



PRISE DE POSITION DU CCBE SUR L'IDENTIFICATION, L'AUTHENTIFICATION ET LES SIGNATURES ÉLECTRONIQUES

Prise de position du CCBE sur l'identification, l'authentification et les signatures électroniques

Le Conseil des barreaux européens (CCBE) est l'organe représentatif d'environ un million d'avocats européens, appartenant aux barreaux qui en font partie, dans 31 pays membres effectifs et 11 pays associés et observateurs. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens. Dans la présente communication, le CCBE répond à la consultation publique que la Commission européenne a lancée sur l'identification, l'authentification et les signatures électroniques.

Étant donné que le questionnaire est en grande partie orienté vers la collecte d'informations et d'avis au niveau des États membres ou des régions, et en raison de la diversité concernant l'adoption et l'utilisation des signatures numériques parmi les barreaux membres du CCBE, le CCBE se retrouve dans l'impossibilité de répondre au questionnaire. En conséquence, au lieu de répondre à l'ensemble spécifique de 29 questions, le CCBE souhaite attirer l'attention de la Commission sur un certain nombre de questions et de sujets de préoccupations plus généraux concernant la profession d'avocat.

À titre d'observation préliminaire, le CCBE constate qu'il existe une certaine confusion en raison de la terminologie employée dans le questionnaire qui, partout, fait référence aux « signatures électroniques ». La directive signatures électroniques (1999/93/CE) établit une distinction entre les « signatures électroniques », « signatures électroniques avancées » et « signatures électroniques qualifiées », les deux dernières étant plus connues sous le nom de « signatures numériques ». Il ressort de l'examen du questionnaire que la consultation concerne presque exclusivement les signatures numériques plutôt que de simples signatures électroniques : la présente réponse part de ce principe.

Le CCBE accueille favorablement la proposition de la Commission européenne de revoir la directive sur les signatures électroniques et de préparer l'initiative prévue sur la reconnaissance mutuelle de l'identification et de l'authentification électroniques. Bien que n'étant pas en mesure d'apporter des commentaires sur les avantages supposés de cette révision pour les entreprises et le commerce, le CCBE tient à s'assurer qu'elle servira et facilitera le développement de systèmes efficaces de justice en ligne et par la même occasion l'amélioration de l'accès à la justice en Europe. Il souligne cependant que toute solution proposée doit à la fois respecter les principes de subsidiarité et être équilibrée en mettant davantage l'accent sur l'interopérabilité que sur l'harmonisation en tant que telle. Les signatures numériques et autres formes d'identification et d'authentification électroniques sont souvent utilisées de manière plus ou moins répandue dans un certain nombre de juridictions afin de permettre aux avocats d'effectuer un large éventail d'opérations, telles que le dépôt de pièces auprès des tribunaux et des administrations publiques ou la conduite de procédures et d'opérations transfrontalières. D'autres applications sont également possibles grâce à ces technologies, par exemple dans les domaines de l'aide judiciaire ou des opérations liées aux honoraires et à la TVA. Il ne faut pas oublier que certains États membres, tel que le Royaume-Uni, n'ont pas recours à un usage intensif des signatures numériques à ces fins au profit de solutions à mots de passe et code PIN.

Dans un souci de faciliter l'accès des citoyens de l'UE à la justice, le CCBE travaille actuellement à un certain nombre de projets, dont la fonction de recherche d'un avocat, ainsi que le développement du portail d'e-justice en collaboration avec la Commission. L'accès du public à la fonction de recherche d'un avocat ne nécessitera pas de signature électronique, et des discussions sont en cours concernant le ou les niveaux d'authentification qui seraient exigés pour l'accès au portail d'e-justice ou certaines parties de celui-ci, en particulier concernant les mérites relatifs, du moins pour certaines fins, de l'accès par signatures numériques et l'accès par mot de passe et code PIN. Le point-clé en matière d'identification et d'authentification électroniques concerne la sécurité des échanges. Le niveau de sécurité doit être adapté à l'information concernée. Lorsqu'il s'agit d'informations confidentielles, par exemple dans le cadre d'une obligation déontologique de l'avocat telle que la confidentialité, un niveau

très élevé de sécurité est nécessaire bien que, comme indiqué ci-dessus, il existe une certaine diversité d'approche selon les États membres quant à la méthode la plus appropriée d'y parvenir.

Néanmoins, l'interopérabilité et, dans certaines circonstances, la convergence technique entre les systèmes nationaux de justice en ligne pourraient être nécessaires afin de garantir un niveau équivalent de sécurité des applications transfrontalières, conformément à la législation communautaire.

C'est la raison pour laquelle le projet nommé [e-CODEX](#) (*e-Justice Communication via Online Data Exchange*) présente un intérêt particulier. Ce projet, auquel le CCBE participe aux côtés des 15 ministères de la justice de 15 États membres de l'UE, vise à développer des blocs de construction utilisables dans ou entre les États membres afin de soutenir les procédures transfrontalières dans le domaine de la justice et cherche à (a) permettre un accès facile et sécurisé des citoyens, des entreprises et des juristes aux discours juridiques dans les autres États membres de l'UE, (b) améliorer l'efficacité transfrontalière des procédures judiciaires à l'aide de normes communes et d'une interopérabilité accrue et (c) améliorer l'efficacité des procédures judiciaires transfrontalières par des normes et des solutions qui facilitent la coopération transfrontalière dans le traitement des affaires.

