COMMISSION
EUROPÉENNE

Bruxelles, le 3.6.2021
COM(2021) 290 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur l'évaluation du règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)

{SEC(2021) 229 final} - {SWD(2021) 130 final}

1. INTRODUCTION

Le présent rapport expose les résultats de l'évaluation du règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (ci-après le «règlement eIDAS»)[1]. L'article 49 du règlement dispose que la Commission procède à un réexamen dudit règlement et évalue, en particulier, s'il convient d'en modifier le champ d'application ou des dispositions spécifiques, compte tenu de l'expérience acquise dans son application ainsi que de l'évolution des technologies, du marché et du contexte juridique[2], et qu'a besoin, ce rapport est accompagné de propositions législatives.

Le document de travail des services de la Commission qui accompagne le présent rapport contient des éléments factuels et des analyses plus détaillés à l'appui de ces conclusions.

1.1. Le cadre eIDAS

Avec l'adoption du règlement eIDAS en 2014, l'UE s'est posée en pionnière en introduisant un premier cadre transfrontalier applicable aux identités numériques et services de confiance, désormais reconnu et respecté à l'échelle mondiale. Ce règlement avait pour objectif de permettre à tous les citoyens de l'UE d'accéder aux services publics partout dans l'Union en utilisant les moyens d'identification électronique délivrés dans leur pays d'origine. Il visait à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant un socle commun pour des interactions électroniques sécurisées et intégrées entre les citoyens, les entreprises et les autorités publiques et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électronique dans l'UE. Il a en outre abrogé la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, qui couvrait essentiellement les seules signatures électroniques.

Conformément à sa base juridique, l'article 114 du traité sur le fonctionnement de l'Union européenne, le règlement avait pour objectif de lever les obstacles existants au fonctionnement du marché intérieur en promouvant le rapprochement des législations des États membres, en particulier la reconnaissance et l'acceptation mutuelles de l'identification électronique, de l'authentification, des signatures et des services de confiance connexes par-delà les frontières, lorsque cela est nécessaire pour l'accès aux procédures ou transactions électroniques et leur exécution.

Avant l'entrée en vigueur du règlement, l'UE ne possédait aucun cadre transfrontalier et intersectoriel complet pour des transactions électroniques sécurisées, fiables et aisées

---

[1] Règlement (UE) nº 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 (JO L 257 du 28.8.2014, p. 73), http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR.

[2] «La Commission procède à un réexamen de l'application du présent règlement et rend compte au Parlement européen et au Conseil, au plus tard le 1er juillet 2020. La Commission évalue, en particulier, s'il convient de modifier le champ d'application du présent règlement ou ses dispositions spécifiques, y compris l'article 6, l'article 7, point f) et les articles 34, 43, 44 et 45, compte tenu de l'expérience acquise dans l'application du présent règlement ainsi que de l'évolution des technologies, du marché et du contexte juridique.»

comprenant l'identification électronique, l'authentification et les services de confiance. La proposition de la Commission [COM(2012) 238 final] du 4 juin 2012 et l'analyse d'impact [SWD(2012) 135 final] l'accompagnant mettaient en évidence les quatre objectifs généraux suivants:

- garantir la mise en place d'un marché unique du numérique;
- promouvoir la mise en place de services publics transfrontaliers essentiels;
- stimuler et renforcer la concurrence au sein du marché unique; et
- améliorer la convivialité (pour les citoyens et les entreprises).

Bien que le règlement atteigne bon nombre de ses objectifs et qu'il soit devenu un élément fondamental pour faciliter le marché unique dans toute une série de secteurs (par exemple pour les services financiers et pour permettre l'accès aux données et leur réutilisation dans les procédures administratives), il possède certaines limites: l'absence d'obligation de notification des schémas nationaux d'identification électronique, le nombre limité d'attributs (éléments d'informations à caractère personnel) susceptibles d'être divulgués de manière fiable à des tiers, l'accent mis par le règlement sur le secteur public et l'absence d'incitations claires à l'emploi des identifications électroniques nationales par les parties privées. En outre, l'écosystème européen de l'identité électronique est réparti entre les différents cadres réglementaires nationaux, les niveaux de gouvernance numérique, la culture et les différents niveaux de confiance dans les institutions publiques.

