

Anthologie de textes sur le secret

Publiés sur le site de F.B. Huyghe

Neuf clefs du secret



1. Nous vivons dans une société du secret

Premier constat : à rebours des discours contemporains sur la société du savoir et sur la transparence, il n'y a pas de société sans secret. Il est le contrepoint de la confiance et de l'interdépendance entre les membres du groupe, comme le conflit est celui de la coopération.

Dans le domaine politique, le secret s'est toujours manifesté sous forme de la dissimulation des crimes de l'État (le cas extrême est l'État totalitaire qui impose le silence sur ses crimes), de la feinte stratégique (cacher ses desseins, s'avancer à couvert, font partie des premières règles politiques) ou encore de la rétention de connaissances (conserver l'exclusivité d'un procédé technique) ou encore de la production délibérée d'incertitude pour troubler l'adversaire ou le citoyen (cacher ce que l'on sait, laisser chacun dans l'ignorance de ce que l'État sait de lui, paralyser les initiatives adverses). L'économie, dans la mesure où elle est affaire de rareté, repose souvent sur le monopole de procédés techniques ou simplement sur une meilleure connaissance que le concurrent de données cruciales.

Le fait que nous adhérons à une idéologie démocratique de la transparence ou qu'il existe des moyens de savoir plus accessibles au citoyen, ne change rien à l'affaire. Plus la technologie progresse, plus les secrets prolifèrent. Leur histoire est l'envers de l'histoire des inventions, la rançon oubliée des progrès de la rationalité et des connaissances. Aujourd'hui la puissance technique et économique repose avant tout sur la possession (donc la protection) de savoirs, sur le contrôle des flux d'informations. La désirabilité du secret s'accroît (ainsi le nombre d'informations qu'une entreprise peut avoir intérêt à conserver pour elle-même augmente).

La multiplication des transmissions et transactions numériques jouent dans le même sens. Seul le secret peut garantir l'identité d'un acteur, l'authenticité, l'intégrité et la confidentialité des échanges. Ainsi, le code personnel ou le mot de passe est souvent notre seule garantie (toute relative) contre toutes sortes de dommages qui vont du viol de notre intimité à une substitution d'identité.

Un des rôles cruciaux du politique devient de contrôler, les moyens et degrés d'accès au secret : cela vaut des systèmes de surveillance planétaires de type Echelon aux bases de données sur les citoyens. Le politique gère son propre secret (le fameux secret d'État), alloue du secret (secret des bases de données, secret déontologique, secret lié à la vie privée, secret des transactions, limites de la traçabilité et de la transparence...) et se dote de moyens de violer le secret (pour lutter contre le crime et le terrorisme, par exemple). Enfin il doit résoudre la contradiction entre la demande de secret au nom de la liberté (celle de l'individu) et d'autres demandes (sécurité, moralité, transparence).

Résultat : nous vivons désormais bardés de codes, obsédés de confidentialité, menacés par toutes sortes de délits d'information ou d'outils de fichage. Comme citoyens nous haïssons le secret (celui de l'État, ce que nous cachent les puissants, ce que nous taisent les médias...), comme particuliers nous le réclamons : nous ne voulons plus être filmés, écoutés, décryptés...

2. Le secret n'est ni le mystère, ni l'intime

Secret et mystère ont certes en commun le fait de cacher et d'être opaque. Dans le mystère c'est la vérité qui est inaccessible soit en raison de sa nature même (religieuse par exemple) soit du fait de nos faibles moyens de connaissance. Contrairement au mystère, le secret est déchiffrable, intelligible. Il n'est pas révélé mais il pourrait bien l'être : c'est par la volonté de quelqu'un ou d'un groupe qu'il n'est pas divulgué

Quant à l'intimité, elle suppose la distinction entre un domaine privé, intime, où nul n'a le droit d'aller voir (fut ce le nom secret ou les parties cachées du corps) et un domaine public où l'on s'affiche et se fait connaître, voire où l'on entre en compétition pour être davantage remarqué. Il va de soi que leurs frontières varient considérablement. On ne révèle pas son intimité pareillement à l'heure du roman épistolaire comme les Liaisons dangereuses ou à l'heure de la téléxhibition ou des millions de blogs. La protection de l'intimité peut mobiliser les techniques du secret mais les deux notions restent distinctes.

3. La valeur du secret repose sur la puissance, la rareté et la protection

Le secret est précieux par :

- la puissance qu'il confère (stratégique, politique...),
- la rareté des connaissances qu'il recouvre (économique, technique...),
- la protection qu'il assure à son détenteur (domaine privé, impunité...).

Il peut porter

sur le passé (qui a fait quoi),

sur le futur, un plan, un traité, une conspiration (qui fera quoi)

ou sur un présent virtuel (comment faire quoi) : c'est le cas des procédés qui permettent de rééditer une performance, comme un brevet, un procédé, un logiciel, un plan de machine et dont on a tout intérêt à conserver l'exclusivité.

Le secret est une arme, un enjeu, une protection, un rapport de force, un pouvoir latent. C'est un processus menacé et maintenu à grand effort. Sa définition la plus cohérente est : " une information que son détenteur rend délibérément inaccessible. " Mais à qui et pour combien de temps ?

4. Pour qu'un secret existe, il faut des initiés et des ennemis

La publicité d'un secret est une notion relative. Il y a toujours des "initiés" : ce peuvent être des conspirateurs qui ont juré silence sur leur vie, mais aussi le Tout-Paris médiatique qui se répète dans les dîners en ville quelques confidences qui n'aboutiront pas dans les journaux. À l'inverse, il existe des informations parfaitement disponibles mais si discrètement diffusées par rapport à leur gravité que cela équivaut presque à un secret. L'étouffement de l'information significative ou dérangeante sous le flux de ce que les médias répètent et signalent comme débat, événement, fait de société, question " qui nous interpelle ", est infiniment plus efficace que toute forme de censure.

