Le chiffrement des données

publié le **20/04/2016**, vu **2739 fois**, Auteur : Noé MARMONIER Avocat

Le chiffrement des données est au coeur de l'actualité, avec le bras de fer qui se poursuit entre Apple et le FBI. Si le débat est apparu Outre-Atlantique, il n'est pas sans poser en droit français de véritables questionnements juridiques, à l'heure ou la CNIL vient d'adouber un tel procédé. Décryptage.

Secret des affaires, chiffrement des données, meme combat !

Le chiffrement des données autant loué que décrié constitue un puissant mécanisme de lutte contre la cybercriminalité et de protection de la vie privée et des données personnelles.

Mais de quoi parlons-nous ? Qu'est ce que le chiffrement ?

Le chiffrement est un procédé de cryptographie, qui vise à rendre impossible la lecture d'un document ou l'accès à un ordinateur ou un smartphone, pour celui qui n'est pas détenteur de la clé de déchiffrement.

Les données à protéger ou à ne pas divulguer sont codées par l'intermédiaire d'un algorithme spécifiquement défini.

Le procédé est donc particulièrement simple en soit, et n'a rien d'illégal.

Quelle utilisation du chiffrement ?

Le chiffrement présente une utilité certaine pour les entreprises innovantes, permettant de sécuriser l'accès à des données confidentielles. C'est un mécanisme pertinent pour les entreprises afin de protéger les secrets industriels et commerciaux qu'elles détiennent.

A ce titre, le chiffrement est une véritable solution contre l'espionnage industriel, et le vol de données confidentielles suite à un piratage informatique.

Le chiffrement est pleinement autorisé, il n'est interdit par aucun texte.

Il est d'ailleurs recommandé pour les entreprises par plusieurs institutions, la DGSI et l'ANSSI (Agence de sécurité des systèmes d'information), et meme pour les particuliers, par la CNIL.

La CNIL a adoptée le 07 avril 2016 une position dans laquelle le chiffrement est approuvé, en ce qu'il est de nature à protéger la vie privée et les données personnelles, élevé au rang de " *composant essentiel pour la sécurité informatique*".

La face cachée du chiffrement est apparue avec l'attaque d'un centre social américain, ou le terroriste détenait un Iphone chiffré, et amplifié par les attentats du 13 novembre ou la NSA a récemment révélé que certaines données échangées entre les auteurs des attaques étaient chiffrées.

Les services de police se plaignent des freins apportés aux enquetes par le chiffrement des données, rendant inexploitable la mine d'informations que représente un smartphone ou un ordinateur.

Quatre autorités judiciaires (*le procureur de la République de Paris, le procureur de Manhattan, le préfet de police de Londres et le Président de la Haute cour de justice espagnole*) ont notamment signé une tribune commune dans le New York Times, accuseant Apple et Google d'avoir instauré un système de chiffrement de leurs appareils, empechant ainsi l'accès pour les enqueteurs, dans le cadre notamment de la lutte contre le terrorisme.

La lutte contre le chiffrement s'organise au nom de la lutte contre le terrorisme : la création "des portes dérobées" :

L'argument de la lutte contre le terrorisme fait mouche pour limiter l'utilisation du chiffrement.

Les moyens d'investigations pour contourner - en partie - une telle difficulté existent déjà et sont pleinement opérationnels en procédure pénale, en enquete comme en instruction :

réquisitions aux opérateurs de téléphonie, écoutes téléphoniques, captation de données à distances, et bientot les IMSI Catcher, mini antenne relais portative dissimulée qui capte et enregistre toutes les données voix, textes émises ou reçues sur un téléphone dans un rayon déterminé, que se verront bientot dotés les enqueteurs, une fois le projet de loi sur la réforme de la procédure pénale bientot adopté.

Face à cette inquitéude des services de police, la réaction ne s'est pas faite attendre, le projet de loi relatif à la lutte contre le terrorisme et la criminalité organisée renforce le montant de l'amende pour celui qui ne collabore pas suffisamment avec les autorités : la limite au chiffrement est bien née.

Les appels en faveur de la création de "portes dérobées" sont de plus en plus pressant, visant à instaurant un moyen technique et juridique de rendre caduc le chiffrement des données pour les nécessités d'une enquete.

A l'image de certaines exceptions comme la copie privée que l'on retrouve en droit de la propriété littéraire et artistique, une exception judiciaire pourrait aisni voir le jour !

L'ANSSI comme la CNIL ont recusés l'instauration de "portes dérobées".

Outre la justification relative à la lutte contre le terrorisme, qui se légitime, une utilisation dévoyée de telles "portes dérobées" vient finalement apporter l'occasion "*d'affaiblir le niveau de sécurité des données personnelles des personnes face à l'ampleur du phénomène cybercriminel*", comme l'affirme justement la CNIL.

Tout est dit !

Le curseur respect de la vie privée/ sécurité n'en a pas terminé d'osciller.

La vigilance ne peut qu'etre nécessaire face à la restriction du chiffrement, qui constitue une protection non de trop dans une société très exposée à la cybercriminalité.