Les anciens Léviathans I – Le contrat social fait 128 bits… ou plus

Qu'est-ce qui fait courir Framasoft ? De la campagne Dégooglisons à l'initiative C.H.A.T.O.N.S quelles idées ont en tête les acteurs et soutiens de l'association ? Vous reprendrez bien une tranche de Léviathan ?

Pour vous inviter à aller au-delà des apparences (la sympathique petite tribu d'amateurs gaulois qui veut modestement mettre son grain de sable dans la loi des entreprises hégémoniques) nous vous proposons non seulement un moment de réflexion, mais pour une fois une série de considérations nourries, argumentées et documentées sur l'état de bascule que nous vivons et dans lequel nous prétendons inscrire notre action avec vous.

Jamais le logiciel libre et les valeurs qu'il porte n'ont été autant à la croisée des chemins, car il ne s'agit pas de proposer seulement des alternatives techniques, c'est un défi économique et politique qu'il doit relever.

Entre les États qui nous surveillent et les GAFAM qui nous monétisent, jamais le refuge du secret, celui de l'intime, n'a été aussi attaqué ni menacé. Pour représenter le monstre à plusieurs têtes, **Christophe Masutti** qui est l'auteur de cette série de réflexions, a choisi la figure emblématique du Léviathan, forgée déjà par Hobbes en particulier pour désigner l'État toujours plus avide de domination.

C'est donc une série de *Léviathans* nouveaux et anciens que nous vous invitons à découvrir par étapes, tout au long de cette semaine, qui vous conduiront peut-être à comprendre et adopter notre démarche. Car une fois établies les sources du

mal et posé le diagnostic, que faire ? Les perspectives que nous proposons seront peut-être les vôtres.

Note de l'auteur :
Chiffrer nos données est un acte censé protéger nos vies privées. Dans le contexte de la surveillance massive de nos communications, il devient une nécessité.

Mais peut-on mettre en balance la notion de vie privée et la paix entre tous que le contrat social est censé nous garantir ? Le prétendu choix entre liberté et sécurité tendrait à montrer que le pouvoir de l'État ne souffre aucune option. Et pourtant, les anciennes conceptions ont la vie dure.

Quand Manuel Valls s'exprime

Dans un article de RUE 89, le journaliste Andréa Fradin revenait sur une allocution du premier ministre M. Valls, tenue le 16 octobre 2015 à l'occasion de la présentation de la *Stratégie nationale pour la sécurité numérique*. Durant son discours, M. Valls tenait ces propos :

> *Mais – s'il était nécessaire de donner à nos services de renseignement les outils indispensables pour assumer leurs missions dans la société numérique – mon gouvernement reste favorable à ce que les acteurs privés continuent de bénéficier pleinement, pour se protéger, de toutes les ressources qu'offre la cryptologie légale.*

Et le journaliste de s'interroger sur la signification de ce que pourrait bien être la « cryptologie légale », dans la mesure où le fait de pouvoir chiffrer des communications ne se pose pas en ces termes. Sur son site, l'ANSSI est très claire :

> *L'utilisation d'un moyen de cryptologie est libre. Il n'y a*

aucune démarche à accomplir.

En revanche, la fourniture, l'importation, le transfert intracommunautaire et l'exportation d'un moyen de cryptologie sont soumis, sauf exception, à déclaration ou à demande d'autorisation.

Si M. Valls s'adressait essentiellement aux professionnels des communications, une telle déclaration mérite que l'on s'y arrête un peu. Elle résonne particulièrement fort dans le contexte juridique, social et émotionnel très particulier qui a vu se multiplier l'adoption de lois et de procédures qui mettent fortement en danger les libertés de communication et d'expression, sous couvert de lutte contre le terrorisme, ainsi que l'illustrait le Projet de loi renseignement au printemps 2015.