Le secret est, étymologiquement, ce qui est séparé, mis à part (du verbe latin *secernere*). Or qui dit séparation dit frontières. Et qui dit frontières dit conflit. Dans tous les cas quelqu'un a une raison de vouloir s'emparer du secret. Ce peut être l'adversaire, le concurrent, le représentant de la loi...). Un autre à une raison de défendre ce secret. L'histoire du secret est une histoire d'épée et de bouclier... Il n'y a donc pas de secret sans ennemi.

5. Le secret est affaire de mémoire, de flux, de codes et de clés

L'histoire du secret dépend de celle des moyens physiques de transmission des biens symboliques, donc des technologies d'une époque [2]. Une idée, un savoir, pour vaincre le temps (se conserver) ou l'espace (atteindre son destinataire) requiert un support matériel, mais aussi un traitement, une mise en ordre, donc un code (fut-ce par le simple code de la langue naturelle). Encoder, qu'il s'agisse de transmettre ou de dissimuler, consiste à ordonner des éléments physiques capables d'emprunter un canal et correspondant à des représentations mentales. Les signaux physiques en question peuvent être des sons, des lettres, un dessin, un vêtement, etc... Ils déterminent un répertoire et une combinatoire.

Autrefois avoir un secret, c'était avoir le monopole d'une information vraie (ou que l'on croyait telle). Désormais conserver un secret, c'est aussi l'accès à ses bases de données, s'assurer contre le risque de l'intoxication, de la fausse information ou de l'information désorganisatrice ou nocive par exemple contre les virus informatiques ou les sabotages via Internet. C'est enfin s'assurer de la non-propagation d'une information nocive, contrôler des passages et des flux, plutôt que connaître des contenus.

6. La lutte pour le secret : une guerre du sens et de la puissance

Une guerre sans fin oppose codeur et décodeur, cryptologue et cryptanalyste, camouflage et repérage, l'art sophistiqué de compliquer la forme du message, et l'analyse subtile des indices et ressemblances. Bien avant la mécanisation du cryptage puis l'informatisation, les hommes ont pratiqué ce mode de communication secrète connu sous le nom barbare de

stéganographie et qui consiste à dissimuler le support du message. Par exemple, les chinois écrivaient leur message sur une fine soie qui était ensuite glissée dans une petite boule de cire que le porteur avalait ! Voir aussi l'encre sympathique. Mais la stéganographie et ses ruses ont une limite : si le message est découvert, son contenu apparaît clairement. D'où le développement parallèle de la cryptographie dont le but est de dissimuler le sens du message [3].

La protection du secret ne repose pas seulement sur le silence des acteurs, les barrières physiques, clefs, gardes ou coffres, ni la dissimulation d'un objet, mais aussi sur des moyens sémantiques, des techniques sophistiquées d'identification, de contrôle d'accès, sur le chiffre et la cryptologie. Garder une chose, cacher un sens. Toutes ces notions prennent une nouvelle dimension avec l'informatique : le codage est désormais délégué à des puces et logiciels et les éléments du texte clair deviennent des séries de 0 et de 1 qui, elles-mêmes, sont comme "brassées" suivant un ordre. La capacité de briser (ou de préserver) de tels n'a plus rien à voir avec l'ingéniosité, mais repose sur la puissance informatique, sur une notion de nombre de tentatives. Garder ou découvrir un secret devient un problème de force de calcul comme gagner une guerre est une question de puissance de feu... et de temps.

7. Qui dit secret dit temps

La National Security Agency américaine (NSA), dont on dit que c'est le premier employeur de mathématiciens au monde, pourrait casser n'importe quel clé. Une simple question de délai... Il n'est point de secret que le temps ne révèle [4]. Mais la valeur du secret est relative dans le temps : avoir un secret c'est savoir avant et savoir pour quelque temps. L'information est du temps concentré (un procédé qui permet d'économiser du temps et des ressources pour obtenir un résultat). Le secret est du temps garanti... la puissance ne fait pas tout.

La disponibilité est une facette essentielle de la lutte pour et autour du secret : elle renvoie à la possibilité concrète d'accéder à un système ou une base où résident des informations. Internet offre des moyens de pénétrer dans des mémoires de tout point. L'espace ne semble plus un obstacle, ni le temps : le violeur de secrets peut agir en temps réel mais aussi à retardement comme le font les "chevaux de Troie" introduits dans les systèmes informatiques pour en prendre le contrôle ultérieurement. L'identité de l'attaquant est assez bien protégée. Du coup, se développent de catégories inattendues d'agresseurs, agissant à faible risque, soit par goût de l'exploit gratuit (hackers), ou par ressentiment et goût du vandalisme (crackers).

8. L'information protège de l'information

L'effraction informatique est invisible et indolore et la pénétration immatérielle : parfois la victime ne réalisera jamais que le secret a été violé. Ou, dans le cas de marquage, de "chips"

etc. elle ignorera qu'il existe un moyen de reconstituer ses activités : il subsiste toujours une trace de tout ce que l'on a reçu et émis, un indice de tous ses mouvements physiques ou virtuels (connexions). Ceci fonctionne dans les deux sens : "prélèvement" d'informations, mais aussi pénétration. Cookies, chevaux de Troie, virus, bombes à retardement, etc. introduisent frauduleusement des machines de guerre (qui opèrent destruction, désorganisation, falsification, etc.) et des machines de contrôle (qui permettront de prélever de l'information ou d'exécuter des instructions) dans les systèmes informatiques. Corollairement, les techniques de défense changent. D'une part, il ne faut pas laisser de points de passages aux signaux hostiles. D'autre part, il faut discriminer ces signaux, faire en sorte que l'information protège contre l'information. Dans le monde virtuel plus que dans le réel, distinguer l'ami de l'ennemi devient un problème crucial et plus seulement pour les soldats.

