De la dépêche secrète aux Crypto Wars (brève histoire politique du chiffrement)

Félix Tréguer – CERI Sciences Po.

Ce texte a été publié dans le numéro 365 de La Chronique, *le magazine d'Amnesty International (avril 2017).*

L'acuité des débats contemporains autour du droit au chiffrement de nos communications et données numériques pourrait faire oublier qu'il renvoie en réalité d'un droit ancien. Il est en effet indéfectiblement lié au secret des correspondances, lui-même protégé depuis le milieu du XVIIIème siècle. Quant à la cryptologie – la « science du secret » –, elle est un art plus ancien encore. Et contrairement aux idées reçues, il semble qu'elle ait de tout temps fait l'objet d'usages triviaux et populaires. Certes, ces derniers furent longtemps marginaux, puisque l'écriture fut pendant longtemps essentiellement réservée aux élites. Mais l'un des plus vieux documents connus adoptant un système de codage est une tablette en argile datant de l'Antiquité retrouvée en Irak, dans laquelle le potier avait dissimulé ses techniques de fabrication en jouant sur les consonnes.

À partir du XVIème siècle, le développement concomitant de l'imprimerie et des postes aboutit à la prolifération de traités sur l'art du chiffrement, non seulement pour les empereurs, espions et diplomates, mais aussi pour les commerçants et hommes d'affaires, pour les savants ou même pour les correspondances intimes, avec la volonté d'échapper aux « cabinets noirs » chargés de la surveillance royale, ou plus simplement aux regards indélicats. Il est aussi, déjà, un outil prisé des dissidents politiques. On sait par exemple que les « pères fondateurs » des États-Unis comme Benjamin Franklin, James Madison ou Thomas Jefferson codaient leurs correspondances. C'est d'ailleurs dans un courrier partiellement codé que, le 27 mai 1789, Madison exposera à Jefferson son idée d'ajouter un *Bill of Rights* à la constitution américaine.

C'est avec l'arrivée de la télégraphie, et l'ouverture progressive de son utilisation au grand public dans la seconde moitié du XIXème siècle, que la cryptographie commence réellement à se démocratiser. Pour les usagers du télégraphe, il s'agit notamment de protéger son intimité vis-à-vis des techniciens chargés de la transmission des messages. Que dit alors la loi ? En France, ce qu'on appelle alors les « dépêches secrètes » (ou « inintelligibles ») sont autorisées, à condition d'être rédigées en signes romains ou en chiffres arabes. Ces codes sont supposés être facilement déchiffrables. Surtout, les bureaux gardent trace de toute communication – ce qu'on appellerait aujourd'hui les « métadonnées ». Un directeur des transmissions télégraphiques à Versailles loue ainsi, dans un écrit de 1870, la contribution du télégraphe à l'ordre public : « la télégraphie réalise pour la sécurité publique l'idéal de M. Vidocq, de terrible mémoire ».

À partir des années 1970, avec l'arrivée des premiers réseaux informatiques, la tension entre confidentialité et surveillance des communications monte d'un cran. À l'époque, la NSA lance un

appel à projet pour le développement d'un standard en matière de chiffrement, qu'elle cherchera délibérément à affaiblir pour être en mesure de casser plus facilement les codes. Cet épisode suscite alors l'intérêt de chercheurs en mathématiques qui, au gré de leurs travaux, vont sortir la cryptographie moderne de son giron militaire et poser les bases théoriques de sa démocratisation à l'ère numérique.

Le génie est sorti de sa bouteille. À la toute fin des années 1980, au sein de la mouvance des « Cypherpunks », des militants passionnés d'informatique font de la cryptographie un art ouvertement contestataire. Elle n'est plus seulement un moyen de déjouer la surveillance du peuple par les États, mais aussi l'outil par lequel il devient possible de systématiser les fuites de documents classifiés, et donc d'opérer une remise en cause radicale des secrets d'État. La *mailing list* éponyme des Cypherpunks sera d'ailleurs l'une des matrices intellectuelles du jeune Julian Assange, au début des années 1990.

Alors qu'Internet est en passe de se démocratiser, les agences de renseignement et de police tentent toutefois de préserver leur mainmise sur ces techniques, déclenchant un conflit politique et juridique resté dans les mémoires comme la première « *Crypto War* ». En 1993, le *New York Times* révèle ainsi que la NSA veut s'octroyer la capacité de lire l'ensemble des données et communications informatiques, au travers d'une puce de chiffrement dotée d'une porte dérobée. Aux États-Unis tout comme en France, le droit est également mobilisé pour empêcher la diffusion sur les réseaux de logiciels de chiffrement, au travers du régime applicable à l'exportation des « biens à double usage » (aux applications à la fois civiles et militaires). C'est grâce à la mobilisation des premiers mouvements de défense des libertés publiques dans l'environnement numérique – mais aussi en raison de l'influence du secteur privé qui a besoin du chiffrement pour développer le commerce électronique – que ces projets seront tenus en échec. Le droit applicable sera d'ailleurs progressivement libéralisé dans la deuxième moitié des années 1990.

Pourtant, en dépit de ces avancées juridiques, la problématique du chiffrement est longtemps restée l'apanage d'une poignée d'experts. Il a fallu les révélations d'Edward Snowden pour que s'opère une véritable prise de conscience quant à l'importance de ces pratiques. Depuis 2013, de nombreux déploiements techniques ont en effet permis de démocratiser l'exercice de ce droit essentiel à la défense de la vie privée et de la liberté de communication. Un droit aujourd'hui menacé par ceux de nos gouvernants qui voudraient continuer de se livrer à une surveillance massive d'Internet.