Référence en cas de citation : D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », juin 2015, dossier publié sur le site www.caprioli-avocats.com.

Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie.

Didier GOBERT[1]

Résumé - Abstract

Après 15 ans d'application de la directive 1999/93/CE sur la signature électronique, le législateur européen a estimé que cette directive était insuffisante, suite au constat notamment que l'Union européenne ne disposait encore d'aucun cadre transnational et intersectoriel complet de nature à garantir des échanges électroniques sûrs, fiables et aisés, qui recouvre tant l'identification et l'authentification électroniques que les services de confiance autres que la signature électronique (cachet, horodatage, recommandé électroniques et authentification de site web).

Pour combler cette lacune, ce législateur a adopté le 23 juillet 2014 le règlement n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui abroge par la même occasion la directive 1999/93/CE.

Cette contribution propose une analyse approfondie des objectifs, principes et nouveautés consacrés par le récent règlement.

After 15 years of implementation of Directive 1999/93/EC on a Community framework for electronic signatures, the European legislator considered that this directive was insufficient, noting in particular that the European Union still had no comprehensive transnational and intersectoral framework such as to guarantee secure, reliable and easy electronic exchanges, covering both the electronic identification and authentication and trust services other than the electronic signature (seal, time stamp, electronic registered delivery service and website authentication).

To fill this gap, the legislator adopted, on 23 July 2014, Regulation N°910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

This contribution deeply analyses the objectives, principles and novelties enshrined in the recent regulation.

[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. 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 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[2]

Le développement des moyens de communication électronique représente une opportunité extraordinaire pour les entreprises et les citoyens soucieux d'utiliser des canaux de distribution rapides et des applications conviviales. Il en est de même pour les administrations qui souhaitent proposer leurs services publics en ligne tant au niveau national que transnational. Toutefois, il semble évident que le développement d'un climat de confiance constitue un préalable nécessaire en raison de certains risques potentiels relatifs notamment à l'identification et à l'authentification des parties, à la transmission ainsi qu'à la conservation de données personnelles et de documents électroniques, à l'intégrité et à la preuve de l'envoi et de la réception de ces derniers.

L'utilisation quotidienne d'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.

Afin d'assurer le développement durable du réseau des réseaux, plusieurs techniques permettent de gagner la confiance des utilisateurs d'Internet. Ces techniques impliquent parfois le recours à un tiers (autorité de certification, horodateur, archiveur, labellisateur, etc.), dont le métier est précisément d'intervenir afin de créer, d'une autre manière que dans l'environnement traditionnel, un contexte dans lequel les transactions peuvent s'opérer en toute confiance et de manière sécurisée. L'on voit ainsi se développer ce que certains ont baptisé – il y a 15 ans déjà – les « nouveaux métiers de la confiance »[3].

Dans ce contexte et ayant manifestement estimé que la confiance devait se mériter, le législateur européen avait déjà adopté en 1999 une directive déterminant le régime juridique applicable aux signatures électroniques et aux activités des prestataires de service de certification[4]. Cette directive a été transposée en droit belge par la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification[5].

Après 15 ans d'application, ce même législateur européen a estimé que cette directive était insuffisante, suite au constat notamment que l'Union européenne (ci-après UE) ne disposait encore d'aucun cadre transnational et intersectoriel complet de nature à garantir des échanges électroniques sûrs, fiables et aisés, qui recouvre tant l'identification et l'authentification électroniques que les services de confiance autres que la signature électronique.

Suite à ce constat, on comprend aisément que le législateur européen n'ait pas tardé à adopter le règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification

[2] Cette contribution est une version approfondie et mise à jour en juin 2015 de l'article « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution ? », publié dans la Revue du Droit des Technologies de l'Information (*R.D.T.I.*), 2014, n°56, pp. 27 à 51.

[3] M. ANTOINE, D. GOBERT et A. SALAÜN, « Le développement du commerce électronique : les nouveaux métiers de la confiance », *in Droit des technologies de l'information, regards prospectifs*, Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, pp. 3 à 32.

[4] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13/12 à 20 du 19 janvier 2000. Pour un commentaire de cette directive, voy. M. ANTOINE et D. GOBERT, « La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet ? », *J.T.D.E.*, avril 2000, n° 68, pp. 73 à 78 et E. CAPRIOLI, « La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques », *Gaz. Pal.*, 2000, pp. 5 à 17.

[5] *M.B.*, 29 septembre 2001, pp. 33070-33078. Pour un commentaire de cette loi, voy. 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. 83 à 172.

électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[6] (ci-après « le Règlement »), à peine plus de deux ans après que la Commission européenne ait publié sa proposition[7].

L'objectif principal de ce Règlement 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 que ce Règlement abroge la directive de 1999, il en reprend néanmoins la plupart de ses dispositions, moyennant quelques modifications, et complète celles-ci par de nouvelles dispositions relatives, d'une part, à la reconnaissance mutuelle au niveau de l'UE 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).

De toute évidence, ce Règlement peut être qualifié de texte ambitieux, qui va bien au-delà d'un simple toilettage de la directive de 1999 mais également au-delà, sur certains aspects, des propositions faites par la Commission en juin 2012. On peut d'emblée parler d'une évolution par rapport à la situation actuelle. Toutefois, est-ce à dire qu'il s'agit d'une révolution ? Nous tenterons de le découvrir au fur et à mesure de nos développements…

Dans un premier temps, nous présentons quelques considérations générales permettant de comprendre le contexte, les objectifs et les grands principes du Règlement. Une fois le contexte posé, nous analysons en profondeur le premier grand et nouveau volet du texte européen qui traite de l'identification électronique ainsi que le deuxième grand volet qui porte sur les services de confiance. Ensuite, nous évoquons quelques considérations relatives aux dispositions finales du Règlement afin de bien comprendre les différentes étapes de mise en œuvre de celui-ci. Enfin, nous terminerons par les marges de manœuvre dont disposent encore les Etats membres malgré le fait que le Règlement soit d'application directe.

I. Considérations générales

Avant de nous lancer dans l'analyse en profondeur des deux grands volets du Règlement, à savoir le premier relatif à l'identification électronique et le second portant sur les services de confiance, il nous semble utile de nous arrêter sur quelques considérations générales en vue de poser le contexte dans lequel l'initiative européenne s'inscrit, d'exposer les objectifs poursuivis, de justifier le choix de l'instrument juridique et enfin d'illustrer les points communs et différences majeures entre les deux volets du Règlement.

A. Les objectifs poursuivis par le Règlement

La lecture de l'exposé des motifs ainsi que de l'ensemble des considérants de la proposition de règlement déposée par la Commission en juin 2012 illustre à suffisance le contexte global dans lequel s'inscrit cette proposition mais également les nombreux objectifs poursuivis par celle-ci. On peut raisonnablement extraire de ceux-ci trois objectifs principaux et rassembleurs, que nous proposons de développer ci-après : lever les obstacles au fonctionnement du marché intérieur, susciter une confiance accrue dans les transactions électroniques, particulièrement transnationales, et renforcer la sécurité juridique lors de l'utilisation de moyen d'identification électronique et de services de confiance, qu'ils soient qualifiés ou non.

Derrière ces objectifs se cache la volonté de stimuler l'innovation et le développement de l'offre de services de confiance et d'identification électronique. Il ne faut donc pas sous-estimer les effets positifs

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

[7] 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

qu'une initiative législative peut engendrer en terme de création et de développement de nouveaux services sur le plan économique.

i. La levée des obstacles au fonctionnement du marché intérieur

L'article 1er du Règlement européen affirme sans ambiguïté le premier objectif poursuivi par celui-ci : assurer le bon fonctionnement du marché intérieur. La base juridique sur laquelle se fonde le Règlement, à savoir l'article 114 du Traité sur le fonctionnement de l'Union européenne, abonde dans le même sens. Cet article touche en effet à l'adoption des mesures législatives européennes rapprochant les dispositions législatives des Etats membres (ci-après EM) en vue d'éliminer les entraves au fonctionnement du marché intérieur.

A la suite de nombreuses études et consultations, la Commission a réalisé une analyse d'impact[8] des différentes options possibles lors de la préparation de la proposition de règlement. Cette analyse pointe les divers éléments qui sont à l'origine de la fragmentation du marché. Nous pouvons les synthétiser comme suit.

Dans le domaine de l'identification électronique, on constate de véritables problèmes d'interopérabilité transnationale. Ceux-ci sont notamment dû à l'existence de solutions différentes selon les EM pour l'identification des personnes (certificat d'authentification, token, login/mot de passe, etc ; certains EM, comme la Belgique, le Danemark et les Pays-Bas, utilisent un numéro unique pour identifier les personnes physiques, alors que d'autres refusent la création d'un numéro unique pour les personnes physiques, comme l'Allemagne et le Portugal[9]), au manque de sécurité juridique résultant de l'absence de reconnaissance transnationale des identifications électroniques ainsi qu'à des incertitudes quant à la responsabilité liée à l'exactitude des données d'identité. Et même lorsque certains EM tentaient de se coordonner de manière volontaire afin de lever ces difficultés, ceux-ci étaient confrontés à une complexité administrative pour mettre en œuvre une telle coordination au moyen d'accords bilatéraux ou multilatéraux, outre le fait que ces accords étaient conclus entre un nombre limités d'Etats.

En ce qui concerne les signatures électroniques, le niveau d'harmonisation apporté par la directive 1999/93/CE semble insuffisant vu le constat que les prestataires de services sont soumis en pratique à des règles différentes en fonction des EM dans lesquels ils offrent leurs services. Plus précisément, les problèmes suivants ont été recensés : des divergences dans la mise en œuvre au niveau national dues tant à des différences d'interprétation de la directive par les EM que à l'application non uniforme des normes techniques, le recours de fait à une dérogation pour les applications du secteur public qui avait pour conséquence de mettre en place des systèmes spécifiques au niveau national, des normes dépassées et des obligations mal définies en matière de contrôle donnant lieu à des problèmes d'interopérabilité transnationale, des différences dans les niveaux de fiabilité et des divergences sensibles dans la manière dont les contrôles étaient opérés.

Enfin, dans le cas des services de confiance associés à la signature électronique (cachet, horodatage et recommandé électroniques), certains EM ont adopté des législations nationales pour certains de ces services, ce qu'ils pouvaient faire vu l'absence de cadre juridique dans l'UE. Toutefois, il en résulte que les prestataires souhaitant proposer leurs services dans plusieurs EM doivent faire face à des coûts élevés pour respecter tant juridiquement que techniquement ces législations nationales, ce qui n'est pas souhaitable dans le cadre d'un fonctionnement optimal du marché intérieur.

La levée de ces différents obstacles grâce au Règlement devrait notamment permettre à l'avenir de s'acquitter de formalités administratives transfrontières de manière plus aisée et rapide, telles que l'inscription d'un étudiant par voie électronique dans une université à l'étranger, le dépôt en ligne par un

[8] Résumé de l'analyse d'impact accompagnant la proposition de règlement du 4 juin 2012 (SWD(2012) 136 final), disponible à l'adresse suivante : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012SC0136&from=FR

[9] Pour une analyse comparée de certains pays sur cette question, voy. http://www.senat.fr/lc/lc181/lc181_mono.html

contribuable de sa déclaration d'impôts dans un autre EM, l'accomplissement de formalités relatives à la santé par un patient à l'étranger voire la consultation de son dossier médical en ligne par un médecin étranger et éviter, le cas échéant, de refaire des examens ou analyses déjà effectués par le patient[10].

ii. Le renforcement de la confiance

Le second objectif principal poursuivi par le Règlement est sans nul doute la création des conditions concrètes visant à renforcer la confiance dans les échanges en ligne. Cet objectif s'avère à ce point important qu'il est exprimé dans l'intitulé du Règlement lui-même ainsi que dans les premières lignes de l'exposé des motifs de la proposition de la Commission : « Le présent exposé décrit le cadre juridique qui est proposé pour susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur. Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique. En effet, si les consommateurs, les entreprises et les administrations n'ont pas confiance, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services »[11].

Rappelons que la confiance dans les relations humaines ne constitue pas un acquis automatique ou un fait accompli ! Il s'agit d'un objectif que l'on tente généralement d'atteindre suite à un processus plus ou moins long, et qui se construit sur la base d'expériences plus ou moins heureuses. Comme dans les relations humaines présentielles, la confiance doit aussi se construire dans le monde virtuel. Mais les éléments qui sont pris en compte pour construire et « tester » cette confiance vont différer suivant que l'on se trouve dans le monde présentiel ou dans le monde électronique. En effet, il ne suffit pas de consulter un site web personnel ou encore de recevoir un courrier électronique ou un message sur un réseau social d'une prétendue personne pour que l'on puisse automatiquement considérer avec une relative certitude que cette personne existe, qu'elle est bien celle qu'elle prétend être et que celle-ci est digne de la confiance qu'elle réclame. Pour s'en convaincre, il suffit de constater le nombre de tentatives de « phishing » encore reçues chaque jour dans sa boîte de courriers électroniques[12], l'usurpation d'identité étant fréquente sur Internet. On ne s'étonnera d'ailleurs pas qu'un des services couvert par le Règlement est l'authentification de site web, service qui permet aux internautes de vérifier qu'ils ont effectivement accès au site Web du commerçant de leur choix et non à un éventuel site fantôme.

Comme le constate la Commission dans son analyse d'impact, « le manque de confiance dans les systèmes électroniques, dans les outils fournis et dans le cadre juridique peut donner l'impression que les garanties juridiques sont moindres que dans le cas d'une interaction physique »[13]. Dans la foulée, elle relève que les principales causes de ce problème sont le fait que le cadre juridique actuel est insuffisamment développé, le manque de coordination dans le développement et le contrôle des services offerts, le manque de transparence quant aux garanties de sécurité et le manque de sensibilisation des utilisateurs. La création d'un cadre juridique harmonisé, transparent et basé sur des mesures de sécurité d'un niveau élevé ainsi que la sensibilisation des utilisateurs pour les convaincre d'adhérer à ce projet commun devraient permettre de combler ces lacunes.

---

[10] Dans le domaine de la santé, des évolutions sont effet attendues suite à l'adoption de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (*J.O.U.E.*, 4 avril 2011). Cette directive instaure un réseau d'autorités nationales chargées de la santé en ligne. Pour assurer la sécurité et la continuité des soins de santé transnationaux, ce réseau est tenu d'établir des orientations concernant l'accès transnational aux données et services électroniques de santé, y compris en soutenant des " mesures communes d'identification et d'authentification, afin de faciliter la transférabilité des données dans le cadre de soins de santé transfrontaliers".

[11] Proposition du 4 juin 2012, *op.cit.*, p. 2.

[12] Pour plus d'informations sur cette notion, et d'une manière générale sur les différents types de spam, voy. « Le spamming en question : exemples illustrés et conseils pratiques », disponible à l'adresse suivante : http://economie.fgov.be/fr/binaries/spamming_in_question_fr_tcm326-42567.pdf

[13] Résumé de l'analyse d'impact, *op.cit.*, p.3.

Depuis plusieurs années, certains auteurs plaident la nécessité de légiférer sur les services de confiance tant au niveau national[14] qu'international[15] avec pour objectif premier de renforcer la confiance des utilisateurs. Dans son troisième avis relatif aux « Pistes pour renforcer la confiance dans le commerce électronique », l'Observatoire des droits de l'internet recommandait également d'élaborer un statut juridique pour les tiers de confiance[16].

Avec l'adoption du Règlement, l'Union européenne veut ainsi créer les conditions permettant de servir cette noble cause. Ce texte offre dès lors le cadre juridique donnant aux citoyens, entreprises et administrations la possibilité de bâtir et de tester cette confiance entre eux lors de leurs échanges sur le réseau des réseaux.

iii. Le renforcement de la sécurité juridique

Le troisième objectif principal poursuivi par le Règlement consiste à renforcer la sécurité juridique, au profit tant des prestataires de services que des utilisateurs de ces services. Comme l'évoque d'ailleurs le premier considérant du Règlement, l'amélioration de la sécurité juridique devrait contribuer au renforcement du climat de confiance[17].

En effet, on a constaté jusqu'à ce jour que le marché des services d'identification électronique ainsi que celui des services de confiance tendait à se développer, mais avec difficulté et un niveau de qualité variable. L'absence de cadre juridique complet et harmonisé entraîne plusieurs inconvénients. Tout d'abord, certains prestataires peu scrupuleux offrent des services insuffisamment fiables sur le plan technique et juridique, tout en laissant parfois croire – à tort – que leurs services répondent aux conditions légales. Ensuite, l'absence de critères minimaux et objectifs de qualité empêche les utilisateurs des services de déterminer quel prestataire est digne de confiance et, partant, de choisir un service apte à satisfaire leurs besoins. Cela crée en outre une situation de concurrence peu saine entre opérateurs « sérieux » et opérateurs plus « farfelus », ce qui met à mal l'innovation et le développement commercial de ces nouveaux services. Enfin, les juges risquent d'être confrontés à des questions épineuses relatives à la portée juridique de ces services, pour lesquels le droit commun s'avère souvent insuffisant.

Le Règlement entend apporter une solution à ces différents problèmes. Désormais, les règles applicables au sein de l'Union européenne seront les mêmes pour tous et d'application directe en droit national. Les prestataires et utilisateurs ne devraient généralement plus être confrontés à des différences entre les législations nationales[18], à des différences dans la qualité des contrôles ou à des spécificités nationales dans le domaine des services publics. Les EM sont tenus de reconnaître les moyens d'identification électronique notifiés conformément au Règlement. Ils sont également tenus d'accepter les services de confiance qualifiés et de leur reconnaître les effets juridiques consacrés par le Règlement. Les

[14] En ce sens, D. GOBERT, « Commerce électronique : vers un cadre juridique général pour les tiers de confiance », *R.D.T.I.*, avril 2004, n° 18, pp. 33 à 56 ; F. COPPENS, « Le recours aux 'tiers de confiance' dans les transactions en ligne – Paiement, signature, recommandé et archivage électronique », *J.T.*, n° 6500, 40-41/2012, pp. 810 à 813 ; P. VAN EECKE, « Nouvelle législation sur les services de confiance en préparation », *Bull. Ass.*, 2013/5, pp. 113 à 130.

[15] En ce sens, E. CAPRIOLI, « Gestion des identités numériques : quel cadre juridique pour la confiance dans les communications électroniques internationales ? », *R.D.T.I.*, n° 45/2011, pp. 29 à 67.

[16] Observatoire des droits de l'internet, avis n° 3, « Pistes pour renforcer la confiance dans le commerce électronique », Juin 2004, pp. 21 à 23, disponible à l'adresse suivante : http://www.internet-observatory.be/internet_observatory/pdf/advices/advice_fr_003.pdf

[17] Considérant n°1 : « Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social. En effet, si les consommateurs, les entreprises et les administrations n'ont pas confiance, *notamment en raison d'un sentiment d'insécurité juridique*, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services » et considérant n° 14 : « Le présent règlement vise à établir un cadre cohérent en vue de fournir des services de confiance d'un niveau de sécurité et de sécurité juridique élevé ».

[18] Comme nous le verrons dans la suite des développements, une nuance doit être apportée à cette affirmation dans la mesure où, pour certains services de confiance, les Etats membres peuvent prévoir des conditions supplémentaires au niveau national, pour autant toutefois que ces dernières ne portent pas préjudice à l'interopérabilité transfrontière.

prestataires de services vont pouvoir déployer leurs activités au sein du marché unique dans des conditions de concurrence loyales et équitables, le Règlement jouant le rôle de filtre qui va permettre de séparer « le bon grain de l'ivraie ». Cette sécurité juridique va en outre leur garantir une relative prévisibilité, qui constitue souvent une condition essentielle dans la décision d'investissement d'un opérateur économique.

Le renforcement de la sécurité juridique ne profite pas uniquement aux relations transfrontières mais joue également au niveau national. En effet, comme nous le verrons par la suite, le chapitre 3 du Règlement relatif aux services de confiance harmonise les conditions à respecter pour pouvoir offrir des services de confiances « qualifiés » et déterminent les effets juridiques privilégiés, en l'occurrence des présomptions, reconnus à ces services.

Précisons d'emblée que le Règlement ne souffle mot sur les hypothèses dans lesquelles une identification, une signature, une datation ou un envoi recommandé seraient requis juridiquement[19]. Il s'agit d'une prérogative des EM. Par contre, si une telle exigence est posée par le droit national, le Règlement indique comment on peut concrètement satisfaire à cette exigence lorsqu'on exerce ses activités dans un environnement électronique. En conséquence, les utilisateurs pourront désormais bénéficier des effets du Règlement non seulement pour leurs transactions transfrontières mais également pour leurs relations intra-nationales. Ce texte s'avèrera particulièrement utile pour les EM ne disposant jusqu'alors d'aucune législation en ce domaine.

B. Le choix du règlement comme instrument juridique

En 1999, le législateur européen a privilégié la directive pour réglementer la signature électronique et les prestataires de service de certification. Le choix du règlement pour remplacer et compléter cette directive pourrait donc surprendre. Pourtant, et même si on constate une tendance de la Commission européenne à recourir de plus en plus souvent au règlement plutôt qu'à la directive ces dernières années, ce choix n'est pas le fruit du hasard.

En effet, la Commission européenne explique dans son analyse d'impact qu'elle a envisagé tous les scénarios possibles et comparé les avantages et inconvénients respectifs[20], pour en conclure que « Le règlement est considéré comme l'instrument juridique le plus approprié. De par son applicabilité directe, conformément à l'article 288 du TFUE, un règlement limitera le morcellement juridique et fournira une plus grande sécurité juridique en instaurant un ensemble harmonisé de règles essentielles contribuant au fonctionnement du marché intérieur »[21].

On ne dévoilera pas un secret en précisant que lors des négociations, l'option du règlement a rapidement fait l'objet d'un accord, hormis l'une ou l'autre intervention isolée au début des discussions manifestant la préférence de principe pour une directive.

Le choix du règlement nous semble judicieux. D'un point de vue juridique, il permet une harmonisation plus poussée et évite les divergences tant d'interprétation juridique que dans la manière d'opérer les contrôles. D'un point de vue opérationnel, il force les EM et prestataires à coopérer plus efficacement en

[19] C'est en ce sens que l'article 2.3. indique que « Le présent règlement n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel ».
[20] La Commission a en effet évalué, d'une part, les options qui consistent à règlementer au moyen soit d'un instrument (qui couvre à la fois l'identification et les services de confiance) soit de deux instruments (à savoir une décision de la Commission sur l'identification électronique et une révision de la directive sur les signatures électroniques) et, d'autre part, les options qui consistent à règlementer au moyen soit d'une directive (qui se limite à lier les États membres quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens) soit d'un règlement (qui a une portée générale, est obligatoire dans tous ses éléments et directement applicable dans tous les États membres), voir résumé de l'analyse d'impact, *op.cit.*, pp. 6 à 8.
[21] Proposition du 4 juin 2012, *op.cit.*, p. 4.

vue de résoudre les problèmes actuels d'interopérabilité technique et de veiller ainsi à ce que les systèmes nationaux – qui sont parfois différents – puissent « se comprendre et se parler ».

