# Les services de confiance depuis le règlement eIDAS et la loi du 21 juillet 2016

Jacquemin, Hervé

*Published in:*
Journal des Tribunaux

*Publication date:*
2017

*Document Version*
le PDF de l'éditeur

Bureau de dépôt : Louvain 1
Hebdomadaire, sauf juillet et août
ISSN 0021-812X
P301031

larcier

stradalex
Journal des tribunaux

http://jt.larcier.be
18 mars 2017 - 136e année
11 - N° 6681
Georges-Albert Dal, rédacteur en chef

## Sommaire

### Doctrine



### Jurisprudence



### Chronique





Doctrine

# Les services de confiance depuis le règlement eIDAS et la loi du 21 juillet 2016

Le règlement UE n° 910/2014 sur l'identification électronique et les services de confiance, applicable pour l'essentiel depuis le 1er juillet 2016, établit un nouveau cadre normatif en matière de signature, de cachet, d'horodatage et de recommandé électroniques. L'authentification de site internet est également visée. Ce règlement est complété par une loi du 21 juillet 2016 qui instaure un régime similaire pour l'archivage électronique. En outre, cette loi régule, notamment, le recommandé hybride et permet au cachet électronique de produire les effets d'une signature. La présente contribution analyse ce nouveau régime, en pointant ses forces et ses faiblesses.

## Introduction

**1. Risques et enjeux d'une dématérialisation croissante des transactions. —** Au sein des entreprises et des pouvoirs publics, la dématérialisation des échanges ou des étapes menant à la conclusion des contrats (des premiers stades de la négociation à leur archivage) est devenue un enjeu stratégique majeur. Elle permet en effet de simplifier les procédures, tout en diminuant les coûts de traitement et de conservation. Parallèlement, les utilisateurs sont généralement demandeurs, dès lors qu'ils comprennent difficilement qu'à l'ère du tout numérique, où leur smartphone leur permet de faire du shopping *online*, réserver leurs prochaines vacances, gérer leurs comptes bancaires, écouter de la musique ou partager tout type de contenu à travers des réseaux sociaux, il leur soit encore demandé, dans certains cas, d'imprimer et de renvoyer un exemplaire papier du contrat signé à la main ou de se présenter physiquement pour que leur identité soit contrôlée.

D'un point de vue strictement technique, il n'y a pas d'obstacle à l'établissement d'un document électronique, susceptible d'être daté, signé et transmis en ligne, avant d'être archivé électroniquement. Il faut toutefois être conscient que tous les procédés disponibles sur le marché ne se valent pas, en ce sens que les garanties offertes en termes d'authentification de l'identité, de préservation de l'intégrité du contenu, de réception effective par le destinataire ou de pérennité de la conservation, peuvent en pratique varier sensiblement. Parallèlement, les fraudes ou, plus largement, la cybercriminalité, sont indéniablement présentes dans l'environnement numérique : contrairement aux relations contractuelles nouées dans un contexte traditionnel, les parties n'ont pas nécessairement l'occasion de se rencontrer et d'être en présence physique l'une de l'autre. Aussi peut-on craindre des usurpations d'identité ou des tentatives de *phishing*, entre autres.

**2. Intervention législative pour garantir la sécurité juridique et gérer les risques. —** Conscient du potentiel de croissance économique offert par la digitalisation et de la nécessité d'instaurer un cadre normatif propice à l'instauration d'un climat de confiance, le législateur est intervenu très tôt — depuis maintenant 20 ans — en matière de signature électronique ou, de manière générale, pour lever les obstacles formels à la conclusion des contrats par voie électronique[1]. On vise les formalités principales (écrit, signature, exemplaires multiples, mentions à la main, etc.) et celles qui sont plus accessoires (datation, transmission par recommandé, conservation, etc.). Dans un cas comme dans l'autre, ces exigences formelles tendent à se multiplier, au point qu'un phénomène de renaissance du formalisme contractuel a pu être observé.

(1) Pour un panorama des initiatives légales ou réglementaires, en Belgique ou à l'étranger, avant le règlement eIDAS ou le Digital Act, voy. H. Jacquemin, « Principes applicables à tous les services de confiance et au document électronique », *L'identification électronique et les services de confiance puis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 102-104, nos 2-3.

Dans ce contexte, les parties prenantes veulent maîtriser — ou, à tout le moins, être en mesure d'évaluer — les risques susceptibles de résulter de la dématérialisation. Aussi doivent-elles savoir si, et à quelles conditions, les procédés utilisés dans l'environnement numérique auront les mêmes effets, sur le plan juridique, que les moyens correspondant dans l'environnement papier. C'est à ce prix qu'elles pourront s'assurer que leur activité économique est conforme aux règles applicables (et resteront à l'abri des sanctions civiles, pénales ou administratives prévues par les textes en vigueur).

Dans un environnement ouvert (où les parties ne se connaissent pas nécessairement), l'intervention d'un tiers, dit « de confiance » a paru requise pour lever certains obstacles formels. C'est le cas pour la signature électronique, le cachet, le recommandé et l'horodatage électroniques, ainsi que pour l'archivage électronique (mais dans une moindre mesure)[2]. Leur activité doit par conséquent être encadrée par le législateur, de sorte que les utilisateurs puissent s'adresser à eux en toute confiance.

**3. Règlement eIDAS. —** Quinze ans après la directive sur la signature électronique[3], constatant que le cadre normatif applicable en la matière demeurait très perfectible et qu'il restait de nombreuses incertitudes pour diverses formalités, sans doute accessoires, mais néanmoins cruciales en pratique (en matière d'horodatage ou de recommandé électroniques, par exemple), le législateur européen a remis l'ouvrage sur le métier.

Aussi la Commission européenne a-t-elle pris l'initiative et déposé une proposition de règlement en juin 2012[4]. Le texte a été adopté deux ans plus tard : il s'agit du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[5] (ci-après, « règlement eIDAS » ou « règlement »)[6].

L'objet du règlement eIDAS est double : « fixer les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre » et instaurer un cadre juridique pour les services de confiance et les documents électroniques[7]. Seul ce second volet retient notre attention dans la présente contribution[8].

L'article 2 du règlement pose deux limites à son domaine d'application. Le règlement ne « s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants »[9]. En outre, il « n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel »[10]. Par contre, le règlement ne limite pas son application aux hypothèses dans lesquelles les formalités seraient requises dans une perspective probatoire ou pour d'autres finalités, telles les exigences requises *ad validitatem*. Peu importe également que les services de confiance soient utilisés dans le secteur privé ou dans le secteur public, de manière transfrontalière ou purement nationale.

Sous la réserve des dispositions listées à l'article 52, § 2, le règlement est applicable depuis le 1er juillet 2016[11].

**4. Digital Act. —** Le règlement eIDAS ne fixe pas, de manière exhaustive, tous les aspects du cadre normatif applicable aux services de confiance, ce qui laisse une certaine marge de manœuvre aux États membres, opportunément exploitée par le législateur belge[12].

Ainsi a-t-il adopté une loi du 21 juillet 2016[13] — généralement qualifiée de « Digital Act » — en s'appuyant sur ses tentatives précédentes (mais, malheureusement, infructueuses)[14].

Cette loi introduit, dans le livre XII du Code de droit économique (sur le droit de l'économie électronique), un titre 2, intitulé « certaines règles relatives au cadre juridique pour les services de confiance[15] ». Il complète, à divers égards, le régime établi par le règlement eIDAS, en introduisant un régime spécifique pour l'archivage électronique, tout en précisant, de manière ponctuelle, divers éléments du cadre normatif applicable à la signature, au cachet, au recommandé et à l'horodatage électroniques. La loi du 21 juillet 2016 fixe les compétences de l'organe de contrôle dans la recherche et la constatation des infractions, tout en sanctionnant pénalement le non-respect des dispositions établies[16]. Enfin, et plus ponctuellement, la loi amende diverses dispositions normatives, dans le Code civil ou en droit du travail notamment[17].

D'un point de vue temporel, les dispositions de cette loi sont, sauf exception[18], entrées en vigueur le jour de sa publication au *Moniteur belge*, soit le 28 septembre 2016[19].

(2) Pour les autres formalités (document électronique, écrit ou mentions manuscrites), la sécurité juridique peut être garantie sans l'intervention d'un tiers de confiance, mais moyennant la consécration de principes directeurs, applicables par ailleurs aux autres services de confiance.
(3) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, *J.O.* L 13 du 19 janvier 2000.
(4) Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, 4 juin 2012, COM(2012) 238 final.
(5) *J.O.* L 257 du 28 août 2014.
(6) Pour une première analyse du règlement, voy. D. Gobert, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution ? », *R.D.T.I.*, 2014/56, pp. 27 et s. ; H. Jacquemin, « Preuve et services de confiance dans l'environnement numérique », *in Pas de droit sans technologie*, Bruxelles, Larcier, 2015, pp. 41 et s. ; H. Jacquemin (dir.), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, 425 p.
(7) Article 1er du règlement.
(8) À ce propos, voy. D. Gobert, « L'identification électronique », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 81 et s.
(9) Article 2, § 2, du règlement. Le considérant n° 21 du règlement donne l'exemple des « systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance [qui] ne devraient pas être soumis aux exigences du présent règlement », tout en précisant que « seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement ». Conformément au principe de la liberté contractuelle, les parties pourraient donc décider, conventionnellement, de reconnaître des effets juridiques à un procédé de signature électronique ou d'horodatage électronique qui ne satisfait pas aux conditions du règlement.
(10) Deux éléments doivent être distingués : l'exigence formelle en tant que telle, prescrite par un texte légal ou réglementaire (la signature requise en matière probatoire, conformément à l'article 1341 du Code civil), d'une part, l'effet juridique reconnu au procédé susceptible d'être mis en œuvre dans l'environnement numérique, d'autre part. Le règlement ne s'applique qu'au second aspect, laissant aux États membres le soin de déterminer quelles exigences formelles qui sont requises, leurs finalités et les sanctions susceptibles d'être prononcées en cas de non-respect.
(11) Des mesures transitoires sont établies à l'article 51, relativement aux certificats et dispositifs de signature électronique qui auraient été établis conformément à la directive 1999/93/CE (ou les lois de transposition).
(12) Sur cette marge de manœuvre, voy. les travaux préparatoires de la loi (*Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 1893/001, pp. 5 et s.) et D. Gobert, « Objectifs, champ d'application et principes généraux : trame de lecture du règlement », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 72 et s.
(13) Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, *M.B.*, 28 septembre 2016. Pour un premier commentaire, voy. D. Gobert, « La loi belge du 21 juillet 2016 mettant en œuvre le règlement européen eIDAS et le complétant avec des règles sur l'archivage électronique : analyse approfondie », octobre 2016, publié sur www.droit-technologie.org.
(14) Voy. en particulier la proposition de loi du 15 avril 2013 modifiant la législation en ce qui concerne l'instauration du droit de l'économie électronique, *Doc. parl.*, Chambre, sess. ord. 2012-2013, n° 2745/001. Voy. aussi l'amendement du gouvernement visant à compléter la proposition de loi portant insertion d'un titre 2, « Certaines règles relatives au cadre juridique pour les signatures électroniques, l'archivage électronique, le recommandé électronique, l'horodatage électronique et les services de certification », dans le livre XII du Code de droit économique, et portant insertion des définitions propres au titre 2 précité et des dispositions d'application de la loi propres au même titre, dans les livres I et XV du Code de droit économique, *Doc. parl.*, Chambre, sess. ord. 2012-2013, n° 2745/004.
(15) À noter que le domaine d'application des dispositions du titre 2 est limité par l'article XII.24, § 2, du C.D.E.
(16) Voy. les articles XV.26 et XV.123 du C.D.E.
(17) Voy. les articles 34 et s. de la loi du 21 juillet 2016.
(18) Voy. *infra*, n° 34.
(19) Arrêté royal du 14 septembre 2016 fixant l'entrée en vigueur de la

**5. Plan. —** Après un panorama des services de confiance régis par le nouveau cadre normatif (1), nous rappelons les principes directeurs devant guider toute démarche de dématérialisation (2), avant d'examiner le régime désormais applicable à ces services, qu'ils soient qualifiés ou non qualifiés (3).

## 1 Panorama des services de confiance

**6. Notions de « service de confiance » et de « prestataire de service de confiance ». —** Au sens du règlement eIDAS, le prestataire de services de confiance est « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié »[20]. Le prestataire de service de confiance qualifié est également défini[21]. Le service de confiance est quant à lui « un service électronique normalement fourni contre rémunération qui consiste :

» a. en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou

» b. en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou

» c. en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services »[22].

