JURIDIQUE

L'authentification saisie par le Droit

L'authentification[1] est une notion au périmètre très vaste (de l'accès à un espace client à la signature d'une opération…) qui parle autant à l'Ingénieur qu'au Juriste. Pourtant, de par ses applications et modalités multiples, elle reste difficile à saisir. Récemment prise en compte par le droit, elle constitue un nouveau sésame du numérique.

Envisagée sous l'angle de la sécurité, l'authentification constitue l'une des conditions sine qua none de la sécurité des systèmes d'information. Ainsi, la norme ISO 27001 fixant les méthodes et pratiques en matière de système de management de la sécurité de l'information (SMSI) prévoit un chapitre 11 relatif à la gestion des droits des utilisateurs et à leur authentification. Il indique notamment les mesures se rapportant au contrôle d'accès (données, réseaux, systèmes), à la gestion des droits, des mots de passe, à la mobilité, etc.

L'authentification dans les textes

L'importance de l'authentification déborde largement le monde de la technique. Elle renvoie habituellement à un impératif juridique fort : en droit, un acte, un fait ou une action doit pouvoir être imputé à une personne déterminée. Il s'agit de rendre compte de ses actes au cours de la vie sociale spécialement dans le numérique. Pourtant, en tant que sésame numérique, le Droit ne l'a envisagée que récemment. La première véritable définition juridique de l'authentification a été introduite dans le Règlement communautaire n° 460/2004 du 10 mars 2004 [2] instituant l'ENISA. Selon son article 4-e, l'authentification est *« la confirmation de l'identité prétendue d'entités ou d'utilisateurs »*.
Elle a été substantiellement reprise en France par le Référentiel général de sécurité (V.1.0) qui énonce, dans son § 3.2. : *« L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine (ci-après désignée* « entité »). Généralement, l'authentification est précédée d'une identification, qui permet à cette entité de se faire reconnaître du système au moyen d'un élément dont on l'a doté. En d'autres termes, s'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité.». La proposition de règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur [3] dans son article 3 définit ainsi l'authentification : *« un processus électronique qui permet de valider l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée électronique »*. Si cette définition reprend l'idée de vérification ou de validation de l'identification électronique, elle étend le concept d'authentification à la validation de l'origine et de l'intégrité d'une donnée électronique.
Le plus souvent, l'authentification est encadrée par contrat, notamment par la signature de conditions d'utilisation en interne ou pour un service en ligne avec une convention de preuve.

Méthodes et risques juridiques liés à l'authentification

Certains secteurs de l'économie se préoccupent d'avantage de l'authentification du fait même des risques juridiques et/ou financiers que son défaut ou son absence pourrait causer.
On pense évidemment au secteur bancaire et financier qui met en exergue l'importance de l'authentification forte : de l'usage d'un mot de passe aléatoire, et plus encore d'une solution d'authentification non rejouable lors de virements sur l'Internet ou d'autres opérations sensibles (Rapport FBF-BDF du 2 mars 2009 sur l'authentification et la sécurité des paiements sur l'Internet) ; de l'authentification forte du client entendue comme *« une procédure de validation de l'identification d'une personne physique ou morale reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories connaissance, possession et inhérence, qui sont indépendants, en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification »* (projet d'art. 4-22 d'une directive sur les services de paiement, dite DSP2 [4]). Cette définition semble faire suite aux recommandations pour la

(1) Eric A. Caprioli, *«De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ?»*, février 2011, Colloque de l'ONU sur le Commerce électronique, 14-16 février 2011, New York, disponible sur le site www.caprioli-avocats.com.

(2) J.O.C.E L 077, 13 mars 2004, p.1 et s.
(3) PE et Cons. UE, prop. de règl. COM(2012)238 : http://ec.europa.eu.. V. Eric A. Caprioli, P. Agosti, La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance, CCE n°2, février 2013, ét. 3.

sécurité des paiements via Internet de la Banque Centrale Européenne (Janvier 2013) [5].

Mais d'autres secteurs requièrent également une garantie d'identité comme celui des envois électroniques (l'article 1369-8 du Code civil exige la garantie de l'identité du destinataire d'une lettre recommandée électronique).

Les différents textes laissent entrevoir deux méthodes d'authentification :

Authentification standard ou à un facteur : l'utilisateur saisit uniquement les informations qu'il possède (ex : login/mot de passe) ;

Authentification forte : elle impose une combinaison de deux canaux distincts : un en ligne, l'autre via le téléphone mobile (ex : OTP) ou via un envoi postal (ex : remise d'un code par recommandé).

Un autre point est de déterminer si l'authentification est ou non rejouable, l'idée étant de faire en sorte que cette dernière est propre à une opération donnée (accès à un site, signature/validation...).

