Transactions électroniques au sein du marché intérieur: identification électronique et services de confiance

2012/0146(COD) - 03/04/2014 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté, par 534 voix pour, 76 voix contre et 17 abstentions, une résolution législative sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Le Parlement a arrêté sa position en première lecture suivant la procédure législative ordinaire. Les amendements adoptés en plénière sont le résultat d'un accord négocié entre le Parlement européen et le Conseil. Ils modifient la proposition comme suit :

Objectif : le règlement viserait à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant **un socle commun pour des interactions électroniques sûres entre les entreprises, les particuliers et les pouvoirs publics** et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électroniques dans l'Union.

Un «service de confiance» a été défini comme un service électronique normalement fourni contre rémunération qui consiste en:

- la création, la vérification et la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envois recommandés électroniques et des certificats relatifs à ces services ou
- la création, la vérification et la validation de certificats pour l'authentification de sites Web ou
- la conservation de signatures, de cachets électroniques ou des certificats relatifs à ces services.

Champ d'application : le règlement s'appliquerait aux **systèmes d'identification électronique notifiés** par un État membre et aux prestataires de services de confiance établis dans l'Union. Il ne s'appliquerait pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés dans le cadre de la législation nationale ou d'accords entre un ensemble défini de participants.

Le règlement devrait être appliqué dans le respect total des principes relatifs à la **protection des données à caractère personnel** énoncés dans la directive 95/46/CE.

Reconnaissance mutuelle : les systèmes d'identification électronique notifiés conformément au règlement devraient préciser les niveaux de garantie **«faible», «substantiel» et/ou «élevé»** des moyens d'identification électronique délivrés.

L'obligation de reconnaître des moyens d'identification électronique ne devrait s'appliquer que lorsque l'organisme du secteur public en question utilise le niveau de garantie «substantiel» ou «élevé» en rapport avec l'accès audit service en ligne.

Notification des systèmes d'identification électronique : les systèmes notifiés par les États membres devraient être accompagnés, entre autres, des **informations suivantes** : i) description du système d'identification électronique notifié, y compris ses niveaux de garantie et l'entité qui délivre les moyens d'identification électronique relevant de ce système; ii) régime de contrôle applicable et des informations sur la responsabilité en ce qui concerne la partie qui délivre le moyen d'identification électronique et la

partie qui gère la procédure d'authentification ; iii) indication de l'entité qui gère l'enregistrement des données d'identification personnelle uniques.

Atteinte à la sécurité : en cas de violation totale ou partielle du système d'identification électronique d'une manière préjudiciable à la fiabilité de l'authentification transnationale de ce système, l'État membre notifiant devrait **suspendre ou révoquer immédiatement l'authentification transnationale** ou les éléments compromis en cause et en informer les autres États membres et la Commission.

Responsabilité : le Parlement et le Conseil ont introduit une nouvelle disposition prévoyant que l'État membre notifiant, la partie qui délivre le moyen d'identification électronique ainsi que la partie qui gère la procédure d'authentification seraient **responsables de tout dommage causé intentionnellement ou par négligence** à toute personne physique ou morale dans une transaction transnationale en raison d'un manquement aux obligations qui leur incombent en vertu du règlement.

Un prestataire de services de confiance qualifié serait **présumé** avoir agi intentionnellement ou par négligence à moins qu'il prouve que les dommages ont été causés sans intention ni négligence de sa part.

Coopération et interopérabilité : les systèmes nationaux d'identification électronique notifiés devraient être interopérables. Le cadre d'interopérabilité viserait à être **neutre du point de vue technologique**, de manière à respecter les divers choix effectués par les États membres. Les États membres devraient coopérer en ce qui concerne l'interopérabilité des systèmes d'identification électronique et la sécurité des systèmes d'identification électronique.

Prestataires de services de confiance provenant de pays tiers : selon le texte amendé, les services de confiance fournis par des prestataires établis dans un pays tiers seraient reconnus comme **équivalents** aux services de confiance qualifiés fournis par des prestataires qualifiés établis dans l'Union si les services provenant du pays tiers sont reconnus en vertu d'un **accord** conclu entre l'Union et des pays tiers ou des organisations internationales.

Accessibilité aux personnes handicapées : dans la mesure où cela est faisable, les services de confiance fournis, ainsi que les produits destinés à l'utilisateur final qui servent à fournir ces services, devraient être accessibles aux personnes handicapées.

Organe de contrôle : les États membres devraient désigner un ou des organes de contrôle chargés d'exécuter les activités de contrôle en application du règlement. Ils devraient également pouvoir statuer, d'un commun accord avec un autre État membre, pour désigner un organe de contrôle sur le territoire dudit autre État membre.

Les organes de contrôle devraient coopérer avec les autorités chargées de la protection des données, par exemple en les informant des résultats des audits des prestataires de services de confiance qualifiés, lorsqu'il apparaît que des règles en matière de protection des données à caractère personnel ont été violées.

Contrôle des prestataires de services de confiance qualifiés : les prestataires de services de confiance qualifiés devraient faire l'objet, **au moins tous les deux ans**, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité.

Label de confiance de l'Union : un label de confiance de l'Union devrait être créé pour identifier les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés. L'utilisation d'un label de confiance devrait se faire **sur une base volontaire** et ne devrait pas entraîner d'autres exigences que celles déjà prévues dans le règlement.

Avant le 1er juillet 2015, la Commission, au moyen d'actes d'exécution, fixerait les caractéristiques 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.