Le « service de confiance qualifié » est également défini par le règlement, mais de manière curieuse et, en tout état de cause, peu utile dans une perspective de qualification : il s'agit en effet du « service de confiance qui satisfait aux exigences du présent règlement »[23].

On examine successivement les différents services de confiance listés dans la définition, ainsi que le service d'archivage électronique, non régulé par le règlement, mais heureusement encadré par la loi belge.

**7. Signature et cachet électroniques. —** Au sens du règlement eIDAS, la signature électronique vise « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer »[24]. Le règlement eIDAS introduit la notion de cachet électronique, qu'il définit comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières »[25].

Qu'il s'agisse de la signature ou du cachet électronique, le règlement introduit trois types de procédés, construits sur le même modèle technique : la signature — ou le cachet — électronique (simple), la signature — ou le cachet — électronique avancé(e)[26] et la signature — ou le cachet électronique — qualifié(e)[27]. Chaque procédé est une déclinaison du précédent, soumis à des conditions complémentaires (et bénéficiant d'un régime spécifique). On regrette que le règlement ait maintenu un régime aussi complexe, qui exige d'articuler trois définitions et donc, trois procédés de signature ou de cachet électronique, d'autant que, pour la signature, il faut au moins ajouter un quatrième procédé dont les conditions sont établies à l'article 1322, alinéa 2, du Code civil. Cette manière de faire est d'autant plus contestable qu'à l'analyse, les effets juridiques de certains procédés sont assez réduits. Sans doute aurait-il pu faire l'économie de la signature et du cachet électronique avancé.

Plusieurs éléments distinguent cependant la signature du cachet. Le signataire[28] est une personne physique, quand le créateur du cachet est une personne morale. Les fonctions attendues du procédé mis en œuvre diffèrent également, en tout cas dans le règlement, puisque la signature électronique est utilisée pour signer ; le cachet quant à lui vise uniquement à garantir l'origine et l'intégrité des données. Il peut par exemple être utilisé pour démontrer qu'un document électronique — ou un bien numérique, tel un logiciel — a été établi par une personne morale et n'a pas subi de modification[29].

Des précisions doivent être apportées pour comprendre la référence à l'acte de « signer », d'une part, signaler qu'en droit belge, le cachet électronique peut également être utilisé à cette fin, d'autre part.

Le règlement eIDAS n'explicite pas l'acception de l'expression de « pour signer », ni les effets juridiques de la signature[30]. En droit privé belge, on admet généralement que les fonctions traditionnellement attendues de la signature manuscrite consistent à marquer l'adhésion du signataire au contenu de l'acte et à authentifier son identité[31]. Dans l'environnement numérique, il faut normalement se référer aux fonctions de la signature électronique telles que listées à l'article 1322, alinéa 2, du Code civil : l'imputabilité à une personne déterminée et le maintien de l'intégrité du contenu[32]. À la lumière des travaux pré-

loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, *M.B.*, 28 septembre 2016.

**(20)** Article 3, 19°, du règlement.

**(21)** Article 3, 20°, du règlement. Le règlement désigne ainsi « un prestataire de service de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut de qualifié ». Deux conditions, tenant à la nature du service fourni et à l'autorisation administrative dont le prestataire a fait l'objet, se dégagent ainsi de cette définition. Nous les examinerons par la suite (*infra*, n^os^ 17 et s.).

**(22)** Article 3, 16°, du règlement.

**(23)** Article 3, 17°, du règlement.

**(24)** Article 3, 10°, du règlement. Sur la signature électronique au sens du règlement, voy. B. Losdyck, « L'usage de signatures électroniques dans le cadre du règlement eIDAS », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 139 et s.

**(25)** Article 3, 25°, du règlement. Sur le cachet électronique au sens du règlement, voy. J.-B. Hubin, « Le cachet électronique des personnes morales », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 175 et s.

**(26)** La signature électronique avancée est « la signature électronique qui satisfait aux exigences énoncées à l'article 26 » (article 3, 11°, du règlement eIDAS). Plus précisément, cette disposition exige que la signature satisfasse aux exigences suivantes : « a) être liée au signataire de manière univoque ; b) permettre d'identifier le signataire ; c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ». Ces conditions renforcent les fonctions d'identification, d'authentification et de maintien de l'intégrité du contenu de l'acte. Suivant le même modèle, le cachet électronique est « un cachet électronique qui satisfait aux exigences énoncée à l'article 36 » (article 3, 26°, du règlement), cette disposition énonçant les mêmes conditions que celles figurant à l'article 26 pour la signature électronique avancée.

**(27)** La signature électronique qualifiée est « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique » (article 3, 12°, du règlement). Les notions de « dispositif de création de signature électronique qualifié » et de certificat qualifié de signature électronique » sont définis par le règlement (article 3, 15° et 23°). Le même modèle est suivi pour le cachet électronique qualifié (article 3, 27°, pour la définition et article 3, 30° et 32°, pour les notions auxquelles celle-ci fait référence).

**(28)** Autrement dit, la « personne physique qui crée une signature électronique » (article 3, 9°, du règlement).

**(29)** Voy. les considérants n^os^ 59 et 65 du règlement eIDAS.

**(30)** Sans doute n'a-t-il pas voulu s'immiscer dans une analyse susceptible de révéler des différences entre les États membres. Aussi renvoie-t-il au droit interne, pour déterminer ce que « signer » signifie. Voy. à ce sujet l'article 2, § 3, du règlement.

**(31)** Voy. H. Jacquemin, *Le formalisme contractuel - Mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, pp. 99 et s., n^os^ 59 et s. Cette dernière fonction est, du reste, la plus importante. À nos yeux, la fonction d'authentification est secondaire par rapport à celle-ci. L'authentification de l'origine n'est pas une fin en soi. On comprendrait d'ailleurs difficilement qu'il en soit autrement, eu égard à l'efficacité, assez réduite, du mécanisme : il n'est guère impossible de reproduire une signature manuscrite (en utilisant un calque, par exemple). En outre, la signature ne crée qu'une présomption réfragable, suivant laquelle elle émane de la personne qui s'en prétend l'auteur, et qu'il est possible de renverser. La fonction d'authentification ne doit être vue que comme une condition d'efficacité de la fonction d'adhésion : il s'agit d'un moyen entièrement dédié à la mise en œuvre de cette autre fonction. En effet, la signature ne peut manifester la volonté de son auteur de s'approprier le contenu de l'acte si ce n'est pas lui, mais un tiers, qui a accompli la formalité.

**(32)** Ces notions d'imputabilité et d'intégrité rappellent un attendu d'un arrêt de la Cour de cassation française du 2 décembre 1997, aux termes duquel « l'écrit [...] peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées » (Cass. fr., 2 décembre 1997, *D.*,

paratoires de la loi et des commentaires doctrinaux, on doit normalement considérer que la notion d'imputabilité couvre les fonctions traditionnellement reconnues à la signature manuscrite[33]. On peut regretter le manque de clarté de la formulation retenue (pourquoi ne pas mentionner clairement les deux fonctions et préférer une notion aussi vague et ambiguë que l'imputabilité ?) et l'ajout d'une fonction que la signature manuscrite ne permet pas d'atteindre, le maintien de l'intégrité du contenu (créant ainsi une discrimination difficilement justifiable entre la signature manuscrite et la signature électronique)[34]. Aussi plaidons-nous pour que le législateur belge amende l'article 1322, alinéa 2, du Code civil, et introduise une définition fonctionnelle de la signature (manuscrite et électronique) dans le Code civil, qui mentionne les deux fonctions traditionnellement reconnues à l'exigence, sans référence à l'intégrité[35].

D'après le règlement eIDAS, le cachet a pour seules fonctions de garantir l'origine et l'intégrité des données. Il ne peut donc pas servir à signer[36]. Le législateur belge a toutefois profité de la marge de manœuvre laissée par le règlement en vue de donner au cachet des effets juridiques similaires à ceux de la signature. Ainsi, conformément à l'article XII.25, § 3, du C.D.E., « sans préjudice des articles 1323 et suivants du Code civil et des dispositions légales et réglementaires concernant la représentation des personnes morales, un cachet électronique qualifié utilisé dans le cadre d'actes juridiques passés exclusivement par ou entre des personnes physiques et/ou morales domiciliées ou établies en Belgique est assimilé à la signature manuscrite de la personne physique qui représente la personne morale qui a créé ce cachet ». N'étant pas un être de chair et d'os, la personne morale agit par ses organes[37] ; concrètement, il s'agit de personnes physiques (ou d'autres personnes morales dont les organes sont des personnes physiques). Contrairement à la signature manuscrite, directement liée à son auteur[38], la signature électronique (ou le cachet électronique, qui mobilise la même technologie) constitue un procédé technique dépersonnalisé que rien n'empêche de lier à une personne morale. Aussi faut-il approuver le pas franchi par le législateur belge en permettant au cachet électronique d'avoir les mêmes effets « engageant » qu'une signature[39].

Enfin, on note encore que le législateur belge a repris la possibilité, déjà mentionnée dans la loi du 9 juillet 2001, consistant à matérialiser la signature électronique du titulaire du certificat. L'équivalent ainsi produit doit satisfaire aux conditions de la signature électronique avancée[40]. Un régime similaire est introduit pour le cachet (matérialisation possible par un équivalent satisfaisant aux exigences du cachet électronique avancé)[41].

**8. Horodatage électronique. —** On entend par horodatage électronique « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant »[42].

Le mécanisme est intéressant dans la mesure où il ne connaît pas, en tant que tel, d'équivalent dans l'environnement « papier ». Pourtant, nombreuses sont les hypothèses dans lesquelles il importe de fixer avec précision le moment auquel le contrat a été conclu ou, plus généralement, l'acte juridique posé[43][44]. Dans certains secteurs, la question est particulièrement sensible : on songe au droit des assurances, pour fixer précisément le point de départ de la couverture[45], ou au droit judiciaire, pour le respect des délais de procédure. Pour l'heure, dans l'environnement papier, on peut se fonder, en matière contractuelle, sur l'une des hypothèses visées à l'article 1328 du Code civil, qui donnent date certaine aux actes sous seing privé, ou établir un acte authentique. À défaut, la date de l'envoi recommandé peut être invoqué mais il constitue tout au plus une présomption de l'homme.

Deux fonctions sont ainsi requises du procédé d'horodatage électronique : indiquer la date et l'heure avec précision et garantir l'intégrité des données auxquelles se rapportent cette date et cette heure[46]. Pour l'instant, le procédé, même qualifié, ne peut toutefois pas être assimilé à une date certaine (ce que l'on regrette)[47].

Une distinction est faite entre l'horodatage électronique (simple) et l'horodatage électronique qualifié, qui doit satisfaire aux conditions de l'article 42[48]. Ce dernier doit apporter des garanties complémentaires en lien avec les deux fonctions précitées. L'article 42, § 1er, du règlement exige ainsi que soient satisfaites les exigences suivantes : « a) il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ; b) il est fondé sur une horloge exacte liée au temps universel coordonné ; et c) il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente ».

1998, p. 192, note D.R. Martin, *J.C.P.*, G., 1998, p. 1105, note L. Grynbaum). Soulignant ce rapprochement, voy. E. Montero, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique "fonctionnaliste" ? », *in Mélanges offerts à Marcel Fontaine*, Bruxelles, Larcier, 2003, p. 188, n° 8.

**(33)** Voy. le rapport fait au nom de la Commission de la justice par B. Somers, *Doc. parl.*, Chambre, sess. ord. 1999-2000 (lég. 50), n° 38/008, p. 30. En doctrine, voy. E. Montero, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *D.A. O.R.*, 2002, p. 16 ; E. Montero, *Les contrats de l'informatique et de l'internet*, tiré à part du *Rép. not.*, Bruxelles, Larcier, 2004, p. 247, n° 189 ; P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *in Le commerce électronique : un nouveau mode de contracter*, Liège, Éd. du Jeune barreau, 2001, p. 114 ; L. Guinotte, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, 2002, p. 558.

**(34)** Pour un regard critique sur la fonction d'intégrité, requise par l'article 1322, alinéa 2, du Code civil, voy. E. Montero, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, pp. 24-25 ; D. Mougenot, *La preuve*, tiré à part du *Rép. not.*, Bruxelles, Larcier, 2012, p. 194, n° 122-3.