Une conséquence fondamentale du choix du règlement, conséquence qui découle de l'effet direct de cet instrument juridique, réside dans le fait que ce dernier peut nécessiter des actes d'exécutions pour sa mise en œuvre. Ces actes d'exécution sont bien entendu adoptés au niveau européen, et non au niveau national. En l'occurrence, le Règlement prévoit l'adoption de nombreux actes d'exécution (obligatoires ou optionnels) pour assurer sa mise en œuvre (notamment pour les listes de confiance, les organes de contrôle, les organismes d'évaluation de la conformité, les différents services de confiance, etc.).

On notera au passage que dans la version de la proposition de la Commission, cette dernière avait proposé un savant dosage entre les mesures pouvant être prises par un acte délégué et celles pouvant être prises par un acte d'exécution.

La différence entre ces deux instruments est fondamentale. Pour l'acte délégué, le pouvoir donné à la Commission est considérable car cette dernière peut décider seule du contenu de cet acte, celui-ci entrant automatiquement en vigueur 2 mois après que la Commission l'ait notifié aux Parlement et Conseil européens, pour autant que ceux-ci n'émettent aucune objection dans ce délai[22]. Pour l'acte d'exécution par contre, l'exercice de la compétence d'exécution par la Commission est strictement encadré afin de permettre aux EM de rester associés à l'élaboration de ces actes. En effet, le règlement n° 182/2011 définit les règles relatives au contrôle de l'exercice des compétences d'exécution de la Commission[23]. Ce contrôle s'effectue au travers des procédures de « comitologie » : la Commission doit soumettre chaque projet d'acte d'exécution à des comités composés de représentants d'EM dans le cadre de la procédure d'examen consacrée par les articles 3 et 5 de ce règlement.

Bien conscients de la différence entre ces deux types d'actes, de nombreux EM ont exprimé le souhait lors des négociations que le recours aux actes délégués soit le plus réduit possible et, le cas échéant, que le mandat de la Commission soit explicitement défini quant aux objectifs, au contenu, à la portée et à la durée de la délégation de pouvoir. Ce souhait a été suivi d'effets puisque le texte adopté ne contient plus… qu'un acte délégué[24] alors qu'il en comptait seize dans la proposition initiale ! Quant aux actes d'exécution, les EM ont veillé à ce que ceux-ci ne portent plus sur des éléments essentiels – qui ont été inscrits dans le Règlement lui-même – mais se limitent à préciser certains détails techniques (détermination des formats ou numéros de standards techniques par exemple).

C. Les deux grands volets du Règlement : l'identification électronique et les services de confiance

S'il est vrai que le Règlement compte six chapitres, les deux chapitres vedettes sont sans nul doute le second chapitre relatif à « l'identification électronique » et le troisième chapitre relatif aux « services de confiance », tant ils contiennent des nouveautés substantielles dans ces deux domaines. Les quatre autres chapitres (qui portent respectivement sur les dispositions générales, les actes délégués, les actes d'exécution et les dispositions finales) contiennent des dispositions « secondaires », essentiellement au service des deux « plats principaux » du menu précités.

Avant de nous concentrer plus précisément sur le contenu de ces deux volets du Règlement, il nous semble utile d'évoquer les points communs mais également les différences entre ceux-ci pour bien comprendre que si les chapitres deux et trois du Règlement sont liés, il restent néanmoins distincts. La Commission a d'ailleurs étudié l'option qui consistait à règlementer ces deux aspects par le biais de deux instruments juridiques distincts voire de règlementer un aspect mais pas l'autre, pour néanmoins conclure

[22] Article 47.
[23] Règlement (UE) n° 182/2011 du Parlement Européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission, *J.O.U.E.*, 28 février 2011, pp. 13 à 18.
[24] Prévu à l'article 30.4.

que « Le recours à un seul instrument pour établir un cadre complet garantirait la cohérence des mesures législatives concernant les différents aspects des eIAS. L'existence de deux instruments distincts pourrait être à l'origine de disparités dans les dispositions juridiques adoptées pour les signatures et l'identification électroniques et, surtout dans l'approche des initiatives »[25].

Ces deux chapitres présentent des points communs, qui peuvent être décrits notamment par les éléments suivants.

Premièrement, l'identification électronique constitue un des aspects de la signature électronique. En effet, une fonction importante de la signature réside dans l'identification du signataire : signer (électroniquement) un document, c'est notamment – mais pas uniquement – s'identifier (électroniquement) en tant qu'auteur de ce document[26]. D'un point de vue pratique et technologique, il n'est d'ailleurs pas toujours facile pour un non initié de distinguer ces deux fonctionnalités (s'identifier et signer). Pour illustrer cette affirmation, on prendra l'exemple de notre carte d'identité électronique belge. La puce de cette carte contient en réalité deux certificats : un certificat d'authentification et un certificat de signature[27]. La technologie sous-jacente à ces certificats (infrastructure à clé publique) ainsi que les applications logicielles pour les utiliser sont les mêmes. Pourtant, la portée juridique liée à l'utilisation de ceux-ci est différente : le certificat d'authentification ne devrait en principe être utilisé que comme clé d'accès à un service en ligne car sa seule finalité est de permettre la vérification et la validation de l'identité. Alors que le certificat de signature devrait quant à lui être utilisé pour engager juridiquement la personne concernée, c'est-à-dire non seulement l'identifier en qualité d'auteur du document (fonction d'identification de la signature) mais également lui permettre de manifester son consentement au contenu de celui-ci (fonction d'adhésion de la signature).

Une seconde similitude réside dans le fait que les deux chapitres du Règlement reposent sur un équilibre entre systèmes volontaires, d'une part, et conséquences obligatoires, d'autre part.

En effet, le second chapitre, qui consacre la reconnaissance mutuelle au niveau de l'UE des moyens d'identification électronique notifiés, ne prévoit aucune obligation pour les EM ni d'introduire ou d'utiliser au niveau national un moyen d'identification électronique ni de notifier à la Commission un tel moyen en vue d'une utilisation transnationale[28]. Par contre, si un EM décide (librement) de notifier dans les conditions du Règlement un (ou plusieurs) moyen d'identification électronique, le Règlement consacre, d'une part, une obligation pour tous les autres EM d'accepter ce moyen d'identification électronique notifié et, d'autre part, une obligation pour l'EM notifiant de fournir un moyen d'authentification en ligne afin de permettre la vérification des données d'identification électronique.

De la même manière, le troisième chapitre relatif aux services de confiance ne consacre, pour les EM ou pour les prestataires, aucune obligation de fournir des services de confiance, qualifiés ou non, et si ceux-ci existent, de les utiliser[29]. Par contre, si un prestataire décide (librement) de fournir un ou plusieurs services de confiance, il a l'obligation de se conformer aux conditions du Règlement[30], particulièrement s'il s'agit de services qualifiés. De plus, un utilisateur de ces services doit pouvoir bénéficier des effets

[25] Résumé de l'analyse d'impact, *op.cit.*, p.8.
[26] Pour un commentaire sur les fonctions de la signature, voy. notamment 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. 43 à 81 ; B. DE GROOTE, « Het bewijs in de elektronische handel – Enkele bedenkingen », *A.J.T.*, 2001, pp. 881-901 ; M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels*, Larcier, septembre 2014, 646 pages ; H. JACQUEMIN, *Le formalisme contractuel : Mécanisme de protection de la partie faible*, Larcier, janvier 2010, 592 pages.
[27] Pour plus d'informations, voy. le contenu du lien suivant : http://economie.fgov.be/fr/consommateurs/Internet/eGovernment/carte_identite_electronique/.
[28] En ce sens, voy. le considérant n°13.
[29] En ce sens, voy. le considérant n°21.
[30] Ce principe doit toutefois être tempéré par un élément important car, comme nous le verrons *infra*, le règlement ne s'applique pas aux services utilisés exclusivement dans des systèmes fermés d'utilisateurs.

juridiques reconnus par le Règlement à chacun des services de confiance qualifiés et non qualifiés et les juridictions nationales sont tenues de reconnaître ces effets juridiques[31].

Une troisième similitude entre les deux chapitres touche à la volonté de promouvoir, comme le confirme l'article 1er du Règlement, un niveau élevé de fiabilité, nécessaire à la concrétisation de l'objectif de renforcement de la confiance[32]. En effet, l'obligation de reconnaissance mutuelle des moyens d'identification électronique notifiés ne portent que sur ceux qui offrent un niveau de garantie « substantiel » ou « élevé », mais pas « faible »[33], tout comme une clause d'assimilation ou des présomptions de respect de garanties bénéficient aux services de confiance « qualifiés » mais pas aux services de confiance « simples ou non qualifiés »[34].

Mais ces deux chapitres se différencient aussi par les éléments suivants.

Tout d'abord, le chapitre deux se limite essentiellement à établir les conditions de reconnaissance mutuelle et d'interopérabilité des moyens d'identification électronique notifiés dans une perspective d'utilisation transfrontière de ceux-ci. Alors que le chapitre trois va plus loin dans l'harmonisation des règles, dès lors que celles-ci sont applicables non seulement à l'utilisation des services de confiance au niveau transfrontière, mais également à leur utilisation au niveau national. La Commission indique d'ailleurs que « l'identification électronique ne peut être abordée, dans le règlement proposé, de façon générique comme les autres services de confiance électroniques car la délivrance des moyens d'identification est une prérogative nationale. La proposition est donc axée sur les aspects strictement transnationaux de l'identification électronique »[35].

Ensuite, et même si les cloisons ne sont pas totalement étanches entre secteurs public et privé, le chapitre deux se focalise principalement sur l'utilisation des moyens d'identification électronique pour accéder à un service en ligne fourni par un organisme du secteur public au sein des EM. Ce chapitre s'inscrit donc dans une perspective de facilitation de mise en place du « gouvernement électronique ». Les destinataires de ce chapitre sont en première ligne les acteurs publics. Le troisième chapitre par contre peut être assimilé à une boîte à outils qui est mise à la disposition tant des administrations publiques pour le déploiement de leurs applications de gouvernement électronique que des acteurs du secteurs privés pour le développement du commerce électronique « Business to Business », « Business to Consumer » voire « Consumer to Consumer ». Les destinataires de ce chapitre sont tant les acteurs publics que privés. En pratique, il est même fort probable que les prestataires de services de confiance qualifiés seront essentiellement des acteurs privés.

Une dernière différence fondamentale entre les deux chapitres réside dans le mécanisme de contrôle. Le chapitre relatif à l'identification électronique ne prévoit aucun mécanisme de contrôle. Outre le fait que les niveaux de garantie « substantiel » et « élevé » sont privilégiés, le législateur européen table sur le fait que les EM ne devraient pas prendre le risque de notifier un moyen d'identification électronique « fantaisiste », ou à tout le moins à la légère, car cette notification est réalisée sous leur responsabilité et un tel moyen ne peut être notifié que pour autant qu'il soit déjà utilisé au sein de l'EM notifiant pour l'accès à au moins un service public. A l'inverse, le chapitre trois instaure un mécanisme de contrôle approfondi pour les prestataires de services de confiance, particulièrement si les services offerts sont qualifiés, auquel cas le contrôle s'exercera *a priori* mais également *a posteriori*. Comme nous le verrons plus loin, il s'agit d'ailleurs d'une évolution substantielle consacrée par le Règlement.

Les différents éléments du décor étant posés, il est temps d'approfondir le contenu des deux grands volets du Règlement.

---

[31] Voy. *infra*.

[32] Voy. notamment les considérants n° 28, 44, 48 et 72.

[33] Le considérant n°19 affirme d'ailleurs d'une manière générale que « La sécurité des schémas d'identification électronique est la clé pour assurer la fiabilité de la reconnaissance mutuelle transfrontalière des moyens d'identification électronique ».

[34] Voy. *infra*.

[35] Proposition du 4 juin 2012, *op.cit.*, p. 4. En ce sens, voy. également le considérant n°12 du règlement.

II. Le volet relatif à l'identification électronique

Pour rappel, de nombreux États membres disposent déjà d'un schéma d'identification électronique, mais ces systèmes diffèrent sur de nombreux points[36]. L'absence de base juridique commune pour la reconnaissance entre les EM ainsi que l'insuffisante interopérabilité transnationale des identifications électroniques nationales constituent des obstacles qui empêchent les particuliers, les entreprises et les administrations de profiter pleinement du marché unique numérique.

Dans ce contexte, un des objectifs du Règlement est donc de lever les obstacles existants à l'utilisation transnationale des moyens d'identification électronique employés dans les EM à des fins d'authentification, au moins pour les services publics. Cet objectif rappelé, voyons maintenant les mesures consacrées par le Règlement pour le réaliser.

A. L'obligation de reconnaissance mutuelle et l'obligation de fournir un moyen d'authentification

Il nous semble opportun de rappeler que le Règlement ne prévoit pas d'obligation pour les EM d'introduire ou d'utiliser au niveau national un moyen d'identification électronique. Il ne consacre pas non plus d'obligation de notifier à la Commission, si un ou plusieurs de ces moyens sont utilisés au niveau national, ce(s) moyen(s) en vue d'une utilisation transnationale[37]. La notification au niveau européen d'un moyen d'identification électronique utilisé au niveau national est donc volontaire.

Malgré le caractère volontaire de la notification, le risque qu'aucun EM ne procède à cette notification, auquel cas le Règlement resterait lettre morte, paraît cependant faible. On peut en effet s'attendre à ce qu'une bonne majorité des Etats de l'Union européenne joue le jeu de la notification, dont notamment les Etats qui sont partenaires du projet européen STORK[38]. Par effet d'entraînement, le pari repose sur l'espoir que les autres EM, attentistes dans un premier temps, suivent le même mouvement.

Si un EM décide de notifier (volontairement) dans les conditions du Règlement un moyen d'identification électronique, cela génère – comme nous l'expliquons ci-après – une obligation à charge de deux parties : une obligation pour les autres EM mais également une obligation pour l'EM notifiant.

Pour ce qui concerne les autres EM, l'article 6 du Règlement qui consacre le principe de reconnaissance mutuelle fait peser sur eux l'obligation d'accepter le moyen d'identification électronique notifié par un EM pour accéder à un service en ligne fourni par un organisme du secteur public de ces EM. Cette obligation de reconnaissance mutuelle est toutefois sujette à plusieurs conditions consacrées par cet article.

Premièrement, la législation ou les pratiques administratives de l'EM qui offre le service public en ligne doivent exiger une identification électronique[39] à l'aide d'un moyen d'identification électronique et une

[36] Nous utiliserons indifféremment le terme « schéma » ou « système » dès lors que le concept de « *schéma* d'identification électronique » est défini par l'article 3, 4) comme un « *système* pour l'identification électronique… ».

[37] L'article 7 indique en effet que « Un schéma d'identification électronique est *susceptible* de notification… ». En ce sens également, voy. le considérant n°13.

[38] Le projet européen STORK, dont 18 Etats membres sont partenaires parmi lesquels la Belgique, a pour objectif de mettre en place une plateforme d'interopérabilité des eID au niveau européen en vue de permettre aux citoyens de réaliser des transactions transfrontières simplement en utilisant son eID nationale (la carte d'identité électronique belge par exemple). Pour plus d'informations sur ce projet, voy. https://www.eid-stork.eu/.

[39] L' « identification électronique » est définie par l'article 3, 1), du règlement comme « le *processus* consistant à *utiliser* des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ».

authentification[40] de celle-ci pour un accès à ce service en ligne. L'identification électronique consiste à utiliser les données relatives à l'identité, donc à montrer qui est une personne, alors que l'authentification consiste à vérifier ces données d'identité, donc à vérifier et confirmer que cette personne est bien celle qu'elle prétend être. Il résulte de cette première condition que si un EM permet un accès libre à un service public en ligne, cet EM n'est pas obligé de soumettre cet accès à une identification électronique et à une authentification, et encore moins à reconnaître les moyens d'identification électronique notifiés par les autres EM…au demeurant non nécessaire pour l'accès à ce service.

Deuxièmement, l'obligation de reconnaissance mutuelle ne pèse qu'à l'égard des moyens d'identification électronique qui sont notifiés à la Commission européenne et qui figurent sur une liste publiée par cette dernière au Journal Officiel de l'Union européenne. Selon l'article 9, la liste des premiers schémas notifiés sera publiée le 18 septembre 2016. A partir du 18 septembre 2015[41] et jusqu'au 18 septembre 2018, les EM peuvent reconnaître les systèmes déjà notifiés mais uniquement sur une base volontaire[42]. Tous les systèmes notifiés après le 18 septembre 2016 devront être publiés, sous forme d'adaptation de la première liste publiée, dans les deux mois qui suivent la date de réception de la notification[43].

Troisièmement, l'obligation de reconnaissance mutuelle est conditionnée au niveau de garantie (qui peut être faible, substantiel ou élevé)[44] tant du moyen d'identification électronique que de celui exigé pour l'accès au service public en ligne qui nécessite une identification[45]. En effet, le niveau de garantie du moyen d'identification électronique devant être reconnu doit correspondre à un niveau égal ou supérieur à celui requis pour accéder au service public en ligne (article 6.1.b). En pratique, ce niveau de garantie doit être au moins « substantiel » car le Règlement exige que l'accès au service public en ligne utilise le niveau de garantie « substantiel » ou « élevé » (article 6.1.b et c). Cela signifie que si un EM exige le niveau « substantiel » pour l'accès à son service public, il doit accepter les moyens d'identification électronique notifiés de niveau « substantiel » mais aussi de niveau « élevé ». Par contre, si ce même EM exige le niveau « faible » pour l'accès à son service, il n'est pas tenu d'accepter un moyen d'identification électronique notifié de niveau supérieur (« substantiel » ou « élevé »)[46]. Dans la même

[40] L' « authentification » est définie par l'article 3, 5), du règlement comme « un *processus* électronique qui permet de *confirmer* l'identification électronique d'une personne physique ou morale (…) ».

[41] Voy. l'article 52.4.

[42] En effet, selon l'article 52.2.c), l'obligation de reconnaissance mutuelle commence à s'appliquer trois ans après la date d'application (le 18 septembre 2015) des actes d'exécution visés à l'article 8, paragraphe 3 et à l'article 12, paragraphe 8, soit le 18 septembre 2018.

[43] Notons que l'article 9.4. prévoit la possibilité pour un EM de soumettre à la Commission une demande, que l'on espère exceptionnelle, visant à retirer de la liste publiée au *JOUE* le schéma d'identification électronique qu'il a notifié. Le cas échéant, la Commission publie cette modification à la liste dans le mois qui suit la date de réception de la demande de l'État membre.

[44] Ces trois niveaux de garantie consacrés par le Règlement sont définis à l'article 8. Cet article détermine également les critères qui doivent être pris en compte lors de l'adoption des actes d'exécution qui préciseront les modalités concrètes et techniques nécessaires à la mise en œuvre de ces niveaux. Comme l'indique le considérant n° 16, les niveaux de garantie caractérisent « le niveau de fiabilité d'un moyen d'identification électronique pour établir l'identité d'une personne, garantissant ainsi que la personne revendiquant une identité particulière est bien la personne à laquelle cette identité a été attribuée. Le niveau de garantie dépend du niveau de fiabilité que le moyen d'identification électronique accorde à l'identité revendiquée ou prétendue d'une personne en tenant compte des processus (par exemple, preuve et vérification d'identité, et authentification), des activités de gestion (par exemple, l'entité délivrant les moyens d'identification et la procédure de délivrance de ces moyens) et contrôles techniques mis en œuvres ». L'article 8.2. précise en outre que, pour les trois niveaux, à savoir faible, substantiel ou élevé, l'objectif poursuivi est respectivement 'réduire le risque, réduire substantiellement le risque ou empêcher' l'utilisation abusive du moyen d'identification électronique ou l'altération de l'identité.

[45] En pratique, les trois niveaux de garantie correspondant aux niveaux 2, 3 et 4 du projet STORK (voy. le considérant n°16). Le certificat d'authentification présent sur la carte d'identité électronique belge correspond au niveau de garantie « élevé », ce qui est le niveau le plus sécurisé parmi ceux visés par le Règlement.

[46] Cela découle de l'article 6.1.c). Cette affirmation pourrait surprendre car sur le plan de la sécurité, qui exige le moins devrait être en mesure d'accepter le plus. Mais ce choix du règlement est probablement dicté par des

logique, un EM n'est pas non plus tenu de reconnaître un moyen d'identification électronique notifié de niveau « faible ». Mais il pourrait le faire sur une base volontaire[47]. Dans le même sens, un EM n'est pas tenu de reconnaître un moyen d'identification électronique notifié de niveau « substantiel » s'il exige lui-même le niveau « élevé » pour l'accès à son service mais, ici aussi, il pourrait le faire sur une base volontaire[48].

Pour ce qui concerne l'EM notifiant, il a l'obligation de fournir un moyen d'authentification en ligne afin de permettre à toute partie utilisatrice établie sur le territoire d'un autre EM de vérifier et confirmer les données d'identification personnelles électroniques (article 7.f)). Cette obligation n'existe que lorsque la partie utilisatrice établie sur le territoire de l'autre EM est un organisme du secteur public qui offre son service en ligne et qui, grâce à ce moyen d'authentification en ligne, pourra ainsi vérifier l'identité du citoyen étranger qui souhaite accéder à ce service.

Le Règlement prévoit que cette « authentification transfrontalière est fournie gratuitement lorsqu'elle est effectuée en liaison avec un service en ligne fourni par un organisme du secteur public » (article 7, f, al.2).

Par contre, et contrairement à la proposition initiale de la Commission, cette exigence de gratuité n'existe pas pour l'authentification dans le cadre de l'accès à un service « privé » en ligne. D'une manière plus générale, le Règlement indique que « Pour les parties utilisatrices autres que des organismes du secteur public, l'État membre notifiant peut définir les conditions d'accès à cette authentification » (article 7, f, al.2). Ainsi, par exemple, si une compagnie d'assurance française décide de permettre à un citoyen belge d'accéder aux services d'assurances en ligne au moyen de sa carte d'identité électronique, l'Etat belge pourrait décider de soumettre l'authentification (c.-à-d. la vérification de l'identité du citoyen belge) opérée par la compagnie française à un tarif, voire à d'autres conditions d'accès.