1.2. Contexte

La fourniture de l'identité numérique connaît des changements fondamentaux. Des entités telles que les banques, les fournisseurs de services de communication électronique et les entreprises de services collectifs, dont certaines sont légalement tenues de collecter des attributs d'identification, capitalisent sur leurs procédures pour se poser en fournisseurs d'identités vérifiées. Des intermédiaires de l'internet, parmi lesquels les principales plateformes de médias sociaux et les grands navigateurs internet[3], font office de facto de gardiens des identités numériques et proposent des solutions dites BYOI (*«bring your own identity»*, «fournissez votre propre identité») permettant à leurs utilisateurs de s'authentifier sur des sites web et des services tiers au moyen de leur profil d'utilisateur. Cette facilité a toutefois un coût: la perte de contrôle des données à caractère personnel divulguées et l'absence de lien entre ces moyens d'identification électronique et une identité physique vérifiée, ce qui complique l'atténuation des risques de fraude et des menaces à la cybersécurité. Les citoyens de l'UE désirent, dans une large majorité, avoir accès à une identité numérique sécurisée qu'ils pourraient utiliser pour accéder aux services en ligne[4]. Enfin, bien qu'il existe de nombreuses divergences de vues sur l'avenir de l'identité numérique, le rôle clé des pouvoirs publics nationaux dans l'élaboration de tout écosystème d'identification numérique de grande envergure doit être dûment pris en considération.

Aujourd'hui, les utilisateurs attendent une expérience en ligne intégrée, des applications mobiles et des solutions d'authentification uniques pour accéder aux services en ligne des acteurs publics comme privés, couvrant tous les cas d'utilisation en matière d'identification,

[3] Par exemple, les utilisateurs de Facebook ou de Google peuvent utiliser leurs comptes pour se connecter au site Booking.com ou encore à EU Login:https://developers.facebook.com/docs/facebook-login/overview https://developers.google.com/identity/.

[4] Eurobaromètre spécial 503: attitudes à l'égard de l'impact de la numérisation sur la vie quotidienne, décembre 2019, voir: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228.

de l'identification par pseudonyme sur une plateforme en ligne à l'identification sécurisée à des services de santé ou de banque en ligne. Une identification en ligne sécurisée et l'échange d'identifiants et d'attributs sont de plus en plus importants à mesure que le nombre de services personnalisés et sensibles à l'identité augmente. La capacité d'identification numérique deviendra un facteur important d'inclusion sociale et la fourniture d'une identité numérique constituera un atout stratégique.

Dans son discours sur l'état de l'Union du 16 septembre 2020, la présidente de la Commission européenne a fait part de l'ambition de cette dernière de fournir une identité numérique sécurisée et fiable à tous les citoyens de l'UE: *«Nous, en Europe, nous voulons un socle de règles qui place l'humain au centre. […] Il portera notamment sur la maîtrise de nos données à caractère personnel, qui nous échappe trop souvent aujourd'hui. Chaque fois qu'une application ou un site web nous propose de créer une nouvelle identité numérique ou de nous connecter facilement via une grande plateforme, nous n'avons aucune idée de ce que deviennent nos données, en réalité. C'est pourquoi la Commission proposera bientôt une identité électronique européenne sécurisée. Une identité fiable, que tout citoyen pourra utiliser partout en Europe pour n'importe quel usage, comme payer ses impôts ou louer un vélo. Une technologie qui nous permettra de contrôler quelles données nous partageons et l'usage qui pourra en être fait.»*

Cette ambition de la Commission a été appuyée par le Conseil européen qui, dans ses conclusions des 1er et 2 octobre 2020, invite la Commission à présenter une proposition d'initiative sur l'identification numérique européenne d'ici la mi-2021.

Dans ses conclusions, le Conseil européen appelle à «*la mise en place, à l'échelle de l'UE, d'un cadre pour une identification électronique publique (e-ID) sécurisée, y compris des signatures numériques interopérables, qui permette aux personnes d'exercer un contrôle sur leur identité et leurs données en ligne et donne accès à des services numériques publics, privés et transfrontières. Il invite la Commission à présenter une proposition d'initiative sur l'identification numérique européenne d'ici la mi-2021*».

L'identification électronique permet aux citoyens et aux entreprises de prouver leur identité au moment d'accéder à des services en ligne. Les services de confiance, tels que les signatures électroniques, rendent les transactions en ligne plus sûres, plus pratiques et plus efficaces. Le règlement eIDAS est le seul cadre transfrontalier relatif à une identification électronique fiable des personnes physiques comme morales et aux services de confiance. Il permet la reconnaissance transfrontalière des identifications électroniques délivrées par les États aux fins de l'accès aux services publics, moyennant la notification des identifications électroniques concernées conformément aux dispositions du règlement. Ce dernier met également en place à l'échelle de l'UE un marché pour des services de confiance reconnus par-delà les frontières et disposant du même statut juridique que les processus traditionnels équivalents sur papier.