Extrait de la conférence « Dégooglisons Internet »

On note que M. Valls précise que les moyens de « cryptologie légale » sont laissés au libre choix des acteurs privés « pour se protéger ». En effet, comme le rappelle l'ANSSI, le fait de fournir un moyen de chiffrer des communications doit faire l'objet d'une déclaration ou d'une autorisation. C'est uniquement dans le choix des systèmes préalablement autorisés, que M. Valls concède aux acteurs privés qui en ressentent le besoin d'aller piocher le meilleur moyen d'assurer la confidentialité et l'authenticité de leurs échanges ou des échanges de leurs utilisateurs.

C'est sans doute cela qu'il fallait comprendre dans cette phrase. À ceci près que rappeler ce genre d'éléments aussi basiques à des acteurs déjà bien établis dans le secteur des communications numériques, ressemble bien plutôt à une mise en garde : il y a du chiffrement autorisé et il y a du chiffrement qui ne l'est pas. En d'autres termes, du point de vue des fournisseurs comme du point de vue des utilisateurs, tout n'est pas permis, y compris au nom de la protection de la vie privée.

La question du choix entre respect de la vie privée (ou d'autres libertés comme les libertés d'expression et de communication) et l'intérêt suprême de l'État dans la protection de ses citoyens, est une question qui est à l'heure actuelle bien loin d'être tranchée (si elle peut l'être un jour). Habituellement caricaturée sur le mode binaire du choix entre sécurité et liberté, beaucoup ont essayé ces derniers temps de calmer les ardeurs des partisans des deux camps, en oubliant comme nous le verrons dans les prochaines sections, que le choix datait d'au moins des premiers théoriciens du Contrat Social, il y a trois siècles. L'histoire de PGP (Pretty Good Privacy) et du standard OpenPGP est jalonnée de cette dualité (sécurité et liberté) dans notre conception du contrat social.

Autorité et PGP

La première diffusion de PGP était déjà illégale au regard du droit à l'exportation des produits de chiffrement, ce qui a valu à son créateur, Philip Zimmermann quelques ennuis juridiques au début des années 1990. La France a finalement suivi la politique nord-américaine concernant PGP en autorisant l'usage mais en restreignant son étendue. C'est l'esprit du décret 99-200 du 17 mars 1999, qui autorise, sans formalité préalable, l'utilisation d'une clé de chiffrement à condition qu'elle soit inférieure ou égale à 128 bits pour chiffrer des données. Au-delà, il fallait une autorisation jusqu'au vote de la *Loi sur l'économie numérique* en 2004, qui fait sauter le verrou des 128 bits (art. 30-1) pour l'usage du chiffrement (les moyens, les logiciels, eux, sont soumis à déclaration[1]).

Si l'on peut aisément mettre le doigt sur les lacunes du *système* PGP[2], il reste qu'une clé de chiffrement à 128 bits, si l'implémentation est correcte, permet déjà de chiffrer très efficacement des données, quelles qu'elles soient. Lorsque les activités de surveillance de masse de la NSA furent en partie révélées par E. Snowden, on apprit que l'une des pratiques consiste à capter et stocker les contenus des communications de manière exhaustive, qu'elles soient chiffrées ou non. En cas de chiffrement, la NSA compte sur les progrès techniques futurs pour pouvoir les déchiffrer un jour où l'autre, selon les besoins. Ce gigantesque travail d'archivage réserve en principe pour l'avenir des questions de droit plutôt inextricables (par exemple l'évaluation du degré de préméditation d'un crime, ou le fait d'être suspect parce qu'on peut établir que 10 ans plus tôt Untel était en relation avec Untel). Mais le principal sujet, face à ce gigantesque travail d'espionnage de tout l'Internet, et d'archivage de données privées lisibles et illisibles, c'est de savoir dans quelle mesure il est possible de réclamer un peu plus que le

seul *respect* de la vie privée. Pour qu'une agence d'État s'octroie le droit de récupérer dans mon intimité des données qu'elle n'est peut-être même pas capable de lire, en particulier grâce à des dispositifs comme PGP, il faut se questionner non seulement sur sa légitimité mais aussi sur la conception du pouvoir que cela suppose.