Le CCBE a déjà pris des mesures importantes pour la profession d'avocat concernant les signatures électroniques et les cartes d'identité électroniques et a publié, par l'intermédiaire de son comité du droit des technologies de l'information, les lignes directrices et recommandations suivantes :

- [Cadre visant à établir un système européen pour les cartes d'identité électroniques](#)
- [Normes techniques pour une interopérabilité des cartes d'identité électroniques](#)
- [Recommandations du CCBE sur les cartes d'identité électroniques pour la profession d'avocat](#)
- [Lignes directrices sur les projets de signatures électroniques et sur l'usage des signatures électroniques pour les avocats](#)

Ces recommandations et lignes directrices ne sont pas obligatoires, et la politique du CCBE, conformément au principe de la proportionnalité, consiste à laisser la décision concernant la méthode de vérification de l'identité à employer, le cas échéant, aux barreaux membres.

L'interopérabilité et la convergence technique plutôt que l'harmonisation

Le contexte ci-dessus expose que l'approche du CCBE vise à parvenir à une interopérabilité complète. Cette approche est en effet cohérente avec le cadre actuel de l'UE concernant les conditions applicables aux signatures électroniques qui, au lieu de chercher à harmoniser les solutions nationales en matière de signatures électroniques (dont les signatures numériques), est fondée sur des principes communs et un ensemble de normes (techniques) minimales permettant une interopérabilité transfrontalière. Les moyens de mise en conformité, le système de la structure nationale, la politique de certification et le financement relèvent de la décision des États membres en fonction de leur situation nationale individuelle. Le CCBE estime que l'adhésion à ce principe doit être maintenue lors de toute révision du cadre juridique sur les signatures électroniques et numériques, l'identité et l'authentification électroniques. L'harmonisation n'est pas nécessaire d'un point de vue technique. La nécessité d'une coopération de l'UE dans ce domaine porte essentiellement sur la demande d'interopérabilité transfrontalière et devrait se concentrer sur des principes et des normes minimales communs afin de faciliter les opérations intra-communautaires. Dans cet esprit, la garantie de la reconnaissance mutuelle totale de ces signatures numériques est primordiale dans les applications elles sont utilisées.

Le consentement électronique

Au sujet de la question 15 du questionnaire de la Commission, le CCBE tient à soulever certaines préoccupations concernant la question du « consentement électronique ». En substance, le sens de « consentement électronique » tel qu'il est employé dans le questionnaire, se rapporte à une simple signature électronique (par opposition à une signature numérique), comme le fait de cliquer sur le bouton « J'accepte » par exemple. Selon le CCBE, la véritable question ne concerne pas tant la technologie de « consentement électronique » mais plutôt sur garantie que la personne qui accepte le

Conseil des barreaux européens – Council of Bars and Law Societies of Europe

association internationale sans but lucratif

Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.eu – www.ccbe.eu

02.05.2011

contenu a vraiment lu ou compris le contenu. Le CCBE s'inquiète du fait que les consommateurs sont très souvent induits en erreur par des informations peu claires et un contenu complexe, et qu'il existe, ou devrait exister, un véritable questionnement, dans une perspective de protection des consommateurs, quant à savoir si le fait de cocher « J'accepte » suffit ou devrait suffire à établir une transaction, indépendamment des questions d'identité ou de la technologie utilisée.

Les défis à venir

De l'examen du cadre juridique communautaire actuel, qui existe depuis plus de dix ans, ressortent clairement un certain nombre de défis auxquels l'Union européenne fait face aujourd'hui en raison de facteurs nouveaux et de l'évolution des technologies. Le CCBE souhaite aborder quelques-uns de ces défis, notamment ceux qui présentent un intérêt particulier pour la profession d'avocat.

L'un de ces défis est la question des **signatures hybrides**. Les signatures numériques sont de plus en plus admises juridiquement, mais les documents électroniques signés numériquement ne sont en fait dignes de confiance que dans la mesure où ils sont maintenus dans leur milieu électronique d'origine. Dès que ce type de document sort de son contexte original, par exemple par impression, cela pose une question concernant son statut juridique. De nos jours, la technologie peut offrir une garantie de sécurité du début à la fin, à savoir que le document imprimé est un extrait légitime du document électronique d'origine. Cependant, d'un point de vue juridique et dans un contexte transfrontalier, la validité des signatures hybride reste incertaine.

Un autre défi qui est source de préoccupations est la question de la **validation à long terme en matière d'archivage électronique des documents**. Que l'on utilise des mots de passe d'utilisateur ou des infrastructures à clés publiques, les documents créés grâce à l'utilisation de signatures numériques auront, après quelques années, perdu leur sécurité technique, par exemple parce que le certificat a été révoqué ou parce que le mot de passe n'est pas plus valable. Certaines juridictions, comme l'Autriche, ont adopté des solutions techniques et législatives mixtes en vue de résoudre ce problème, mais d'un point de vue juridique et dans un contexte transfrontalier, la validité à long terme de ces documents demeure incertaine.

Il existe une autre question liée qui se réfère à **l'espérance de vie des systèmes électroniques** utilisés pour les applications de justice en ligne. Ces systèmes doivent garantir, si nécessaire au moyen de mises à jour régulières, qu'il est toujours possible d'accéder au contenu des applications concernées tout en préservant leur sécurité. À cet égard, il convient de noter que certains systèmes peuvent poser des problèmes (du moins ceux qui dépendent de logiciels propriétaires) au fil du temps par manquement des fournisseurs du produit, et que de réels problèmes peuvent survenir lorsque la mise à jour ne peut être assurée de manière continue.

Par souci de sécurité juridique, le CCBE estime que l'occasion pourrait être saisie d'introduire un peu de clarté quant à certaines de ces questions lors de l'examen de la directive sur les signatures électroniques.