Introduction générale

1 Préambule : l'homme, le secret et le pouvoir

S'il n'est pas encore tout à fait déplacé d'appliquer quelques principes, il faut mettre sans doute en exergue celui qui, avec Rabelais, nous exhorte à ne pas pratiquer de science sans conscience, sous peine de ruine de l'âme. Historiquement, le rapport de la société des hommes avec le secret est un sujet sensible. Il nous a paru primordial de retracer une brève histoire du secret dans l'humanité, afin de dégager clairement les enjeux à l'œuvre dans la démocratisation des techniques d'écriture secrète. En effet, il apparaît que les implications d'un développement de ces techniques dépassent de loin les seules perspectives marchandes.

L'adjectif "secret" provient du verbe latin "secernere", qui signifie "écarter", il entre dans la langue française vers 1180 ; le substantif "secret", qui dérive lui du neutre de l'adjectif latin "secretus", se répand vers 1380 hors du Poitou, où il est attesté depuis 1110 (la victoire de notre prononciation du mot "secret" sur sa variante de l'époque "segret" a dû attendre le XVIIIème siècle.) On doit donc en déduire que pendant les deux premiers siècles, les gens disaient plus volontiers "C'est secret", que "C'est un secret", chargeant ainsi dès l'origine le mot avec une certaine gravité. L'invention de la langue autour du secret s'arrête, puis reprend un peu avant la fin du XVIème siècle (époque à laquelle se structure le français moderne). C'est seulement à partir de 1560 qu'est attesté le sens de "mystère", il a donc fallu encore presque deux siècles pour que le mot commence à s'émanciper de sa gravité première. "Etre dans le secret", qui date de 1690, commence alors seulement à connoter le mot politiquement, pour l'associer à la pratique du complot, fort répandue à l'époque. Il serait plaisant de pouvoir comparer cette évolution du mot secret dans les différentes langues. Le mot se charge de multiples sens tous très voisins (le secret était aussi un débarras isolé dans les habitations, d'où découle l'expression *mettre au secret*). Parmi les onze que recense Littré, on trouve "Qui ne peut être point pénétré", relatif à la cryptographie[1], et "Qui n'est pas apparent, visible", relatif à la stéganographie[2]. Au passage, l'article *stéganographie* est plus laconique, évoquant une simple "écriture en signes secrets et convenus", et est illustré avec une citation prenant "secret" dans son acception cryptographique[3] !

A l'heure où les menaces sur la liberté d'expression sont chaque jour moins camouflées, il importe de mesurer le fantastique rôle des techniques numériques d'écriture secrète dans la

[1]"Vous n'aurez point pour moi de langages secrets" - Racine, *Britannicus*, II, 3.

[2]"Oui, vos moindres discours ont des grâces secrètes" - Racine, *Esthétique*, III, 4.

[3]"La stéganographie, l'art facile de combiner des lettres ne présentant un sens que pour les initiés qui possèdent la clef, existe de toute antiquité." Cahun, *Liberté*, 27 mai 1867.

dynamique qui oppose depuis toujours les individus à leurs formes d'organisation politique[4]. Pour cela, nous interrogeons la transition historique subtile entre vouloir lire et pouvoir écrire un secret. Les étapes de ce passage sont marquées par les différentes stratégies que les dirigeants ont successivement employées pour maintenir la cohésion de la communauté autour d'eux. Cette mise au point liminaire se propose essentiellement de replacer les techniques d'écriture secrète dans leur contexte global, et non plus seulement suivant la seule perspective actuelle, marchande en l'occurence, comme il arrive trop souvent.

1.1 Lire un secret

Il semble bien que la relation de l'homme au secret n'est pas aussi claire qu'il peut y paraître a priori. Historiquement, il s'avère que l'on a d'abord cherché à lire un secret, et que l'écriture (e.g. la maîtrise) des secrets a été l'objet d'une attention plus tardive, fondée sur l'organisation de l'homme en communautés, aux jeux de pouvoirs complexes, et conditionnée par la création d'outils adéquats. Lire le cours, présumé secret, des événements a été la grande affaire des hommes depuis leur accession au stade de créature intellectuelle, capable de prendre consciemment en compte la succession d'observations d'événements environnementaux importants, souvent bouleversants pour la communauté. Dans la plupart des tribus agraires, un dépositaire important du pouvoir dans la communauté était celui censé établir le contact avec le monde des représentations ésotériques influant sur la prospérité du groupe. Il faut y lire l'embryon des premières croyances, et partant celui des premières religions[5]. Le chamane, le prêtre, le mage, tous sont les représentants de cette interface avec l'illusion première nécessaire à l'homme, celle du secret encore à découvrir, de l'accès rare à la connaissance totale. On notera le caractère éminemment anthropologique de la plupart des textes religieux fondateurs, la morale étant l'outil par lequel on codifie de manière irrévocable, apparemment ex nihilo (donc secrètement, car on trace alors la ligne de partage fondamentale entre ce qui relève du sacré et du profane), des règles censées maximiser la prospérité du groupe. Les règles d'association entre individus mâles et femelles ont généralement pour but de minimiser les risques de dégénérescence génétique[6], et les règles de respect de l'intégrité physique des autres individus ont généralement un effet économique bénéfique car stabilisateur, sur le développement de la communauté.