Si PGP a finalement été autorisé, il faut bien comprendre quelles en sont les limitations légales. Pour rappel, PGP fonctionne sur la base du binôme clé publique / clé privée. Je chiffre mon message avec ma clé de session, générée aléatoirement à 128 bits (ou plus), et cette clé de session est elle-même chiffrée avec la clé publique du destinataire (qui peut largement excéder les 128 bits). J'envoie alors un paquet contenant a) le message chiffré avec ma clé de session, et b) ma clé de session chiffrée par la clé publique de mon destinataire. Puis, comme ce dernier possède la clé privée qui va de pair avec sa clé publique, lui seul va pouvoir déchiffrer le message. On comprend donc que la clé privée et la clé publique ont des rôles bien différents. Alors que la clé privée sert à chiffrer les données, la clé publique sert contrôler l'accès au contenu chiffré. Dans l'esprit du décret de 1999, c'est la clé de session qui était concernée par la limitation à 128 bits.

PGP a donc été autorisé pour au moins trois raisons, que je propose ici à titre de conjectures :

- parce que PGP devenait de plus en plus populaire et qu'il aurait été difficile d'en interdire officiellement l'usage, ce qui aurait supposé une surveillance de masse des échanges privés (!),
- parce que PGP est une source d'innovation en termes de services et donc porteur d'intérêts économiques,
- parce que PGP, limité en chiffrement des contenus à 128 bits, permettait d'avoir un étalon de mesure pour justifier la nécessité de délivrer des autorisations pour des systèmes de chiffrement supérieurs à 128 bits,

> c’est-à-dire des chiffrements hautement sécurisés, même si la version autorisée de PGP est déjà très efficace. Après 2004, la question ne se pose plus en termes de limitation de puissance mais en termes de surveillance des moyens (ce qui compte, c’est l’intention de chiffrer et à quel niveau).

En somme c’est une manière pour l’État de retourner à son avantage une situation dans laquelle il se trouvait pris en défaut. Je parle en premier lieu des États-Unis, car j’imagine plutôt l’État français (et les États européens en général) en tant que suiveur, dans la mesure où si PGP est autorisé d’un côté de l’Atlantique, il aurait été de toute façon contre-productif de l’interdire de l’autre. En effet, Philip Zimmermann rappelle bien les enjeux dans son texte « Pourquoi j’ai écrit PGP ». La principale raison qui justifie selon lui l’existence de PGP, est qu’une série de dispositions légales entre 1991 et 1994 imposaient aux compagnies de télécommunication américaines de mettre en place des dispositions permettant aux autorités d’intercepter en clair des communications. En d’autres termes, il s’agissait d’optimiser les dispositifs de communication pour faciliter leur accès par les services d’investigation et de surveillance aujourd’hui tristement célèbres. Ces dispositions légales ont été la cause de scandales et furent en partie retirés, mais ces intentions cachaient en vérité un programme bien plus vaste et ambitieux. Les révélations d’E. Snowden nous en ont donné un aperçu concret il y a seulement deux ans.

Inconstitutionnalité de la surveillance de masse

Là où l’argumentaire de Philip Zimmermann devient intéressant, c’est dans la justification de l’intention de créer PGP, au delà de la seule réaction à un contexte politique dangereux. Pour le citer :

> *[…] Il n'y a rien de mal dans la défense de votre intimité. L'intimité est aussi importante que la Constitution. Le droit à la vie privée est disséminé implicitement tout au long de la Déclaration des Droits. Mais quand la Constitution des États-Unis a été bâtie, les Pères Fondateurs ne virent aucun besoin d'expliciter le droit à une conversation privée. Cela aurait été ridicule. Il y a deux siècles, toutes les conversations étaient privées. Si quelqu'un d'autre était en train d'écouter, vous pouviez aller tout simplement derrière l'écurie et avoir une conversation là. Personne ne pouvait vous écouter sans que vous le sachiez. Le droit à une conversation privée était un droit naturel, non pas seulement au sens philosophique, mais au sens des lois de la physique, étant donné la technologie de l'époque. Mais avec l'arrivée de l'âge de l'information, débutant avec l'invention du téléphone, tout cela a changé. Maintenant, la plupart de nos conversations sont acheminées électroniquement. Cela permet à nos conversations les plus intimes d'être exposées sans que nous le sachions.*

