

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.

Didier GOBERT¹

Résumé

Deux ans après l'adoption du règlement européen sur l'identification électronique et les services de confiance (eIDAS), le législateur belge a assumé ses responsabilités en adoptant la loi du 21 juillet 2016 qui met en œuvre et qui complète celui-ci.

Même si les dispositions d'un règlement européen sont d'application directe, et n'impliquent pas nécessairement de transposition en droit national comme c'est le cas pour une directive, il n'empêche que certaines dispositions relatives aux « services de confiance » de ce règlement nécessitent une intervention législative au niveau national afin d'assurer leur mise en œuvre. Le règlement n'étant pas d'harmonisation maximale, le législateur belge a en outre exploité les marges de manœuvres laissées par le texte européen en consacrant des dispositions visant à créer un cadre juridique complet et cohérent pour l'archivage électronique.

Cette contribution propose une analyse approfondie des objectifs, principes et nouveautés consacrés par cette loi du 21 juillet 2016, qui insère ainsi un titre 2 intitulé « Certaines règles relatives au cadre juridique pour les services de confiance » dans le livre XII « Droit de l'économie électronique » du Code de droit économique.

¹ Didier GOBERT est conseiller-juriste au Service Public Fédéral Economie, Direction générale de la Réglementation Economique, responsable du Service droit de l'économie électronique. A ce titre, il a participé à la rédaction de la loi commentée dans le cadre de cette contribution. Il a occupé le siège de la Belgique lors de la négociation du projet de règlement eIDAS au groupe de travail du Conseil européen, et fait partie de la délégation belge du groupe d'experts et du Comité eIDAS institué auprès de la Commission européenne. Il est représentant de la Belgique au groupe d'experts commerce électronique de la CNUDCI. Il est également formateur en droit de l'informatique et des réseaux. Les opinions exprimées dans cette contribution sont exclusivement celles de son auteur et n'engagent nullement son administration.

L'auteur remercie Jean-Philippe MOINY, attaché au SPF Economie, pour sa relecture attentive et ses commentaires constructifs.

Il remercie également Eric CAPRIOLI, avocat au barreau de Paris et délégué français au groupe d'experts commerce électronique de la CNUDCI, pour les nombreuses discussions fructueuses ainsi que ses éclairages avisés en sa qualité de praticien, ayant une expérience pointue en ce domaine et une connaissance appréciable des besoins du marché.

Table des matières

Introduction

- I. Contexte et principes généraux
 - A. Du règlement eIDAS à la loi belge du 21 juillet 2016
 - B. Pourquoi des règles sur l'archivage électronique ?
 - C. Les objectifs et principes généraux applicables à l'archivage électronique
- II. Analyse méthodique et approfondie des dispositions de la loi
 - A. Principes généraux et présomptions
 - i. Maintien du principe de la liberté de choix (art. XII.25, §1er)
 - ii. Mise en œuvre de l'exception au profit des réseaux fermés (art. XII.24, §3)
 - iii. Recours judiciaire aux concepts du règlement (art. XII.25, §2)
 - iv. Confirmation de la signature des personnes morales (art. XII.25, §3)
 - v. Clause de non-discrimination, obligation et présomptions légales (art. XII.25, §§ 4 à 8)
 - a. Le principe de non-discrimination
 - b. Les présomptions légales
 - c. L'obligation de recourir aux services de confiance qualifiés dans certaines hypothèses
 - vi. La lutte contre les affirmations trompeuses (art. XII.25, §§ 9 et 10)
 - vii. La matérialisation des signatures et cachets électroniques (art. XII.25, §§ 11 et 12)
 - B. Les exigences relatives au service d'archivage électronique (qualifié)
 - C. Les exigences relatives au service d'envoi recommandé électronique qualifié
 - D. De la révocation, de la suspension et de l'expiration des certificats qualifiés de signature électronique et de cachet électronique
 - E. De la partie utilisatrice d'une signature électronique qualifiée ou d'un cachet électronique qualifié
 - F. De l'arrêt des activités d'un prestataire de services de confiance qualifié
 - G. L'organe de contrôle et ses pouvoirs
 - H. Les sanctions (pénales)
 - I. Les dispositions modificatives et abrogatoires

Conclusion

Introduction

Le 21 juillet 2016, jour de notre fête nationale, le Roi Philippe a sanctionné et promulgué la loi² 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 n° 1999/93/CE (ci-après loi du 21 juillet 2016 et règlement 910/2014)³.

Même si techniquement un règlement européen n'exige pas une transposition en droit national comme c'est le cas pour une directive, le chapitre III du règlement 910/2014 relatif aux « services de confiance » nécessite une intervention législative au niveau national afin d'assurer sa mise en œuvre. Par ailleurs, le texte européen laissait des marges de manœuvres qui ont été exploitées par le législateur belge, consacrant ainsi des dispositions visant à créer un cadre juridique complet et cohérent pour l'archivage électronique.

Notre pays est un des premiers Etats membres à avoir adopté la loi de mise en œuvre du règlement 910/2014, faisant ainsi figure de bon élève. Néanmoins, nous reconnaissons que le texte, tel que publié au Moniteur belge, ne rend pas la lecture et la compréhension de la nouvelle loi aisée, et cela en raison essentiellement de contraintes légistiques. Cette contribution vise à donner les clés de lecture de ce texte afin de permettre à chacun d'appréhender de manière concrète les avantages et opportunités qu'il offre.

Dans un premier temps, nous présentons les orientations et principes généraux permettant de comprendre le contexte, les objectifs et comment la loi s'articule avec le règlement 910/2014. Ensuite, nous analysons en profondeur et de manière méthodique les différentes dispositions de la loi.

I. Contexte et principes généraux

A. Du règlement eIDAS à la loi belge du 21 juillet 2016

On le sait, le législateur européen a adopté le 23 juillet 2014 le règlement n° 910/2014 du Parlement européen et du Conseil du sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive

² 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 « Certaines règles relatives au cadre juridique pour les services de confiance » 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, *Moniteur belge*, 28/09/2016 ainsi que l'erratum publié au *Moniteur belge* du 06/10/2016, p. 68539.

³ Pour un commentaire approfondi de ce règlement européen : D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », juin 2015, <<http://www.caprioli-avocats.com/images/pdf/ReglementeIDAS.pdf>> (consulté le 01/10/2016) ; Sous la direction de H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Collection du Crids, Bruxelles, Larcier, Mars 2016.

1999/93/CE⁴, à peine plus de deux ans après que la Commission européenne ait publié sa proposition⁵.

L'objectif principal de ce règlement 910/2014 consiste à mettre en place un cadre juridique en vue de susciter la confiance accrue dans les transactions électroniques au sein du marché intérieur. S'il est vrai qu'il abroge la directive de 1999, il en reprend néanmoins la plupart de ses dispositions relatives à la signature électronique, moyennant quelques modifications, et complète celles-ci par de nouvelles dispositions relatives, d'une part, à la reconnaissance mutuelle au niveau de l'Union européenne des schémas d'identification électronique notifiés et, d'autre part, aux services de confiance complémentaires à la signature électronique (le cachet, l'horodatage et le service d'envoi recommandé électroniques ainsi que l'authentification de site Internet).

Le règlement 910/2014 compte six chapitres. Les deux chapitres principaux sont le second chapitre relatif à « l'identification électronique » et le troisième chapitre relatif aux « services de confiance » dans la mesure où ils contiennent des nouveautés substantielles dans ces deux domaines. Les quatre autres chapitres (qui portent respectivement sur les dispositions générales, les documents électroniques, les actes délégués et d'exécution, et les dispositions finales) contiennent des dispositions « secondaires », essentiellement au service des deux chapitres précités.

Le chapitre II du règlement 910/2014 relatif à « l'identification électronique » fonctionne de manière autonome et ne nécessite pas nécessairement d'intervention législative au niveau national⁶.

Par contre, le chapitre III du règlement 910/2014 relatif aux « services de confiance » nécessite une intervention législative au niveau belge afin d'assurer sa mise en œuvre. D'une part, ce règlement abroge la directive 1999/93/CE. La loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification⁷, qui transpose cette directive, devait logiquement subir le même sort dès lors que les dispositions relatives à la signature électronique sont désormais consacrées dans le règlement, qui est d'application directe. D'autre part, plusieurs dispositions du règlement 910/2014 renvoient au droit national pour leur mise en œuvre, soit de manière obligatoire soit de manière optionnelle (par exemple, pour régler la question des sanctions applicables ainsi que la désignation de l'organe de contrôle et ses pouvoirs).

⁴ *J.O.U.E.* du 28/08/2014, L 257/73 à 114.

⁵ Proposition de règlement du Parlement européen et du Conseil du 4 juin 2012 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (COM(2012) 238 final), disponible à l'adresse suivante : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:fr:PDF> (consulté le 01/10/2016).

⁶ En tout cas pas sur le plan de sa mise en œuvre. Toutefois, rien n'interdit au législateur national de consacrer des dispositions qui précisent ou complètent les dispositions européennes, pour autant qu'elles ne portent pas atteinte à ces dernières.

⁷ *M.B.*, 29 septembre 2001.

La loi du 21 juillet 2016 permet d'assurer cette mise en œuvre. Elle complète en outre le règlement 910/2014⁸, particulièrement en introduisant de nouvelles dispositions belges visant à créer un cadre juridique complet et cohérent pour l'archivage électronique.

Comme l'indique le considérant n° 25 du règlement 910/2014 « Les États membres devraient rester libres de définir d'autres types de services de confiance, en plus de ceux qui figurent sur la liste fermée des services de confiance prévus par le présent règlement, aux fins de leur reconnaissance au niveau national comme des services de confiance qualifiés ». Le législateur belge n'a pas manqué de tirer profit de cette liberté en consacrant un corps de règles complet visant à encadrer juridiquement l'offre et l'utilisation des services d'archivage électronique, et ainsi assurer leur reconnaissance au niveau national comme des services de confiance qualifiés.

Par ailleurs, le considérant n° 24 du même règlement prévoit que « Les États membres peuvent conserver ou instaurer des dispositions nationales, conformes au droit de l'Union, ayant trait aux services de confiance, pour autant que ces services ne soient pas complètement harmonisés par le présent règlement ». Ainsi, la loi belge consacre des dispositions relatives à la révocation, la suspension et l'expiration des certificats qualifiés de signature et de cachet électroniques, à l'envoi recommandé hybride, à la partie utilisatrice d'une signature électronique qualifiée ou d'un cachet électronique qualifié, à l'arrêt des activités d'un prestataire de services de confiance qualifié offrant un ou plusieurs services de confiance qualifiés et à la possibilité d'identifier une personne physique qui se cache derrière un pseudonyme ou un cachet électronique.

Pour pouvoir intégrer ces multiples dispositions en droit belge, la nouvelle loi insère un titre 2 dans le livre XII, intitulé « Droit de l'économie électronique », du Code de droit économique (ci-après CDE). Ce titre 2 traite de « certaines règles relatives au cadre juridique pour les services de confiance ». Afin de disposer d'un ensemble de dispositions cohérentes qui s'inscrivent dans la structure et la logique du Code de droit économique, les définitions propres au titre 2 du livre XII ainsi que les compétences spécifiques et les peines relatives aux infractions au titre 2 du livre XII, sont insérées respectivement dans les livres I, XV et XVII du Code de droit économique.

Les règles belges s'inscrivent dans les objectifs et la philosophie du règlement 910/2014. Elles reprennent enfin les mêmes principes que ceux édictés par le règlement 910/2014 pour les autres services de confiance (signature, cachet, horodatage, recommandé électroniques). On note par ailleurs que les dispositions relatives à l'archivage électronique ainsi qu'au service d'envoi recommandé hybride s'inspirent des principes essentiels d'une proposition de loi traitant du même sujet et discutée lors de la précédente législature⁹.

Les dispositions du chapitre III du règlement 910/2014 sont entrées en application le 1er juillet 2016. Il était logique que le législateur belge ne traîne pas afin d'assurer une entrée en vigueur des dispositions belges (presque) à la même date.

⁸ Voy. l'article XII.24, §§1 et 2, du CDE inséré par l'article 5 de la loi du 21 juillet 2016.

⁹ *Doc.parl.*, Chambre, 2013-2014, 53-2745/006, adoptée le 28 octobre 2013 par la Commission de l'économie à la chambre.

B. Pourquoi des règles sur l'archivage électronique ?

L'utilisation quotidienne du réseau Internet, et l'apparence de liberté qui en découle, ne doit pas faire oublier que la confiance dans les relations humaines a souvent été bâtie au gré des rencontres entre partenaires potentiels et suite à la formalisation de leurs engagements éventuels. Il convient donc de maintenir un tel climat de confiance dans un monde virtuel dans lequel les parties ne se voient ni ne s'entendent et dans lequel l'aspect immatériel des échanges pose la question du caractère bien réel de ceux-ci, particulièrement dans les réseaux ouverts à tout venant.

Ainsi, le développement harmonieux des échanges sur les réseaux numériques suppose sans aucun doute le maintien voire le renforcement de la « sécurité » et de la « confiance ». Le règlement 910/2014 poursuit particulièrement cet objectif. Certes, ce règlement consacre des dispositions fondamentales relatives à la signature, au cachet, à l'horodatage et au service d'envoi recommandé électroniques. Toutefois, il ne prévoit pas de cadre juridique cohérent pour l'archivage électronique.

Tout au plus, le règlement 910/2014 consacre en son article 34 une disposition relative au service de *conservation* qualifié des signatures électroniques qualifiées. Celui-ci se limite à indiquer que « Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique » tout en précisant que la Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables à ce service de conservation et que ce dernier est présumé satisfaire aux exigences, que l'on considèrera comme générales, lorsqu'il respecte ces normes.

On pourrait qualifier cet article « d'embryon de disposition » sur l'archivage électronique¹⁰. Ceci étant, de là à dire que le règlement harmonise les règles relatives à un service général et complet d'archivage électronique, comme il l'a fait pour la signature, le cachet, l'horodatage et le recommandé électroniques, il y a un pas (de géant) que nous ne franchirons pas, tant les questions à régler dans le cadre de l'archivage électronique sont nombreuses et variées¹¹. Nous le regrettons et nous constatons que le législateur européen disposait d'une opportunité qu'il n'a malheureusement pas saisie¹². Faute d'accord au niveau européen, le législateur belge a pris ses responsabilités au niveau national.

¹⁰ Voy. en ce sens le considérant n° 61 qui indique que « Le présent règlement devrait prévoir la conservation à long terme des informations, afin d'assurer la validité juridique des signatures et cachets électroniques sur de longues périodes de temps, et de garantir qu'elles pourront être validées indépendamment de l'évolution technologique ».

¹¹ Pour un aperçu de ces nombreuses questions, voy. notamment « L'archivage électronique et le droit », ouvrage collectif sous la direction de M. DEMOULIN, Collection du CRIDS, Larcier, Mai 2012, 198 pages ; E. Caprioli, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.187 et s. ; M. DEMOULIN et D. GOBERT, « L'archivage dans le commerce électronique : comment raviver la mémoire? », in M. DEMOULIN (dir.), *Commerce électronique, de la théorie à la pratique*, Cahiers du CRID, 2003, n° 23, pp. 101 à 130.

¹² Ce qui s'explique en partie par la crainte de certains EM que l'on touche aux règles nationales de fond relatives à l'archivage... Cette crainte était injustifiée car, à l'instar des autres services de confiance, le règlement se serait limité à créer un équivalent électronique de l'archivage papier et ainsi de déterminer dans quelles conditions l'archivage pouvait aussi avoir lieu sous forme électronique, sans toucher aux règles de fond.

En effet, les documents établis à des fins juridiques doivent souvent être conservés pendant plusieurs années. Ce devoir de conservation est, d'une part, induit par des obligations de conservation directes (par exemple dans le droit économique, le droit des sociétés, le droit fiscal, le droit comptable, le droit du travail et de la sécurité sociale, le droit judiciaire) et, d'autre part, de manière indirecte par les délais légaux de prescription et le droit de la preuve. Dans la pratique, il s'avère cependant difficile de conserver durant une longue période des données électroniques sans subir de dégradation au niveau de la lisibilité et de l'intégrité. Les évolutions technologiques sont si rapides que les documents créés au moyen d'un logiciel à un temps donné ne sont plus lisibles au bout d'une certaine période, ou que des fichiers sécurisés au moyen de techniques considérées aujourd'hui comme sûres perdent de leur sécurité au bout de quelques années. Si ces problématiques existent, elles ne sont pas pour autant ingérables. Mais pour pouvoir garantir la lisibilité, la durabilité et l'intégrité de données électroniques au gré du temps, il y a lieu de suivre certains principes et procédures spécifiques qui méritaient une attention législative.

En effet, bien que ces données électroniques puissent, techniquement, être conservées de manière sécurisée, elles courent le risque de perdre leur portée juridique. Cela s'explique par le fait que, dans le domaine de l'archivage, le droit ne tient pas encore suffisamment compte de la manière dont la fiabilité des données est garantie dans un contexte électronique, les dispositions ayant été essentiellement conçues dans un environnement papier. En particulier, les règles en matière de preuve établissent une distinction entre écrit original et copie, la copie ayant une valeur juridique inférieure en raison de la fiabilité limitée d'une copie dans un environnement papier¹³. Cette distinction traditionnelle entre original et copie peut poser problème dans le cadre de l'archivage électronique dans la mesure où elle n'est pas toujours pertinente. Cela implique notamment que les données électroniques qui sont conservées selon les règles de l'art en vue d'une conservation fiable à long terme ne sont, dans l'état actuel du droit, considérées que comme des copies et donc discriminées par rapport à leurs équivalents sur papier.