[4]Sur le secret en tant que ferment communautaire, voir par exemple *La communauté inavouable* (notamment la partie consacrée au groupe *Acéphale*), de Maurice Blanchot, Minuit, 1996.

[5]La paléo-anthropologie a récemment établi que les premières sépultures à caractère religieux datent de -100000 ans, et qu'elles ont été le fait tant de l'homme de Néanderthal (habitant l'Europe, aujourd'hui disparu), que de l'*homo sapiens* dont nous descendons (et qui lui seul semble avoir découvert l'art). Les deux hominidés étaient en outre si génétiquement différents qu'il faut parler de deux espèces distinctes (aucune descendance commune possible bien qu'ils se soient côtoyés pendant des millénaires), mais ont toutes les deux connu l'angoisse métaphysique. Voilà qui, un siècle plus tard, crédite Renan de manière posthume, lequel se plaignait de ce que "Hegel est insoutenable dans le rôle exclusif qu'il attribue à l'humanité, laquelle n'est sans doute pas la seule forme consciente du divin, bien que ce soit la plus avancée que nous connaissions." (cité par G. Campioni in *Les lectures françaises de Nietzsche*, PUF, 2001, p. 94)

[6]Voir entre autres *L'Érotisme*, de Georges Bataille (pour une présentation, certes encore hégélienne, des aspects communautaristes), Minuit, 1957, et *Histoire naturelle de l'amour*, de Helen Fisher (pour une mise en perspective avec le règne animal en général), Robert Laffont, 1998. Par exemple, la ruine des Habsbourg en Europe est due aux tares mentales des héritiers, conçus après trop de mariages consanguins.

La genèse de ces règles (la religion est littéralement ce qui relie les hommes entre eux) peut être vue comme le terreau expérimental de la pratique politique. Les deux sentiments les plus souvent inspirés aux individus par les dirigeants pour les tenir ensemble en pratique semblent être la peur et l'espoir, alternant au rythme des phases de crise et de prospérité. Si en temps de crise un groupe est davantage soudé par la peur, la paix et le développement économique nécessitent un liant social tout aussi efficace mais moins coûteux. L'espoir de déchiffrer l'apparition de phénomènes bouleversants comme les catastrophes naturelles, les épidémies et les guerres, pour s'en protéger, constitue le plus clair de l'effort humain en temps de paix, afin d'arriver à l'illusion d' "un monde qui ne se contredise pas, ni ne trompe, ni ne change, un monde *vrai* - un monde où l'on ne souffre pas..." [7] Ces événements restant en général rares à l'échelle de l'individu, même dans les époques les plus troublées, il a bien fallu, puisque l'expérience de personne n'était assez longue, se résoudre à introduire l'inconnu dans le raisonnement - ou plus précisément à raisonner juste sur des concepts ésotériques. Ainsi, pour reprendre l'exemple de Mircea Eliade[8], lorsqu'il s'agit de se sédentariser, une communauté choisira bien sûr la proximité d'un cours d'eau, et si aucun autre avantage naturel ne peut être exploité, décidera au hasard de la situation du campement sur ce cours d'eau. On préférera l'endroit où tel chasseur a abattu son premier oiseau, ou l'endroit où il vient de pleuvoir.

Plus les choix stratégiques faits pour la communauté devaient paraître indiscutables, plus ils devaient donner l'impression de résulter d'un processus ésotérique, dont les règles de production étaient d'autant moins accessibles au plus grand nombre (par définition). Au besoin, on pourra s'aider de la figure d'un dieu terrifiant poussant parfois l'absurde jusqu'à exiger des sacrifices humains dans la communauté (cf. les cultes de Baal et Moloch[9] en Europe ou celui des dieux Incas). Les choix et règles établies à l'occasion de la formation de la communauté sont appelées le mythe. Ce qui est important ici n'est pas tant le résultat de l'oracle que le secret avec lequel il est produit. Plus un mode de production d'oracles passe pour incompréhensible, plus l'oracle est réputé sage. Le mouvement premier de l'esprit humain est de repérer des similitudes entre les événements et les choses, de valider telle prophétie et d'infirmer telle autre, et par là de légitimer telles croyances, de les hiérarchiser, de les sélectionner minutieusement, afin de rendre le monde habitable poétiquement comme dirait Hölderlin (la validation par l'esprit des illusions destinées à l'âme constitue une condition nécessaire de l'humanité). Il est d'ailleurs notoire que l'homme a dépensé énormément plus de ressources et gaspillé beaucoup plus de forces pour des motifs irrationnels que rationnels. Dans le but de préserver la cohésion du groupe à travers les âges, il a fallu devenir capable de transmettre le mythe, au début de manière orale puis de manière écrite. Dans le cas des croyances comportant un héritage écrit, il est apparu nécessaire de sacraliser l'ouvrage relatant le mythe. Notre époque mesure autant qu'une autre les aberrations et la bêtise irrationnelle qui en découlent. La sacralisation de l'ouvrage mythique ouvre la voie à une nouvelle forme de prophétie, basée sur l'étude du texte sacré.