**(35)** Ce faisant, il ménagerait le principe d'équivalence fonctionnelle et simplifierait les obligations des parties qui souhaiteraient utiliser un mécanisme de signature électronique (d'autant qu'à l'analyse, mais de manière critiquable, la jurisprudence belge néglige de vérifier si la fonction a effectivement été préservée. Voy. C.T. Bruxelles, 11 octobre 2013 et 14 février 2014, *R.D.T.I.*, 2014/56, p. 115 et la note de J.-B. Hubin, « Signature scannée : quand une technologie simple confronte le juriste à des questions complexes ». Dans l'arrêt du 11 octobre 2013, la cour du travail avait bien noté l'exigence du maintien de l'intégrité. Pourtant, dans l'arrêt du 14 février 2014 (la cour ayant posé des questions aux parties et ordonné une réouverture des débats), elle accorde des effets juridiques à une signature scannée sans vérifier que la fonction a effectivement été préservée.

**(36)** Il ne s'agit donc pas de la signature électronique d'une personne morale. On note que la loi du 9 juillet 2001 consacrait expressément la signature électronique des personnes morales, en son article 4, § 4. L'assimilation automatique des signatures électroniques avancées qui respectent les conditions établies par cette disposition s'appliquait en effet sans préjudice « qu'elle soit réalisée par une personne physique ou *morale* » (nous soulignons). Concrètement, la signature ne serait plus celle de la personne physique, intervenant au titre d'organe de la société, pour engager celle-ci, mais celle de la personne morale (même si, *de facto*, une personne physique devra *a priori* intervenir pour activer le logiciel de signature). Sur la signature électronique des personnes morales, voy. B. Vanbrabant, « La signature électronique des personnes morales », *in La preuve*, Liège, Formation permanente C.U.P., 2002, pp. 174 et s. Voy. aussi *Doc. parl.*, Chambre, sess. ord. 1999-2000, n° 322/001, pp. 15 et s.

**(37)** Article 61, § 1er, du Code des sociétés.

**(38)** C'est d'ailleurs la personnalisation du graphisme qui permet d'atteindre la fonction d'authentification de l'identité.

**(39)** Voy. à cet égard *Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 1893/001, pp. 16-17.

**(40)** Article XII.25, § 11, du C.D.E.

**(41)** Article XII.25, § 12, du C.D.E.

**(42)** Article 3, 33°, du règlement.

**(43)** Par exemple, pour déterminer la loi applicable, *ratione temporis*, s'assurer que les parties avaient la capacité juridique au moment de s'engager ou calculer un délai de prescription.

**(44)** Sur l'horodatage électronique, voy. M. Demoulin, « Aspects juridiques de l'horodatage des documents électroniques », *in Commerce électronique : de la théorie à la pratique*, Bruxelles, Bruylant, 2003, pp. 43 et s.

**(45)** Voy. en ce sens l'article 57, § 7, de la loi du 4 avril 2014 relative aux assurances, aux termes duquel, « dès leur réception, l'assureur procédera au datage systématique des propositions d'assurance, des polices présignées et des demandes d'assurance ».

**(46)** Voy. l'article 41, § 2, du règlement, qui énonce clairement ces fonctions et présume qu'elles sont remplies dans l'hypothèse de l'horodatage électronique qualifié.

**(47)** Voy. l'article XII.25, § 10, du C.D.E., qui énonce que, « sous réserve de l'application de l'article 1328 du Code civil, un prestataire de service d'horodatage électronique qualifié ou non qualifié ne peut à aucun moment laisser entendre, directement ou indirectement, que son service confère date certaine ». Le non-respect de cette exigence est puni d'une sanction pénale de niveau 5 (article XV.123 du C.D.E.). Les travaux préparatoires précisent que « la mention "sous réserve de l'application de l'article 1328 du Code civil" vise à laisser la porte ouverte au développement d'horodatages électroniques par des officiers publics aptes à conférer date certaine au sens de l'article 1328 » (*Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 1893/001, p. 24).

**(48)** Article 3, 34°, du règlement.

**9. Service d'envoi recommandé électronique. —** Le service d'envoi recommandé électronique est le « service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée »[49].

Le règlement eIDAS liste ainsi les fonctions attendues du service d'envoi recommandé électronique : preuve de l'envoi et de la réception des données et maintien de leur intégrité (puisqu'elles doivent être protégées des risques de perte, de vol ou de modification). On regrette à cet égard que les fonctions attendues du recommandé électronique ne correspondent pas parfaitement à celles du recommandé papier traditionnel et sont en réalité plus nombreuses[50].

Comme pour les précédents services de confiance, le législateur définit le service d'envoi recommandé électronique qualifié[51] et renvoie, à ce propos, aux exigences établies à l'article 44 du règlement, qui renforce les conditions à respecter.

L'instauration d'un cadre juridique pour le recommandé électronique était attendue : la législation fourmille en effet d'hypothèses dans lesquelles un envoi recommandé est requis.

Il est utile de noter que la loi du 21 juillet 2016 complète le règlement eIDAS en encadrant le recommandé hybride : le prestataire de services de confiance qualifié qui offre des services d'envoi recommandé électronique qualifié doit ainsi respecter les exigences de l'annexe II du livre XII. Concrètement, il s'agit de matérialiser, au format papier, un envoi recommandé initialement généré au format électronique, pour le mettre sous enveloppe, et l'expédier physiquement à travers le réseau classique.

**10. Certificat d'authentification de site internet. —** Le dernier service de confiance régi par le règlement eIDAS, quoique de manière partielle — est la délivrance de certificats d'authentification de site internet. Il s'agit de l'« attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré »[52]. L'objectif est clairement de lutter contre le *phishing* ou d'autres pratiques frauduleuses semblables.

Le règlement définit également le certificat qualifié d'authentification de site internet, qui doit être délivré par un prestataire de services de confiance qualifié et satisfaire aux conditions listées dans l'annexe IV.

**11. Service d'archivage électronique. —** Le législateur belge a heureusement pris le relais de son homologue européen pour encadrer le service d'archivage électronique[53]. On trouve de nombreuses dispositions légales ou réglementaires qui imposent expressément de conserver les données ou les documents pendant une période plus ou moins longue[54]. Par ailleurs, dans une perspective probatoire, il est recommandé de conserver ceux-ci au moins pendant la durée de délai de prescription applicable[55].

Le service d'archivage électronique est défini comme étant « service de confiance supplémentaire à ceux visés par l'article 3, § 16, du règlement 910/2014, qui consiste en la conservation de données électroniques ou la numérisation de documents papiers, et qui est fourni par un prestataire de services de confiance au sens de l'article 3, § 19, du règlement 910/2014 ou qui est exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale »[56].

L'archivage électronique vise non seulement la conservation des données générées dès l'origine au format électronique, mais également les données résultant d'une numérisation des documents « papier ». Sur le plan de la formulation, l'alternative entre « la conservation de données électroniques ou la numérisation de documents papiers » nous paraît toutefois maladroite puisque la numérisation (ou le scan) de documents papiers est leur conversion en données électroniques, opération qui constitue un préalable à leur conservation ultérieure au format électronique (mais qui se distingue de la conservation en tant que telle)[57].

On regrette aussi que la définition ne liste pas les fonctions que le procédé doit préserver dans l'environnement numérique : ces fonctions résultent néanmoins de la présomption établie à l'article XII.25, § 5, alinéa 2, qui exige que les données électroniques soient conservées de manière à les « préserver de toute modification, sous réserve des modifications relatives à leur support ou leur format électronique ». Ici aussi, on aurait espéré que l'accent soit davantage mis sur ce qui constitue le cœur du service d'archivage, à savoir une conservation qui s'inscrit dans la durée contractuellement convenue (généralement, à la lumière des exigences légales), et qui permet à l'utilisateur de récupérer les informations archivées sous un format lisible (c'est cette possibilité de consultation ultérieure des données archivées qui justifie que les données aient été conservées). La fonction consistant à empêcher les modifications est importante mais, d'après nous, plus accessoire.

Comme pour les autres services de confiance du règlement eIDAS, le service d'archivage électronique qualifié est également défini[58], et soumis à des conditions additionnelles de nature à garantir que les fonctions attendues du procédé sont atteintes avec un niveau renforcé de sécurité technique (et donc, juridique).

Il est intéressant de noter que, contrairement aux autres services de confiance, s'agissant de l'archivage électronique (qualifié ou non qualifié), il est expressément prévu qu'il peut être fourni par un prestataire de service de confiance ou « exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale ». Cette entité pourrait donc s'abstenir de faire appel à un tiers, en exploitant le service elle-même, en interne. Cette option doit être approuvée, d'autant que, comme on le verra, les conditions à remplir pour bénéficier du statut de qualifié — et, par conséquent, d'effets juridiques offrant un niveau élevé de sécurité juridique — sont moins sévères que pour les prestataires tiers (*infra*, n° 28).

En lien avec l'archivage se pose la question de la valeur des copies et de la possibilité de détruire l'original papier après numérisation. À cet égard, outre l'ajout d'un nouvel alinéa à l'article 1334 du Code civil, on aura égard à l'article XII.25, § 6, du C.D.E., qui dispose que « sous réserve de l'application d'exigences légales ou réglementaires particulières, une copie numérique effectuée à partir d'un document sur support papier est présumée en être une copie fidèle et durable lorsqu'elle

**(49)** Article 3, 36°, du règlement. On regrette à cet égard que, par souci de cohérence, le législateur belge n'ait pas modifié la définition de l'envoi recommandé figurant à l'article 131, 9°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques où il est défini comme « un service garantissant forfaitairement contre les risques de perte, vol ou détérioration et fournissant à l'expéditeur, le cas échéant à sa demande, une preuve de la date du dépôt de l'envoi postal et/ou de sa remise au destinataire ».
**(50)** Sur les fonctions du recommandé, voy. E. Montero, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées », *in Commerce électronique : de la théorie à la pratique*, coll. Cahier du CRID n° 23, Bruxelles, Bruylant, 2003, pp. 75 et s. Comp. D. Gobert, « Le règlement européen du 23 juillet 2014... », *op. cit.*, pp. 47-48, qui appuie cette solution.
**(51)** Article 3, 37°, du règlement.
**(52)** Article 3, 38°, du règlement.
**(53)** Sur ce thème, avant l'adoption du règlement eIDAS et du Digital Act, voy. M. Demoulin et D. Gobert, « L'archivage dans le commerce électronique : comment raviver la mémoire ? », *in Commerce électronique : de la théorie à la pratique*, Bruxelles, Larcier, 2003, pp. 101 et s. ; M. Demoulin (dir.), *L'archivage électronique et le droit*, Bruxelles, Larcier, 2012, 195 p. ; M. Demoulin, « De l'archivage électronique à la gouvernance informationnelle : quelle place pour le juriste ? », *in Let's go digital - Le juriste face au numérique/De digitale uitdaging van de jurist*, Bruxelles, Bruylant, 2015, pp. 199 et s. Pour une première analyse du projet de loi belge, en lien avec le règlement eIDAS, voy. O. Vanreck, « Service d'archivage électronique : le service de confiance délaissé par le règlement n° 910/2014 », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 215 et s.
**(54)** Voy. par exemple l'article 60 du Code T.V.A. (conservation de la facture), l'article 195 du Code des sociétés (conservation des livres et documents sociaux) ou l'article 1er, § 3, de l'A.R. du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre (conservation du dossier médical).
**(55)** En droit commun des obligations et des contrats, le délai est de dix ans (article 2262*bis* du Code civil).
**(56)** Article I.8, 17°, du C.D.E.
**(57)** Il eût été plus correct, d'après nous, de définir ce service comme le « service de confiance supplémentaire [...], qui consiste en la conservation de données électroniques, *résultant, le cas échéant,* de la numérisation de documents papiers ».
**(58)** Voy. l'article I.18, 18°, du C.D.E. : « service d'archivage électronique fourni par un prestataire de services de confiance qualifié au sens de l'article 3, § 20, du règlement 910/2014 se conformant aux dispositions du titre 2 et de l'annexe I du livre XII ou exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale et se conformant aux dispositions du même titre et de la même annexe, à l'exception des e), i), j) et k) ».

est réalisée et conservée au moyen d'un service d'archivage électronique qualifié. Dans ce cas, la destruction de l'original papier est autorisée, sous réserve de l'application des dispositions légales et réglementaires relatives à la préservation et à l'élimination des archives du secteur public, en particulier de l'article 5 de la loi du 24 juin 1955 relative aux archives ».

## 2 Principes directeurs

**12. Quatre principes directeurs. —** Au moment de lever les obstacles formels, plusieurs principes directeurs sont généralement consacrés — ou, à tout le moins, mis en œuvre — par le législateur : la liberté de ne pas recourir à l'électronique, le principe de non-discrimination, le principe d'équivalence fonctionnelle et la neutralité technologique.