2. PRINCIPALES CONCLUSIONS DE L'EVALUATION

Les principales conclusions de l'évaluation, sur la base des critères d'évaluation, sont résumées sous les rubriques ci-après.

2.1. Efficacité

Les dispositions relatives à l'identité électronique ont débouché sur la création du réseau eIDAS, dont la mission est de permettre aux détenteurs d'un schéma d'identification

électronique notifié d'accéder aux services publics en ligne dans d'autres États membres de l'UE. Pour l'heure, seul un nombre limité de schémas d'identification électronique a été rendu interopérable à l'échelle de l'UE[5].
Le règlement eIDAS a permis d'établir une sécurité juridique en ce qui concerne la responsabilité, la charge de la preuve, l'effet juridique et les aspects internationaux des services de confiance. Toutefois, certaines difficultés persistent. La disponibilité et l'adoption des services de confiance ont crû dans l'UE depuis l'adoption du règlement eIDAS, mais il existe des différences entre les États membres et entre les différents services de confiance.

Malgré certains résultats, le plein potentiel du règlement n'a pas été atteint en ce qui concerne l'efficacité. Seul un nombre limité de schémas d'identification électronique a été notifié, ce qui restreint la part de la population de l'UE couverte par un tel schéma notifié (à 59 %). L'acceptation des identifications électroniques notifiées est limitée, car tous les nœuds eIDAS ne sont pas opérationnels, le nombre de services publics qui permettent cette notification ou sont connectés à l'infrastructure reste limité, et des erreurs techniques empêchent les utilisateurs de s'authentifier en pratique.

En ce qui concerne les services de confiance, l'objectif de neutralité technologique ancré dans le règlement a donné lieu à des interprétations diverses par les États membres des exigences de ce dernier, notamment en raison de l'absence d'adoption d'actes d'exécution complémentaires. S'il est impossible de conclure que des conditions de concurrence équitables ont été instaurées à l'échelle de l'UE, le règlement eIDAS a néanmoins permis la mise en place d'un cadre solide qui peut être complété par des normes et exigences nécessaires pour réduire l'actuelle fragmentation du marché et pallier les divergences d'interprétation par les organes de contrôle et les organismes d'évaluation de la conformité, ainsi que d'une coopération renforcée entre les organes de contrôle.

2.2. Efficience

Il ressort de l'évaluation de référence que les coûts quantifiables excèdent pour l'heure les bénéfices. Dans le domaine de l'identification électronique, cela s'explique par la lenteur de l'adoption et l'absence de concrétisation des avantages escomptés.

Les principaux groupes de parties prenantes pour lesquelles le volet «identification électronique» du règlement eIDAS a généré des coûts et des bénéfices sont les autorités nationales, les opérateurs de nœuds eIDAS, les fournisseurs d'identification électronique et les prestataires de services. En ce qui concerne les services de confiance, il s'agit des organes d'accréditation, des organismes d'évaluation de la conformité et des organes de contrôle, ainsi que des prestataires de services de confiance qualifiés et non qualifiés.

Pour les parties prenantes particulières, une grande partie des bénéfices sont des bénéfices escomptés (bénéfices futurs) et sont, par conséquent, difficilement quantifiables. Les coûts récurrents de gouvernance dans le domaine des services de confiance sont limités et principalement liés à la mise en conformité. Pour les parties prenantes particulières, une grande partie des bénéfices sont purement hypothétiques à ce stade (bénéfices futurs) et difficilement quantifiables. Pour les prestataires de services de confiance, les bénéfices

[5] Depuis l'entrée en vigueur du volet du règlement consacré à l'identification électronique en septembre 2017, 14 États membres ont notifié au moins un schéma; quatre en ont notifié plusieurs. Au total, 19 schémas d'identification électronique ont été notifiés à ce jour: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

prennent la forme de recettes tirées de la fourniture de services de confiance dans d'autres pays de l'UE et d'un élargissement de leur part de marché.