L'évocation de la Constitution des États-Unis est tout à fait explicite dans l'argumentaire de Philip Zimmermann, car la référence à laquelle nous pensons immédiatement est le Quatrième amendement (de la *Déclaration des Droits*) :

> *Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir.*

En d'autres termes, la surveillance de masse est anticonstitutionnelle. Et cela va beaucoup plus loin qu'une simple affaire de loi. Le Quatrième amendement repose

essentiellement sur l'adage très britannique *my home is my castle*, c'est à dire le point de vue de la *castle doctrine*, une rémanence du droit d'asile romain (puis chrétien). C'est-à-dire qu'il existe un lieu en lequel toute personne peut trouver refuge face à l'adversité, quelle que soit sa condition et ce qu'il a fait, criminel ou non. Ce lieu pouvant être un temple (c'était le cas chez les Grecs), un lieu sacré chez les romains, une église chez les chrétiens, et pour les peuples qui conféraient une importance viscérale à la notion de propriété privée, comme dans l'Angleterre du XVI^{e} siècle, c'est la demeure. La naissance de l'État moderne (et déjà un peu au Moyen Âge) encadra fondamentalement ce droit en y ajoutant des conditions d'exercice, ainsi, par exemple, dans le Quatrième Amendement, l'existence ou non de « présomptions sérieuses ».

Microsoft : Do you need a backdoor… to you castle ?

État absolu, soif d'absolu

Le besoin de limiter drastiquement ce qui ressort de la vie privée, est éminemment lié à la conception de l'État moderne et du contrat social. En effet, ce qui se joue à ce moment de l'histoire, qui sera aussi celui des Lumières, c'est une conception rationnelle de la vie commune contre l'irrationnel des temps anciens. C'est Thomas Hobbes qui, parmi les plus acharnés du pouvoir absolu de l'État, traumatisé qu'il était par la guerre civile, pensait que rien ne devait entraver la survie et l'omnipotence de l'État au risque de retomber dans les âges noirs de l'obscurantisme et du déchaînement des passions. Pour lui, le pacte social ne tient que dans la mesure où, pour le faire respecter, l'État peut exercer une violence incommensurable sur les individus qui composent le tissu social (et ont conféré à l'État l'exercice de cette violence). Le pouvoir de l'État s'exerce par la centralisation et la soumission à l'autorité, ainsi que le résume très bien Pierre Dockès dans son article « Hobbes et le pouvoir »[3].

Mais qu'est-ce qui était irrationnel dans ces temps anciens, par exemple dans la République romaine ? Beaucoup de choses à vrai dire, à commencer par le polythéisme. Et justement, l'*asylum* latin fait partie de ces conceptions absolues contre lesquelles les théoriciens du contrat social se débattront pour trouver des solutions. L'État peut-il ou non supporter l'existence d'un lieu où son pouvoir ne pourrait s'exercer, en aucun cas, même s'il existe des moyens techniques pour le faire ? C'est le *tabou*, dans la littérature ethnologique, dont la transgression oblige le transgresseur à se soumettre à une forme d'intervention au-delà de la justice des hommes, et par là oblige les autres hommes à l'impuissance face à cette transgression innommable et surnaturelle.

À cet absolu générique s'opposent donc les limitations de l'État de droit. Dans le Code Civil français, l'article 9 stipule : « Chacun a droit au respect de sa vie privée. Tout

est dans la notion de respect, que l'on oublie bien vite dans les discussions, ici et là, autour des conditions de la vie privée dans un monde numérique. La définition du respect est une variable d'ajustement, alors qu'un absolu ne se discute pas. Et c'est cette soif d'absolu que l'on entend bien souvent réclamée, car il est tellement insupportable de savoir qu'un ou plusieurs États organisent une surveillance de masse que la seule réaction proportionnellement inverse que peuvent opposer les individus au non-respect de la vie privée relève de l'irrationnel : l'absolu de la vie privée, l'idée qu'une vie privée est non seulement inviolable mais qu'elle constitue aussi l'*asylum* de nos données numériques.

