Implications juridiques de l'HTTPS

Retour au sommaire de la lettre

Domaine :	Recherche	Référencement
Niveau :	Pour tous	Avancé

La sécurisation des sites web grâce au protocole HTTPS/SSL est actuellement dans l'air du temps. Mais, si de nombreux points techniques doivent être mis en oeuvre dans une telle migration, les aspects juridiques sont loin d'être négligeables pour être en phase avec les lois européennes. Petit état des lieux des procédures à vérifier si vous envisagez de passer le pas pour votre site web...

Le protocole HTTP est bien connu de tous dans la mesure où il a été un des tous premiers à être disponible sur Internet et, bien sûr, le Web. L'HTTPS, à savoir « protocole de transfert hypertexte sécurisé » est une combinaison de l'http avec une couche de chiffrement comme le SSL ou le TLS permettant de sécuriser la liaison.

Ce protocole est fortement utilisé désormais car il permet l'authentification de l'internaute et donc de l'utilisation de son compte / données personnelles. Il est, de plus, utilisé dans les transactions électroniques (banque en ligne, achats en ligne, etc.). Sa couche sécurisée est encadrée juridiquement et le https doit, depuis l'adoption par le Parlement européen du nouveau règlement (UE) No 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques, être appréhendé dans un cadre très particulier.

Qu'est ce que le https ?

Le https permet d'identifier les personnes accédant à un site et de garantir un certain niveau de sécurité et de confidentialité. La sécurité des informations transmises est basée sur l'utilisation d'un algorithme de chiffrement, et sur la reconnaissance de validité du certificat d'authentification du site visité (SSL).

La plupart des certificats utilisés sont de type X509. Dans le cas des serveurs web, ces certificats sont utiles pour fournir plusieurs sites HTTPS sur une seule adresse IP. En effet, en HTTPS, l'échange du certificat se fait avant que le navigateur client n'ait transmis le nom de domaine qui l'intéresse. Or, si le certificat fourni par le serveur ne contenait pas le nom requis par le client, celui-ci déclencherait une alerte de sécurité.

En somme, le https peut être défini en un http et une couche SSL, garantissant ainsi une navigation sécurisée.

Les actuelles obligations de sécurité

La loi Informatique et libertés impose des exigences en matière de sécurité. Aussi étonnant que cela puisse paraître, il s'agit aujourd'hui du seul texte de portée générale qui impose une sécurité informatique (même s'il existe de nombreux textes spécifiques à certains secteurs qui traitent également de cette problématique).

Le responsable du traitement (en l'espèce, le responsable qui édite le site ou le service web) est tout d'abord tenu de prendre « toutes précautions » utiles au regard de la nature des données et des risques présentés par le traitement pour « préserver la sécurité des données » et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Cette obligation de sécurité, définie aux articles 34 et 35 de la loi informatique et libertés et dont la violation est pénalement sanctionnée, a été précisée par la Cnil. Aux termes d'une délibération portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes d'information, la Cnil précise qu'il appartient *« aux détenteurs ou aux utilisateurs de fichiers nominatifs de prendre, sous leur responsabilité, préalablement à toute*

mise en œuvre d'une application informatique, compte tenu de la finalité du traitement, du volume des informations traitées et de leur degré de sensibilité (…) les mesures générales de sécurité nécessaires » (Délibération n°81-94 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes d'information)
Le non-respect du principe de sécurité est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-17 du Code pénal).

De plus, les obligations de sécurité sont également fixées par les articles 323-1 et suivants du Code pénal (portant sur les intrusions et autres piratages). Il est important de comprendre qu'une société qui n'aurait pas mis en œuvre les mesures nécessaires à la sécurisation de son système d'information ne saurait se prévaloir d'un accès frauduleux dans son système d'information et ne pourrait pas porter plainte pour piratage le cas échéant (Cour d'appel de Paris, 30 octobre 2002).

En d'autres termes, la mise en place de systèmes permettant d'améliorer sensiblement la sécurité informatique permet de respecter les principes de la loi Informatique et libertés. A ce titre, la mise en place d'un https répond à cette contrainte.

L'ordonnance du 24 aout 2011 a, de surcroît, créé une obligation de notifier à la CNIL, toute attaque informatique touchant des données personnelles, lorsqu'elle est subie par un *« fournisseur de services de communications électroniques accessibles au public »*. Il s'agit des opérateurs devant être déclarés auprès de l'ARCEP (par exemple, les fournisseurs d'accès à internet ou de téléphonie fixe et mobile). Les sites, tels que les banques en ligne, les sites d'e-commerce ou les télé-services des administrations, ne sont pas concernés. Le champ de l'ordonnance est suffisamment large pour que les *« fournisseurs de services de communications électroniques »* prennent leur précaution et sécurisent les accès, notamment en intégrant l'https.

