A. Vitard, « La CNIL suédoise condamne la police pour avoir utilisé la technologie de Clearview AI », L'Usine digitale, 12 fév 2021, https://www.usine-digitale.fr/article/la-cnil-suedoise-condamne-la-police-pour-avoir-utilise-la-technologie-de-clearview-ai.N1060624

reconnaissance faciale de *Clearview AI*[114]. Pour leur part, conscients des dérapages possibles en matière de reconnaissance faciale, les géants du numérique ont mis en demeure la *start-up Clearview AI* de cesser toute collecte d'images sur leurs sites. Ils ont mêmes, momentanément, ou complètement, cessé leurs ventes de logiciels de reconnaissance faciale. L''Union américaine pour les liberté civile (ACLU) a en outre obligé Clearview AI, par un règlement conclu le 9 mai 2022, de cesser la vente de ses bases de données biométriques aux entreprises et autres acteurs privés conformément à la loi sur la confidentialité des informations biométriques de l'Illinois (BIPA) dans l'Illinois et plus généralement aux Etats-Unis[115].

Le point de vue ambigu de l'Union européenne sur la reconnaissance faciale. Initialement, la Commission européenne avait envisagé d'interdire la reconnaissance faciale sur les lieux publics pour une durée de trois à cinq ans. Cette ambition a été abandonnée en janvier 2020[116]. En février 2020, elle a eu le projet de constituer une base de données unique et partagée avec les Etats-Unis sur la reconnaissance faciale, dans la continuité de la convention *Prüm ayant constitué* des bases de données d'empreintes digitales et d'ADN aux fins de lutter contre le terrorisme, la criminalité et la migration illégale[117]. Par ailleurs, suite au livre blanc portant sur « Intelligence artificielle – une approche européenne axée sur l'excellence et la confiance »[118], le 21 avril 2021, la Commission européenne a émis une proposition de règlement au Parlement et au Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes

[114] La Presse canadienne, le 7 juillet 2020, https://ici.radio-canada.ca/nouvelle/1717708/intelligence-artificielle-clearview-ai-protection-vie-privee-canada

[115] Ces différentes informations ont été officialisées par l'ACLU le 9 mai 2022 via Twitter : https://twitter.com/ACLU/status/1523712568761540608 ; ACLU illilois « Dans Big Win, le règlement garantit que clearview AI est conforté à la loi révolutionnaire sur la confidentialité biométrique de l'Illinois », 9 mai 2022, https://www.aclu-il.org/en/press-releases/big-win-settlement-ensures-clearview-ai-complies-groundbreaking-illinois-biometric

[116] F. Yun Chee, "L'UE abandonne l'idée d'interdire la reconnaissance facile dans les espaces publics", Reuters, 30 janvier 2020, https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q?feedType=RSS&feedName=technologyNews ; Parlement européen, « Cross-boder Exchange and Comparison of forensic DNA Data in the Context of the Prüm Decision", Juin 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf

[117] N. Burova, « Vers un fichier unique pour la reconnaissance faciale au sein de l'UE ? », Les numériques, 26/02/2020, https://www.lesnumeriques.com/vie-du-net/vers-un-fichier-unique-pour-la-reconnaissance-faciale-au-sein-de-l-ue-n147605.html ; Z. Campbell, C. Jones, « Des fuites de rapports montrent que la police de l'UE prévoit un réseau paneuropéen de bases de données de reconnaissance faciale », The Intercept, 21 fév. 2021, https://theintercept.com/2020/02/21/eu-facial-recognition-database/

[118] COM (2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

législatifs de l'Union [119]. Celle-ci précise, dans le considérant 18, que « *L'utilisation de systèmes d'IA pour l'identification biométrique à distance « en temps réel » de personnes physiques dans des espaces accessibles au public à des fins répressives est considérée comme particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux* ». Toutefois, dans le considérant suivant, après avoir relevé que « *l'utilisation de ces systèmes à des fins répressives devrait être interdite* », la proposition de règlement envisage trois cas d'exception : la recherche de victimes potentielles d'actes criminels, y compris les enfants disparus, certaines menaces pour la vie ou la sécurité physiques des personnes physiques, y compris les attaques terroristes ; et la détection, la localisation, l'identification ou les poursuites à l'encontre des auteurs ou des suspects de certaines infraction pénales strictement circonscrites. Reste à savoir si ces dispositions sont suffisantes pour préserver effectivement les droits et les libertés fondamentales des personnes et leur vie privée, ce qui n'est pas évident à la lecture de l'avis critique du Comité européen de la protection des données et du contrôleur européen de la protection des données (EDPD/EDPS) [120]. Dans la continuité de cette proposition, en septembre 2021, le service de recherche du Parlement européen a publié une « analyse approfondie » portant sur la « Réglementation de la reconnaissance faciale au sein de l'Union européenne »[121]. En octobre 2021, par une résolution adoptée par 377 voix pour, 248 contre, et 62 abstentions, les députés européens ont manifesté leur volonté d'interdire les bases de données privées de reconnaissance faciale[122], de même que l'interdiction de la reconnaissance automatisée des personnes dans les espaces publics pour éviter tout risque de surveillance. Une exception a été toutefois émise pour les citoyens soupçonnés d'un crime. En avril 2022, la Présidence française du Conseil de l'Union européenne a présenté différentes modifications à l'égard du futur règlement sur l'intelligence artificielle, l'*Artificial Intelligence Act,* tendant à élargir les cas de recours par les forces de l'ordre à la reconnaissance biométrique en

[119] COM (2021) 206 final, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0206
[120] EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 june 2021, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
[121] Parlement européen, Service de recherche, «Réglementation de la reconnaissance faciale au sein de l'Union européenne », septembre 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0206
https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_FR.pdf
[122] Parlement européen, « Utilisation de l'intelligence artificielle par les forces de police : les députés contre la surveillance de masse », Communiqué de presse, 6 oct 2021, https://www.europarl.europa.eu/news/fr/press-room/20210930IPR13925/utilisation-de-l-ia-par-la-police-les-deputes-contre-la-surveillance-de-masse

supprimant notamment la notion aux enfants disparus et en élargissant son recours en matière pénale[123], alors même que, dans le même temps, la Cour de justice de l'Union européenne, le 5 avril 2022 a confirmé que *« le droit de l'Union s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques aux fins de la lutte contre les infractions grave* », ce qui constitue une limite aux investigations numériques étatiques en matière pénale[124] . A la lecture de ces stratégies politiques mouvantes, il reste difficile de se faire une idée de la volonté réelle de l'Union européenne qui, selon les circonstances, prend position pour ou contre le recours à la reconnaissance faciale. Cette valse d'hésitations montre toute la difficulté d'avoir une position ferme et unique sur ce sujet présentant nombre d'atouts, mais aussi des risques majeurs, posant au fond la question de la légitimité de la reconnaissance faciale comme moyen d'identification et d'authentification numérique.