Outre la conservation électronique de données créées sous forme électronique, on observe depuis de nombreuses années le besoin de numériser (scanner) des documents papiers pour les conserver sous forme électronique. Les administrations et entreprises tentent par ce biais de gérer plus efficacement l'espace physique réservé aux archives et l'accès aux informations. Les documents numérisés sont ici aussi considérés par le droit comme une copie, ce qui oblige les entreprises à conserver les documents sur papier pour des raisons de sécurité juridique. On constate que dans certains secteurs particuliers (sécurité sociale, matières fiscales), des réglementations spécifiques permettent aux entreprises actives dans ces secteurs ainsi qu'aux administrations publiques de scanner, sous certaines conditions de fiabilité, des originaux sur papier avec maintien de leur portée juridique¹⁴. Avec la loi du 21 juillet 2016, le législateur a

¹³ Pour une analyse détaillée de ces notions et de leurs conséquences, voy. D. MOUGENOT, *La preuve*, tiré à part du Répertoire Notarial, 4^{ème} édition, Larcier, Juin 2012, pp. 276 et s..

¹⁴ Voy. notamment : Arrêté royal du 15 mars 1999 relatif à la valeur probante, en matière de sécurité sociale et de droit du travail, des informations échangées, communiquées, enregistrées, conservées ou reproduites par les services ministériels et les parastataux du Ministère de l'Emploi et du Travail, *M.B.*, 5 juillet 1999 ; Arrêté royal du 9 janvier 2000 relatif à la force probante des informations utilisées par l'Administration des Pensions pour l'application de la législation dont elle est chargée, *M.B.*, 24 février 2000 ; Arrêté royal du 26 avril 2007 modifiant l'arrêté royal du 27 avril 1999 relatif à la force probante des données enregistrées, traitées, reproduites ou

généralisé le système à l'ensemble des domaines en créant la possibilité de scanner des documents sur papier de manière fiable, sans perdre leur valeur juridique, au profit tant de l'ensemble du secteur public que des entreprises, peu importe leurs secteurs d'activités, et des particuliers.

Jusqu'à présent, le marché des services d'archivage électronique tendait à se développer, mais avec difficulté et un niveau de qualité variable. L'absence de cadre juridique entraînait plusieurs inconvénients. Tout d'abord, certains prestataires peu scrupuleux pouvaient offrir des services insuffisamment fiables sur le plan technique et juridique, au détriment tant des utilisateurs que des prestataires plus sérieux. Ensuite, l'absence de critères minimaux de qualité empêchait les utilisateurs des services de faire le tri, sur la base de leurs besoins, entre les différents prestataires en fonction de leur niveau (peu visible) de qualité. Cette absence de critères objectifs et clairs constituait également un frein auprès des prestataires souhaitant se lancer dans cette activité et engager les investissements nécessaires à cette fin. Par ailleurs, les juges risquaient d'être confrontés à des questions juridiques épineuses relatives à ces services, notamment quant à la validité ou la valeur probatoire de ceux-ci, pour lesquelles le droit commun s'avérait souvent insuffisant.

Enfin, il nous semble évident que lorsqu'on envisage la conclusion, la transmission et la conservation d'un acte juridique dans un processus électronique, il convient d'encadrer juridiquement la totalité des étapes du processus, en ce compris l'étape ultime qui consiste en l'archivage de l'acte, et pas uniquement sa signature, sa datation et son envoi. Avec la loi du 21 juillet 2016, le législateur belge encadre utilement et opportunément le dernier maillon de la chaîne.

C. Les objectifs et principes généraux applicables à l'archivage électronique

Le législateur belge a tout mis en œuvre pour édicter des règles sur l'archivage électronique qui s'articulent efficacement et s'intègrent autant que faire se peut dans le cadre juridique existant au niveau européen, en vue notamment de profiter de cet acquis. L'objectif du législateur n'était manifestement pas d'édicter une législation belgo-belge, qui aurait été déconnectée du contexte juridique européen. A cet égard, les travaux parlementaires indiquent que le point de départ de cette « législation est que les règles soient de nature pragmatique, simples à mettre en œuvre et s'inscrivent dans la mesure du possible dans les principes déjà établis par le règlement 910/2014 pour les services de confiance. De cette manière, il pourra être fait usage des définitions et obligations générales à charge des prestataires de services de confiance établies par le règlement

communiquées par les dispensateurs de soins et les organismes assureurs, *M.B.*, 18 juin 2007 ; art. 13 de la Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, *M.B.*, 13 octobre 2008 ; Arrêté royal du 10 mai 2015 relatif à la force probante des données enregistrées, traitées, communiquées au moyen de techniques photographiques et optiques par les hôpitaux, ainsi qu'à leur reproduction sur papier ou sur tout autre support lisible pour l'application dans les soins de santé, *M.B.*, 11 juin 2015 ; Arrêté royal du 28 novembre 1995 relatif à la force probante, en matière de sécurité sociale des travailleurs indépendants, des informations utilisées par l'Administration et les organismes coopérants en matière de sécurité sociale des travailleurs indépendants, *M.B.*, 29 décembre 1995 ; L'article 14 *alinéa* 3 de la loi du 4 avril 2014 relative aux assurances ; art. 53*octies*, §§ 3 et 4 du Code de la TVA ; art. 314*bis* et 339/1 du Code des impôts sur les revenus.

910/2014. De plus, il est possible de s'appuyer sur les procédures et le système de contrôle mis en place par ce dernier »¹⁵.

Le corps de règles envisagé cherche manifestement à atteindre un subtil et difficile équilibre entre souplesse et sécurité. D'une part, le législateur souhaite établir un cadre relativement souple pour stimuler l'offre des services d'archivage électronique, dans le respect des contraintes européennes, mais également leur utilisation aisée. D'autre part, ce cadre doit être suffisamment sécurisant pour protéger les utilisateurs de ces services et assurer un niveau minimum de qualité. Enfin, toujours dans la perspective de stimuler le marché et permettre aux utilisateurs de gérer efficacement leurs risques juridiques, diverses présomptions sont prévues en faveur des services d'archivage électronique considérés comme « qualifiés » au sens de la loi ainsi qu'en faveur des autres services de confiance qualifiés au sens du règlement.

On note également que, à l'instar du régime déjà applicable aux autres services de confiance dans le cadre du règlement 910/2014¹⁶, le cadre juridique relatif à l'archivage électronique est envisagé comme une « boîte à outils juridiques » permettant aux utilisateurs de recourir à ce service en vue de gérer leurs risques par rapport principalement aux données ou documents présentant une valeur juridique. Par contre, les travaux parlementaires précisent que « ce cadre n'est pas particulièrement destiné à s'appliquer aux systèmes informatiques que les organisations utilisent, dans un but de fonctionnement optimal de ces dernières, pour stocker des données de tous types n'ayant pas de valeur juridique particulière »¹⁷. On le comprend, l'objectif du législateur n'est manifestement pas de vouloir réglementer de manière contraignante toutes les formes de conservations de données électroniques mais plutôt d'offrir un cadre juridique *ad hoc* afin d'offrir de la sécurité juridique aux utilisateurs qui décideraient librement d'y recourir pour la conservation essentiellement de données électroniques ayant une certaine utilité juridique.

A l'image de ce qui est prévu par le règlement 910/2014 pour les autres services de confiance, le prestataire de services d'archivage électronique peut décider librement d'offrir ces services sans nécessairement se conformer à l'ensemble du régime légal instauré pour les services de confiance qualifiés. En effet, il peut se limiter à offrir un service d'archivage électronique « simple », appelé également « non qualifié ». Mais il peut aussi offrir un service d'archivage électronique « qualifié », avec pour avantage de bénéficier d'une certaine reconnaissance juridique (en l'occurrence des présomptions) mais pour contrainte de devoir se soumettre aux dispositions du règlement 910/2014 et de celles de la loi, qui sont applicables au prestataire de services de confiance qualifié.

En vue de renforcer la sécurité juridique mais également de promouvoir l'utilisation du nouveau cadre légal applicable principalement aux services de confiance qualifiés, le législateur a consacré des présomptions au profit des services qui sont conformes aux exigences légales et réglementaires relatives aux services d'archivage électronique « qualifiés » : présomption de conformité à l'obligation légale ou réglementaire d'archivage de documents, d'intégrité du contenu du document électronique ainsi que de conformité entre l'original et sa copie

¹⁵ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, pp. 9 et 10.

¹⁶ Voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 11 et 23.

¹⁷ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.10.

numérique. Des présomptions comparables sont également prévues pour les autres services de confiance qualifiés, et complètent celles déjà consacrées par le règlement 910/2014 (cfr. *infra*).

Les présomptions au profit des services d'archivage électronique qualifiés concernent non seulement les documents ou les données électroniques archivés par le biais des services prestés par un prestataire *tiers*, mais également les documents ou les données électroniques archivés par le biais de services exploités par un organisme du secteur public ou une personne physique ou morale pour son propre compte, *en interne*.

Cette distinction (archivage par un prestataire *tiers* ou *en interne*) découle de la lecture des nouvelles définitions insérées à l'article I.18,17° et 18°, du CDE. Elle est justifiée par la volonté d'offrir de la souplesse et une réduction des coûts, et ainsi permettre particulièrement aux grosses organisations de mettre en place directement en interne leur propre système d'archivage électronique qualifié (et bénéficiant ainsi des présomptions), tout en leur évitant de devoir passer par un prestataire extérieur, dont l'activité principale consiste à offrir un service d'archivage électronique qualifié (qui pourrait présenter un coût supérieur, même si aucune analyse économique permettant de confirmer ce présupposé n'existe à ce jour).

Pour bénéficier des présomptions que nous analyserons par la suite, le prestataire doit respecter les exigences spécifiques relatives aux services d'archivage électronique qualifiés consacrées par les dispositions de la loi et de ses annexes ainsi que les dispositions applicables aux prestataires de services de confiance qualifiés prévues par le règlement 910/2014. Le prestataire doit en outre soit se conformer à la procédure de lancement d'un service de confiance qualifié visée par le règlement 910/2014 s'il offre son service au public (aux *tiers*) soit se déclarer volontairement auprès de l'Organe de contrôle s'il exploite le service pour son propre compte (*en interne*), l'Organe pouvant alors procéder à un contrôle d'initiative s'il le juge utile.

Si le prestataire offre ou exploite pour son propre compte un service d'archivage électronique qui n'est pas qualifié, il n'est pas obligé de se conformer à la procédure de lancement ou de se déclarer auprès de l'Organe de contrôle, de sorte qu'il n'y a pas de restriction à l'exercice de ces activités. De même, les services d'archivage électronique non qualifiés ne sont pas nécessairement dépourvus de reconnaissance juridique et les documents issus de leurs services pourront être invoqués devant les tribunaux. Simplement, ils ne bénéficieront pas des présomptions prévues par la loi. Les utilisateurs de ces services non qualifiés seront donc tenus, le cas échéant, d'apporter la preuve que ces services répondent à l'ensemble des conditions fonctionnelles de nature à assurer la validité ou la valeur probatoire de ceux-ci. On le voit, le législateur s'inspire des effets liés aux clauses de non-discrimination et d'assimilation déjà bien connus depuis des années pour la signature électronique¹⁸.

¹⁸ Pour un commentaire relatif aux clauses de non-discrimination et d'assimilation dans le cadre de la signature électronique, voy. E. MONTERO, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », in *La Preuve*, Formation permanente CUP, Liège, Volume 54, mars 2002, p. 75 à 81 ; B. DE GROOTE, « Het bewijs in de elektronische handel – Enkele bedenkingen », *A.J.T.*, 2001, pp. 881 à 901 ; P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique » in *Le commerce électronique : un nouveau mode de contracter ?*, Editions du jeune barreau de Liège, 2001, pp. 112 et s. ; M. E. STORME, « De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen », *R.W.*, 9 juin 2001, n° 41, pp. 1505 à 1525.

Si les règles relatives à l'archivage électronique consacrées par le législateur belge sont originales, leur champ d'application est toutefois limité au territoire de notre Royaume, faute d'harmonisation au niveau européen. L'article XII.24, §2, du CDE indique clairement que « Il [les nouvelles dispositions du titre 2 du livre XII du CDE] fixe certaines règles complémentaires au règlement 910/2014 relatives au cadre juridique pour les services (...) offerts par un prestataire de services de confiance *établi en Belgique* ou pour un service d'archivage électronique exploité pour son propre compte par un organisme du secteur public ou une personne physique ou morale *établi en Belgique* ». Les travaux parlementaires précisent toutefois que la « loi ne s'applique qu'aux prestataires de services de confiance établis en Belgique. Mais rien n'interdit à un prestataire établi dans un autre Etat de l'Union européenne de se soumettre volontairement aux dispositions de ce projet relatives aux services d'archivage électronique, non visés par le règlement 910/2014, et particulièrement aux services qualifiés en vue de bénéficier des présomptions y associées »¹⁹.

Outre les nouvelles dispositions du règlement 910/2014 et de la loi belge, on rappelle que les activités des prestataires qui offrent des services d'archivage électronique (et de manière générale, des services de confiance) sont aussi soumises à des règles ressortissant au droit des contrats, au droit de la responsabilité, aux pratiques du marché et à la protection des consommateurs ou encore aux services de la société de l'information. Ainsi, lorsqu'un prestataire offre ses services, il peut se voir appliquer les règles relatives à la publicité trompeuse ou mensongère. De même, si le prestataire de services de confiance peut être considéré comme prestataire de services de la société de l'information, il est tenu de fournir une série d'informations générales relatives à son activité professionnelle, tel que prévu par le livre XII du CDE. Ces dispositions étant déjà d'application, seuls les aspects spécifiques aux services de confiance, et particulièrement aux services d'archivage électronique, ont été réglés par la loi du 21 juillet 2016.

¹⁹ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.12.

II. Analyse méthodique et approfondie des dispositions de la loi

Le lecteur attentif constatera une double numérotation des articles dans la loi du 9 juillet 2016. Celle-ci résulte de contraintes légistiques imposées par le Conseil d'Etat²⁰. La loi n'a donc pas utilisé un seul article pour introduire le nouveau titre 2 intitulé « Certaines règles relatives au cadre juridique pour les services de confiance » dans le livre XII du Code de droit économique ainsi que l'ensemble des dispositions de ce titre. Elle a au contraire consacré différents articles pour introduire chaque titre, sous-titre et disposition de ce titre 2. Afin de faciliter la lecture et la compréhension des articles, nous avons jugé opportun de se référer dans le cadre de cette contribution à la numérotation des articles utilisée dans le CDE plutôt qu'à celle de la loi.

A. Principes généraux et présomptions

i. Maintien du principe de la liberté de choix (art. XII.25, §1^{er})

Le premier paragraphe de l'article XII.25 reprend sans modification l'article 4, § 1^{er}, de la loi du 9 juillet 2001. Il est intéressant de constater que le législateur confirme à nouveau après 15 ans, et malgré le fait que les outils électroniques soient désormais bien intégrés dans la vie quotidienne d'une majorité de citoyens, le principe selon lequel toute personne conserve le libre choix du support (papier ou électronique) par lequel il pose ses actes juridiques. Il étend par ailleurs ce principe à l'ensemble des services de confiance consacré par le règlement 910/2014 et par la loi du 21 juillet 2016 (signature, cachet, horodatage, envoi recommandé et archivage électroniques). Cela signifie notamment qu'une personne *ne peut être contrainte* de signer un contrat par la voie électronique ou d'envoyer ou recevoir un recommandé électronique²¹. Elle ne le fera que si une disposition légale le prévoit ou si elle l'accepte contractuellement.

Cette disposition a été reprise dans la loi dans l'objectif notamment de ne pas accroître inutilement la fracture numérique. Elle ne poursuit pas l'objectif de freiner la digitalisation des processus mais vise simplement à ce que cette digitalisation se fasse de manière équilibrée.

Précisons d'abord que cette disposition ne porte que sur les « actes juridiques » c'est-à-dire les actes réalisés volontairement en vue de produire des effets de droit (ce qui n'inclut pas tous les échanges électroniques).

Cette disposition prévoit uniquement qu'une partie ne peut pas contraindre une autre partie à poser un acte juridique par voie électronique. Il est toutefois possible de déroger à ce principe si une disposition légale spécifique (notamment pour les relations B2G ou C2G), ayant fait l'objet d'un débat parlementaire, l'impose « unilatéralement » aux usagers (citoyens et entreprises).

²⁰ La recommandation n° 118 du « Guide de rédaction des textes législatifs et réglementaires – Principes de technique législative » du Conseil d'Etat (2008) stipule que « Lorsque vous modifiez plusieurs articles d'un même acte législatif ou d'actes législatifs différents, rédigez un article modificatif pour chaque article à modifier. Cette méthode est imposée par le principe du vote article par article. Elle a en outre l'avantage d'offrir une vue claire de toutes les modifications effectuées. », <http://www.raadvst-consetat.be/?lang=fr&page=technique_legislative> (consulté le 01/10/2016).

²¹ En partant du présupposé que l'envoi ou la réception d'un recommandé est un acte posé en vue de produire des effets de droit.

Par ailleurs, un acte juridique peut toujours être posé par voie électronique si toutes les parties marquent leur accord (dans ce cas, il n'y a pas de « contrainte »). Dès lors, tant dans les relations B2B mais aussi B2C ou B2G ou C2G voire C2C, les parties peuvent toujours convenir contractuellement que les actes juridiques soient posés par voie électronique.

Pour le reste, nous invitons le lecteur à se reporter aux travaux préparatoires de la loi du 9 juillet 2001 pour déterminer la portée et l'interprétation à donner à cet article²².

ii. Mise en œuvre de l'exception au profit des réseaux fermés (art. XII.24, § 3)

Le troisième paragraphe de l'article XII.24 du CDE fait application de la dérogation consacrée par l'article 2.2. du règlement 910/2014 au profit des « systèmes fermés » et l'étend aux nouvelles dispositions nationales. Le premier alinéa de ce paragraphe stipule que « En application de l'article 2, paragraphe 2, du règlement 910/2014, tous les composants utilisés pour les signatures électroniques, les envois recommandés électroniques, l'horodatage électronique et l'archivage électronique, fournis gratuitement ou contre paiement par une autorité administrative au sens de l'article 14 des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973, en exécution des missions qui lui sont confiées par ou en vertu d'une loi, sont exclus du champ d'application du règlement 910/2014, du présent titre et de ses annexes ».