Nous revenons sur chacun d'eux et examinons de quelle manière ils sont traités dans le règlement eIDAS[59] et la loi du 21 juillet 2016.

**13. Liberté de (ne pas) recourir à l'électronique. —** Conformément à l'article XII.25, § 1er, du C.D.E., « à défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique ». Dès lors qu'aucune disposition du règlement eIDAS — ni aucun considérant — ne s'oppose à un tel principe, le législateur belge était libre de l'introduire dans le Code de droit économique.

Le principe figurait déjà, en termes identiques, à l'article 4, § 1er, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, abrogée par la loi du 21 juillet 2016. Pour comprendre la portée et la signification du principe, on peut donc se référer aux travaux préparatoires de la loi du 9 juillet 2001[60] et aux commentaires doctrinaux qui avaient été rédigés à cet égard[61]. On retient principalement que l'autonomie de la volonté des parties doit prévaloir, et que rien ne les empêche de décider de recourir, ou pas, à l'électronique

**14. Principe de non-discrimination. —** Le règlement eIDAS applique expressément le principe de non-discrimination à la signature électronique[62], au cachet électronique[63], à l'horodatage électronique[64] et aux données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique[65], en interdisant notamment que l'effet juridique et la recevabilité comme preuve en justice leur soient refusés au seul motif qu'ils se présentent sous forme électronique ou que le service n'est pas qualifié. S'agissant du service d'archivage électronique, il est consacré par l'article XII.25, § 4, du C.D.E.[66]

Le règlement eIDAS applique également le principe de non-discrimination au document électronique, qui ne constitue pas un service de confiance en tant que tel, en énonçant que « l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique »[67].

L'interdiction de toute discrimination est double, en ce qu'elle s'applique, d'une part, au bénéfice d'un service de confiance qualifié (par rapport à un service non qualifié), d'autre part, au bénéfice d'un service de confiance — par définition de nature électronique — par rapport à un procédé correspondant dans l'environnement papier (une signature manuscrite par exemple). Cette double déclinaison du principe de non-discrimination ne repose pas sur le même objectif.

Dans le premier cas, le législateur intervient sur le marché des services de confiance qui, comme on le sait, peuvent être qualifiés et non qualifiés. Les services de confiances qualifiés sont soumis à des conditions très lourdes mais, en contrepartie, les effets qui leur sont attachés offrent un niveau de sécurité juridique plus élevé (*infra*, nos 17 et s.). Le législateur européen est néanmoins conscient que, suivant l'hypothèse concernée, il ne faut pas nécessairement disposer d'un service qualifié. Autrement dit, il existe un marché pour les services qualifiés et un marché pour les services non qualifiés. Aussi interdit-il que tout effet juridique leur soit refusé au seul motif que le service de confiance n'est pas qualifié. La liberté des parties de recourir à un service plutôt qu'à l'autre est ainsi préservée. On verra toutefois que le législateur belge met à mal cette liberté en imposant, sans justification raisonnable, de recourir à des services qualifiés dans de nombreuses hypothèses (*infra*, no 34).

Dans le second cas, c'est la dématérialisation des échanges, et le recours aux technologies de l'information et de la communication dans les transactions électroniques, que le législateur entend défendre. Le règlement eIDAS perdrait tout effet utile si, en cas de litige, la juridiction pouvait tout simplement refuser d'examiner le procédé (un procédé de signature électronique appliqué à un courriel, par exemple) au seul motif qu'il est électronique.

**15. Principe d'équivalence fonctionnelle. —** Dans le courant des années quatre-vingt, parallèlement aux progrès techniques, des auteurs ont rapidement cerné les enjeux juridiques posés par le développement de l'informatique et des technologies de l'information. Ils ont esquissé les premières solutions en la matière, essentiellement sous l'angle du droit de la preuve[68]. Si d'autres solutions ont également été proposées, la théorie des équivalents fonctionnels a progressivement pris corps, avant d'être consacrée, au niveau international, par la CNUDCI, dans sa loi type sur le commerce électronique[69] (1996). Les travaux de celle-ci ont inspiré le législateur européen, puis belge.

(59) À ce sujet, voy. H. Jacquemin, « Principes applicables à tous les services de confiance et au document électronique », *op. cit.*, pp. 110 et s.
(60) On note d'ailleurs que les travaux préparatoires de la loi du 21 juillet 2016 (*Doc. parl.*, Chambre, sess. ord. 2015-2016, no 1893/001, p. 15) renvoient explicitement à ceux de la loi du 9 juillet 2001 (en particulier, *Doc. parl.*, Sénat, sess. ord. 2000-2001, no 2-662/4, p. 5). À l'époque, lors des discussions parlementaires, le ministre a indiqué que « la disposition du paragraphe 1er ne concerne pas les relations entre particuliers mais bien les relations des particuliers avec les autorités. Il est évident que des personnes morales privées et des personnes physiques sont libres de prévoir que des actes juridiques peuvent avoir lieu entre elles par voie électronique ».
(61) D. Gobert, « Cadre juridique pour les signatures électroniques et les services de certification », *La preuve*, Liège, Formation permanente CUP, vol. 54, 2002, p. 109.
(62) Article 25, § 1er, du règlement.
(63) Article 35, § 1er, du règlement.
(64) Article 41, § 1er, du règlement.
(65) Article 43, § 1er, du règlement.
(66) D'un point de vue légistique, la formulation employée, suivant laquelle « l'effet juridique et la recevabilité d'un archivage électronique comme preuve en justice ne peuvent être refusés... » nous paraît critiquable : ce n'est pas le service d'archivage électronique en tant que tel qui est soumis au principe de non-discrimination mais les données électroniques conservées au moyen de celui-ci. Aussi la disposition aurait-elle dû être formulée comme suit : « l'effet juridique et la recevabilité *des données conservées au moyen d'un service* d'archivage électronique comme preuve en justice ne peuvent être refusés... ».
(67) Article 46 du règlement. Le document électronique est défini de manière large par le règlement eIDAS comme « tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel » (article 3, 35o, du règlement). La notion est plus large que l'écrit puisque le contenu peut également être sonore, visuel ou audiovisuel. Par contre, aucune indication n'est donnée relativement aux fonctions attendues de la formalité. La proposition de la Commission du 4 juin 2012 était nettement plus ambitieuse puisqu'elle indiquait les fonctions à respecter pour que le document électronique soit jugé équivalent au document imprimé.
(68) Voy. en ce sens les réflexions de B. Amory et Y. Poullet, « Le droit de la preuve face à l'informatique et à la télématique : approche de droit comparé », *D.I.T.*, 1985/5, pp. 11 et s. ; M. Fontaine, « La preuve des actes juridiques et les techniques nouvelles », *in La preuve*, actes du colloque organisé les 12 et 13 mars 1987 à l'U.C.L., pp. 1 et s. ; J. Larrieu, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? - Contribution à l'étude juridique des notions d'écriture et de signature », *Cahier Lamy droit de l'informatique*, 1988, H, pp. 8 et s. ; N. Verheyden-Jeanmart, *La preuve*, Bruxelles, Larcier, pp. 233-234, nos 492-493 ; Y. Poullet, « Les transactions commerciales et industrielles par voie électronique - De quelques réflexions autour du droit de la preuve », *in Le droit des affaires en évolution - Le juriste face à l'invasion informatique*, Bruxelles, Bruylant, 1996, pp. 39 et s. ; E. Davio, « Preuve et certification sur Internet », *R.D.C.*, 1997, pp. 660 et s. ; R. Steennot, « Juridische problemen in het kader van de elektronische handel », *R.D.C.*, 1999, pp. 671 et s.
(69) Comme indiqué dans le Guide pour son incorporation, « la loi type propose [...] une nouvelle approche, parfois désignée sous l'appellation "approche fondée sur l'équivalent fonctionnel", qui repose sur une analyse des objectifs et des fonctions de l'exigence traditionnelle de documents papier et vise à déterminer comment ces objectifs ou fonctions pourraient être assurés au moyen des techniques du commerce électronique » (*Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, New-York, Publ. des Nations unies, 1999, p. 21, no 16). À ce propos, voy. de E. Caprioli et R. Sorieul, « Le commerce international électronique : vers l'émergence de règles juridiques transnationales », *J.D.I.*, 2, 1997, p. 382. Sur ce principe, on consultera aussi M. Demoulin, *Droit du commerce électronique et équivalents fonctionnels - Théorie critique*, coll.

Ce principe part du constat que les procédés mis en œuvre dans l'environnement papier pour accomplir les formes prescrites ne peuvent être reproduits comme tels lorsque le contrat est conclu par voie électronique. Si l'on souhaite que des rapports contractuels puissent être noués par ce biais, il doit être possible d'identifier les procédés à mettre en œuvre dans l'environnement numérique. Suivant la théorie des équivalents fonctionnels, on ne définit pas une exigence de forme par référence à un procédé technique particulier (le support papier pour l'écrit, le graphisme personnel et manuscrit apposée directement sur le support pour la signature, etc.) mais à la lumière des fonctions qu'elle permet de remplir (garantir la lisibilité, la pérennité, voire l'intégrité de l'information, pour l'écrit, par exemple). Deux procédés accomplis respectivement dans l'environnement traditionnel (le support papier pour l'écrit, par exemple) et dans l'environnement numérique (un document au format pdf enregistré sur un CD-ROM pour l'écrit, par exemple) sont alors jugés *équivalents* s'ils permettent de remplir les *fonctions* minimales reconnues à la formalité (l'écrit, en l'occurrence). Cette équivalence entre les procédés signifie que, sur le plan juridique, ils ont les mêmes effets et sont interchangeables. Autrement dit, la formalité prescrite est valablement accomplie dans l'environnement numérique lorsque le procédé choisi permet d'atteindre les fonctions reconnues à l'exigence.

En droit belge, ce principe est consacré à l'article XII.15, § 1er, du Code de droit économique, aux termes duquel « toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées »[70].

Sans l'affirmer expressément, le règlement eIDAS applique le principe d'équivalence fonctionnelle aux principales formalités puisque, comme on l'a vu, les procédés susceptibles d'être utilisés sont définis à l'aune des fonctions attendues d'eux. Ces fonctions sont construites par référence au procédé correspondant dans l'environnement papier, en tout cas lorsqu'il existe[71], même s'il faut constater qu'à divers égards, l'équivalence fonctionnelle est loin d'être parfaite (voy. *supra*, nos 7 et s.).

**16. Principe de neutralité technologique. —** Le principe de neutralité technologique est à la base de toutes les interventions normatives en lien avec l'accomplissement des formes dans l'environnement numérique[72]. Suivant celui-ci, les dispositions normatives doivent rester neutres et ne pas désigner expressément une technologie déterminée : eu égard à la rapidité des progrès scientifiques et techniques, il est en effet hautement probable que cette technologie devienne à brève échéance totalement obsolète. Il faudrait dès lors modifier les textes normatifs continuellement, pour qu'ils correspondent aux standards techniques minimaux, de nature à maintenir le niveau de sécurité requis.

Le principe est consacré par les considérants nos 26 et 27 du règlement eIDAS : après avoir constaté que « vu la rapidité de l'évolution technologique, le présent règlement devrait consacrer une approche qui soit ouverte aux innovations », il est indiqué que « le présent règlement devrait être neutre du point de vue de la technologie. Les effets juridiques qu'il confère devraient pouvoir être obtenus par tout moyen technique, pour autant que les exigences posées par le présent règlement soient satisfaites ».

La consécration de ce principe doit assurément être approuvée, même s'il paraît clair — mais ce n'est pas contestable en soi — qu'en posant les conditions applicables notamment à la signature, le législateur avait en tête les procédés créés au moyen de la cryptographie asymétrique[73].

Les stipulations figurant dans le règlement formulent les exigences en termes de mesures à prendre et de fonctions à préserver. Le texte ne dit donc pas, par exemple, qu'il faut respecter la norme ISO unetelle ou recourir à la cryptographie asymétrique. Compétence est toutefois donnée à la Commission européenne d'établir, au moyen d'actes d'exécution, les numéros de référence de normes (techniques ou organisationnelles) à respecter[74]. Le règlement préserve ainsi le principe de neutralité technologique, tout en permettant au secteur de disposer d'informations claires quant aux exigences techniques auxquelles les prestataires sont soumis (et que la Commission veillera à actualiser si nécessaire). Le règlement prévoit d'ailleurs que le prestataire est présumé respecter les exigences que ses dispositions énoncent lorsque les normes en question sont respectées. En matière d'archivage électronique qualifié, compétence est donnée au Roi pour établir de telles normes, étant entendu que le prestataire qui les respecte est, dans ce cas, présumé satisfaire à tout ou partie des exigences du titre 2 du livre XII et de son annexe I[75].