***Les risques de biais ou d'erreur de la reconnaissance faciale, facteur de discriminations et d'erreurs*[125]**. A la complexité même des choix stratégiques concernant l'opportunité ou pas de recourir à la reconnaissance faciale, d'autres limites, imputables à la reconnaissance faciale, viennent poser le questionnement de son intérêt. Le recours même à des systèmes d'intelligence artificielle sont potentiellement sources de biais ou d'erreurs à l'origine de discriminations contestables. Tout dépend des modèles adoptés en matière de technologies algorithmiques, des types de systèmes apprenants, de leur conception, de leur déploiement et de la qualité des systèmes de données employés où les humains interfèrent encore beaucoup. Plusieurs types de biais[126] peuvent être intégrés volontairement et intentionnellement, avec ou sans finalités légitimes et proportionnées, ce qui, dans ce dernier cas, revient à des formes de manipulations. Les inégalités générées par les biais sont

[123] A. Vitard, « La France ne veut pas bloquer l'utilisation de l'IA par les forces de l'ordre », L'usine digitale, 6 avril 2022, https://www.usine-digitale.fr/article/la-france-ne-veut-pas-bloquer-l-utilisation-de-l-ia-par-les-forces-de-l-ordre.N1991227 ; L. Bertuzzi, « La présidence française propose des modifications aux dispositions répressives de la loi sur l'IA », Euractiv, 5 avril 2022, https://www.euractiv.com/section/digital/news/french-presidency-pitches-changes-to-law-enforcement-provisions-in-the-ai-act/

[124] CJUE, Communiqué de presse n°58/22, 5 avril 2022, Arrêt dans l'affaire C-140/20 Commissionner of the Garda Siochana e.a., https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-04/cp220058fr.pdf ; arrêt : https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=1788990

[125] R. Schwartz, A. Vassilev & al, « Vers une norme d'identification et de gestion des biais en IA », NIST, Special Publication, 1270, 15 mars 2022, https://www.nist.gov/publications/towards-standard-identifying-and-managing-bias-artificial-intelligence

[126] Pour la présentation des différents types de biais : Telecom, ParisTech, P. Bertail, D. Bounie, C. Stephan, W. Patrick, « Algorithmes : biais, discrimination et équité », Février 2019, https://www.telecom-paris.fr/wp-content-EvDsK19/uploads/2019/02/Algorithmes-Biais-discrimination-equite.pdf

susceptibles de décrédibiliser la reconnaissance faciale, de remettre en cause la confiance des utilisateurs, et même être à l'origine de possibles actions en responsabilité. Les marges d'erreurs sont d'autant plus préoccupantes lorsqu'elles sont utilisées dans le cadre d'enquêtes judiciaires. Par exemple, le projet de recherche *Genders hades* démontre, à partir de 1270 images de personnes, les biais et les taux d'erreurs concernant le recours à l'intelligence artificielle, particulièrement concernant l'identification du sexe à l'étude du visage des personnes de couleurs foncées[127]. Le paroxysme des biais a été mis en évidence à l'égard d'un logiciel de reconnaissance facile de Google ayant appréhendé un couple d'Afro-américains comme des gorilles[128]. L'afro-américain, *Robert Julian-Borchak Williams* a été arrêté à tort après qu'un système de reconnaissance faciale l'ait répertorié à comme auteur d'un vol à l'étalage. Il a ainsi été conduit dans un centre de détention. Il a, par la suite, reçu des excuses du procureur du comté de Wayne[129]. Conscients des dérapages potentiels des systèmes d'intelligence artificielles en lien avec la reconnaissance faciale, les députés européens, après avoir dénoncés les risques, ont, en octobre 2021, préconisé la transparence des algorithmes suffisamment documentés et leur traçabilité, ainsi que des contrôles humains et juridiques élevés, particulièrement dans le cadre des services répressifs[130]. Sans interdire le recours aux systèmes d'intelligences artificielles axés sur les reconnaissances faciales, les parlementaires limitent leurs conditions d'utilisation. Cette nécessaire prudence est d'autant plus indispensable que l'utilisation de la reconnaissance faciale ne cesse de se déployer au prétexte d'expérimentations, lesquelles restent peu encadrées. Elle est encore plus justifiée puisque se développent des systèmes de reconnaissance faciale seconde génération, dont l'objet est de déterminer la probabilité de crimes avant même qu'ils ne se réalisent, à l'exemple de la mise en place de caméras de surveillance dotées d'IA par la police de Séoul[131]. Il s'avère par conséquent indispensable que les possibilités de reconnaissances faciales demeurent extrêmement limitées et que les États membres, ainsi que la Commission

[127] Projet de recherche Gender Shades, « Dans quelle mesure les services IBM, Microsoft et Face++ devinent-ils le sexe d'un visage », http://gendershades.org/overview.html
[128] « Le logiciel de reconnaissance faciale de Google confond le portrait d'Afro-américains avec des gorilles », Huffpost, 2 juill 2015, https://www.huffingtonpost.fr/2015/07/02/logciel-reconnaissance-faciale-google-confond-afro-americains-gorilles_n_7711592.html
[129] C. du Cachemire, « Accusé à tort par un algorithme », New York Times, 24 juin 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html
[130] Parlement européen, « Utilisation de l'intelligence artificielle par les forces de police : les députés contre la surveillance de masse », Communiqué de presse, 6 oct 2021, https://www.europarl.europa.eu/news/fr/press-room/20210930IPR13925/utilisation-de-l-ia-par-la-police-les-deputes-contre-la-surveillance-de-masse
[131] A. Le Denn, « Le district de Séoul s'équipe de caméras dotées d'IA pour détecter un crime avant même qu'il ne soit commis », L'usine Digitale, 2 janvier 2020, https://www.usine-digitale.fr/article/le-district-de-seoul-s-equipe-de-cameras-dotees-d-ia-pour-detecter-un-crime-avant-meme-qu-il-ne-soit-commis.N916679

européenne, prévoient des conditions restreintes, de même que des contrôles et des sanctions.

35. **La mise en place d'autre moyens d'identification susceptibles de tracer les personnes au détriment de leurs libertés et vie privée**. Dans la lignée de la reconnaissance faciale, des moyens tels que les QR Code, les objets connectés, la monnaie virtuelle sont susceptibles de tracer les activités des personnes, de les identifier, de connaître certains éléments de leur vie privée (lieux, personnes croisées, achats, consommations), ce qui indirectement revient à des formes extensives d'identités numériques personnalisées mises en place par les autorités publiques et les entreprises privées.