Les travaux parlementaires justifient cette disposition comme suit²³. Le règlement et le titre 2 du livre XII contiennent des dispositions qui mettent en place un système général pour la prestation de services de confiance (signature, cachet, horodatage, recommandé et archivage électroniques). Cependant, il est vrai que depuis plusieurs années, certaines administrations ont mis en place des systèmes spécifiques, notamment par le biais de lois spéciales dans le domaine de la sécurité sociale et de la santé par exemple. Ces systèmes ont nécessité des investissements importants et sont déjà en cours d'utilisation ou sur le point de l'être. L'objectif de ce nouveau paragraphe 3 de l'article XII.24 est d'indiquer que le régime général pour les services de confiance élaboré par la loi du 21 juillet 2016 ne porte pas préjudice à ces systèmes spécifiques mis en place dans certains services publics particuliers par le biais de lois spéciales.

Toutefois, on relève utilement le message envoyé par le législateur – via ces mêmes travaux parlementaires –, particulièrement aux administrations qui souhaiteraient recourir à l'avenir aux services de confiance : « dans un objectif d'harmonisation des systèmes, d'augmentation du niveau de sécurité (juridique et technique) des transactions et de simplification administrative pour l'ensemble des acteurs, le législateur recommande à l'ensemble des administrations de tout mettre en œuvre à l'avenir pour utiliser les services de confiance qualifiés visés par le règlement et le présent titre 2, ou à tout le moins de s'en rapprocher le plus possible ».

Cette recommandation nous semble heureuse. Gageons que les administrations la suivent et que le gouvernement donne des instructions allant dans le même sens. De manière plus générale, et sans nier le marché potentiel des services de confiance *non qualifiés*, nous appuyons les actions

²² Voy. particulièrement, *Doc. Parl.*, Sén., sess. Ord. 2000-2001, n° 2-662/4, p.5. Voy. également D. GOBERT, « Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001 », in *La preuve*, Liège, Formation permanente CUP, 2002, vol. 54, pp. 108 à 110.

²³ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, pp.14 et 15.

de nature à promouvoir l'émergence d'une offre de services de confiance *qualifiés* dans des conditions de concurrence saine ainsi que l'utilisation de ceux-ci. Ces actions constitueraient un message positif à l'égard des entreprises hésitant encore à investir dans l'offre de ce type de service, craignant de ne pas pouvoir rentabiliser leurs investissements si la demande était insuffisante.

Par ailleurs, la promotion de tels services devraient créer un effet d'entraînement. En effet, plus les services de confiance qualifiés seront utilisés, plus les applications intégrant ceux-ci se développeront, se standardiseront et seront conviviales pour l'utilisateur, plus ces services seront interopérables et plus leur coût diminuera²⁴ tout en offrant un niveau de sécurité technique et juridique élevé. Dans la situation actuelle, on constate une tendance pour les entreprises ou administrations à mettre en place ou utiliser des systèmes relativement différents, ce qui crée, d'une part, des problèmes d'interopérabilités dès que l'on veut travailler en réseau ouvert et plus global et, d'autre part, une multiplication (parfois inutile) des moyens de signature (ou autres services de confiance) pour l'utilisateur²⁵.

Par ailleurs, les organismes de normalisation nationaux, européens et internationaux travaillent pour l'instant au développement ou à la mise à jour des normes pour les services de confiance *qualifiés*. Outre les bienfaits résultant du processus de normalisation (harmonisation des pratiques, amélioration de l'interopérabilité, augmentation de la qualité et de la fiabilité des produits et services, facilitation du commerce international par la suppression des barrières,...), la publication dans un futur proche de ces normes devrait faciliter la mise en œuvre opérationnelle de ces services au sein des entreprises et administrations²⁶.

On note que la dérogation consacrée par l'article XII.24 n'est pas totale. En effet, le second alinéa de cet article énonce que « Néanmoins, les articles 25, paragraphe 1, 41, paragraphe 1, et 43, paragraphe 1, du règlement 910/2014 sont applicables aux composants utilisés pour les signatures électroniques, les envois recommandés électroniques et l'horodatage électronique visés à l'alinéa premier ». De la sorte, le législateur veut s'assurer que, peu importe le contenu des législations spécifiques, les clauses de non-discrimination consacrées par le règlement puissent s'appliquer à certains services de confiance (signature, horodatage et recommandé électroniques) utilisés dans le cadre de ces systèmes spécifiques. On constate que cette disposition ne vise pas la clause de non-discrimination consacrée au profit du cachet électronique. Ce service de confiance étant relativement nouveau, on présume qu'il n'est pas utilisé dans les systèmes spécifiques, ce qui expliquerait cet oubli du législateur. Le renvoi à l'article 35.1. du règlement 910/2014 aurait toutefois pu être utile pour une éventuelle utilisation

²⁴ A notre connaissance, aucune étude à ce jour ne permet de démontrer que l'utilisation de services de confiance *non qualifiés* présenterait (nécessairement) un coût inférieur à celle de services de confiance *qualifiés*. Par contre, une certitude existe : seul ce dernier offre une sécurité juridique optimale.

²⁵ Lui-même irrité par la complexité et les difficultés pratiques résultant de cette diversité.

²⁶ Pour résumer la complémentarité entre la législation et la norme, la législation répond à la question du « quoi » au niveau juridique sur la base d'une approche fonctionnelle et générale alors que la norme répond à la question du « comment faire » au niveau du processus métier, et donc sur le plan opérationnel. La norme permet aux organisations de traduire des concepts abstraits en une réalité plus opérationnelle permettant une mise en œuvre concrète des exigences légales. S'il est vrai que l'élaboration et la publication des normes ne sont pas obligatoires, on reconnaît qu'il sera plus facile pour une organisation de savoir comment mettre en œuvre les différentes exigences légales ainsi que de se faire auditer en présence de ces normes.

future de ce cachet dans le cadre de systèmes spécifiques au sein d'administration publique. La disposition ne vise pas non plus la clause de non-discrimination contenue à l'article XII.25, §4, du CDE au profit de l'archivage électronique. Ici aussi, un renvoi n'aurait pas été inutile.

Il convient enfin de préciser que si, dans le cadre de ces « systèmes fermés », il est recouru à un ou plusieurs services de confiance « qualifiés » au sens du règlement 910/2014 et du titre 2 du livre XII du CDE, les prestataires qui offrent ces services qualifiés ainsi que ces services restent tenus de respecter les exigences du règlement 910/2014 et du titre précité²⁷.

iii. Recours judiciaires aux concepts du règlement (art. XII.25, § 2)

Le second paragraphe de l'article XII.25 stipule que « Les termes du présent titre non définis à l'article I.18. s'entendent conformément aux définitions de l'article 3 du règlement 910/2014 ».

Les travaux parlementaires justifient ce choix comme suit : « en vue de répondre à l'objectif de s'inscrire dans la philosophie, les principes et les procédures établis par le règlement 910/2014, il a été jugé préférable de se référer aux définitions pertinentes déjà consacrées par celui-ci »²⁸.

Nous ne pouvons qu'appuyer ce choix du législateur belge, faisant ainsi preuve de réalisme (européen) et de pragmatisme. Cela permet en outre d'inscrire plus aisément les règles belges sur l'archivage électronique dans le contexte juridique européen et, pourquoi pas, inspirer le législateur européen lors d'une révision future du règlement 910/2014²⁹.

iv. Confirmation de la signature des personnes morales (art. XII.25, § 3)

Le troisième paragraphe de l'article XII.25 confirme en droit belge la possibilité pour les personnes morales de signer électroniquement, possibilité déjà consacrée par le législateur depuis la loi du 9 juillet 2001³⁰.

En effet, l'article 4, § 4 de cette loi stipulait : « Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, *qu'elle soit réalisée par une personne physique ou morale.* ».

²⁷ En ce sens, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, p. 24 ; *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 15.

²⁸ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, pp.15 et 16.

²⁹ On rappelle à cet égard l'obligation à charge de la Commission de rédiger un premier rapport d'évaluation le 1^{er} juillet 2020 (art. 49 du règlement 910/2014). L'objectif essentiel de ce rapport est d'évaluer s'il est nécessaire ou non de modifier le champ d'application du règlement ou ses dispositions spécifiques, compte tenu de l'expérience acquise dans le cadre de son application ainsi que de l'évolution des technologies, du marché et du contexte juridique. On constate que l'article 49 vise certaines dispositions, en particulier l'article 34 relatif au service de conservation qualifié des signatures électroniques qualifiées (certains EM souhaitant aller beaucoup plus loin en vue de consacrer un service d'archivage électronique qualifié).

³⁰ Sur la question de la signature des personnes morales en droit belge, voy. B. VANBRABANT, « La signature électronique des personnes morales », in *La preuve*, Liège, Formation permanente CUP, 2002, vol. 54, pp. 173 à 228 ; D. MOUGENOT, *La preuve*, tiré à part du Répertoire Notarial, 4^{ème} édition, Larcier, Juin 2012, pp. 216 à 217. En droit français, voy. E. Caprioli, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.166 à 168.

Toutefois, la formulation de la disposition ayant le même objet dans la loi du 21 juillet 2016, a été adaptée en vue de tenir compte des modifications apportées par le règlement 910/2014. Désormais, le libellé est le suivant : « 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. ».

Cette nouvelle formulation se justifie par les raisons suivantes. Alors que la directive 1999/93/CE permettait de délivrer des certificats de signature électronique tant à des personnes physiques qu'à des personnes morales, le règlement opère une distinction entre le certificat de signature électronique et le certificat de cachet électronique³¹. Même si la technologie ainsi que les outils matériels et logiciels utilisés pour créer un cachet électronique peuvent être identiques à ceux utilisés pour la création d'une signature électronique, le cachet électronique se distingue principalement de la signature électronique en ce que cette dernière est, selon le règlement, réservée aux personnes physiques (le certificat permet notamment d'identifier une *personne physique* selon l'article 3.9. du règlement 910/2014 et le point c) de son annexe I), alors que le cachet est dédié aux personnes morales (le certificat permet notamment d'identifier une *personne morale* selon l'article 3.24. du règlement 910/2014 et le point c) de son annexe III).

Par ailleurs, le règlement prévoit que la signature électronique est utilisée par une personne physique « pour signer » (articles 3.9. et 3.10.). Elle a donc un pouvoir « engageant » pour ladite personne. A l'inverse, le règlement ne prévoit pas que, à lui seul, le cachet électronique puisse engager juridiquement une personne morale. L'article 3.25. prévoit que ce dernier permet de « garantir l'origine et l'intégrité » des données cachetées. Chaque Etat membre reste néanmoins libre de prévoir au niveau national que l'utilisation du cachet électronique peut engager directement la personne morale sur le plan juridique. Il est clair que le règlement 910/2014 n'impose pas que le consentement d'une personne morale soit toujours donné par une signature électronique d'une personne physique, cette question n'ayant pas été harmonisée au niveau européen. Cette affirmation découle notamment d'une lecture *a contrario* du considérant n° 58 du règlement³² ainsi que de la lecture du considérant n° 60 (*cf. infra*). On note également que la Commission européenne n'a émis aucune observation sur cette disposition belge, donnant un pouvoir « engageant » au cachet électronique, dans le cadre de la notification officielle opérée conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information.

³¹ Pour une analyse détaillée de cette distinction et de ce nouveau service de confiance (cachet électronique), voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 38 à 40 ; J.B. HUBIN, « Le cachet électronique des personnes morales » in *L'identification électronique et les services de confiance depuis le règlement eIDAS*, sous la direction de H. JACQUEMIN, Collection du Crids, Bruxelles, Larcier, Mars 2016, pp. 175 et s.

³² Le considérant n° 58 stipule que « Lorsqu'une transaction exige d'une personne morale un cachet électronique qualifié, une signature électronique qualifiée du représentant autorisé de la personne morale devrait être également recevable. ».

Cette liberté donnée par le texte européen – dont on rappelle qu'elle est déjà utilisée en droit belge depuis 2001 – a donc été assez logiquement exploitée, comme indiqué plus haut, par le législateur dans le cadre de la loi du 21 juillet 2016. Nous appuyons cette disposition car, même si cette possibilité n'avait pas été consacrée par le législateur belge, nous pensons qu'un juge aurait pu à l'avenir prendre une décision ayant le même effet dans un cas d'espèce³³. Dans ce contexte, une disposition légale claire et prévisible nous semble préférable.

On précise que l'assimilation consacrée par l'article XII.25, §3, du CDE ne s'applique, d'une part, que si le cachet électronique est qualifié et, d'autre part, que si ce cachet est « utilisé dans le cadre d'actes juridiques », dont on rappelle qu'il s'agit d'une manifestation intentionnelle de volonté dans le but de produire des effets de droit. En d'autres mots, l'assimilation ne jouera que lorsque le cachet est précisément utilisé pour manifester son consentement mais le cachet n'aura aucun effet « engageant » s'il est utilisé en dehors du cadre de la passation d'actes juridiques.

Pour le reste, une personne morale peut bien entendu décider d'utiliser un cachet dans d'autres hypothèses, ayant soit aucun effet juridique soit un objectif juridique différent, telles que pour authentifier tout bien numérique d'une personne morale, comme un code logiciel ou des serveurs³⁴.

Dès lors qu'elle est en mesure de connaître clairement les effets attribués au cachet, chaque personne morale reste donc libre de l'utilisation qu'elle en fait, de déterminer les personnes physiques à qui elle remet le matériel et les données pour générer ce cachet et de poser les conditions et limites d'utilisation en son sein, comme elle le fait déjà quotidiennement dans le cadre de délégations de pouvoirs. A ce titre, rien n'empêche une personne morale – par exemple, pour des questions de gestion interne et externe – d'exiger de toute personne physique qui la représente en utilisant le cachet, d'indiquer son identité dans les relations avec les tiers. Elle peut également interdire à certains membres de son personnel d'utiliser le cachet pour engager juridiquement l'entreprise, ceux-ci devant se limiter à l'utiliser pour garantir l'intégrité et l'origine de logiciels, de serveurs ou de documents purement informationnels par exemple.

On note que, contrairement à la situation actuelle dans laquelle une personne physique qui a quitté la société pourrait toujours utiliser abusivement sa signature manuscrite pour engager son ancienne société, le cachet permet d'éviter un tel risque grâce à la possibilité pour l'organe de la personne morale de révoquer le certificat (en quelques minutes) dès que la personne physique utilisatrice du cachet a quitté l'entreprise³⁵.

Afin de rester conforme au règlement européen et de ne pas créer d'obstacles à l'utilisation transfrontière du cachet électronique qualifié, le texte précise que cette assimilation ne vaut que

³³ En effet, dès lors qu'un cachet électronique (qualifié) permet de « garantir l'origine et l'intégrité » des données, il n'y a plus qu'un (petit) pas à franchir pour que le juge puisse considérer – sur la base des circonstances de l'espèce – que la personne morale a ainsi voulu exprimer une volonté en vue de produire des effets de droit ou adhérer à un acte juridique.

³⁴ En ce sens, le considérant n° 65 du règlement 910/2014 indique que « Outre le document délivré par une personne morale, les cachets électroniques peuvent servir à authentifier tout bien numérique de ladite personne, tel un code logiciel ou des serveurs ».

³⁵ Quant aux garanties offertes par le cachet électronique à la personne morale, voy. J.B. HUBIN, *op.cit.*, p. 201.

lorsque le cachet est « utilisé dans le cadre d'actes juridiques exclusivement posés par ou passés entre des personnes physiques et/ou morales domiciliées ou établies en Belgique ».

On note également que la disposition légale indique expressément qu'elle est sans préjudice des articles 1323 et suivants du Code civil (il est par exemple possible de contester un cachet électronique qualifié qui aurait été utilisé pour engager une personne morale dans le cadre d'un acte sous seing privé) et sans préjudice des règles concernant la représentation des personnes morales (théorie de l'organe, application des règles relatives au mandat (général ou spécial), obligations et formalités de publicité, théorie du mandat apparent, etc.).

Cette nouvelle méthode d'engagement des personnes morales s'inscrit donc dans le cadre juridique existant, permettant ainsi aux entreprises d'exploiter au mieux les principes bien connus de représentation des personnes morales. Les premiers commentateurs voient même en ce nouvel outil (le cachet électronique) de véritables avantages sur le plan de la sécurité juridique et de la gestion opérationnelle, tant pour la personne morale qui l'utilise que pour les « destinataires de communications électroniques émanant de représentants d'une personne morale »³⁶.

On rappelle qu'un certificat de cachet électronique n'identifie *a priori* aucune personne physique, telle que par exemple la représentante légale de la personne morale, la personne bénéficiant d'une délégation de pouvoir au sein de cette personne morale et/ou le porteur physique du dispositif de création de cachet électronique (ce qui n'empêche toutefois pas la personne morale elle-même – par exemple, en vue de respecter les exigences du Code des sociétés ou pour des questions de gestion interne – d'exiger de toute personne physique qui la représente d'indiquer son identité dans les relations avec les tiers). Or, et comme le législateur belge lui reconnaît un pouvoir engageant, connaître la personne physique qui « se cache » derrière un cachet électronique et qui crée matériellement ou pratiquement ce cachet (la personne morale n'ayant pas d'existence matérielle) peut parfois s'avérer utile.

Le législateur européen était conscient de cette nécessité. Ainsi, le considérant n° 60 du règlement 910/2014 stipule que « Les prestataires de services de confiance délivrant des certificats qualifiés de cachet électronique devraient mettre en œuvre les mesures nécessaires afin de pouvoir établir l'identité de la personne physique représentant la personne morale à laquelle le certificat qualifié de cachet électronique est fourni, lorsque cette identification est nécessaire au niveau national dans le cadre d'une procédure judiciaire ou administrative ». Toutefois, cette « obligation » (qui a une valeur réduite car uniquement consacrée par un considérant) est doublement limitée. D'une part, elle ne pèse que sur le prestataire de services de confiance délivrant des certificats qualifiés de cachet électronique, et non sur le titulaire. D'autre part, elle n'oblige *a priori* ce prestataire qu'à pouvoir identifier la personne physique *représentante légale* de la personne morale qui fait la demande de certificats qualifiés de cachet électronique au nom de cette personne morale, et non toutes les personnes physiques bénéficiant d'une délégation de pouvoir spécifique au sein de cette personne morale.

