economie
SPF Economie, P.M.E., Classes moyennes et Energie

Le règlement européen n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance

Présentation synthétique

Le législateur européen a adopté en 1999 une directive déterminant le régime juridique applicable aux signatures électroniques et aux activités des prestataires de service de certification[1]. 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[2].

Après 15 ans d'application, ce même législateur européen a estimé que cette directive était insuffisante, constatant 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.

A la suite de ce constat, le législateur européen a adopté le règlement n° 910/2014 du Parlement européen et du Conseil 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[3].

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).

1. Considérations générales

1.1. Les objectifs poursuivis par le règlement

Parmi les nombreux objectifs poursuivis par le règlement, nous pouvons raisonnablement mettre en avant trois objectifs principaux et rassembleurs.

Le **premier** consiste à lever les obstacles au fonctionnement du marché intérieur, obstacles qui sont notamment de nature juridique et technique. 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 contribuable de sa déclaration d'impôts dans un autre Etat membre,
- 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 que le patient qu'il soigne a déjà effectués.

[1] 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.
[2] *M.B.*, 29 septembre 2001, pp. 33070-33078.
[3] *J.O.U.E.* du 28.08.2014, L 257/73 à 114.

Le **second** objectif vise à susciter une confiance accrue dans les transactions électroniques, particulièrement transnationales. 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 ».

Rappelons que la confiance dans les relations humaines ne constitue pas un acquis automatique ou un fait accompli ! Comme dans les relations humaines présentielles, la confiance doit aussi se construire dans le monde virtuel. 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 prétend mériter. Pour s'en convaincre, il suffit notamment de constater le nombre de « phishing » encore reçus chaque jour dans nos boîtes de courrier électronique, l'usurpation d'identité étant fréquente sur internet. Avec l'adoption du règlement, l'Union européenne vient enfin de créer les conditions permettant de garantir cette confiance. Ce texte offre ainsi les outils concrets 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.

Le **troisième** objectif consiste à renforcer la sécurité juridique, au profit tant des prestataires de services que des utilisateurs de ces services. En effet, on a constaté jusqu'à ce jour que le marché des services d'identification électronique ainsi que des services de confiance tendait à se développer, mais avec difficulté et un niveau de qualité variable. Ce qui crée un problème de sécurité juridique.

Le règlement entend apporter une solution à ce problème. Désormais, les règles applicables au sein de l'Union européenne sont les mêmes pour tous et d'application directe en droit national. Les Etats membres 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. Le règlement offre aussi aux prestataires de service de confiance une sécurité juridique notamment en leur garantissant une relative prévisibilité, qui constitue souvent une condition essentielle dans la décision d'investissement d'un opérateur économique.

Précisons que le règlement ne souffle mot sur les hypothèses selon lesquelles une identification, une signature, une datation ou un envoi recommandé serait requis juridiquement, question qui relève de la prérogative des Etats membres. Par contre, si une telle exigence est requise par le droit national, le règlement indique comment on peut concrètement satisfaire à cette exigence lorsqu'on exerce ses activités dans un environnement électronique.

Derrière ces trois 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 qu'une initiative législative peut engendrer en terme de création et de développement commercial de nouveaux services économiques.

1.2. Le choix du règlement comme instrument juridique

Concernant l'instrument juridique, le législateur européen a opté pour le règlement, dont les dispositions sont directement applicables en droit national, et non pour une directive. 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 Etats membres et prestataires à coopérer plus efficacement en 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 réside dans le fait que ce dernier peut nécessiter des actes d'exécution 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.).

1.3. 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 chapitres principaux précités.

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

Premièrement, l'identification électronique qui fait l'objet du second chapitre constitue un des aspects de la signature électronique, elle-même traitée dans le troisième chapitre. En effet, une fonction importante de la signature réside dans l'identification du signataire : signer (électroniquement) un document, c'est notamment s'identifier (électroniquement) en tant qu'auteur de ce document.