Quant à la définition des conditions d'accès aux services d'authentification en général, et sous réserve du point ci-après, les dispositions du Règlement sont relativement muettes. Tout au plus, le considérant 17 indique que « la possibilité d'authentification prévue par un État membre devrait être accessible aux parties utilisatrices du secteur privé établies en dehors du territoire de cet État membre aux mêmes conditions que celles qui sont appliquées aux parties utilisatrices du secteur privé établies sur le territoire dudit État membre » et le considérant 19 que « Chaque fois qu'un schéma d'identification électronique exige des parties utilisatrices qu'elles utilisent un matériel ou un logiciel particulier au niveau national, l'interopérabilité transfrontière requiert que ces États membres n'imposent pas cette exigence et les coûts qui y sont associés aux parties utilisatrices établies en dehors de leur territoire ». Mais il ne s'agit que de considérants… Ces conditions pourraient-elles aller jusqu'à refuser l'accès à ce moyen d'authentification à une partie utilisatrice du secteur privé ? Le considérant 17 semble l'envisager en indiquant que « Ces conditions d'accès peuvent indiquer si le moyen d'authentification relatif au schéma notifié est actuellement accessible aux parties utilisatrices du secteur privé ». Cette conclusion semble assez logique dès lors que l'utilisation par le secteur privé des moyens d'identification électronique ne repose que sur une base volontaire.

Le Règlement ajoute que les « États membres n'imposent aucune exigence technique disproportionnée aux parties utilisatrices qui envisagent de procéder à cette authentification, lorsque de telles exigences empêchent ou entravent sensiblement l'interopérabilité des schémas d'identification électronique notifiés » (article 7, f, al.3)[49]. Comme nous le verrons dans le point suivant, le Règlement veille

difficultés liées à des considérations d'interopérabilité technique. Ceci étant, rien ne semble empêcher un EM d'accepter ces niveaux supérieurs au niveau « faible » sur une base volontaire.

[47] Voy. l'article 6.2. Le cas échéant, cela suppose probablement que l'EM en question exige le niveau « faible » pour l'accès à son service car il est peu probable qu'un EM se satisfasse, même sur une base volontaire, d'un moyen d'identification électronique de niveau inférieur à celui exigé pour l'accès à son propre service (niveau « substantiel » ou « élevé » par exemple).

[48] En ce sens, voy. le considérant n°15.

[49] Cette possibilité d'authentification doit-elle être offerte de manière permanente ? Le texte du règlement ne le précise pas formellement mais cette condition semble assez logiquement implicite. A tout le moins, l'exposé des

particulièrement à éviter toute atteinte à l'interopérabilité, atteinte qui serait un obstacle évident à l'utilisation transnationale des moyens d'identification électronique. Cette disposition vise indistinctement toutes les parties utilisatrices, qu'elle soient issues du secteur public ou du secteur privé.

Pour bien comprendre ces obligations respectives (obligation de reconnaissance pour les autres EM des moyens d'identification électronique notifiés et obligation pour l'EM notifiant de fournir un moyen d'authentification), un exemple fictif s'impose. L'Etat français offre un service public permettant, tant à un citoyen français qu'à un autre citoyen de l'Union européenne, de procéder à une demande en ligne d'immatriculation d'un véhicule. Pour l'accès à ce service, l'Etat français exige le niveau de garantie « substantiel ». Si un citoyen belge souhaite accéder à ce service français à l'aide de sa carte d'identité électronique belge en vue de faire une demande d'immatriculation française, il convient au préalable de vérifier si l'Etat belge a notifié à la Commission cette carte et si ce moyen d'identification électronique se trouve sur la liste publiée au Journal Officiel. Si c'est le cas, et comme la carte d'identité belge correspond au niveau de garantie « élevé » (à savoir, un niveau de garantie supérieur au niveau « substantiel »), l'Etat français a l'obligation de reconnaître la carte d'identité électronique belge et de permettre ainsi au citoyen belge de s'identifier à l'aide de sa carte lorsqu'il procède à sa demande d'immatriculation. Quant à l'Etat belge, il a l'obligation de mettre à disposition du service public français un moyen d'authentification gratuit en ligne afin de permettre à ce dernier, en qualité de « partie utilisatrice », de vérifier et valider l'identité prétendue par le citoyen belge au moyen de sa carte d'identité électronique.

Précisons enfin que l'obligation de reconnaissance mutuelle ne porte que sur la finalité *d'authentification* transfrontalière d'un service en ligne (article 6.1). En effet, comme l'indique le considérant 14, le « principe de la reconnaissance mutuelle ne devrait concerner que l'authentification d'un service en ligne. L'accès à ces services en ligne et leur fourniture finale au demandeur devraient être étroitement liés au droit de recevoir de tels services dans les conditions fixées par la législation nationale ». En d'autres mots, chaque EM reste libre de déterminer les conditions d'accès au service, le contenu du service, le niveau de garantie pour s'authentifier, la manière de fournir le service, de décider si ce service est disponible ou non au demandeur en fonction des catégories prédéfinies…

Pour terminer ce point relatif à la reconnaissance mutuelle, le Règlement ne prévoit par contre aucune obligation pour le secteur privé de reconnaître et d'accepter les moyens d'identification électronique notifiés pour l'accès à leurs services en ligne transfrontières. Toutefois, conscient des potentialités offertes par les fonctions d'identification et d'authentification électroniques liées à ces moyens qui seront utilisés dans et entre les EM pour l'accès aux services publics, le considérant 17 invite les EM à « encourager le secteur privé à utiliser sur une base volontaire, aux fins de l'identification exigée par des services en ligne ou des transactions électroniques, les moyens d'identification électronique relevant d'un schéma notifié ».

B. Le préalable nécessaire à la reconnaissance mutuelle : l'intéropérabilité

Avant de nous lancer dans le développement des conditions que doivent remplir les EM pour pouvoir notifier un schéma d'identification électronique, il nous parait primordial de nous focaliser un instant sur une exigence préalable essentielle pour que l'obligation de reconnaissance mutuelle puisse être suivie d'effet sur le terrain : l'interopérabilité.

On notera que les auteurs de la proposition de règlement ont tiré les leçons des erreurs du passé, en l'occurrence des lacunes de la directive 1999/93/CE en matière d'interopérabilité[50]. Il serait en effet vain de consacrer des obligations juridiques – tout aussi légitimes qu'elles soient – si en parallèle les

motifs de la proposition de la Commission indique que « la possibilité d'authentification doit être offerte sans interruption » (p.6).

[50] Même s'il est vrai que cette dernière ne traitait pas des schémas d'identification électronique mais portait uniquement sur la signature électronique.

conditions ne sont pas mises en œuvre pour veiller à ce que les différents systèmes nationaux puissent « se parler et se comprendre » du point de vue des aspects techniques, organisationnels et de sécurité.

Ainsi, l'article 12 relatif à la « Coopération et l'interopérabilité » indique dans son premier paragraphe que « Les schémas nationaux d'identification électronique notifiés en vertu de l'article 9, paragraphe 1, sont interopérables » et ajoute au second paragraphe que « Aux fins du paragraphe 1, un cadre d'interopérabilité est établi ». Il ne s'agit pas uniquement d'un souhait ou d'une recommandation du législateur européen. Le texte consacre clairement une obligation de résultat qui pèse mutuellement sur la Commission et sur les EM.

Tout d'abord, cette obligation relative à l'interopérabilité pèse sur la Commission car cette dernière est tenue, selon l'article 12.8., de prendre les mesures d'exécution[51] pour fixer les conditions uniformes nécessaires à l'interopérabilité, conditions qui se traduiront par l'établissement du « cadre d'interopérabilité ». Ces conditions uniformes doivent notamment veiller à être neutre du point de vue technologique, à ne défavoriser aucune solution technique nationale et à suivre dans la mesure du possible les normes européennes et internationales[52]. Concrètement, le cadre d'interopérabilité devra notamment comprendre une référence aux exigences techniques minimales liées aux niveaux de garantie visés par le Règlement[53], une table de correspondance entre les niveaux de garantie nationaux des schémas d'identification électronique notifiés et les niveaux de garantie du Règlement, une référence aux exigences techniques minimales en matière d'interopérabilité, une référence à un ensemble minimum de données d'identification personnelles représentant de manière univoque une personne physique ou morale qui est contenu dans les schémas d'identification électronique et de normes opérationnelles communes de sécurité[54].

La Commission est également tenue d'arrêter[55], au moyen d'actes d'exécution, les modalités de procédure nécessaires pour faciliter la coopération entre les EM[56]. Cette coopération doit en effet pouvoir fonctionner correctement dès lors qu'elle contribue à assurer l'interopérabilité.

Ainsi, comme l'indique l'article 12.5., l'obligation relative à l'interopérabilité pèse aussi sur les EM. Ceux-ci sont tenus de coopérer en ce qui concerne l'interopérabilité et la sécurité des schémas d'identification électronique, et ce dans l'objectif d'assurer un niveau élevé de confiance et de sécurité correspondant au degré de risque[57]. Cette obligation de coopération vise les schémas qui sont déjà notifiés mais également ceux que les EM entendent notifier à l'avenir. En effet, en vue d'être efficace, l'obligation de coopération relative à l'interopérabilité et la sécurité joue donc tant postérieurement que préalablement à la notification. A cette fin, l'article 7, g), prévoit que, six mois au moins avant la notification, l'EM notifiant doit fournir aux autres EM une description du schéma d'identification électronique qu'il entend notifier[58].

Concrètement, la coopération entre les EM consistera en un échange d'informations, d'expériences et de bonnes pratiques concernant tous les aspects des schémas d'identification électronique, en une

[51] Au plus tard le 18 septembre 2015.
[52] Article 12.3.
[53] Pour rappel, il s'agit des niveaux de garantie « faible », « substantiel » et « élevé ».
[54] Article 12.4.
[55] Au plus tard le 18 mars 2015. La Commission a respecté les délais puisque l'acte d'exécution a été adopté le 24 février 2015 : Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, *JOUE*, 25 février 2015, disponible via le lien suivant : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32015D0296
[56] Article 12.7.
[57] *Ibidem*.
[58] C'est également dans le même ordre d'idée que l'acte d'exécution relatif aux modalités de procédure nécessaires pour faciliter la coopération entre les EM doit être adopté six mois avant l'acte d'exécution fixant le cadre d'interopérabilité, espérant ainsi que la coopération permettra tant aux EM qu'à la Commission de fixer précisément ce cadre d'interopérabilité.

évaluation par les pairs des schémas d'identification électronique relevant du Règlement et en un examen des évolutions pertinentes dans le secteur de l'identification électronique[59]. Pratiquement, cette volonté de coopérer entre une grande majorité d'EM s'est manifestée rapidement, et avant même que le Règlement entre en vigueur et que les actes d'exécutions soient adoptés, puisque ces derniers ont directement participés de manière active au groupe d'experts eIDAS mis en place par la Commission le 27 mars 2014[60]. Cette réalité démontre une certaine volonté politique partagée au sein de l'UE d'aller de l'avant sur ces questions. Rappelons enfin que cette coopération s'exprime également dans le cadre de la « comitologie » liée à l'adoption des actes d'exécution.

C. Les conditions de la notification

Certes, on l'a vu, un EM n'est nullement tenu de procéder à la notification d'un ou de plusieurs schémas d'identification électronique qu'il utiliserait au niveau national. Toutefois, s'il décide de le faire, il devra montrer « patte blanche » et satisfaire aux conditions cumulatives fixées par l'article 7 du Règlement. Ces conditions poursuivent l'objectif principal du Règlement qui est de renforcer la confiance et de tirer le niveau de sécurité vers le haut.

Dès lors que certaines conditions ont déjà été abordées au gré des précédents développements, nous nous limiterons à approfondir celles non encore analysées et à énumérer les autres.

La première condition exige que les moyens d'identification électronique[61] relevant de ce schéma d'identification électronique soient délivrés soit par l'EM notifiant lui-même, soit dans le cadre d'un mandat de l'EM notifiant soit, indépendamment de l'EM notifiant, mais pour autant qu'ils soient reconnus par ce dernier[62]. On notera d'emblée qu'il convient de ne pas confondre la « notification » du schéma d'identification électronique de la « délivrance » du moyen d'identification électronique. La « notification » est toujours effectuée par un EM, comme le prévoit l'article 9, alors que la « délivrance » peut-être réalisée par une entité autre qu'un EM, et notamment par une entité privée comme le permet le Règlement[63]. Le cas échéant, l'EM peut décider soit de mandater en son nom une entité privée qui dispose de l'expertise dans le domaine de la délivrance des moyens d'identification électronique soit aller plus loin en considérant qu'un moyen d'identification électronique déjà utilisé par une entité privée pour ses besoins propres est éligible au titre de la notification et, ainsi, de le « reconnaître »[64] et de le notifier dans le cadre de la procédure prévue par le Règlement.

La seconde condition stipule que les moyens d'identification électronique « peuvent être utilisés pour accéder au moins à un service fourni par un organisme du secteur public et qui exige l'identification électronique dans l'État membre notifiant »[65]. L'idée qui se cache derrière cette condition consiste à présumer qu'un moyen d'identification électronique offre en principe un niveau de fiabilité acceptable si l'EM notifiant utilise ce moyen pour l'accès à ses propres services publics au niveau national, ou en tout cas, à au moins un de ces services.

---

[59] Article 12.6.

[60] Pour plus d'informations sur ce groupe d'experts informel, voy. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3032&news=1

[61] La carte d'identité électronique belge par exemple.

[62] Article 7.a).

[63] Le considérant 13 indique d'ailleurs en ce sens que les EM « devraient également pouvoir décider d'impliquer ou non le secteur privé dans la fourniture de ces moyens ».

[64] On peut se demander si la notion de « reconnaissance » implique une responsabilité globale dans le chef de l'EM qui notifie. Nous verrons par la suite que ce n'est pas nécessairement le cas. En effet, contrairement à la proposition de règlement qui prévoyait que les « moyens d'identification électronique sont délivrés par l'EM notifiant ou en son nom ou *sous sa responsabilité* », le texte adopté opère par contre dans l'article 11 un « saucissonnage » des responsabilités entre les différents acteurs en fonction de leurs interventions respectives.

[65] Article 7, b).

La troisième condition indique que le schéma d'identification électronique et que les moyens d'identification électronique délivrés dans ce contexte répondent aux exigences d'au moins un des niveaux de garantie prévus par le Règlement, à savoir le niveau « faible », « substantiel » ou « élevé »[66]. Seuls ces trois niveaux de garantie sont éligibles à la notification mais rappelons que, si le Règlement permet de notifier un moyen d'identification électronique de niveau « faible », ce dernier ne tombe pas pour autant sous l'obligation de reconnaissance mutuelle mais relève uniquement de la reconnaissance sur une base volontaire.

La quatrième condition prévoit que l'EM notifiant veille, d'une part, à ce que les données d'identification personnelles représentent « de manière univoque » la personne en question et, d'autre part, que ces données soient attribuées conformément aux spécifications techniques, aux normes et aux procédures pour le niveau de garantie concerné, à la personne au moment de la délivrance du moyen d'identification électronique relevant de ce schéma[67]. Le second élément de la condition devant être précisé par un acte d'exécution, nous nous limiterons au premier élément de celle-ci. D'interminables discussions ont été tenues lors des négociations sur le terme *ad hoc* qui devait être utilisé : le texte de la proposition utilisait les termes « sans ambiguïté » alors que les termes « de manière univoque », « uniquement » ou « de manière unique » ont été proposés lors des négociations, pour finalement retenir le terme « de manière univoque » (« uniquely » en anglais) dans le texte adopté[68]. Nous nous contenterons de préciser que l'objectif de cette notion est de garantir que la « personne revendiquant une identité particulière est bien la personne à laquelle cette identité a été attribuée »[69], et personne d'autre. Il convient donc de veiller à ce qu'une même identification électronique ne permette pas d'identifier plusieurs personnes différentes. L'exposé des motifs de la proposition de la Commission précise en outre que « Cette obligation signifie non pas qu'une personne ne peut pas avoir plusieurs moyens d'identification électronique, mais que les moyens doivent tous renvoyer à la même personne »[70].

La cinquième condition indique que la partie « délivrant » le moyen d'identification électronique relevant de ce schéma veille à ce que ce moyen soit attribué à la personne visée à la quatrième condition conformément aux spécifications techniques, aux normes et aux procédures pour le niveau de garantie concerné. Comme pour la condition précédente, cette condition doit être précisée par un acte d'exécution. Nous nous bornerons donc à rappeler que la partie qui délivre un moyen d'identification électronique peut être tant un EM qu'une entité privée (bénéficiant d'un mandat ou d'une « reconnaissance » de l'EM). Nous précisons également que l'acte d'exécution qui doit être adopté vise à assurer la fiabilité et la qualité notamment de la procédure visant à confirmer et vérifier l'identité de la personne qui demande la délivrance d'un moyen d'identification électronique, de l'entité qui délivre et de la procédure de délivrance de ces moyens ainsi que du mécanisme d'authentification permettant à une partie utilisatrice de confirmer l'identité d'une personne qui utilise ce moyen d'identification électronique[71].

Les sixième et septième conditions ont déjà été développées, nous n'y revenons pas. Il s'agit respectivement de l'obligation pour l'EM notifiant, d'une part, de rendre disponible en ligne un moyen d'authentification[72] et, d'autre part, d'avoir fourni aux autres EM une description du schéma d'identification électronique qu'il souhaite notifier depuis au moins six mois, et ce notamment dans un objectif d'interopérabilité[73].

[66] Article 7, c) et article 8.3.
[67] Article 7, d).
[68] Lors des dernières discussions en juin 2014 avec les juristes linguistes du Conseil sur les différentes versions linguistiques du texte, les termes « de manière univoque » ont finalement été préférés au terme « uniquement » pour la version française du texte, et cela même si le texte anglais conserve le terme « uniquely ».
[69] Considérant n°16. L'exposé des motifs de la proposition de la Commission précisait pour sa part que « Les États membres doivent établir un lien univoque entre les données d'identification électronique et la personne concernée ».
[70] Proposition du 4 juin 2012, *op.cit.*, p. 6.
[71] Article 8.3.
[72] Article 7, f).
[73] Article 7, g).

La dernière condition précise que le schéma d'identification électronique, pour pouvoir être notifié, doit satisfaire aux exigences de l'acte d'exécution qui détermine le cadre d'interopérabilité[74]. Il résulte de cette exigence qu'un schéma ne pourra pas être notifié tant que cet acte d'exécution, ainsi que les autres précités, ne sont pas adoptés, soit au plus tard le 18 septembre 2015. Après cette date, les premières notifications peuvent avoir lieu et les EM peuvent reconnaître les schémas déjà notifiés, mais uniquement sur une base volontaire jusqu'au 18 septembre 2018.

Ces diverses conditions qui sont formulées dans l'article 7 doivent être complétées par une autre condition qui découle indirectement de l'article 9.1. Cette condition touche à la transparence et impose ainsi à l'EM notifiant de communiquer à la Commission non seulement une liste d'informations au moment de la notification mais également, et ce dans les meilleurs délais, toutes modifications ultérieures de ces informations. Ces informations consistent notamment en une description du schéma d'identification électronique et de ses éléments (dont l'authentification et la concordance au cadre d'interopérabilité), ses niveaux de garantie, l'entité ou les entités qui délivrent les moyens d'identification électronique, le régime de contrôle applicable[75], des informations sur la responsabilité des différentes parties intervenantes, l'indication de l'entité ou des entités qui gèrent l'enregistrement des données d'identification personnelle uniques[76] et les dispositions concernant la suspension ou la révocation du schéma d'identification notifié, de l'authentification ou des parties compromises en cause[77].

D. Les conséquences de la notification : obligation en cas d'atteinte à la sécurité et responsabilité

Dès lors qu'un schéma d'identification électronique a été notifié par un EM, il découle du Règlement, outre l'application du principe de reconnaissance mutuelle sur lequel nous ne revenons pas, des conséquences qui touchent tant aux atteintes à la sécurité qu'à la responsabilité.

L'article 10 prévoit en effet que si le schéma d'identification électronique notifié ou le moyen d'authentification sont violés ou partiellement compromis « d'une manière préjudiciable à la fiabilité de l'authentification transfrontalière de ce schéma », l'EM notifiant suspend ou révoque immédiatement le moyen d'authentification transfrontalière ou les éléments compromis en cause et en informe les autres EM et la Commission.

On notera ici deux différences importantes par rapport à la proposition initiale de la Commission[78]. D'une part, les obligations liées aux éventuelles atteintes à la sécurité ne sont plus « noyées » dans un sous point d'un article qui traitait des conditions de la notification mais font désormais l'objet d'un article spécifique dédié à cette problématique, ce qui témoigne de l'importance accordée par le législateur européen à celle-ci. D'autre part, la disposition finalement adoptée n'envisage plus la suspension ou la révocation de la globalité du schéma d'identification électronique notifié mais semble uniquement se focaliser sur la suspension ou la révocation du *moyen d'authentification transnational* ou des éléments compromis risquant de porter atteinte à la *fiabilité de l'authentification transnationale*. Le Règlement ne prévoit donc la suspension ou la révocation que si il existe un risque quant à la fiabilité de l'authentification transnationale. Par contre, le Règlement ne semble pas vouloir s'immiscer dans la réaction que pourrait adopter l'EM relative à l'utilisation et l'authentification purement nationales de ce schéma et moyen d'authentification violés ou partiellement compromis.

Dans l'hypothèse d'une suspension ou d'une révocation suite à une atteinte à la sécurité, le choix étant laissé à l'EM en fonction de l'importance de cette atteinte, deux cas de figure peuvent se présenter.

---

[74] Article 7, h).
[75] Contrairement au chapitre 3 relatif aux services de confiance, le règlement n'instaure aucun régime de contrôle harmonisé pour le volet identification électronique. Ce dernier est laissé à la liberté des EM qui, tout au plus, doivent communiquer des informations sur le « régime de contrôle applicable ».
[76] Par exemple, le service responsable du registre national au sein du SPF Intérieur en Belgique.
[77] Article 9.1.
[78] Proposition du 4 juin 2012, *op.cit.*, article 6.1.(d).

Soit il est remédié dans un délai de maximum trois mois à l'atteinte ou à l'altération, auquel cas l'EM notifiant rétablit l'authentification transnationale et en informe les autres EM et la Commission dans les meilleurs délais. A cet égard, il peut paraître étonnant de permettre le *rétablissement* de l'authentification nationale alors que des éléments compromis auraient été *révoqués*, et non simplement *suspendus*[79]. A l'analyse, ce cas de figure est toutefois envisageable notamment dans le cas où les éléments compromis révoqués ont été retirés et remplacés par d'autres plus fiables.

Soit il n'est pas remédié à l'atteinte ou à l'altération dans un délai de trois mois à compter de la suspension ou de la révocation, auquel cas l'EM notifie le retrait au niveau transnational du schéma d'identification électronique aux autres EM et à la Commission. Le cas échéant, la Commission publie dans les meilleurs délais les modifications à la liste des schémas notifiés dans le *JOUE*. A compter de cette publication, l'obligation de reconnaissance mutuelle dans le cadre de l'utilisation transnationale prend fin. Un tel schéma d'identification électronique pourrait-il encore être utilisé au niveau national dans ce cas ? Le Règlement n'aborde pas cette question mais, si une telle hypothèse venait à se présenter, il serait pour le moins irresponsable qu'un EM continue à utiliser à l'échelon national un tel schéma compromis et pour lequel il n'a pas été possible de remédier aux atteintes dans un délai de trois mois !