De là découle le caractère crucial de l'identification (authentification et signature). L'impératif du "prouve qui tu es" forme le pendant de la revendication d'anonymat du citoyen. La valeur probante du document numérique et de la signature électronique soulève des questions de liberté publique autant que d'économie. En l'absence physique de l'individu accrédité, reste à faire appel à l'emploi de symboles : prouver que l'on sait A, pour démontrer que l'on est X et avoir le droit de savoir B ou de pénétrer (numériquement) en Y. Le tout en laissant une signature, une empreinte, une preuve de son passage.

9. Le secret dépend des médiasphères

Qu'on l'examine sous ses trois aspects de publicité, de disponibilité et de lisibilité, le secret a changé de statut : pour le garder, il ne suffit plus de se taire, pour le vaincre, il faut bien davantage que des indicateurs ou des espions.

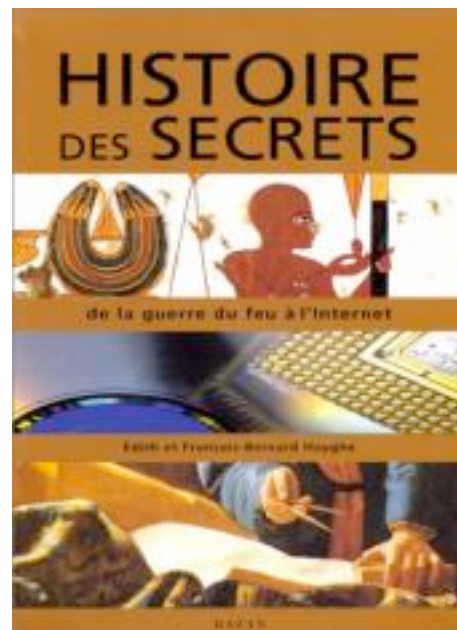
Maîtrise du secret et viol du secret reflètent un rapport de force militaire, politique, économique, technique et idéologique. Il se pourrait que la puissance se confonde désormais avec la faculté de savoir ou de dissimuler et que la part du secret s'accroisse à mesure que les techniques dites de l'intelligence et de la connaissance prédomine.

Histoire des secrets

Edith et F.B. Huyghe

Editeur : Hazan 2000

Dans la société dite de l'information, nombre de secrets, ceux des brevets, des logiciels, des inventions, ceux que traquent l'intelligence économique et l'espionnage industriel ont acquis une valeur immense. Le secret devient une revendication des simples citoyens, soucieux de défendre leur sphère privée, inquiets des systèmes de surveillance et de fichage qui se développent, souci quelque peu contradictoire avec une exigence croissante de protection des mêmes citoyens. Quant à l'État il n'a plus seulement à dissimuler quelques traités compromettants, quelques armes de pointe ou quelques vilénies de ses espions ou de ses sbires : ce sont des millions de documents que tout État démocratique doit garder secrets pour des raisons stratégiques, économiques, techniques ou de libertés publiques. Le tout sur fond de technologies de la communication qui permettent la pénétration clandestine voire la falsification de millions de données, communications, connections, archives...



Raison de plus pour vouloir comprendre ce que fut l'histoire des secrets. Elle est l'envers de l'histoire des inventions, la rançon oubliée de l'histoire des progrès de la communication et des connaissances. Les matières et les objets les plus familiers et les plus anciens, papier, soie, miroir, porcelaine, etc. furent, parfois pendant des siècles, porteurs de mystères, celui de leur origine, de leur fabrication, de leur utilisation. Il s'ensuit des aventures étonnantes : explorations, guerres, vols, espionnage. Et des révolutions : quand Byzance a su cultiver le ver à soie, les Portugais dessiner la forme du Cap de Bonne Espérance ou Gutenberg imprimer des caractères mobiles sur une feuille de papier, l'histoire a changé.

Secret et conflit : de la ruse à l'infodominance

(extrait de « Autour des secrets » colloque du Forum de Nancy)



Partons de l'idée que le secret est une information que son détenteur rend délibérément inaccessible. D'où une relation duale et dramatique. L'essence du secret, à suivre l'étymologie (secernere) est d'être séparé, exclu. Or, une telle opération ne se fait pas sans travail ni résistance, sans peine ni opposition. Qui a un secret a nécessairement un adversaire, fut-il virtuel : au mieux ou au pire, celui qui menacerait ledit secret s'il venait à en apprendre l'existence. Cet adversaire, ce peut aussi être soi-même : c'est du moins ce que la psychanalyse nous enseigne : nos secrets nous menacent et nous les menaçons. Nous défendrons ici une conception du secret qui en fait une des formes, des causes et des instruments du conflit, au moins autant qu'un moyen de l'éviter. Le secret serait donc justiciable d'une approche polémologique (comment se produit le conflit), stratégique (comment les acteurs emploient force et intelligence à défendre et attaquer le secret) d'une histoire des techniques (avec quels moyens) et, on s'en doute, d'une médiologie, puisqu'il est ici question de ce que nous croyons et de la façon dont nous les transmettons ou pas.