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 Etats membres 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. Par contre, si un Etat membre 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 Etats membres d'accepter ce moyen d'identification électronique notifié et, d'autre part, une obligation pour l'Etat membre 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 aucune obligation pour les Etats membres ou pour les prestataires de fournir des services de confiance, qualifiés ou non, et si ceux-ci existent, de les utiliser. Par contre, si un prestataire décide (librement) de fournir un ou plusieurs services de confiance, celui-ci a l'obligation de répondre aux conditions du règlement pour pouvoir offrir de tels services (sauf s'ils sont utilisés exclusivement dans des systèmes fermés d'utilisateurs), particulièrement s'ils sont 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. Les juridictions nationales sont tenues d'appliquer ces effets juridiques.

Une **troisième similitude** entre les deux chapitres touche à la volonté de promouvoir un niveau élevé de fiabilité, nécessaire à la concrétisation de l'objectif de renforcement de la confiance. 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 », 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 ».

Ces deux chapitres se différencient cependant 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. Le chapitre trois va quant à lui 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.

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 Etats membres. Ce chapitre s'inscrit donc dans une perspective de facilitation de mise en place du « gouvernement électronique ». Les destinataires de ce chapitre sont avant tout 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.

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 règlement table sur le fait que les Etats membres 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 directe ou indirecte et un tel moyen ne peut être notifié que pour autant qu'il soit déjà utilisé au sein de l'Etat membre 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*.

2. Le volet relatif à l'identification électronique

Un des objectifs du règlement est de lever les obstacles à l'utilisation transnationale des moyens d'identification électronique employés dans les Etats membres à des fins d'authentification, au moins pour les services publics. Cet objectif posé, voyons maintenant les mesures consacrées par le règlement pour le réaliser.

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

Comme déjà indiqué, le règlement ne prévoit aucune obligation pour les Etats membres ni d'introduire ou d'utiliser au niveau national un moyen d'identification électronique ni de notifier à la Commission, si un ou plusieurs de ces moyens sont utilisés au niveau national, un ou plusieurs de ces moyens en vue d'une utilisation transnationale. La notification au niveau européen d'un moyen d'identification électronique utilisé au niveau national est donc volontaire.

Si un Etat membre décide de notifier (volontairement) dans les conditions du règlement un moyen d'identification électronique, cela génère une obligation à charge de deux parties : une obligation pour les autres Etats membres mais également une obligation pour l'Etat membre notifiant.

Pour ce qui concerne les autres Etats membres, le règlement fait peser sur eux, moyennant le respect de certaines conditions, une obligation de reconnaissance mutuelle. Concrètement, les autres Etats membres sont obligés de permettre l'identification aux services en ligne fournis par leurs organismes du secteur public via le moyen d'identification notifié par l'Etat membre notifiant.

Pour ce qui concerne l'Etat membre notifiant, celui-ci 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 Etat membre de vérifier et confirmer les données d'identification personnelles électroniques. A tout le moins, cette obligation existe lorsque la partie utilisatrice établie sur le territoire de l'autre Etat membre 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 ».

Pour bien comprendre ces obligations respectives (obligation de reconnaissance pour les autres Etats membres des moyens d'identification électronique notifiés et obligation pour l'Etat membre 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 cette carte à la Commission 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 de l'Etat 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. En d'autres mots, chaque Etat membre 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 ...

2.2. Les conditions de la notification

Certes, on l'a vu, un Etat membre 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 nombreuses conditions 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.

2.3. 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 Etat membre, il découle du règlement, outre l'application du principe de reconnaissance mutuelle, des conséquences qui touchent tant aux atteintes à la sécurité qu'à la responsabilité.

Le règlement 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'Etat membre notifiant suspend ou révoque immédiatement l'authentification transfrontalière ou les éléments compromis en cause et en informe les autres Etats membres et la Commission.

Le règlement traite de la responsabilité liée aux schémas d'identification électroniques notifiés. Le texte adopté opère un « saucissonnage » des responsabilités entre les différents acteurs (Etat membre notifiant, partie qui *délivre* le moyen d'identification électronique et partie qui *gère* la procédure d'authentification) en fonction de leurs interventions respectives.

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 Etats membres peuvent prévoir un régime de partage de responsabilité différent (plus étendu ou moins étendu).

Le règlement 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, la régime de responsabilité 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.

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

L'objectif principal du chapitre trois du règlement consacré aux services de confiance consiste à instaurer un cadre juridique général concernant l'utilisation de ces services. 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.

