Temps : 3’00’’

LA SÉCURISATION DU TRAFIC DES DONNÉES PERSONNELLES DEVIENT UN FONDAMENTAL POUR TOUTE ENTREPRISE. APRÈS DES DÉCENNIES DE LAISSER-ALLER, LE LÉGISLATEUR, LES NAVIGATEURS ET LES UTILISATEURS ATTENDENT AUJOURD’HUI DE TOUT ACTEUR DIGITAL UN MINIMUM DE SÉCURITÉ.

Dans les méandres encore floues de la cyber-sécurité, l’adoption d’un protocole HTTPS constitue une porte d’entrée, et même un prérequis quasiment obligatoire pour toute présence sécurisée en ligne.

QU’EST CE QUE LE HTTPS ?

Le protocole HTTP (Hyper Text Transfer Protocol) permet l’échange des données entre le navigateur utilisé par l’internaute et le serveur hébergeant le site internet. Pour faire simple, le HTTPS (Hyper Text Transfer Protocol Secure) est une version sécurisée du protocole HTTP, par l’ajout d’un protocole cryptée : le SSL (ou TLS dans sa version la plus récente). En pratique, l’action du protocole SSL crypte les échanges de données de l’utilisateur et évite leur récupération par un tiers malveillant.

Il existe une large échelle des degrés de cryptage SSL selon les besoins de protection.

La présence de ce cryptage est aisément identifiable : un protocole HTTPS dans l’URL, un cadenas accolé et un certificat SSL consultable par l’internaute (ces éléments pouvant varier selon le degré de protection adoptée).

Destiné à l’origine aux sites de e-commerce ou ceux traitant des données sensibles (banques, assurances, services publiques), le protocole HTTPS est aujourd’hui prisé par tous les sites corporate. Plusieurs facteurs sont à l’origine de cette amplification.

LES ATOUTS : SÉCURITÉ, CONFIANCE ET RÉFÉRENCEMENT

L’entrée en application du RGPD, à partir de mai 2018, renverse la responsabilité de la protection des données vers l’entreprise. A sa charge donc de « *garantir une sécurité appropriée (…) à l’aide de mesures techniques ou organisationnelles appropriées* » (article 5 alinéa 1/F).

La disposition implique indirectement l’adoption d’un protocole HTTPS pour l’ensemble des formulaires en ligne sur lesquels sont transmis des données à caractère personnelles. A noter que la CNIL recommande la mise en œuvre d’un protocole de cryptage TLS, le SSL risquant de devenir obsolète.

Dans le secteur des cabinets d’avocats et des experts comptable, la multiplication des formulaires (veille juridique, newsletter simulations…) implique le recours au HTTPS, afin d’être en conformité avec les dispositions du règlement européen.

Le HTTPS offre par ailleurs des bénéfices extra-sécuritaires. Les différentes études sur les habitudes de consommation des internautes démontrent qu’un site sans certificat SSL/TLS a un impact négatif sur l’utilisateur et, en conséquent, sur la marque.

Autre avantage, le recours au HTTPS influe sur le référencement du site concerné. D’une part, le navigateur Google Chrome prévient désormais (depuis le 17 octobre 2017) l’utilisateur lorsque celui-ci est sur un site non-sécurisé par un protocole HTTPS. À l’inverse, un site sécurisé profite naturellement d’un meilleur référencement sur le moteur de recherche, Google ayant adopté une politique incitative de migration vers le HTTPS.

LE JUSTE PRIX

Le certificat SSL, assorti au protocole HTTPS, est valide durant un an. Les prix et les prestataires sont extrêmement variés sur le marché. La fourchette de prix s’établit entre 20 et 1500 euros/an, avec une protection moyenne autour de 500 euros/an.

Il est important d’ajuster le niveau de sécurité à la sensibilité des données récoltées. Pour un site de cabinet d’avocat – sans possibilité de paiement en ligne ou d’échange de données ultra-sensibles – il n’est pas nécessaire d’opter pour une protection experte. Le cas des experts comptables est sensiblement différent avec l’émergence des plateformes automatisées, induisant une protection accrue.

S’il est nécessaire de mener une réflexion cohérente sur le degré de protection voulu, la migration vers un protocole HTTPS s’impose comme une nécessité pour tous les acteurs économiques en ligne.