

Affaires 389.140 et 389.896

Note en délibéré

French Data Network
La Quadrature du Net
Fédération des fournisseurs d'accès à Internet associatifs

Le 2 février 2016

L'audience publique du 1er février sur les affaires 389140 et 389896 appelle de la part des exposants quelques observations faisant l'objet de cette note en délibéré. Si la présente note ne porte que sur deux points — le traitement de correspondances privées et de données personnelles — les exposants n'en maintiennent pas moins l'ensemble des moyens et conclusions développés dans leurs précédentes écritures.

Sur la notion et l'interception de correspondance privée. L'analyse faite par Mme le rapporteur public souffre de diverses lacunes.

D'une part, aux yeux du rapporteur public, la consultation d'une page Web ne saurait être assimilée à de la correspondance privée. Une telle analyse est entachée d'une erreur manifeste d'appréciation. En effet, le rapporteur public ne tient compte ni de la nature, ni du contenu de la multitude et de la grande diversité de pages Web existantes, ni de l'usage qui en est fait. Ainsi, l'utilisation d'outils de communication et plateformes grand public tel que *Gmail*, ou l'outil de discussion instantanée de *Facebook* (appelé *Messenger*), qui sont des pages Web, constituent indubitablement une correspondance privée.

Sur ce point, il est d'ailleurs à observer que l'article 34 du projet de loi pour une République numérique, tel qu'adopté en première lecture par l'Assemblée nationale, prévoit de modifier l'article L. 32-3 du code des postes et des communications électroniques pour y insérer un II disposant que : « Les personnes qui éditent un service de communication au public en ligne, au sens du deuxième alinéa du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, permettant à leurs utilisateurs d'échanger des correspondances, ainsi que les membres de leur personnel, respectent le secret de celles-ci. Le secret couvre le contenu de la correspondance, l'identité des correspondants ainsi que, le cas échéant, l'intitulé du message et les documents joints à la correspondance. »

Preuve en est qu'un service de communication au public en ligne peut aussi permettre l'échange de correspondances privées.

D'autre part, la redirection par nom de domaine, comme les exposants le précisait dans leurs précédents mémoires (*cf.* point II.4 des mémoires en

réplique), entraîne la redirection de tout ou partie du trafic de courrier électronique vers l'adresse mise en place par le ministère de l'intérieur. Cette redirection, qui n'est pas celle désignée par le législateur, relève bien de l'interception de correspondance privée, ou de la destruction de celle-ci, si les serveurs mis en place par le ministère de l'intérieur sont configurés pour ne pas recevoir de courrier électronique. La même analyse vaut, *mutatis mutandis*, pour l'ensemble des protocoles possibles pour de la correspondance (messagerie instantanée, par exemple).

Les éléments techniques détaillés par les exposants dans leurs précédents mémoires sur les effets du blocage par DNS sur la messagerie électronique en particulier, et sur les protocoles relevant de la correspondance privée en général, n'ont d'ailleurs pas été contestés par le ministère en défense. Si par extraordinaire, un doute devait persister dans l'esprit des membres de la formation de jugement sur le sérieux et la qualité des analyses des exposants, ces derniers l'invitent à avoir recours à une expertise sur ce point particulier conformément à l'article R. 621-1 du code de justice administrative.

Sur le traitement des données à caractère personnel. Quant à la nature des données collectées en premier lieu, les exposants ne peuvent qu'insister sur le caractère personnel des données transmises à la plateforme du gouvernement lors du blocage. Pour rappel, dès le 12 mars 2014 (*cf.* CE 12 mars 2014, *Société Pages Jaunes Groupe*, req. n° 353193, Rec. T. p. 663-669-778), votre juridiction considérait déjà que le collecte d'« adresses IP associées aux contenus, date et heure des requêtes effectuées » constituait un traitement de données à caractère personnel — or, il s'agit précisément des mêmes données dont nous dénonçons présentement la collecte par l'administration.

Le Conseil d'État alignait alors sa jurisprudence sur celle de la Cour de justice de l'Union européenne qui avait jugé, dans son arrêt *Scarlet* (*cf.* CJUE, 24 novembre 2011, *Scarlet c. SABAM*, affaire C-70/10, point 51), s'agissant « des adresses IP des utilisateurs », que « ces adresses [sont] des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs ».

À cet égard, tant votre jurisprudence que celle de la Cour de justice fut parfaitement suivie par celle de la CNIL qui, justement, prévenait dans son avis rendu quant aux dispositions attaquées que l'administration devrait se soumettre aux obligations de la loi du 6 janvier 1978 si elle entendait traiter les données auxquelles elle aurait accès via la technique de blocage, soulignant le caractère personnel de ces dernières.

Enfin, l'administration dispose de prérogatives lui permettant d'associer directement ces données — et particulièrement l'adresse IP — aux personnes qu'elles concernent en s'en enquérant auprès des opérateurs de télécommunications, et ce même sans l'autorisation d'un juge (voir le livre VIII du code de la sécurité intérieure). Dès lors, ces données sont, en l'espèce, particulièrement identifiantes — et tel est le critère permettant d'établir le caractère personnel des données en cause.

De plus, quand bien même l'administration ne s'enquerrait pas auprès

des opérateurs de l'identité des abonnés, les données collectées resteraient, ensemble, suffisamment uniques pour individualiser les personnes qu'elles concernent et, ainsi, revêtir un caractère personnel (tel que démontré au point I.2 du mémoire en réplique des exposants).

Quant à l'existence d'un traitement en second lieu, les exposants rappellent que, bien qu'il se défende de les « exploiter », le ministère de l'intérieur a reconnu qu'il « enregistre » ces données. Il fait même usage des adresses IP ainsi collectées puisqu'elles lui permettent de dresser des statistiques relatives au nombre de tentatives de consultation des sites bloqués¹. Or, aux termes de l'article 2, alinéa 3, de la loi du 6 janvier 1978, « constitue un traitement de données à caractère personnel [...] notamment *la collecte* » de telles données.

1. Voir la réponse du gouvernement, en date du 22 décembre 2015, à la question parlementaire n° 74166 de M. Lionel Tardy : « L'adresse IP est enregistrée. Les adresses IP ainsi collectées ne sont pas exploitées mais permettent une comptabilisation précise du nombre de connexions à chacune des pages bloquées. Les premiers chiffres enregistrés depuis la mise en place du dispositif font apparaître plus de 30 000 connexions par semaine concernant les sites de pédo-pornographie, et 250 connexions en moyenne par semaine concernant les sites à caractère terroriste ». Disponible à l'adresse : <http://questions.assemblee-nationale.fr/q14/14-74166QE.htm>.