## 3 Régime applicable aux prestataires et aux services de confiance (qualifiés et non qualifiés)

**17. *Summa divisio*. —** Le règlement établit une *summa divisio* entre, d'une part, les prestataires de services de confiance qualifiés et les services de confiance qualifiés, d'autre part, les prestataires de service de confiance non qualifiés et les services de confiance non qualifiés.

Après avoir examiné les exigences applicables aux prestataires et aux services qualifiés et non qualifiés (A), nous déterminons les effets respectifs qui en résultent (B), à l'aune desquels les utilisateurs peuvent faire le choix de recourir à l'un ou à l'autre (pour autant que le choix existe effectivement).

**18. Organe de contrôle. —** Pour s'assurer que les prestataires de services de confiance — spécialement les PSC qualifiés — sont dignes... de la confiance que le règlement eIDAS — et le C.D.E. — leur accorde, celui-ci impose la désignation d'un « organe de contrôle » par les États membres[76]. Son rôle est précisé par l'article 17 du règlement. En Belgique, cet organe de contrôle est créé au sein du S.P.F. Economie, P.M.E., Classes moyennes et Énergie[77].

Parmi d'autres, ils est tenu de réaliser des contrôles *a priori* et *a posteriori* des prestataires de services de confiance qualifiés (et des services de confiance qualifiés qu'ils fournissent). Si nécessaire, ils doivent également prendre des mesures de contrôle *a posteriori* à l'égard des prestataires de services de confiance non qualifiés (et des services qu'ils fournissent), s'ils sont informés que les dispositions du règlement seraient méconnues[78].

Le règlement pose aussi les bases d'une assistance mutuelle entre les organes de contrôle des États membres[79].

CRIDS, Bruxelles, Larcier, 2014.
**(70)** Le paragraphe 2 de cette disposition applique ensuite la théorie aux formalités rencontrées le plus souvent en pratique : l'écrit, la signature et la mention manuscrite. Encore faut-il que l'hypothèse soit couverte par l'article XII.15 (voy. notamment les exclusions figurant à l'article XII.16 du C.D.E.).
**(71)** Tel n'est pas le cas, par exemple, pour l'authentification de site internet ou l'horodatage électronique.
**(72)** Voy. le considérant no 8 de la directive sur la signature électronique ou la loi type de la CNUDCI de 2001 sur les signatures électroniques et le Guide pour son incorporation, New York, Publ. des Nations unies, 2002, p. 35, no 82.
**(73)** Sur ce point, voy. J.-N. Colin, « Du secret à la confiance... quelques éléments de cryptographie », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 7 et s.
**(74)** Voy. les articles 24, § 5 (exigences applicables aux Ps.c. qualifiés), 27, § 4 (signatures électroniques dans les services publics), 28, § 6 (certificats qualifiés de signature électronique), 29, § 2 (dispositifs de création de signature électronique qualifiés), 32, § 3 (validation des signatures électronique qualifiées), 33, § 2 (services de validation qualifié des signatures électroniques qualifiées), 34, § 2 (services de conservation qualifié des signature électroniques qualifiées), 37, § 4 (cachets électroniques dans les services publics), 38, § 6 (certificats qualifiés de cachet électronique), 42, § 2 (établissement du lien entre la date et l'heure et les données, et les horloges exactes, en matière d'horodatage électronique), 44, § 2 (processus d'envoi et de réception des données en matière de service d'envoi recommandé électronique) et 45, § 2 (certificats qualifiés d'authentification de sites internet).
**(75)** Article XII.28, § 3, du C.D.E.
**(76)** L'article 17, § 1er, du règlement exige en effet qu'ils désignent « un organe de contrôle établi sur leur territoire ou, d'un commun accord avec un autre État membre, un organe de contrôle établi dans cet autre État membre. Cet organe est chargé des tâches de contrôle dans l'État membre qui a procédé à la désignation. Les organes de contrôle sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour l'exercice de leurs tâches ».
**(77)** Voy. la définition figurant à l'article I.18, 16o, du C.D.E.
**(78)** Sur ce point, voy. aussi le considérant no 36 du règlement.
**(79)** Article 18 du règlement.

## A. Conditions applicables aux prestataires et services qualifiés et non qualifiés

### 1. Régime harmonisé pour tous les prestataires et services, qualifiés et non qualifiés

**19. Exigences en matière de sécurité. —** L'article 19, § 1er, du règlement impose aux prestataires qualifiés et aux prestataires non qualifiés de prendre « les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents ».

En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur le service fourni ou sur les données à caractère personnel qui y sont conservées, une obligation de notification pèse sur les prestataires, vis-à-vis de l'organe de contrôle[80] et, le cas échéant, des bénéficiaires des services de confiance concernés[81], conformément à l'article 19, § 2, du règlement. La notification doit intervenir dans les meilleurs délais. Pour la notification à l'organe de contrôle, le règlement impose un délai de 24 heures prenant cours à partir de leur connaissance par le prestataire de confiance. On ne négligera pas la charge (administrative et financière) que représente une telle obligation, particulièrement si le prestataire a plusieurs milliers (ou millions, pour des multinationales du secteur des télécoms, par exemple) de clients. Le cas échéant, il peut être requis d'informer les organes de contrôles d'autres États membres et l'ENISA, voire le public en général, si l'organe de contrôle décide qu'il est dans l'intérêt public de procéder à une telle divulgation[82].

**20. Données à caractère personnel et accessibilité aux personnes handicapées. —** L'article 5 du règlement, dont l'application ne se limite pas aux services de confiance, exige que les traitements de données à caractère personnel se fasse conformément à la directive 95/46/CE. Dès le 25 mai 2018, on appliquera le règlement général sur la protection de données[83]. En Belgique, en cas d'utilisation de la carte d'identité électronique, on sera particulièrement attentif aux exigences figurant dans la loi du 8 août 1983 organisant un registre national des personnes physiques, en particulier, à l'article 8, aux termes duquel « l'autorisation d'utiliser le numéro d'identification du Registre national est octroyée par le comité sectoriel du Registre national visé à l'article 15, aux autorités, aux organismes et aux personnes visés à l'article 5, alinéa 1er. Le comité sectoriel envoie dans les trente jours après sa décision une copie de celle-ci au ministre de l'Intérieur et au ministre de la Justice. (...) »[84].

L'article 15 du règlement prévoit que « dans la mesure du possible, les services de confiance fournis, ainsi que les produits destinés à un utilisateur final qui servent à fournir ces services, sont accessibles aux personnes handicapées ». En ce sens, le considérant no 29 indique que l'évaluation de la faisabilité doit notamment se faire à l'aune de considérations d'ordre technique et économique.

**21. Archivage électronique. —** En matière d'archivage électronique, l'article XII.27 du C.D.E. énonce qu'« un prestataire de service d'archivage électronique satisfait aux dispositions du règlement 910/2014 applicables au prestataire de services de confiance non qualifié ». L'objectif du législateur est manifestement de renvoyer aux exigences de sécurité de l'article 19 du règlement[85].

### 2. Régime différencié pour les prestataires et services de confiance qualifiés ou non qualifiés

**22. Exigences applicables aux prestataires et services de confiance non qualifiés. —** En ce qui concerne les prestataires et les services de confiance non qualifiés, les seules exigences auxquelles ils sont soumis, conformément au règlement eIDAS ou à la loi du 21 juillet 2016, figurent aux articles 5, 15 et 19 du règlement (*cfr supra*, nos 19-21). Il s'agit des conditions auxquelles sont également soumis les prestataires et les services de confiance qualifiés.

**23. Exigences applicables aux prestataires et services de confiance qualifiés. —** Quant aux prestataires et aux services de confiance qualifiés, ils doivent non seulement respecter les exigences figurant aux articles 5, 15 et 19 du règlement eIDAS (*cfr supra*, nos 19-21), mais également les conditions qui leur sont propres, au moment de lancer leur activité (*infra*, no 24), en cours d'exercice de celle-ci (*supra*, no 2), ainsi qu'au moment d'y mettre fin (*infra*, no 26), ou de dissoudre le contrat portant sur le service d'archivage (*infra*, no 27).

Le législateur belge établit par ailleurs des conditions spécifiques lorsqu'une personne exploite le service d'archivage électronique qualifié pour son propre compte (*infra*, no 28).

Pour garantir l'effectivité de la distinction mise en place entre les prestataires et les services qualifiés, d'une part, les prestataires et les services non qualifiés, d'autre part, le législateur belge interdit à tout prestataire de services de confiance de « laisser entendre, directement ou indirectement, qu'il offre un service de confiance qualifié s'il ne se conforme pas aux dispositions » du règlement eIDAS ou du Digital Act[86], sous peine d'une sanction pénale de niveau 5[87].

**24. Conditions pour lancer un service de confiance qualifié. —** Lorsqu'un prestataire de services de confiance veut fournir des services de confiance qualifiés et obtenir le statut de prestataire de service de confiance qualifié, il doit préalablement obtenir une autorisation de l'organe de contrôle. La procédure est décrite à l'article 21 du règlement. Elle s'applique également aux prestataires de service d'archivage électronique qualifiés[88].

Le régime est ainsi diamétralement opposé à celui qui prévalait sous l'empire de la directive de 1999 en matière de signature électronique puisqu'elle interdisait aux États membres de soumettre les prestataires de services de certification à un régime d'autorisation préalable[89]. Le système mis en place par le règlement offre davantage de garanties quant au prestataire même si on peut craindre que cette exigence ait un effet dissuasif. Conformément aux lois de transposition de la directive de 1999, les prestataires fournissant des services de signature électronique qualifiée étaient très rares. *A fortiori*, avec cette exigence additionnelle, on peut sérieusement douter qu'ils soient plus nombreux...

La notification soumise par le prestataire à l'organe de contrôle doit être accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité[90].

C'est principalement sur cette base que l'organe de contrôle vérifiera le respect des exigences du règlement et, en cas d'appréciation positive, leur accordera le statut de « qualifié » (normalement dans un délai de trois mois à compter de la notification[91]).

**(80)** Il peut aussi s'agir d'autres organes compétents (le règlement cite l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, autrement dit la Commission de protection de la vie privée, pour la Belgique).
**(81)** Cette exigence ne s'impose que « lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni ».
**(82)** Article 19, § 2, du règlement.
**(83)** 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.* L 119 du 4 mai 2016.
**(84)** Sur ce point, voy. E. Degrave et C. de Terwangne, « Règlement eIDAS et secteur public : la carte d'identité électronique belge : instrument d'une identité numérique européenne », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 361 et s.
**(85)** *Doc. parl.*, Chambre, sess. ord. 2015-2016, no 1893/001, pp. 24-25.
**(86)** Article XII.25, § 9, du C.D.E.
**(87)** Article XV.123 du C.D.E., qui sanctionne aussi « quiconque aura usurpé la qualité de prestataire de services de confiance qualifié sans être inscrit sur la liste de confiance visée à l'article 22 du règlement 910/2014 ».
**(88)** Article XII.28, § 1er, du C.D.E., renvoyant aux dispositions du règlement eIDAS applicables aux prestataires de services de confiance qualifiés.
**(89)** Article 3, § 1er, de la directive 1999/93/CE. Un régime volontaire d'accréditation pouvait toutefois être organisé (article 3, § 2, de la directive).
**(90)** La notion est définie l'article 3, 18o, du règlement.
**(91)** Le règlement autorise toutefois l'organe de contrôle à prolonger le délai pour autant qu'il informe le prestataire, en lui indiquant les raisons du retard et le délai nécessaire pour achever la mission.

Il est primordial que toutes les parties prenantes (les parties utilisatrices, les prestataires et les autorités publiques compétentes) sachent avec certitude qui sont les prestataires qualifiés. Aussi incombe-t-il aux États membres d'établir, de publier et de mettre à jour des listes de confiance[92]. De son côté, la Commission met à la disposition du public les informations permettant de consulter ces listes (et de connaître l'organisme chargé de les publier). Cette publication sur une liste de confiance est importante puisque les prestataires ne peuvent fournir des services dits « qualifiés » qu'à partir du moment où leur statut est indiqué sur celles-ci[93]. À cet instant, ils peuvent également utiliser le label de confiance de l'Union[94] et l'apposer, par exemple, sur leur site internet ou tout autre document promotionnel.