Qu'il s'agisse de la vie privée, de la propriété privée ou de la liberté d'expression, à lire la Déclaration des droits de l'homme et du citoyen de 1789, elles sont toujours soumises à deux impératifs. Le premier est un dérivé de l'impératif catégorique kantien : « ne fais pas à autrui ce que tu n'aimerais pas qu'on te fasse » (article 4 de la Déclaration), qui impose le pouvoir d'arbitrage de l'État (« Ces bornes ne peuvent être déterminées que par la Loi ») dans les affaires privées comme dans les affaires publiques. L'autre impératif est le principe de souveraineté (article 3 de la Déclaration) selon lequel « Le principe de toute Souveraineté réside essentiellement dans la Nation. Nul corps, nul individu ne peut exercer d'autorité qui n'en émane expressément ». En d'autres termes, il faut choisir : soit les règles de l'État pour la paix entre les individus, soit le retour à l'âge du surnaturel et de l'immoralité.

À l'occasion du vote concernant la Loi Renseignement, c'est en ces termes que furent posés nombre de débats autour de la vie privée sous l'apparent antagonisme entre sécurité et liberté. D'un côté, on opposait la loi comme le moyen sans lequel il ne pouvait y avoir d'autre salut qu'en limitant toujours plus les libertés des individus. De l'autre côté, on voyait la loi comme un moyen d'exercer un pouvoir à d'autres fins (ou

profits) que la paix sociale : maintenir le pouvoir de quelques uns ou encore succomber aux demandes insistantes de quelques lobbies.

Mais très peu se sont penché sur la réaction du public qui voyait dans les révélations de Snowden comme dans les lois « scélérates » la transgression du tabou de la vie privée, de l'*asylum*. Comment ? Une telle conception archaïque n'est-elle pas depuis longtemps dépassée ? Il y aurait encore des gens soumis au *diktat* de la Révélation divine ? et après tout, qu'est-ce qui fait que j'accorde un caractère absolu à un concept si ce n'est parce qu'il me provient d'un monde d'idées (formelles ou non) sans être le produit de la déduction rationnelle et de l'utilité ? Cette soif d'absolu, si elle ne provient pas des dieux, elle provient du monde des idées. Or, si on en est encore à l'opposition Platon *vs.* Aristote, comment faire la démonstration de ce qui n'est pas démontrable, savoir : on peut justifier, au nom de la sécurité, que l'État puisse intervenir dans nos vie privées, mais au nom de quoi justifier le caractère absolu de la vie privée ? Saint Augustin, au secours !

À ceci près, mon vieil Augustin, que deux éléments manquent encore à l'analyse et montrent qu'en réalité le caractère absolu du droit à la vie privée, d'où l'État serait exclu quelle que soit sa légitimité, a muté au fil des âges et des pratiques démocratiques.

Dialogue entre droit de savoir et droit au secret

C'est l'autorité judiciaire qui exerce le droit de savoir au nom de la manifestation de la vérité. Et à l'instar de la vie privée, la notion de vérité possède un caractère tout aussi absolu. La vie privée manifeste, au fond, notre soif d'exercer notre droit au secret. Ses limites ? elles sont instituées par la justice (et particulièrement la jurisprudence) et non par

le pouvoir de l'État. Ainsi le Rapport annuel 2010 de la Cour de Cassation exprime parfaitement le cadre dans lequel peut s'exercer le droit de savoir en rapport avec le respect de la vie privée :

> *Dans certains cas, il peut être légitime de prendre connaissance d'une information ayant trait à la vie privée d'une personne indépendamment de son consentement. C'est dire qu'il y a lieu de procéder à la balance des intérêts contraires. Un équilibre doit être trouvé, dans l'édification duquel la jurisprudence de la Cour de cassation joue un rôle souvent important, entre le droit au respect de la vie privée et des aspirations, nombreuses, à la connaissance d'informations se rapportant à la vie privée d'autrui. Lorsqu'elle est reconnue, la primauté du droit de savoir sur le droit au respect de la vie privée se traduit par le droit de prendre connaissance de la vie privée d'autrui soit dans un intérêt privé, soit dans l'intérêt général.*

