Les crypto-wars: le chiffrement dans le viseur du gouvernement français

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE VENDREDI 29 AVRIL 2016

Jeu de câbles de la société Cellebrite, destinés à la récupération des données de différents téléphones. © Reuters.

Bernard Cazeneuve, Jean-Jacques Urvoas et Manuel Valls © Reuters

Bernard Cazeneuve, Jean-Jacques Urvoas et Manuel Valls © Reuters

Depuis quelques mois, plusieurs responsables politiques dénoncent l'usage du chiffrement, qui bloquerait le travail de la justice, et réclament l'installation de *« backdoors »*, de portes dérobées, dans les logiciels. Il s'en est fallu de peu que cette mesure soit votée lors du passage du projet de loi sur la réforme pénale à l'Assemblée. Mais le débat ne fait que débuter. La CNIL met en garde contre des mesures qui pourraient remettre en cause *« un élément vital de notre sécurité »*.

Le directeur de la NSA l'a affirmé : les attaques de Paris *« ne seraient pas arrivées »* sans le chiffrement. *« Certaines communications »* des terroristes étaient *« chiffrées »*, a expliqué **le 18 février dernier Michael Rogers**, empêchant ainsi de les détecter *« en amont »*. Le patron de l'agence de renseignement américaine n'a pas donné plus de détails. Mais ses propos ont eu un fort retentissement en France où, depuis quelques mois, le débat sur le chiffrement fait rage.

Cela fait en réalité longtemps que le chiffrement est dans le viseur des autorités et qu'un tour de vis sur cette technologie est annoncé. Lors des discussions sur le projet de loi renseignement en début d'année 2015, le ministère de l'intérieur évoquait déjà, officieusement, le chiffrement comme son prochain chantier. Au mois d'août, le procureur de Paris, François Molins, cosignait, avec trois homologues américain, britannique et espagnol, **une tribune** publiée dans le *New York Times* intitulée *« Quand le chiffrement des téléphones bloque la justice »*. Le 2 septembre, le magistrat récidivait dans **une interview à *L'Express***, où il affirmait qu'il était devenu impossible de déverrouiller *« les nouvelles générations de mobiles »*. François Molins cite même un cas précis, un téléphone retrouvé dans le cadre de l'enquête sur Sid Ahmed Ghlam, assassin présumé d'Aurélie Châtelain et suspecté d'avoir préparé un attentat contre une église à Villejuif.

Les attaques du 13-Novembre à Paris et la tuerie de San Bernardino, aux États-Unis, en décembre 2015, n'ont fait qu'enflammer le débat. En janvier 2016, la députée Les Républicains Nathalie Kosciusko-Morizet **déposait un amendement** au projet de loi numérique alors en cours d'examen, visant à imposer aux fabricants de logiciels de chiffrement la solution miracle, et au cœur de la polémique : les « *backdoors* », des portes dérobées. Cette pratique consiste à installer volontairement une vulnérabilité secrète dans un système pour pouvoir ensuite l'exploiter à son seul profit. Le problème, dénoncent ses opposants, est justement que ces vulnérabilités restent rarement « secrètes » et conduisent à une remise en cause globale de la sécurité.

Bernard Cazeneuve, Jean-Jacques Urvoas et Manuel Valls © Reuters

L'amendement de Nathalie Kosciusko-Morizet avait été **rejeté par le gouvernement**. Mais comme elle l'expliquait dans son exposé des motifs, le but était avant tout *« d'ouvrir le débat sur les voies et les moyens de garantir l'accès aux données pour des raisons de sécurité nationale et dans le cadre d'une enquête judiciaire »*. Et celui-ci ne faisait effectivement que débuter. Le chiffrement a notamment été au cœur des débats sur le nouveau **projet de loi de réforme pénale** déposé à l'Assemblée le 3 février.

Le texte, actuellement en commission mixte paritaire après avoir été voté en termes différents par les députés et les sénateurs, prévoit déjà un durcissement des sanctions en cas de refus de donner une clef de chiffrement. Actuellement, **l'article 434-15-2 du code pénal** punit en effet de trois ans de prison et 45 000 euros d'amende le fait de ne pas remettre une clef de déchiffrement réclamée dans le cadre d'une enquête. La peine est portée à cinq ans de prison

et 70 000 euros d'amende lorsque le déchiffrement *«aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets»*. Le projet de loi prévoit de porter cette dernière amende à 150 000 euros. **L'article 60-1 du code de procédure pénale** permet quant à lui au procureur *« de requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique »* la remise de clefs de déchiffrement. En cas de refus, la peine est de 3 700 euros d'amende. Le projet de loi prévoit de la porter à 15 000 euros lorsque le refus émane d'une personne morale, *« tel un constructeur d'appareils ou un prestataire de services»*.