Le secret ne constitue pas seulement un facteur discriminant entre ceux qui le possèdent et ceux qui en sont exclus. Ni une simple composante du pouvoir et par l'imprévisibilité qu'il confère et par le prestige qu'il confère. C'est un processus qui pourrait bien être faire partie des universaux anthropologiques. Le secret serait à ranger parmi les « propres de l'homme », comme la technique, le langage, l'organisation politique, auxquels il est toujours lié. Tous les hommes ont des secrets et nous serions tentés de dire qu'aucun animal n'en a, pas plus qu'il ne peut mentir. Certes, avec son corps, il peut réaliser des ruses et des feintes, cacher ce qu'il veut protéger, s'abstenir d'émettre des signaux, faire le mort, il peut en quelque sorte « être » secret. Mais, pas plus qu'il ne peut exprimer une information imaginaire, il ne peut conserver ou dissimuler un énoncé. Avoir un secret, c'est-à-dire pouvoir le conserver, le refuser à tel, mais le livrer à tel autre, le partager ou le négocier, tout cela suppose des capacités culturelles.

Avec raison Simmel fait du secret le contrepoint de l'interdépendance et de la confiance nécessaire dans tout groupe humain, comme il voit dans le conflit la rançon de la coopération. Pas de société sans secret. Il est présent, en puissance, derrière tout ce qui nous réunit : la croyance, la politique, la production. Mais, en même temps, sa forme et son ampleur dépendent de facteurs historiques et technologiques.

Le secret peut porter sur le passé (qui a fait quoi), sur le futur, un plan, un traité, une conspiration (qui fera quoi) ou sur un présent virtuel (comment faire quoi) : c'est le cas des procédés qui permettent de rééditer une performance, comme un brevet, un logiciel, un plan. Mais surtout, il traverse tous les domaines de notre activité.

Des initiations sacrées aux arcanes de la puissance

Ainsi, il hante le sacré, dont le domaine déborde celui de religion, notion occidentale tardive. Des rites magiques aux théologies monothéistes en passant par les cultes à Mystères, il subsiste partout une forme quelconque d'initiation. Suivant une tendance peut-être générale, tout enseignement conférant des pouvoirs ou un statut, comme celui du jeune chasseur, du myste, de l'acousmate, ne saurait se dispenser sans rites, épreuves et serments de mutisme, menaces. La transmission doit être réservée à un impétrant spirituellement préparé et fiable. Faute de quoi la connaissance folle ou dangereuse serait profanée.

Ce secret rituel ou spirituel relie les initiés qu'ils cherchent l'art de chasser le bison, le salut de leur âme, les moyens de fabriquer la pierre philosophale ou les desseins du grand Architecte. Souvent, une forêt de symboles, un enchevêtrement d'indices ou d'arcanes sont censés protéger le secret des dieux ou du Cosmos. Sous des formes différentes, les trois monothéismes connaissent la tentation ésotérique voire gnostique : réinterpréter l'écriture sacrée ou la Création comme un cryptogramme. Entre l'initiation, qui consiste à maîtriser la transmission pour protéger la vérité, et l'ésotérisme qui suppose un sens dissimulé derrière le sens apparent, le sacré est toujours entouré de défenses.

Ce n'est pas moins vrai pour l'économie. Le secret est un moyen de produire de la rareté, donc d'augmenter ou de conserver une valeur. Cette rareté peut être celle des moyens. Garder l'exclusivité d'une technique, de l'emplacement d'une ressource, en constitue la forme la plus évidente. Il y a avantage à se réserver l'accès ou la fabrication de richesses. Ce fut vrai, des siècles durant, pour des matériaux ou des objets : soie, verre, épices, poudre, papier, porcelaine ont, suivant les périodes, fait la fortune de leurs détenteurs exclusifs. À l'époque industrielle, la formule du coca-cola ou tout autre secret protégé par des brevets ou des coffres-forts ont constitué un capital inestimable. C'est encore plus vrai avec la dématérialisation de l'économie. Quand celle-ci consiste toujours davantage à « vendre » de la connaissance ou des états de conscience, , comme actuellement, le secret devient la seule protection contre la duplication, facilitée par le numérique, et le seul remède contre l'obsession du piratage ou de la déstabilisation. Il devient le garant invisible d'un capital intangible.

L'instrument de l'échange lui-même, l'argent, suppose un secret, puisqu'il faut bien qu'une autorité ait le monopole de sa formule et nous préserve de sa prolifération. Ceci peut s'obtenir par un identifiant, tel le filigrane d'un billet qui résiste à l'imitation. Un système bancaire ou financier est une machine à gérer du secret, celui des comptes bancaires ou des transactions électroniques. Désormais, des méthodes sophistiquées combinant cryptographie et moyens de surveillance assurent que le paiement émane bien de un tel est bien valable sans dévoiler pour autant la nature de la transaction, ni celle des moyens de certification. Demain le moyen de sécuriser l'échange peut aussi être « biométrique ». L'identification à distance repose sur des techniques de mesure de nos impulsions nerveuses, d'identification de l'iris de notre œil ou de notre voix, de transmission et vérification de nos empreintes digitales ou tous les autres procédés qui recourent à ce code secret oublié : notre code génétique.

Il est un domaine de l'activité humaine dont le rapport avec le secret est essentiel : le politique. Le politique est une activité conflictuelle opposant des groupes poursuivant des finalités inconciliables. Il recourt tout naturellement au secret quand il s'agit de surprendre et protéger. Des conspirateurs qui se dissimulent, une censure qui recèle des documents, une police secrète, d'autant plus efficace que les citoyens en ignorent les pouvoirs effectifs et les crimes réels, forment trois manifestations d'une seule logique. Elle vise à la conservation d'un avantage contre l'adversaire actuel ou potentiel, voire contre le peuple pour l'empêcher de s'indigner et se révolter. Il faut dissimuler l'inavouable, cacher ses fins être imprévisible, impressionner ceux qui ignorent la source et l'étendue de ses pouvoirs, se réserver la connaissance des moyens efficaces. Ces principes-là sont immémoriaux.