Pour naître, cette forme de prophétie nouvelle a nécessité d'élargir l'espace des oracles possibles, de le rendre virtuellement infini - sa crédibilité en dépendait. Ce sont les chercheurs

[7] Nietzsche, *Fragments Posthumes*, 9 [60], automne 1887.

[8] *Le sacré et le profane*, Gallimard, 1965.

[9] Termes qui tous deux désignent le maître, le seigneur. Cf. Voltaire, *Dictionnaire philosophique*, Religion, Seconde Question.

hébraïques les premiers qui ont opéré la connexion entre le secret et le nombre[10]. En effet, l'interprétation ésotérique de la bible hébraïque, la Cabale, repose à la fois sur les occurrences des suites de lettres et sur l'association d'un nombre à une lettre. Sans doute pour la première fois, la Cabale investit le nombre comme objet de divination, comme voie d'accès à la connaissance totale, comme vecteur du secret. Et de fait, même un moderne bon teint manifeste davantage de curiosité envers la numérologie qu'envers la lecture des entrailles du chat du voisin[11], la lecture de n'importe quel hebdomadaire imprimé sur papier bon marché suffit à s'en convaincre. Toutefois, le nombre cabalistique diffère beaucoup du nôtre : il méprise l'algèbre[12]. Seule est prise en compte sa signification symbolique ésotérique, ainsi par exemple du nombre sept qui représente la puissance. Dans l'optique consistant à percer le grand secret de la création, il semble qu'il faille se doter du nombre et d'une logique[13], fut-elle fantasque[14]. Tous les moyens sont donc bons pour générer l'illusion nécessaire à la communauté, mais les premiers et encore les plus profonds sont ésotériques, apparemment seuls habilités à rendre à l'homme l'intelligibilité perdue des événements extérieurs qu'il subit.

1.2 Ecrire un secret

La complexité des communautés et la richesse de leurs interactions ainsi que le développement économique acquis en temps de paix ont été à l'origine de régimes politiques

[10]Plus tard, et toujours dans le but de justifier le mythe par le secret, Voltaire rappelle qu'au début de notre ère "on reprocha aussi aux premiers chrétiens la supposition de quelques vers acrostiches d'une ancienne sybille, lesquels commençaient tous par les lettres initiales du nom de Jésus-Christ, chacune dans leur ordre." (Voltaire, *Dictionnaire philosophique*, article *Christianisme*, Recherches historiques sur le Christianisme, Gallimard, 1994, p. 175)

[11]"La curiosité n'est pas un goût pour ce qui est bon ou ce qui est beau, mais pour ce qui est rare, unique, pour ce qu'on a et que les autres n'ont point.", La Bruyère, *Les Caractères*, XIII, 2, De la mode.

[12]"L'apparente "objectivité" du calcul est toujours une illusion. Ses opérations ne s'appliquent à la réalité qu'au prix d'une réduction telle que ses résultats ne s'y rapportent que de ce point de vue particulier." - M. Bounan, *Sans valeur marchande*, Le sujet de la science, Allia, 2001.

[13]"[...] A la base de la construction logique du nombre figure donc un axiome non analytique, qui est en réalité une assertion relative à l'univers [son infinité]", R. Blanché et J. Dubucs, *La logique et son histoire*, Armand Collin, 1970, p. 339.

