Prédiction, chiffrement et libertés

Description

À l'ère de la lutte contre le terrorisme, cet avis du CNNum pose la question des atteintes à la vie privée qui seraient acceptables au nom de la sécurité nationale et de la protection des personnes. Et il répond qu'il serait contre-productif et même dangereux d'autoriser les pouvoirs publics à espionner davantage les activités numériques de la population. Par conséquent, rien ne saurait justifier d'obliger les services et applications qui chiffrent les données de bout en bout à donner leurs clés aux pouvoirs publics. Alors que, tant au niveau national qu'au niveau de l'Union européenne, les législateurs sont particulièrement soucieux d'encadrer les services de communication électronique cryptés, le sujet est plus sensible que jamais. Il met aux prises une liberté et une sécurité qui semblent inconciliables et il n'est pas certain qu'une bonne réponse existe. Pour le dire de façon très directe, mais pas nécessairement caricaturale : soit un État « Big Brother » portera des atteintes excessives au secret des communications privées, soit des attentats qui auraient pu être empêchés ne le seront pas. Le CNNum fait le choix de dénoncer la « *trajectoire sécuritaire préoccupante* » des pouvoirs publics et de soutenir le chiffrement des services.

Le CNNum s'était autosaisi, durant l'été 2016, d'un sujet délicat : le chiffrement des communications électroniques, technologie permettant de coder les informations afin qu'elles ne soient visibles que de leurs expéditeurs et destinataires. Cette autosaisine faisait suite à l'annonce commune par les ministres de l'intérieur français et allemand du renforcement substantiel des moyens (technologiques et juridiques) permettant de déchiffrer les communications électroniques. Ces dernières sont en effet de plus en plus exploitées afin de développer et d'organiser des cellules terroristes. Un an plus tard, tandis que des attaques terroristes continuent de se produire à intervalles réguliers, la question du chiffrement est toujours sur la table. Elle suscite de vifs débats entre, d'une part, les défenseurs d'un État et d'une police forts et protecteurs et, d'autre part, les défenseurs des libertés individuelles, de la vie privée et des données personnelles.

Dans son avis remis le 12 septembre 2017, le CNNum précise sa position sur le chiffrement et élargit sa réflexion à la protection des droits et libertés sur internet. Selon lui, il serait malvenu de soumettre à davantage de contraintes les services de communication cryptés tels que Whatsapp, Viber, iMessage ou surtout Telegram. Le chiffrement serait ainsi, selon le CNNum, un « *rempart contre la surveillance de masse* » et « *l'arbitraire des États* ».

L'innovation technologique n'est en soi ni bonne ni mauvaise, elle permet à la fois aux malfaiteurs de fomenter plus aisément leurs actes et aux services de police d'identifier et de surveiller les éventuels criminels. Or, le droit, selon qu'il sera permissif ou contraignant, pourrait faire en sorte que les nouvelles technologies de communication profitent aux uns plus qu'aux autres. C'est cette délicate problématique qui

a récemment préoccupé le CNNum, autorité consultative chargée d'éclairer les pouvoirs publics sur les questions touchant aux nouvelles technologies de l'information et de la communication.

Le gouvernement français souhaite accéder aux clés de chiffrement des services de communication grand public afin de faciliter le travail d'investigation numérique des policiers et des services de renseignement. Pour les défenseurs des droits et libertés sur l'internet, au côté desquels le CNNum se place, une dérive sécuritaire serait à redouter. Les pouvoirs publics pourraient être tentés de généraliser la surveillance, donc de recourir à une surveillance de masse, ce qui susciterait une défiance des utilisateurs vis-à-vis des outils numériques qui, entre autres conséquences, ne profiterait guère aux acteurs du *e-commerce*.