En d'autres termes, il n'y a aucun archaïsme dans la défense de la vie privée face à la décision publique : c'est simplement que le débat n'oppose pas vie privée et sécurité, et en situant le débat dans cette fausse dialectique, on oublie que le premier principe de cohésion sociale, c'est la justice. On retrouve ici aussi tous les contre-arguments avancés devant la tendance néfaste des gouvernements à vouloir automatiser les sanctions sans passer par l'administration de la justice. Ainsi, par exemple, le fait de se passer d'un juge d'instruction pour surveiller et sanctionner le téléchargement « illégal » d'œuvres cinématographiques, ou de vouloir justifier la surveillance de toutes les communications au nom de la sécurité nationale au risque de suspecter tout le monde. C'est le manque (subi ou consenti) de justice qui conditionne toutes les dictatures.

Le paradoxe est le suivant: en situant le débat sur le registre sécurité *vs.* liberté, au nom de l'exercice légitime

du pouvoir de l'État dans la protection des citoyens, on place le secret privé au même niveau que le secret militaire et stratégique, et nous serions alors tous des ennemis potentiels, exactement comme s'il n'y avait pas d'État ou comme si son rôle ne se réduisait qu'à être un instrument de répression à disposition de quelques-uns contre d'autres, ou du souverain contre la Nation. Dans ce débat, il ne faudrait pas tant craindre le « retour à la nature » mais le retour à la servitude.

Le second point caractéristique du droit de savoir, est qu'on ne peut que lui opposer des arguments rationnels. S'il s'exerce au nom d'un autre absolu, la vérité, tout l'exercice consiste à démontrer non pas le *pourquoi* mais le *comment* il peut aider à atteindre la vérité (toute relative qu'elle soit). On l'autorise alors, ou pas, à l'aune d'un consentement éclairé et socialement acceptable. On entre alors dans le règne de la déduction logique et de la jurisprudence. Pour illustrer cela, il suffit de se pencher sur les cas où les secrets professionnels ont été cassés au nom de la manifestation de la vérité, à commencer par le secret médical. La Cour de cassation explique à ce sujet, dans son Rapport 2010 :

> *[…] La chambre criminelle a rendu le 16 février 2010 (Bull. crim. 2010, no 27, pourvoi no 09-86.363) une décision qui, entre les droits fondamentaux que sont la protection des données personnelles médicales d'une part, et l'exercice des droits de la défense d'autre part, a implicitement confirmé l'inopposabilité du secret au juge d'instruction, mais aussi la primauté du droit de la défense qui peut justifier, pour respecter le principe du contradictoire, que ce secret ne soit pas opposable aux différentes parties.*

Au risque de rappeler quelques principes évidents, puisque nous sommes censés vivre dans une société rationnelle, toute tentative de casser un secret et s'immiscer dans la vie

privée, ne peut se faire *a priori* que par décision de justice à qui l'on reconnaît une légitimité « prudentielle ». Confier ce rôle de manière unilatérale à l'organe d'exercice du pouvoir de l'État, revient à nier ce partage entre l'absolu et le rationnel, c'est à dire révoquer le contrat social.