[14]Dans son étude consacrées aux fous littéraires (*Aux confins des ténèbres*, Gallimard, 2002), Raymond Queneau évoque ces psychotiques persuadés d'avoir résolu la quadrature du cercle. Par exemple, un de ces Quadrateurs, Lucas, en cherchant le volume d'une pyramide accepte sans trop s'émouvoir que $\sqrt{6-\sqrt{3}} = 6$ et $2-\sqrt{3} = 3$! Il déclare que le calcul différentiel et intégral, *puisqu'il* ne reconnaît qu'une seule valeur à π, conduit à des résultats "non seulement inexacts, mais même contradictoires". Entre autres, il nie encore l'existence du dodécaèdre, de l'hyperbole, il expose une méthode unique de résolution des équations de n'importe quel degré, l'aire de ses cercles est indépendante de leur périmètre, etc. Lucas et une cinquantaine d'autres ont servi de matière à Queneau pour son Chambernac rédigeant son Encyclopédie des sciences inexactes dans *Les Enfants du limon*. Ils ont tous été *publiés*, parfois même décorés comme Joseph Lacomme, analphabète, qui apprit à compter avec les numéros des maisons dans les rues, et calcula que $\pi = 25/8$ en creusant inlassablement son puit nuit et jour (approximation tout de même moins bonne que celle d'Archimède, mais que ses admirateurs, car il en eut, trouvaient meilleure au motif que le résultat tombe juste après la 3ème décimale). Joseph Lacomme obtint plusieurs distinctions et diplômes à la fin du XIXème siècle, dont une médaille de la Société des sciences et des arts de Paris, pour ses travaux sur la quadrature du cercle, qui connurent une quinzaine de réimpressions (Queneau, *op. cit.*, p. 80). La plupart de ces brillants exposés se terminent par un auto-portrait pathétique du nouveau démiurge ou par un délire de persécution, pouvant aller dans son intensité jusqu'à dissoudre la grammaire elle-même.

variés, tendant à la démocratie en cas de période de prospérité longue. On peut arguer du fait que les régimes politiques et leurs moyens d'existence s'intellectualisent avec la prospérité du groupe et son importance. Ainsi, il est sans doute plus sûr de recourir aux médias pour influencer des millions de personnes plutôt que d'envoyer l'armée. Le même raisonnement n'est pas nécessairement valable pour des groupes plus petits. Historiquement, la conquête puis la conservation du pouvoir est l'affaire d'une minorité, dans l'écrasante majorité des civilisations. La taille des groupes à diriger augmentant, il a fallu à la minorité des maîtres développer des moyens moins coûteux que les guerres et les sacrifices pour garantir la cohésion des individus autour d'elle. L'expérience a voulu que la connaissance a priori d'information sur l'adversaire aidait à prendre souvent une longueur d'avance sur lui. Le besoin d'un échange sûr d'information sensible, qu'on ne pouvait intercepter, se faisait jour. Deux grandes voies ont été retenues : brouiller le contenu de l'information à transmettre, et rendre la transmission indétectable. Les deux techniques semblent avoir été développées en parallèle, de manière ad hoc. La première évoluerait vers la cryptographie moderne dès lors que les outils algébriques seraient disponibles, la seconde poursuivrait son chemin autour d'évolutions souvent proches de recettes de cuisine, fédérant le tout sous le terme de stéganographie[15].

Si vouloir lire un secret est à l'origine de la divination, pouvoir en écrire relève de la politique et de ses moyens. C'est la nature supposée de l'émetteur de l'information secrète, humaine ou non, qui fait qu'on parle de divination ou de science. La séparation tardive entre l'alchimie et la chimie comme entre la sorcellerie et la médecine[16] relève de la même évolution menant d'une approche irrationnelle, parce que fondée sur trop peu d'observations, à une science se caractérisant par la mise en relation abstraite d'observations plus nombreuses réputées ainsi plus fiables. Cependant, si le développement de la chimie et de la médecine correspond à une volonté d'aménager des conditions d'existence physique, il faut reconnaître que celui de la cryptographie et de la stéganographie a pour unique objet les conditions d'existence politique de l'homme. Longtemps l'apanage des militaires[17] et de la classe dirigeante, ces techniques semblent bénéficier aujourd'hui d'une relative libéralisation avec l'émergence de notions comme le respect de la vie privée et du secret des correspondances dans les civilisations les plus prospères. Il est possible d'y distinguer un des signes du déplacement du pouvoir de la sphère politique vers la sphère purement économique. En effet, la généralisation du secret dans l'usage des communications entre individus ne laisse pas d'affaiblir l'Etat dans sa relation avec l'individu, ce qui est au passage une des caractéristiques de l'illusion marchande aujourd'hui en vogue.

A l'heure où l'écrasante majorité des communications entre communautés prospères s'effectue sous forme numérique, il faut accepter que le nombre termine sa révolution secrète

[15]Nous renvoyons au beau livre de Simon Singh, *Histoire des Codes Secrets*, J.C. Lattès, 1999, pour plus de détails sur les techniques utilisées en cryptographie au cours des âges.

[16]"Le grand et puissant docteur de la Renaissance, Paracelse, en brûlant les livres savants de toute l'ancienne médecine, les grecs, les juifs et les arabes, déclare n'avoir rien appris que de la médecine populaire, des bonnes femmes, des bergers et des bourreaux ; ceux-ci étaient souvent d'habiles chirurgiens (rebouteurs d'os cassés, démis), et de bons vétérinaires." - Jules Michelet, *La Sorcière*, IX, Satan médecin. Les positions sociales ambiguës du rebouteux et de la sorcière sont magistralement illustrées, respectivement, dans les deux nouvelles *Le rebouteux* et *L'enfant* d'Octave Mirbeau (*Contes cruels*, Les Belles Lettres, 2000).