Les QR Codes. Le développement du QR code, inventé par le japonais *Masahiro Hara* pour un usage dans le secteur automobile est une technologie sous licence libre depuis 1999. Intégré aux *smartphones*, il s'est intensifié depuis plusieurs années. Le QR code, permettant le flash du « sans contact », a fait l'objet d'un important développement dans le cadre des passes sanitaires pour la gestion de la pandémie Covid19. Utilisé par une marge toujours plus importante de la population nationale, il permet de simplifier les démarches administratives, d'obtenir des informations de toutes natures, de faciliter les paiements, de permettre l'accès à certains services (transports, aéroports, gares, musées, panneaux publicitaires, etc.). Il peut même se déployer à l'échelle de l'Union européenne, à l'exemple des passes sanitaires comprenant un QR code avec un identifiant unique ayant permis la libre circulation des personnes vaccinées. Cette modalité permet de mieux se projeter vers de nouvelles formes d'identités numériques, susceptibles d'être développées à l'avenir, ainsi que de ses dangers potentiels à l'exemple de l'installation de QR codes sur les portes des maisons de la minorité musulmane ouïghoure dans le Xinjiang, pratique dénoncée par l'ONG Human Rights Watch[132]. Au surplus, le FBI a récemment mis en garde contre les QR Codes malveillants permettant de dérober des données personnelles des utilisateurs[133].

Les objets connectés. En raison de l'émergence de l'internet des objets (IoT) et de son développement exponentiel les années qui viennent, les objets connectés, à l'exemple de ceux développés dans le domaine de la santé[134],

[132] T. Embury Dennis, « La Chine installe des QR code sur les maisons musulmanes Ouïghoures dans le cadre de la répression de sécurité de masse », Independent, 12 sept 2018, https://www.independent.co.uk/news/world/asia/china-uyghur-muslims-xinjiang-province-qr-codes-security-crackdown-hrw-a8532156.html

[133] FBI, « Les criminels falsifient les QR Codes pour voler les fonds des victimes », 18 janvier 2022, https://www.ic3.gov/Media/Y2022/PSA220118

[134] T. Jourdan, A. Boutel & C. Frindel, « Vers la protection de la vie privée dans les objets connectés pour la reconnaissance d'activité en santé », Revue des Sciences et ecthnologies de l'information, Série TSI, Lavoisier, 20 déc 2019, https://hal.inria.fr/hal-02421854/document

peuvent enregistrer de nombreuses données personnelles, en lien avec l'identité de la personne. Ces données peuvent, par la suite, être utilisées afin de mieux connaître le profil des personnes, ce qui correspond à des formes complémentaires d'identités numériques.

La monnaie virtuelle. La cryptomonnaie, monnaie virtuelle européenne, susceptible de se déployer par le biais de la Banque centrale européenne en 2023, pourrait aussi être susceptible de répertorier les dépenses effectuées par les utilisateurs. Elle constituerait une forme spéciale d'identité numérique économique permettant de recenser les dépenses de chaque utilisateur.

Les Smart Cities. Les « villes intelligentes » peuvent aussi apporter des capacités supplémentaires de centralisation de la collecte de données par la mise en place toujours plus importante de dispositifs de vidéosurveillance, de reconnaissance faciale et de recours aux QR Codes. Elles peuvent ainsi constituer un moyen encore plus important de collecte généralisée de données personnelles et de données de masse, renforçant sans cesse les modalités de surveillance au détriment des libertés fondamentales et de vie privée. La vigilance s'impose d'autant plus en considération des risques de déploiement d'un crédit social par les États membres.

Au-delà même des différents moyens permettant d'étendre l'identité numérique de chaque personne, de plus en plus tracée, émergent les risques d'un crédit social restrictif des libertés fondamentales et de la vie privée.

B – Les risques d'un crédit social restrictif des libertés fondamentales et de la vie privée

36. **L'émergence d'un crédit social régalien en dépit des règles protectrices des libertés fondamentales et de la vie privée.** Normalement, l'identité numérique régalienne doit se conformer à la protection des libertés individuelles et respecter la vie privée des usagers conformément à l'article 19 de la Déclaration universelle des droits de l'homme[135], aux articles 8 et 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)[136], aux dispositions du RGPD, à l'article 9 du code civil[137] et à l'article premier de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Pourtant, alors même que ces textes constituent le socle des droits fondamentaux protecteurs des personnes directement concernées par

[135] Déclaration des droits de l'homme, article 19 portant sur la liberté d'opinion.
[136] Conv. EDH, articles 8 et 9, intervenant sur la protection de la vie privée et de la liberté d'expression.
[137] Article 9 du Code civil visant la protection de la vie privée.

l'identité numérique, derrière une politique d'incitation à des comportements vertueux et conformistes (1), se profile un crédit social européen (2).

1 – D'une politique d'incitation à des comportements vertueux et conformistes

37. **La mise en place d'incitations à des comportements vertueux et conformistes par une gouvernance responsable, prospère et efficace**. La mise en place progressive d'une gouvernance responsable, prospère et efficace de l'identité numérique, au niveau de l'Union européenne et/ou des États membres est une réponse à de multiples crises : politiques (tensions géopolitiques, terrorismes), économiques, environnementales et sanitaires. L'enjeu est d'inciter progressivement les citoyens à adopter des comportements vertueux destinés à leur apporter plus de paix, de sérénité, de tranquillité publique, avec en échange, des simplifications dans les démarches administratives, lors des achats de biens et de services, de meilleur suivi médical, etc. Progressivement, elle s'introduit aussi dans les écoles, permettant de vérifier la scolarisation des enfants au nom de l'obligation scolaire et de « rassurer » les parents de l'arrivée de leurs enfants. En d'autres termes, ce mode de gouvernance européen, légitimé au nom de l'intérêt général, conduirait à inciter les citoyens à adopter des comportements de plus en plus conformistes au détriment de leurs libertés. Les personnes, n'adoptant pas de comportement « irréprochable » en matière de consommation, dont les seuils seraient définis strictement par les autorités au nom d'une meilleure santé, de la protection de l'environnement, de la paix sociale et de la lutte contre les actes terroristes, pourraient alors être sanctionnés par la mise en place d'un crédit social européen.

2 – à un crédit social européen ?

38. **Les risques de dérapages en matière de risques de surveillance excessive et de restriction des libertés.** Si incontestablement, l'identité numérique présente l'intérêt de la protection des personnes physiques dans le cadre de la mise en place stricte des dispositions du RGPD, des dérapages restent envisageables en matière de surveillance et de restriction des libertés par l'Union européenne et les États membres.