3.1. Principes généraux et tronc commun aux services de confiance

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

Le troisième chapitre relatif aux services de confiance ne consacre aucune obligation pour les Etats membres ou pour les prestataires de 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.

Par ailleurs, le règlement consacre une dérogation au profit des « systèmes fermés ». En effet, le règlement stipule expressément 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 ».

3.1.2. 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 répondre aux conditions du règlement pour pouvoir offrir de tels services, particulièrement s'ils sont 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.

Le règlement opère une distinction importante entre services de confiance *qualifiés* et *non qualifiés*. 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, le choix dépendra de la stratégie juridique et de la politique de gestion de risques de l'utilisateur, tout en précisant que l'on peut difficilement préjuger *a priori* de la (non) qualité d'un service de confiance non qualifié. Si la personne utilise ces services dans un domaine dans lequel on peut se satisfaire d'un niveau de sécurité et de fiabilité faibles et/ou pour des opérations juridiques pour lesquelles le risque de contestation est faible voire acceptable, elle pourra se contenter d'un service non qualifié. A l'inverse, si un 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, on lui conseillera de recourir à un service de confiance qualifié.

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, et à la prévisibilité juridique qui en découle.

En effet, tous les services de confiance qualifiés bénéficient d'une clause d'assimilation 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 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 « uniquement » 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. 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.

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

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 y retrouve la procédure d'autorisation préalable. 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 de confiance qualifié, il doit soumettre à l'organe de contrôle une notification de son intention accompagnée d'un rapport sur l'évaluation de la conformité délivré par un organisme d'évaluation de la conformité.

L'organe de contrôle vérifie que le prestataire et le service de confiance qu'il fournit respectent les exigences du règlement. 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 ».

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.

Les listes de confiance sont une des pierres angulaires du règlement. En effet, celles-ci 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 ».

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

On admettra que 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, le règlement prévoit la création d'un label de confiance de l'Union qui identifierait 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 d'autres services de confiance, contribuant ainsi à la transparence du marché.

L'utilisation de ce label par les prestataires qualifiés repose sur une base volontaire. Le cas échéant, le prestataire doit veiller à ce qu'un lien vers la liste de confiance concernée soit disponible sur son site internet.

3.1.5. Régime de contrôle

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

L'organe de contrôle est tenu de contrôler tous les prestataires de services de confiance, qu'ils soient qualifiés ou non. Toutefois, le rôle 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'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 ». 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 mais également *a posteriori* dans le cadre d'un audit périodique (tous les deux ans), d'un éventuel audit extraordinaire sur demande de l'organe de contrôle ou encore à la suite d'une éventuelle notification par le prestataire d'une atteinte à la sécurité. Le règlement met à charge des prestataires les frais liés aux audits précités.

Soit il s'agit d'un prestataire de services de confiance *non qualifiés*, auquel cas 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 ».

3.1.6. Responsabilité des prestataires de service de confiance

Le texte relatif à la responsabilité des prestataires de service de confiance opère 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 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.

- A l'inverse, s'il s'agit d'un prestataire de services de confiance *qualifiés*, la charge de la preuve pèse sur ce prestataire. En effet, il est présumé responsable, à moins qu'il prouve que les dommages résultant d'un manquement à ses obligations prévues par le règlement 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, le règlement permet aux prestataires de services de confiance de ménager contractuellement leur responsabilité. En effet, le règlement les autorise à fixer des limites, sous deux conditions, à l'utilisation des services qu'ils proposent. Premièrement, les clients doivent être dûment informés à l'avance des limites fixées. Deuxièmement, ces limites doivent être reconnaissables par des tiers, 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. Le cas échéant, ils ne sont pas tenus pour responsables des dommages résultant de l'utilisation de services allant au-delà de ces limites.

3.1.7. Aspects internationaux

Dans une économie mondialisée et un environnement internet qui ne connaît pas les frontières, le règlement ne pouvait passer outre une disposition visant à étendre les « effets bénéfiques » du règlement en dehors de l'Union européenne.

Ainsi, le règlement 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.

Le législateur européen a également veillé à ce que les prestataires établis dans l'Union bénéficient du principe de réciprocité. Ainsi, « 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 ».

3.2. 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.