L'article 11 traite de la responsabilité liée aux schémas d'identification électroniques notifiés. Ici aussi, on constate une différence fondamentale entre le texte adopté et la proposition de règlement de la Commission. En effet, alors que cette dernière prévoyait une responsabilité de l'EM notifiant tant pour la *délivrance* du moyen d'identification électronique[80] que pour tous les aspects liés à *l'authentification* en ligne[81], le texte adopté opère un « saucissonnage » des responsabilités entre les différents acteurs (EM notifiant, partie qui *délivre* le moyen d'identification électronique et partie qui *gère* la procédure d'authentification) en fonction de leurs interventions respectives[82].

Concernant l'EM, celui-ci est responsable du dommage causé en raison d'un manquement à son obligation[83], d'une part, de veiller à ce que les données d'identification personnelles représente « de manière univoque » la personne en question et que ces données soient attribuées conformément aux spécifications techniques, aux normes et aux procédures pour le niveau de garantie concerné, à la personne au moment de la délivrance du moyen d'identification électronique relevant de ce schéma[84] et, d'autre part, de veiller à rendre disponible une authentification transnationale en ligne, à la gratuité de celle-ci lorsqu'elle est utilisée pour l'accès à un service public et à éviter tout exigence technique disproportionnée de nature préjudiciable à l'interopérabilité[85].

Concernant la partie qui délivre le moyen d'identification électronique, celle-ci est responsable du dommage causé en raison d'un manquement à son obligation[86] de veiller à ce que ce moyen soit bien attribué à la personne à laquelle l'EM a attribué les données d'identification personnelle, et cela conformément aux spécifications techniques, aux normes et aux procédures pour le niveau de garantie concerné, qui devront être déterminées par un acte d'exécution.

[79] En effet, la suspension est plutôt envisagée quand il existe seulement un doute sur une violation éventuelle , auquel cas on lui donne un effet *temporaire* pour se réserver le temps de vérifier, alors que la révocation est utilisée quand la violation est certaine et que l'élément corrompu ne doit plus pouvoir être utilisé, auquel cas on lui donne un effet *définitif*.

[80] L'article 6.1.(a) de la proposition de la Commission prévoyait que les « moyens d'identification électronique sont *délivrés* par l'EM notifiant ou en son nom ou *sous sa responsabilité* ».

[81] L'article 6.1.(e) de la proposition de la Commission stipulait que « l'Etat membre notifiant est responsable : (i)… ; et (ii) de la possibilité *d'authentification* indiquée au point d) ».

[82] Voy. le considérant n°18.

[83] Article 11.1., qui renvoie aux obligations visées à l'article 7, points d) et f).

[84] Voy. *supra* les développements relatifs à la quatrième condition de notification.

[85] Voy. *supra* les développements relatifs au moyen d'authentification.

[86] Article 11.2., qui renvoie à l'obligation visée à l'article 7, point e).

Quant au moyen d'authentification, s'il est vrai que l'EM assume une part de responsabilité comme indiqué ci-dessus, le Règlement prévoit aussi que la partie qui *gère la procédure d'authentification* est responsable du dommage causé en raison d'un manquement à l'obligation d'assurer la gestion *correcte* de l'authentification visée à l'article 7, point f). Ici, par contre, le Règlement ne souffle mot sur la manière d'évaluer le caractère correct ou non de la « gestion de l'authentification »…

On précisera que ces responsabilités respectives consacrées par le Règlement ne valent que pour les dommages causés dans le *cadre d'une transaction transnationale*. Pour les transactions nationales, le Règlement ne s'applique pas et les EM peuvent prévoir un régime de partage de responsabilité différent (plus ou moins étendu).

L'article 11.5. prévoit en outre que ce régime de partage de responsabilité est « sans préjudice de la responsabilité incombant, au titre du droit national, aux parties à une transaction effectuée à l'aide de moyens d'identification électronique relevant du schéma d'identification électronique notifié ». En d'autres mots, le régime de responsabilité prévu par le Règlement ne porte que sur les aspects précités du schéma d'identification électronique mais ne touche en rien à la responsabilité éventuelle liée au contenu ou à l'exécution de la transaction elle-même entre les parties.

Enfin, l'article 11.4. indique que ce régime de partage de responsabilité s'applique « conformément aux dispositions nationales en matière de responsabilité ». Comme le précise le considérant n° 18, il n'affecte donc pas ces règles nationales, par exemple, celles relatives à la définition des dommages, aux règles procédurales ou aux règles relatives à la charge de la preuve.

On peut regretter ce morcellement des responsabilités[87]. Certes, il est possible que ces différentes obligations soient exercées par l'EM lui-même, auquel cas l'ensemble des responsabilité sont assumées par ce dernier. Mais il arrivera aussi souvent que la délivrance du moyen d'identification électronique et la gestion de la procédure d'authentification soient assurées par d'autres parties, notamment des acteurs privés. Dans ce cas, on peut craindre que, dans un domaine aussi complexe, si un problème se pose, les parties se renvoient l'une l'autre les responsabilités dès lors qu'il ne sera pas toujours aisé d'identifier la cause du problème. Il faut en outre espérer que ce partage de responsabilité ne pousse certains EM, peut-être un peu trop laxistes, à notifier des schémas dont… ils n'assument pas toutes les responsabilités !

L'analyse du premier volet relatif à l'identification électronique étant terminée, attelons-nous maintenant à l'examen de l'autre grand volet du Règlement portant sur les services de confiance.

III. Le volet relatif aux services de confiance (qualifiés)

L'objectif principal du chapitre 3 du Règlement consiste à instaurer un cadre juridique général concernant l'utilisation des services de confiance[88]. Contrairement à la directive 1999/93/CE qui se limitait à réglementer la signature électronique et les prestataires de service de certification, le Règlement couvre d'autres services de confiance, et les prestataires qui offrent ces services, tels que le cachet, l'horodatage et le service d'envoi recommandé électroniques ainsi que l'authentification de site Internet.

Cette extension se comprend aisément. Une législation dont le champ d'application était limité à l'intervention du tiers de confiance dans le cadre de l'utilisation de signatures électroniques et de certificats d'identité n'avait pas beaucoup de sens. Lorsqu'on envisage la conclusion, la transmission et la

[87] D'autant qu'il eût été aisé pour l'EM, qui aurait assumé une responsabilité de première ligne, de régler les questions de responsabilités par le biais de clauses contractuelles *ad hoc* (« back-to-back ») permettant à cet EM de se retourner contre cet acteur qui a procédé à la *délivrance* du moyen d'identification électronique et/ou à la *gestion de la procédure d'authentification*, comme le fait quotidiennement une entreprise principale avec ses sous-traitants dans le domaine informatique ou dans d'autres domaines.

[88] Considérant n° 21 et article 1, b) et c).

conservation d'un acte juridique dans un processus totalement électronique, il devient difficile de s'affranchir de dispositions qui encadrent juridiquement l'offre des autres services précités. En effet, il s'avère important de garantir la fiabilité de ces services mais aussi d'assurer la reconnaissance juridique de ceux-ci, et *in fine* de veiller à garantir la validité et la preuve de l'acte juridique conclut électroniquement à l'aide de ces services.

On pourrait évidemment s'interroger sur l'initiative de la Commission et sur la nécessité de légiférer dans cette matière. Dans son analyse d'impact, la Commission a d'ailleurs envisagé l'option qui consistait à abroger la directive 1999/93/CE et à s'abstenir de toute nouvelle intervention règlementaire dans le domaine de l'identification électronique et des services de confiance, pour finalement conclure à la nécessité de réglementer[89]. De surcroît, et comme ils l'ont fait pour la problématique de la signature électronique[90], certains auteurs pourraient estimer qu'une modification de la législation n'est pas souhaitable pour encadrer ces nouveaux services. Ils inviteraient à faire confiance aux juges pour développer les potentialités des textes généraux existants[91]. On doit leur donner raison et tort à la fois.

On doit leur donner en partie raison car, comme le constate D. Mougenot, la « jurisprudence a déjà fait preuve d'une grande capacité à élaborer des systèmes juridiques complexes à partir de textes très généraux »[92]. Les pays anglo-saxons fonctionnent d'ailleurs plus largement sur ce système de la « case law ».

Mais on doit également leur donner tort pour plusieurs raisons. D'une part, ces décisions sont isolées et manifestement insuffisantes pour établir un régime juridique clair qui serait source de sécurité juridique et qui permettrait de pousser vers le haut la qualité des services, à tout le moins dans nos pays de droit civil. Comme le fait remarquer très justement D. Mougenot, dont on rappelle qu'il est lui-même au cœur du métier en sa qualité de juge au tribunal de commerce de Mons, pour que la jurisprudence puisse exercer sa capacité d'innovation, « encore faut-il que les juges aient à se prononcer sur des cas d'espèce. Or, nous avons relevé le petit nombre de litiges soumis à la justice (…) La mise sur pied d'un droit de la preuve de nature jurisprudentielle risque fort de prendre du temps et de rester lacunaire »[93]. Ce constat déjà fait il y a presque 20 ans est manifestement encore d'actualité ! D'autre part, même si certains juges ont l'occasion de se prononcer en faveur d'une approche fonctionnelle, ceux-ci risquent de régler le problème de manière partielle, en fonction du cas d'espèce, sans vision générale et cohérente de la problématique. Ajoutons en outre que, contrairement à l'approche jurisprudentielle qui ne peut se développer que sur la base de litiges, l'intervention législative permet de poursuivre un objectif préventif et d'éviter précisément la naissance de litige, outre le fait que cela offre de la prévisibilité et de la sécurité juridique pour les prestataires et utilisateurs des services.

De plus, on saisit mal ce qui justifierait que l'on n'exige aucun niveau minimum de fiabilité en matière d'horodatage, de recommandé électronique voire d'archivage électronique alors que l'on exige depuis la directive de 1999 le respect de garanties techniques et juridiques minimales en vue d'assimiler une signature électronique *qualifiée* à une signature manuscrite, et de lui reconnaître ainsi les mêmes effets juridiques. Or, sur le plan probatoire, il est tout aussi important de disposer de moyens de preuve « solides » en vue de convaincre le juge de la réalité et de la date d'un envoi mais aussi de la non altération du document malgré l'écoulement du temps. Si le respect de garanties minimales n'est pas imposé aux opérateurs de ces services, des discussions techniques et délicates à trancher naîtront

[89] Résumé de l'analyse d'impact, *op.cit.*, pp. 6 et 7.

[90] Concernant le domaine de la signature électronique, voy. D. AMMAR, « Preuve et vraisemblance — contribution à l'étude de la preuve technologique », *R.T.D.civ.*, 1993, p. 532 ; A. MYNARD, « Télématique et preuve en droit civil québecois et français : une antinomie ? », *D.I.T.*, 1992, p. 21.

[91] On pense par exemple en droit belge à l'article 1322, alinéa 2, du Code civil ou à l'article XII.15 du Code de droit économique visant à adopter une approche fonctionnelle des exigences de forme dans le cadre de la conclusion de contrats par voie électronique.

[92] D. MOUGENOT, « Droit de la preuve et technologies nouvelles : synthèse et perspectives », *Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, p. 98.

[93] D. MOUGENOT, *op.cit.*, p. 99.

inévitablement devant le juge à convaincre, ce qui crée une insécurité juridique certaine. A juger de la piètre qualité des services offerts par certains opérateurs, exiger un niveau minimum de fiabilité et de sérieux ne semble pas superflu. Raisonner autrement reviendrait à laisser croire aux utilisateurs qu'ils disposent de moyens de preuve électroniques (rarement gratuits)… qui en pratique risquent de ne rien prouver ! Il devenait donc opportun de lever l'incohérence légale et de supprimer ce régime discriminatoire qui existe actuellement dans notre droit.

Enfin, des contacts et questions fréquemment posées par les administrations ou entreprises dans ce domaine, on constate de manière récurrente que ces dernières souhaitent une règlementation sur les services de confiance pour des raisons évidentes de sécurité juridique. En effet, celles-ci ne semblent pas disposées à utiliser de manière généralisée des services d'horodatage ou de recommandé électronique, voire d'abandonner l'archivage papier au profit de l'archivage électronique, ce qui entraîne parfois une destruction irréversible des archives papiers, tant que le législateur ne leur garantit pas une relative certitude quant à la valeur juridique tant de ces services que des documents électroniques qui en font l'objet.

Ces considérations sur l'opportunité d'une réglementation en la matière étant faite, nous abordons dans un premier temps les principes généraux qui sous-tendent le chapitre 3 pour ensuite nous focaliser tout à tour sur les différents services de confiances réglementés.

A. Principes généraux et tronc commun aux services de confiance

i. La mise en place d'un régime optionnel et la dérogation pour les « systèmes fermés »

Rappelons que le troisième chapitre relatif aux services de confiance n'oblige pas les prestataires à fournir des services de confiance, qu'ils soient qualifiés ou non. Si un prestataire propose un ou plusieurs services de confiance, le Règlement n'oblige pas ce dernier à offrir tous les services de confiance visés par le Règlement. Le Règlement n'impose pas non plus aux citoyens, entreprises ou administrations d'utiliser les services de confiance qui seraient proposés sur le marché[94].

Pour utiliser une métaphore, le Règlement se limite à créer une « garde-robe »[95] dans laquelle on y trouve deux « costumes juridiques » principaux : le costume juridique applicable aux services de confiance qualifiés et celui applicable aux services de confiance non qualifiés. Le Règlement n'oblige aucun acteur économique à porter un de ces costumes juridiques voire les deux. Il n'impose pas non plus de porter toutes les pièces du costume : un prestataire pourrait offrir des services de signature et cachet électroniques, sans toutefois offrir des services d'horodatage et d'envoi recommandé électroniques. Le Règlement permet également de « dépareiller » les pièces des deux costumes : un prestataire pourrait offrir des services de signature électronique qualifiée mais se limiter à offrir des services de cachet, d'horodatage et d'envoi recommandé électroniques non qualifiés. Même si cela nous semble hypothétique, il est donc théoriquement possible qu'aucun acteur n'offre par exemple des services de confiance qualifiés à l'avenir ou qu'aucun utilisateur ne recoure à ces services s'ils étaient offerts[96]. C'est notamment en ce sens que le régime mis en place par le Règlement peut être qualifié d'optionnel.

Par ailleurs, le Règlement consacre une dérogation au profit des « systèmes fermés ».

[94] Selon le considérant n°21, le règlement « ne devrait pas imposer d'obligation générale d'y recourir ou d'installer un point d'accès pour tous les services de confiance existants ».
[95] On pourrait également parler de « boîte à outils ».
[96] Cette dernière hypothèse est toutefois relativement hypothétique dès lors que le considérant n°69 encourage également « Les institutions, organes et organismes de l'Union (…) à reconnaître l'identification électronique et les services de confiance couverts par le présent règlement (…) ».

En effet, l'article 2.2. stipule expressément[97] que le « règlement ne s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants ». Le considérant n°21 reprend ce principe tout en précisant « … et qui n'ont pas d'effets sur des tiers. Par exemple, les systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance ne devraient pas être soumis aux exigences du présent règlement. Seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement ».

Même si ce point n'est pas exprimé dans le Règlement, il semble aller de soi que si un prestataire offre ses services en « système fermé »[98], il ne devrait pas pouvoir à la fois prétendre offrir des services de confiance « qualifiés » dans le cadre de ce système fermé et, en même temps, revendiquer le bénéfice de la dérogation. Selon nous, le fait de déclarer offrir des services de confiance « qualifiés » impliquerait pour le prestataire d'accepter implicitement de se soumettre aux exigences du Règlement relatives à cette catégorie de services, et donc de renoncer implicitement au bénéfice de la dérogation au profit des « systèmes fermés ». Raisonner autrement reviendrait à vider le Règlement de son contenu, à tout le moins en ce qui concerne les exigences et le régime de contrôle applicables aux services « qualifiés ».

En d'autres mots, les prestataires de service(s) de confiance ayant opté et obtenu le statut « qualifié » devraient se soumettre aux exigences du Règlement pour les services qualifiés ayant reçu le "blanc-seing" de l'organe de contrôle et étant inscrit sur la liste de confiance (cf. *infra*, point iii). Néanmoins, rien n'empêcherait le même prestataire de fournir par ailleurs des services non qualifiés en « système fermé », qui ne seraient alors pas assujettis aux exigences du Règlement.

ii. Services de confiance qualifiés *versus* non qualifiés

S'il est vrai que le Règlement repose sur un système optionnel, on rappellera par contre que si un prestataire décide (librement) de fournir un ou plusieurs services de confiance, celui-ci a l'obligation de se conformer aux conditions du Règlement, particulièrement s'il s'agit de services qualifiés. De plus, un utilisateur de ces services doit pouvoir bénéficier des effets juridiques reconnus par le Règlement à chacun des services de confiance qualifiés et non qualifiés, et les juridictions nationales sont tenues de reconnaître ces effets juridiques.

Ces considérations nous permettent de mettre le doigt sur l'importance de la distinction entre services de confiance *qualifiés* et *non qualifiés* ainsi que d'expliquer les conséquences de cette distinction.

Le Règlement consacre désormais le concept de service de confiance « qualifié »[99]. Comme l'indique le considérant n°28 « les notions de service de confiance *qualifié* et de prestataire de services de confiance *qualifié* devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis ». Nous saluons la consécration et la généralisation de ce concept. Outre le fait qu'il simplifie la lecture et la compréhension des dispositions du Règlement, il permet également d'accroître la confiance des petites et moyennes entreprises et des consommateurs dans le marché intérieur et de promouvoir l'utilisation des services de confiance.

[97] Ce que la directive 1999/93/CE s'était limitée à faire dans son considérant n°16.

[98] On reconnaîtra que cette notion reste nébuleuse. Ceci étant, on observera souvent que, dans un système fermé, les services de confiance n'apparaissent que comme accessoires d'un service principal (par exemple dans les réseaux bancaires – Isabel, SWIFT - ou de sécurité sociale) offert par une entreprise ou une administration. Ce type de situation se rencontre régulièrement dans les réseaux où les services sont destinés à être utilisés par les membres d'un groupe d'entreprises ou d'une société coopérative. Par ailleurs, on notera que dans un tel système, la question de la valeur probante des services de confiance utilisés est directement réglée par la loi ou la convention qui institue ce réseau fermé, ce qui réduit l'intérêt ou la nécessité de passer par les conditions du Règlement permettant de bénéficier de la clause d'assimilation ou des présomptions...

[99] Qui est une généralisation du concept de *certificat qualifié* déjà utilisé timidement dans la directive 1999/93/CE.

Le considérant n° 35 stipule que « Tous les prestataires de services de confiance devraient être soumis aux exigences du présent règlement… » tout en précisant que « Toutefois, eu égard au type de services fournis par les prestataires de services de confiance, il y a lieu de faire une distinction, au niveau de ces exigences, entre, d'une part, les prestataires de services de confiance qualifiés et, d'autre part, les prestataires de services de confiance non qualifiés ». Comme on le verra par la suite, les services de confiance qualifiés, et les prestataires qui les offrent, sont soumis à de nombreuses conditions relativement strictes, ce qui n'est pas le cas pour les services non qualifiés.

Dans ce contexte, on pourrait légitimement se demander quel serait l'intérêt de recourir à un service de confiance qualifié plutôt qu'à un service non qualifié. Deux éléments essentiels permettent d'illustrer cet intérêt.

Premièrement, et pour prendre une autre métaphore, le service de confiance non qualifié peut être comparé au modèle de base d'un véhicule « traditionnel » alors que le service de confiance qualifié s'apparenterait à un véhicule de grosse cylindrée, dotés de 4 roues motrices et de toutes les options. Pourquoi utiliser un modèle plutôt que l'autre ? La réponse dépendra de la stratégie juridique et de la politique de gestion de risques de l'utilisateur. Soit ce dernier utilise ces services dans un domaine dans lequel on peut se satisfaire d'un niveau de sécurité et fiabilité faible et/ou pour des opérations juridiques pour lesquelles le risque de contestation est faible voire acceptable. Dans ce cas, il pourra se contenter d'un service non qualifié de la même manière qu'il n'est pas nécessaire de disposer d'un véhicule suréquipé pour rouler 20 km par jour sur des routes bien entretenues et sans obstacle. Soit l'utilisateur se sert de ces services dans un domaine dans lequel un niveau de sécurité élevé est requis tant les risques d'attaques ou de fraudes sont importants et/ou pour des opérations juridiques pour lesquelles on ne peut se permettre de prendre le risque d'une contestation tant les enjeux (financiers ou autres) sont considérables. Dans ces hypothèses, on lui conseillera de recourir à un service de confiance qualifié de la même manière que s'il veut accéder au sommet d'une montagne en passant par un chemin semé d'embûches et de nombreux bourbiers, on lui conseillera d'utiliser un véhicule *ad hoc* lui permettant de franchir aisément ces obstacles en (relative) sécurité[100].

Une seconde raison qui justifie le recours à un type de service plutôt qu'à l'autre trouve sa source dans les effets juridiques qui y sont liés[101], et à la prévisibilité juridique qui en découle.

En effet, tous les services de confiance qualifiés bénéficient d'une clause d'assimilation[102] ou de présomptions, dispensant ainsi son utilisateur de la charge de la preuve en cas de contestation. Ainsi, l'article 25.2. indique que « L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite », l'article 35.2. que « Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet

[100] L'utilisation de cette métaphore nous oblige toutefois à nuancer notre propos dans la mesure où rien ne permet de préjuger de la qualité réelle d'un service de confiance non qualifié. En effet, on peut imaginer que ce dernier garantisse un niveau de qualité et de sécurité équivalent voire supérieur à celui d'un service de confiance qualifié (comme c'est le cas par exemple dans certains systèmes fermés, notamment dans le domaine bancaire). Néanmoins, on reconnaîtra qu'aucune procédure, hormis une éventuelle décision d'un juge dans le cadre d'un recours sur la valeur juridique de ce service, ne permet de le vérifier au préalable, contrairement au service de confiance qualifié comme nous le verrons dans la suite de notre contribution.

[101] Les considérants n° 22 et 23 indiquent d'ailleurs que l'objectif du règlement est de faire en sorte qu'il soit « possible d'utiliser les services de confiance comme moyen de preuve en justice dans tous les États membres » et de « rendre obligatoire leur reconnaissance ».

[102] Pour un commentaire relatif à la clause 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. 75-81 ; B. DE GROOTE, « Het bewijs in de elektronische handel – Enkele bedenkingen », *A.J.T.*, 2001, pp. 881-901 ; 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. 1505-1525.

électronique qualifié est lié », l'article 41.2. que « Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure », l'article 43.2. que « Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié ».