2.3. Pertinence

L'écosystème de l'identification électronique a profondément changé depuis l'adoption du règlement eIDAS; les fournisseurs privés de moyens d'identification y occupent une place de plus en plus importante. Étant donné la croissance des opérations numériques, tous les citoyens de l'UE devraient avoir accès à une identité numérique interopérable et sécurisée, ce qui n'est pas encore le cas aujourd'hui. Les objectifs du cadre juridique eIDAS restent pertinents pour répondre à la problématique de départ, en particulier la nécessité de réduire la fragmentation du marché en garantissant l'interopérabilité transfrontalière et intersectorielle des services de confiance par l'adoption de normes communes. Tant le champ d'application actuel du règlement eIDAS que l'accent placé par ce dernier sur les schémas d'identification électronique notifiés par les États membres de l'UE et sur l'accès aux services publics en ligne semblent trop limités.

Une série d'obstacles majeurs à l'adoption du cadre par les utilisateurs et les prestataires de services du secteur privé ont empêché la pleine exploitation du potentiel du cadre réglementaire. Malgré l'inclusion de références aux solutions eIDAS dans plusieurs actes législatifs sectoriels de l'UE, le règlement eIDAS n'a pas encore répondu aux besoins de certains secteurs (parmi lesquels les secteurs de l'éducation, bancaire, des voyages et de l'aviation). Pour ces secteurs, le cadre actuel pèche entre autres par l'absence d'attributs spécifiques par domaine.

La principale tension réside dans la capacité du cadre eIDAS à rester en phase avec les dernières évolutions technologiques dans le domaine des services de confiance. L'extension de la liste des services de confiance, notamment par l'introduction d'un service d'archivage électronique, d'un service de confiance à l'appui des identifiants d'identité portables et d'un service de confiance pour les registres électroniques, permettrait de répondre à une série de cas d'utilisation et donnerait aux citoyens et aux entreprises la possibilité de prouver leur identité ou attributs/caractéristiques de manière numérique, sans avoir à présenter de documents physiques.

2.4. Cohérence

Il ressort de l'évaluation que le volet du règlement relatif à l'identification électronique repose sur un système généralement cohérent de reconnaissance mutuelle des moyens d'identification électronique basé sur la notification et l'examen par les pairs. Le cadre relatif aux services de confiance prévoit quant à lui un système de contrôle cohérent pour ces services. Toutefois, certaines difficultés ont été recensées et entachent la cohérence interne du règlement.

En ce qui concerne l'identification électronique, le système de notification et d'examen par les pairs prévu dans le cadre eIDAS visait à donner naissance à une interprétation commune du niveau de garantie fournie par un schéma d'identification électronique, mais l'évaluation de la mise en œuvre pratique montre que ce n'est pas toujours le cas. En dépit de la neutralité technologique et de la souplesse prônées par le cadre, il n'existe encore aucune lecture commune de ce qui constitue un niveau de garantie substantiel et élevé. L'accent placé sur les services publics contraste avec la possibilité pour l'utilisateur de limiter les données transmises au minimum nécessaire pour s'identifier à un service donné; en effet, le jeu de

données minimal est toujours transmis pour permettre l'identification de la personne. La mise en œuvre de l'actuel système eIDAS ne permet pas à l'utilisateur de faciliter l'application des principes du RGPD en matière de minimisation des données et de respect de la vie privée par défaut en contrôlant les données qu'il entend partager et avec qui.

Les règles relatives à l'évaluation des prestataires de services de confiance au regard des exigences fonctionnelles du règlement applicables à l'octroi du statut de «service de confiance qualifié» affichent certaines faiblesses. En effet, le rôle des organismes d'évaluation de la conformité n'est pas suffisamment détaillé en ce qui concerne leurs obligations et responsabilités, ainsi que leur niveau de compétence. Certaines dispositions laissent aux États membres le soin de reconnaître ou non certaines méthodes d'identification (la vérification biométrique, par exemple) à l'échelle nationale, ce qui entrave l'égalité réglementaire et crée une incertitude.

2.5. Valeur ajoutée de l'UE

Le règlement eIDAS a incité les États membres à déployer des solutions nationales d'identification électronique; toutefois, la valeur ajoutée de ce cadre a été fortement limitée en raison de sa faible couverture et de son adoption et son utilisation limitées. Concernant les services de confiance, le règlement a fourni un cadre juridique commun applicable à leur utilisation, ce qui a entraîné une réduction de la fragmentation du marché et une hausse de leur adoption. Les services de confiance permettent aux administrations publiques de se moderniser, de convertir leurs services au numérique et de délivrer des justificatifs par voie numérique avec, à la clé, une réduction de la charge administrative.