C'est pourquoi, durant l'été 2016, dans une tribune signée notamment par Isabelle Falque-Pierrotin, présidente de la CNIL, et Mounir Mahjoubi, ancien président du CNNum devenu aujourd'hui secrétaire d'État chargé du numérique, les autorités ont été invitées à éviter les « *solutions de facilité* » aux potentielles « *conséquences graves et non anticipées* ». À travers son avis du 12 septembre 2017, le CNNum prolonge ce raisonnement. Sans surprise, l'instance consultative défend le « *droit au chiffrement* » des nouveaux services de communication électronique. Elle juge que l'affaiblissement, même pour des raisons légitimes, de ce qui fait l'essence du chiffrement (le secret des échanges qu'il garantit) aurait des répercussions fortes sur l'écosystème de l'internet. Celui-ci repose en effet sur une confiance que le chiffrement des données permet de conforter.

Alors que le projet de loi antiterroriste destiné à remplacer l'état d'urgence est examiné à l'Assemblée nationale, le CNNum qualifie le chiffrement des données d' « *élément vital de notre sécurité en ligne* ». Aussi en vient-il à regretter que « *les pouvoirs publics semblent engagés dans une spirale infernale* ». Et d'ajouter : « *L'affaiblissement des moyens de chiffrement, aujourd'hui largement diffusés dans les services grand public, aurait sans aucun doute une efficacité très limitée sur l'infime minorité d'utilisateurs qui les utilisent pour cacher des desseins criminels. En effet, le développement de logiciels non contrôlables, faciles à distribuer et offrant un niveau de sécurité très élevé est à la portée de n'importe quelle organisation criminelle* ». Le CNNum met ainsi l'accent sur le fait qu' « *il n'existe pas de technique d'affaiblissement systémique du chiffrement qui ne permettrait de viser que les activités criminelles. Limiter le chiffrement pour le grand public reviendrait alors à en accorder le monopole aux organisations qui sauront en abuser* ». Par conséquent, il faudrait abandonner purement et simplement l'idée de contrôler les systèmes de chiffrement.

Cependant, à l'aune des profils des djihadistes ayant perpétré les récents attentats et des groupuscules auxquels ils appartenaient, au vu du faible niveau d'organisation et du haut niveau d'improvisation qui étaient les leurs, on peut mettre en doute des explications selon lesquelles « *interdire le chiffrement n'aurait aucun sens [car] toutes les techniques de chiffrement sont dans le domaine public et n'importe quel groupe serait capable de recréer ses propres applications chiffrées s'il le voulait* ». Mais le Conseil fait aussi observer combien l'élément déclencheur de la radicalisation des djihadistes serait essentiellement le contact humain, *i.e.* hors ligne, physique. Il cite un rapport de l'Unité de coordination de la lutte antiterroriste (UCLAT) selon lequel le facteur décisif serait dans 95 % des cas un contact humain.

Les États sont tentés d'obliger les constructeurs et fournisseurs de services numériques à introduire des « portes dérobées » dans leurs systèmes (des *backdoors* : accès aux applications de chiffrement dont seuls les pouvoirs publics détiendraient les clés). Or, rappelle le CNNum, diverses cyberattaques, dans l'actualité récente, ont attesté du risque que fait courir le maintien volontaire de failles de sécurité. N'importe quelle puissance étrangère ou groupe de pirates informatiques pourrait potentiellement identifier cette faille et l'exploiter à des fins dramatiques pour le service concerné et pour ses utilisateurs.

Par ailleurs, le Conseil note que si le chiffrement permet de se préserver du regard intrusif des États, il permet aussi de se préserver du regard intrusif des acteurs économiques, notamment des GAFA. Ceux-ci ont bien compris que les informations personnelles sont le pétrole du xxi^{e} siècle et que, par voie de conséquence, les nouveaux modèles économiques dépendent de la bonne connaissance des vies, des habitudes et des centres d'intérêt des utilisateurs des services. Ainsi le CNNum, plutôt que de prôner la limitation ou l'encadrement du chiffrement, soutient une « *promotion massive auprès du public, des acteurs économiques et des administrations* ». Pour les entreprises, le chiffrement « *reste le meilleur rempart contre l'espionnage économique* », tandis que pour l'État, « *il s'agit d'une condition de sa souveraineté* ».

Prédiction, chiffrement et libertés, avis du Conseil national du numérique, septembre 2017

Categorie

1. A lire en ligne

date créée
28 février 2018
Auteur
borisbarraud