A l'inverse, les services de confiance non qualifiés bénéficient simplement de la clause de non-discrimination qui consiste à considérer que l'effet juridique et la recevabilité du service de confiance non qualifié comme preuve en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du même service de confiance qualifié[103]. En cas de contestation, il appartient donc à l'utilisateur de ces services d'apporter la preuve que ceux-ci sont suffisamment fiables et de tenter de convaincre le juge qu'ils offrent les garanties normalement attendues de ces services. Une telle contrainte éventuelle, et le risque qui en résulte si cette preuve (technique) n'est pas apportée à suffisance, peut être de nature à dissuader certains utilisateurs à recourir aux services de confiance non qualifiés.

iii. Procédure d'autorisation préalable pour lancer un service de confiance qualifié et liste de confiance

Comme déjà indiqué, les services de confiance qualifiés, et les prestataires qui les offrent, sont soumis à des exigences plus strictes que celles applicables aux services non qualifiés, ce qui justifie notamment les effets juridiques privilégiés (clause d'assimilation et présomptions) qui leurs sont reconnus. Parmi ces exigences, on retrouve la procédure d'autorisation préalable consacrée par l'article 21. Cette procédure doit impérativement être suivie et aboutir avant de commencer à offrir des services de confiance qualifiés, contrairement à l'offre de services de confiance non qualifiés qui n'est soumise à aucune autorisation, procédure ou formalité préalable.

Concrètement, si un prestataire a l'intention de commencer à offrir un (ou plusieurs) service(s) de confiance qualifié(s), il doit soumettre à un organe de contrôle national (cf. *infra*, point v) une notification de son intention accompagnée d'un rapport sur l'évaluation de la conformité délivré par un organisme d'évaluation de la conformité[104].

L'organe de contrôle vérifie que le prestataire et le service de confiance qu'il fournit respectent les exigences du Règlement[105]. Si c'est le cas, il accorde le « statut qualifié » au prestataire et au service de confiance qu'il fournit et en informe, au plus tard trois mois après la notification initiale du prestataire, l'organisme chargé de la tenue et de la mise à jour des « listes de confiance » établies par l'article 22 du Règlement[106].

---

[103] Voy. les articles 25.1., 35.1., 41.1. et 43.1.

[104] Selon l'article 3,18), un "organisme d'évaluation de la conformité" est un organisme défini à l'article 2, point 13), du règlement (CE) n° 765/2008 (du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, JO L 218 du 13.8.2008, p. 30), qui est accrédité conformément audit règlement comme étant compétent pour effectuer l'évaluation de la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit.

[105] Afin de faciliter le processus de contrôle et de lancement des services, le règlement encourage « des échanges préliminaires entre des prestataires de services de confiance qualifiés potentiels et l'organe de contrôle compétent en vue de faciliter les vérifications préalables à la fourniture de services de confiance qualifiés » (considérant n°45).

[106] Pour la date d'entrée en application du règlement, le 1er juillet 2016, les organes de contrôle devront idéalement se préparer en vue de faire face à un probable afflux de demandes émanant de prestataires distincts et pouvant porter sur des services différents. Le cas échéant, ces organes devraient examiner ces multiples demandes en même temps et dans un délai (en principe) de 3 mois.

Le prestataire de service de confiance qualifié ne peut pas commencer à fournir le service de confiance qualifié tant que le statut « qualifié » n'est pas indiqué sur la liste de confiance[107].

Une non-indication de ce statut sur la liste de confiance dans les trois mois qui suivent la notification initiale du prestataire pourrait s'expliquer par l'une des raisons suivantes. Soit l'organe de contrôle juge que le prestataire et le service de confiance ne respectent pas toutes les exigences du Règlement (ce qui en principe aurait déjà dû apparaitre dans le rapport sur l'évaluation de la conformité précité), auquel cas il refuse l'attribution du statut qualifié. Soit l'organe de contrôle n'a pas été en mesure de terminer sa vérification dans le délai de trois mois, auquel cas l'article 21.2, al.3, prévoit qu'il en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification. Le cas échéant, et si le retard était dû à des causes indépendantes du prestataire, on peut raisonnablement attendre de l'organe de contrôle qu'il mette en œuvre tous les moyens possibles pour réduire au maximum ce délai, et éviter ainsi au prestataire de subir trop de retard dans la commercialisation de ces services. Soit, et c'est la dernière hypothèse, l'organe de contrôle a respecté le délai de trois mois mais l'organisme chargé de la tenue des listes de confiance a tardé à exécuter cette mise à jour ! En effet, et de manière assez étonnante, le Règlement ne souffle mot d'un délai à charge de cet organisme. Ici aussi, on peut raisonnablement estimer qu'un délai de quelques heures voire quelques jours serait un maximum acceptable.

Les listes de confiance consacrées par l'article 22 sont une des pierres angulaires du Règlement[108]. En effet, elles seront sécurisées et accessibles en ligne à tout moment, permettant ainsi à tout utilisateur de vérifier aisément et de manière fiable si un prestataire auquel il compte recourir est effectivement inscrit sur la liste et dispose du « statut qualifié ».

Plus précisément, l'article 22 stipule, d'une part, que ce sont les EM qui sont responsables d'établir, de tenir à jour et de publier, de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance mais que d'autre part, ils sont tenus de communiquer à la Commission, dans les meilleurs délais, des informations relatives à l'organisme chargé de la tenue des listes nationales de confiance, ainsi que des détails précisant où ces listes sont publiées, indiquant les certificats utilisés pour apposer une signature électronique ou un cachet électronique sur ces listes et signalant les modifications apportées à ces listes. L'article 22.4. précise que la Commission met à la disposition du public, par l'intermédiaire d'un canal sécurisé, ces différentes informations. De la sorte, la Commission centralisera l'ensemble des listes de confiance nationales en un seul point, ainsi accessibles à tous les citoyens de l'Union européenne.

Pour que ces listes de confiance puissent être créées et mises à la disposition du public de manière sécurisée tant au niveau national qu'au niveau européen, l'article 22.5. consacre l'obligation pour la Commission de préciser, au moyen d'actes d'exécution, les informations contenues dans ces listes de confiance et de définir les spécifications techniques et les formats applicables à celles-ci. Ces actes d'exécution doivent être adoptés au plus tard le 18 septembre 2015[109].

On le voit, et contrairement à la directive 1999/93/CE qui se limitait à mettre en place un système de « déclaration » préalable par les prestataires qualifiés et l'éventualité d'un contrôle *a posteriori* sans délai spécifique, le Règlement consacre une régime « d'autorisation » préalable. Ainsi, le Règlement instaure une procédure durant laquelle l'organe de contrôle ne dispose (en principe) que de 3 mois pour examiner et valider ou non la demande et prendre ainsi la décision d'octroyer ou non le statut « qualifié » au

[107] Cette affirmation découle d'une lecture *a contrario* de l'article 21.3.

[108] En ce sens, le considérant n° 46 indique que « Les listes de confiance sont des éléments essentiels pour fonder la confiance des opérateurs économiques, car elles indiquent le statut qualifié du prestataire de service au moment du contrôle ».

[109] La liste de confiance établie par la décision 2009/767/CE de la Commission, modifiée par la décision 2010/425/UE de la Commission, servira probablement de base à la préparation des actes d'exécution pris en vertu du présent règlement.

prestataire[110]. Par ailleurs, l'intervention de l'autorité de contrôle ne se limite plus à contrôler les prestataires de signature électronique mais s'étend aux prestataires de tous les autres services de confiance (cachet, horodatage, envoi recommandé et authentification de site web).

On notera aussi que le texte du Règlement adopté a sensiblement évolué par rapport à la version initiale proposée par la Commission, dont l'article 17 permettait au prestataire de fournir ses services dès la notification de sa demande et la remise du rapport d'audit, sans même attendre la décision (qui pouvait être négative) de l'autorité de contrôle. On peut se réjouir de cette évolution qui démontre la prise de conscience du législateur européen de la nécessité, dans un tel domaine, de tout mettre en œuvre pour renforcer la confiance du citoyen en ces services et éviter qu'un prestataire commence à commercialiser des services de confiance qualifiés pour peut-être apprendre après quelques mois par l'organe de contrôle que les services…ne sont pas qualifiés. Mais il faut reconnaître que, ce faisant, le législateur égratigne au passage le traditionnel principe de l'interdiction de mettre en place un régime d'autorisation préalable qu'il a lui-même consacré notamment dans la directive « commerce électronique »[111].

iv. Le label de confiance de l'Union pour les services de confiance qualifiés

La confiance dans les services en ligne et leur commodité sont essentiels pour que les utilisateurs tirent pleinement avantage des services électroniques et qu'ils s'y fient en connaissance de cause. À cet effet, l'article 23 du Règlement prévoit la création d'un label de confiance de l'Union qui permet d'identifier les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés. De la sorte, ce label distinguerait clairement les services de confiance qualifiés des services de confiance non qualifiés, contribuant ainsi à la transparence du marché[112].

La création de ce label ne se trouvait pas dans la proposition de la Commission mais résulte d'une demande insistante du Parlement européen. Nous pouvons appuyer cette initiative car elle est de nature à renforcer la transparence et la confiance. De surcroît, elle est peu contraignante car l'utilisation du label par les prestataires n'est prévue que sur une base volontaire[113].

Ainsi, l'article 23.1. stipule que lorsqu'un prestataire a obtenu le statut qualifié et que celui-ci est inscrit sur la liste de confiance, il peut utiliser le label de confiance de l'Union pour indiquer d'une manière simple, claire et reconnaissable les services de confiance qualifiés qu'il fournit. Le cas échéant, il doit veiller à ce qu'un lien vers la liste de confiance concernée soit disponible sur son site Internet[114].

On notera enfin que, si l'utilisation de ce label par les prestataires repose sur une base volontaire, la Commission est par contre tenue d'établir pour le 1er juillet 2015 au plus tard, au moyen d'actes d'exécution, les spécifications relatives à la forme et notamment à la présentation, à la composition, à la taille et à la conception du label de confiance de l'Union pour les services de confiance qualifiés[115].

---

[110] On notera au passage que le règlement ne souffle mot du régime volontaire d'accréditation, qui était autorisé par la directive. Ceci étant, il faut reconnaître que le régime « d'autorisation préalable » établi par le règlement se rapproche sensiblement du régime d'accréditation, tant au niveau des objectifs que dans la procédure et les effets…

[111] Article 4 de la directive (CE) 2000/31 du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *J.O.*, L. 178, 17 juillet 2000.

[112] Ses détracteurs invoqueront, à l'inverse, que ce label mettra inutilement ou exagérément les services de confiance qualifiés sur un piédestal, au détriment du développement des services de confiance non qualifiés. Nous ne le croyons pas car nous pensons qu'il existe un marché différent pour ces deux catégories de services.

[113] Considérant n°47.

[114] Article 23.2.

[115] Article 23.3. Cet acte d'exécution a été adopté le 22 mai 2015. Règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés, *JOUE*, 23 mai 2015, disponible via le lien suivant : http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1434707231806&uri=CELEX:32015R0806

v. Régime de contrôle

A l'instar de la directive 1999/93/CE, le Règlement fait obligation aux EM d'instaurer un système adéquat permettant de contrôler les prestataires de services de confiance. Toutefois, et comme nous allons le voir, le Règlement va bien au-delà en consacrant une obligation pour les EM de désigner un organe de contrôle ainsi qu'en précisant et en étendant le mandat de cet organe[116]. 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 EM.

Comme indiqué, l'article 17 fait obligation aux EM de désigner un organe de contrôle, et de doter ces derniers des pouvoirs nécessaires et des ressources adéquates pour l'exercice de leurs tâches. Pour procéder à cette désignation, le Règlement laisse le choix à l'EM entre un organe de contrôle établi sur son territoire ou un organe de contrôle établi sur le territoire d'un autre EM, moyennant l'accord préalable de cet autre EM[117]. Une fois désigné, l'EM est tenu de notifier à la Commission les coordonnées de cet organe de contrôle.

L'organe de contrôle est tenu de contrôler tous les prestataires de services de confiance, qu'ils soient qualifiés ou non. Toutefois, on peut immédiatement tempérer ce principe en précisant que l'intervention de cet organe va sensiblement varier en fonction de la catégorie à laquelle appartient le prestataire contrôlé.

Soit il s'agit d'un prestataire de services de confiance *qualifiés*, auquel cas l'article 17, 3., a) stipule que l'organe est tenu de contrôler les prestataires « établis sur le territoire de l'État membre qui a procédé à la désignation afin de s'assurer, par des activités de contrôle *a priori et a posteriori*, que ces prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences fixées dans le présent règlement ».

Les nombreuses exigences à charge des prestataires qualifiés, et les effets juridiques dont bénéficient leurs services, justifient que ceux-ci fassent l'objet d'un contrôle minutieux, sans lequel la confiance placée en eux pourrait être ébranlée. Ceux-ci font donc l'objet d'un contrôle *a priori* dans le cadre de la procédure de lancement d'un service de confiance qualifié[118] mais également *a posteriori* dans le cadre de l'audit périodique (tous les deux ans)[119], d'un éventuel audit extraordinaire sur demande de l'organe de contrôle[120] ou encore suite à une éventuelle notification par le prestataire d'une atteinte à la sécurité[121]. Il convient de préciser que le Règlement met à charge des prestataires les frais liés aux audits précités.

[116] 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) !

[117] 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 malheureusement pas abouti…

[118] Article 21.

[119] Article 20.1. Ce contrôle bisannuel a pour but de confirmer que le prestataire se conforme toujours aux exigences du règlement.

[120] Article 20.2. Cet audit extraordinaire peut être demandé à tout moment. Le cas échéant, et vu la charge et les frais que peuvent représenter un tel audit pour le prestataire, le considérant n°43 précise que « il convient que l'organe de contrôle applique, notamment, les principes de bonne administration, y compris l'obligation de motiver ses décisions, ainsi que le principe de proportionnalité. Par conséquent, l'organe de contrôle devrait dûment justifier sa décision d'exiger une évaluation spécifique de la conformité ».

[121] Article 19.

Soit il s'agit d'un prestataire de services de confiance *non qualifiés*, auquel cas l'article 17, 3., b) indique que l'organe doit uniquement « prendre des mesures, *si nécessaire*, en ce qui concerne les prestataires (…) établis sur le territoire de l'État membre qui a procédé à la désignation, par des activités de contrôle *a posteriori*, *lorsqu'il est informé que* ces prestataires de services de confiance non qualifiés ou les services de confiance qu'ils fournissent ne satisferaient pas aux exigences fixées dans le présent règlement ».

Cette disposition a fait l'objet de nombreuses discussions lors des négociations entre partisans d'un contrôle étendu des prestataires non qualifiés et partisans de l'absence de contrôle de ces prestataires. C'est finalement une solution de compromis qui a été retenue. Il convient ainsi de retenir que, ayant pris conscience de la charge de travail et des responsabilités que cela pouvait engendrer pour l'organe de contrôle, la volonté du législateur européen est d'éviter que cet organe soit tenu à une « obligation générale de contrôler des prestataires de services non qualifiés »[122] tout en essayant d'éviter l'absence totale de réactions de l'organe de contrôle dans l'hypothèse où un problème grave serait constaté auprès d'un prestataire non qualifié. Comme le précise le considérant n°23, « les prestataires de services de confiance non qualifiés devraient être soumis à un contrôle *a posteriori allégé et réactif* justifié par la nature de leurs services et activités. L'organe de contrôle *ne devrait intervenir que lorsqu'il est informé* (par exemple, par le prestataire de services de confiance non qualifié lui-même, par un autre organe de contrôle, par une notification émanant d'un utilisateur ou d'un partenaire économique ou sur la base de ses propres investigations) qu'un prestataire de services de confiance non qualifié ne satisfait pas aux exigences du présent règlement ».

Les tâches concrètes de l'organe de contrôle sont multiples et variées. Elles sont énumérées de manière non limitative à l'article 17.4.. En synthèse, ces tâches consistent notamment en :

- la coopération (échanges de bonnes pratiques et enquêtes conjointes par exemple) avec d'autres organes de contrôle et l'assistance mutuelle en cas de demande d'un de ces derniers[123] ;

- l'analyse des rapports d'évaluation de la conformité dans le cadre tant de la procédure de lancement[124] que de l'audit bisannuel ou extraordinaire[125] ;

- l'injonction aux prestataires de corriger tout manquement aux obligations fixées par le Règlement ;

- l'information des autres organes de contrôle et du public en cas d'atteintes à la sécurité ou de pertes d'intégrité[126] et, le cas échéant, des autorités chargées de la protection des données lorsque ces atteintes et/ou les audits montrent une violation des règles en matière de protection des données à caractère personnel ;

- la préparation et l'envoi à la Commission de son rapport annuel sur ses principales activités, accompagné d'un résumé des éventuelles notifications d'atteinte à la sécurité[127] ;

- l'attribution du statut qualifié conformément à la procédure de lancement[128] ou le retrait éventuel de ce statut dans le cas où un (ou plusieurs) manquement (grave) constaté par l'autorité ne sont

[122] Considérant n° 36.
[123] Article 18. En principe, un organe de contrôle est tenu de répondre positivement à une demande d'assistance mutuelle faite par un organe d'une autre EM. Toutefois, l'article 18.2. énumère les hypothèses dans lesquelles cette assistance peut être refusée.
[124] Article 21.
[125] Article 20.
[126] Conformément à l'article 19.
[127] Article 17.6. L'article 17.7. prévoit que la Commission met ce rapport annuel à la disposition des EM. Comme l'indique le considérant n° 40, cette obligation permet à « la Commission et aux États membres d'évaluer l'efficacité du mécanisme de contrôle renforcé instauré par le présent règlement (…) et serait déterminant pour faciliter l'échange de bonnes pratiques entre les organes de contrôle et permettrait de vérifier la mises en œuvre cohérente et efficace des exigences de contrôle essentielles dans tous les États membres ».

pas résorbés[129], et le cas échéant, la transmission de ces informations à l'organisme chargé de la mise à jour de la liste de confiance nationale ;

- la vérification de l'existence et de l'application correcte des dispositions relatives aux plans d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse son activité[130], y compris la façon dont les informations restent accessibles conformément à l'article 24.2.h).

vi. Les exigences applicables aux prestataires de services de confiance

Le Règlement procède clairement à une distinction entre les exigences applicables à l'ensemble des prestataires de services de confiance, qualifiés ou non, et celles uniquement applicables aux prestataires de services de confiance qualifiés.

Le tronc commun applicable à l'ensemble des prestataires de services de confiance concerne uniquement les exigences de « sécurité » consacrées par l'article 19. On sait que le « traumatisme » engendré notamment par l'affaire « Diginotar » aux Pays-Bas a marqué tous les experts en ce domaine[131]. On ne dévoilera pas un secret en indiquant que cette affaire apparaissait systématiquement en trame de fond lorsque les discussions au Conseil européen portaient sur les exigences relatives à la sécurité.

Ce tronc commun se traduit par une obligation générale de sécurité et par une obligation de notification en cas d'atteinte à la sécurité.

L'article 19.1. prévoit en effet que tous les prestataires « prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents ».

L'article 19.2. stipule que tous les prestataires « notifient, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés (…) toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées ». Le même article ajoute que cette notification doit également être faite dans les meilleurs délais à la personne physique ou morale à laquelle le service de confiance a été fourni si cette atteinte risque de lui porter préjudice.

Dans l'hypothèse où les conséquences de l'atteinte seraient importantes, le Règlement prévoit en outre l'obligation pour l'organe de contrôle, d'une part, d'informer les organes de contrôle des autres EM concernés ainsi que ENISA[132], notamment lorsque l'atteinte concerne deux EM ou plus et, d'autre part, d'informer le public ou d'exiger du prestataire de services de confiance qu'il le fasse, dès lors qu'il constate qu'il est dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité.

---

[128] Article 21.

[129] Article 20.3. Pour prendre cette décision de retrait de la liste de confiance, l'organe de contrôle doit tenir compte en particulier, de l'ampleur, de la durée et des conséquences de ce manquement. Cette décision de retrait peut porter sur le prestataire lui-même, impliquant par voie de conséquence tous les services qualifiés qu'il offre, ou simplement un des services qualifiés qu'il offre.

[130] Article 24.2.i). Comme l'indique le considérant n° 41, cette obligation poursuit l'objectif « d'assurer la pérennité et la durabilité des services de confiance qualifiés et d'accroître la confiance des utilisateurs dans la continuité de ces services ».

[131] Sur cette affaire et ses conséquences, voy. notamment http://en.wikipedia.org/wiki/DigiNotar ; http://www.computerworld.com/s/article/9233138/One_year_after_DigiNotar_breach_Fox_IT_details_extent_of_compromise

[132] European Union Agency for Network and Information Security : http://www.enisa.europa.eu/

L'article 24, quant à lui, détermine les (nombreuses) exigences applicables uniquement aux prestataires de services de confiance qualifiés, qui doivent être scrupuleusement respectées afin d'être reconnus comme tels. Vu la longue énumération de ces exigences, outre le fait que celles-ci s'inspirent globalement de l'annexe II de la directive 1999/93/CE, nous nous permettons de renvoyer à la lecture de l'article 24 ainsi qu'à certains commentaires faits à l'époque sur l'annexe II de la directive[133].

Pour le reste, nous nous limiterons à formuler les commentaires suivants.

L'article 24.1. détermine les méthodes permettant de vérifier l'identité et les éventuels attributs spécifiques d'une personne physique ou morale qui demande un certificat qualifié (pour une signature ou un cachet électronique par exemple). Le Règlement propose au prestataire de services de confiance qualifié quatre méthodes pour opérer cette vérification, qui peut se réaliser soit en présentiel soit à distance. On précisera toutefois que même si cette vérification peut être faite à distance, elle ne pourra l'être que via des moyens fiables qui ont nécessité au début du processus de délivrance une présence en personne ou, à tout le moins, qui offrent une garantie équivalente en termes de fiabilité à la présence en personne.

Concernant la transparence relative au statut du certificat, le Règlement prévoit désormais que les prestataires qui délivrent des certificats qualifiés fournissent à toute partie utilisatrice des informations sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace[134]. En outre, lorsque le même prestataire révoque un certificat, il enregistre cette révocation dans sa base de données relative aux certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication[135]. Les articles 28.4. et 38.4. précisent enfin que « Si un certificat qualifié (…) a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur ».

Selon le Règlement, un certificat qualifié doit donc pouvoir être révoqué, et ce Règlement harmonise les règles dans l'hypothèse d'une révocation. Qu'en est-il d'une éventuelle suspension d'un certificat qualifié ? Pour la suspension, le Règlement n'harmonise que partiellement la question. En effet, le considérant n°53 indique clairement que le Règlement n'impose pas « aux prestataires de services de confiance ou aux EM de recourir à la suspension, mais devrait prévoir des règles en matière de transparence, dans les cas où cette pratique est disponible ». Comme le souligne le même considérant, 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. La sécurité juridique impose que le statut de suspension d'un certificat soit toujours clairement indiqué »[136].