39. **L'exemple du crédit social chinois.** Mis en place en 2014, le « système de crédit social » (shehui xinyong tixi) est assimilable à une surveillance de la vie quotidienne des citoyens chinois. Il a été développé par le gouvernement pour des finalités associées au sens civique des personnes pour une société socialiste harmonieuse, vertueuse et sécuritaire. Ceci renvoie à la fois à un comportement individuel (régime alimentaire, sport) et collectif (normes

sociales, standards de comportements tels que ne pas traverser lorsque le feu est rouge ou encore ne pas sortir en public en pyjama[138]). Toutes les données numériques sont utilisées de manière instantanée, non seulement par les autorités étatiques (coffre-fort numérique), mais aussi par des entreprises telles que les banques, les assurances et les géants du numérique. Ces données sont ensuite potentiellement mises à disposition des autorités. Grâce au recours du QR code, ainsi qu'à la reconnaissance faciale, les autorités chinoises mettent ainsi en place le système de « scoring » (notation sociale) de chaque citoyen en fonction de son comportement faisant l'objet d'une surveillance numérique constante par la police. Les gestes quotidiens sont ainsi enregistrés, stockés et analysés en temps réel par la police chinoise. Les citoyens, obtenant une note sociale faible, sont pénalisés par la désactivation à distance de certains de leurs droits, réduisant ainsi leurs possibilités de déplacement, restreignant l'obtention d'un visa, limitant la possibilité d'obtenir un rendez-vous médical, une chambre d'hôtel sans caution ou l'obtention de moyens de crédits[139]. Plus récemment, des déposants bancaires, qui ne pouvaient plus accéder à leurs fonds, ont pris la décision de manifester contre des banques chinoises. Afin de bloquer cette démarche, les autorités ont mis les applications de santé au rouge afin de bloquer les déplacements[140]. Bien que le crédit social de la Chine s'explique à la fois compte-tenu par les choix politiques, l'histoire, la culture et la densité de la population, il demeure un modèle d'autant plus important à analyser que l'Union européenne, ainsi que les États membres semblent avoir des propensions à s'en inspirer.

40. **Vers un crédit social européen ou national des États** ?

Les possibles dérapages des États concernés. La Commission européenne est de plus en plus incitée à mettre en place certaines modalités de surveillance, s'apparentant à des formes de crédits sociaux. Si en octobre 2021, les députés européens se sont prononcés, à l'occasion d'une résolution, contre « *les systèmes de notation sociale qui tentent d'évaluer la fiabilité des citoyens en fonction de leur comportement ou de leur personnalité* », et contre la *« police prédictive basée sur des données comportementales* » [141] , les autorités

[138] « Pyjamas en public : une ville chinoise s'excuse d'avoir « fait honte » aux habitants », BBC News, 21 janvier 2020, https://www.bbc.com/news/world-asia-china-51188669
[139] Sébastien Le Belzic, Documentaire sur le crédit social en Chine « Ma femme a du crédit », janvier 2022, YouTube https://youtu.be/Jt2HA7jfzj8
[140] E. Tham, « La manifestation contre les banques chinoises stopées par les codes de la santé virant au rouge, selon les déposants », Reuters, 16 juin 2022, https://www.reuters.com/world/china/china-bank-protest-stopped-by-health-codes-turning-red-depositors-say-2022-06-14/
[141] Parlement européen, « Utilisation de l'intelligence artificielle par les forces de police : les députés contre la surveillance de masse », Communiqué de presse, 6 oct 2021, https://www.europarl.europa.eu/news/fr/press-room/20210930IPR13925/utilisation-de-l-ia-par-la-police-les-deputes-contre-la-surveillance-de-masse

étatiques pourraient néanmoins être incitées à désactiver à distance certaines activités, pourtant essentielles pour les citoyens telles que la couverture santé pour ceux ne respectant pas la prise de médicaments, le permis de conduire en cas de perte de trop de points ou encore les moyens de paiement en cas de découvert important. Des comportements appréhendés comme « *inadéquats* » (tabagisme, obésité, non confinement pour les personnes atteintes par la Covid19) ou à l'origine de situations environnementales déficientes (consommation de trop d'énergie ou de trop litres d'essence), seraient susceptibles de mener au blocage automatique et à distance de certains services. Dans ce sens, le rapport d'information de Véronique Guillotin, Christine Lavarde et René-Paul Savary, déposé le 3 juin 2021 au nom de la délégation sénatoriale à la prospective sur « les crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés », fait état d'une réunion où un rapporteur propose, à propos de la gestion de la pandémie que, « *Dans un cas extrême, les données médicales d'un individu positif pourraient être croisées avec ses données de géolocalisation, et en cas de violation de sa quarantaine, conduire à une information des forces de l'ordre, où, par exemple, à une désactivation de ses moyens de paiement ou à une amende automatiquement prélevée sur son compte bancaire* (…) »[142]. Le recours aux passes sanitaires, notamment le certificat Covid numérique de l'UE, a démontré la possibilité d'interdire l'accès de certains citoyens réticents à la politique vaccinale nationale, à certains lieux et transports. Bien qu'intervenant dans le contexte particulier de pandémie Covid19, justifié par des finalités sanitaires, une importante vigilance s'impose concernant les critères justifiant de telles restrictions de droits.

L'installation croissante des dispositifs de reconnaissances faciales dans les lieux publics attentatoires aux libertés justifiant des moyens proportionnels aux enjeux de protection. Au-delà même des passes sanitaires, pourrait se développer un crédit social européen grâce aux portefeuilles d'identités numériques et aux moyens d'identifications associés à l'instar de la ville de Bologne qui, fin mars 2022, a officiellement annoncé un portefeuille du citoyen vertueux[143], ou encore, par le biais du digital wallet,

[142] Sénat, Rapport n°673, V. Guillotin, C. Lavarde et R-P Savary, « les crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés », p143, propos tenus lors d'une réunion du 6 mai 2021 « Examen en délégation », https://www.senat.fr/rap/r20-673/r20-6731.pdf ; https://www.senat.fr/rap/r20-673/r20-673.html Pour un billet d'humeur apportant différentes critiques sur ce rapport : Y. Chatelain, « Le Sénat admiratif du solutionnisme technologique à la chinoise », Contrepoints, 22 juin 2021, https://www.contrepoints.org/2021/06/22/400029-le-senat-admiratif-du-solutionniste-technologique-a-la-chinoise?via=Contrepoints&utm_source=boutonspartage&utm_medium=SOCIAL&utm_campaign=Twitter

[143] BolognaToday, « Piano digitale, un cervellone per il traffico et premi ai cittadini virtuosi », 29 mars 2022, https://www.bolognatoday.it/cronaca/piano-digitale-comune-bologna.html

développé par la société Thales[144]. Les moyens de vidéosurveillances déjà implantés dans les lieux stratégiques, mais aussi de plus en plus déployés dans des endroits plus courants, comprenant la reconnaissance faciale et le recours aux QR Codes ; seraient ainsi utilisés par les autorités publiques. Ces pratiques provoqueraient une « massification de la surveillance », au risque d'une surveillance policière pour des finalités sécuritaires sans cesse plus évoquées, plus seulement au niveau national mais aussi européen[145] dans la lignée de la proposition de règlement relatif à l'échange automatisé de données pour la coopération policière[146]. L'accès à certains lieux de consommation et de loisirs (cafés, restaurants, magasins, cinémas, musées) et services (administratifs, privés) pourraient être assujettis à des comportements vertueux, les personnes étant écartées en cas de consommation excessive d'alcool, de tabac, de viande, d'électricité, d'essence, achats de biens représentant un taux de CO2 élevé, de non tri des déchets, etc. De telles restrictions de libertés, justifiées par des « devoirs », au nom de l'intérêt commun, pourraient conduire à des dérapages incontrôlés, particulièrement par le biais de pénalités.