Des siècles avant notre ère, les philosophes chinois de l'école des « légistes » exaltaient déjà la nécessité politique du secret :

Quand « Le Prince a perdu son mystère/ Des tigres s'attachent à ses pas » avertissait le livre de Han Fei .

Ce classique chinois fait l'éloge de qui «ne révèle point ses ressorts». Notre propre tradition philosophique n'ignore pas l'efficacité de la ruse, depuis que les Grecs exaltent la Métiis, ni ne néglige l'art de cacher pour surprendre.

A la Renaissance, la pensée politique européenne fait du secret une vertu une qualité de l'homme d'exception. Ce caractère rend son possesseur plus redoutable (« Qui ne sait dissimuler ne sait régner » disait Louis XI). Savoir surprendre est une des aptitudes du Prince. Le secret se rattache aux « arcanes », méthodes occultes du souverain, arme d'exception répondant à des fins exceptionnelles. Les *arcana Republicæ* puissances dissimulées au sein de l'État, les *arcana dominandi*, méthodes pour manipuler le peuple ou l'opinion, les *arcana belli* techniques guerrières constituent une panoplie. Le jésuite Gracian exaltera pareillement le secret « sceau de la capacité » politique car « C'est la marque d'une supérieure maîtrise de soi et se vaincre en cela est un triomphe véritable."

Mais le secret politique devient vite plus trivial voire bureaucratique. Dans les sociétés modernes, il se gère en masse et au quotidien. Généralement, il suppose un méta-secret : le secret de ce qui est secret dans un certain ordre politique. L'instance politique détermine, au moins dans l'abstrait, la forme et l'intensité du conflit sur son territoire. De la même façon, elle contrôle droit du secret et droit au secret là où elle est souveraine. Elle l'alloue ou l'autorise à certains – secrets de l'intimité, de la vie privée – elle l'impose à d'autres - secret défense ou secret d'État, secret professionnel. Elle en contrôle les instruments. C'est ce que démontre l'interdiction faite aux citoyens de posséder ou d'exporter des logiciels de cryptologie trop puissants, au même titre que des armes de guerre . Dans nos systèmes, l'État dessine les territoires du secret sous forme d'un triagle : secret des citoyens entre eux, secret de l'État à l'égard les citoyens et celui des citoyens face à l'État. Dans tous les cas, il s'agit de tracer la frontière entre une connaissance licite (et le cercle des initiés peut être fort

vaste) et sa diffusion nocive parce que contraire aux intérêts généraux, aux règles déontologiques, aux droits des individus, au moral de la population, etc.

Le régime le plus démocratique suppose de tels droits au secret, ne serait-ce que celui du vote ou de la correspondance. Ils protègent la vie privée et l'exercice de la pensée libre. Il limite la connaissance que les individus peuvent acquérir sur leurs vies respectives pour en rendre la cohabitation supportable. Enfin, ce même système démocratique ne peut totalement renoncer à son propre secret, pour conserver sa liberté d'action : procédés, fonds, services, traités secrets, et autres attributs d'une raison d'État échappent au droit ordinaire. Quant aux États totalitaires, le secret leur est consubstantiel : chacun se méfie de l'autre, personne n'ose dire à haute voix des vérités connues de tous, des « secrets ouverts ». Il se rend ainsi complice du silence général et renforce le pouvoir qui le surveille. Il se peut que celui-ci occulte des pans entiers de réalité la plus évidente : l'existence du Goulag, ou celle des villes stratégiques dites secrètes, non photographiées, non mentionnées sur les cartes, en ex-U.R. S.S.

Secret dans la transparence

Mais aujourd'hui ? Revenons sur cette notion ressassée selon laquelle notre société serait de l'information. Société du Savoir pour les optimistes : la connexion des intelligences et le partage des connaissances rendront désuète toute politique de rétention de l'information. Société du spectacle, pour les critiques : nous nous épuisons à poursuivre et consommer des signes, esclaves des apparences. Pour Guy Debord "Le secret généralisé se tient derrière le spectacle, comme le complément décisif de ce qu'il montre et, si l'on descend au fond des choses, comme sa plus importante opération." Et le père du situationnisme d'énumérer les traits principaux de nos modernes sociétés du spectacle : renouvellement technologique incessant, fusion économique étatique, secret généralisé, faux sans réplique, présent perpétuel.

Société de l'exhibition, peut-être : à l'ère de loft story, des Web cams, des psyshows, chacun, de l'homme politique au manager branché, dévoile sa personnalité voire son intimité. Histoire d'être « star un quart d'heure », de « changer le regard des autres » ou « d'être visible », on montre tout : âme, fesses et confesse.

Certains y trouvent des raisons d'optimisme. Les juges et les caméras pourchassent les mystères. Internet se moque des censures et des frontières. Les hommes politiques promettent plus de clarté et moins de langue de bois. De la transparence dans la politique, nous passons à la transparence de la politique. Elle devient l'art d'exprimer et satisfaire des « demandes ». L'entreprise se veut communicante, éthique et ouverte. La vie privée fait le succès public. Quelle place pour l'archaïque secret ? Baudrillard répond : « Que deviennent les choses jadis secrètes ? Elles deviennent occultes, clandestines, maléfiques : ce qui était simplement secret, c'est-à-dire donné à s'échanger dans le secret, devient le mal et doit être aboli, exterminé. »

Les forces dominantes semblent bien sonner le glas du secret :

- La Mondialisation : elle fait circuler choses, gens, idées, images
- Le Marché : il suppose l'échange généralisé
- Les Médias : les médias de masse mettent tout sur la place publique du village global ; les nouveaux médias informatiques offrent toutes les données « où je veux, quand je veux, comme je veux »
- La Morale ou plutôt le Moralisme triomphe : contre les systèmes autoritaires, les lois du silence ou les discriminations, il se réclame des différences et des transparences, du débat public, de la libre expression.