Dès lors, les articles 28.5. et 38.5. autorisent les EM à établir des règles nationales relatives à la suspension temporaire d'un certificat qualifié pour autant que les deux conditions suivantes soient remplies. 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

[133] Voy. les références citées à la note de bas de page n°4. Pour un commentaire des même exigences dans la loi belge du 9 juillet 2001 qui transpose la directive 1999/93/CE, voy. D. GOBERT, *op. cit.*, note de bas de page n°5. Voy. également E. CAPRIOLI, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.229 et s. On notera que l'annexe II de la directive ne s'appliquait qu'aux prestataires de service de certification délivrant des certificats qualifiés pour la signature électronique alors que l'article 24 du règlement s'applique plus largement à l'ensemble des prestataires de services de confiance qualifiés, sans égard au(x) service(s) offert(s) par ces derniers.

[134] Article 24.4.

[135] Article 24.3.

[136] C'est le cas en Belgique, qui prévoit notamment le mécanisme de suspension des certificats de signature et d'authentification utilisés dans le cadre de la carte d'identité électronique.

de données relative aux certificats et le statut de suspension est visible, pendant la période de suspension, auprès du service fournissant les informations sur le statut du certificat. On se demande s'il n'eût pas été plus opportun d'exiger, comme c'est le cas pour la révocation, la visibilité des données relatives à la période de suspension « à tout moment », et non uniquement « pendant la période de suspension »[137].

Enfin, relevons que les points e) et f) de l'article 24.2. prévoient une obligation générale d'utiliser des « systèmes et produits fiables ». Afin de faciliter la tâche aux prestataires, l'article 24.5. donne la possibilité à la Commission de déterminer, au moyen d'actes d'exécution, les numéros de référence des normes applicables à ces systèmes et produits fiables. Si les prestataires respectent ces normes, ils sont présumés satisfaire aux exigences du Règlement.

vii. Responsabilité des prestataires de service de confiance

Le texte relatif à la responsabilité des prestataires de service de confiance finalement adopté a sensiblement évolué par rapport à celui de la proposition de règlement de la Commission[138].

Alors que la proposition de règlement consacrait une présomption de responsabilité à charge de tous les prestataires de service de confiance en cas de non-respect du Règlement, l'article 13 du Règlement opère à l'inverse une distinction claire entre prestataires qualifiés et non qualifiés.

S'il s'agit d'un prestataire de services de confiance *non qualifiés*, la charge de la preuve du comportement fautif du prestataire de service pèse sur la personne physique ou morale qui a subi les dommages. Il lui incombe donc de prouver que, intentionnellement ou par négligence, le prestataire a manqué à ses obligations prévues par le Règlement et que le dommage est la conséquence de ce manquement.

S'il s'agit d'un prestataire de services de confiance *qualifiés*, la charge de la preuve de l'exécution non fautive de ses obligations pèse sur ce prestataire. En effet, il est présumé responsable, à moins qu'il ne prouve que les dommages ont été causés sans intention ni négligence de sa part.

Cette distinction se justifie essentiellement par la volonté du législateur européen de ne pas faire peser un régime juridique trop lourd sur les prestataires non qualifiés, au risque de freiner le développement de cette catégorie de prestataires, d'autant que les services offerts par ces derniers ne bénéficient pas des « incitants » qui découlent des clauses d'assimilation ou des présomptions exposées plus haut.

Par ailleurs, et contrairement à la proposition de la Commission qui ne prévoyait rien sur ce point, l'article 13.2. permet aux prestataires de services de confiance de ménager contractuellement leur responsabilité. En effet, afin de faciliter l'évaluation du risque financier que les prestataires de services de confiance pourraient devoir supporter ou qu'ils devraient couvrir au moyen d'une police d'assurance, le Règlement les autorise à fixer des limites, sous deux conditions, à l'utilisation des services qu'ils proposent. Le cas échéant, ils ne sont pas tenus pour responsables des dommages résultant de l'utilisation de services allant au-delà de ces limites.

Les deux conditions sont les suivantes. Premièrement, les clients doivent être dûment informés à l'avance des limites fixées. Deuxièmement, ces limites doivent être reconnaissables par des tiers[139], par exemple par l'insertion d'une notice relative à ces limites dans les conditions applicables au service fourni ou par d'autres moyens reconnaissables[140]. Contrairement à la directive, le Règlement n'exige donc plus

[137] Il est vrai que, *a priori*, on ne lève la suspension d'un certificat que si on acquiert une relative certitude que ce dernier n'a pas été usurpé. Mais rien n'empêche *a posteriori* de se rendre compte que l'on s'est trompé… De surcroît, durant la période de suspension, aucun acte ne devrait être posé à l'aide de ce certificat puisqu'il a en principe perdu sa validité durant cette période.

[138] Proposition du 4 juin 2012, *op.cit.*, article 9, p. 25.

[139] Notamment par une partie utilisatrice, telle une partie qui vérifie une signature ou un cachet électronique ou encore un destinataire d'un envoi recommandé électronique par exemple.

[140] Considérant n°37.

que ces limites soient indiquées dans le certificat qualifié lui-même, ce qui est assez logique puisque tous les services de confiance n'utilisent pas nécessairement un certificat. Ceci étant, rien n'empêche un prestataire de signature ou de cachet électronique d'indiquer ces limites dans le certificat. Cette pratique présente un double avantage : de la sorte, ces limites seront assurément reconnaissables par des tiers[141] et elles pourraient éventuellement bénéficier à l'utilisateur du service de confiance[142].

Précisons en outre que, selon l'article 13.3., les principes présentés « s'appliquent conformément aux règles nationales en matière de responsabilité ». Le considérant n°37 ajoute que le « règlement n'affecte donc pas ces règles nationales, par exemple celles relatives à la définition des dommages, au caractère intentionnel ou à la négligence, ou les règles procédurales applicables en la matière ».

Enfin, le Règlement ne traite pas de la responsabilité de la partie utilisatrice, cette question étant laissée au droit national[143].

viii. Aspects internationaux et accessibilité aux personnes handicapées

Dans une économie mondialisée et un environnement Internet qui ne connaît pas les frontières, le Règlement ne pouvait se dispenser d'une disposition visant à étendre ses « effets bénéfiques » en dehors de l'Union européenne.

Ainsi, l'article 14 prévoit que « les services de confiance fournis par des prestataires de services de confiance établis dans un pays tiers sont reconnus comme équivalents, sur le plan juridique, à des services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union lorsque les services de confiance provenant du pays tiers sont reconnus en vertu d'un accord conclu entre l'Union et le pays tiers concerné ou une organisation internationale ». Seul l'accord international permet désormais d'assurer la reconnaissance des services de confiance qualifiés au-delà des frontières de l'Union[144].

L'accord devra veiller à ce que les prestataires établis dans un pays tiers soient soumis aux mêmes exigences que celles applicables aux prestataires établis dans l'Union, c'est-à-dire à toutes les exigences du Règlement, y compris celles relatives au contrôle, à la procédure d'autorisation préalable et à l'inscription sur la liste de confiance[145].

Les négociateurs de la proposition de règlement ont également veillé à ce que les prestataires établis dans l'Union bénéficient du principe de réciprocité[146]. Ainsi, l'accord international prévoira également que « les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union sont reconnus comme équivalents, sur le plan juridique, à des services de confiance fournis par des prestataires de services de confiance dans le pays tiers ou par l'organisation internationale avec lesquels l'accord est conclu ».

Enfin, on notera la volonté du législateur européen de tout mettre en œuvre pour que les personnes handicapées puissent utiliser les services de confiance dans les mêmes conditions que les autres consommateurs. A cet effet, l'article 15 stipule que « Dans la mesure du possible, les services de confiance fournis, ainsi que les produits destinés à un utilisateur final qui servent à fournir ces services,

[141] A tout le moins plus reconnaissables que si elles étaient « dissimulées » dans les conditions d'utilisation uniquement disponibles sur le site web du prestataire.
[142] Par exemple, une personne qui signe électroniquement ou qui appose un cachet électronique ne devrait pas être tenues au-delà des limites indiquées dans le certificat, limites dont la partie utilisatrice est dûment informée par la consultation du certificat lors de la vérification de la signature ou du cachet.
[143] Voy. *infra*.
[144] En effet, le Règlement n'a pas repris les deux autres mécanismes de reconnaissance consacrés par l'article 7.1. a) et b) de la directive 1999/93 (accréditation du prestataire établi dans un pays tiers ou garantie de ses services par un prestataire établi dans l'Union).
[145] Article 25.2. a).
[146] Ce que la directive n'avait prévu que de manière optionnelle dans son article 7.3.

sont accessibles aux personnes handicapées ». Le considérant 29 précise que « L'évaluation de la faisabilité devrait inclure, entre autres, des considérations d'ordre technique et économique ».

Les principes généraux applicables à l'ensemble des services de confiance étant présentés, concentrons-nous désormais sur chaque services de confiance, que nous allons commenter successivement.

B. Les services de confiance en particulier

i. Les signatures électroniques

La section 4 du chapitre 3 relative aux signatures électroniques est probablement celle qui offre le moins de nouveautés dans le Règlement, dans la mesure où elle reprend en grande partie les dispositions de la directive 1999/93/CE. Après, il est vrai, certaines reformulations, précisions, suppressions et ajouts. Nous nous limiterons à commenter les modifications et nouveautés substantielles apportées par le Règlement. Pour le surplus, et pour éviter d'allonger inutilement la présente contribution, nous nous permettons de renvoyer à la lecture des dispositions du Règlement ainsi qu'aux commentaires relatifs à la directive de 1999[147].

L'article 25 relatif aux effets juridiques des signatures électroniques reprend les clauses déjà bien connues, d'une part, de non-discrimination et, d'autre part, d'assimilation qui avaient été consacrées par l'article 5 de la directive[148]. Il simplifie toutefois la formulation de ces clauses, ce qui rend plus aisé leur lecture et leur compréhension.

Le Règlement prévoit que, si on utilise une signature électronique *qualifiée*, son effet juridique est équivalent à celui d'une signature manuscrite. Le Règlement ne va pas plus loin dans l'harmonisation. En d'autres mots, il appartient au droit national de définir l'effet juridique produit par la signature manuscrite, et donc celui de la signature électronique qualifiée, effet qui peut varier d'un EM à l'autre… On reconnaîtra dès lors que l'article 25.3., qui consacre le principe de reconnaissance mutuelle des signatures électroniques qualifiées, pourrait n'avoir qu'un effet limité dans le cadre de certaines transactions transfrontières !

Si on utilise une signature électronique *non qualifiée*, celle-ci ne peut pas se voir refuser un effet juridique au seul motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de la signature électronique qualifiée[149]. Pour le reste, et ici aussi, il appartient au droit national de définir l'étendue des effets juridiques produits par les signatures électroniques non qualifiées.

L'article 27 consacre des nouveautés touchant à l'utilisation des signatures électroniques *avancées* dans les services publics. Une signature électronique avancée est une catégorie intermédiaire qui se situe entre la signature électronique « simple » et la signature électronique « qualifiée », catégorie qui doit satisfaire aux quatre exigences stipulées dans l'article 26[150]. S'il est vrai que cette catégorie intermédiaire ne bénéficie pas de la clause d'assimilation, il a été constaté que les services publics dans les EM utilisent néanmoins différents formats de signature électronique avancée pour signer électroniquement leurs documents. Il semblait donc nécessaire de faire en sorte que les EM, lorsqu'ils reçoivent des documents signés électroniquement, puissent prendre en charge techniquement au moins un certain nombre de formats de signature électronique avancée.

---

[147] Articles 25 à 34 du règlement. Pour un commentaire de la directive 1999/93/CE, voy. les références citées à la note de bas de page n°4. Pour un commentaire des même exigences dans la loi belge du 9 juillet 2001 qui transpose la directive 1999/93/CE, voy. D. Gobert, *op. cit.*, note de bas de page n°5.

[148] La portée et l'intérêt de cette distinction ont déjà été développés dans le sous-point ii) des principes généraux ci-avant, auquel nous renvoyons le lecteur.

[149] Considérant n° 49.

[150] Ces exigences correspondent *grosso modo* à celles qui étaient contenues dans l'article 2, 2) de la directive de 1999.

A cet effet, l'article 27.5. charge la Commission de définir « pour le 18 septembre 2015 au plus tard, au moyen d'actes d'exécution, les formats de référence des signatures électroniques avancées ou les méthodes de référence lorsque d'autres formats sont utilisés ». Sur cette base, les points 1 et 2 de l'article 27 prévoient que si un EM exige une signature électronique avancée pour utiliser un service en ligne offert par un organisme du secteur public ou pour l'utiliser au nom de cet organisme, il est tenu de reconnaître les signatures électroniques avancées (et de niveaux supérieurs) au moins dans les formats ou utilisant les méthodes définis dans les actes d'exécution précités. Une telle exigence devrait permettre une plus grande harmonisation (technique) mais également une facilitation de l'utilisation transfrontière des signatures électroniques avancées.

L'article 27.3. indique que les EM « *n'exigent pas*, pour une utilisation transfrontalière dans un service en ligne offert par un organisme du secteur public, de signature électronique présentant un niveau de sécurité supérieur à celui de la signature électronique qualifiée ». Une exigence comparable était déjà consacrée par l'article 3.7. de la directive sous une formulation « permissive »[151]. Toutefois, la formulation « interdictive » utilisée par le Règlement démontre une volonté de mettre fin à toutes exigences supplémentaires dans le secteur public qui pourraient porter atteinte à l'utilisation transfrontière des signatures électroniques (qualifiées).

L'article 28 détermine les exigences applicables aux certificats qualifiés de signature électronique, cet article renvoyant lui-même aux exigences techniques de l'annexe I. On retiendra que cette liste d'exigences est maximale. En effet, en vue d'assurer l'interopérabilité et la reconnaissance transfrontalière des certificats qualifiés, les EM ne peuvent pas prévoir d'autres exigences obligatoires[152]. Toutefois, le Règlement permet, au niveau national, d'intégrer dans les certificats qualifiés des attributs spécifiques supplémentaires pour autant que ceux-ci soient non obligatoires et qu'ils n'affectent pas l'interopérabilité et la reconnaissance des signatures électroniques qualifiées[153]. On notera enfin que la Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés, et que ceux-ci sont présumés satisfaire aux exigences fixées à l'annexe I lorsqu'ils respectent ces normes. Gageons que la Commission mette rapidement en œuvre cette faculté en vue de faciliter la tâche des fournisseurs de tels certificats.

Les articles 29 à 31 du Règlement sont consacrés aux dispositifs de création de signature électronique qualifiés[154]. Il s'agit concrètement de dispositifs logiciel (de cryptologie par exemple) et/ou matériel (une carte à puce par exemple) qui sont configurés en vue de créer une signature électronique (qualifiée). Les exigences à respecter pour ces dispositifs sont fixées à l'annexe II. Tout comme pour les certificats qualifiés, la Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux dispositifs de création de signature électronique qualifiés. Ces derniers sont présumés satisfaire aux exigences fixées à l'annexe II lorsqu'il respecte ces normes.

L'article 30 prévoit en outre une exigence supplémentaire pour les dispositifs de création de signature électronique qualifiés : la *certification* de leur conformité avec les exigences fixées à l'annexe II. Cette certification est opérée par les organismes publics ou privés compétents désignés par les EM. Pour les y aider, le Règlement impose judicieusement à la Commission d'établir, au moyen d'actes d'exécution, une liste de normes relatives à l'évaluation de la sécurité des produits informatiques. Une fois certifiés, les EM sont tenus de les notifier à la Commission, qui est ainsi chargée d'établir, de publier et de mettre à jour

[151] Article 3.7. de la directive 1999/93/CE : « Les États membres *peuvent* soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Ces exigences *ne doivent pas* constituer un obstacle aux services transfrontaliers pour les citoyens ».

[152] Article 28.2.

[153] Article 28.3. et considérant n°54. Ce dernier donne comme exemple d'attribut spécifique des « identifiants uniques », mais pourrait selon nous aussi viser des qualifications ou titres liés à une personne tels que médecin, avocat, notaire, administrateur-délégué, …

[154] Voy. aussi les considérants n° 51, 52, 55 et 56.

une liste des dispositifs de création de signature électronique qualifiés qui sont certifiés. Cette certification n'existait pas dans le directive 1999 et n'était prévue que de manière facultative dans la proposition de règlement de la Commission. Elle est désormais obligatoire. Certes, cette certification offre un niveau supplémentaire d'assurance et de sécurité mais représente aussi un coût non négligeable pour les fournisseurs. Espérons que ce coût ne sera pas de nature à restreindre l'offre de signatures électroniques qualifiées…

Par rapport à la directive, le Règlement innove également en consacrant les articles 32 et 33 relatifs au processus et au service de *validation* des signatures électroniques qualifiées.

L'article 32 détermine l'ensemble des éléments qui doivent être vérifiés durant le processus de validation pour pouvoir confirmer la validité d'une signature électronique qualifiée, dont notamment la validité du certificat qualifié au moment de la signature. Cet article ajoute que le système de validation doit fournir à la partie utilisatrice le résultat correct du processus de validation et permettre à celle-ci de détecter tout problème pertinent relatif à la sécurité.

L'article 33 traite du service de validation qualifié des signatures électroniques qualifiées. Celui-ci stipule que ce service ne peut être fourni que par un prestataire de services de confiance qualifié, que ce dernier doit fournir une validation qui respecte les exigences de l'article 32 et que le service doit permettre aux parties utilisatrices de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire.

Comme pour les autres éléments techniques liés à la signature électronique, la Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables à la validation et au service de validation qualifié des signatures électroniques qualifiées. Cette validation et ce service sont présumés satisfaire aux exigences des articles 32 et 33 lorsqu'ils respectent ces normes.

On notera que si le Règlement promeut la validation et l'offre de service de validation de signature électronique qualifiée[155], tout en déterminant les conditions, il ne consacre par contre aucune obligation à charge de la partie utilisatrice de vérifier la signature et ne prévoit pas non plus de responsabilité particulière de cette partie en cas de non vérification préjudiciable de la signature. Cette question semble donc relever de la prérogative des EM. Ceci étant, on peut espérer que, dans un objectif de sécurité juridique, les articles 32 et 33 feront de la validation de signatures électroniques qualifiées une procédure aisée, adaptée à toutes les parties et généralisée au sein de l'Union.

Le Règlement 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 qualifiera de générales, lorsqu'il respecte ces normes.

On pourrait qualifier cet article « d'embryon de disposition » sur l'archivage électronique[156]. 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

[155] Voy. considérant n° 57.

[156] 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 ».

l'archivage électronique sont nombreuses et variées[157]. Nous le regrettons et nous constatons que le législateur européen disposait d'une opportunité qu'il n'a malheureusement pas saisie[158].

On notera enfin que le Règlement permet l'utilisation de pseudonymes dans les transactions électroniques[159], et plus particulièrement dans les certificats de signature électronique[160]. Le cas échéant, il doit être clairement indiqué qu'il s'agit d'un pseudonyme. Le Règlement ne prévoit par contre aucune obligation pour le fournisseur de conserver l'identité des personnes qui « se cachent » derrière un pseudonyme, ce qui peut être nécessaire dans le cadre de procédure judiciaire. Cette obligation d'identification est laissée à la liberté des EM comme le confirme le considérant n° 33 : « Les dispos itions relatives à l'utilisation de pseudonymes dans des certificats ne devraient pas empêcher les États membres d'exiger l'identification des personnes en vertu du droit national ou du droit de l'Union ».

ii. Le cachet électronique *versus* la signature électronique

La section 5 du chapitre 3 traite des cachets électroniques. Ce nouveau service de confiance créé par le Règlement permet de certifier le lien entre les données électroniques « cachetée » et une personne morale[161]. Il s'agit d'une espèce de « sceau » électronique sécurisé dédié aux personnes morales[162]. Le considérant n° 59 précise que « Les cachets électro niques devraient servir à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document ». Le considérant n° 65 ajoute 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 ».

En pratique, la technologie ainsi que les outils matériels et logiciels utilisés pour créer un cachet électronique sont identiques à ceux utilisés pour la création d'une signature électronique. Le cachet électronique se distingue toutefois principalement de la signature électronique en ce que cette dernière est réservée aux personnes physique alors que le cachet est dédié aux personnes morales. L'utilisateur et le créateur d'une signature électronique, et la personne qui est identifiée comme telle dans le certificat[163], est donc une personne physique[164]. Par contre, l'utilisateur et le créateur d'un cachet

[157] 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.

[158] Et qui s'explique en partie par la crainte (injustifiée mais néanmoins exprimée) 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, l'objectif du règlement eut été uniquement de 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.

[159] Article 5.

[160] Annexe I. L'utilisation de pseudonyme ne semble toutefois pas envisagé/permis pour les cachets électroniques (voir annexe III).

[161] De nombreuses discussions relatives à la notion de « personne morale » ont eu lieu au Conseil lors des négociations. Le constat ayant été fait qu'il n'existe pas d'harmonisation européenne en ce domaine, le règlement ne contient pas de définition de cette notion. Tout au plus, le considérant n° 68 indique que « La notion de "personne morale", d'après les dispositions du traité sur le fonctionnement de l'Union européenne relatives à l'établissement, laisse aux opérateurs le choix de la forme juridique qu'ils jugent appropriée pour l'exercice de leur activité. Par conséquent, on entend par "personne morale", au sens du traité sur le fonctionnement de l'Union européenne, toute entité constituée en vertu du droit d'un État membre ou régie par celui-ci, quelle que soit sa forme juridique ».

[162] La version anglaise utilise d'ailleurs le terme « seal », et non le terme « stamp ».

[163] L'article 3.14) définit le « certificat de signature électronique » comme « une attestation électronique qui associe les données de validation d'une signature électronique *à une personne physique* et confirme au moins le nom ou le pseudonyme de cette personne ».

[164] Les articles 25 à 34 relatifs à la signature électronique utilise d'ailleurs le terme de « signataire » qui est défini par l'article 3.9) comme « une *personne physique* qui crée une signature électronique ».

électronique, et la personne qui est identifiée comme telle dans le certificat[165], est une personne morale[166].

Un deuxième différence fondamentale réside dans les effets liés respectivement aux signature et cachet électroniques, ou à tout le moins aux effets que le Règlement n'a pas voulu donner au cachet électronique.

En effet, l'article 3.10) définit clairement la signature électronique comme « des données sous forme électronique (…) que le signataire *utilise pour signer* ». Or on sait que dans la plupart des EM, et même si le Règlement ne traite pas de cette question et n'harmonise pas les effets juridiques liés à la signature manuscrite, « signer » signifie non seulement s'identifier en tant qu'auteur du document mais également exprimer son consentement sur le contenu de ce dernier. Le fait d'utiliser sa signature (manuscrite ou électronique) a donc un pouvoir « engageant » pour la personne physique qui l'utilise.