En ce qui concerne la partie relative à l'identification électronique, les besoins qui justifiaient l'adoption du règlement à l'époque restent d'actualité et l'abrogation de ce dernier entraînerait une fragmentation et aurait des effets délétères sur d'autres domaines législatifs reposant sur le cadre eIDAS. Il serait possible d'accroître la valeur ajoutée européenne du cadre réglementaire en y apportant certaines adaptations (par exemple en facilitant l'utilisation par le secteur privé des identifications électroniques publiques de confiance et en définissant un cadre pour l'échange de certains attributs et identifiants fournis par les secteurs public et privé). Quant aux services de confiance, certains obstacles issus d'interprétations nationales et/ou de législations nationales divergentes persistent et limitent leur adoption.

3. REVISION DU CADRE EIDAS

Le règlement eIDAS joue un rôle fondamental de facilitation du marché unique dans différents secteurs [par exemple: dans le secteur bancaire pour fournir certaines données d'identité requises pour faciliter le respect des règles de lutte contre le blanchiment d'argent[6]; la directive sur les services de paiement (DSP2)[7], qui s'appuie sur les services de confiance eIDAS, tels que les sceaux électroniques et les certificats d'authentification de sites web qualifiés pour attester l'authenticité des sites web des prestataires de services de paiement tiers; et les identifications électroniques fondées sur le règlement eIDAS qui sont une condition préalable à l'échange transfrontière de certificats administratifs et sont essentielles à

[6] Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) nº 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

[7] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE, 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE.

la bonne mise en œuvre et au bon fonctionnement du principe «une fois pour toutes» à compter de 2023[8]]. Le cadre relatif aux services de confiance bénéficie d'une reconnaissance internationale et constitue la base d'un projet de dispositions[9], qui devrait devenir un modèle de loi des Nations unies sur les services de confiance dans le commerce électronique en 2021; il forme également le socle des négociations actuellement menées à l'OMC au sujet du commerce électronique[10].

Toutefois, de nombreux changements ont été observés depuis l'adoption du cadre eIDAS en 2014. Celui-ci se fonde sur des systèmes nationaux d'identification électronique qui suivent des normes diverses. Par ailleurs, il se concentre sur un segment relativement restreint des besoins des citoyens et des entreprises en matière d'identification électronique, à savoir l'accès transfrontalier sécurisé aux services publics. Ces services concernent surtout les 3 % de la population de l'UE[11] qui résident dans un État membre de l'UE différent de celui dans lequel ils sont nés.

Depuis lors, la numérisation de toutes les fonctions de la société s'est considérablement accrue, en particulier depuis l'apparition de la pandémie de COVID-19, qui a eu un effet très marqué sur la vitesse de la numérisation. En conséquence, la fourniture de services tant publics que privés devient de plus en plus numérique. Les citoyens et les entreprises attendent un haut niveau de sécurité et de simplicité d'utilisation dans toutes leurs activités en ligne, telles que la présentation de leur déclaration fiscale, l'inscription dans une université étrangère, l'ouverture d'un compte bancaire à distance ou l'introduction à distance d'une demande de prêt, la location d'une voiture, la création d'une entreprise dans un autre État membre, l'authentification pour les paiements en ligne, la participation à un appel d'offres en ligne, etc.

Il en découle une très nette augmentation de la demande de moyens d'identification et d'authentification en ligne, ainsi que d'échange sécurisé d'informations en lien avec l'identité, les attributs ou les qualifications par voie numérique, le tout avec un niveau élevé de protection des données[12]. Cette hausse a entraîné un changement de paradigme, orienté vers des solutions avancées et pratiques capables d'intégrer une variété de données et certificats vérifiables en lien avec l'utilisateur. À ce jour, les moyens d'identification électronique et les services de confiance prévus par le cadre eIDAS ne permettent pas de répondre à cette demande, en raison des limites de ce dernier. Les moyens d'identification et d'authentification élaborés par le secteur privé en dehors du cadre eIDAS, quant à eux, n'y répondent que partiellement. S'ils offrent des services d'authentification de tiers conviviaux (comme l'utilisation d'un compte Facebook ou Google pour se connecter à différents services), ils sont fréquemment utilisés pour accéder à des services en ligne privés non réglementés qui n'exigent pas un niveau élevé de sécurité. Toutefois, ils ne sauraient offrir le même niveau de sécurité juridique et de protection des données et de la vie privée, principalement en raison du

---

8 À compter de 2023, le principe «une fois pour toutes» permettra aux administrations publiques de réutiliser et de partager de manière transparente et sûre les données et les documents déjà transmis par les citoyens [article 14 du règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, JO L 295 du 21.11.2018, p. 1].