[17]"La cryptographie est un auxiliaire puissant de la tactique militaire." - Général Lewal, *Etudes de guerre*.

débutée avec la Cabale et devienne une sorte de matière première sur laquelle toute puissance politique ou économique cherche à développer son pouvoir. Le nombre est devenu aujourd'hui notre principal vecteur du secret. En pratique, le mouvement de la libéralisation des techniques de secret numérique est double. Premièrement, en protégeant mieux le secret des correspondances, c'est l'Etat qui a le plus à craindre pour sa cohésion, en permettant à des minorités de mieux s'organiser (l'internationalisation et la sécurisation des communications entre syndicats, entre opposants politiques et entre journalistes ne sont que des symptômes de la même évolution). Aucun Etat n'ayant jamais fait confiance à ses citoyens, il faut en déduire que le pouvoir, au sens des moyens de la cohésion du groupe, s'est déplacé de la sphère politique[18]. Si les techniques numériques du secret prennent un tel essor, il faut interroger le principal bénéficiaire de cette libéralisation. Il est tout de même troublant que des techniques d'ordinaire si pointues et cruciales tombent tout à coup dans l'escarcelle du public[19], même si pour déchiffrer les messages, les Etats préfèrent en général se servir de moyens détournés[20]. Deuxièmement, de nos jours, non seulement les communications sont numériques, mais beaucoup de marchandises s'échangent encore sous cette forme (les communications elles-mêmes sont d'abord et avant tout des marchandises suivant le dogme actuel). Il importe donc de protéger le nombre-marchandise, et les efforts en ce sens tendent à montrer que c'est là que s'est déplacé l'objet du pouvoir. Il réside à présent non seulement dans la maîtrise du nombre support de communication, mais aussi dorénavant dans celle du nombre support de marchandise. En quelque sorte, et à puissance de calcul constante, la longueur de clef autorisée par un Etat mesure le déplacement du pouvoir vers la sphère économique (i.e : la quantité globale d'information que l'Etat accepte de ne plus pouvoir connaître rapidement).

Les dernières années laissent présager d'une mise sous tutelle de l'internet par les Etats afin d'assurer le libre échange des marchandises, y compris et surtout numériques. Aux États-Unis, l'extension du Digital Millenium Copyright Act (DMCA) s'appelle le Super-DMCA : dans six États (Caroline du Sud, Floride, Géorgie, Alaska, Tennesse et Colorado), il est désormais illégal d'utiliser le chiffrage du courrier électronique, un pare-feu, de partager sa connexion xDSL avec un tiers, etc. car dans ce cas l'origine et le destinataire de la communication sont inconnus du fournisseur d'accès. Extrait du texte de loi du Colorado[21], partagé textuellement par les six États car issu de la MPAA[22] (Motion Picture Association of America) :

```
A person commits a violation under this section if he or she knowingly
(...) possesses, uses, manufactures, develops, assembles, distributes,
transfers, imports into this state, licenses, leases, sells, offers to
```

[18]Plus incisif, Emmanuel Todd diagnostique un néant de volonté politique dont l'incompétence économique des élites serait le fondement, voir *L'illusion économique*, Gallimard, 1998.

[19]Le fait le plus troublant ici n'est pas que des Etats permettent l'utilisation de ces techniques (ils n'autorisent que ce qu'ils savent être en mesure de déchiffrer), mais le fait que des livres et des publications sur le sujet soient si facilement accessibles.

[20]Comme par exemple le programme Carnivore du FBI qui agit comme un vers sur le réseau et envoie directement les clefs privées des utilisateurs à la NSA, voir : http ://www.fbi.gov/hq/lab/carnivore/carnivore2.htm.

[21]http ://www.leg.state.co.us/2003a/inetcbill.nsf/fsbillcont/A2F0DA113DF2BFC087256CC2006BFB94 ?Open&file=1303_ren.pdf

[22]Texte de la MPAA : http ://www.eff.org/IP/DMCA/states/sdmca_model_final.pdf

```
sell, promotes, or advertises for sale, use, or distribution any
communication device to :
- [...]
- conceal or to assist another to conceal from any communication
service provider, or from any lawful authority, the existence or place
of origin or destination of any communication that utilizes a
communication device.
```