Les risques de manipulations des personnes et des masses suite à l'exploitation, par les systèmes d'intelligence artificielle, des données d'identité numérique. Le crédit social pourrait même aller au-delà de la surveillance et de la notation. Il serait susceptible, grâce à une collecte gigantesque des données, et avec les techniques de l'intelligence artificielle, d'anticiper les comportements des personnes afin de « prévenir certains évènements avant qu'ils ne se produisent »[147]. Grâce au profilage, appréhendé, conformément à l'article 4.4 du RGPD, comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* » et aux données d'interactions, de plus en plus performants[148], le crédit social pourrait alors

[144] Le Digital Id Wallet de Thales, YouTube, 27 mai 2021, https://www.youtube.com/watch?v=YSb0nLRte_A

[145] « Réformes de l'échange des données policières en Europe : vers une surveillance renforcée ? » ; The conversation, 16 mai 2022, https://theconversation.com/reforme-de-lechange-des-donnees-policieres-en-europe-vers-une-surveillance-renforcee-182778

[146] Sur le sujet : CEPD, Avis du CEPD sur la proposition de règlement relatif à l'échange automatisé de données pour la coopération policière, 2 mars 2022, https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-automated-data_en

[147] « Un vaste système de vidéosurveillance biométrique à Marseille attaqué en justice », Le Monde, 21 janvier 2020, https://www.lemonde.fr/pixels/article/2020/01/21/a-marseille-un-systeme-de-videosurveillance-biometrique-attaque-en-justice_6026735_4408996.html

[148] A-M. Cretu, F. Monti & al, « Les données, d'interactions sont identifiables même sur de longues périodes », Nature Communications, 13, 313 (2022), https://doi.org/10.1038/s41467-021-27714-6

constituer le moyen de contrôler certains citoyens potentiellement déviants et de les inciter à respecter certaines règles de comportement imposées pour la paix sociale avec, le cas échéant, des sanctions dissuasives en cas de non-respect. Certes, l'article 22 du RGPD pose le droit, pour la personne concernée « *de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* » mais des exceptions sont posées par ce même article, notamment la faculté pour le droit de l'État membre de d'y soustraire. Reste à savoir si les possibilités envisagées par les autorités étatiques permettront de maintenir un équilibre entre les droits des individus quant à leurs libertés et la protection de leur vie privée, et la nécessité de protéger la collectivité. Là encore, d'importants contrôles, notamment par les CNIL européennes, seront nécessaires, de même que, le cas échéant, des sanctions. Une vigilance majeure sera d'autant plus nécessaire que la Commission nationale consultative des droits de l'homme (CNCDH), lors de son avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, en date du 7 avril 2022, « *recommande, d'une part, d'interdire certains usages de l'IA jugés trop attentatoires aux droits fondamentaux, tels que le scoring social ou l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public. D'autre part, elle recommande de faire peser sur les utilisateurs d'un système d'IA des exigences en mesure de garantir le respect des droits fondamentaux : une étude d'impact, une consultation des parties prenantes, une supervision du système tout au long de son cycle de vie* »[149]. Cette mise en garde à l'égard des risques de dérapages et les préconisations de précautions à prendre *a minima* devraient plus que jamais être prises en considération au nom de la protection des citoyens français et, plus généralement, des ressortissants des États membres de l'UE.

41. **Des initiatives dans la lutte contre les risques croissants de crédit social national et européen**

Les actions nécessaires de contrôles des autorités nationales et européennes. Outre une indispensable transparence des autorités publiques des États justifiant les raisons permettant de telles restrictions, des modalités de contrôle, notamment par le biais des CNIL des pays de l'Union européenne et du Comité européen de protection des données s'avèrent indispensables. Dans ce sens, le CEDP a adopté, le 12 mai 2022, des lignes directrices sur l'utilisation de technologies de reconnaissance faciale par les autorités

[149] CNCDH, « Adoption de l'avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux », 7 avril 2022, https://www.cncdh.fr/node/2348

répressives et judiciaires »[150], lesquelles rappellent que les outils de reconnaissance faciale doivent être utilisés dans le « strict respect de la directive Police-Justice »[151] et « être proportionnés, comme le prévoit la Charte des droits fondamentaux de l'Union européenne ». Il liste par ailleurs la nécessité de prohiber certaines activités telles que « l'identification biométrique à distance des individus dans les espaces accessibles au public, des systèmes de reconnaissance faciale qui classent les individus sur la base de leurs données biométrique dans des groupes en fonction de l'ethnie, du texte, de l'orientation politique ou sexuelle ou d'autres motifs de discrimination ; la reconnaissance faciale ou des technologie similaires permettant de déduire les émotions d'une personne physiques, etc. ».

Les actions croissantes des associations et des membres de la société civile. Par ailleurs, la société civile doit, elle aussi, être amenée à réagir, à l'instar de la Quadrature du Net ayant déposé, le 24 mai 2022, une « plainte collective contre la technopolice » mentionnant que « *l'espace public est surveillé par un million de caméras qui, de plus en plus, sont équipées de logiciels visant à détecter des comportement « indésirables ». La police utilise la reconnaissance faciale 1600 fois par jour à partir des 8 millions de visages du fichier TAJ, et enregistre dans le fichier TES le visage de toute personne demandant un passeport ou une carte d'identité* »[152]. Il est proposé aux membres de la société civile de rejoindre la plainte collective ayant pour objet d' « attaquer devant la CNIL le ministère de l'intérieur et l'Etat français » en donnant mandat à la Quadrature du Net d'agir. Cette méthode d'implication directe des citoyens intervient dans un contexte où la société civile a tendance de plus en plus à réagir et à intervenir à l'égard des grandes problématiques que sont la liberté et l'écologie. Cette plainte collective intervient à la suite d'un rejet, par le Conseil d'Etat, le 26 avril 2022[153], des requêtes de la quadrature du

[150] CNIL, « Le CEPD publie des lignes directrices sur le calcul des amendes RGPD et sur l'utilisation de la reconnaissance faciale par les autorités, 17 mai 2022, https://www.cnil.fr/fr/le-cepd-publie-des-lignes-directrices-sur-le-calcul-des-amendes-rgpd-et-sur-lutilisation-de-la

[151] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, JOUE, 04.05.2016, L.119/89, https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0089.01.FRA ; CNIL, « Directive « Police-Justice » : de quoi parle-ton ? », 20 février 2019, https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t

[152] La Quadrature du net, « Plainte collective contre la technopolice », 22 mai 2022, https://www.laquadrature.net/2022/05/24/plainte-collective-contre-la-technopolice/ Site dédié : https://technopolice.fr/plainte/

[153] CE, 10ème Chambre, n°442364, 26 avril 2022, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364

Net concernant l'utilisation massive de la reconnaissance facile par la police dans le « traitement des antécédents judiciaires »[154].