**25. Exigences applicables aux prestataires de services de confiance qualifiés (dans l'exercice de leur activité). —** L'article 24 du règlement liste les nombreuses exigences applicables, de manière générale, aux prestataires de services de confiance qualifiés.

Les prestataires qui délivrent des certificats qualifiés doivent vérifier l'identité et, éventuellement, les attributs de la personne physique ou morale à laquelle celui-ci est délivré[95]. Des règles encadrent également l'établissement et la mise à jour d'une base de données relative aux certificats, ainsi que la révocation éventuelle de ceux-ci (l'opération de révocation en tant que telle et l'information qui doit en être donnée).

Le règlement énumère aussi, au paragraphe 2 de l'article 24, diverses obligations tenant aux obligations d'information vis-à-vis de l'organe de contrôle (a) ou des parties utilisatrices (d), aux compétences de leur personnel et sous-traitants éventuels (b), aux ressources financières et aux assurances (c), à la fiabilité et à la sécurité des systèmes et produits mis en place (e à g), à l'archivage des informations pertinentes concernant les données délivrées et reçues (h), ou à la continuité de leurs activités, par la mise en place d'un plan actualisé d'arrêt (i).

Le règlement impose aux prestataires de services de confiance qualifiés de faire l'objet d'un audit dont les résultats doivent être transmis à l'organe de contrôle[96]. Il doit être réalisé tous les 24 mois, au frais du prestataire, par un organisme d'évaluation de conformité. Cet audit peut aussi être demandé par l'organisme de contrôle à tout moment[97]. L'organe de contrôle peut être amené à imposer au prestataire de corriger certains manquements aux exigences prévues par le règlement et, à défaut de réponse satisfaisante, la sanction peut aller jusqu'à priver le prestataire ou le service concerné du statut de « qualifié »[98].

En complément de ces exigences d'ordre général, il faut ajouter les conditions propres à certains services de confiance qualifiés.

En matière de signature (et de cachet), le règlement détermine les exigences relatives aux certificats qualifiés de signature (ou de cachet) électronique[99], aux dispositifs de création de signature électronique qualifiés (les exigences applicables à ceux-ci, la certification des dispositifs et la publication de ceux-ci)[100], ainsi qu'à la validation et la conservation des signatures (et des cachets) électroniques qualifiés[101]. Des conditions figurent également aux annexe I à III du règlement et aux articles XII.31 et suivants du C.D.E, concernant la révocation, la suspension et l'expiration des certificats qualifiés de signature électronique et de cachet électronique. On relève aussi les articles XII.34 et XII.35 qui ont trait à l'utilisation d'un service de validation qualifié, permettant à la partie utilisatrice de bénéficier d'une présomption.

Pour les services d'archivage électronique, il faut respecter les exigences de l'annexe I du livre XII du C.D.E.[102]

**26. Arrêt des activités d'un prestataire de services de confiance qualifié. —** Le règlement eIDAS reste malheureusement très vague sur la question — pourtant capitale en pratique — de l'arrêt, par un prestataire de services de confiance qualifié, de ses activités. On trouve uniquement l'obligation de sauvegarder les données et de disposer d'un plan actualisé d'arrêt des activités afin d'assurer la continuité des activités, ce qui doit être vérifié par l'organe de contrôle[103].

Conscient des conséquences potentiellement préjudiciables d'un tel arrêt, le législateur belge s'attache à compléter le cadre normatif en précisant « les conditions et modalités de mise en œuvre du plan d'arrêt des activités »[104]. L'intention est assurément louable, même si, d'après nous, le législateur belge aurait pu se montrer plus exigeant. On note aussi que ces règles ne s'appliquent qu'aux prestataires soumis à l'autorité de l'organe de contrôle, ce qui exclut les prestataires de services de confiance qualifiés soumis aux organes de contrôle des autres États membres et dont leurs services de confiance peuvent être utilisés par les consommateurs belges avec les mêmes effets juridiques, par application du principe de reconnaissance mutuelle (*infra*, n° 32).

L'article XII.36 du C.D.E. impose au prestataire de services de confiance qualifié qui offre un ou plusieurs services de confiance qualifiés, d'informer « l'Organe de contrôle dans un délai raisonnable de son intention de mettre fin à au moins une de ses activités ainsi que de toute action ou fait qui pourrait conduire à la cessation d'au moins une de ses activités. Dans ce cas, il doit tenter la reprise de celles-ci par un autre prestataire de services de confiance ». D'après nous, il eût été préférable que l'organe de contrôle soit informé sans délai et tenu au courant de l'état d'avancement des opérations de reprise éventuelle. Nous sommes également d'avis que les pouvoirs publics — ou une entité désignée par eux — devraient avoir l'obligation, à titre transitoire ou définitif, sauvegarder les données de manière à garantir le respect de l'obligation prévue à l'article 24, § 2, h), du règlement eIDAS (enregistrement et accessibilité des informations pertinentes concernant les données délivrées et reçues par le prestataire, notamment à de fins probatoires ou de continuité du service). Elle repose en effet sur le prestataire mais, s'il cesse ses activités, on peut craindre qu'elle ne soit pas suivie d'effets (spécialement en cas de cessation totale de ses activités).

L'article XII.36, alinéas 2 et suivants, envisage ensuite l'hypothèse dans laquelle la reprise des activités n'est pas possible[105]. Pour les activités consistant en la délivrance de certificats qualifiés de signature ou de cachet, le prestataire doit avertir leurs titulaires et révoquer les certificats dans les deux mois. S'agissant des services d'archivage, d'horodatage et de recommandé électronique, les utilisateurs doivent être informés sans délai[106] de la date d'arrêt du service. Dans tous les cas, le prestataire doit également informer la personne concernée des mesures prises pour satisfaire à l'obligation prévue à l'article 24, § 2, h), du règlement eIDAS. S'agissant de l'archivage, le prestataire doit aussi leur offrir « la possibilité de transférer les données dans les trois mois et sans frais supplémentaires vers un autre prestataire de services de confiance qualifié ou de se faire restituer les données conformément à l'article XII.38 ». Pour les services de recommandé, il est requis que les envois effectués avant cet arrêt des activités soient transmis à leur destinataire.

**(92)** Article 22 du règlement.
**(93)** Article 21, § 3, du règlement.
**(94)** Article 23 du règlement. Voy. le règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés, *J.O.* L 128 du 23 mai 2015, ainsi que la décision d'exécution (UE) 2015/1505 de la Commission du 8 septembre 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, § 5, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, *J.O.* L 235 du 9 septembre 2015.
**(95)** Article 24, § 1er, du règlement. Cette disposition indique par qui et comment cette vérification peut être faite, conformément au droit national. Sur ce thème, voy. aussi l'art. XII.26 du C.D.E. qui impose une obligation de collaboration du prestataire avec les autorités administratives ou judiciaires compétentes, lorsque le titulaire du certificat de signature électronique utilise un pseudonyme, ou au moment d'établir l'identité et les pouvoir de représentation de la personne physique qui fait pratiquement usage du cachet électronique qualifié (le non-respect de cette dernière obligation de collaboration, visée à l'article XII.26, alinéa 2, étant par ailleurs sanctionné pénalement par l'article XV.123 du C.D.E.).
**(96)** Article 20, § 1er, du règlement.
**(97)** Article 20, § 2, du règlement.
**(98)** Article 20, § 3, du règlement.
**(99)** Article 28 pour la signature et article 38 pour le cachet.
**(100)** Article 29-31 pour la signature et article 39 pour le cachet.
**(101)** Article 32-34 pour la signature et article 40 pour le cachet.
**(102)** Voy. l'article XII.28, § 1er, du C.D.E., qui renvoie à cette annexe I.
**(103)** Article 17, § 4, i), et article 24, § 2, h) et i), du règlement eIDAS.
**(104)** *Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 1893/001, pp. 28-29.
**(105)** *A priori*, l'obligation du prestataire reste peu contraignante puisqu'il doit seulement « tenter » la reprise. Il en résulte que l'impossibilité pourrait résulter de sa seule volonté (parce que, par exemple, les conditions financières proposées par le repreneur ne lui conviennent pas).
**(106)** À noter que cette obligation d'informer les personnes concernées doit être fournie sans délai pour les services d'archivage, de recommandé et d'horodatage, mais pas pour les certificats qualifiés de signature ou de cachet (ce qui est difficilement compréhensible).

Curieusement, une procédure différente est prévue lorsque l'arrêt des activités intervient pour des raisons indépendantes de la volonté du prestataire de services de confiance qualifié ou en cas de faillite. Dans cette hypothèse, il doit, d'une part, informer immédiatement l'organe de contrôle, d'autre part, « informe[r] les utilisateurs des mesures prises pour satisfaire à l'obligation visée à l'article 24, § 2, point h), du règlement 910/2014 et procède[r], le cas échéant, à la révocation des certificats qualifiés »[107]. Le motif des « raisons indépendantes de la volonté du prestataire » nous paraît très vague. À tout le moins, les conditions de la force majeure auraient pu être visées. On regrette aussi qu'aucune obligation, même de moyen, ne soit imposée au prestataire (voire au curateur, dans le cadre de la faillite), pour tenter la reprise des activités. De manière générale, une solution de « back up » offerte ou organisée par les pouvoirs publics n'aurait probablement pas été superflue, de sorte que les finalités probatoires et de continuité du service, visées à l'article 24, § 2, point h), du règlement, puissent effectivement être atteintes.

**27. Obligation de restitution des données lorsque le contrat relatif au service d'archivage électronique qualifié prend fin. —** En cas de dissolution du contrat relatif au service d'archivage électronique, pour quelque motif que ce soit, l'article XII.38 du C.D.E. interdit au prestataire qualifié d'opposer à l'utilisateur un quelconque droit de rétention des données et lui impose de demander, par envoi recommandé, le sort qui doit être réservé aux données qui avaient été confiées. On aurait pu espérer une formulation plus positive du droit à la portabilité ou à la restitution des données. Quant à l'exigence de l'envoi recommandé, elle nous paraît exagérément lourde en ce qu'elle est requise de manière systématique. Il eût été plus raisonnable de permettre à l'entreprise de prendre contact avec l'utilisateur par le canal habituel de communication (une adresse *e-mail* par exemple) et de passer au recommandé uniquement lorsque l'utilisateur n'y réserve pas de suite.

S'agissant des données à caractère personnel, cette exigence devra être articulée avec le droit à la portabilité des données consacré à l'article 20 du Règlement général sur la protection des données. Le cas échéant, il faudra aussi avoir égard, en matière de contenus numériques (comme l'archivage électronique), au droit à la récupération des contenus, figurant dans la proposition de directive sur certains aspects des contrats de fourniture de contenus numériques[108].

À la suite de l'interpellation du prestataire, l'utilisateur peut opter pour la restitution des données ou leur transfert vers un autre prestataire. Il incombe alors au prestataire de restituer « les données et, le cas échéant, les informations visées à l'article 24, § 2, point h), du règlement 910/2014 à l'utilisateur du service ou [de] les transf[érer] vers l'autre prestataire désigné dans un délai raisonnable et sous une forme lisible et exploitable convenue avec l'utilisateur du service ou avec le nouveau prestataire, en accord avec l'utilisateur du service »[109].

L'article XII.38, § 2, alinéa 2, du C.D.E. ajoute qu'« en l'absence de réponse de l'utilisateur dans les trois mois de la demande visée à l'alinéa 1er, le prestataire peut procéder à la destruction des données, sauf interdiction expresse d'une autorité judiciaire ou administrative compétente et sous réserve de l'application des dispositions légales et réglementaires relatives à la préservation et à l'élimination des archives du secteur public, en particulier de l'article 5 de la loi du 24 juin 1955 relative aux archives ».

De manière générale, on se demande encore pour quelle raison ces obligations (voire certaines d'entre elles seulement) s'appliquent uniquement au prestataire de services d'archivage électronique qualifié et pas à tout prestataire de services d'archivage, peu importe qu'il ait été qualifié ou pas. En tout état de cause, dans le règlement général de protection des données ou dans la proposition de directive sur les contrats de fourniture de contenus numérique, on ne trouve pas de telles distinctions.

**28. Conditions spécifiques pour exploiter un service d'archivage électronique qualifié pour son propre compte. —** En matière d'archivage électronique, le législateur belge a prévu que l'organisme du secteur public ou la personne physique ou morale souhaitant bénéficier d'un tel service pouvait faire appel à un tiers (autrement dit, à un prestataire de services de confiance qualifié ou non qualifié qui respecte les exigences précitées) ou le faire en interne, en exploitant le service pour son propre compte.