La sûreté des échanges est un droit naturel et universel

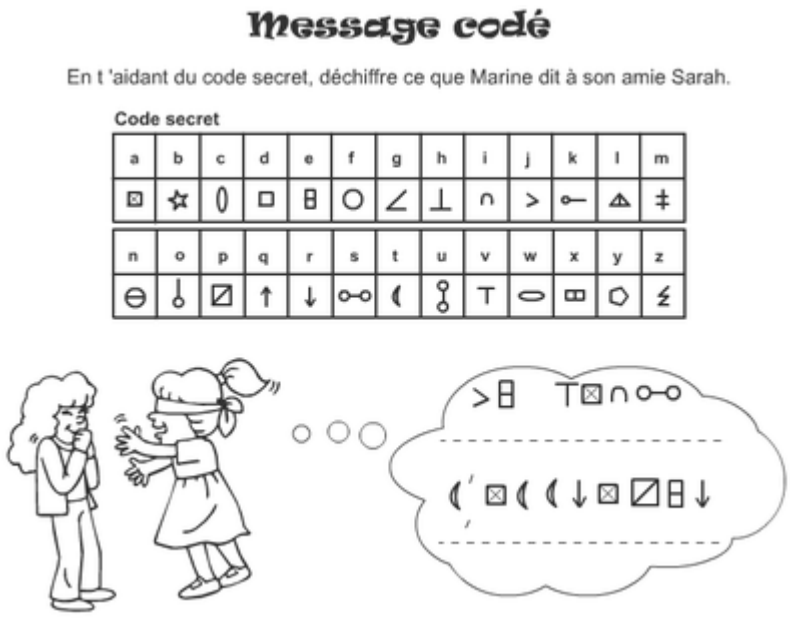
Comme le remarquait Philip Zimmermann, avant l'invention des télécommunications, le droit à avoir une conversation privée était aussi à comprendre comme une loi physique : il suffisait de s'isoler de manière assez efficace pour pouvoir tenir des échanges d'information de manière complètement privée. Ce n'est pas tout à fait exact. Les communications ont depuis toujours été soumises au risque de la divulgation, à partir du moment où un opérateur et/ou un dispositif entrent en jeu. Un rouleau de parchemin ou une lettre cachetée peuvent toujours être habilement ouverts et leur contenu divulgué. Et d'ailleurs la principale fonction du cachet n'était pas tant de fermer le pli que de l'authentifier.

C'est pour des raisons de stratégie militaire, que les premiers chiffrements firent leur apparition. Créés par l'homme pour l'homme, leur degré d'inviolabilité reposait sur l'habileté intellectuelle de l'un ou l'autre camp. C'est ainsi que le chiffrement ultime, une propriété de la nature (du moins, de la logique algorithmique) a été découvert : le chiffre de Vernam ou système de chiffrement à masque jetable. L'idée est de créer un chiffrement dont la clé (ou masque) est aussi longue que le message à chiffrer, composée de manière aléatoire et utilisable une seule fois. Théoriquement impossible à casser, et bien que présentant des lacunes dans la mise en œuvre pratique, cette méthode de chiffrement était accessible à la puissance de calcul du cerveau humain. C'est avec l'apparition des machines que les dés ont commencés à

être pipés, sur trois plans :

- en dépassant les seules capacités humaines de calcul,
- en rendant extrêmement rapides les procédures de chiffrement et de déchiffrement,
- en rendant accessibles des outils puissants de chiffrement à un maximum d'individus dans une société « numérique ».

Dans la mesure où l'essentiel de nos communications, chargées de données complexes et à grande distance, utilisent des machines pour être produites (ou au moins formalisées) et des services de télécommunications pour être véhiculées, le « droit naturel » à un échange privé auquel faisait allusion Philip Zimmermann, passe nécessairement par un système de chiffrement pratique, rapide et hautement efficace. PGP est une solution (il y en a d'autres).



PGP est-il efficace ? Si le contrôle de l'accès à nos données peut toujours nous échapper (comme le montrent les procédures de surveillance), le chiffrement lui-même, ne serait-ce qu'à 128 bits « seulement », reste à ce jour assez crédible. Cette citation de Wikipédia en donne la mesure :

À titre indicatif, l'algorithme AES, dernier standard

> *d'algorithme symétrique choisi par l'institut de standardisation américain NIST en décembre 2001, utilise des clés dont la taille est au moins de 128 bits soit 16 octets, autrement dit il y en a 2^{128}. Pour donner un ordre de grandeur sur ce nombre, cela fait environ $3,4\times10^{38}$ clés possibles ; l'âge de l'univers étant de 10^{10} années, si on suppose qu'il est possible de tester 1 000 milliards de clés par seconde (soit $3,2\times10^{19}$ clés par an), il faudra encore plus d'un milliard de fois l'âge de l'univers. Dans un tel cas, on pourrait raisonnablement penser que notre algorithme est sûr. Toutefois, l'utilisation en parallèle de très nombreux ordinateurs, synchronisés par internet, fragilise la sécurité calculatoire.*