Pour ces raisons, et à l'instar d'une obligation comparable prévue à l'article 8, § 3, de la loi du 9 juillet 2001, le second alinéa de l'article XII.26 du CDE prévoit également une obligation à

³⁶ En ce sens, voy. J.B. HUBIN, *op.cit.*, pp. 199 à 202.

charge de la personne morale établie en Belgique qui demande un ou plusieurs certificats qualifiés de cachet électronique. Ainsi, cette personne morale, titulaire du ou des certificats qualifiés de cachet électronique, est tenue de mettre en œuvre les mesures nécessaires (par exemple, en créant en interne et en mettant à jour une base de données sécurisée) afin de pouvoir établir le nom, la qualité et les pouvoirs de la personne physique qui représente la personne morale et qui fait pratiquement usage du cachet électronique qualifié. Grâce à cette obligation, le titulaire et, le cas échéant, les autorités administratives ou judiciaires compétentes qui agissent dans le cadre de la recherche et de la constatation d'infractions, peuvent établir l'identité et les pouvoirs de représentation de la personne physique pour chaque utilisation du ou des cachets. Afin d'assurer un traitement proportionné des données à caractère personnel ainsi qu'un maximum de sécurité juridique tant pour la personne morale que pour les tiers qui traitent avec cette personne morale, les travaux préparatoires précisent que « les données visées au second alinéa de l'article XII.26 ne sont accessibles qu'aux seules personnes visées dans cet alinéa, et en aucun cas aux tiers »³⁷.

Cette obligation consacrée par le second alinéa de l'article XII.26 du CDE est jugée fondamentale par le législateur. Pour s'en convaincre, on constate que ce dernier a prévu une sanction pénale particulière en cas de non-respect de cette obligation. Le nouvel article XV.123 du CDE stipule en effet que « Est puni d'une sanction du niveau 5, (...) quiconque aura commis une infraction aux dispositions de l'article XII.26, alinéa 2 », la sanction de niveau 5 étant l'avant dernière plus haute sanction consacrée par le Code de droit économique (amende pénale de 250 à 100.000 euros et emprisonnement d'un mois à un an ou d'une de ces peines seulement).

v. Clause de non-discrimination, obligation et présomptions légales (art. XII.25, §§ 4 à 8)

Les paragraphes 4 à 8 de l'article XII.25 du CDE consacrent des présomptions légales au profit des services d'archivage, d'envoi recommandé et d'horodatage électroniques qualifiés, ce qui devrait contribuer à leur utilisation, ainsi qu'une clause de non-discrimination au profit du service d'archivage électronique et une obligation de recourir à des services de confiance qualifiés dans certaines hypothèses bien définies.

a. Le principe de non-discrimination

Le quatrième paragraphe de l'article XII.25 du CDE vise à consacrer un principe de non-discrimination au profit du service d'archivage électronique, comme le règlement 910/2014 le fait déjà pour les autres services de confiance³⁸. A l'instar des dispositions européennes précitées, le paragraphe 4 stipule que « L'effet juridique et la recevabilité d'un archivage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet archivage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'archivage électronique qualifié ».

Ainsi, les services d'archivage électronique qui ne sont pas « qualifiés » parce qu'ils ne répondent pas à toutes les conditions du règlement, du titre 2 du livre XII et de son annexe I, ne

³⁷ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.18.

³⁸ Respectivement l'article 25.1. pour la signature électronique, l'article 35.1. pour le cachet électronique, l'article 41.1. pour l'horodatage électronique et l'article 43.1. pour l'envoi recommandé électronique.

sont pas pour autant privés de reconnaissance juridique. Toutefois, les documents issus de ces services ne bénéficient pas des présomptions prévues aux paragraphes 5 et 6 de l'article XII.25 du CDE. Celui qui recourt à ces services non qualifiés devra donc, en cas de contestation, prouver qu'ils présentent les qualités requises pour satisfaire à telle obligation légale ou réglementaire d'archivage ou que l'intégrité du contenu du document a bien été préservée. Les travaux parlementaires précisent par ailleurs qu'il « découle de ce principe de non-discrimination la confirmation qu'il est désormais possible de recourir à l'archivage au format électronique pour répondre à une obligation légale ou réglementaire d'archivage. L'archivage « papier classique » ne doit plus être le seul admissible »³⁹.

b. Les présomptions légales

En ce qui concerne les présomptions, le législateur en consacre deux types : une présomption irréfragable au profit des services d'archivage, d'envoi recommandé et d'horodatage électroniques qualifiés, et une présomption réfragable au profit du service d'archivage électronique qualifié.

Les premiers alinéas des paragraphes 5, 7 et 8 de l'article XII.25 du CDE consacrent une présomption irréfragable au profit des services d'archivage, d'envoi recommandé et d'horodatage électroniques *qualifiés*. Cette dernière consiste à affirmer que lorsqu'une loi ou un arrêté prévoit implicitement ou explicitement une « obligation de conserver certains documents ou données » ou une « obligation de recourir à un envoi recommandé », ou encore une « obligation de datation de documents ou de données », cette obligation légale ou réglementaire est présumée respectée, sans pouvoir en apporter la preuve contraire, si les documents et données ont été conservés au moyen d'un « service d'archivage électronique *qualifié*, tel que défini à l'article I.18,18° du CDE » ou d'un « service d'envoi recommandé électronique *qualifié* au sens du règlement 910/2014 », ou encore « si la date est établie au moyen d'un service d'horodatage électronique *qualifié* au sens du règlement 910/2014 ».

Le second alinéa du paragraphe 5 consacre une présomption réfragable au profit du service d'archivage électronique *qualifié*⁴⁰. Selon cette présomption, l'intégrité des données électroniques est préservée si celles-ci sont conservées au moyen d'un service d'archivage électronique *qualifié*⁴¹. Il est désormais possible de produire ces données, auprès d'un partenaire, de l'administration, voire en justice, sans devoir prouver qu'elles n'ont subi aucune modification au cours du processus d'archivage. En cas de contestation, la charge de la preuve est renversée,

³⁹ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.19.

⁴⁰ Une telle présomption réfragable ne devait pas être consacrée par le législateur belge pour les services d'envoi recommandé électronique *qualifié* et d'horodatage électronique *qualifié* car le législateur européen en consacre déjà une respectivement aux articles 43.2. et 41.2. du règlement 910/2014.

⁴¹ On note au passage que l'intégrité est une des garanties essentielles attendues du service d'archivage électronique (qu'il soit qualifié ou non). En effet, l'article I.18.17° du CDE définit le service d'archivage électronique comme un service qui consiste en la « conservation »... : « conserver » signifie au sens commun du terme maintenir un bien en bon état, le préserver de toute altération, garder la même qualité. La « conservation » implique donc, par nature, la garantie d'intégrité. Cette affirmation est confirmée indirectement à la page 18 de l'exposé des motifs qui indique que « Celui qui recourt à ces services [d'archivage électronique] non qualifiés devra donc prouver qu'ils présentent les qualités requises (...) et prouver que l'intégrité du contenu du document a bien été préservée ».

ce qui constitue un véritable avantage pour l'utilisateur d'un tel service : il appartient à l'autre partie qui conteste la réalité du maintien de l'intégrité de renverser la présomption.

Cette notion d'intégrité du document doit s'entendre raisonnablement d'un point de vue juridique. Ainsi, les travaux parlementaires précisent que « On ne tient donc pas compte des modifications de support ou de format qui sont nécessaires au bon déroulement du processus d'archivage électronique et au maintien de la lisibilité des données »⁴².

Le paragraphe 6 de l'article XII.25 du CDE et le nouvel alinéa de l'article 1334 du Code civil visent à apporter une solution au problème de l'insécurité juridique lié à la numérisation (scan) des originaux papiers. On le sait, l'une des raisons principales pour lesquelles les entreprises ou les administrations décident de recourir à un système d'archivage électronique est notamment la perspective de réduire l'espace de stockage physique occupé par les archives papiers au sein de l'organisation. De nombreuses entreprises et administrations poursuivent généralement l'objectif de pouvoir numériser tous les documents papiers, et les détruire ensuite, tout en ayant la certitude que leurs documents numérisés soient reconnus juridiquement. Or, de nombreuses législations exigent encore la conservation d'un document en original (papier), ce qui peut poser problème pour le document électronique issu d'une numérisation d'un document papier.

Afin d'apporter une solution à cette difficulté, le législateur belge consacre deux dispositions, qui doivent être lues en combinaison l'une avec l'autre. Celles-ci visent à permettre la numérisation de documents initialement sur papier et la destruction du support original (sous réserve de dispositions spécifiques contenues dans la loi du 24 juin 1955 relative aux archives), à condition que la numérisation se soit déroulée conformément à un processus fiable et sécurisé qui permette de garantir tant la fidélité de la copie que la conservation durable de celle-ci.

La première disposition, à savoir le paragraphe 6 de l'article XII.25 du CDE, énonce 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 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 ». Cette disposition permet de présumer que les scan des originaux papiers sont des copies fidèles et durables du document papier original dès lors que l'on recourt à un service d'archivage électronique *qualifié*, tel que défini à l'article I.18,18° du CDE et répondant aux conditions de cette disposition. Comme le confirme l'article 1334 du Code civil ci-après, cette présomption est réfragable : celui à qui on oppose la copie présumée fidèle et durable pourra donc tenter de démontrer qu'elle ne présente en réalité pas les qualités alléguées.

La seconde disposition insère un nouvel alinéa à l'article 1334 du Code civil⁴³ : « Lorsque le titre original n'existe plus, une copie numérique effectuée à partir de celui-ci a la même valeur

⁴² *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.19.

⁴³ Comme l'indique les travaux parlementaires, ce nouvel alinéa « s'inspire à la fois du droit français et du droit luxembourgeois, nos deux voisins ayant déjà adapté leur Code civil en vue de mieux prendre en considération, dans une certaine mesure, les copies numériques », *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.30.

probante que l'écrit sous seing privé, dont elle est présumée, sauf preuve contraire, être une copie fidèle et durable si elle a été réalisée au moyen d'un service d'archivage électronique qualifié conforme au livre XII, titre 2, du Code de droit économique fixant certaines règles relatives au cadre juridique pour les services de confiance ». Cette disposition élève la copie fidèle et durable au rang d'original, lui octroyant ainsi la même valeur probante, lorsque le document copié était à l'origine un acte sous seing privé et qu'il est recouru à un service d'archivage électronique *qualifié*.

Concernant ce nouvel alinéa de l'article 1334 du Code civil, on note les précisions suivantes apportées dans les travaux parlementaires :

« Cette disposition ne concerne que les copies d'actes sous seing privé. Le statut des copies numériques des actes authentiques devra être fixé dans le cadre juridique des actes authentiques électroniques, non visés par le présent projet de loi. Quant aux reproductions numériques des documents constituant des commencements de preuve par écrit, des présomptions ou des copies, il ne semble pas utile de leur conférer un statut particulier.

Cette disposition n'envisage que l'hypothèse où le titre original n'existe plus, autrement dit l'hypothèse où l'on a procédé à la numérisation de l'original pour le détruire ensuite et ne conserver que sa copie numérique. Autrement dit, si l'original subsiste, il primera sur la copie numérique, qui fera foi uniquement de ce qui est contenu au titre original, dont la représentation peut toujours être exigée (art. 1334, al. 1er, C. civ.) »⁴⁴.

On souligne enfin que les services d'archivage électronique, utilisés pour la numérisation de documents, qui ne sont pas « qualifiés » - parce qu'ils ne répondent pas à toutes les conditions du règlement 910/2014, du titre 2 du livre XII du CDE et de son annexe I - ne sont pas pour autant privés de reconnaissance juridique. Celui qui invoque ce document à la place du document original devra cependant établir qu'il s'agit d'une copie fidèle de ce document et qu'elle a été conservée dans des conditions de nature à assurer sa pérennité et le maintien de l'intégrité de son contenu. Cette preuve établie, le document sera admis au titre de copie ayant une valeur probante « améliorée » susceptible de convaincre plus facilement le juge. Les travaux parlementaires précisent toutefois que ce document « ne pourra cependant pas bénéficier de la valeur d'original que lui confère le second alinéa de l'article 1334 du Code civil »⁴⁵.

c. L'obligation de recourir aux services de confiance qualifiés dans certaines hypothèses

Le législateur belge consacre une disposition originale qui consiste en l'obligation, lorsque l'on décide de travailler dans un environnement électronique, de recourir à un service de confiance *qualifié* chaque fois qu'une formalité papier équivalente serait exigée de manière expresse dans la réglementation.

Ainsi, le troisième alinéa du paragraphe 5 de l'article XII.25 du CDE prévoit que lorsqu'une obligation de conservation (peu importe l'expression utilisée dans le texte conservation, archivage,...) est imposée de manière expresse par un texte légal ou réglementaire, il y a une

⁴⁴ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, pp.30 et 31.

⁴⁵ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p.21.

obligation de recourir à un service d'archivage électronique *qualifié*. Le second alinéa du paragraphe 7 du même article prévoit la même obligation de recourir à un service *qualifié* lorsqu'il existe une obligation légale ou réglementaire expresse de recourir à un envoi recommandé (peu importe l'expression utilisée dans le texte⁴⁶). Enfin, le second alinéa du paragraphe 8 consacre la même exigence lorsqu'une obligation de datation de données ou de documents (peu importe l'expression utilisée dans le texte) est imposée de manière expresse par un texte légal ou réglementaire.

A première lecture, cette obligation pourrait paraître surprenante. Mais après réflexions, elle semble s'intégrer harmonieusement dans notre système juridique actuel, et se justifier particulièrement au regard de notre régime probatoire et des finalités sous-jacentes à ce dernier.

Les travaux parlementaires motivent cette obligation comme suit : « L'analyse des textes permet de constater que chaque fois que le législateur ou le Roi exigent de manière expresse une obligation de conservation, [un envoi recommandé ou encore une obligation de datation de données ou de documents], cette exigence est motivée par un objectif de disposer de garanties élevées [respectivement] quant à la lisibilité dans le temps et à l'intégrité d'un document, [quant à la réalité et à la date de l'envoi et de réception d'un document ou encore quant à l'exactitude de cette date], et plus largement de sécurité juridique. Cette sécurité juridique profite tant à l'ensemble du système qu'aux parties, et en particulier à la partie faible (par exemple, un consommateur, un travailleur, etc.). Grâce aux présomptions dont il bénéficie, seul le service (...) *qualifié* permet de répondre de manière raisonnable et préalable (c'est-à-dire sans devoir recourir au juge) à cet objectif de sécurité juridique »⁴⁷. Ce faisant, on évite de mettre une partie utilisatrice de ces services de confiance en difficulté en cas de contestation.

La consécration d'une telle obligation « d'ordre formel » par le législateur belge est opportune. En effet, dans les nombreux cas où le législateur ou le Roi exigent de manière expresse une obligation de conservation, de datation ou d'envoi recommandé, l'objectif recherché est principalement de disposer de garanties non seulement élevées sur le plan de la sécurité juridique mais également équivalentes à celles offertes dans l'environnement papier⁴⁸. Cet objectif peut notamment être motivé par des raisons d'intérêt général, de protection de la partie faible ou

⁴⁶ Envoi recommandé, courrier recommandé, lettre recommandée (à la poste), etc. On rappelle par ailleurs que s'il est vrai que certaines dispositions légales ou réglementaires font encore explicitement référence à la notion de « courrier recommandé à la poste », l'article 7, § 2, de la loi du 13 décembre 2010 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges et modifiant la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, confirme désormais le principe selon lequel ces mots ne peuvent plus être utilisés ou interprétés pour faire obstacle ni à l'utilisation d'un envoi recommandé autre que physique (donc électronique), ni au recours à un prestataire d'envoi recommandé (physique ou électronique) autre que bpost (voir l'article 135, § 2 de la loi du 21 mars 1991).

⁴⁷ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, pp.19, 21, 22 et 32.

⁴⁸ On note d'ailleurs que cette tendance est déjà suivie par le législateur depuis des années dans le domaine de la signature électronique. En effet, de nombreuses dispositions légales – qu'il est impossible d'inventorier ici – exigent pour la conclusion de certains contrats ou l'accomplissement de formalités diverses, le recours à une signature électronique qualifiée ou un équivalent technologique sur le plan de la sécurité (signature via carte eID par exemple), sans que les parties ne disposent de la possibilité d'opter pour un mécanisme moins sécurisé de signature électronique dans le cadre de l'application de la clause de non-discrimination.

d'une partie tierce (qui peut notamment être l'Etat, soumis à un impératif de bonne gestion - opérationnelle et budgétaire -, et d'efficacité de ses contrôles, etc.).

Cette obligation est par ailleurs l'application du principe d'équivalence fonctionnelle, déjà consacré dans d'autres législations dont celle sur le commerce électronique (voyons particulièrement l'article XII.15, § 1^{er} du CDE). Comme nous l'expliquons ci-après, il est correcte d'affirmer que seul un service de confiance *qualifié* permet de préserver les qualités fonctionnelles de son équivalent papier. Ce faisant, on préserve également le système de preuve belge ainsi que la répartition traditionnelle de la charge de la preuve entre les parties, et on évite une distorsion de régime selon que les parties agissent dans le monde physique ou dans le monde électronique.

En effet, dans le monde papier, un acte sous seing privé (écrit signé de la main des parties), éventuellement archivé en original (c'est-à-dire en l'état), est considéré comme un « moyen de preuve parfait »⁴⁹, qui ne doit pas être complété par d'autres moyens de preuve et qui lie le juge. En cas de contestation de cet original, celui-ci est présumé avoir été rédigé et signé par le signataire ainsi identifié mais également être resté intègre. Ce moyen de preuve bénéficie de la recevabilité mais surtout de la force probante⁵⁰ et, en cas de contestation, l'utilisateur qui invoque ce moyen n'a pas la charge de la preuve⁵¹. Si on passe dans le monde électronique et que l'on utilise une signature électronique *qualifiée*, on bénéficie du même effet juridique (force probante et renversement de la charge de la preuve) grâce à la clause d'assimilation consacrée par l'article 25.2. du règlement eIDAS. Si on utilise un autre service de confiance *qualifié* (cachet, horodatage, envoi recommandé et archivage électroniques), on bénéficie également du même effet juridique (force probante et renversement de la charge de la preuve) grâce aux présomptions prévues au profit de ces services *qualifiés*.