Pourtant, il semblerait, sinon que le secret soit partout -et la vérité ailleurs, comme le proclame X-Files - du moins que la lutte par, pour et contre le secret s'étende . Les indices pullulent : événements étouffés, données sensibles dissimulées.

Le secret suscite des politiques de rétention, surveillance, dissimulation, pénétration, tromperie impliquant des acteurs étatiques et infra-étatiques, économiques et idéologiques, des groupes et des particuliers. Quelques indices :

- Le nombre de documents classifiés (des millions !) augmente ,
- Les révélations vraies ou fausses sur diverses formes d'Omerta dans nos sociétés : agissements de pédophiles, turpides financières des partis politiques ou divers scandales de type épidémies agro-alimentaires,
- Les fameuses « grandes oreilles » de la National Security Agency, qui, soit dit en passant, ont fait négliger la formidable montée en puissance de la N.R.O., National Recognition Organisation, les « yeux » des satellites espions ,
- Les luttes quotidiennes des internautes pour le droit de crypter, contre le traçage, et le fichage, pour la protection de la vie privée
- La place dans les doctrines militaires et géostratégiques de notions comme la domination informationnelle, la panoptisme, ou l'intelligence totale, via le cyberspace et l'espace stratosphérique .
- Les affaires d'infoguerre économique : elles se résument généralement à des affaires de vrais secrets violés ou de faux secrets révélés pour déstabiliser .

Alors, vrai ou faux ? Ou alors, bon secret, celui du citoyen, ultime refuge de la liberté versus mauvais secret, celui du Système, de Big Brother qui, pour recourir au contrôle invisible plutôt qu'à la violence visible, n'en serait pas moins redoutable ?

Pour répondre, il faut en revenir à la définition du secret comme conflit : à l'idée que le secret est secret contre quelqu'un dont il faut se protéger et qui représente un concurrent ou une menace.

Tout confirme cette parenté entre secret et conflit que ce soit comme enjeu (lutte pour connaître le secret ou le défendre), comme arme (la dissimulation des moyens ou des objectifs pour mener l'offensive) ou enfin comme mode d'évitement du conflit (en cachant à l'autre sa faute ou sa faiblesse). Le secret est une relation agonale, où les objectifs de

chacun des camps sont incompatibles. Chacun s'efforce de vaincre la résistance de l'autre, passivement ou activement. Interdire de faire par l'usage de la force, (y compris sous la forme extrême qui consiste à éliminer l'autre), et interdire de savoir par l'usage d'informations, (dont évidemment le secret), sont, au final, deux manifestations d'un même dessein.

Un secret pour personne n'existe pas, sinon sous la forme plaisante du secret de Polichinelle. Un secret caché à tous, sans détenteur, est une contradiction dans les termes. Un secret sans objet est apparence ou farce. N'étant ni l'invisible, ni l'ineffable, ni l'incompréhensible, ni l'inconnu même s'il en adopte les apparences, le secret n'est pas non plus le mystère. Le mystère émane de choses qui échappent, et, peut-être, échapperont toujours à notre intelligence. Le secret suppose des gens qui possèdent une information et ne la laissent pas connaître à d'autres. Il doit être connu d'au moins une personne et caché à une autre. Il doit, pouvoir s'énoncer sous forme de description d'une réalité vraie ou fausse. Qu'il porte sur une information imaginaire ou délirante n'en change pas la nature.

Bref, si pour qu'il y ait secret, il faut qu'il y ait risque réel ou imaginaire, sa connaissance se trouver valorisée. Valorisé négativement quand sa perte entraînerait un dommage, le secret peut l'être positivement : celui qui est seul à détenir l'information, réalise des performances propres ou, plus simplement, vend son information rare. Mais même cette valeur positive renvoie toujours au risque de perte. Le secret ne vaut que tant qu'il est contrôlé et que l'on sait qui sait. Il suppose nécessairement une crainte : crainte d'un événement (si on savait mon secret, je serais arrêté, par exemple), d'un jugement (je serais disqualifié aux yeux de l'opinion) ou de la perte d'une exclusivité (je ne serais plus le seul à pouvoir faire ceci). Il sous-entend antagonisme au moins potentiel envers un adversaire concret ou envers une force abstraite Loi, Opinion, Société. Le secret garantit immunité, exclusivité ou supériorité.

Cette trilogie détenteur-contenu-menace, appelle un quatrième élément : la protection. Il faut des moyens matériels pour maintenir ce rapport délibéré et asymétrique. Il se peut que l'existence même du secret soit ignorée, qu'il n'en existe ni indice ni soupçon et seul le détenteur puisse le trahir et se trahir par un aveu. Dans ce cas limite, la situation est simple : le silence suffit. Il faudrait alors parler d'une stratégie d'abstention : ne pas dire, ne pas trahir, agir sur soi, ne pas laisser filtrer d'indice. Mais cette stratégie appelle vite des compléments : stratégies de rétention, contrainte, ou confusion. Elles agissent sur les choses qu'elles cachent, sur les gens qu'elles empêchent de savoir ou de faire savoir et enfin sur les signes qu'elles brouillent.

Technologies de la dissimulation

Souvent donc, le secret requiert des manœuvres complexes : dissimulation ou protection de traces physiques -enfermer un document dans un coffre, interdire une zone d'accès- ou dissimulation des signes et signaux -chiffrement, stéganographie ou tactiques de déception-. Enfin, il y a la contrainte pure et simple. Elle peut consister en une menace, celle des foudres de la loi, des lois de l'honneur de l'omerta maffieuse ou de la colère divine.