Les limites du chiffrement sont donc celles de la physique et des grands nombres, et à ce jour, ce sont des limites déjà largement acceptables. Tout l'enjeu, désormais, parce que les États ont montré leur propension à retourner l'argument démocratique contre le droit à la vie privée, est de disséminer suffisamment les pratiques de chiffrement dans le corps social. Ceci de manière à imposer en pratique la communication privée-chiffrée comme un acte naturel, un libre choix qui borne, en matière de surveillance numérique, les limites du pouvoir de l'État à ce que les individus choisissent de rendre privé et ce qu'ils choisissent de ne pas protéger par le chiffrement.

Conclusion

Aujourd'hui, la définition du contrat social semble passer par un concept supplémentaire, le chiffrement de nos données. L'usage libre des pratiques de chiffrement est borné officiellement à un contrôle des moyens, ce qui semble suffisant, au moins pour nécessiter des procédures judiciaires bien identifiées dans la plupart des cas où le droit de savoir

s'impose. Idéalement, cette limite ne devrait pas exister et il devrait être possible de pouvoir se servir de systèmes de chiffrement réputés inviolables, quel que soit l'avis des gouvernements.

L'inviolabilité est une utopie ? pas tant que cela. En 2001, le chercheur Michael Rabin avait montré lors d'un colloque qu'un système réputé inviolable était concevable. En 2005, il a publié un article éclairant sur la technique de l'hyper-chiffrement (hyper encryption) intitulé « Provably unbreakable hyper-encryption in the limited access model », et une thèse (sous la direction de M. Rabin) a été soutenue en 2009 par Jason K. Juang, librement accessible à cette adresse. Si les moyens pour implémenter de tels modèles sont limités à ce jour par les capacités techniques, la sécurité de nos données semble dépendre de notre volonté de diminuer davantage ce qui nous sépare d'un système 100% efficace d'un point de vue théorique.

Le message de M. Valls, à propos de la « cryptologie légale » ne devrait pas susciter de commentaires particuliers puisque, effectivement, en l'état des possibilités techniques et grâce à l'ouverture de PGP, il est possible d'avoir des échanges réputés privés à défaut d'être complètement inviolables. Néanmoins, il faut rester vigilant quant à la tendance à vouloir définir légalement les conditions d'usage du chiffrement des données personnelles. Autant la surveillance de masse est (devrait être) inconstitutionnelle, autant le droit à chiffrer nos données doit être inconditionnel.

Doit-on craindre les pratiques d'un gouvernement plus ou moins bien intentionné ? Le Léviathan semble toutefois vaciller : non pas parce que nous faisons valoir en droit notre intimité, mais parce que d'autres Léviathans se sont réveillés, en dehors du droit et dans une nouvelle économie, sur un marché dont ils maîtrisent les règles. Ces nouveaux Léviathans, il nous faut les étudier avec d'autres concepts que ceux qui définissent l'État moderne.

Pour aller plus loin :

- La série d'articles sur le framablog
  - Les nouveaux Léviathans Ia
  - Les nouveaux Léviathans Ib
  - Les nouveaux Léviathans IIa
  - Les nouveaux Léviathans IIb
  - Les nouveaux Léviathans III
  - Les nouveaux Léviathans IV
  - Les Nouveaux Léviathans V
  - Les anciens Léviathans I
  - Les anciens Léviathans II
- La série d'article au complet (fichier .epub)

---

1. On peut se reporter au site de B. Depail (Univ. Marne-La-Vallée) de qui expose les aspects juridiques de la signature numérique, en particulier la section « Aspects juridiques relatifs à la cryptographie ».↩
2. Voir « Surveillance généralisée : aux limites de PGP », *MISC*, **75**, 2014.↩
3. Pierre Dock□s, « Hobbes et le pouvoir », *Cahiers d'économie politique*, **50**.1, 2006, pp. 7-25.↩