III – Propositions

42. Différentes propositions, ayant pour objet de consolider l'identité numérique, se justifient pour répondre aux besoins des États membres de l'Union européenne et des ressortissants, ainsi que pour remédier aux risques qui y sont associés.

A – La mise en place d'identités numériques régaliennes accessibles pour tous

43. Alors même que le numérique est par essence technique et reste difficile à appréhender pour nombre de ressortissants de l'Union européenne, les États membres doivent prendre la mesure de l'importance d'une identité numérique régalienne accessible à tous. Ceci suppose *a minima* sa gratuité pour éviter tout risque de discrimination et de stigmatisation pour ceux qui ne pourraient pas y avoir accès. Outre ces principes d'égalité et d'accessibilité, doivent aussi être envisagées des solutions d'accompagnement telles que l'information, la formation, l'assistance par des médiateurs pour les personnes touchées par l'illectronisme ou l'illettrisme numérique. En outre, des mesures doivent être prises pour pallier à la désertification numérique préjudiciable aux personnes ayant à faire face de plus en plus à des formalités administratives numériques dépendantes de leur identité numérique. A cette fin, les États membres doivent être incités à assurer une couverture numérique territoriale aussi large que possible.

B – Le renforcement de la souveraineté numérique des États membres et de l'Union européenne en matière d'identité numérique

44. L'identité numérique, outil essentiel du pouvoir régalien des États membres sur leurs ressortissants, impose de reconnaître leur souveraineté absolue en la matière. Elle permet de consolider la souveraineté numérique de l'Union européenne génératrice d'un socle d'éléments interopérables entre les identités numériques des États membres souverains. Si l'identité numérique doit demeurer régalienne en termes de souveraineté, des compromissions doivent être envisagées avec les entreprises ayant déjà mis en place des identités numériques privées, à condition d'être encadrées afin de protéger les citoyens.

[154] La Quadrature du Net, « Le Conseil d'Etat sauve la reconnaissance faciale du fichier TAJ », 3 mai 2022, https://www.laquadrature.net/2022/05/03/le-conseil-detat-sauve-la-reconnaissance-faciale-du-fichier-taj/

1 – La réaffirmation du monopole des États membres en matière d'identité numérique publique

45. La souveraineté des États membres passe par leurs pouvoirs régaliens sur l'identité numérique de leurs ressortissants. A ce titre, il leur faut conserver leur monopole. L'identité numérique régalienne a en effet pour particularité d'exprimer l'appartenance à un pays, à une nation, compte-tenu de ses spécificités propres. A cet effet, l'identité numérique régalienne doit surpasser toute autre identité, qu'elle soit européenne ou privée.

    Par ailleurs, les États membres doivent avoir recours soit à des moyens étatiques internes (ressources internes : agents, moyens de stockages), soit à des entreprises nationales ou européennes, n'ayant pas de partenariats avec les géants du numérique ou toute autre entreprise extérieure à l'UE. L'identité numérique régalienne, constituant un domaine très sensible, autant pour la souveraineté des États, que pour les citoyens concernant leur vie privée et leurs libertés, toutes les mesures de sécurité et d'indépendance doivent être, à ce titre, adoptées. Bien qu'il soit fait mention régulièrement à la supériorité technique des géants du numérique concernant les outils techniques, les autorités publiques doivent privilégier leurs entreprises nationales et européennes pour inciter celles-ci à investir dans la recherche et l'innovation leur permettant de devenir *leaders* techniques et opérationnels. Il en va du soutien des entreprises nationales et européennes, de leur pérennité, de leur positionnement concurrentiel au niveau mondial. Au surplus, des études doivent être envisagées concernant les niveaux techniques de l'ensemble des entreprises concernées, permettant d'établir des comparatifs aux fins de mieux mesurer l'effectivité des affirmations concernant la supériorité technique de certaines grandes entreprises. Tout l'enjeu est de donner aux États membres les moyens de mesurer de manière effective leur véritable impact pour être à même de réagir efficacement, d'inciter les entreprises à investir dans ce domaine, d'engager des partenariats avec elles pour les hisser à des niveaux techniques supérieurs qui soient compétitifs. Cette stratégie, opérée en Chine, qui s'est avérée fructueuse dans le domaine du numérique, pourrait être transposée à l'échelle de l'Union européenne et des États membres.

2 – Le pouvoir contenu mais solide de l'Union européenne en matière d'interopérabilité des identités numériques publiques des États membres

46. Alors que l'Union européenne tende actuellement à prendre de plus en plus d'essor dans le domaine du numérique par son implication toujours plus forte par divers projets de règlements en préparation, son intervention doit rester

limitée à l'interopérabilité des identités numériques publiques des États membres lors de la révision du règlement eIDAS. La référence à l'identité numérique européenne est susceptible de constituer un risque pour la souveraineté des États membres si elle vient concurrencer les identités numériques étatiques. Par conséquent, il paraît indispensable que des discussions soient engagées au niveau des États membres et de l'Union européenne pour circonscrire strictement leurs pouvoirs respectifs à l'égard de l'identité numérique. Cette délimitation est importante puisqu'elle permettra aussi de consolider le socle des éléments communs permettant la liberté de circulation et de commerce entre les États membres, ce qui constitue un élément majeur permettant d'asseoir la souveraineté européenne.

3 – L'encadrement normatif nécessaire des identités numériques privées

47. Au-delà même de la confirmation du monopole des États membres à l'égard de leurs identités numériques régaliennes, différentes règles, venant encadrer les identités numériques privées, doivent être prévues pour plusieurs raisons. La première est la protection des ressortissants puisque les éléments de l'identité numérique peuvent avoir des effets directs sur leur vie privée et leurs libertés. La seconde est que certaines entreprises, particulièrement les géants du numériques, prennent une ampleur telle dans le domaine du numérique, que ce soit par les données personnelles qu'ils possèdent déjà, par leurs outils et par leur puissance économique, qu'il importe de les circonscrire dans leurs actions en matière d'identité numérique. Il en va de la souveraineté européenne et de celle des États membres, ainsi que du jeu de la libre concurrence pour toutes les entreprises en lien avec l'identité numérique. Celles-ci peuvent en effet être remises en cause par les situations de monopoles de la part des GAFAM, ce qui renvoie à des risques majeurs de dépendances et de pouvoirs d'influences, ainsi que de manipulation à l'égard des ressortissants européens. Les États membres et l'Union européenne doivent par conséquent rester vigilants lors de leurs interventions normatives, sur les actions puissantes de *lobbying* des grandes entreprises. Ceci suppose des contrôles renforcés et, le cas échéant, des sanctions dissuasives. Les CNIL européennes ont un rôle essentiel à jouer.