Le secret repose autant sur des moyens techniques de maîtriser traces, signes ou gens, sur des organisations et sur des puissances symboliques, que sont les croyances partagées. Cette relation conflictuelle implique des politiques raffinées. Ceci est d'autant plus vrai qu'interviennent des outils ou processus de haute technologie pour conserver, transporter ou traiter de l'information .

La technologie numérique rend la notion de secret plus protéiforme que jamais. Le secret protégeait contre l'imitation, la dénonciation ou l'anticipation - disons contre le Même, le Supérieur, l'Adversaire. Il a acquis d'autres fonctions. Désormais il protège contre la localisation dans l'espace, le traçage dans le temps, le profilage, la prédiction de comportements, la prise de commande, celle d'un ordinateur ou d'un réseau. Loin de faire reculer le secret, la technologie lui trouve plus d'emploi que ne l'aurait prévu notre imagination.

Il est des secrets dont l'unique fonction est de rester tels. Peu importe leur contenu, seule compte leur rareté organisée. Ils identifient des possesseurs légitimes, certifient ou limitent le nombre de copies autorisées, qu'il s'agisse d'objets ou de données reproductibles. Telle est la fonction d'un mot de passe, d'un marqueur caché, ou d'une ligne de code informatique interdisant la duplication d'un original. De tels secrets conventionnels garantissent non seulement que l'information n'est pas prélevée, mais aussi qu'elle n'est pas falsifiée. Le secret conventionnel atteste également qu'elle émane bien de qui l'on croit et prouve qui y a accès. La complication de ces systèmes de connaissance restreinte est à la mesure de la rapidité et de l'ubiquité des transmissions en réseau. Là où il y a des nœuds de pouvoir, prolifèrent secret et contrôle. Deleuze en avait bien vu le rapport avec les techniques de rétention et de certification: " Dans les sociétés de contrôle l'essentiel n'est plus une signature ou un nombre, mais un chiffre : le chiffre est un mot de passe, tandis que les sociétés disciplinaires sont réglées par des mots d'ordre. "

Une polémologie du secret à inventer devrait aussi faire la part belle aux mentalités, aux stratégies et aux idéologies. Notamment à celles qui imprègnent l'actuelle doctrine stratégique des U.S.A. Elle s'articule autour de la notion de domination informationnelle ou infodominance . C'est, dans l'idéal, la situation du stratège qui dispose sur le champ de bataille de capteurs perfectionnés, de satellites et instruments d'interception, de moyens de communication et réaction instantanée. Cette vision postule le panoptisme au profit de l'armée dominante qui doit tout savoir de l'adversaire. Ce dernier est rendu sourd, aveugle, incapable de communiquer, ses infrastructures critiques bien vite paralysées par un bombardement chirurgical ou une cyberattaque. Du point de vue qui nous intéresse ici, cela équivaut à la volonté de percer tous les secrets grâce à la technologie. La guerre zéro-risque suppose l'intelligence-zéro secret.

L'infodominance a débordé ce domaine strictement militaire pour devenir un projet géostratégique. Dans un monde qu'ils pensent déterminé par la révolution numérique, les U.S.A. se voient chargés d'une mission de « monitoring de la globalisation » . Cela implique la détection, la prévention ou au pire la préclusion, c'est-à-dire la répression par la force le plus tôt possible, de tout trouble : État voyou, opération mafieuse, péril écologique,

terrorisme... À l'échelle militaire tactique ou géopolitique, pareille ambition de contrôler toute l'information suppose une transparence absolue au profit de l'acteur principal, l'hyperpuissance.

L'infodominance, c'est donc le monopole planétaire du secret. Réel ou fantasmagorique : cela est une autre question. Car il se pourrait bien qu'en s'efforçant de rendre le monde extérieur lisible, gérable et prédictible, donc de conserver à son seul profit la possibilité du secret, la société de l'information la plus avancée du monde, d'une part, s'assigne une mission impossible et, d'autre part, se désigne d'elle-même comme cible de tous les ressentiments.

Même obsession du secret chez d'autres acteurs, en apparence tout à l'opposé, les internautes libertaires ou protestataires. Tout tourne autour du secret, celui qu'ils réclament et qu'ils veulent illimité ou le secret qu'ils soupçonnent ou dénoncent derrière toute forme d'autorité ou d'institution.

Les facteurs qui poussent à cette guerre généralisée ne tiennent pas seulement à l'imaginaire des hackers ou aux imaginations des généraux. Des raisons plus tangibles poussent États, entreprises, groupes militants ou particuliers à s'affronter par, pour, contre le secret.

D'abord, il existe de plus en plus d'informations stratégiques dont il y a intérêt à conserver le monopole, ne serait-ce qu'en termes de valeur marchande : découvertes et techniques performantes ou connaissances plus triviales, comme une base de données sur les habitudes de consommateurs. Même prolifération des informations dont il faut empêcher la reproduction pour des raisons patrimoniales, des droits intellectuels et financiers sur des données reproductibles. La frontière s'atténue entre connaissances rares, celles que collecte l'intelligence dite ouverte, et les véritables secrets protégés par la loi ou par des boucliers numériques.

Comme, de surcroît, l'acteur économique doit pressentir les tendances porteuses dans les innovations ou les goûts du public, et mettre en avant son image et sa réputation, il redoute autant la perte du secret, qu'il porte sur ce qu'il sait (et qui constitue sa réelle richesse) que sur ce qu'il est (et qui le rend vulnérable).