Par contre, l'effet juridique est différent pour les documents ou formalités réalisées à l'aide de services de confiance *non qualifiés* (dont on rappelle qu'ils ne bénéficient pas d'une clause d'assimilation ou des présomptions). En effet, ceux-ci ne sont ni nécessairement considérés comme des moyens de preuve parfaits et ne bénéficient pas de la force probante (ils pourraient devoir être complétés par d'autres moyens de preuve afin de convaincre le juge). Tout au plus, bénéficient-ils de la clause de non-discrimination : le juge doit se donner la peine d'examiner le moyen de preuve mais il en apprécie librement sa valeur probante. Par ailleurs, en cas de contestation, il appartient à l'utilisateur du service de confiance *non qualifié* de prouver que ce dernier est réellement fiable (la charge de la preuve pèse sur ses « épaules »)⁵².

Dans ce contexte, on comprend que, sans l'obligation légale, les parties auraient pu opter pour un service *non qualifié* plutôt que *qualifié* lorsqu'elles œuvrent dans un environnement électronique. Or, laisser le choix à un consommateur ou un travailleur, par exemple, d'opter pour un service

⁴⁹ J.B. DENIS, « Quelques aspects de l'évolution récente du système des preuves en droit civil », *Rev. trim. dr. civ.*, 1977, pp. 673 ; D. MOUGENOT, *La preuve*, tiré à part du Répertoire Notarial, 4^{ème} édition, Larcier, Juin 2012, p. 73 ; D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001/7, n° 6000, p. 117.

⁵⁰ Pour la distinction entre valeur probante et force probante, voy. D. MOUGENOT, *La preuve*, tiré à part du Répertoire Notarial, 4^{ème} édition, Larcier, Juin 2012, pp. 84 à 86.

⁵¹ L'acte authentique et l'envoi recommandé bénéficient également de ces effets en tant que moyen de preuve.

⁵² Ce type de litige pourrait être long et coûteux, vu la nécessité de recourir à des experts.

non qualifié et lui laisser croire⁵³ qu'il peut bénéficier d'un moyen de preuve offrant la même sécurité juridique que son équivalent papier serait déraisonnable voire prêterait à confusion. De surcroît, s'ajoute le fait que ce consommateur ou travailleur se verrait contraint, suite à une simple contestation de l'autre partie (l'entreprise ou son employeur), d'aller en justice pour convaincre le juge que le moyen de preuve qu'il s'est constitué... est fiable, ce qui est un comble⁵⁴.

Sans l'obligation consacrée par le législateur belge, on devrait faire face à divers effets néfastes. On mettrait en péril notre système probatoire belge comme nous venons de l'expliquer. On ne respecterait pas le principe légal de l'équivalence fonctionnelle car l'équivalent électronique non qualifié n'offrirait pas les mêmes garanties fonctionnelles que la formalité papier. On créerait une discrimination juridique suivant que l'exigence légale expresse est assurée dans le monde physique (par exemple, un envoi recommandé physique bénéficie de la force probante)⁵⁵ ou dans le monde électronique (un envoi recommandé électronique non qualifié ne bénéficie pas de la force probante mais uniquement de la recevabilité, le juge restant libre d'apprécier sa valeur probante)⁵⁶. Enfin, on priverait tant les parties que les tiers bénéficiaires du respect de ces formalités de la sécurité juridique minimale acceptable (notamment l'administration qui doit par exemple pouvoir vérifier la certitude d'une date afin d'éviter que les parties n'antidatent un document).

Nous nous permettons même de pousser le raisonnement plus loin : si le législateur n'avait pas consacré cette obligation, nous aurions ouvert la porte à la possibilité de remettre en cause toutes les exigences légales d'ordre formel ou probatoire⁵⁷ qui sont motivées par les mêmes considérations d'intérêt général et de sécurité juridique. En effet, si on permet de recourir à un service de confiance *non qualifié* lorsque le législateur impose une telle formalité, on devrait assez logiquement aussi permettre aux parties de recourir à des écrits non signés, à des courriers postaux non recommandés, etc., laissant aux parties le soin de convaincre le juge en cas de contestation. Mais ce faisant, on perdait les nombreux bénéfices, particulièrement en terme de sécurité juridique, que nous apporte le système de preuve réglementée – apprécié de longue date dans nos pays civilistes – et on tomberait dans un système de preuve (totalement) libre, proche de celui connu en droit anglo-saxon.

⁵³ Vu la technicité et la finesse d'une telle distinction, on peut raisonnablement s'attendre à ce qu'une part importante de citoyens soit peu ou mal informée sur cette problématique et ses conséquences.

⁵⁴ On rappelle que le service *qualifié* bénéficie de présomptions car, pour pouvoir offrir un tel service, le prestataire doit respecter de nombreuses conditions strictes (notamment en termes de sécurité) consacrées par le législateur européen et belge. Ces conditions font l'objet d'un **contrôle approfondi et préalable** par un organisme d'audit accrédité ainsi que par l'autorité de contrôle. Le service *non qualifié*, par contre, ne fait pas l'objet de ces différents contrôles préalables. Cela ne signifie pas pour autant que la qualité de ce service est moindre. Toutefois, le seul moyen d'obtenir cette confirmation dépendra de la décision du juge dans le cadre d'un **contrôle a posteriori** en cas d'éventuelle contestation.

⁵⁵ On sait que les parties n'ont pas d'autres choix que de recourir à l'envoi recommandé tel que réglementé par la législation postale.

⁵⁶ Sans l'obligation légale, les parties auraient conservés le choix entre envoi recommandé électronique qualifié ou non qualifié.

⁵⁷ L'exigence générale de signature d'un document, de recourir à un envoi recommandé, de datation, d'utilisation d'un support durable, de publication de certains actes, etc..

D'aucuns pourraient également s'interroger sur la conformité au droit européen de cette obligation belge de recourir à un service de confiance qualifié dans les hypothèses précitées, particulièrement au regard du règlement 910/2014 et des clauses de non-discrimination consacrées par ce dernier.

Selon nous, cette exigence consacrée par le législateur belge, que l'on peut qualifier d'obligation « d'ordre formel », est expressément permise par l'article 2.3. de ce règlement qui stipule qu'il « n'affecte pas le droit national relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel ». Le législateur national conserve donc une liberté en ce domaine.

Un commentateur s'interroge récemment, certes avec toutes les nuances requises, sur la question de savoir si la clause de non-discrimination s'impose également au législateur national, auquel cas ce dernier violerait cette clause en imposant le recours à un service de confiance qualifié (au détriment des services non qualifiés), pour en conclure – de manière mitigée – que « le législateur doit en tout cas s'efforcer de respecter l'esprit de la règle »⁵⁸.

Notre opinion sur ce point est plus tranchée. A cet égard, il est nécessaire de bien comprendre la portée et les limites de la clause de non-discrimination.

Il convient en effet de rappeler que, historiquement (dans la directive de 1999), la clause de non-discrimination a été rédigée à une époque où on a essentiellement voulu indiquer que la signature n'était plus uniquement manuscrite (dans le cadre de l'environnement papier) mais devait pouvoir prendre une forme électronique. Par ailleurs, cette clause se limite à dire que l'effet juridique ou la recevabilité d'un service de confiance comme preuve en justice ne peuvent être refusés au seul motif qu'il est électronique ou non qualifié. Cette clause s'adresse au juge dans son pouvoir d'appréciation et lui dit : « *vous ne pouvez pas d'emblée rejeter un moyen de preuve au seul motif qu'il est électronique ou que le service de confiance n'est pas qualifié* », tout en laissant pour le reste la liberté totale au juge d'apprécier sa valeur probatoire et de considérer ainsi s'il fait preuve ou pas des engagements réellement pris entre les parties, du respect de l'intégrité ou de la réalité d'un envoi et de sa date. Le même raisonnement vaut donc pour tous les services de confiance (signature, cachet, horodatage, envoi recommandé et archivage).

Mais cette clause ne s'adresse pas au législateur et ne lui interdit donc rien. Ainsi, si le législateur exige, particulièrement pour les raisons légitimes évoquées plus haut et comme le lui permet l'article 2.3. du règlement 910/2014, un service de confiance *qualifié* comme condition de validité ou de preuve du contrat, d'une datation ou d'un envoi par exemple, cette exigence doit être respectée par les parties et par le juge. Dans ce contexte, si le juge rejetait un service de confiance *non qualifié*, ce ne serait pas au seul motif que ce service est électronique ou non qualifié mais au motif supplémentaire qu'il ne respecte pas l'exigence légale nationale formelle d'utiliser un service de confiance *qualifié* comme condition de validité ou de preuve du contrat, de la date ou de l'envoi.

⁵⁸ H. JACQUEMIN, « Principes applicables à tous les services de confiance et au document électronique » in L'identification électronique et les services de confiance depuis le règlement eIDAS, sous la direction de H. JACQUEMIN, Collection du Crids, Bruxelles, Larcier, Mars 2016, pp. 114 à 116.

Si on pousse à fond le raisonnement relatifs aux (prétendus) effets du principe de non-discrimination, et selon nous contestable, cela signifierait que le législateur ne pourrait pas exiger ou le juge ne pourrait pas admettre des catégories intermédiaires de signature électronique non qualifiées (très sécurisée mais où il manque une petite condition pour être qualifiée) au motif que cela discriminerait les signatures électroniques moins sécurisées voire totalement non sécurisées. Cela serait absurde et irait à l'encontre de l'esprit et l'objectif du règlement 910/2014 qui est de promouvoir la confiance, ce qui se fait essentiellement par l'augmentation de la fiabilité et de la sécurité.

On note enfin que la Commission européenne n'a émis aucune observation sur cette disposition belge dans le cadre de la notification officielle opérée conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information. Même si nous devons toujours rester prudent, on peut raisonnablement en déduire que la Commission européenne n'y a pas vu de difficultés au regard des textes européens, et en particulier de la clause de non-discrimination.

Pour terminer, il convient de préciser divers éléments permettant de bien comprendre la portée de cette obligation de recourir dans certaines hypothèses à un service de confiance qualifié. Cette obligation ne s'applique que si les trois conditions cumulatives suivantes sont remplies.

Tout d'abord, l'utilisateur doit opter pour la voie électronique. Ce dernier conserve toujours le choix de réaliser les formalités (archivage, datation, envoi recommandé) dans le monde papier ou électronique. Cela découle non seulement de l'article XII.25, §1^{er} du CDE déjà commenté mais également des mots « ...si l'utilisateur du service opte pour la voie électronique » que l'on trouve dans le troisième alinéa du paragraphe 5 et le second alinéa des paragraphes 7 et 8 de l'article XII.25 du CDE. En d'autres mots, il n'y a pas d'obligation absolue de recourir à un service de confiance électronique qualifié. Si une entreprise, une administration ou un citoyen considère que le recours à un service de confiance qualifié (archivage, horodatage, envoi recommandé) est trop complexe et/ou coûteux (ce qui n'est pas démontré à ce jour), il peut renoncer à la voie électronique et continuer à utiliser les équivalents papiers.

Ensuite, l'obligation n'existe que si « un texte légal ou réglementaire prévoit une exigence *expresse* » d'archivage, de recommandé ou de datation. Dans toutes les autres hypothèses, notamment celles où les parties souhaitent uniquement se ménager un moyen de preuve sans qu'un texte ne les y impose, les utilisateurs restent libres d'utiliser des services de confiance qualifiés ou non qualifiés. Le cas échéant, ces utilisateurs ne doivent pas perdre de vue les effets juridiques différents associés à ces services.

Enfin, par application du principe général de droit « *lex specialis derogat legi generali* », l'obligation ne s'applique que si une disposition légale ou réglementaire spécifique ne prévoit pas une autre solution. En effet, le troisième alinéa du paragraphe 5 et le second alinéa des paragraphes 7 et 8 de l'article XII.25 du CDE stipulent clairement que l'obligation s'applique « Sous réserve de l'application d'exigences légales ou réglementaires particulières ». Des

dispositions spécifiques, dans certains secteurs, peuvent donc permettre le recours à des services de confiance non qualifiés au sens du règlement 910/2014 et de la loi⁵⁹.

On note enfin que sur le plan de l'application opérationnelle de cette obligation, le législateur a fait preuve de prudence pragmatique. En effet, les travaux parlementaires précisent que « comme la mise en œuvre opérationnelle des services qualifiés dépendra tant de l'existence de normes internationales/européennes/nationales et des actes d'exécution de règlement 910/2014 que de l'offre de tels services sur le marché, l'entrée en vigueur de [cette obligation] pourrait être postérieure à celle de la plupart des dispositions du présent projet de loi (1er juillet 2016). (...) Ces dispositions n'entreront pas en vigueur en Belgique tant qu'il n'existe pas sur le marché belge et/ou européen une offre acceptable et opérationnelle de ces services de confiance qualifiés ainsi qu'une concurrence suffisante permettant de garantir un prix raisonnable »⁶⁰. Cette prudence du législateur a été suivie par le Roi. En effet, l'arrêté royal relatif à l'entrée en vigueur des dispositions de la loi du 21 juillet 2016⁶¹ prévoit expressément en son article 1^{er} que les dispositions de la loi entrent en vigueur le jour de la publication au Moniteur belge de l'arrêté (donc le 28 septembre 2016), à l'exception toutefois des articles XII.25, § 5, alinéa 3, § 7, alinéa 2, § 8, alinéa 2, XII.34 et XII.35 du Code de droit économique. L'entrée en vigueur de ces dispositions est reportée à une date ultérieure et indéterminée, cette dernière dépendant de la réalisation des conditions précitées.

vi. La lutte contre les affirmations trompeuses (art. XII.25, §§ 9 et 10)

Afin d'éviter que des prestataires sur le marché ne soient tentés de laisser croire que les services de confiance sont qualifiés alors que leurs services ne correspondent pas aux critères de qualité requis, le législateur a jugé opportun de consacrer une disposition qui stipule que « Un prestataire de service de confiance ne peut à aucun moment laisser entendre, directement ou indirectement, qu'il offre un service de confiance qualifié s'il ne se conforme pas aux dispositions du règlement 910/2014, du présent titre et de ses annexes, relatives à ces services » (art. XII.25, § 9).

On rappelle en effet qu'un prestataire ne peut pas offrir un service de confiance qualifié s'il ne répond pas à toutes les exigences du règlement 910/2014 et, le cas échéant, du titre 2 du livre XII du CDE et de ses annexes. Le législateur entend écarter tout risque de confusion à cet égard. Un prestataire qui offre à la fois des services de confiance qualifiés et non qualifiés (ce qui est permis par le règlement et la loi belge) pourrait par ailleurs intentionnellement faire une utilisation inadéquate du label de confiance (réservé aux services qualifiés) prévu par l'article 23

⁵⁹ Outre les références déjà citées à la note de bas de page 14, voy. notamment : Arrêté royal du 22 mars 1993 relatif à la valeur probante, en matière de sécurité sociale, des informations enregistrées, conservées ou reproduites par des institutions de sécurité sociale, *M.B.*, 1^{er} avril 1993 ; L'article 60, §5, al.4 du Code de la TVA ; L'article 315bis du Code des impôts sur les revenus.

⁶⁰ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 32.

⁶¹ Arrêté royal du 14 septembre 2016 fixant l'entrée en vigueur de la 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, *Moniteur belge*, 28 septembre 2016 ainsi que l'*erratum* publié au *Moniteur belge* du 06/10/2016, p. 68540.

du règlement 910/2014, ce qui aurait pour conséquence de laisser croire à l'utilisateur que tous ses services sont qualifiés⁶². La nouvelle obligation permet d'empêcher ces pratiques et poursuit l'objectif tant d'éviter de tromper la légitime confiance des utilisateurs que d'assurer une concurrence loyale entre les prestataires de services de confiance.

Dans le même esprit, le paragraphe 10 de l'article XII.25 du CDE indique 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 ».

La tentation pourrait en effet être grande pour un prestataire de service d'horodatage électronique (qu'il soit qualifié ou non) de recourir à la notion civiliste de « date certaine »⁶³, à laquelle sont attachés des effets juridiques particuliers, en vue de promouvoir son service. Or comme le précisent les travaux parlementaire, « l'article 1328 du Code civil ne confère date certaine qu'en trois hypothèses précises : la mort, l'enregistrement et la constatation dans des actes dressés par un officier public. Dès lors, en dehors de ces hypothèses, il n'est pas acceptable de dire que l'horodatage électronique puisse conférer date certaine »⁶⁴. Afin d'éviter des pratiques de publicité trompeuse et les allégations de mauvaise foi, la nouvelle loi interdit le recours à cette expression et permet d'éviter ainsi toute ambiguïté.

Cela n'empêche pas à terme, que la notion de « date certaine » évolue. A cet égard, les travaux parlementaires mentionnent que « La mention *sous la 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 »⁶⁵. Vu les conditions strictes ainsi que le régime de contrôle auquel est soumis un prestataire qualifié de service d'horodatage électronique qualifié, il semble acceptable de considérer que ce service qualifié permette de conférer « date certaine », même si son prestataire qualifié n'est pas un officier public au sens strict. Pour ce faire, il suffirait pour le législateur d'ajouter cette quatrième hypothèse à l'article 1328 du Code civil.