Lors des débats à l'Assemblée nationale, plusieurs députés, notamment le socialiste Yann Galut et le républicain (LR) Éric Ciotti, ont déposé des amendements visant à porter l'amende qui frappe les constructeurs récalcitrants jusqu'à respectivement 1 et 2 millions d'euros, ou encore à tout simplement interdire la commercialisation de leur produit. Ces mesures seront quasiment toutes écartées, l'amendement d'Éric Ciotti étant rejeté d'une seule voix. Mais un amendement, présenté par Philippe Goujon (LR), a été adopté contre l'avis du gouvernement. Il prévoit de sanctionner le refus des sociétés d'une peine maximale de 5 ans de prison et 350 000 euros d'amende.

Selon nos informations, il s'en est fallu de peu pour que le tour de vis soit bien plus sévère. Au sein du gouvernement, tous n'étaient pas opposés aux différents amendements déposés par les députés. Bernard Cazeneuve et le ministre de la justice, Jean-Jacques Urvoas, ont ainsi demandé à aller plus loin que l'amendement Goujon, en instaurant des sanctions qui auraient contraint les fabricants à installer des *backdoors*. Selon une source gouvernementale, plusieurs membres du gouvernement, dont la secrétaire d'État au numérique Axelle Lemaire, se sont opposés au ministre de l'intérieur et au garde des Sceaux. Et ils auraient finalement obtenu gain de cause lors d'un arbitrage du premier ministre, Manuel Valls.

Lors de l'examen du texte en séance publique, **le jeudi 3 mars**, les débats ont été l'occasion de violentes charges contre le chiffrement, soutenues par le ministre de la justice Jean-Jacques Urvoas. Le garde des Sceaux a annoncé à cette occasion avoir déjà entamé un processus de discussions internationales au sein de l'Union européenne et avec les Américains. *« Nous avons dépassé le stade de la réflexion pour aborder celui des modes opératoires*, affirme Jean-Jacques Urvoas. *Je n'ai aucun doute sur nos chances de réussite, d'autant plus que le Parlement, en particulier l'Assemblée nationale, nous aiguillonne. Avec cette épée dans nos reins, nous irons encore plus vite puisque nous partageons la même ambition et la même motivation. »*

La question des *backdoors*, voire d'une interdiction partielle du chiffrement, va très vite revenir sur la table. Et la discussion s'annonce d'emblée animée. Car face aux tentations sécuritaires, les opposants ne manquent pas. Ceux-ci ont d'ailleurs reçu, fin mars, un soutien inattendu de la part de l'armée. Le 28 mars, ***Le Parisien*** **révélait** le contenu d'une note classifiée du Secrétariat général de la défense et de la sécurité nationale (SGDSN), qui dépend du premier ministre, s'inquiétant du débat actuel et demandant la suppression de l'amendement de Philippe Goujon. Encore une fois, l'argument avancé par le SGDSN est qu'il est impossible d'introduire des *backdoors* sans affaiblir l'ensemble de la sécurité informatique. *« Créer une telle faille reviendrait, selon cette note, à faciliter les attaques informatiques susceptibles de nuire à la sécurité nationale et à la compétitivité des entreprises françaises, qui seraient plus exposées à l'espionnage informatique »*, résume *Le Parisien*.

Une analyse partagée par la Commission nationale de l'informatique et des libertés (CNIL). En présentant son bilan annuel, le vendredi 8 avril, la commission a tenu à faire **du chiffrement un des « enjeux de 2016 »**, et ainsi à faire passer quelques messages. Un dispositif de *backdoors« créerait un risque collectif tendant à affaiblir le niveau de sécurité des personnes face à l'ampleur du phénomène cybercriminel »*,

affirme la CNIL. Par ailleurs, *« il serait très complexe à mettre en œuvre, de manière sûre, alors que les applications sont globalisées et mondialisées »*.

Plus globalement, la commission reconnaît le chiffrement comme un *« élément vital »* de la vie numérique. *« Dans un contexte de numérisation croissante de nos sociétés et d'accroissement exponentiel des cybermenaces, le chiffrement est un élément vital de notre sécurité »*, explique-t-elle. *« Il contribue aussi à la robustesse de notre économie numérique et de ses particules élémentaires que sont les données personnelles. »« Protéger les données personnelles dans l'univers numérique, à l'aide notamment du chiffrement*, poursuit la commission, *c'est aussi protéger un droit fondamental et, au-delà, l'exercice des libertés individuelles dans cet univers. »*

Cette prise de position forte en faveur du chiffrement est accompagnée de quelques mises en garde. La CNIL s'y oppose aux appels lancés pour un durcissement de la législation et rappelle que le droit existant prévoit déjà des mesures permettant d'obtenir *« la remise des clés de déchiffrement, s'agissant des personnes mises en cause ou des tiers tels que les prestataires de services de cryptographie s'ils ont connaissance de la convention secrète de déchiffrement »*.

La CNIL rappelle au passage au législateur les larges pouvoirs dont dispose la police pour obtenir tout type de données ou informations, pouvoirs fortement renforcés par les différents projets de loi sécuritaires adoptés ces dernières années : *« [...] les réquisitions numériques, l'accès aux données de connexion, les interceptions de correspondances, les enregistrements audiovisuels, la captation de données informatiques affichées à l'écran ou introduites au clavier, ou encore le recours à des experts techniques dans le cas de données chiffrées. »*

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.