48. Des règles communes au niveau de l'Union européenne nécessitent d'être envisagées en parallèle de celles relatives à l'interopérabilité. Elles pourraient soit renvoyer aux dispositions déjà existantes du RGPD concernant la protection des données personnelles, soit prévoir des contraintes complémentaires directement associées à la protection de l'identité numérique des ressortissants européens (stockage, transmission à des pays tiers).

C – La mise en place d'une gouvernance solide et efficace de l'identité numérique dans un écosystème global

49. Une identité numérique régalienne forte des États membres passe par une gouvernance à la hauteur des enjeux majeurs qu'elle représente : souveraineté de chaque État, contrôles des ressortissants par les autorités étatiques, gestion administrative efficace et sécurisée. Il en va de la confiance des citoyens à l'égard de l'identité numérique étatique. Pour ce faire, une gouvernance transparente s'avère essentielle. Cette nécessité, rappelée avec force par le rapport portant sur « L'identité numérique » déposé le 8 juillet 2020 par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis[155], impose que les citoyens disposent d'informations précises et régulières concernant la gestion de l'identité numérique : les personnes responsables (agents publics concernés, délimitation de leurs pouvoirs, de leurs accès aux données personnelles et à l'identité numérique), les moyens mis à contribution (stockage, gestion de moyens de supports). Cette information doit être déployée par les sites internet officiels des ministères concernés, ainsi qu'à d'autres niveaux, plus de proximité, permettant un accès plus aisé (site des mairies exposant non seulement les formalités de constitution de la carte d'identité, du passeport, mais aussi celles portant sur l'identité numérique régalienne, sites de portefeuilles d'identités numériques). Outre cette information publique, les autorités publiques concernées (Ministère, agents) devraient aussi remettre un rapport annuel de leurs activités au Parlement, rendu public auprès des citoyens sur les sites précédemment envisagés. Là encore, des dispositifs de contrôles et des sanctions dissuasives devraient accompagner les obligations envisagées par les acteurs concernés par la gouvernance de l'identité numérique publique. Par ailleurs, en cas de recours à des prestataires et fournisseurs extérieurs, des cahiers des charges stricts devraient être élaborés, de même que les appels d'offres qui devraient être mis en œuvre de manière transparente. Une fois retenus, les interventions de ces acteurs devraient être fréquemment évaluées, autant par le biais de certifications régulières, que par des contrôleurs indépendants.

50. La gouvernance des moyens de l'identité numérique devrait par ailleurs être appréhendée dans un écosystème global intégrant à la fois les contraintes environnementales présentes et futures, mais aussi sécuritaires. Dans ce dernier cas, les États membres devraient prévoir des dispositifs européens de stockages hautement sécurisés, en recourant exclusivement à des moyens publics de stockages ou, le cas échéant, à des moyens privés, à condition que

[155] Assemblée nationale Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique » a été déposé le par Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis, https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information

les entreprises soient nationales ou européennes et qu'elles n'aient pas de partenariat avec les entreprises hors UE. Ce choix est d'autant plus crucial pour éviter tout risque de dépendance de quelque manière que ce soit (matières premières, énergie), ou de blocages en cas de conflits.

D – Le déploiement de la recherche et de l'innovation concernant les moyens d'identité numérique

51. Compte-tenu des transformations techniques continues du numérique, les États membres devraient envisager des dispositifs permettant de renforcer les moyens de la recherche et de l'innovation associés à l'identité numérique. Des appels à projet pourraient être envisagés autant au niveau de l'Union européenne, que des États membres. Il en va de la solidité des identités numériques régaliennes, mais aussi de la consolidation de la souveraineté des États membres et de l'Union européenne qui doivent être en mesure d'envisager des dispositifs techniques solides, ergonomiques et sécurisés. La recherche constitue une priorité d'autant plus justifiée en raison des incidences de l'ordinateur quantique qui pourraient remettre en cause les codes d'accès et du déploiement majeur des cyberattaques constituant des risques majeurs pour les identités numériques régaliennes.

E – Le renforcement des moyens sécuritaires face aux problèmes de cybersécurité

52. Plus que jamais, la cybersécurité devient un enjeu majeur de l'identité numérique régalienne, mais aussi privée dans la mesure où elle concerne directement les données sensibles des citoyens affectant directement leur vie privée et leurs libertés. L'importance des cyberattaques de ces dernières années met en exergue l'attrait de ces données par les cyberpirates, qui peuvent les revendre sur le *darknet,* ou encore procéder à des rançonnages auprès des intéressés (services publics responsables des identités numériques régaliennes, entreprises et citoyens). Outre des actions directes destinées à inciter à la prévention (1), se pose la question de l'opportunité de la centralisation des données (2).

1 – L'importance d'actions collectives concertées en matière de prévention

53. L'Union européenne et les États membres ont intérêt à intervenir activement par des actions collectives concertées en matière d'information, de formation, d'incitations, voire même d'obligations pour les activités les plus à risques telles que, par exemple, les moyens de stockages, d'accès, d'utilisation des données

sensibles. Il peut en être ainsi concernant les mises à jour régulières des systèmes informatiques, les sauvegardes indépendantes, les cyberscores ou encore les référentiels de sécurité. Des bonnes pratiques de sécurité peuvent aussi être envisagées, de même que des certifications, labélisations par les organismes accrédités, contrôlés régulièrement par les États membres.

2 – Des réflexions à mener sur les risques de centralisation des données sensibles

54. Paradoxalement, alors même que l'identité numérique nécessite un regroupement des données sensibles personnelles, elle devient, par le biais de la centralisation, un risque majeur en matière de piratage potentiel. Dans cette perspective, des recherches doivent être menées sur les risques d'une telle centralisation, complétées par d'autres, plus axées sur les moyens alternatifs permettant d'y remédier. Par exemple, pourraient être envisagés des dispositifs de traçabilité par la *blockchain*, ce qui permettrait non seulement d'agir contre les risques de cyber-piratage, mais aussi, le cas échéant, de constituer des preuves de premier plan en cas de mise en œuvre des responsabilités des acteurs en lien avec l'identité numérique, qu'il s'agisse des autorités ou agents étatiques concernés, ou encore, le cas échéant, des citoyens n'ayant pas pris toutes les précautions élémentaires en matière de sécurisation des données.

F– La mise en place de contrôles renforcés

55. Les données sensibles des citoyens, composantes de l'identité numérique, étant du ressort du RGPD, il convient d'inciter le comité européen de protection des données, ainsi que les CNIL européennes au niveau des États membres à opérer des contrôles renforcés, autant pour les systèmes numériques publics, que pour ceux relevant de la sphère privée. Les États membres pourraient aussi prévoir des dispositifs complémentaires de contrôles adaptés au profil de chacun des acteurs concernés. Des sanctions dissuasives devraient aussi être envisagées en cas de non-respect des dispositifs de protection liés aux identités numériques. Il pourrait aussi être fait appel à l'ANSSI au niveau national ou aux autorités similaires des États membres aux fins de contrôler la fiabilité des systèmes utilisés, l'enjeu étant de détecter des failles de sécurité ou des vulnérabilités. En cas de dérives associées aux identités numériques, mettant en cause les libertés individuelles et la vie privée des citoyens par les autorités étatiques, l'action du Parlement pourrait aussi être envisagée. En vertu de l'article 24 de la Constitution, celui-ci a vocation à exercer une mission de contrôle à l'égard de l'action du gouvernement. Dans cette perspective, les décisions et les actions associées à l'identité numérique, entrant dans cette

sphère de contrôle, pourraient permettre d'assurer un contrepoids, à condition que l'indépendance même du Parlement à l'égard de l'exécutif puisse être assurée.