Les pratiques visées par les paragraphes 9 et 10 de l'article XII.25 du CDE sont bien évidemment trompeuses. Outre l'éventuelle application des règles relatives aux pratiques déloyales prévues par le livre VI du Code de droit économique, le législateur a estimé qu'elles devaient faire l'objet de sanctions pénales particulières. Ainsi, le nouvel article XV.123 du CDE énonce que « Est puni d'une sanction du niveau 5, 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 ou quiconque aura laissé entendre, directement ou indirectement, qu'il offre un service de confiance qualifié en violation de l'article XII.25, §9, ou quiconque aura laissé entendre, directement ou indirectement, que son service confère date certaine en violation de l'article XII.25, §10 (...) ». On rappelle que la sanction de niveau 5 constitue l'avant dernière

⁶² Pour plus d'informations sur ce label de confiance, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, p. 28.

⁶³ Sur cette notion, voy. D. MOUGENOT, *La preuve*, tiré à part du Répertoire Notarial, 4^{ème} édition, Larcier, Juin 2012, pp. 260 et s.

⁶⁴ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 24.

⁶⁵ *Ibidem*.

plus haute sanction consacrée par le Code de droit économique, prévoyant une amende pénale de 250 à 100.000 euros et un emprisonnement d'un mois à un an ou d'une de ces peines seulement.

vii. La matérialisation des signatures et cachets électroniques (art. XII.25, §§ 11 et 12)

Les paragraphes 11 et 12 de l'article XII.25 visent à permettre la matérialisation en toute sécurité juridique des documents établis par voie électronique et assortis, soit d'une signature électronique, soit d'un cachet électronique. Le paragraphe 11 reprend le contenu du paragraphe 6 de l'article 4 de la loi du 9 juillet 2001, moyennant l'adaptation des références, désormais faites aux dispositions du règlement 910/2014. Ce paragraphe 6 de l'article 4 de la loi du 9 juillet 2001 avait été introduit par la loi du 15 février 2012⁶⁶, adoptée de manière relativement inaperçue à l'époque. Il nous semble donc utile de rappeler le contexte et les objectifs poursuivis par cette loi.

La loi du 15 février 2012 s'inscrivait dans une perspective d'e-government, le législateur constatant que des administrations souhaitaient utiliser toute la palette des technologies de l'information et de la communication pour communiquer avec le citoyen et pour l'informer. Ainsi, certaines administrations communales notamment ont souhaité établir des copies et des extraits par voie électronique afin de les délivrer ensuite au citoyen, que ce soit sous forme électronique ou en version papier.

La matérialisation d'un document généré et signé électroniquement semblait toutefois encore poser problème. En effet, si la technologie permettant de matérialiser ces documents établis par la voie électronique est disponible, c'est-à-dire en les imprimant sans perdre la fiabilité technique du document électronique (on parle de « signatures hybrides »), il subsistait néanmoins une insécurité juridique quant à l'utilisation de ces techniques. La loi de 2012 entendait ainsi remédier à cette insécurité juridique.

Pour ce faire, le texte consacrait la possibilité de matérialiser une signature électronique pour autant que la signature sous forme matérialisée remplisse les mêmes conditions que celles applicables à la signature électronique avancée, telles que formulées à l'article 2, alinéa 2, 2°, de la loi du 9 juillet 2001. Selon les travaux parlementaires de la loi de 2012, les technologies utilisées pour la matérialisation de la signature garantissent le respect de ces conditions. Ces technologies « permettent, notamment par le biais d'un scanner, d'un lecteur à code-barres ou même d'un simple code de référence, apposé sur la copie, de demander le document numérique original revêtu de la signature numérique originale »⁶⁷.

Même si les travaux parlementaires laissent planer une certaine confusion sur ce point⁶⁸, il semble que le texte légal se limite uniquement à permettre juridiquement la matérialisation d'une signature électronique tout en fixant les conditions de cette matérialisation. Le résultat de cette matérialisation ne constitue ni plus ni moins qu'une « copie » au sens juridique⁶⁹. Cette copie

⁶⁶ M.B., 7 mars 2012.

⁶⁷ *Doc.parl.*, Chambre, 2010-2011, 53-1450/001, 11 mai 2011, p. 5.

⁶⁸ *Doc.parl.*, Chambre, 2010-2011, 53-1450/001, 11 mai 2011, p. 4.

⁶⁹ La formulation de la disposition initiale proposée précisait d'ailleurs « *Lors de la délivrance de copies ou d'extraits certifiés conformes, la signature du titulaire de certificat...* », ce qui semble envisager le cas particulier de

présente toutefois l'avantage de permettre d'accéder à tout moment, grâce au code de référence, au « document numérique *original* revêtu de la signature numérique *originale* » comme le confirme l'extrait des travaux parlementaires indiqués ci-avant⁷⁰. De là à dire que le résultat de cette matérialisation a la même validité que son original électronique, il y a un pas que nous ne franchirions pas, particulièrement si la signature électronique ainsi matérialisée est qualifiée⁷¹, à tout le moins sans une analyse approfondie préalable des technologies en question⁷². Si c'était le cas, on s'interrogerait sur la réelle valeur de ce document matérialisé, particulièrement si l'original électronique disparaissait.

On note que si la proposition de loi initiale ne concernait que les extraits et attestations communaux, il a été décidé d'élargir – via un amendement discuté et adopté⁷³ – le champ d'application de la disposition pour qu'elle puisse s'appliquer à la relation entre une entreprise privée et un citoyen, et de manière générale à l'ensemble du secteur public et privé⁷⁴.

La loi du 21 juillet 2016 reprend les mêmes principes que ceux consacrés par le législateur de 2012. Il adapte toutefois la terminologie en permettant, via le paragraphe 11, la matérialisation de la signature électronique et via le paragraphe 12, de manière identique, celle du cachet électronique.

B. Les exigences relatives au service d'archivage électronique (qualifié)

Pour rappel, une des spécificités de la loi du 21 juillet 2016 consiste à consacrer des dispositions inédites et originales visant à encadrer juridiquement le service d'archivage électronique (qualifié) en tant que service de confiance à part entière, ce que le règlement européen n'a pas réalisé. Pour ce faire, le législateur insère deux nouvelles définitions aux 17° et 18° de l'article I.18, du CDE ainsi que des dispositions particulières pour le service d'archivage électronique aux articles XII.27 à 29 du même code.

L'article I.18, 17° définit le « service d'archivage électronique » comme un « service de confiance supplémentaire à ceux visés par l'article 3, paragraphe 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, paragraphe 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 ».

la remise de copies ou d'extraits (ceux-ci fussent-ils certifiés conformes). Ces mots, qui expriment la volonté initiale des auteurs de la proposition, ont disparu lors de l'adoption de l'amendement visant à étendre la disposition au secteur privé, ce qui renforce la confusion quant à la réelle portée juridique de la disposition (confirmation légale de la possibilité de faire une (simple) copie permettant d'accéder facilement à l'original ou volonté du législateur d'octroyer à cette copie la même valeur juridique que l'original ?).

⁷⁰ A cet égard, nous sommes dans une hypothèse relativement comparable à celle de l'article 1334, alinéa 1^{er} du Code civil relatif aux copies : « Les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée ».

⁷¹ La disposition semble s'appliquer à toute forme de signature électronique, sans distinguer s'il s'agit d'une signature électronique qualifiée ou non.

⁷² Sur le plan des principes, il nous semblerait surprenant de reconnaître automatiquement à une signature électronique avancée (matérialisée) la même validité juridique que celle d'une signature électronique qualifiée.

⁷³ *Doc.parl.*, Chambre, 2010-2011, 53-1450/003, amendement, 28 juin 2011.

⁷⁴ *Doc.parl.*, Chambre, 2010-2011, 53-1450/004, rapport, 13 juillet 2011.

Le 18° du même article définit le « service d'archivage électronique *qualifié* » comme un « service d'archivage électronique fourni par un prestataire de services de confiance qualifié au sens de l'article 3, paragraphe 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 de e), i), j) et k) ».

Ces définitions méritent un mot d'explication. Elles enseignent que les services d'archivage électronique peuvent être soit fourni par un prestataire de services de confiance au profit du public soit exploité par un organisme du secteur public ou une personne physique ou morale pour son propre compte. Nous avons déjà commenté partiellement cette distinction *supra*⁷⁵, que nous complétons par le point suivant.

Cette distinction s'avère importante car seul l'archivage électronique qualifié « exploité pour son propre compte » bénéficiera de certaines dérogations prévues par l'article XII.28, § 2, du CDE. Il est donc nécessaire de pouvoir aisément la mettre en œuvre. Selon nous, un double critère pourrait être utilisé pour opérer la distinction entre service d'archivage électronique qui, d'une part, est offert par un prestataire de service de confiance *tiers* et d'autre part, est *exploité pour son propre compte* par un organisme du secteur public ou une personne physique ou morale. Le premier est celui de l'objet de l'activité principale. Le second est celui de l'existence d'un intérêt ou pas à l'égard des données ou du document archivés.

Concernant le premier critère, si l'activité principale de l'entreprise a pour objet le service d'archivage électronique lui-même⁷⁶, celle-ci sera considérée comme un prestataire de service de confiance qui offre ses services au public, et qui devra se soumettre à toutes les exigences du règlement 910/2014 et de la loi du 21 juillet 2016, particulièrement s'il est qualifié. Si par contre, le service d'archivage électronique n'apparaît que comme service "accessoire", qui vient en support de son activité principale qui est autre (par exemple, services bancaires, services d'assurances, secrétariat social, consultance en ressources humaines, entreprises pharmaceutique, etc), ce service pourra être considéré comme "exploité pour le compte propre".

Le second critère, cumulatif au premier, pose la question de savoir si l'organisation ou la personne, qui exploite le service d'archivage électronique pour son compte propre, est également une des parties ayant intérêt aux données ou documents archivés. Ce second critère pourrait se déduire de l'extrait suivant des travaux parlementaires : « On peut s'attendre à ce que, dans cette hypothèse, l'organisme du secteur public ou la personne qui exploite pour son propre compte le service d'archivage *veille particulièrement au respect des exigences dans la mesure où il ne peut pas se permettre de perdre le bénéfice des présomptions consacrées à l'article XII.25 pour les documents archivés dont il est partie* »⁷⁷. Si un prestataire prétend exploiter pour son propre compte un service d'archivage électronique qualifié, et ainsi revendiquer le bénéfice des

⁷⁵ Voy. les développements dans le point C. « Les objectifs et principes généraux applicables à l'archivage électronique » de la première partie de cette contribution.

⁷⁶ Cela pourra se déduire notamment de l'objet social de l'entreprise, de la manière dont elle présente ses activités à ses clients potentiels (via des communications ou publicités diverses), etc.

⁷⁷ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 26.

dérogrations prévues à l'article XII.28, §2, du CDE, mais que l'on constate qu'il n'a aucun intérêt – apprécié notamment par rapport à son activité principale – au regard des droits et obligations consacrés par les données ou documents ainsi archivés, il pourrait perdre le bénéfice des dérogations précitées et serait considéré comme un prestataire de service de confiance *tiers* pour cette activité (qui ne serait d'ailleurs plus nécessairement qualifiée d'accessoire par rapport à l'activité principale invoquée).

Les définitions des points 17° et 18° de l'article I.18, du CDE révèlent également que ces services peuvent être soit non qualifiés, auquel cas la grande majorité des dispositions du règlement et de la loi ne sont pas applicables, soit qualifiés, toutes les conditions légales européennes et belges devant alors être respectées.

Ces définitions se veulent neutres d'un point de vue technologique. Ainsi, elles laissent la porte ouverte à l'utilisation de toutes technologies ou autres services de confiance susceptibles d'assurer l'intégrité d'un document, tels une signature ou un cachet électroniques avancés ou qualifiés. Il ne faut pas perdre de vue que l'objectif de l'archivage électronique n'est pas uniquement d'assurer l'intégrité à un temps X mais plus largement de maintenir cette intégrité et d'en garantir la vérifiabilité pendant une durée parfois longue, ainsi que d'assurer la vérifiabilité de l'identité et la lisibilité dans le temps de ce document, et cela malgré les changements technologiques et des formats. Le maintien de ces garanties implique la mise en place de processus qui vont largement au-delà de la simple utilisation d'une signature électronique (avancée ou qualifiée) ou d'un cachet du même type. Le législateur européen en était d'ailleurs bien conscient, raison pour laquelle il a adopté l'article 34 du règlement relatif au « service de *conservation* qualifié des signatures électroniques qualifiées » (et l'article 40 pour le cachet électronique).

Par ailleurs, ces définitions assimilent les services d'archivage électronique et leurs prestataires à des services de confiance et à leurs prestataires au sens du règlement 910/2014. De la sorte, le législateur belge atteint l'objectif, déjà indiqué, de s'inscrire dans la philosophie, les principes et les procédures établis par ce règlement. On précise que cette assimilation « n'implique pas qu'un prestataire d'un service d'archivage électronique serait tenu d'offrir un ou plusieurs des services de confiance visés par le règlement »⁷⁸.

Les définitions précisent enfin qu'il existe deux catégories d'archivage : l'archivage électronique de données originellement électroniques et celui de documents papiers numérisés (scanning). La loi du 21 juillet 2016 donne ainsi la possibilité de prêter ou d'exploiter librement l'une ou l'autre de ces catégories d'archivage voire les deux.

Les articles XII.27 à 29 du CDE visent, à l'instar des autres services de confiance prévus dans le règlement 910/2014, d'une part, à distinguer les services d'archivage électronique qualifiés et non qualifiés et, d'autre part, à indiquer que les services d'archivage électronique sont soumis, par analogie, aux mêmes exigences que celles applicables à l'ensemble des services de confiance.

⁷⁸ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 13.

L'article XII.27 stipule que le prestataire de service d'archivage électronique *non qualifié* doit satisfaire aux dispositions du règlement applicables au prestataire de service de confiance non qualifié. En pratique, cela se traduit essentiellement en une obligation générale de sécurité et en une obligation de notification en cas d'atteinte à la sécurité, consacrées par l'article 19 du règlement 910/2014.

L'article XII.28 détermine les exigences applicables au prestataire de service d'archivage électronique *qualifié*.

En premier lieu, il doit se soumettre aux dispositions du règlement 910/2014 applicables aux prestataires de services de confiance qualifiés. Outre les obligations de sécurité visées à l'article 19 précité, ces dispositions visent principalement les exigences communes énoncées à l'article 24, l'obligation de se soumettre au contrôle de l'Organe visé à l'article 17 selon les modalités prévues à cet article et à l'article 20, l'obligation de passer préalablement par la procédure de lancement d'un service de confiance qualifié consacrée par l'article 21 (sous réserve de l'exception expliquée ci-après), l'obligation d'être inscrit sur la liste de confiance et, le cas échéant, le respect de l'article 34 relatif au service de conservation qualifié des signatures électroniques qualifiées⁷⁹.

Secondement, le prestataire doit se soumettre aux exigences prévues par le titre 2 du Code de droit économique (commentées *supra* et *infra*) ainsi que son annexe I. Cette dernière décrit les exigences essentielles auxquelles doivent satisfaire les prestataires de services de confiance établis en Belgique offrant des services d'archivage électronique qualifiés. Ces exigences, auxquelles nous renvoyons le lecteur, sont de nature organisationnelle et technique et ont pour but d'accroître la fiabilité du service. Un prestataire de services n'est pas tenu de respecter ces exigences mais n'a, s'il ne s'y conforme pas, pas le droit de demander le statut qualifié pour ses services et ceux-ci ne bénéficient pas des présomptions consacrées à l'article XII.25.

Concernant le service d'archivage électronique qualifié, nous rappelons que l'article XII.28 prévoit qu'il peut être soit fourni par un prestataire de service de confiance au profit du public, auquel cas il devra répondre à toutes les exigences précitées, soit exploité par un organisme du secteur public ou une personne physique ou morale pour son propre compte, auquel cas il n'est pas tenu de répondre à certaines exigences.

Le second paragraphe de l'article XII.28 dispense en effet cet organisme du secteur public ou personne qui exploite pour son propre compte le service de respecter certains exigences qui sont spécifiques à l'offre de services au public (24.2.a), d) et i) du règlement ainsi que points e), i), j) et k) de l'annexe I du titre 2). Il dispense également de se soumettre à la procédure préalable de lancement d'un service de confiance qualifié consacrée par l'article 21 du règlement, de l'audit tous les 24 mois visés par l'article 20.1. du règlement et de l'inscription sur la liste de confiance.

⁷⁹ Pour un commentaire de ces exigences, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 21 et s. ; Sous la direction de H. JACQUEMIN, *L'identification électronique et les services de confiance depuis le règlement eIDAS*, *op.cit.*.

Dans cette hypothèse et comme déjà indiqué, le législateur estime que « l'on peut s'attendre à ce que l'organisme du secteur public ou la personne qui exploite pour son propre compte le service d'archivage veille particulièrement au respect des exigences dans la mesure où il ne peut pas se permettre de perdre le bénéfice des présomptions consacrées à l'article XII.25 pour les documents archivés dont il est partie »⁸⁰. Cette dispense ne signifie pas pour autant l'absence de tout contrôle. En effet, le second paragraphe impose à l'organisme du secteur public et à la personne qui exploite le service de procéder à une déclaration préalable contenant diverses informations auprès de l'Organe de contrôle⁸¹, déclaration devant être accompagnée d'un rapport d'évaluation effectué par un organisme d'évaluation de la conformité accrédité. Sur cette base, l'Organe de contrôle peut toujours décider de procéder à un contrôle et, le cas échéant, constater que toutes les conditions ne sont pas remplies pour obtenir le statut « qualifié » et ainsi bénéficier des présomptions précitées.

Le troisième paragraphe de l'article XII.28 du CDE énonce que « Sans préjudice de l'article 34, paragraphe 2, du règlement 910/2014, le Roi peut déterminer les numéros de référence des normes applicables au service d'archivage électronique qualifié. Le service d'archivage électronique qualifié qui respecte ces normes est présumé satisfaire à tout ou partie des exigences du présent titre et de l'annexe I. Le cas échéant, le Roi spécifie les exigences présumées satisfaites ». Cette disposition s'inspire très largement des dispositions prévues dans le règlement 910/2014 pour les autres services de confiance. Elle consacre une faculté et non une obligation pour le Roi, faculté qui ne pourra être exercée que si les normes *ad hoc* sont élaborées sur le marché et que celles-ci permettent raisonnablement de répondre aux exigences légales, ce qu'il appartient au Roi de juger. Nous espérons néanmoins que cette faculté pourra être exercée rapidement, tant ces normes peuvent être utiles sur le plan de la gestion opérationnelle et du risque juridique (grâce à la présomption) pour les prestataires qui souhaitent offrir des services qualifiés.