Dans ce dernier cas, et conformément à l'article XII.28, § 2, du C.D.E., cette entité est dispensée de respecter certaines exigences imposées à tout prestataire au moment de lancer son activité ou en cours d'exercice de celle-ci : pas d'audit tous les 24 mois (article 20, § 1er) ; pas d'autorisation préalable de la part de l'organe de contrôle avant de lancer l'activité (article 21) ; pas d'information de l'organe de contrôle de toute modification dans la fourniture des services et de l'intention éventuelle de cesser les activités (article 24, § 2, a) ; pas d'information à fournir à la personne désireuse d'utiliser le service (article 24, § 2, d) ; pas de plan actualisé d'arrêt d'activité afin d'assurer la continuité du service (article 24, § 2, i) ; pas de réponse à fournir à l'utilisateur suite à sa demande de restitution des données (annexe 1 du livre XII du C.D.E., point e) ; pas d'informations à fournir aux utilisateurs du service, avant la conclusion du contrat et en cours d'exercice de celui-ci (annexe 1 du livre XII du C.D.E., point i) ; pas d'obligation de faire preuve d'impartialité vis-à-vis des utilisateurs de son service et des tiers (annexe 1 du livre XII du C.D.E., point j) et pas d'obligation de disposer des moyens financiers suffisants (annexe 1 du livre XII du C.D.E., point k).

Si l'entité est dispensée d'obtenir une autorisation préalable, elle reste tenue de faire une notification à l'organe de contrôle, en lui communication des renseignements d'identification, ainsi qu'« un rapport d'évaluation, effectué à ses frais, par un organisme d'évaluation de la conformité, confirmant le respect des exigences du règlement 910/2014, du présent titre et de son annexe I »[110]. La loi impose alors à l'organe de contrôle de lui délivrer un récépissé dans les cinq jours ouvrables suivant la réception des informations, tout en lui donnant la possibilité, « s'il le juge utile notamment sur la base du rapport d'évaluation », de procéder à un contrôle[111].

## B. Effets de la qualification ou de la non-qualification

### 1. Présentation systématique des effets juridiques applicables aux services qualifiés et aux services non qualifiés

**29. Différences entre les services qualifiés et les services non qualifiés. —** On observe des différences importantes — et logiques — entre les effets attachés aux services de confiance qualifiés ou non qualifiés, en termes de clause d'assimilation ou de présomption (*infra*, nº 30), de responsabilité (*infra*, nº 31) et de reconnaissance internationale (*infra*, nº 32).

Les services de confiance non qualifiés bénéficient seulement de la clause de non-discrimination, qui interdit de leur refuser tout effet juridique ou, sur le plan probatoire, de les déclarer irrecevables sous prétexte qu'ils se présentent sous forme électronique ou qu'ils ne sont pas qualifiés (*supra*, nº 14).

**30. Clause d'assimilation ou présomption pour les services de confiance qualifiés. —** Les services de confiance qualifiés bénéficient d'un clause d'assimilation ou d'une présomption légale ayant pour effet de renverser la charge de la preuve.

Aux termes de l'article 25, § 2, du règlement, « l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite ». *A priori*, le juge ne dispose d'aucune marge d'appréciation et il doit assimiler le procédé à une signature manuscrite. D'après nous, il doit rester possible d'administrer la preuve contraire.

Pour d'autres services de confiance, le règlement présume — de manière réfragable — que les fonctions reconnues à la formalité (et expressément mentionnées) sont atteintes. Tel est le cas pour le cachet électronique qualifié[112] (présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électro-

(107) Article XII.37 du C.D.E.
(108) Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fournitures de contenus numériques, COM(2015) 634 final, article 13, § 2, c) et article 16, § 4, b) : « le fournisseur procure au consommateur les moyens techniques lui permettant de récupérer tout contenu fourni par ce dernier et toutes autres données produites ou générées par suite de l'utilisation du contenu numérique par le consommateur, dans la mesure où ces données ont été conservées par le fournisseur. Le consommateur a le droit de récupérer le contenu sans inconvénient majeur, dans un délai raisonnable et dans un format de données couramment utilisé ».
(109) Article XII.38, § 2, alinéa 3, du C.D.E.
(110) Article XII.28, § 2, du C.D.E.
(111) Article XII.28, § 2, du C.D.E.
(112) Article 35, § 2, du règlement.

nique qualifié est lié), l'horodatage électronique qualifié[113] (présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure), le service d'envoi recommandé électronique qualifié[114] (présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié) et, en droit belge, le service d'archivage électronique qualifié[115] (présomption que les données ont été conservées de manière à les préserver de toute modification, sous réserve des modifications relatives à leur support ou leur format électronique). Pour le cas plus particulier de l'authentification de site internet, aucune présomption n'est établie.

Curieusement, pour l'horodatage, le recommandé et l'archivage électroniques, le législateur belge double cette présomption d'une autre présomption, figurant cette fois dans le Code de droit économique, suivant laquelle « sous réserve de l'application d'exigences légales ou réglementaires particulières, lorsqu'une obligation de conservation des données ou des documents [ou une obligation de datation des données ou des documents, ou un recommandé], est imposée, de manière expresse ou tacite, par un texte légal ou réglementaire, cette obligation est présumée satisfaite par le recours à un service d'archivage électronique qualifié [ou d'horodatage électronique qualifié ou de recommandé électronique qualifié] »[116]. Cette présomption nous paraît inutile, dans la mesure où elle résulte déjà de la présomption suivant laquelle les fonctions sont atteintes par le recours à un service qualifié (si on présume que les fonctions sont atteintes, il faut nécessairement en conclure que l'exigence de datation, de recommandé ou d'archivage est satisfaite). Le législateur belge était pourtant conscient de l'existence d'une présomption réfragable dans le règlement pour le recommandé et l'horodatage mais, comme l'indiquent les travaux préparatoires, « dans un objectif de sécurité juridique, le présent projet complète ce principe et cette présomption réfragable par une présomption irréfragable »[117]. Le seul intérêt de ces clauses consisterait donc à affirmer le caractère irréfragable de la présomption. Si tel était l'objectif, pourquoi ne pas le dire clairement dans la disposition légale et se contenter d'une assertion, du reste très faiblement justifiée, dans les travaux préparatoires ? D'après nous, ce faisant, le législateur belge ajoute un effet que le règlement ne prévoyait pas, portant ainsi atteinte à l'objectif de fonctionnement du marché intérieur poursuivi par l'instrument européen. L'articulation du caractère réfragable et irréfragable des deux présomptions aboutit également à un régime contradictoire. D'après le règlement, on peut en effet démontrer que le procédé n'a pas permis de garantir le caractère exact de la date ou la bonne réception du recommandé (par exemple), puisque cette présomption est réfragable ; par contre, par application du droit belge, on doit présumer, sans preuve contraire possible que le même procédé satisfait l'obligation de datation ou de recommandé. S'agissant de l'archivage, il faut également articuler une présomption réfragable sur les fonctions[118] avec une présomption irréfragable sur l'obligation de conservation[119][120] : on peut donc démontrer que service d'archivage électronique qualifié n'a pas permis de préserver les données de toute modification (présomption réfragable sur les fonctions) ; par contre, et nonobstant cette preuve contraire, l'obligation de conservation sera présumée satisfaite par le recours à un service d'archivage électronique qualifié (sans qu'il soit possible de renverser la présomption). Il faudra donc considérer que l'obligation légale de conservation est respectée, alors même que la démonstration de l'atteinte à l'intégrité du contenu a été faite.

Qu'en est-il des services de confiance qui ne sont pas qualifiés (et qui ne bénéficient donc pas de la clause d'assimilation ou de la présomption) ?

Sous peine de méconnaître le principe de non-discrimination consacré par ailleurs (et qui interdit de priver d'effet juridique les services de confiance qui ne sont pas qualifiés), il faut admettre que les parties utilisatrices aient la possibilité de démontrer que la signature, le cachet, l'horodatage, le service d'envoi recommandé ou le service d'archivage respectent les fonctions reconnues à chaque procédé, de manière à convaincre le juge de leur donner des effets juridiques.

S'agissant de la signature, les États membres retrouvent sur ce point leur marge de manœuvre[121], puisque la définition figurant à l'article 3, 10°, du règlement eIDAS renvoie à la finalité de « signer », sans indiquer les fonctions attendues de la signature. Pour la signature électronique, c'est le rôle joué par l'article 1322, alinéa 2, du Code civil (sur ce point, voy. *supra*, n° 14).

S'agissant des autres services de confiance il n'était pas indispensable de compléter le cadre normatif dans la mesure où, contrairement à la signature, le règlement (ou le C.D.E., pour l'archivage électronique) veille à indiquer clairement les fonctions attendues de ces services.

On note encore que la signature électronique *avancée* et le cachet électronique *avancé* peuvent être reconnus, moyennant certaines conditions, si un État membre exige ce type de signature (le cas échéant qui repose sur un certificat qualifié) pour utiliser un service en ligne offert par un organisme du secteur public ou pour l'utiliser au nom de cet organisme[122]. *A fortiori*, dans ce cas, les signatures ou cachets électroniques présentant un niveau de sécurité plus élevé (tels que la signature ou le cachet électroniques qualifiés) se voient reconnaître les mêmes effets. Cette disposition tend à compliquer le régime mis en place (puisqu'il crée une autre catégorie de signature électronique) : le considérant n° 50 du règlement le justifie cependant par le fait que « les autorités compétentes dans les États membres utilisent actuellement différents formats de signature électronique avancée pour signer électroniquement leurs documents ».

**31. Responsabilité. —** Aux termes de l'article 13, § 1er, du règlement, « [...] les prestataires de service de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement ». Cette disposition s'applique également aux prestataires de services d'archivage électronique, qualifiés ou non qualifiés[123].

Le règlement instaure un régime probatoire plus favorable aux parties utilisatrices de services fournis par des prestataires de services de confiance qualifiés puisque, dans ce cas, le prestataire est présumé avoir agi intentionnellement ou par négligence[124]. Pour les autres prestataires, c'est le droit commun qui s'applique et il incombe à la victime de prouver que le prestataire a agi intentionnellement ou par négligence[125].

On note qu'il est permis aux prestataires de services de confiance de poser des limites à l'utilisation des services fournis (indiquer par exemple que le service de signature ou d'horodatage électronique n'est pas garanti pour des montants supérieurs à 1.000.000 EUR ou dans certaines matières — comme des paiements). Cette limite — et l'exonération limitative de responsabilité qui en découle — sera étroitement liées aux garanties obtenues par les prestataires auprès de leurs compagnies d'assurance (tenant compte des risques financiers qu'ils sont prêts à assumer)[126]. Encore faut-il, comme le rappelle l'article 13, § 2, du règlement, que les clients soient dûment informés, au préalable, de telles limites, et qu'elles puissent être reconnues par des tiers.

**32. Reconnaissance mutuelle au sein de l'Union. —** Parmi les objectifs du règlement figure le bon fonctionnement du marché intérieur. Il doit se traduire par une libre prestation des services de confiance sur le territoire de l'Union (dans le chef des prestataires qui les fournissent et des parties utilisatrices qui y recourent). Concrètement, il faut permettre à un client belge qui conclut un contrat avec une entreprise française d'utiliser un procédé d'horodatage électronique fourni par une entreprise finlandaise.

**(113)** Article 41, § 2, du règlement.
**(114)** Article 43, § 2, du règlement.
**(115)** Article XII.25, § 5, alinéa 2, du C.D.E.
**(116)** Article XII.25, § 5, alinéa 1er, article XII.25, § 7, alinéa 1er et article XII.25, § 8, alinéa 1er, du C.D.E.
**(117)** *Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 1893/001, p. 21 (pour le recommandé) et p. 22 (pour l'horodatage).
**(118)** Article XII.25, § 5, alinéa 2, du C.D.E.
**(119)** Article XII.25, § 5, alinéa 1er, du C.D.E.
**(120)** Sur le caractère réfragable ou irréfragable, voy. *Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 1893/001, p. 19.
**(121)** S'agissant de la signature, voy. le considérant n° 49 : « il appartient au droit national de définir l'effet juridique produit par les signatures électroniques, à l'exception de l'exigence prévue dans le présent règlement selon laquelle l'effet juridique d'une signature électronique qualifiée devrait être équivalent à celui d'une signature manuscrite ».
**(122)** Articles 27 et 37 du règlement.
**(123)** Article XII.29 du C.D.E.
**(124)** Article 13, § 1er, alinéa 3, du règlement.
**(125)** Article 13, § 1er, alinéa 2, du règlement.
**(126)** Sur ce point, voy. le considérant n° 37 du règlement.

