Snobée sur l'antiterrorisme, la CNIL met en garde le gouvernement sur le chiffrement

Ignorée. Dans une série « d'observations » publiées sur son site, la CNIL s'étonne d'avoir purement et simplement été tenue à l'écart du projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, le énième du genre présenté le 21 juin dernier en Conseil des ministres. Un texte renfermant des mesures qui « *conduisent à l'élargissement des cas de collecte et d'exploitation des données personnelles* », selon la CNIL. Une façon pour la Commission d'affirmer qu'elle aurait dû être consultée au préalable, comme le prévoit d'ailleurs la loi pour une République numérique, d'octobre dernier, qui avait élargi les cas de consultation de la CNIL à toute règle nouvelle portant sur le traitement des données personnelles.

Un domaine dans lequel le texte du gouvernement d'Edouard Philippe fait plus que s'aventurer. Avec des mesures touchant notamment aux données d'enregistrement et de réservation des passagers aériens (PNR, Passenger Name Record), au placement sous surveillance électronique ou à l'interception et à l'exploitation des communications électroniques par voie hertzienne.

PNR : l'expérimentation européenne entérinée

Ce qui conduit la Commission à émettre un certain nombre d'observations sur le fond. La CNIL s'étonne par exemple que le champ et les finalités de la mesure portant sur l'obligation de déclaration des numéros d'abonnement et identifiants d'usagers dans le cadre du renseignement antiterroriste soient si flous. « *La Commission relève que cette obligation est susceptible de concerner un champ très large de services de communication, tels que la téléphonie fixe ou mobile, la transmission vocale sur Internet, les SMS, les courriels, les messageries instantanées, etc. Ce champ n'est pas précisé ni limité par le projet de loi. Le texte ne prévoit pas davantage les finalités et les conditions d'utilisation de ces numéros et identifiants* », écrit la CNIL, qui demande des clarifications permettant de garantir la proportionnalité de ces mesures.

Autre sujet de fâcherie : le PNR, ce fichier répertoriant les déplacements des individus via les transports aériens (le projet de loi prévoyant d'ailleurs des extensions au domaine maritime). Un traitement de données instauré à titre « *expérimental* » par une directive européenne que le texte de Gérard Collomb, le ministre de l'Intérieur, pérennise sans autre forme de procès, selon l'analyse de la CNIL. « *Le traitement mis en œuvre au niveau national est en outre plus étendu que ce que prévoit la directive, dans la mesure où il peut être utilisé, par les services de renseignement, à des fins de prévention des atteintes aux intérêts fondamentaux de la nation* », ajoute l'organisme.

Contrôler les fichiers de renseignement

Voyant ses prérogatives foulées au pied par le gouvernement, la CNIL envoie un message à l'exécutif. Ce dernier trouvera dans l'organisme dirigé par Isabelle Falque-Pierrotin un aiguillon sur deux sujets : le contrôle des fichiers de renseignement et l'affaiblissement éventuel du chiffrement. Sur le premier point, la Commission pointe une contradiction actuelle. En effet, si les fichiers de

renseignement, largement dopés ces derniers mois et années par les nouvelles possibilités de collecte de données offertes par les législations successives, restent soumis à la loi Informatique et Libertés, aucun organisme de contrôle externe n'est chargé de vérifier le respect de ces principes. « *Prévoir un tel contrôle est une garantie qu'appelle l'Etat de droit* », écrit la CNIL.

Chiffrement : la tentation des backdoors

Sur le chiffrement, la Commission estime que les mesures spécifiques déjà en place forment un socle suffisant, assurant un équilibre entre sécurité et respect des données personnelles. « *L'ensemble des outils susceptibles d'être mobilisés pour accéder à des données chiffrées ou contourner les dispositifs de chiffrement, qui ne peuvent être mis en œuvre que dans certaines conditions précises, forment un arsenal juridique solide* », estime la CNIL, qui avertit le gouvernement du « *risque collectif* » que feraient peser des mesures plus radicales. Comme la mise en place de backdoors, la création des clefs maîtres ou l'interdiction, pour le grand public, d'utiliser librement les technologies de chiffrement.

Des tentations bien présentes à qui refont surface après chaque attentat. Mi-juin encore, Londres et Paris annonçaient, à l'occasion de la visite de la Première ministre britannique en France, un plan d'action commun pour lutter contre l'utilisation de l'Internet à des fins terroristes. Au menu notamment : la possibilité pour les forces de l'ordre d'accéder aux contenus chiffrés… sans avoir recours à des backdoors. Les deux capitales n'avaient toutefois donné aucune indication sur la façon dont cet accès privilégié des services de sécurité pourrait être aménagé… sans affaiblir la sécurité de l'ensemble, donc des échanges électroniques aujourd'hui au cœur de notre économie.

A lire aussi :

Steve Kremer, Inria : « affaiblir le chiffrement, c'est grotesque »

Europe : vers un marché unique… de la réquisition de données

Chiffrement : Emmanuel Macron marche en rond

Crédit photo : ©-kebox-Fotolia.com