9 https://undocs.org/en/A/CN.9/WG.IV/WP.167

10 Voir, par exemple, les documents de session du groupe de travail IV sur le commerce électronique de la CNUDCI, session du 6 au 9 avril 2021, https://uncitral.un.org/fr/working_groups/4/electronic_commerce

11. https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

12 En Italie, par exemple, le nombre d'utilisateurs du schéma d'identification public SPID (lancé en 2016) était d'environ cinq millions à la fin de l'année 2019. Aujourd'hui, on dénombre plus de 18 millions d'utilisateurs actifs (voir https://avanzamentodigitale.italia.it/it/progetto/spid), avec une augmentation constante d'environ un million d'utilisateurs par mois. Tandis qu'on dénombrait environ 55 millions d'utilisations du schéma SPID en 2019, 32,4 millions d'utilisations ont été recensées pour le seul mois de février 2021.

fait qu'ils échappent à un contrôle extérieur et ne peuvent fournir de lien vers une identification électronique sécurisée et fiable délivrée par les pouvoirs publics.

En février 2020, la Commission s'est engagée, dans le cadre de sa stratégie visant à façonner l'avenir numérique de l'Europe[13], à réviser le règlement eIDAS en vue d'en améliorer l'efficacité, d'étendre son application au secteur privé et de promouvoir une identité numérique fiable pour l'ensemble des citoyens et des entreprises de l'UE. L'apparition de la pandémie de COVID-19 a mis en évidence le caractère urgent de cette révision. La perturbation des services publics et privés classiques et la nécessité soudaine d'accéder et de recourir à des services publics et privés de tout type en ligne ont fait apparaître les limites du cadre eIDAS concernant les bénéfices escomptés pour les citoyens, les entreprises et les pouvoirs publics, six ans après son adoption. Un règlement eIDAS révisé et renforcé permettrait de répondre aux nouvelles exigences du marché et de la société en répondant aux besoins de solutions liées aux moyens publics d'identification électronique de confiance, mais également d'attributs et d'identifiants fournis par les secteurs public et privé, qui sont tous entièrement gérés par l'utilisateur et reconnus dans l'ensemble de l'UE pour accéder aux services tant publics que privés. Cela permettrait de soutenir de nombreux cadres réglementaires existants ou proposés et, de ce fait, de renforcer le marché unique de l'UE.

4. CONCLUSIONS

Dans l'ensemble, le règlement eIDAS a contribué à l'approfondissement du marché unique et a jeté les bases de la création d'un marché des services d'identification et de confiance dans l'UE, en appuyant le besoin sans cesse croissant de transactions numériques sécurisées. Néanmoins, dans un esprit prospectif, compte tenu de l'évolution des objectifs et des attentes des utilisateurs, le règlement eIDAS doit être rendu plus efficace, plus efficient, plus cohérent et plus pertinent, afin de répondre aux nouveaux objectifs stratégiques, aux attentes des utilisateurs et à la demande du marché, tout en tenant compte des dernières évolutions dans le domaine de la numérisation.

Le marché commence à évoluer vers un nouvel environnement dans lequel la priorité n'est plus la fourniture et l'utilisation d'identités numériques monolithiques, mais bien la fourniture et l'utilisation d'attributs spécifiques en lien avec ces identités. On observe une demande croissante de solutions d'identité électronique susceptibles d'apporter ces capacités, qui permettraient de gagner en efficacité et de garantir, dans toute l'UE, un niveau élevé de confiance dans les services des secteurs privé comme public pour lesquels il est nécessaire de pouvoir identifier et authentifier les utilisateurs avec un degré élevé de garantie.

En l'état, le règlement eIDAS n'est pas en mesure de répondre à ces nouvelles demandes du marché compte tenu de ses limites intrinsèques au secteur public, de la difficulté pour les prestataires privés de services en ligne de se connecter au système, de sa disponibilité insuffisante dans tous les États membres et de sa souplesse insuffisante pour répondre à des cas d'utilisation variés.

[13] Commission européenne, 2020, stratégie intitulée «Façonner l'avenir numérique de l'Europe».