Voilà qui n'a clairement plus rien à voir avec la protection des artistes, et investit le fournisseur d'accès de tous les droits, sans aucune contrepartie pour le consommateur qui se voit au passage dépouillé de son droit à la vie privée. Ce texte illustre comment un Etat parvient à organiser sa survie (à travers sa mission de surveillance) avec l'aide d'un acteur du monde économique : le fournisseur d'accès. Toutefois, priver les individus du secret de leurs communications se révèle en pratique aussi inefficace[23] que délétère. En France par exemple, la récente Loi sur la confiance dans l'Economie Numérique vise, entre autres, à restreindre la liberté d'expression des utilisateurs du réseau afin d'empêcher que puisse être porté atteinte à l'image des personnes morales, censées ne pas pouvoir se défendre face à des avis que pourraient exprimer des personnes physiques sur des forums ou des pages personnelles. En particulier, tout contenu jugé diffamatoire par une personne morale ou physique devra être retiré, sans jugement de justice quant au fond[24], qui devra faire l'objet d'une procédure connexe. Une autre forme d'atteinte à l'expression libre est celle plus classique des régimes autoritaires qui filtrent le contenu passant au travers de leur pare-feu national. En concurrence des agressions marchandes et autoritaires contre le premier espace d'expression libre et mondial, il est naturel de développer des outils nouveaux de communication. C'est le sens des initiatives portées par exemple par le groupe d'hacktivistes Cult of the Dead Cow[25], tant par le développement d'un réseau peer-to-peer crypté que par la mise à disposition du public d'un navigateur web avec fonctions de stéganographie intégrées[26]. Ces initiatives, loin d'être isolées, témoignent de la subtilité avec laquelle se remodèlent sous nos yeux les rapports des Etats, et des personnes morales en général, avec les individus.

Si un message crypté peut facilement être détecté et stoppé, il n'en va pas de même pour un contenu invisible. Outre les implications politiques insoupçonnées portées par les techniques abordées ici, il faut encore souligner les extraordinaires perspectives ouvertes par le tatouage, tant pour l'authentification des données multimédia dont les média sont friands que pour la libre diffusion de contenus par les particuliers. En effet, il devient pour la première fois possible de se passer des majors dans la diffusion et la rémunération des artistes[27].

[23] La CIA, qui faisait écouter les conversations privées de Ben Laden à ses visiteurs avant 2001, fait aujourd'hui pénitence : dans tout le flot de communications interceptées elle a vu passer l'annonce des attentats de septembre, mais n'a pas su faire remonter correctement l'information, lui attribuer de la valeur. Voir encore les campagnes de blocage d'Echelon par email, en ajoutant une liste de mots-clefs destinés à provoquer systématiquement un traitement par le système (terrorist, bomb, T4, white house, nuclear, etc.) en vue de saturer ses capacités dans un grand bruit de fond sémantique.

[24] Voir l'article 43-8 de la LEN, disponible sur http ://www.telecom.gouv.fr/internet/projet_len.html

[25] Extrait de la déclaration cDc : "We are hackers and free speech advocates, and we are developing technologies to challenge state-sponsored censorship of the Internet.", accessible sur http ://www.cultdeadcow.com/cDc_files/declaration.html

[26] http ://sourceforge.net/projects/camerashy

[27] Des groupes aussi talentueux (mais déjà connus !) que Public Enemy ou Smashing Pumpkins ont court-

Le tatouage pourrait être utilisé par un lecteur approprié pour établir des statistiques de popularité fonction du nombre de fois qu'un morceau est réellement joué. A l'opposé de la vision faisant de ces techniques un outil de plus dans le conditionnement des individus en purs consommateurs, se dessine la possibilité de pouvoir communiquer sûrement, de vérifier l'intégrité du contenu éditorial d'un médium, de favoriser la diversité culturelle... Sans risque de trop se méprendre, il est possible d'affirmer que la problématique de la mise à disposition du public des outils stéganographiques réside à long terme dans la mise en place de formes d'organisation sociale nouvelles[28]. Cet objectif impose de développer un système efficace de recherche, d'éducation et de culture, toutes exigences qui s'accordent mal de la censure, et qui nécessitent réciproquement de généraliser l'usage de techniques fiables d'écriture secrète chez les individus. Franklin voyait juste historiquement : on n'échange pas impunément sa liberté contre sa sécurité.

2 Positionnement de la thèse

Les techniques numériques d'écriture secrète font depuis une dizaine d'année l'objet d'une attention accrue de la part des chercheurs en traitement du signal, théorie de l'information, sécurité ou encore même en droit. En effet, profitant de l'imperfection des sens humains, il devient possible de dégager un degré de liberté dans la représentation numérique d'un contenu afin d'y cacher de l'information. La plupart des média numériques ont déjà été mis à profit pour ce style particulier d'applications : le texte, le son, l'image. Il est même possible de tatouer un programme exécutable en machine (ici, c'est la perception temporelle de l'exécution du programme que l'on exploite). Si la grande majorité des travaux dans ce domaine a porté jusqu'à présent sur l'image, le son et la video, en raison des volumes importants de ce type de média échangés sur le réseau, c'est à présent vers les prochains types de média appelés à davantage s'échanger qu'il faut se tourner : essentiellement la géométrie.