Concernant les effets juridiques des signatures électroniques, le règlement reprend les clauses déjà bien connues, d'une part, de non-discrimination et, d'autre part, d'assimilation qui avaient été consacrées par la directive. 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. Dès lors, il appartient toujours au droit national de définir l'effet juridique produit par la signature manuscrite.

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. 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 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 transfrontalières des certificats qualifiés, les Etats membres ne peuvent pas prévoir d'autres exigences obligatoires.

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.

Par rapport à la directive, le règlement innove en consacrant des exigences relatives au processus et au service de *validation* des signatures électroniques qualifiées. Grâce à ces dispositions, on devrait voir se généraliser l'utilisation de services de validation permettant aux parties utilisatrices de recevoir le résultat du processus de vérification d'une signature électronique qualifiée d'une manière automatisée, fiable et efficace.

On notera enfin que le règlement permet l'utilisation de pseudonymes dans les transactions électroniques, et plus particulièrement dans les certificats de signature électronique. Le cas échéant, il doit être clairement indiqué qu'il s'agit d'un pseudonyme.

3.3. Le cachet électronique versus la signature électronique

Ce nouveau service de confiance créé par le règlement permet de certifier le lien entre les données électroniques « cachetées » et une personne morale. Il s'agit d'une espèce de « sceau » électronique sécurisé dédié aux personnes morales. Le règlement précise que « Les cachets électroniques devraient servir à prouver qu'un document électronique a été

délivré par une personne morale en garantissant l'origine et l'intégrité du document ». Il ajoute également 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 ».

S'il est vrai que 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 fondamentalement de la signature électronique en ce que cette dernière est réservée aux personnes physiques alors que le cachet est dédié aux personnes morales. Une deuxième différence fondamentale réside dans les effets liés respectivement aux signature et cachet électroniques : la signature électronique est *utilisée pour signer*, et ainsi engager la personne physique signataire, alors que le cachet ne permet pas, au sens du règlement, d'engager la personne morale mais se limite à *garantir l'origine et l'intégrité des données électroniques « cachetées »*.

Concernant les effets juridiques des cachets électroniques, le règlement consacre aussi deux clauses.

- La première 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 établit une présomption réfragable selon laquelle : « 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 ».

3.4. L'horodatage électronique

L' horodatage électronique (en anglais « time stamping ») est défini par le règlement 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 » 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 place.

Concernant les effets juridiques des horodatages électroniques, le règlement consacre à nouveau deux clauses.

- La première 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 ».

3.5. Le service d'envoi recommandé électronique

Le règlement définit le service d'envoi recommandé électronique 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 (technique et 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.

Certes, ce service n'est pas encore utilisé de manière généralisée dans de nombreux Etats membres mais le législateur européen y voit une opportunité pour ouvrir de nouvelles possibilités de le commercialiser.

Concernant les effets juridiques du service d'envoi recommandé électronique, le règlement consacre aussi deux clauses.

- La première 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 donne 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 semble considérer 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.

3.6. L'authentification de site internet

L'objectif principal du service d'authentification de site internet 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 tran-

sactions commerciales en ligne, 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.

On note 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.

3.7. Les documents électroniques

Le règlement consacre 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 ». Certes minimaliste, on reconnaîtra au moins à cette disposition l'intérêt de tenter de promouvoir l'utilisation des documents électroniques et d'éviter toute discrimination par rapport aux documents papiers.

4. Les dispositions finales : entrée en vigueur, entrée en application et mesures transitoires

Le dernier chapitre relatif aux dispositions finales nous donnent les éléments permettant de comprendre comment le règlement va progressivement être mis en œuvre, depuis que ce dernier a été publié au Journal Officiel de l'Union européenne le 28 août 2014. Ainsi, ce chapitre contient des dispositions relatives à l'entrée en vigueur, à l'entrée en application, 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 Etats membres pour se préparer et/ou adapter leurs systèmes aux dispositions du nouveau règlement, le règlement 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 au JOUE. 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 les dispositions relatives 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 d'un groupe d'experts informel).

Pour ce qui concerne les dispositions relatives à l'identification électronique, la situation est plus complexe. 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 le règlement 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 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, que, 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.

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 règlement 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 qualifié 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.

SPF Economie, P.M.E., Classe moyenne et Energie
Décembre 2014

Règlement (UE) n ° 910/2014