Les travaux parlementaires précisent que « les mots *Sans préjudice de l'article 34, paragraphe 2, du règlement 910/2014* signifient que les éventuelles normes déterminées par le Roi doivent respecter les éventuelles normes déterminées par la Commission européenne. Le Roi peut donc déterminer librement les normes pour le service d'archivage électronique qualifié que si la Commission n'a pas exercé sa faculté visée à l'article 34, paragraphe 2, du règlement ou que pour les autres aspects relatifs à ce service non visés par l'article 34 précité (tels que les aspects liés à la numérisation) »⁸².

⁸⁰ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 26.

⁸¹ L'organe de contrôle est défini à l'article I.18,16°, du CDE comme « l'organe visé à l'article 17, paragraphe 1, du règlement 910/2014, créé au sein du Service public fédéral Economie, PME, Classes moyennes et Energie, composé des agents visés à l'article XV.2. et chargé des tâches de contrôle des prestataires établis en Belgique de services de confiance, y compris de services d'archivage électronique ». Cette définition poursuit un double objectif : affirmer, d'une part, que l'Organe de contrôle est constitué au sein du Service public fédéral Economie, PME, Classes moyennes et Energie, tout en laissant le soin au Ministre de désigner - conformément à l'article XV.2. du Code de droit économique - en son sein les agents chargé du contrôle (il s'agit des agents de la Direction générale Qualité et Sécurité) et, d'autre part, que cet Organe est chargé du contrôle des prestataires établis en Belgique non seulement des services de confiance visés par le règlement 910/2014 mais également des services d'archivage électronique visés par la loi, peu importe que ces derniers services soient offerts au public ou exploités en interne.

⁸² *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 26.

L'article XII.29 stipule que « L'article 13 du règlement 910/2014 s'applique au prestataire de service d'archivage électronique qualifié ou non en raison d'un manquement aux obligations prévues par le règlement 910/2014, le présent titre et son annexe I ». De la sorte, le législateur belge étend le régime de responsabilité déjà existant pour les prestataires de services de confiance visés dans le règlement 910/2014, aux prestataires de services d'archivage électronique qualifiés ou non⁸³.

C. Les exigences relatives au service d'envoi recommandé électronique qualifié

Le service d'envoi recommandé électronique est déjà en grande partie harmonisé par les articles 43 et 44 du règlement 910/2014⁸⁴. Mais comme nous l'avons déjà indiqué, le considérant n° 24 de ce règlement concède que les services de confiance visés par le texte européen ne sont pas (tous) complètement harmonisés, et qu'une certaine marge de manœuvre existe encore au niveau national. Le législateur belge ne s'est pas privé d'exploiter cette marge de manœuvre, avec parcimonie toutefois et la volonté évidente de ne pas imposer des contraintes inutiles à l'offre d'un tel service.

Ainsi, le premier alinéa de l'article XII.30. du CDE indique que « Sans préjudice des dispositions du règlement 910/2014 applicables au prestataire de services de confiance qualifié et au service d'envoi recommandé électronique qualifié, le prestataire de services de confiance qualifié qui offre un service d'envoi recommandé électronique qualifié satisfait aux exigences visées à l'annexe II du présent titre ». En réalité, cette annexe II ne contient pas d'exigences contraignantes supplémentaires à celles prévues par le règlement mais plutôt des dispositions qui complètent utilement celles consacrées par le texte européen en vue de permettre et d'encadrer l'envoi recommandé *hybride* utilisé dans le cadre d'un envoi recommandé électronique qualifié. Cette forme alternative et intermédiaire d'envoi recommandé, non visée par le règlement, offre la possibilité à un expéditeur d'envoyer son recommandé sous forme électronique tout en veillant à ce que le destinataire le reçoive sous enveloppe au format papier, suite à une matérialisation par un opérateur postal. Si, et seulement si car il ne s'agit pas d'une obligation⁸⁵, un prestataire décide d'offrir un tel service d'envoi recommandé *hybride*, alors il est tenu de respecter les exigences contenues à l'annexe II.

Ces exigences sont les suivantes :

- le prestataire remet l'envoi recommandé électronique matérialisé à un prestataire de services postaux, au plus tard le jour ouvrable suivant le dépôt par l'expéditeur de l'envoi

⁸³ Pour un commentaire de ce régime de responsabilité, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 33 et 34.

⁸⁴ Pour un commentaire du régime juridique européen applicable au service d'envoi recommandé électronique, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 41 et 44 ; C. VERDURE, « Règlement eIDAS : quelles nouveautés en matière d'horodatage et de recommandé électroniques ? » in *L'identification électronique et les services de confiance depuis le règlement eIDAS*, sous la direction de H. JACQUEMIN, Collection du Crids, Bruxelles, Larcier, Mars 2016, pp. 203 et s.

⁸⁵ Cette affirmation découle de la formulation du second alinéa de l'annexe II qui indique que « Le prestataire d'un service d'envoi recommandé électronique qualifié *peut*, à la demande de l'expéditeur, procéder à la matérialisation de l'envoi recommandé sous forme papier et à sa mise sous enveloppe ».

recommandé électronique qualifié, et informe l'expéditeur de la date à laquelle l'envoi a été physiquement déposé auprès de ce prestataire (afin que cet expéditeur puisse vérifier que ce délai du « jour ouvrable suivant » est bien respecté) ;

- en vue de respecter la législation postale, ce prestataire de services postaux doit être en possession d'une licence attribuée par l'IBPT ;
- la date figurant sur l'accusé d'envoi recommandé électronique est assimilée à la date du dépôt de l'envoi recommandé auprès d'un prestataire de services postaux, pour autant que l'envoi ne soit plus modifiable ni annulable par l'expéditeur. La date effective « du dépôt » est donc bien celle de l'envoi électronique, et non la date de remise de l'envoi recommandé électronique matérialisé au prestataire de services postaux. Cette assimilation poursuit l'objectif de "légaliser" cette date, et éviter toute contestation éventuelle, lorsque des textes légaux ou réglementaires (anciens) prévoient, dans une formulation désuète car pensée uniquement dans un contexte papier (et de monopole de la poste), qu'une formalité ou un acte est considéré comme accompli "à la date du dépôt de la lettre recommandée à la poste" ou une formulation équivalente ;
- comme cette date est importante pour les raisons que nous venons d'évoquer, la date figurant sur l'accusé d'envoi recommandé électronique doit également figurer sur ou dans l'envoi matérialisé ;
- le prestataire doit conserver les preuves de dépôt des envois auprès de l'opérateur postal pendant cinq ans ;
- le partage des responsabilités entre le prestataire d'un service d'envoi recommandé électronique qualifié et le prestataire de services postaux doit être spécifié à l'expéditeur dans les conditions du service d'envoi recommandé *hybride*.

Par ailleurs, le législateur consacre un second alinéa qui stipule que « Sans préjudice des normes éventuelles déterminées par la Commission conformément à l'article 44, paragraphe 2, du règlement 910/2014, le Roi peut fixer des exigences supplémentaires à celles visées à l'annexe II et déterminer les numéros de référence des normes applicables au service d'envoi recommandé électronique qualifié. Le service d'envoi recommandé électronique qualifié qui respecte ces normes est présumé satisfaire à tout ou partie des exigences du présent titre et de l'annexe II. Le cas échéant, le Roi spécifie les exigences présumées satisfaites ».

Cette disposition est comparable à celle déjà prévue pour le service d'archivage électronique qualifié (art. XII.28, §3). Le lecteur est donc renvoyé aux commentaires de cette dernière. Un petit ajout qui se matérialise par les mots « le Roi peut fixer des exigences supplémentaires à celles visées à l'annexe II » mérite toutefois l'attention. En consacrant cette faculté pour le Roi, on perçoit une volonté du législateur d'éviter d'imposer *a priori* des contraintes inutiles à l'offre d'un tel service – déjà en grande partie harmonisé par le règlement – mais également une certaine prudence à l'égard d'un service relativement nouveau qui pourrait nécessiter certains ajustements *a posteriori* si des difficultés venaient à apparaître, auquel cas le Roi pourra intervenir.

A cet égard, une première difficulté d'interprétation – qui pourrait le cas échéant déjà faire l'objet d'un « éclaircissement royal » au niveau de la Belgique, faute d'intervention éventuelle au niveau européen – est apparue concernant les points b) et c) de l'article 44.1. du règlement 910/2014. En effet, le point b) de cette disposition impose au prestataire de « garantir

l'identification de l'expéditeur *avec un degré de confiance élevé* ». Le point c) impose au même prestataire de « garantir l'identification du destinataire avant la fourniture des données » sans plus de précisions. La question se pose de savoir si l'identification du destinataire doit se faire avec un niveau de garantie équivalent, supérieur ou inférieur à celui de l'expéditeur ?

Dans l'attente d'un éventuel éclaircissement européen ou national, une réponse à cette question délicate, ne faisant l'objet d'aucune explication spécifique dans le règlement, est proposée. Cette tentative d'interprétation est d'autant plus difficile que cette disposition a fait l'objet de modifications dans les derniers jours de la négociation au niveau européen, sans qu'il n'y ait eu de discussions approfondies sur ce point.

Concernant la législation postale belge, l'arrêté royal du 24 avril 2014 portant réglementation du service postal donne par contre davantage de précisions quant à la distribution des envois « enregistrés » (c'est-à-dire notamment les envois recommandés). Ainsi, l'article 8 précise que le recommandé est remis « en échange de la signature du destinataire (...) moyennant vérification de l'identité de la personne qui le réceptionne ». La preuve de la vérification de l'identité est faite « par la capture manuscrite, photographique ou électronique du titre d'identité ou tout autre moyen de preuve jugé utile. La preuve de la vérification d'identité est conservée pendant minimum 13 mois par le prestataire de services postaux ». Certes, cet arrêté n'est applicable qu'aux envois recommandés « physiques » (belges) mais on ne voit pas ce qui justifierait que l'identification du destinataire se fasse de manière plus laxiste dans le cadre de l'envoi recommandé électronique qualifié que cela ne l'est dans le cadre du recommandé physique.

S'il est vrai qu'il n'existe pas d'arguments de texte dans le règlement 910/2014 qui permettent de répondre précisément à cette question, d'autres exigences légales issues d'autres textes, d'origine nationale et/ou européenne, permettent de constater que le prestataire devra tout mettre en œuvre pour garantir de manière efficace l'identification du destinataire avant la fourniture des données. Il s'agit particulièrement, et sans que cette liste soit exhaustive, du droit au "respect des communications" consacré par l'article 7 de la charte des droits fondamentaux de l'UE, du "secret des lettres" consacré par l'article 29 de la Constitution belge, de la législation relative à la protection des données à caractère personnelle (dont l'article 5 du règlement 910/2014 rappelle le respect) qui prévoit que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour assurer la confidentialité et la sécurité des traitements des données à caractère personnel.

Si l'identification du destinataire n'était pas vérifiée et garantie de manière sérieuse "avant la fourniture des données", le prestataire risquerait de remettre l'envoi recommandé électronique qualifié à une autre personne que le destinataire envisagé, et ainsi porter atteinte aux droits précités ("respect des communications", "secret des lettres", confidentialité et sécurité des traitements...). Même si le règlement 910/2014 laisse libre quant à la méthode d'identification du destinataire que le prestataire va mettre en place, nous ne pouvons que conseiller de recourir à une méthode offrant un haut niveau de fiabilité quant à l'identification. A cet égard, et même s'il ne s'agit pas du seul moyen possible, une identification/authentification via la carte d'identité électronique belge est certainement approprié.

On note enfin que dans la proposition initiale de règlement eIDAS, la Commission proposait d'utiliser les mots "identification univoque de l'expéditeur et du destinataire", et donc consacrait une exigence d'identification avec le même degré de fiabilité tant pour l'expéditeur que le destinataire⁸⁶.

D. De la révocation, de la suspension et de l'expiration des certificats qualifiés de signature électronique et de cachet électronique

Le règlement 910/2014 consacre des dispositions (articles 24.3., 24.4., 28.4. et 38.4.) relatives à la transparence concernant le statut d'un certificat qualifié ainsi que les effets d'une éventuelle révocation. Ainsi, il prévoit que les prestataires qui délivrent des certificats qualifiés de signature ou de cachet électroniques fournissent à toute partie utilisatrice des informations sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés⁸⁷. Toutefois, le règlement reste muet sur les cas dans lesquels un certificat qualifié peut être révoqué.

L'article XII.31 du CDE vise à compléter utilement les articles précités du règlement européen en spécifiant les différentes hypothèses dans lesquelles un prestataire de services de confiance qualifié qui délivre des certificats qualifiés de signature ou de cachet électroniques est tenu de révoquer un certificat qualifié.

Ainsi, ce prestataire est tenu de procéder à la révocation dans les cas suivants :

- le titulaire du certificat, préalablement identifié, le demande ;
- il existe des raisons sérieuses pour admettre que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité des données de création de signature électronique ou de cachet électronique a été violée ;
- les tribunaux ont ordonné des mesures consistant à interdire au prestataire de continuer à offrir ses services, tel que prévu à l'article XV.26, § 4, du CDE ;
- le prestataire de services de confiance qualifié arrête ses activités sans qu'il n'y ait reprise de la totalité de celles-ci par un autre prestataire de services de confiance qualifié garantissant un niveau de qualité et de sécurité équivalent ;
- le prestataire de services de confiance qualifié est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire, après avoir vérifié l'exactitude de cette information.

Si le prestataire de services de confiance qualifié révoque le certificat qualifié pour l'une de ces raisons, il « informe le titulaire de certificat de la révocation et motive sa décision, sauf en cas de demande, de décès ou de dissolution du titulaire de certificat ».

⁸⁶ Proposition de règlement du Parlement européen et du Conseil du 4 juin 2012 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (COM(2012) 238 final), disponible à l'adresse suivante : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:fr:PDF> (consulté le 01/10/2016).

⁸⁷ Pour un commentaire du régime juridique européen applicable à la révocation des certificats qualifiés, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 32 et 33.

L'article XII.32 du CDE spécifie les obligations à charge du titulaire de certificat en cas de doutes sérieux quant au maintien de la confidentialité des données de création de signature ou de cachet électronique (vol du code PIN ou de la clé privée de signature par exemple) ainsi qu'en cas d'arrivée à échéance ou de révocation d'un certificat qualifié de signature électronique ou de cachet électronique.

Le titulaire de certificat est défini par l'article I.18, 15°, du CDE comme « une personne physique ou morale à laquelle un prestataire de service de confiance a délivré respectivement un certificat de signature électronique ou un certificat de cachet électronique ». Cette notion n'est pas utilisée dans le règlement 910/2014. Elle fait néanmoins référence à deux services de confiance couverts par celui-ci (signature électronique et cachet électronique). Cette notion est utile dans le cadre de loi du 21 juillet 2016 pour de nombreuses dispositions qui mettent en œuvre ou complètent le règlement (utilisation d'un pseudonyme dans un certificat de signature électronique, utilisation d'un cachet électronique, hypothèse de la révocation des certificats comme évoqué ici, hypothèse de l'arrêt des activités par le prestataire).

Ainsi, l'article XII.32 stipule, d'une part, que « En cas de doutes sérieux quant au maintien de la confidentialité des données de création de signature électronique ou de cachet électronique ou de perte de conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat » et, d'autre part, que « Lorsqu'un certificat de signature électronique ou de cachet électronique est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut, après l'expiration du certificat ou après révocation, utiliser les données de création de signature électronique ou de cachet électronique correspondantes pour créer une signature électronique ou un cachet électronique ou faire certifier ces données par un autre prestataire de service de confiance ».

Quant au prestataire de service de confiance qualifié, l'article XII.32 du CDE prévoit une obligation à sa charge d'informer le titulaire d'un certificat qualifié de son expiration un mois avant celle-ci.

L'article XII.33 du CDE vise à garantir légalement une pratique déjà mise en place par les prestataires de services de confiance en Belgique : la suspension temporaire de certificat. Comme le souligne le considérant n° 53 du règlement 910/2014, la « suspension de certificats qualifiés est, dans un certain nombre d'États membres, une pratique opérationnelle établie des prestataires de services de confiance qui est différente de la révocation et entraîne une perte temporaire de validité d'un certificat ». Toutefois, le même considérant ajoute que « La sécurité juridique impose que le statut de suspension d'un certificat soit toujours clairement indiqué » et qu'il convient de « prévoir des règles en matière de transparence, dans les cas où cette pratique est disponible ».

C'est la raison pour laquelle un prestataire établi en Belgique est tenu – s'il met en place une telle procédure de suspension temporaire, ce que lui permettent le règlement et l'article XII.33 du CDE – de respecter les exigences contenues aux articles 28.5. et 38.5. Ces exigences se traduisent par le respect de deux conditions. D'une part, le certificat qualifié temporairement suspendu doit perdre sa validité pendant la période de suspension. D'autre part, la période de suspension doit clairement être indiquée dans la base de données relative aux certificats et le

statut de suspension doit être visible, pendant la période de suspension, auprès du service fournissant les informations sur le statut du certificat.

E. De la partie utilisatrice d'une signature électronique qualifiée ou d'un cachet électronique qualifié

Les articles XII.34 et 35 du CDE déterminent les effets juridiques liés à l'utilisation d'un *service de validation qualifié* d'une signature électronique qualifiée ou d'un cachet électronique qualifié. Si le règlement 910/2014 promeut la validation et l'offre de service de validation de signature électronique qualifiée et de cachet électronique qualifié, tout en déterminant les conditions dans ses articles 32, 33 et 40, il ne consacre par contre aucune obligation à charge de la partie utilisatrice de vérifier la signature ou le cachet. Comme le précisent les travaux parlementaires « Une telle obligation ne pourrait pas non plus être mise à charge de la partie utilisatrice par le droit national, au risque de créer une condition supplémentaire contraire au règlement 910/2014. Toutefois, rien n'interdit aux Etats membres de consacrer des dispositions qui visent à inciter la partie utilisatrice à procéder à la validation »⁸⁸.