Par contre, l'article 3.25) définit le cachet électronique comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique *pour garantir l'origine et l'intégrité de ces dernières* ». Le Règlement se garde bien d'utiliser le verbe « signer » pour le cachet électronique. Le Règlement ne prévoit donc pas que, à lui seul, le cachet électronique puisse engager juridiquement une personne morale[167]. Le Règlement n'a de toute évidence pas voulu toucher aux règles nationales de représentation des personnes morales[168].

Contrairement à la Belgique ou à l'Espagne qui connaissent la signature des personnes morales, et qui autorisent donc qu'un certificat de signature identifiant une personne morale puisse être utilisé pour engager juridiquement cette dernière, d'autres pays n'ont pas fait preuve d'une telle ouverture. Pour éviter tout risque de confusion mais également respecter la diversité des systèmes juridiques, le Règlement a donc fait le choix de créer deux services de confiance distincts en fonction de la catégorie d'utilisateur (personne physique ou morale) et de limiter la finalité du cachet électronique à la garantie de l'origine et à l'intégrité des données couvertes par ce cachet. Ceci étant, chaque EM reste libre de prévoir au niveau national que l'utilisation du cachet électronique peut engager directement la personne morale sur le plan juridique, alors même qu'aucune personne physique ne serait identifiée en tant que telle dans le cadre de l'utilisation de ce cachet. Par contre, pour les pays qui connaissent déjà la signature

[165] L'article 3.29) définit le « certificat de cachet électronique » comme « une attestation électronique qui associe les données de validation d'un cachet électronique *à une personne morale* et confirme le nom de cette personne ». Un certificat de cachet électronique n'identifie donc aucune personne physique, telles 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. Or, 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. Pour cette raison, le considérant n° 60 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 ».

[166] Pour le cachet électronique, le règlement n'utilise d'ailleurs pas le terme « signataire » mais simplement celui de « créateur de cachet », définit par l'article 3.24) comme « une *personne morale* qui crée un cachet électronique ».

[167] A cet égard, on lira avec beaucoup de prudence le considérant n° 58 qui indique 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 ». On se gardera de déduire de ce considérant que le cachet électronique pourrait, aux yeux du règlement, avoir la valeur et les effets d'une signature (d'une personne morale) pour plusieurs raisons : ce considérant se limite à la recevabilité (« recevable »), la valeur d'un considérant reste réduite, particulièrement face à des dispositions claires et, enfin, les négociations tenues au Conseil européen excluent une telle interprétation.

[168] 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, 4ème édition, Larcier, Juin 2012, pp. 216-217. En droit français, voy. E. Caprioli, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.166 à 168.

électronique des personnes morales, il ne semble plus possible de délivrer un certificat de signature électronique au nom d'une personne morale, ce certificat étant désormais réservé aux personnes physiques. Ces pays devront dès lors utiliser les certificats de cachet électronique tout en spécifiant au niveau national que ceux-ci ont valeur de signature.

Tout comme pour la signature électronique, l'article 35 relatif aux effets juridiques des cachets électroniques consacre deux clauses. La première, dite de « non-discrimination », indique que « L'effet juridique et la recevabilité d'un cachet électronique comme preuve en justice ne peuvent être refusés au seul motif que ce cachet se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié ». La seconde clause ne sera par contre pas appelée « clause d'assimilation » car, contrairement à la signature manuscrite, le cachet ne connaît pas de concept juridique universel auquel le cachet électronique qualifié pourrait être assimilé. La clause va par contre établir une présomption réfragable : « Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié ». Rappelons que cette présomption n'implique pas, au sens du Règlement, qu'un document électronique « estampillé » par un cachet électronique qualifié engage juridiquement la personne morale.

Pour le reste, les dispositions applicables aux cachets électroniques dans les services publics, aux certificats qualifiés de cachet électronique ainsi qu'aux dispositifs de création, à la validation et à la conservation des cachets électroniques qualifiés sont sensiblement les mêmes que celles applicables aux signatures électroniques. Nous renvoyons donc aux développements rédigés à ce sujet dans le titre précédent.

iii. L'horodatage électronique

La section 6 du chapitre 3 du Règlement porte sur l'horodatage électronique (en anglais « time stamping »). L'horodatage électronique est défini par l'article 3.33) comme « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ». Que ce soit pour des raisons juridiques ou non, le recours à un service de datation de données électroniques peut souvent s'avérer utile. Celui-ci peut servir à dater[169] des documents électroniques tels que des contrats, des engagements unilatéraux, des renoms, des lettres de licenciement, des actes introductifs d'instance, etc. Mais il permet également de dater des événements tels que l'accès à un document, l'envoi d'un document, la conclusion d'une transaction ou la clôture d'un dossier.

Vu l'intérêt que présente ce type de service dans le cadre des transactions électroniques, le législateur européen a jugé utile, à l'instar des autres services de confiance, de lui consacrer une section en vue, d'une part, de déterminer les effets juridiques liés à ces horodatages électroniques et, d'autre part, d'établir les exigences applicables aux horodatages électroniques qualifiés.

Tout comme pour les deux premiers services de confiance, l'article 41 relatif aux effets juridiques des horodatages électroniques consacre deux clauses. La première, dite de « non-discrimination », indique que « L'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié ». La seconde clause établit une présomption réfragable au profit des horodatages électroniques qualifiés : « Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure ».

Pour être réputé « qualifié » au sens du Règlement et bénéficier de la présomption réfragable exposée ci-dessus, le service d'horodatage doit répondre à trois exigences fixées par l'article 42.

[169] La notion doit s'entendre au sens large dans la mesure où le service permet de déterminer de manière précise tant la date que l'heure. La définition utilise d'ailleurs à dessein le terme « instant » et non celui de « date ». Sur cette notion et ce service, voy. E. Caprioli, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.169 et s.

Premièrement, il doit « lier la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ». Cette condition de maintien d'intégrité tombe sous le sens et porte bien entendu tant sur les données de datation (qui permettent de vérifier la date) que sur les données datées (par exemple le contrat).

Deuxièmement, le service d'horodatage doit être « basé sur une horloge exacte liée au temps universel coordonné ». L'objectif premier de ce service consiste à fournir une date fiable et précise. L'obligation de le lier au temps universel coordonné[170] permet de remplir cet objectif.

Troisièmement, le service d'horodatage doit être « signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente ». Cette exigence permet d'offrir un niveau de sécurité relativement élevé quant à l'origine et à l'intégrité du service. La notion de « méthode équivalente » pourrait surprendre quant à son imprécision. Le considérant n° 62 précise toutefois à ce égard que « En cas de recours à une méthode autre que le cachet électronique avancé ou la signature électronique avancée, il devrait revenir au prestataire de services de confiance qualifié de démontrer, dans le rapport d'évaluation de la conformité, que ladite méthode assure un niveau de sécurité équivalent et satisfait aux obligations énoncées dans le présent règlement ».

On notera enfin que, à l'instar des autres services de confiance, la Commission peut, au moyen d'actes d'exécution, établir les numéros de référence des normes en ce qui concerne l'établissement du lien entre la date et l'heure et les données, et les horloges exactes. L'établissement du lien entre la date et l'heure et les données et les horloges exactes sont présumés satisfaire aux exigences relatives aux horodatages électroniques qualifiés précitées lorsqu'ils respectent ces normes.

iv. Le service d'envoi recommandé électronique

La section 7 du chapitre 3 du Règlement traite du service d'envoi recommandé électronique[171]. Celui-ci est défini par l'article 3.36) comme « un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée ». Il s'agit *grosso modo* d'un équivalent électronique de l'envoi recommandé physique ou papier que l'on connaît depuis des décennies dans le monde postal, c'est-à-dire un service électronique qui permet d'apporter une relative certitude juridique sur le fait que des données électroniques ont été envoyées et reçues de manière intègre ainsi que sur la date d'envoi et de réception de ces données[172].

---

[170] Le Temps universel coordonné est une échelle de temps adoptée comme base du temps civil international par la majorité des pays du globe. Il s'agit d'une échelle de temps comprise entre le « Temps atomique international », qui est stable mais déconnecté de la rotation de la Terre, et le Temps universel (TU), directement lié à la rotation de la Terre et donc lentement variable. Le terme « coordonné » indique que le Temps Universel Coordonné est en fait identique au Temps atomique international dont il a la stabilité et l'exactitude à un nombre entier de secondes près, ce qui lui permet de coller au temps universel à moins de 0,9 s près (source : http://fr.wikipedia.org/wiki/Temps_universel_coordonn%C3%A9).

[171] La version anglaise utilise la notion de « electronic registered delivery service ».

[172] Sur la question de l'envoi recommandé électronique en droit belge, voy. notamment E. MONTERO, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées » *in Le commerce électronique : de la théorie à la pratique*, Cahiers du CRID, n° 23, Bruxelles, Bruylant, 2003, pp. 69 à 99 ; O. VAN CUTSEM, « L'évolution technologique et le monde postal. La validité juridique du courrier recommandé électronique en Belgique », *C.J.*, n°3/2003, pp. 43 à 48. En droit français, voy. E. Caprioli, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.175 et s.

Certes, ce service n'est pas encore utilisé de manière généralisée dans de nombreux EM mais le législateur européen y voit une opportunité pour ouvrir de nouvelles possibilités de commercialisation au niveau paneuropéen[173].

Même si la modification peut paraître anodine à première lecture, on notera une avancée fondamentale entre la proposition de la Commission et le texte finalement adopté. En effet, la proposition initiale utilisait le concept de « service de fourniture électronique ». Outre le fait que ce concept pouvait prêter à confusion[174] et ne correspondait à aucun concept juridique connu et usité dans de nombreux droits nationaux, ce concept laissait subsister un doute quant à la volonté du législateur européen d'harmoniser les règles applicables à l'envoi recommandé électronique, envisagé comme un équivalent de l'envoi recommandé papier.

Désormais, le doute est levé. Le texte adopté consacre l'équivalent électronique d'un concept juridique bien connu tant des spécialistes du droit que du grand public et utilisé dans de nombreuses législations et réglementations : le concept d'envoi recommandé. De surcroît, il détermine les effets juridiques ainsi que les exigences que doivent respecter les prestataires qui souhaitent offrir ce service de confiance, particulièrement s'il est qualifié.

A l'instar des autres services de confiance, l'article 43 relatif aux effets juridiques du service d'envoi recommandé électronique consacre deux clauses. La première, dite de « non-discrimination », indique que « L'effet juridique et la recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique comme preuve en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'envoi recommandé électronique qualifié ». La seconde clause établit une présomption réfragable au profit du service d'envoi recommandé électronique qualifié : « Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié ».

Contrairement au recommandé physique qui offre généralement la possibilité à l'expéditeur de demander ou pas un accusé de réception, le législateur européen semble avoir généralisé l'accusé de réception pour le service d'envoi recommandé électronique, et considéré cette fonctionnalité comme partie intégrante du service. En d'autres mots, lorsqu'on offre ou utilise un service d'envoi recommandé électronique, l'expéditeur ne dispose plus de la possibilité d'opter pour l'envoi recommandé sans accusé de réception. Cette conclusion peut se déduire du texte tant de la définition que de la clause consacrant la présomption réfragable : la définition indique que le service permet d'apporter « …la preuve de leur envoi *et* de leur réception… », et la présomption porte sur « … l'envoi de ces données par l'expéditeur identifié *et* à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi *et* de la réception ». Même si cela différencie quelque peu les deux formes de service d'envoi recommandé (papier et électronique), nous appuyons ce choix du législateur européen, car le recommandé électronique avec accusé de réception (automatique) offre plus de garanties pour l'expéditeur, sans que sa mise en œuvre ne soit ni plus complexe ni plus onéreuse qu'un recommandé électronique sans accusé. Alors que pour le recommandé physique, la demande d'un accusé de réception constitue une charge de traitement supplémentaire pour l'opérateur et le facteur qui le délivre.

[173] Considérant n° 66. L'Italie et l'Autriche par exemple connaissent et utilisent déjà largement ce service. En Belgique, Certipost avait proposé ce service en 2003 (http://www.bpost.be/site/fr/postgroup/press/releases/2003/ppr_CERTIPOST_20030716.html) mais semble avoir arrêté sa commercialisation dans l'attente d'une législation en ce domaine (http://www.bpost.be/site/fr/business/send_post/registered/registered_electronic.html).

[174] En effet, la « fourniture ou livraison électronique » pouvait s'interpréter largement comme visant les services de téléchargement d'un logiciel par exemple ou de streaming dans le domaine audiovisuel, ce qui ne semblait toutefois pas être l'intention de la Commission …

Par contre, il semble moins clair si le Règlement entend forcer l'accusé de réception du destinataire ou si ce dernier garde la possibilité, après avoir été informé qu'un recommandé électronique lui a été envoyé, d'accepter ou de refuser la fourniture des données faisant l'objet de cet envoi. Selon nous, le Règlement ne tranche et n'harmonise pas cette question. Dès lors, chaque EM conserve la liberté de choix entre l'une ou l'autre option au niveau national, pour autant que ce choix ne crée pas d'obstacles à l'utilisation transfrontière de ce service d'envoi recommandé électronique[175]. Il découle, selon nous, de cette exigence de libre circulation au sein du marché intérieur, une exigence indirecte d'interopérabilité entre les services d'envoi recommandé électronique[176]. Dès lors, on peut imaginer que l'Italie impose la réception obligatoire, sans laisser la possibilité au destinataire de refuser la fourniture des données recommandées[177], alors que la Belgique maintienne la possibilité pour le destinataire de refuser l'envoi recommandé électronique de manière implicite (il ne réagit pas à la notification après un certain délai, ce qui donnera lieu à un accusé de non-délivrance) ou explicite (il indique qu'il ne souhaite pas recevoir les données recommandées, ce qui donnera lieu à un accusé de refus)[178]. Dans un tel système, l'Italie et la Belgique devrait donc veiller à respecter les exigences du pays du destinataire en cas d'utilisation transfrontière. Concrètement, cela signifierait que chaque pays devrait mettre en place un mécanisme technique assurant l'interopérabilité entre les systèmes et le respect des spécificités nationales. Ce mécanisme technique devrait donc permettre, d'une part, au destinataire italien de recevoir automatiquement les données recommandées expédiée par un belge, sans que ce destinataire puisse refuser les données et, d'autre part, au destinataire belge de pouvoir refuser les données recommandées (et de ne pas connaître l'identité de l'expéditeur italien tant qu'il n'a pas pris sa décision d'acceptation ou de refus).

On remarquera que, contrairement aux précédents services de confiance, l'article 43 ne contient pas un troisième paragraphe relatif à la reconnaissance mutuelle des services d'envoi recommandé électronique qualifiés, qui aurait pu être formulé comme suit : « Un service d'envoi recommandé électronique qualifié délivré dans un État membre est reconnu en tant que service d'envoi recommandé électronique qualifié dans tous les États membres ». Probablement un oubli du législateur européen qui, selon nous, ne prête pas à conséquence tant ce principe de reconnaissance mutuelle découle de l'instrument juridique lui-même, à savoir le règlement, des principes généraux relatifs au marché intérieur rappelés dans l'article 4 et du considérant n° 66 qui indique que « Il est es sentiel de prévoir un cadre juridique en vue de faciliter la reconnaissance transfrontalière entre les systèmes juridiques nationaux existants en matière de services d'envois recommandés électroniques ».

Pour être réputé « qualifié » au sens du Règlement et bénéficier de la présomption réfragable exposée ci-dessus, le service d'envoi recommandé électronique doit répondre aux exigences fixées par l'article 44.

Premièrement, il doit être « fourni par un ou plusieurs prestataires de services de confiance qualifiés ». Rappelons que les prestataires de services *qualifiés* sont soumis à des exigences strictes, dont le respect est assuré dans le cadre d'un régime de contrôle rigoureux. Les mots « un ou plusieurs » ont été utilisés en vue de couvrir l'hypothèse éventuelle dans laquelle un expéditeur envoie son recommandé électronique par le biais de son prestataire alors le destinataire recevra ce recommandé par le biais de

[175] En ce sens, voy. l'article 4 et le considérant n° 24.

[176] On peut d'ailleurs s'attendre à, ou à tout le moins espérer, que l'acte d'exécution relatif à ce service détermine des normes qui veillent à assurer l'interopérabilité entre les services d'envoi recommandé électronique offerts par les différents prestataires.

[177] Ce qui semble en fait être le cas en Italie dans le cadre de la PEC - Posta elettronica certificata (https://www.postacertificata.gov.it/home/index.dot) mis en place par le Gouvernement. Ce service, assimilé et ayant même valeur juridique qu'un envoi recommandé papier, ne permet pas au destinataire de refuser l'envoi recommandé électronique : celui-ci est censé être reçu dès que l'envoi arrive dans sa boîte PEC, peu importe que le destinataire l'ai lu ou pas. Pour plus d'informations, voy. http://qualitapa.gov.it/relazioni-con-i-cittadini/open-government/strumenti-della-pa-digitale/la-posta-elettronica-certificata/.

[178] Dans cette hypothèse, le prestataire ne devrait pas communiquer au destinataire l'identité de l'expéditeur du recommandé électronique tant que ce destinataire n'a pas exprimé sa décision d'accepter ou de refuser ce recommandé. En d'autres mots, le prestataire ne devrait donc pas autoriser de refus du destinataire après que l'identité de l'expéditeur de l'envoi recommandé électronique ait été communiquée.

son propre et autre prestataire. A cet égard, le second alinéa de l'article 44.1. indique que « Dans le cas où les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences fixées aux points a) à f) s'appliquent à tous les prestataires de services de confiance qualifiés ». Bien entendu et une fois encore, une telle hypothèse ne peut se produire que si les plateformes respectives des prestataires sont interopérables.

Deuxièmement, le service doit garantir « l'identification de l'expéditeur avec un degré de confiance élevé ». Cette obligation vise notamment à éviter l'envoi de faux recommandés par de faux expéditeurs mais également à assurer que la preuve de l'envoi et de la délivrance du recommandé électronique soit reçue par la même personne que celle qui a expédié l'envoi recommandé. A cette fin, le prestataire de service est libre d'utiliser le moyen le plus approprié, qui pourrait selon nous être fixé contractuellement entre le prestataire de service et l'utilisateur de ce service (en l'occurrence l'expéditeur), pour autant que ce moyen permettre une identification « avec un degré de confiance élevé ».

Troisièmement, le service doit garantir « l'identification du destinataire avant la fourniture des données ». Cette obligation vise à garantir que la personne qui prend connaissance de l'envoi recommandé électronique est bien celle qu'elle prétend être et qu'elle a effectivement ce droit de prise de connaissance. Dans le cas d'une procuration, il conviendrait selon nous de contrôler non seulement l'identité de la personne qui prend connaissance de l'envoi recommandé mais également l'authenticité et l'intégrité de la procuration et le fait que celle-ci est bien donnée par le destinataire du recommandé électronique. Cette exigence d'identification préalable à la fourniture des données signifie également qu'un système qui consisterait à envoyer directement un recommandé électronique à la simple adresse de courrier électronique non sécurisé d'un destinataire (donnée par l'expéditeur) ne respecte pas l'obligation du Règlement. Certes, l'adresse de courrier électronique pourrait être utilisée par le prestataire pour notifier au « présumé » destinataire qu'un recommandé électronique est disponible mais le prestataire ne pourra lui délivrer les données « recommandées » qu'après avoir dûment identifié le destinataire à l'aide d'un moyen approprié. A cet égard, il nous semble évident qu'une adresse de courrier électronique non sécurisée ne suffit pas, à elle seule, pour identifier le destinataire du recommandé électronique « avec un degré de confiance élevé ».

Quatrièmement, « l'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié de manière à exclure toute possibilité de modification indétectable des données ». Cette exigence relative au maintien de l'intégrité ne nécessite pas de commentaires, et découle en outre de la définition du concept consacrée par l'article 3.36).

Cinquièmement, « toute modification des données nécessaire pour l'envoi ou la réception de celles-ci » est permise pour autant toutefois que cette modification « est clairement signalée à l'expéditeur et au destinataire des données ».

Sixième et dernière condition, « la date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié ». Peu importe que ce service d'horodatage électronique qualifié soit offert par le même prestataire que celui qui preste le service d'envoi recommandé électronique ou par un autre prestataire.

A l'instar des autre services de confiance, le Règlement prévoit la possibilité pour la Commission de déterminer, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux processus d'envoi et de réception de données. Le processus d'envoi et de réception de données est présumé satisfaire aux exigences énoncées dans le Règlement lorsqu'il respecte ces normes. On reconnaîtra toutefois que pour ce service relativement nouveau, le processus de normalisation volontaire au sein des organismes européens et internationaux[179] en la matière n'en est qu'à ses débuts. Le nouveau Règlement incitera très probablement ces organismes à consacrer une partie de leur énergie au processus de standardisation pour ce service.

[179] Tels que par exemple le CEN (European Committee for Standardization), l'ETSI (European Telecommunications Standards Institute) ou ISO (International Organization for Standardization).

v. L'authentification de site internet

La section 8 porte sur l'authentification de site internet. L'objectif principal de ce service consiste à garantir l'authenticité du lien entre un site web et son responsable. En effet, on ne compte plus à ce jour le nombre d'enseignes qui sont victimes de « phishing », c'est-à-dire d'escrocs qui créent de faux sites internet, copies conformes du vrai site internet, en vue de se faire passer pour une société ou une personne physique (par exemple dans le domaine bancaire ou de la location de logements de vacances) et ainsi soutirer des sommes d'argent aux internautes un peu trop naïfs. Dans l'objectif de renforcer le climat de confiance dans le cadre des transactions commerciales en ligne[180], ce service d'authentification de site internet vise essentiellement à garantir aux internautes, par le biais d'un certificat qualifié d'authentification de site internet, la véracité et la légitimité du site internet et le fait que la personne physique ou morale indiquée comme responsable du site est bien celle qu'elle prétend être.

Cette section a fait l'objet d'âpres discussions lors des négociations au Conseil et on relèvera qu'on a été à deux doigts de l'exclusion de cette section dans le texte adopté. Ce contexte explique le peu de dispositions consacrées à ce service de confiance dans le Règlement.

L'unique article 45 consacré à ce service ne souffle mots des effets juridiques liés à ce service. Il appartiendra donc au juge, en fonction des circonstances de l'espèce, de déterminer les effets juridiques que l'on peut lui attribuer, au regard notamment des garanties apportées par le certificat qualifié lié à ce service.

L'article 45 stipule seulement que « Les certificats qualifiés d'authentification de site internet satisfont aux exigences fixées à l'annexe IV » et que « La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site internet. Un certificat qualifié d'authentification de site internet est présumé satisfaire aux exigences fixées à l'annexe IV lorsqu'il respecte ces normes ».