Le tatouage est aujourd'hui déjà assez vieux de ses quinze ans pour souffrir de quelques malentendus. Le plus grossier consistant à dire qu'il sera l'outil ultime pour lutter contre le piratage des contenus multimédia. Il faut tout d'abord attirer l'attention sur le fait, symptomatique, que seul a été mesuré le manque à gagner dû au piratage. Personne ne semble croire que le piratage, parce qu'il offre un accès plus large aux contenus, n'aiguise l'acuité du consommateur, et le détourne des réalisations préformatées à grands frais : cette façon d'envisager le phénomène réduit l'individu exclusivement à sa seule abstraction économique. Les majors comptent en fait surtout sur l'aspect psychologique de dissuasion offert par le tatouage. Paradoxalement, les majors ont été parmi les premières à ne pas croire à la chimère de la sécurisation totale des échanges par le tatouage. Par contre, autant les applications

circuité les chaînes de distribution classique en proposant le téléchargement d'albums depuis leur site. En outre, l'offre d'Apple avec son iStore permet de faire payer la musique sans le coût de distribution, et connaît un beau succès.

[28]"Peut-être le temps est-il très proche où l'on s'avisera que la pierre angulaire des édifices sublimes et inconditionnés que les philosophes dogmatiques se sont plus à élever n'étaient au fond que superstition populaire venue d'un temps immémorial, quelconque jeu de mot peut-être, suggestion aberrante de la grammaire, ou encore généralisation téméraire de quelques faits limités, très personnels, d'un caractère très humain, trop humain." - Nietzsche, *Par delà Bien et Mal*, Préface.

fiables de type orwellien semblent compromises, autant des applications relevant de la vérification de l'intégrité des contenus échangés restent un but parfaitement atteignable. Plus généralement, les techniques dites de *Trusted Computing* offrent aux majors une excellente garantie de confiance dans la machine cliente... mais les pirates ne tarderont pas à en profiter eux aussi pour garantir à leurs propres systèmes le même niveau de sécurité [65].

Les précédents travaux en tatouage font apparaître des verrous technologiques encore à lever avant une utilisation à grande échelle, nous aurons l'occasion de les présenter. En fait, y compris pour la géométrie, les leçons sont nombreuses à tirer des travaux en tatouage d'image. En particulier, les principaux cadres applicatifs restent les mêmes, avec leurs jeux de contraintes. D'une manière générale, nous essaierons dans ce travail de multiplier les analogies entre le tatouage de la géométrie et celui des média plus conventionnels.

Ce travail vise à explorer les différentes pistes en vue de l'implantation de techniques numériques d'écriture secrète sur un type bien particulier de médium : les surfaces maillées triangulées. En effet, il apparaît que ce type de médium sera de plus en plus utilisé à mesure que le débit du réseau permettra son acheminement et que les machines disposeront de la puissance de calcul nécessaire à son traitement. Pour l'heure, les données géométriques restent volumineuses, même si ce verrou technologique tend à s'effacer, notamment par le développement récent de méthodes efficaces de compression. En réalité, le principal écueil au traitement automatisé de ces données d'un genre particulier réside dans l'absence d'outils mathématiques adaptés aussi performants que l'analyse de Fourier ou l'analyse par ondelettes peuvent l'être sur des média classiques. Toutefois, nous montrerons que cet écueil se fait plus ou moins sentir en fonction du cadre applicatif considéré. Malgré tout, il reste évident que l'absence d'outils de traitement du signal sur des surfaces maillées reste très pénalisant pour le développement crédible de méthodes de tatouage robuste.

La plupart des travaux prenant pour objet les surfaces maillées sont à l'heure actuelle en plein essor. Qu'il s'agisse de compression, de paramétrisation, de remaillage ou d'échantillonnage, aucun de ces points pourtant cruciaux ne semble encore avoir trouvé une forme stable. Il faut donc percevoir ce travail comme un panorama de ce qui est possible dans l'état actuel des connaissances.

3 Plan du manuscript

Dans le premier chapitre, nous détaillerons les différents cadres applicatifs dans lesquels les techniques numériques d'écriture secrète sont les plus adaptées. Nous en profiterons pour clarifier notre lexique, mentionner quelques principes de base en sécurité, et présenter les principales techniques utilisées tant à l'incrustation qu'à l'extraction de l'information cachée. Il s'agit d'une introduction sous l'angle systémique du tatouage. Nous présenterons aussi les différents types d'attaque possible sur un tatouage, et nous donnerons enfin une typologie des stéganalystes et de leurs moyens.

Le deuxième chapitre sera l'occasion de présenter les principales représentations de l'information tridimensionnelle : nuages de points, NURBS, maillages surfacique et volumique. Nous expliquerons pourquoi nous avons voulu consacrer ce travail aux maillages surfaciques triangulés. Puis, nous préciserons les spécificités de l'information surfacique maillée, et ses répercussions sur les stratégies de tatouage à mettre en œuvre dans l'état actuel des connais-

sances. Nous définirons quelques termes de topologie et nous présenterons la relation d'Euler, essentiellement afin de préciser le type d'objets maillés que nous pourrons traiter. En particulier, nous nous attacherons à montrer comment représenter en mémoire un maillage suivant ses propriétés topologiques, comment on peut comparer deux tels maillages, et nous préciserons les premières observations dont il faudra tenir compte pour élaborer une méthode de tatouage sur ces objets.