Au-delà de ces règles de sécurité informatiques posées par la loi et dont le https permet de répondre correctement, il convient de souligner que le législateur européen a récemment introduit un corpus très important en termes de sécurité informatique, certifications et autres procédures d'authentification

L'apport du règlement européen

La directive sur la signature électronique de 1999 n'a pas rencontré le succès espéré. En effet, il était prévu de mettre en place un (vrai) système de certification électronique, basé sur un principe selon lequel chaque Etat reconnait et valide les prestataires de certificats / cachets d'horodatage qui peuvent vendre leurs prestations au grand public. Ce système devait, dans l'esprit et au départ, copier le système américain, mais celui-ci n'était que privé et en rien encadré par la puissance publique (qui écartait fermement le secteur privé dès que la sphère militaire pouvait être concernée).

Ainsi, les Européens ont finalement développé un système propre, avec des procédures de validation des opérateurs privés sévères et très techniques.

Or, d'une part, le chiffre d'affaires n'a pas été au rendez-vous et d'autre part, les procédures des Etats étaient tellement spécifiques, que les opérateurs européens ne pouvaient finalement opérer que dans leur pays d'origine et non dans l'Union européenne.

La Commission a donc décidé de modifier la législation et d'adopter un texte unique pour tous, imposant ainsi la reconnaissance automatique dans toute l'Union européenne.

Concrètement, les deux systèmes opérant sur Internet et intégrant le https / SSL / TLS sont :
- Principalement des opérateurs américains (dont Google et son Google Internet Authority ou Verisign) ;
- Très accessoirement et rarement des opérateurs européens.

Or, les opérateurs américains ne sont pas soumis aux contraintes de la réglementation européenne, à l'obligation de passer par des procédures de validation, la nécessité d'acheter et de gérer des certificats homologués par une autorité publique (l'ANSSI en France par exemple). En d'autres termes, le niveau de sécurité est plus faible, mais le coût de ce service est également beaucoup plus faible. D'où la clé de leur succès.

En effet, la législation souffre d'un énorme problème : les juges refusent souvent de l'appliquer. Tout le cœur du problème vient de là. La loi, européenne ou française, précise que la sécurité est présumée acquise, que l'authentification et la non-répudiation (et donc, la perfection de la preuve) sont réputées totales lorsqu'on utilise un certificat qualifié (sans entrer dans les détails, afférent à une signature électronique avancée). Lorsque l'on utilise pas ce certificat, il n'y a pas de présomption et en cas de problème, c'est à l'éditeur du site Internet / Web service de démontrer ces caractéristiques (de sécurité et de fiabilité).

En conséquence, logiquement on doit se dire qu'acheter les services d'un opérateur européen qui délivre des certificats répondant aux critères de la loi permet de se mettre à l'abri en cas de problème (piratage, problème de preuve, etc…). Or, ces cas sont arrivés à plusieurs reprises et - à notre connaissance - quasiment jamais, un juge français n'a osé écarter les certificats (non légaux) des opérateurs ne respectant pas les critères et notamment des opérateurs américains (type Verisign).

Ainsi, acheter plus cher un service légal n'est actuellement quasiment jamais récompensé par la justice. C'est au demeurant précisément parce qu'il existe ce que nous appelons un « laxisme » judiciaire que le marché des certificats qualifiés est si difficile et que les opérateurs proposant des certificats non qualifiés ou ne répondant pas à la loi française ou européenne peuvent vendre avec une telle différence de prix avec un tel succès.

Le nouveau règlement ne traite pas le problème puisque ce sont les juges qui doivent accepter d'appliquer la loi.

En revanche, preuve de l'influence incroyable des opérateurs américains en Europe, les « certificats qualifiés d'authentification de site Internet » viennent d'être reconnus juridiquement et même encadrés. Ainsi, les certificats qualifiés d'authentification de site web contiennent :
- une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de site internet ;
- un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi et le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels ;
- au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans les registres officiels ;
- des éléments de l'adresse, dont au moins la ville et l'État, de la personne à laquelle le certificat est délivré et, le cas échéant, ces éléments tels qu'ils figurent dans les registres officiels ;
- le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;
- des précisions sur le début et la fin de la période de validité du certificat ;
- le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;
- la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat ;
- l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé ;
- l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

En conséquence, à compter du 1er juillet 2016, date d'entrée en vigueur du règlement, les sites en https devront respecter ces critères et donc, avoir des opérateurs proposant des certificats basés sur ces principes. Sauf si les juges refusent toujours d'appliquer la législation et qu'il n'y ait alors aucun intérêt à dépenser plus pour ne pas être plus protégé juridiquement…

Alexandre Diehl
Avocat à la Cour, cabinet Lawint (http://www.lawint.com/)