Les exigences fixées à l'annexe IV permettent de comprendre les garanties offertes par ce certificat qualifié d'authentification de site internet. En effet, ce certificat sécurisé[181] contient notamment les coordonnées du prestataire délivrant le certificat, les coordonnées de la personne physique ou morale qui exploite le site internet ainsi que le nom de domaine exploité par cette personne en vue de rendre accessible son site internet. Il semble aller de soi que le prestataire ne devrait pas délivrer le certificat qualifié sans avoir vérifié au préalable les informations indiquées dans ledit certificat.

On note enfin que la fourniture par le prestataire et l'utilisation par les responsables de sites internet de ce service d'authentification de sites internet se font entièrement sur une base volontaire, et ne fait pas obstacle à l'utilisation ou à l'offre d'autres moyens ou méthodes permettant d'authentifier un site internet[182].

L'avenir nous dira si ce service de confiance s'avère être un « gadget » du législateur européen ou s'il est réellement utilisé. Quoiqu'il en soit, nous appuyons l'adoption de cette disposition par le législateur, dont le seul risque est qu'elle reste lettre morte…

vi. Les documents électroniques

L'article 46 est la seule disposition du Règlement consacrée aux documents électroniques. Cette disposition n'est pas localisée dans une section particulière du chapitre 3, ce qui est assez logique dans la mesure où le document électronique ne constitue pas un service de confiance en tant que tel mais est plutôt l'objet d'un ou plusieurs services de confiance. L'article 46 fait dès lors l'objet d'un chapitre 4,

[180] Voy. en ce sens le considérant n° 67.
[181] Il s'agit en fait de la même technologie que celle utilisée pour la signature électronique ou le cachet électronique.
[182] Considérant n° 67.

consacré uniquement aux documents électroniques. Selon nous, cet article aurait tout aussi bien pu être inséré dans le premier chapitre dédié aux dispositions générales.

On constate que, en comparaison avec la disposition plus ambitieuse qui avait été proposée par la Commission[183], la disposition finalement retenue peut être qualifiée de minimale. Tout au plus l'article 46 consacre-t-il une clause de non-discrimination au profit des documents électroniques : « L'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique ». Les oppositions exprimées sur la proposition de la Commission lors des négociations au Conseil étaient à ce point fortes, que le Règlement se limite à accoucher d'une souris sur cette question. On lui reconnaîtra au moins l'intérêt de tenter de promouvoir l'utilisation des documents électroniques et d'éviter toute discrimination par rapport aux documents papiers.

IV. Les dispositions finales : entrée en vigueur, mesures transitoires et réexamen

Le dernier chapitre relatif aux dispositions finales nous donnent les éléments permettant de comprendre comment le Règlement va progressivement être mis en œuvre. Ainsi, ce chapitre contient des dispositions relatives à l'entrée en vigueur, à l'abrogation de la directive 1999/93/CE, à des mesures transitoires et au réexamen futur du Règlement.

En vue de permettre à la Commission de lancer immédiatement le processus d'adoption des actes d'exécution mais également de laisser le temps aux EM pour se préparer et/ou adapter leurs systèmes aux dispositions du nouveau Règlement, l'article 52 opère une distinction entre l'entrée en vigueur du Règlement et l'entrée en application des dispositions de celui-ci.

Le Règlement est entré en vigueur le 17 septembre 2014, à savoir le vingtième jour suivant sa publication le 28 août 2014 au Journal Officiel de l'Union européenne. Ceci étant, il faudra attendre le 1er juillet 2016 pour observer d'un point de vue concret les changements fondamentaux apportés par le Règlement.

En effet, le principe est que le Règlement est applicable à partir du 1er juillet 2016, à l'exception toutefois d'une série de dispositions visées par le second paragraphe de l'article 52 que entrent en application soit avant, soit après le 1er juillet 2016.

Dans les grandes lignes, on retiendra essentiellement que le chapitre 3 relatif aux services de confiance entre en application à partir du 1er juillet 2016, à l'exception des dispositions relatives à l'adoption des actes d'exécution (optionnels ou obligatoires) qui sont nécessaires à l'offre et au bon fonctionnement des services de confiance. Le processus d'adoption de ces actes a bien entendu été lancé par la Commission depuis le 17 septembre 2014 (et même avant cette date dans le cadre du groupe d'experts informel[184]).

Pour ce qui concerne le chapitre 2 relatif à l'identification électronique, la situation est plus complexe, et nous nous permettons de renvoyer le lecteur au point II de cette contribution. Nous retiendrons essentiellement que le processus d'adoption des actes d'exécution a démarré depuis le 17 septembre 2014, que la reconnaissance volontaire des moyens d'identification électronique notifiés peut démarrer à partir du 18 septembre 2015 et que la reconnaissance mutuelle de ces moyens deviendra obligatoire le 18 septembre 2018 au plus tôt.

Dès lors que l'article 50 prévoit que la directive 1999/93/CE est abrogée avec effet au 1er juillet 2016, il semblait important de consacrer des mesures transitoires pour garantir la sécurité juridique aux prestataires de services de certification qui œuvraient conformément à cette directive. Ainsi, pour permettre à ces prestataires de continuer à offrir leurs services dans le respect des dispositions du

[183] Voy. l'article 34 de la proposition du 4 juin 2012, *op.cit.*, p.38.

[184] La consultation des experts est effectivement préconisée par le législateur européen qui indique dans le considérant n°70 que « Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts ».

Règlement, l'article 51 prévoit que, d'une part, les dispositifs sécurisés de création de signature conformes à la directive sont considérés comme des dispositifs de création de signature électronique qualifiés conformes au Règlement et, d'autre part, les certificats qualifiés délivrés aux personnes physiques au titre de la directive sont considérés comme des certificats qualifiés de signature électronique au titre du présent Règlement jusqu'à leur expiration. Cela signifie donc que les nouvelles cartes d'identité électronique belges délivrées depuis le printemps 2014 sous l'empire de la directive de 1999, et qui contiennent un certificat qualifié valable 10 ans, continueront à être valable pendant cette période après l'entrée en application du Règlement.

Par contre, le Règlement ne semble pas prévoir de mesure transitoire pour les certificats qualifiés de signature électronique délivrés aux personnes morales au titre de la directive. S'il s'agit d'un oubli du législateur européen, on reconnaîtra que les conséquences sont lourdes. Ces certificats devraient en effet perdre leur validité à partir du 1er juillet 2016.

L'article 51 ajoute que le prestataire de services de certification qui délivre des certificats qualifiés au titre de la directive 1999/93/CE soumet un rapport d'évaluation de la conformité à l'organe de contrôle le plus rapidement possible et au plus tard le 1er juillet 2017. Jusqu'à la présentation d'un tel rapport d'évaluation de la conformité et l'achèvement de l'évaluation par l'organe de contrôle, ce prestataire de services de certification est considéré comme un prestataire de services de confiance qualifié au titre du Règlement. Le prestataire dispose donc d'un délai d'un an à dater de l'entrée en application du chapitre 3 pour régulariser sa situation. Si le même prestataire ne soumet pas de rapport d'évaluation de la conformité dans le délai indiqué ou si l'organe de contrôle estime que le rapport n'est pas concluant, ce prestataire de services de certification n'est pas considéré comme un prestataire de services de confiance qualifiés au titre du Règlement à partir du 2 juillet 2017. Dès lors, nous ne pouvons que conseiller dès à présent aux prestataires qui délivrent des certificats qualifiés de suivre de près l'adoption des actes d'exécution et de préparer progressivement leur mise en conformité aux dispositions du nouveau Règlement afin d'éviter toute déconvenue à partir du 2 juillet 2017….

On notera enfin l'obligation à charge de la Commission de rédiger un premier rapport d'évaluation le 1er juillet 2020[185]. 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 l'application du Règlement ainsi que de l'évolution des technologies, du marché et du contexte juridique. On constate que l'article 49 vise certaines dispositions en particulier[186], dont on se doute qu'elles ont dû faire l'objet de discussions difficiles lors des négociations… Après ce premier rapport, la Commission rédigera tous les quatre ans un rapport sur les progrès accomplis dans la réalisation des objectifs du Règlement.

V. La marge de manœuvre laissée aux Etats Membres

Nous savons que le législateur a opté pour un règlement, et non une directive, car l'effet d'application directe lié à cet instrument juridique permet une harmonisation plus efficace. Nous savons également que pour les services de confiance, le Règlement rappelle dans son article 4 le principe du marché intérieur selon lequel « Il n'y a pas de restriction à la fourniture de services de confiance, sur le territoire d'un État membre, par un prestataire de services de confiance établi dans un autre État membre pour des raisons qui relèvent des domaines couverts par le présent règlement » et que « Les produits et les services de

[185] Article 49.

[186] Il s'agit de l'article 6 (relatif à la reconnaissance mutuelle des moyens d'identification électronique notifiés), l'article 7, point f) (relatif à la mise à disposition d'un moyen d'authentification en ligne en vue de vérifier les données d'identification électronique) et les articles 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), 43 et 44 (relatifs au service d'envoi recommandé électronique, dispositions arrachées en fin de négociations…) et 45 (relatif à l'authentification de site Internet, certains EM ne voyant pas l'intérêt d'un tel service).

confiance qui sont conformes au présent règlement sont autorisés à circuler librement au sein du marché intérieur ».

Peut-on en conclure que toutes les questions sont harmonisées et qu'il ne reste plus aucune possibilité pour les EM de consacrer certaines spécificités au niveau national ? Il nous semble que non. Une certaine marge de manœuvre semble laissée aux EM[187].

En effet, comme relevé à diverses reprises dans cette contribution, certaines dispositions du Règlement renvoient au droit national pour le traitement de certaines questions[188]. De plus, le considérant n°25 indique que « 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 ». Ainsi, et sous réserve de l'article 34 relatif au service de conservation qualifié des signatures électroniques qualifiées, le Règlement ne consacre pas de section relative à l'archivage électronique comme service de confiance en tant que tel. Chaque EM reste donc libre de prévoir 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 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 ». Le législateur européen semble donc reconnaître que les services de confiance visés par le Règlement ne sont pas (tous) complètement harmonisés. Cette reconnaissance de principe exprimée, on admettra qu'il semble plus délicat pour un EM de déterminer précisément quels services de confiance visés par le Règlement ne sont pas complètement harmonisés et sur quels aspects l'EM conserve une marge de manœuvre.

Dans certaines hypothèses, le Règlement l'indique clairement.

C'est par exemple le cas pour l'article 28 qui stipule que « Les certificats qualifiés de signature électronique ne font l'objet d'aucune exigence obligatoire allant au-delà des exigences fixées à l'annexe I ». Dès lors, concernant les certificats qualifiés de signature électronique, les EM ne peuvent pas prévoir d'autres exigences *obligatoires* en terme de contenu que celles qui sont prévues à l'annexe I. Par contre, le Règlement permet, au niveau national, d'intégrer dans les certificats qualifiés d'autres mentions que celles prévues à l'annexe I, telles que par exemple des attributs spécifiques supplémentaires. Toutefois, cette faculté laissée aux EM est conditionnée au fait, d'une part, que ces mentions ne soient pas obligatoires (un prestataire belge, et *a fortiori* étranger, n'est pas tenu d'inclure ces mentions dans les certificats qualifiés qu'il délivre) et, d'autre part, qu'elles n'affectent pas l'interopérabilité et la

[187] A cet égard, le législateur belge a déjà lancé diverses initiatives dans le domaine des services de confiance, qui n'ont malheureusement jamais totalement abouti jusqu'à présent. On relève particulièrement la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance, restée lettre morte dans la mesure où les arrêtés royaux nécessaires à l'application de cette loi, qui devaient être publiés pour le 31/12/2007, n'ont jamais été adoptés ; les articles 38 à 52 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, dont l'objectif était d'introduire le recommandé électronique en droit belge, mais qui ont dû être abrogés par l'article 24 de la loi du 31 mai 2011 portant des dispositions diverses en matière de télécommunications car la procédure de notification à la Commission européenne n'a pas été respectée ; et enfin, la proposition de loi 2745 du 15 avril 2013 portant insertion d'un titre 2, "Certaines règles relatives au cadre juridique pour les signatures électroniques, l'archivage électronique, le recommandé électronique, l'horodatage électronique et les services de certification", dans le livre XII du Code de droit économique, et portant insertion des définitions propres au titre 2 précité et des dispositions d'application de la loi propres au même titre, dans les livres Ier et XV du Code de droit économique, qui a failli aboutir en novembre 2013 mais qui a été logiquement suspendue par la Commission européenne en raison de la proposition de règlement eIDAS négociée au niveau européen.

[188] Voy. particulièrement les articles 2.2., 2.3., 5.2., 6.1., 11.4., 11.5., 12.3.a), 17.5., 18.3., 24.1., 24.2., 28.5. et 38.5.

reconnaissance des signatures électroniques qualifiées au niveau transfrontière. On le comprend, cette dernière condition d'interopérabilité technique risque souvent de constituer un frein à la volonté de consacrer certaines spécificités nationales.

C'est également le cas pour les articles 28.5. et 38.5. qui autorisent les EM à établir des règles nationales relatives à la suspension temporaire d'un certificat qualifié pour autant que les deux conditions suivantes soient remplies. 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 est visible, pendant la période de suspension, auprès du service fournissant les informations sur le statut du certificat.

Mais dans de nombreux autres cas, les choses sont moins claires et il appartiendra à chaque EM de prendre ses responsabilités s'il souhaite régler certains aspects au niveau national. Le cas échéant, pour chaque mesure envisagée, le législateur national gardera à l'esprit la nécessité d'éviter toute mesure nationale susceptible de porter préjudice au principe de marché intérieur rappelé ci-dessus, et particulièrement toute mesure qui constitue un obstacle à l'intéropérabilité des services de confiance au niveau transnational.

Dans ce contexte, on se risque de proposer divers exemples de problématiques qui ne pourraient plus être réglées au niveau national ainsi que d'autres qui pourraient encore l'être.

Sur le plan des restrictions, un EM ne devrait donc pas pouvoir :

- établir une disposition qui stipule que, au niveau national (et *a fortiori* au niveau transfrontière), les signatures électroniques qualifiées n'ont pas les mêmes effets juridiques que la signature manuscrite. Une telle disposition serait contraire à l'article 25.2. ;

- établir une disposition qui stipule que, au niveau national (et *a fortiori* au niveau transfrontière), les signatures électroniques non qualifiées (par exemple, le simple scan d'une signature manuscrite) ne valent rien, n'ont aucun effet juridique et ne peuvent même pas être examinées par le juge. Une telle disposition serait contraire à l'article 25.1. ;

- modifier la procédure de lancement d'un service de confiance qualifié visée à l'article 21 ou encore modifier la liste des exigences applicables aux prestataires de services de confiance qualifiés prévues à l'article 24.

Par contre, dans le cadre du chapitre relatif aux services de confiance, un EM devrait pouvoir :

- établir une règle qui prévoit que, au niveau national, certains types de signatures électroniques non qualifiées ont les mêmes effets que la signature manuscrite[189]. Toutefois, cette règle ne vaudrait pas au niveau transfrontière. Par exemple, si une loi finlandaise stipulait que le scan de la signature manuscrite a les mêmes effets juridiques que la signature manuscrite, cette disposition serait applicable entre citoyens, entreprises et administrations finlandais mais ne pourrait, par contre et sous réserve des règles définissant le droit applicable, pas être invoquée par une entreprise finlandaise à l'égard d'une entreprise belge avec laquelle elle est en relation d'affaires, le droit belge ne connaissant pas cette assimilation ;

- déterminer les effets juridiques attachés à l'utilisation d'une signature manuscrite. Par ailleurs, un EM reste libre de déterminer les effets probatoires des différents moyens de preuve, les cas dans lesquels une signature est exigée à des fins de validité ou de preuve de l'acte juridique, les autres effets liés à l'utilisation d'une signature, tels que la signature simplement pour « réception » ou pour prise de connaissance, etc. ;

[189] En ce sens, voy. le considérant n° 49.

- prévoir que, au niveau national, l'utilisation du cachet électronique permet à la personne morale de signer et donc, à lui seul, d'engager juridiquement cette personne morale ;

- préciser les pouvoirs reconnus à l'organe de contrôle afin de lui permettre d'exercer efficacement sa mission (par exemple, pouvoir intervenir à tout moment au sein de l'entreprise, saisir des documents ou fichiers informatiques, etc.) ;

- établir une disposition qui stipule que, au niveau national, l'utilisation d'un service de recommandé électronique qualifié est réputée satisfaire à l'obligation légale ou réglementaire de recourir à un envoi recommandé ;

- établir une disposition qui stipule que, au niveau national, l'utilisation d'un service d'horodatage électronique qualifié est réputée satisfaire à l'obligation légale ou réglementaire de recourir à la datation de données ou de documents ;

- réglementer certains aspects supplémentaires non réglementés par le Règlement. Par exemple, un EM pourrait consacrer des règles relatives aux envois recommandés hybrides[190] ; des règles qui encadreraient de manière globale et cohérente la fourniture de services d'archivage électronique, qui couvriraient tant l'archivage électronique de documents qui sont originairement électroniques que la numérisation de documents originairement papiers ; des règles qui interdiraient à un prestataire, qui ne répond pas aux conditions du Règlement, de prétendre offrir des services qualifiés, et de consacrer des sanctions civile et/ou pénale le cas échéant ;

- consacrer une disposition nationale imposant au prestataire établi sur le territoire de conserver l'identité des personnes qui « se cachent » derrière un pseudonyme utilisé dans un certificat de signature électronique ou celle de la personne physique qui « se cache » derrière un cachet électronique et qui crée matériellement ou pratiquement ce cachet. La faculté de prévoir une telle obligation, cautionnée par les considérants n°33 et 60, peut notamment s'avérer utile dans le cadre de procédures judiciaires ou administratives ;

- consacrer une obligation à charge de la partie utilisatrice de vérifier la signature électronique ou, à tout le moins, de prévoir une responsabilité particulière pour cette partie en cas de non vérification préjudiciable de cette signature électronique. Rappelons en effet que si le Règlement promeut la validation et l'offre de service de validation de signature électronique qualifiée, il ne consacre par contre rien en ce qui concerne la partie utilisatrice, question qui relève de la prérogative des EM ;

- déterminer les sanctions applicables en cas de non-respect des dispositions du Règlement, comme le prévoit son article 16. Ce dernier stipule d'ailleurs que ces sanctions doivent être effectives, proportionnées et dissuasives.

Conclusion

Dans les premières lignes de cette contribution, nous nous interrogions sur la question de savoir si le Règlement européen du 23 juillet 2014 constituait un évolution ou une révolution au regard de la situation actuelle.

On peut considérer qu'il s'agit d'une évolution dès lors que le nouveau texte ne part pas de zéro mais reprend une série de dispositions de la directive de 1999, tout en prenant soin de les adapter sur la base de l'expérience acquise depuis 15 ans et d'écarter celles ayant montrés leur inefficacité. On constatera également que la clé de voûte relative aux effets juridiques consacrée par la directive de 1999, exprimée par les désormais célèbres clauses de non-discrimination et d'assimilation, a été reprise par le

[190] Ce concept vise une forme particulière d'envoi recommandé qui est envoyé par voie électronique par l'émetteur, puis imprimé par un opérateur postal et remis au destinataire par ce dernier.

Règlement et étendue à l'ensemble des services de confiance. Le Règlement permet également de faire évoluer le système mis en place par la directive en distinguant clairement la signature électronique, réservée aux personnes physiques pour signer, du cachet électronique, dédié aux personnes morales mais sans toutefois stipuler que ce dernier permet, à lui seul, d'engager juridiquement la personne morale, ce qui aurait constitué une révolution au niveau européen. Le Règlement a également veillé à permettre une évolution progressive en retardant l'entrée en application au 1er juillet 2016 et en consacrant des mesures transitoires, permettant ainsi aux EM et aux prestataires de disposer du temps nécessaire pour procéder aux adaptations requises par le Règlement.

Mais on peut également parler de révolution, que nous qualifierons de positive et constructive, dans la mesure où le législateur européen a profité de l'occasion pour créer un cadre transnational et intersectoriel presque complet et de nature à garantir des échanges électroniques sûrs, fiables et aisés. On constate en effet que les sujets et services traités par le Règlement sont largement plus variés que la seule question de la signature électronique couverte par la directive de 1999.

Ce législateur aurait pu rester prudent et se limiter à maintenir la directive en l'état ou simplement adapter les quelques dispositions qui ont montré leur faiblesse. Il aurait également pu traiter les deux grands volets du Règlement dans des instruments juridiques séparés, ce qui aurait limité le risque de ne pas aboutir. Ces options ont d'ailleurs été analysées par la Commission, pour ensuite être abandonnées. On constate aussi que le législateur a délaissé la directive au profit du règlement, instrument juridique plus efficace en terme d'harmonisation.

Au contraire, le législateur européen a pris la décision ambitieuse de consacrer de nouvelles dispositions tant sur l'identification électronique que sur les services de confiance autres que la signature électronique (cachet, horodatage et recommandé électroniques ainsi que authentification de site web). De surcroît, il a pris la décision courageuse d'aborder toutes ces questions dans le même instrument juridique que constitue le règlement.

On observe également que le législateur européen renforce et harmonise plus largement le système de supervision, jugé trop « fragile » jusqu'alors dans le cadre de la directive, notamment en raison de la trop grande liberté laissée aux EM. A cet égard, les services de confiance qualifiés, et les prestataires qui les offrent, sont soumis à des exigences strictes, qui font l'objet d'un contrôle *a posteriori* mais également *a priori* par l'organe de contrôle. Ce contrôle *a priori* s'effectue dans le cadre de la procédure d'autorisation préalable, procédure qui doit impérativement être suivie et aboutir avant que le prestataire ne puisse offrir des services de confiance qualifiés. Même si nous la jugeons justifiée, il s'agit ici aussi d'une révolution dès lors que cette procédure déroge au principe d'interdiction de mettre en place un régime d'autorisation préalable consacré par plusieurs autres textes européens.

Nous considérons enfin que ce Règlement instaure un bon équilibre entre souplesse, stimulation et sécurité. Il offre de la souplesse dès lors qu'il apparaît plus comme une boîte à outils juridique à disposition des prestataires et utilisateurs que comme un instrument contraignant incontournable. Il crée un cadre qui stimule tant l'innovation que l'offre de services de confiance et l'utilisation de moyens d'identification électronique. Enfin, il établit un système qui présente un niveau de sécurité technique et juridique élevé, ce qui contribue à renforcer la confiance des utilisateurs.

Pour terminer, nous émettrons un petit bémol. Nous regrettons en effet que le législateur européen n'ait pas profité de l'occasion pour consacrer une section relative à l'archivage électronique comme service de confiance en tant que tel, et prévoir ainsi un corps de règle complet harmonisé visant à encadrer juridiquement l'offre et l'utilisation des services d'archivage électronique, couvrant l'archivage électronique tant des documents électroniques, que des documents créés originairement sous forme papier puis numérisés. Il s'agit peut-être d'une problématique qu'il conviendra de soulever dans le cadre du premier rapport d'évaluation du Règlement en 2020…

Didier GOBERT
Juin 2015