En ce sens, le règlement consacre un principe de reconnaissance mutuelle de certains services de confiance qualifiés. Il énonce ainsi que « la signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les États membres »[127]. Des clauses similaires sont introduites pour les cachets électroniques qualifiés[128] et l'horodatage électronique qualifié[129]. Curieusement, rien n'est prévu pour le service d'envoi recommandé électronique qualifié ou la délivrance de certificats qualifiés d'authentification de sites internet.

Qu'en est-il des services de confiance non qualifiés ou des deux services de confiance qualifiés qui ne bénéficient pas de la clause de reconnaissance mutuelle ? Le principe de marché intérieur tel que consacré à l'article 4 du règlement leur est applicable. En son paragraphe 1er, cette disposition interdit en effet de restreindre « la fourniture de services de confiance, sur le territoire d'un État membre, par un prestataire établi dans un autre État membre, pour des raisons qui relèvent des domaines couverts par le présent règlement ». Quant au paragraphe 2, il autorise les services de confiance conformes au règlement à circuler librement au sein du marché intérieur.

Cette reconnaissance mutuelle ne s'applique pas au service d'archivage électronique, qui n'est pas harmonisé par le règlement : les dispositions introduites par la loi du 21 juillet 2016 ne s'appliquent en effet qu'aux prestataires établis en Belgique[130].

### 2. Critères à prendre en compte au moment d'opter pour le qualifié ou le non qualifié

**33. Analyse de risque. —** Comme on l'a vu, des conditions particulièrement rigoureuses doivent être observées par les prestataires s'ils veulent obtenir le statut de qualifié et lancer leur activité (*supra*, no 22). Parallèlement dans l'exercice même de leur activité, de nombreuses obligations leur sont imposées, en lien avec les services de confiance qu'ils délivrent (*infra*, nos 26 et s.). Il en résulte des contraintes techniques et organisationnelles importantes ainsi qu'une charge administrative et financière très lourde. Autrement dit, il est hautement probable qu'au sein des États membres, voire au niveau de l'Union, de tels prestataires soient finalement peu nombreux.

Le respect de ces conditions donne lieu à l'application d'un régime juridique plus favorable aux parties utilisatrices du service de confiance : les effets juridiques des services de confiance qualifiés leur permettent de bénéficier d'une clause d'assimilation ou d'une présomption légale (*supra*, no 30) ; le prestataire qualifié est présumé avoir agi intentionnellement ou par négligence (*supra*, no 31) ; les services qualifiés sont reconnus en tant que tels dans tous les États membres (*supra*, no 32)[131].

Au contraire, les services de confiance non qualifiés bénéficient d'effets juridiques soumis à l'aléa de la preuve (et aucune présomption ne peut être invoquée en termes de responsabilité). Le risque existe donc que la preuve ne puisse pas être apportée (même si, très clairement, et suivant le procédé utilisé, il peut fort bien ne pas se réaliser).

Tout dépend en définitive du risque que l'on est prêt à assumer, lorsque l'on recourt à un service de signature, de cachet, de recommandé, d'horodatage ou d'archivage électronique. Si l'enjeu financier — ou le risque en général — est faible, sans doute n'est-il pas requis de déployer l'artillerie lourde en surprotégeant l'opération : pour donner un exemple concret, on ne passe pas devant le notaire pour constater l'achat de quelques meubles de jardin entre particuliers (même si, sur le plan probatoire, la sécurité juridique est renforcée en recourant à l'acte authentique plutôt qu'à l'acte sous seing privé). Par contre, s'il s'agit d'un contrat portant sur plusieurs millions d'euros et que la date de signature est primordiale, on sera bien avisé de recourir à des services d'horodatage et de signature électroniques qualifiés.

**34. Obligation légale de recourir à un service de confiance qualifié. —** Il est important de noter que, dans un certain nombre d'hypothèses, le législateur belge s'est substitué à la volonté des parties (et à leur liberté d'opter pour un service qualifié ou un service non qualifié) pour leur imposer, sans choix possible, de recourir à un service de confiance qualifié.

En matière de recommandé, d'horodatage et d'archivage, il s'agit d'une obligation transversale générale. Aux termes de l'article XII.25, § 5, alinéa 3, « sous réserve de l'application d'exigences légales ou réglementaires particulières, lorsqu'une obligation de conservation de données ou de documents est imposée de manière expresse par un texte légal ou réglementaire, il est recouru à un service d'archivage électronique qualifié si l'utilisateur du service opte pour la voie électronique ». Des dispositions similaires existent pour l'obligation de datation des données ou des documents[132] et l'envoi recommandé[133].

On ne trouve pas d'obligation générale en matière de signature ou de cachet électronique. Pour ces formalités, le législateur est intervenu au cas par cas : ainsi en matière de crédit à la consommation, l'article VII.78 du C.D.E prévoit que le contrat est conclu par la signature manuscrite ou la signature électronique de toutes les parties contractantes. La signature électronique peut être une signature électronique qualifiée ou un cachet électronique qualifié[134], ou « autre signature électronique qui satisfait aux critères que le Roi peut fixer afin de garantir l'identité des parties, leur consentement sur le contenu du contrat de crédit et le maintien de l'intégrité de ce contrat »[135].

Dans certains cas, et moyennant une justification adéquate, on peut admettre que le législateur impose un service de confiance qualifié[136]. Il faut toutefois se garder de le généraliser sans analyse préalable, comme le fait, à tort selon nous, le législateur pour le recommandé, l'horodatage et l'archivage électronique. Les travaux préparatoires le justifient par un motif de sécurité juridique[137]. Un commentateur va plus loin, n'hésitant pas à affirmer, à tort selon nous, que, sans cette obligation, le système probatoire belge serait mis en péril, le principe d'équivalence fonctionnel méconnu, et des discriminations juridiques créées[138]. Nous ne partageons pas cette analyse. Il faut au contraire laisser aux parties la liberté de choix du service auquel elles veulent souscrire, et le choix corrélatif du risque qu'elles acceptent d'assumer, le cas échéant. C'est cette analyse de risque, et du libre choix des moyens de preuve, qui fonde le système probatoire, de droit supplétif, tel qu'il est mis en place en Belgique : les parties peuvent (mais ne doivent pas) opter pour l'acte authentique en lieu et place de l'acte sous seing privé, disposer d'un écrit signé qui respecte les conditions de l'article 1325 ou 1326 du Code civil, ou se satisfaire d'un commencement de preuve par écrit, etc. Pourquoi modifier cette philosophie dans l'environnement numérique ? Quant au principe d'équivalence fonctionnelle, il sera assurément méconnu si on limite son application aux seuls services qualifiés. Quel sens peut avoir la clause de non-discrimination si, après avoir jugé le procédé recevable, le juge ne peut en aucun cas le juger équivalent, fonctionnellement, au procédé correspondant dans l'environnement papier ?

En outre, on complique inutilement la tâche des acteurs économiques, avec des exigences lourdes, complexes et coûteuses, qui sont disproportionnées par rapport à celles qu'ils assumaient dans l'environnement papier. En matière d'archivage papier ou de datation des documents, par exemple, aucune exigence spécifique n'est imposée, sans

(127) Article 25, § 3, du règlement.
(128) Article 35, § 3, du règlement.
(129) Article 41, § 3, du règlement.
(130) Voy. l'article XII.24, § 2, du C.D.E. En ce sens, voy. D. Gobert, « La loi belge du 21 juillet 2016 mettant en œuvre le règlement européen eIDAS et le complétant avec des règles sur l'archivage électronique : analyse approfondie », octobre 2016, publié sur www.droit-technologie.org, p. 11.
(131) Sur ce point, l'objectif du règlement est clair : aux termes du considérant no 28, « pour accroître, en particulier, la confiance des petites et moyennes entreprises (P.M.E.) et des consommateurs dans le marché intérieur et pour promouvoir l'utilisation des services et produits de confiance, les notions de service de confiance qualifié et de prestataire de services de confiance qualifié devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis ».
(132) Article XII.25, § 8, alinéa 2, du C.D.E.
(133) Article XII.25, § 7, alinéa 2, du C.D.E.
(134) Au sens des articles 3, 12o ou 3, 17o, du règlement eIDAS.
(135) Même dans ce genre hypothèse, on peut se demander si l'exigence d'une signature qualifiée était justifiée (voy. H. Jacquemin et C.-J. Joly, « Focus sur certaines applications du règlement eIDAS dans le domaine financier », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 330 et s.).
(136) Sur ces critères, voy. H. Jacquemin, « Principes applicables à tous les services de confiance et au document électronique », *op. cit.*, p. 115.
(137) *Doc. parl.*, Chambre, sess. ord. 2015-2016, no 1893/001, pp. 19 et s.
(138) D. Gobert, « La loi belge du 21 juillet 2016 mettant en œuvre le règlement européen eIDAS et le complétant avec des règles sur l'archivage électronique : analyse approfondie », octobre 2016, publié sur www.droit-technologie.org, pp. 22 et s.

que cela semble poser de difficulté en pratique. Pourquoi dès lors faire preuve d'un tel dirigisme réglementaire dans l'environnement électronique ? Cette exigence est d'autant plus excessive qu'à l'heure actuelle, il n'existe pas encore de marché suffisamment mûr permettant de choisir un prestataire qualifié en faisant utilement jouer la concurrence. Le législateur en est d'ailleurs conscient puisque l'entrée en vigueur des dispositions concernées[139] est reportée *sine die* (mais laissée à l'appréciation discrétionnaire du Roi). Faisant référence aux travaux préparatoires[140], le rapport au Roi précédant l'arrêté royal qui fixe l'entrée en vigueur de la loi du 21 juillet 2016 indique en effet que « le report de l'entrée en vigueur à une date ultérieure de ces dispositions s'explique par le fait que le caractère opérationnel de celles-ci dépendra notamment de l'adoption de certains actes d'exécution prévus par le règlement 910/2014, de l'existence de normes nationales, européennes et/ou internationales pour certains services de confiance (notamment envoi recommandé électronique et archivage électronique) ainsi que de l'existence sur le marché belge et/ou européen d'une offre acceptable et opérationnelle de ces services de confiance qualifiés ainsi que d'une concurrence suffisante permettant de garantir un prix raisonnable ».

## Conclusion

**35. — Sécurité juridique et technique renforcée. —** Le règlement eIDAS vise à instaurer un climat de confiance propice au développement du commerce électronique. De manière générale, le règlement doit être approuvé, en ce qu'il renforce la sécurité juridique et technique concernant les services de confiance. Le principal reproche tient à l'absence de cadre cohérent et complet en matière d'archivage électronique, comme pour les autres services de confiance. Le législateur belge est toutefois intervenu sur ce point, ce qui doit être approuvé.

Il faut toutefois reconnaître que le régime mis en place est parfois très complexe (et peu lisible). Il fait aussi la part belle aux prestataires de services de confiance qualifiés et aux services de confiance qualifié, même si l'on peut craindre qu'au final, les prestataires intéressés restent très rares. Ainsi, le législateur belge va très (trop) loin, en ce qu'il impose de recourir à un service de confiance qualifié dans de très nombreuses hypothèses, sans réflexion systématique préalable sur la justification d'une telle charge administrative et financière, à l'aune des objectifs poursuivis.

**36. En pratique... —** Les objectifs poursuivis par le règlement ne seront atteints que si le marché — on vise tant les prestataires que les destinataires des services — se montre plus réactif que lors de l'adoption de la directive sur la signature électronique, il y a 15 ans. Il faut en effet espérer que les acteurs économiques soient davantage convaincus par les dispositions du règlement et, respectivement, offrent ou utilisent les services de confiance encadrés par celui-ci.

Sans doute des initiatives pourraient-elles être prises par les pouvoirs publics pour promouvoir — sans nécessairement imposer — le recours à ces services et, en quelque sorte, amorcer la machine...

À défaut, on peut craindre — et regretter — que ces dispositions restent lettre morte et soient une nouvelle occasion manquée de renforcer la confiance et développer les transactions en ligne.

Hervé JACQUEMIN
*Chargé de cours à l'Université de Namur (CRIDS)*
*Avocat au barreau de Bruxelles*

(139) Il s'agit de l'article XII.25, § 5, alinéa 3, § 7, alinéa 2, § 8, alinéa 2, du C.D.E. (voy. l'article 1er de l'A.R. du 14 septembre 2016).

(140) *Doc. parl.*, Chambre, sess. ord. 2015-2016, no 1893/001, p. 32.