DNS via HTTPS : Mozilla élargit le débat

Comment orchestrer la mise en place, dans Firefox, du DNS *via* HTTPS ? C'est le sujet d'une consultation publique qu'organise Mozilla. Les « parties intéressées » ont jusqu'au 4 janvier 2021 pour répondre. Parmi elles, les FAI.

Ces derniers sont nombreux à avoir fait part de leur inquiétude. Principal motif : le DoH (*DNS over HTTPS*) complique la mise en œuvre de leurs systèmes de filtrage. Aussi bien ceux à vocation commerciale (contrôle parental) que ceux implémentés pour se conformer aux lois (lutte contre le piratage, le terrorisme, la pédopornographie…).

Ces systèmes de filtrage reposent sur l'analyse des requêtes DNS. C'est-à-dire celles qui permettent de faire la correspondance entre les noms de domaines et les adresses IP associées.
Avec le DoH – spécification RFC 8484 -, l'ensemble de cette chaîne est chiffré : non seulement les requêtes, mais aussi les réponses des résolveurs DNS.

DNS *via* HTTPS : au mépris de la loi ?

La mise en place du protocole sur la version stable de Firefox est effective depuis deux ans. Mais elle n'est active par défaut qu'aux États-Unis, depuis février 2020.
La consultation publique vise à accompagner le déploiement dans d'autres zones géographiques. Mozilla cherche notamment à comprendre dans quelle mesure ses objectifs de protection de la vie privée et de la sécurité sont conciliables avec l'architecture technique d'Internet. Y compris les systèmes de filtrage.

Les considérations juridiques sont une part importante de la consultation. En particulier eu égard au programme TRR (Trusted Recursive Resolver). Mozilla constitue, par ce biais, un catalogue de fournisseurs DNS « alternatifs ». N'entrent dans ce cercle que ceux qui prennent des engagements sur la protection des données des utilisateurs. Entre autres, un délai de rétention qui ne dépasse pas 24 heures.

Un tel engagement entre en conflit avec des lois. Par exemple, au Royaume-Uni, l'Investigatory Powers Act. Le texte oblige les FAI à conserver pendant un an l'historique des sites que visitent leurs clients.

Dans ce contexte de tensions, Mozilla a fait des concessions. use-application-dns.net en est une illustration. Les administrateurs réseau peuvent exploiter ce domaine spécifique pour signaler la présence d'un résolveur DNS local qui implémente des fonctionnalités ne faisant pas bon ménage avec le DoH.

Photo d'illustration © chiqui – shutterstock.com