Les traitements pouvant être appliqués à une structure maillée surfacique diffèrent sensiblement de ceux concernant les types plus classiques de données. Nous présenterons notamment en détails trois grands schémas de compression de l'information géométrique surfacique, puis nous procéderons à l'inventaire des manipulations possibles, suivant qu'elles modifient ou non la structure sur laquelle est représentée l'information géométrique. Cette liste, non exhaustive car en constante évolution, sera l'objet du troisième chapitre. Nous avons souhaité réserver une place à part pour le codage de source car nous trouverons là l'occasion de présenter divers parcours du maillage, et il sera utile de les avoir à l'esprit pour comprendre comment en tirer parti afin d'optimiser le nombre de sites pouvant être tatoués. Au fil des manipulations présentées, nous tenterons de les classer de manière économique : suivant qu'un pirate y a un accès plus ou moins facile.

C'est alors seulement que nous serons en mesure de présenter dans le quatrième chapitre les méthodes de tatouage existantes pour les surfaces maillées. Nous distinguerons tout d'abord les méthodes spatiales des méthodes mettant en jeu un espace de tatouage plus complexe. Les méthodes utilisant un espace de tatouage complexe sont souvent fondées sur une représentation bien particulière du maillage (décomposition spectrale, *progressive mesh*, etc.) Nous passerons brièvement sur le détail de la représentation (sauf pour la décomposition spectrale), pour saisir les grandes options retenues par les concepteurs des méthodes de tatouage. En nous intéressant aux méthodes spatiales, nous isolerons plus particulièrement les méthodes dites à configuration géométrique. Pour ces méthodes, nous nous attarderons sur la notion importante d'arrangement de l'information cachée, et nous en préciserons les trois types possibles. Nous donnerons une analogie avec le tatouage d'image pour les deux premiers types, mais le troisième demeure propre aux maillages (nous aurons toutefois l'occasion de présenter deux méthodes l'utilisant).

Dans le cinquième chapitre, nous présenterons nos travaux en tatouage par invariants géométriques, avec des applications possibles en stéganographie et en authentification. A cette occasion, les trois types d'arrangement de l'information cachée seront séparément mis à profit. Nous serons alors en mesure de les associer à des cadres applicatifs particuliers. En particulier, nous commencerons par présenter chaque méthode de tatouage (pour la stéganographie et l'authentification) avec son parcours naïf du maillage correspondant. Puis, nous donnerons un algorithme de parcours du maillage qui optimise le nombre de sites tatouables auxquels on peut accéder. Nous expliciterons alors les modifications minimes induites par l'utilisation du parcours optimal, et les options que nous avons retenues pour prouver l'efficacité de notre méthode. Dans le cas de la stéganographie, nous pourrons garantir une borne sur la capacité (proportionnelle au nombre de sites tatouables pouvant être accédés) et sur la distortion introduite dans le maillage. Dans le cas de l'authentification, nous saurons optimiser la répétition du message sur le maillage en cachant un bit par triangle dans la totalité des triangles.

Enfin, nous explorons au sixième chapitre une méthode de tatouage mettant en jeu un

espace particulier de représentation de l'information géométrique : celui de la décomposition spectrale de la géométrie. Cet espace nous a semblé propice à l'élaboration de méthodes de tatouage plus robustes. Nous présenterons en détails comment parvenir à une telle décomposition. Pour cela, nous introduirons en préliminaire la notion de paramétrisation, et nous illustrerons avec la paramétrisation harmonique de Tutte, que nous avons retenue. Nous aurons également besoin de définir un opérateur laplacien (topologique) sur le graphe de connexité du maillage, nous en donnerons différentes variantes suivant le calcul de leurs poids. Nous serons alors en mesure de définir la décomposition spectrale. Nous pourrons alors établir la distinction entre bases de décompositon fixe et optimale. Pour des raisons de temps de calcul et de relative indépendance vis à vis de la topologie du maillage, nous verrons en quoi l'implantation de telles méthodes fondées sur la décomposition spectrale nécessite de partitionner le maillage en disque topologiques "augmentés" jusqu'à contenir tous le même nombre de points. Nous avons développé une alternative à la méthode d'augmentation classique, qui autorise un recouvrement entre les disques (nous montrerons au passage l'amélioration apportée par notre méthode d'augmentation dans l'optique d'une transmission progressive de la géométrie). Enfin, nous exposerons notre méthode de tatouage dont nous présenterons les performances face à l'attaque de compression spectrale et diverses autres attaques.