Bassem Zein

Les documents électroniques et l'administration des preuves

Résumé de l'exposé en langue allemande de Helmut Rüssmann aux Journées d'informatique juridique 2004 à Berne

L'exposé examine les problèmes juridiques que pose en droit allemand l'utilisation d'un document électronique dans la procédure d'administration des preuves. Le document électronique est-il admis comme moyen de preuve? Si oui, lequel? Comment juger de sa force probante et déterminer son authenticité et l'intégrité de son contenu? Une partie ou des tiers doivent-ils produire des documents électroniques en leur possession?

[Rz 1] Le droit allemand de procédure ne pose pas d'obstacle à ce qu'une preuve soit administrée au moyen d'un document électronique. Ce sont les règles sur l'inspection locale qui s'appliquent ou, si des connaissances techniques particulières sont requises, celles régissant l'expertise. Le document électronique ne satisfait par contre pas à la définition du document écrit que pose le code de procédure civile allemand (ci-après: ZPO). Le régime particulier prévu pour les document écrits privés (§ 416 ZPO) ne s'applique donc pas. La force probante du document électronique est soumise de ce fait à la règle générale de la libre appréciation du juge (§ 286 ZPO).

[Rz 2] Le document électronique présente des possibilités de falsification plus nombreuses que le document écrit. Certes, la falsification faite par l'auteur au moment de la rédaction est aussi peu visible sur un écrit que sur un document électronique. Mais une falsification faite après coup sur le document électronique n'est pas décelable à l'aide des systèmes d'exploitation ou des programmes dont sont habituellement équipés les ordinateurs personnels. Il en va de même si quelqu'un envoie un courrier électronique sous le nom de quelqu'un d'autre ou si une commande en ligne contient des indications fausses.

[Rz 3] La force probante d'un document électronique est donc incertaine. La signature électronique offre une solution à ce problème. Elle permet de déceler les manipulations du contenu et d'identifier l'auteur d'un document électronique.

[Rz 4] La signature électronique comprend une clé publique accessible à tous sur internet et une clé privée accessible (idéalement) au seul titulaire des deux clés. Supposons que Bob corresponde avec Tina. Bob garantit la confidentialité du message s'il le crypte avec la clé publique de Tina. Elle seule peut en effet le décrypter avec sa clé privée. Si, en plus, Bob 'signe' le message avec sa clé privée à lui, Tina ouvrira le message avec la clé publique de Bob et saura que le message vient de lui (authentification). Bob peut également gagner du temps en comprimant le texte avant de le 'signer'. Tina pourra toujours déceler toute manipulation ultérieure en comparant le texte comprimé de Bob ouvert avec sa clé publique et le texte comprimé qu'elle obtient à partir du message qu'elle a reçu.

[Rz 5] L'identité du titulaire de la clé privée doit être certifiée par un tiers, qui garantit l'attribution d'une clé privée à son titulaire désigné. Dans des structures publiques et anonymes, cette tâche doit être attribuée à une institution, nommée dans le monde digital 'trustcenter'. Le titulaire d'une clé privée attestera de son identité auprès d'elle.

[Rz 6] Pour que les «trustcenters» soient réellement fiables, ils doivent remplir certaines exigences, posées en Allemagne par la *Signaturgesetz (SigG)*. Cette loi prévoit plusieurs types de signatures électroniques (§ 2 ch. 1 à 3 SigG), la plus sûre étant la signature électronique qualifiée. Elle doit être basée sur un certificat qualifié, délivré par un fournisseur de services de certification. Le fournisseur n'est pas soumis à autorisation, mais il doit s'annoncer à l'autorité compétente et ne peut exercer que s'il remplit certaines conditions.

[Rz 7] La question de la force probante d'un document signé électroniquement se pose. Le § 292a ZPO, en vigueur depuis 2001, a limité la liberté d'appréciation du juge (§ 286 ZPO) pour ce qui est des déclarations de volonté. Il prévoit que la signature électronique rend l'authenticité de la déclaration vraisemblable. La vraisemblance ne peut être renversée que par des faits permettant de douter sérieusement que la déclaration émane du titulaire de la clé privée. La *Justizkommunikationgesetz*, actuellement devant le Parlement allemand, introduit un nouvel §371a dans la ZPO, qui reprend la règle de la vraisemblance pour tous les documents électroniques. Il soumet également le

document signé électroniquement au régime particulier appliqué aux documents écrits. Cette nouveauté est toutefois sans valeur pour les documents privés, car le § 416 ZPO exprime une tautologie ne facilitant en rien la preuve: il faut prouver que le document émane de l'auteur pour qu'il soit légalement admis que le document émane de l'auteur.

[Rz 8] La question de la force probante de la signature électronique aurait pu être résolue sans que le législateur n'intervienne. On aurait pu en effet appliquer le critère de la première vraisemblance, développé par la jurisprudence. Ce critère se fonde sur l'expérience de la vie. Or il n'y a pas d'expérience établie permettant de déduire l'authenticité d'un document du fait qu'il est signé électroniquement. La jurisprudence n'aurait donc pas nécessairement admis la vraisemblance, comme le fait la loi.

[Rz 9] En admettant qu'une solution législative soit nécessaire, le législateur, plutôt que de prévoir la vraisemblance, aurait dû prévoir une présomption. Elle ne devrait en outre intervenir que si l'accès à la clé privée est protégé par un test biométrique. Le risque d'accès d'un tiers non autorisé à la clé privée constitue en effet la faiblesse principale de la signature électronique. La carte à puce et l'introduction d'un code PIN ne constituent pas une protection suffisante à cet égard.

[Rz 10] Le devoir de collaborer des parties et de tiers est la dernière question à examiner. Avant la réforme de la ZPO, en vigueur depuis le 1er janvier 2002, la partie qui avait la charge de la preuve était incitée à produire un document électronique en sa possession: si elle ne le faisait pas et que le fait n'était pas prouvé, elle risquait de perdre le procès. Par contre, la partie adverse ne subissait pas de conséquence négative si elle ne produisait pas un document en sa possession, à moins d'y être obligée par le droit matériel. De même, un tiers n'avait pas d'obligation à cet égard. Cette situation était insatisfaisante et contredisait les règles sur le témoignage, qui obligent en principe toute personne à témoigner. Elle a donné lieu à de nombreuses critiques et a été partiellement atténuée par la pratique. Le législateur a finalement réagi et doté l'Allemagne d'une législation moderne dans cette matière, comparable à celles de ses Etats voisins. Depuis le 1er janvier 2002, une partie ou un tiers ont un devoir de produire un document en leur possession à moins qu'ils puissent invoquer un motif de refus prévu par la loi. L'accès aux documents électroniques pour l'administration de la preuve est ainsi assuré.

Lic. iur. Bassem Zein est collaborateur scientifique à l'Office fédéral de la justice.

Le présent article est un résumé de l'exposé en langue allemande de Helmut Rüssmann aux Journées d'informatique juridique 2004: Helmut Rüssmann, Beweisführung mit elektronischen Dokumenten, in: Jusletter 8. November 2004.

Rechtsgebiet:	Informatik und Recht
Erschienen in:	Jusletter 8. November 2004
Zitiervorschlag:	Bassem Zein, Les documents électroniques et l'administration des preuves, in: Jusletter 8. November 2004
Internetadresse:	http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=3511