Ainsi, les articles XII.34 et 35 prévoient que la partie utilisatrice - c'est-à-dire celle qui reçoit un document faisant l'objet d'une signature ou d'un cachet électronique de son auteur - bénéficie d'une présomption de validité de cette signature ou de ce cachet au sens des articles 32, 33 et 40 du règlement 910/2014 si elle vérifie cette signature ou ce cachet qualifié au moyen d'un service de validation qualifié conforme à ces articles. La disposition précise que cette présomption ne joue que si la partie utilisatrice procède à cette vérification avant de se fier à cette signature ou à ce cachet. En effet, si la partie ne vérifie pas la signature ou le cachet avant de s'y fier, et ne conserve pas la preuve de cette vérification, des contestations pourraient toujours naître par la suite, par exemple si le document signé l'avait été au moyen d'un certificat expiré, révoqué ou suspendu ou encore non qualifié, ce que le service de validation aurait dû détecter. Cette présomption permet en outre d'opérer un renversement de la charge de la preuve en cas de contestation.

F. De l'arrêt des activités d'un prestataire de services de confiance qualifié

Si on veut assurer la pérennité et la durabilité des services de confiance qualifiés et accroître la confiance des utilisateurs dans la continuité de ces services, le législateur pouvait difficilement éviter la problématique liée à l'arrêt éventuel des activités d'un prestataire de services de confiance qualifié et de consacrer des dispositions en vue de gérer au mieux ce risque potentiel.

Au niveau européen, le règlement 910/2014 n'élude pas la question mais se limite essentiellement à consacrer l'obligation de disposer d'un plan actualisé d'arrêt d'activité, afin d'assurer la continuité du service, et une sauvegarde des données (voyons les articles 17.4.i) et 24.2.h) et i) du règlement). Toutefois, le règlement ne dit rien sur le contenu et les modalités de mise en œuvre de ce plan d'arrêt d'activité, ce que les Etats membres sont en mesure de préciser en vue d'encadrer au mieux et de limiter au maximum les conséquences préjudiciables d'un arrêt.

⁸⁸ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, p. 28.

Les articles XII.36 à 38 du CDE visent à préciser les conditions et modalités de mise en œuvre du plan d'arrêt d'activité. Ces dispositions font une distinction entre l'arrêt volontaire et l'arrêt involontaire (par exemple, une faillite). Dans la première hypothèse, le prestataire doit en premier lieu tout mettre en œuvre pour tenter la reprise des activités dont il envisage la cessation par un autre prestataire de services de confiance qualifié. Si ce n'est pas possible, il doit alors en informer les utilisateurs et prendre des mesures spécifiques en vue de réduire au maximum le préjudice pour ces derniers et répondre aux obligations du règlement 910/2014. Dans tous les cas, il doit en outre informer l'organe de contrôle, qui pourra ainsi suivre de près ce processus délicat et veiller au respect scrupuleux des exigences européennes et nationales. Vu la technicité de ces dispositions, nous renvoyons pour le reste à la lecture de celles-ci.

G. L'organe de contrôle et ses pouvoirs

A l'instar de la directive 1999/93/CE, le règlement 910/2014 fait obligation aux Etats membres d'instaurer un système adéquat permettant de contrôler les prestataires de services de confiance, particulièrement s'ils sont qualifiés⁸⁹. Toutefois, le règlement va bien au-delà de la directive en consacrant une obligation pour les Etats membres de désigner un organe de contrôle ainsi qu'en précisant et en étendant le mandat de cet organe⁹⁰. Cette évolution traduit la volonté de la Commission et du législateur européen non seulement de renforcer mais également d'harmoniser plus largement le système de supervision, jugé trop « fragile » jusqu'à alors dans le cadre de la directive, notamment en raison de la trop grande liberté laissée aux Etats membres.

L'article 17 du règlement fait obligation aux Etats membres de désigner un organe de contrôle. Pour procéder à cette désignation, le règlement laisse le choix à l'Etat membre entre un organe de contrôle établi sur son territoire ou un organe de contrôle établi sur le territoire d'un autre Etat membre, moyennant l'accord préalable de cet autre Etat membre⁹¹. Pour rappel, le législateur belge a pris l'option d'instituer un organe de contrôle belge chargé de contrôler les prestataires établis en Belgique. Ainsi, l'article I.18,16°, du CDE indique que cet organe est créé au sein du Service public fédéral Economie, PME, Classes moyennes et Energie, et est composé plus particulièrement des agents de la Direction générale Qualité et Sécurité.

L'article 17 fait aussi obligation aux Etats membres de doter cet organe de contrôle des pouvoirs nécessaires et des ressources adéquates pour l'exercice de ses tâches. A cet effet, les articles 26 et 27 de la loi du 21 juillet 2016 insèrent dans le livre XV, titre 1er, chapitre 2, de CDE, une section 5 intitulée « Les compétences particulières en matière de recherche et de constatation des

⁸⁹ L'organe de contrôle est tenu de contrôler tous les prestataires de services de confiance, qu'ils soient qualifiés ou non. Toutefois, on rappelle que l'intervention de cet organe va sensiblement varier en fonction de la catégorie à laquelle appartient le prestataire contrôlé. Pour un commentaire des nombreuses tâches dévolues par le règlement européen à l'organe de contrôle, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*, pp. 26 à 33.

⁹⁰ Là où la directive consacrait seulement un point 3 dans l'article 3, le règlement consacre désormais 5 articles à la problématique du contrôle (17 à 21).

⁹¹ Cette seconde option pourrait être utile pour les petits EM n'ayant pas nécessairement les moyens de créer un tel organe de contrôle au niveau national, particulièrement si les prestataires sont peu nombreux. Lors des négociations au Conseil, certains (petits) EM avaient également proposé une troisième option qui consistait à mettre en place un système subsidiaire de contrôle au niveau européen, au profit des EM qui ne souhaitent pas assurer la supervision au niveau national, en avançant des arguments légitimes tels que l'harmonisation des contrôles, la réduction des coûts, l'augmentation de l'expertise et de l'efficacité. Cette proposition n'a toutefois pas abouti...

infractions au livre XII », section qui contient des compétences spécifiques applicables dans le cadre du règlement 910/2014 et du titre 2 du livre XII du CDE.

Ainsi, l'article XV.26 du CDE reprend en partie les dispositions relatives au contrôle de l'article 20 de la loi du 9 juillet 2001 tout en prévoyant que celles-ci complètent les nombreuses dispositions générales relatives au contrôle qui sont déjà contenues dans les chapitres 1 et 3 du titre 1er du livre XV du Code de droit économique ainsi que celles du règlement. Ces dispositions s'ajoutent notamment à la possibilité pour l'Organe de contrôle de retirer le statut qualifié conformément à l'article 20 du règlement 910/2014.

Plus particulièrement, l'article XV.26 du CDE prévoit que :

« §1^{er}. (...).

§ 2. (...). L'Organe de contrôle peut faire appel aux services d'un ou de plusieurs experts afin de l'aider dans sa mission de contrôle. Les experts désignés doivent être indépendants, financièrement et organisationnellement, par rapport aux prestataires de services de confiance.

§ 3. Lorsque l'Organe de contrôle constate qu'un prestataire de services de confiance établi en Belgique n'observe pas les exigences du règlement 910/2014, du livre XII, titre 2 ou de ses annexes, il le met en demeure et fixe un délai raisonnable, apprécié au regard de la nature et de la gravité du manquement, endéans lequel le prestataire de services de confiance doit avoir pris les mesures nécessaires afin de remédier à ces manquements.

§ 4. Si après l'expiration de ce délai, les mesures nécessaires n'ont pas été prises, le ministre ou son délégué peut :

- a) défendre au prestataire de services de confiance qualifié de continuer à offrir des services de confiance qualifiés et
- b) enjoindre au prestataire de services de confiance qualifiés d'informer immédiatement les utilisateurs de ses services de la perte du statut qualifié ou
- c) défendre, en application de l'article 17, paragraphe 3, point b) du règlement 910/2014, au prestataire de services de confiance non qualifié de continuer à offrir des services de confiance non qualifiés ».

H. Les sanctions (pénales)

L'article 16 du règlement 910/2014 fait obligation aux Etats membres de fixer « le régime des sanctions applicables aux violations du présent règlement. Les sanctions prévues sont effectives, proportionnées et dissuasives ». Au-delà de cette obligation européenne, le législateur a également consacré un régime de sanctions pour le non-respect des dispositions nationales insérées notamment dans le titre 2 du livre XII du Code de droit économique.

A cet effet, l'article 28 de la loi du 21 juillet 2016 insère un nouvel article XV.123 dans le CDE, qui consacre diverses sanctions pénales pour le non-respect d'obligations, déjà commentées plus haut, que le législateur belge juge comme fondamentales. Cet article stipule que « Est puni d'une sanction du niveau 5, 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 ou

quiconque aura laissé entendre, directement ou indirectement, qu'il offre un service de confiance qualifié en violation de l'article XII.25, § 9, ou quiconque aura laissé entendre, directement ou indirectement, que son service confère date certaine en violation de l'article XII.25, §10 ou quiconque aura commis une infraction aux dispositions de l'article XII.26, alinéa 2 ». On rappelle que la sanction de niveau 5 constitue l'avant dernière plus haute sanction consacrée par le Code de droit économique (amende pénale de 250 à 100.000 euros et emprisonnement d'un mois à un an ou d'une de ces peines seulement).

Nous précisons que les sanctions pénales consacrées par l'article XV.123 du CDE ne sont pas les seules sanctions susceptibles de frapper le prestataire qui ne respecterait pas les dispositions du règlement et de la loi belge. En effet, d'autres formes de sanctions sont déjà consacrées par l'application de dispositions existantes. Il s'agit notamment des règles générales du titre 1er, chapitres 1 et 3, du livre XV du CDE (notamment les règles d'avertissement et de publicité), du livre XVII du même Code (action en cessation, l'article XVII.22 prévoyant que cette action peut être formée à la demande de l'Organe de contrôle), de l'article XV.26 inséré par l'article 27 de la loi du 21 juillet 2016 commenté plus haut ainsi que de l'article 20.3. du règlement 910/2014 qui donne la possibilité à l'organe de contrôle de retirer le statut qualifié dans certaines conditions. La combinaison de ces différents jeux de sanctions permet de disposer de sanctions effectives, proportionnées et dissuasives en cas de non-respect des différentes dispositions du règlement et de la loi belge, comme le préconise le règlement.

I. Les dispositions modificatives et abrogatoires

La loi du 21 juillet 2016 contient de nombreuses dispositions modificatives, dont le premier objectif est d'opérer un toilettage des textes, sans nécessairement toucher au fond des dispositions. Ce toilettage vise à intégrer la nouvelle terminologie désormais harmonisée par le règlement européen ainsi qu'à tenir compte de l'abrogation de la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance⁹², remplacée par les nouvelles dispositions du titre 2 du livre XII du CDE.

A titre d'exemple, plusieurs dispositions du CDE (articles VII.78 et XII.15) sont modifiées en vue de remplacer le concept de signature électronique tel que défini à l'article 4, § 4, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification par celui de signature électronique *qualifiée* défini à l'article 3.12. du règlement 910/2014. Dans la même logique, l'article 135, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques a été modifié pour adapter les références au concept d'envoi recommandé électronique.

Par ailleurs, la loi du 3 juin 2007 portant des dispositions diverses relatives au travail⁹³ avait inséré dans la législation du travail un certain nombre de dispositions permettant de conclure des contrats de travail par la voie électronique. Cette législation faisait cependant référence à la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance en ce qui concerne l'archivage électronique des contrats, désormais rapportée par la loi du 21 juillet

⁹² M.B., 17 juillet 2007.

⁹³ M.B., 23 juillet 2007.

2016⁹⁴. Ainsi, les articles 35 à 44 contiennent des dispositions modificatives visant à aligner la législation du travail (qui exigeait le recours à un archivage électronique conforme à la loi du 15 mai 2007) sur les nouvelles dispositions insérées par la loi du 21 juillet 2016 (en exigeant désormais un archivage électronique qualifié conforme aux dispositions du livre XII, titre 2, du Code de droit économique).

Pour les législations qui n'auraient pas fait l'objet des modifications *ad hoc*, le législateur prévoit en son article 47 une clause transversale qui stipule que « Les lois ou arrêtés royaux existants qui font référence à la loi visée à l'article 32, 1^o [loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification] sont présumées faire référence aux dispositions équivalentes du règlement (UE) n^o 910/2014 (...) et aux dispositions équivalentes du livre XII, titre 2, du Code de droit économique telles qu'insérées par la présente loi ». Par exemple, lorsque le législateur exige dans une autre loi « une signature créée par la carte d'identité électronique » ou une « signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, visée à l'article 4, § 4, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification », il faut désormais comprendre qu'il s'agit de la « signature électronique qualifiée » visée à l'article 3.12. du règlement 910/2014⁹⁵.

Enfin, l'article 32 abroge la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, ainsi que son arrêté royal d'exécution du 6 décembre 2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés. Cette abrogation est logique car, d'une part, cette loi transposait en droit belge la directive 1999/93/CE, qui est elle-même abrogée par le règlement 910/2014 depuis le 1^{er} juillet 2016 et, d'autre part, les dispositions relatives à la signature électronique sont désormais consacrées dans le règlement, qui est d'application directe en droit national.

L'article 33 rapporte la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance. Cette loi n'a en effet jamais été d'application, faute d'arrêtés d'exécution. Le délai accordé au Roi pour prendre les arrêtés d'exécution nécessaires est expiré de longue date. Le règlement 910/2014 et la loi du 21 juillet 2016 contiennent désormais toutes les dispositions pertinentes en matière de services de confiance et peut donc remplacer intégralement la loi du 15 mai 2007 précitée.

⁹⁴ Rapporter une loi consiste à l'abroger avec effet rétroactif.

⁹⁵ *Doc.parl.*, Chambre, 2015-2016, 54-1893/001, 14 juin 2016, pp. 31 et 32.

Conclusion

Le législateur belge est un des premiers au niveau européen à avoir adopté la loi de mise en œuvre du règlement 910/2014, ce qui mérite d'être souligné.

Ce faisant, il apporte en temps opportun des réponses claires à diverses questions relatives aux « services de confiance » que le législateur européen avait laissé le soin de régler au niveau national. Ainsi, le législateur détermine précisément les sanctions applicables en cas de non-respect des dispositions du règlement et de la loi belge relatives aux services de confiance précités. Il désigne aussi officiellement l'organe de contrôle et détermine ses pouvoirs, organe qui va jouer un rôle essentiel dans la procédure de lancement des services de confiance « qualifiés », dans le contrôle des prestataires qui les offrent ainsi que pendant la période transitoire permettant aux prestataires qualifiés sous le règne de la directive de 1999 de se « régulariser ». Le même législateur profite de l'occasion pour faire le ménage et ainsi abroger la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ainsi que la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance.

Le législateur belge aurait pu rester prudent et se limiter à adopter les quelques dispositions techniques de mise en œuvre du règlement. Au contraire, ce législateur n'a pas manqué de tirer profit des marges de manœuvres laissées par le législateur européen et a pris la décision ambitieuse de consacrer au niveau belge un corps de règles complet et cohérent visant à encadrer juridiquement l'offre et l'utilisation des services d'archivage électronique (qualifiés) en Belgique. Cette initiative peut être saluée. En effet, lorsqu'on envisage la conclusion, la transmission et la conservation d'un acte juridique dans un processus électronique, il semble important de couvrir juridiquement la totalité des étapes du processus, en ce compris l'étape ultime qui consiste en l'archivage de l'acte, et pas uniquement sa signature, sa datation et son envoi. Avec la loi du 21 juillet 2016, le législateur encadre utilement et opportunément le dernier maillon de la chaîne, ce que le règlement européen n'a pas fait.

Les règles belges s'inscrivent dans les objectifs et la philosophie du règlement 910/2014. Elles reprennent les mêmes principes que ceux édictés par ce règlement pour les autres services de confiance (signature, cachet, horodatage, recommandé électroniques). Elles visent par ailleurs à couvrir tant l'archivage électronique de documents originellement électroniques que l'archivage électronique de documents papiers (dans le cadre d'une numérisation-scan).

Au-delà du régime original relatif à l'archivage électronique, la loi belge consacre également des dispositions relatives à l'envoi recommandé hybride, à la révocation, la suspension et l'expiration des certificats qualifiés de signature et de cachet électroniques, à la partie utilisatrice d'une signature électronique qualifiée ou d'un cachet électronique qualifié, à l'arrêt des activités d'un prestataire de services de confiance qualifié offrant un ou plusieurs services de confiance qualifiés et à la possibilité d'identifier une personne physique qui se cache derrière un pseudonyme ou un cachet électronique.

Les dispositions envisagées cherchent manifestement à atteindre un équilibre entre souplesse et sécurité. A l'instar du régime déjà applicable aux autres services de confiance dans le cadre du règlement 910/2014, le cadre juridique relatif à l'archivage électronique est envisagé comme une « boîte à outils juridiques » permettant aux utilisateurs de recourir à ce service en vue de gérer leurs risques par rapport principalement aux données ou documents présentant une valeur juridique. A cet effet, diverses présomptions sont prévues en faveur des services d'archivage électronique considérés comme « qualifiés » au sens de la loi ainsi qu'en faveur des autres services de confiance qualifiés au sens du règlement.

Cette « boîte à outils juridiques » étant désormais mise à la disposition de l'ensemble des acteurs du marché, gageons que ceux-ci en tirent profit intelligemment et prennent les actions utiles – chacun à son niveau – afin d'assurer, d'une part, une offre suffisante, concurrentielle et opérationnelle de ces services de confiance qualifiés et, d'autre part, une utilisation optimale dans le cadre de la politique de gestion des risques.

Didier GOBERT
Octobre 2016