56. En complément de ces modalités de contrôles régaliennes, devraient aussi être mises en place des autorités de contrôles indépendants aux États par le biais d'organismes extérieurs constitués d'experts et de citoyens. L'enjeu serait de mettre des gardes fous destinés à limiter tout accès des autorités publiques sur les identités numériques régaliennes. Ce contrôle extérieur, au titre de contrepouvoirs, pourrait être d'autant plus justifié compte-tenu de l'émergence croissante de moyens d'identifications numériques complémentaires tels que la reconnaissance faciale et les QR codes, de plus en plus utilisés, lesquels pourraient faire l'objet de dérives telles que le crédit social ou encore des risques de manipulations de personnes individuelles ou de masses. Dans ce sens, Mesdames Marietta Karamanli, Christine Hennion et Monsieur Jean-Michel Mis, à l'occasion de leur rapport « L'identité numérique »[156], préconisent une instance de contrôle et de supervision indépendante et multi parties prenantes associant des acteurs académiques, associatifs et administratifs. La proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 concernant l'établissement d'un cadre pour une identité numérique européenne préconise le contrôle direct des citoyens en ces termes : «*la sécurité et le contrôle assurés par le cadre européen relatif à une identité numérique devraient donner aux citoyens et aux résidents pleinement confiance dans le fait que le cadre européen relatif à une identité numérique donnera à chacun les moyens de contrôler qui a accès à son jumeau numérique et à quelles données exactement* »[157]. Dans le cas d'un contrôle effectué par les citoyens, celui-ci pourrait être justifié par l'article 34 de la Constitution en matière de droits civiques et de libertés fondamentales accordées à ceux-ci pour l'exercice des libertés publiques[158]. Des modalités d'information et de formation pourraient être envisagées pour que ceux-ci soient à même de procéder à une expertise citoyenne indépendante lors des processus d'évaluations. Ceux-ci devraient aussi faire l'objet d'accompagnement adéquat en cas de besoins d'éclaircissements ou d'approfondissement par différentes informations et explications complémentaires. A cet égard, les CNIL des États membres pourraient être amenées à intervenir, à condition de les doter de moyens

[156] Assemblée nationale Rapport d'information n°3190 du 8 juillet 2020 portant sur « L'identité numérique », préc.
[157] COM (2021) 281 final, la proposition du 3 juin 2021 en vue de modifier le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&from=EN
[158] Constitution, 4 octobre 1958, article 34, https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006527502/1958-10-05

complémentaires suffisants et adéquats et de garanties renforcées d'indépendance.

G – L'accentuation de la responsabilité des acteurs pour plus de protection des identités numériques

57. Les identités numériques étant par essence sensibles compte-tenu des données personnelles des citoyens, les États membres et l'Union européenne doivent non seulement responsabiliser les acteurs en termes de prévention, mais aussi les rendre responsables en cas d'incidents majeurs (1). La protection des données passe par des contrôles et des sanctions adaptés (2). Des mesures assurantielles doivent en outre être envisagées pour sécuriser et renforcer le dispositif de l'identité numérique (3).

1 – De la responsabilisation à la responsabilité des différents acteurs

58. Les données constituant les identités numériques régaliennes ou privées, étant par essence largement convoitées, en aval différentes mesures de précautions doivent être préconisées afin de responsabiliser les acteurs qu'ils soient des autorités publiques, des entreprises (prestataires, fournisseurs) ou des citoyens. Il leur faut par conséquent bénéficier d'informations et de formations adaptées et régulières les incitant à la vigilance et à l'action par des mesures diverses telles que les mises à jour, le changement de mots de passe, les stockages sur des supports extérieurs, etc.

59. En plus de ces actions de base tenant à la responsabilisation, le cas échéant, en cas de comportements risqués et fautifs des acteurs, ayant contribué à la fuite des données sensibles, à leur accessibilité ou à leur piratage aisé faute de précautions suffisantes, des responsabilités peuvent être envisagées. Les règles de droit commun, civiles, administratives ou encore pénales, sont alors applicables au niveau des États membres.

2 – Les couvertures assurantielles suffisantes

60. Dans la continuité des procédures de contrôles et des actions de responsabilités, les États membres devraient imposer des couvertures assurantielles minimales, au moins à la charge des prestataires extérieurs mais aussi à l'égard des différentes acteurs internes. D'importants préjudices pourraient en effet émerger, autant au niveau même des systèmes d'identités numériques mis en place par les autorités publiques, que de ceux associés aux données personnelles sensibles des ressortissants. Des préjudices

économiques majeurs pourraient aussi être envisagés pour les entreprises recourant aux dispositifs numériques régaliens si ceux-ci étaient, par exemple, piratés en raison de systèmes numériques insuffisamment sécurisés.

Au sujet de l'auteur :

Bénédicte Bévière-Boyer est maîtresse de conférences-HDR en droit privé à l'Université de Paris 8 et rattachée au Centre de recherches juridiques de Paris 8. Ses travaux de recherches portent sur le droit de la bioéthique, de l'éthique et du numérique. Elle a dirigé 8 ouvrages collectifs, écrit plus de 70 articles et 80 chroniques d'actualités. Elle organise régulièrement des colloques sur des thèmes d'actualité en lien avec plusieurs universités chinoises. Elle dirige le M2 droit de la santé, numérique et intelligence artificielle à l'Université de Paris 8.

Au sujet de la Chaire Digital, Gouvernance et Souveraineté :

La mission de la Chaire Digital, Gouvernance et Souveraineté de Sciences Po est de créer un écosystème unique pour rapprocher l'univers des entreprises technologiques du monde de la recherche académique, du monde politique, de la société civile, et des incubateurs de politiques publiques et de régulation du numérique. Ces relations nécessitent un écosystème de recherche, d'innovation et de formation qui soit pluridisciplinaire, international et en prise directe avec la sphère publique.

Portée par l'École d'Affaires Publiques, elle est résolument pluridisciplinaire pour penser de façon holistique les transformations économiques, juridiques, sociales ou encore institutionnelles entraînées par la transition numérique.

La Chaire Digital, Gouvernance et Souveraineté est dirigée par **Florence G'sell**, professeure de droit à l'Université de Lorraine, enseignante à l'École d'Affaires Publiques de Sciences Po. Elle bénéficie du précieux soutien de ses partenaires :