Pour mettre en œuvre cette « non-rejouabilité », de nombreuses méthodes s'appuient sur des One Time Password (OTP) envoyés par SMS sur un téléphone portable ou un token et plus récemment sur la reconnaissance vocale (ex : expérimentation du procédé Talk to Pay, autorisé par la CNIL) [6].

De nombreux risques doivent être pris en compte : dénégation d'un acte juridique électronique ; introduction et accès frauduleux aux systèmes d'information et données ;

utilisation délictuelle des réseaux : infractions liées aux paiements ou facilitées ou liées à l'utilisation des TIC : diffamation, diffusion de contenus illicites, usurpation d'identité, phishing...

Dans l'Union européenne, l'identification directe ou indirecte des personnes physiques implique le respect des règles applicables aux données à caractère personnel par le responsable du traitement. Une proposition de règlement des données à caractère personnel est en cours [7]. Il reste que dans un environnement en constante évolution que l'analyse des risque juridiques et opérationnels impose de plus en plus souvent l'utilisation de procédés d'authentification forte.

Les sanctions judiciaires

Les décisions relatives au défaut d'authentification sont rares et doivent être envisagées comme sanctionnant une mesure de sécurité informatique défaillante. Ainsi, aux Etats Unis, dans une décision du Tribunal de l'Illinois (affaire Shames Yeakel vs Citizen Financial Bank) du 21 août 2009 (Case 07 C 5387), les juges ont accueilli favorablement la plainte d'une victime d'une cyber-attaque sur son compte bancaire en ligne, déposée contre l'établissement bancaire. Ce jugement remettait en cause l'authentification à facteur unique pour protéger l'accès aux comptes bancaires en ligne.

En France, la Cour d'appel de Versailles le 18 novembre 2010 [8], a jugé une question de sécurité connexe pour engager la responsabilité d'une banque, concernant l'utilisation frauduleuse d'un mot de passe par un conjoint indélicat pour accéder à un compte d'épargne « commun ». La sécurité du process n'était pas suffisamment forte et conforme à l'état de l'art.

En outre, la loi a intégré au Code pénal le délit d'usurpation d'identité avec l'article 226-4-1 du Code pénal (LOPPSI 2 du 14 mars 2011) : *« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. ».*

Les auteurs

Eric A. CAPRIOLI,
Avocat à la Cour de Paris, Docteur en droit, Vice-Président du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), expert aux Nations Unies.

Pascal AGOSTI,
Avocat associé, Docteur en droit.
http://www.caprioli-avocats.com

Et la CNIE ?

Bloqué dans le désert des Tartares, le marché est toujours dans l'attente de la Carte Nationale d'Identité Electronique. Après maintes tentatives avortées, la loi du 27 mars 2012 relative à la protection de l'identité a organisé les procédures de délivrance et de gestion des documents d'identité électronique (carte d'identité et passeport). Selon son article 3, la future carte d'identité électronique devait contenir, dans une puce, des données permettant à l'internaute de prouver son identité et de signer des transactions sur internet, et ainsi de lutter contre l'usurpation d'identité ; cette possibilité était déjà prévue dans certains pays voisins comme la Belgique. Toutefois, le Conseil constitutionnel a censuré cette disposition, au motif que cet article manquait de précision. Pour pallier l'attente de cet outil « incontestable » d'authentification le label IDéNum, lancé le 1er février 2010, a donné lieu à la création d'une société Idénum le 11 mars 2013 ('Euro-information, La Poste, SFR, Solocal Group et la Caisse des Dépôts).

Actuellement, la CNIE semble de nouveau sur la sellette, le Ministre de l'Intérieur privilégiant la sécurisation de la procédure en amont de la fabrication du titre (Etat civil, justificatifs de domicile) et la traçabilité des titres [9]. L'authentification délivrée par l'Etat ne mérite pourtant pas pareils atermoiements. ■

(4) COM(2013) 547 /3, 2013/0264 (COD) .

(5) PE et Cons. UE, prop. de règl. COM https://www.ecb.europa.eu/pub/pdf/other/recommendationspaymentaccountaccessservicesdraftpc201301en.pdf.

(6) V. Délibération n° 2013-198 du 11 juillet 2013 autorisant la Banque Postale à mettre en œuvre à titre expérimental un système d'authentification des titulaires de cartes de paiement par biométrie

(7) V. Eric Caprioli et Isabelle Cantéro, Les données à caractère personnel au coeur de la sécurité et des libertés numériques, MagSecurs, n°36, p. 29 et s.

(8) Cour d'appel de Versailles, 16ème ch. 18 novembre 2010, n° 09/06634, Marie-Paule C. épouse A. c/ SA Natixis Interepargne, Comm. Com. électr. N°10, octobre 2011, comm. 94, Note Eric A. Caprioli.

(9) http://www.assemblee-nationale.fr/14/cri/2013-2014/20140056.asp