À mesure que l'économie devient immatérielle, s'accroît l'intérêt qu'il y a à empêcher la concurrence d'accéder à des informations sensibles, un fichier de clientèle ou un projet de recherche et développement. Il faut interdire la diffusion ou l'usage de données, ou plus brutalement encore se défendre contre l'espionnage économique, la déstabilisation. Parallèlement à la défense de la « réputation » et à la prévention de la « crise informationnelle », la protection du patrimoine numérique donc de son intégrité, de son authenticité, de sa pérennité ou sa confidentialité deviennent une branche capitale de l'activité économique. Le risque de ne pas savoir à temps ou de laisser savoir engendre une insécurité obsédante. Et nous ne traiterons pas ici de l'immense domaine de l'économie criminelle, forcément clandestine.

Le domaine du contrôle

Autrefois avoir un secret c'était avoir le monopole d'une information vraie, rare ou importante. Désormais le secret protège aussi des bases de données, et des systèmes entiers du prélèvement ou de la falsification de l'information. Il est au cœur des réseaux et des flux. Si les secrets sont désirables, ils sont aussi vulnérables et redoutables. Tous les traits que l'on prête aux nouvelles technologies - se jouer du temps et de la distance, rendre accessibles et navigables des mémoires quasi illimitées, réunir en un code unique sons, images, textes et programmes, permettre la connexion de toutes les intelligences : tout cela implique autant de possibilités de violer des secrets.

Nos mémoires sont « externalisées » c'est-à-dire confiées à des puces de silicone et électrons invisibles. Il devient aisé de les pénétrer instantanément, par des moyens modestes, sans péril. En période de « monoculture technique » si une faille apparaît dans un système de sécurité, la façon de contourner ses défenses est vite connue. Nos transactions ou communications se font à distance, électroniquement, d'où la multiplication de traces qu'il est possible de récupérer, rapprocher pour « profiler » les individus. Avec les télé-transactions, il est facile de se faire passer pour un autre et d'agir à sa place. Dans la mesure où nous employons les mêmes vecteurs, protocoles et logiciels, l'intérêt d'en percer le secret augmente. Dans une économie du temps et de l'accès, le secret compte davantage. L'information est du temps concentré ; c'est un procédé qui permet d'économiser du temps et des ressources pour obtenir un résultat. Le secret gardé est du temps garanti.

L'effraction informatique est invisible et indolore et la pénétration immatérielle : parfois la victime ne réalise pas que le secret a été violé. Ou, dans le cas de marquage, de "chips", elle ignorera qu'il existe un moyen de reconstituer ses activités : il subsiste toujours une trace de tout ce que l'on a reçu et émis, un indice de tous ses mouvements physiques ou virtuels (connexions). Ceci fonctionne dans les deux sens : "prélèvement" d'informations, mais aussi pénétration. Cookies, chevaux de Troie, virus, bombes à retardement... introduisent frauduleusement dans les systèmes informatiques des machines de guerre qui opèrent destruction, désorganisation, falsification, mais aussi des machines de contrôle. Celles-ci permettront de prélever de l'information ou d'exécuter des instructions. Les techniques de défense changent : ne pas laisser de points de passages aux signaux hostiles, sélectionner ces signaux, faire en sorte que l'information protège contre l'information. Dans le monde virtuel plus que dans le réel, distinguer l'ami de l'ennemi est crucial. D'où de nouveaux secrets en cascade : qui discriminer, comment discriminer.

De là aussi, le rôle de l'identification -authentification et signature-. Le "prouve qui tu es" répond à la revendication d'anonymat de l'utilisateur. Il vit armé de codes, obsédé par la confidentialité, menacé par des délits informationnels ou des outils de fichage. Comme citoyens nous haïssons le secret (celui de l'État, ce que nous cachent les puissants, ce que nous taisent les médias...), comme particuliers nous le réclamons : nous ne voulons plus être filmés, écoutés, décryptés... Paradoxe : il faut un moyen secret pour s'identifier, et un moyen secret pour être assuré de son anonymat. Ce peut être un logiciel, un mot de passe,.

Ces équations - traçabilité, plus accessibilité, plus externalisation des savoirs, plus dépendance des procédés de traitement - se prêtent aussi bien à l'action hégémonique des

puissants par surveillance et contrôle qu'à l'activité de déstabilisation des faibles. Désormais, le secret doit protéger l'information contre les risques de publicité, et, dans le même temps, en garantir la disponibilité et la lisibilité : il est indissociable du système même d'information, au cœur du processus de traitement et de décision. La puissance se confond avec la faculté de savoir ou de dissimuler.

Les technologies post-modernes donneraient alors une singulière actualité à la sentence de Lao-Tseu : “ Les armes du pouvoir ne se laissent point apercevoir ” (Tao-te-king verset 36)



- La prolifération du secret
Patrimoine informationnel, sécurité, intimité

En intelligence économique (préservation du patrimoine informationnel), en stratégie, dans le domaine technique, politique mais aussi dans la vie quotidienne pour assurer notre sécurité et notre intimité contre délits et surveillance, le secret prolifère dans une société qui se voudrait de communication et de transparence.

Le secret est, étymologiquement, ce qui est séparé, mis à part (du verbe latin *secernere*). Qui dit séparation dit frontières. Et qui dit frontières dit conflit.

Le secret est précieux par la puissance qu'il confère (stratégique, politique...), par la rareté des connaissances qu'il recouvre (économique, technique...), par la protection qu'il assure à son détenteur (intimité, impunité...). Il peut porter sur le passé (qui a fait quoi), sur le futur, un plan, un traité, une conspiration (qui fera quoi) ou sur un présent virtuel (comment faire quoi) : c'est le cas des procédés qui permettent de rééditer une performance, comme un brevet, un procédé, un logiciel, un plan de machine et dont on a tout intérêt à conserver l'exclusivité. Dans tous les cas quelqu'un a une raison de vouloir s'emparer du secret (l'adversaire, le concurrent, le représentant de la loi...) et un autre à le défendre. Pas de secret sans ennemi.

Le secret est une arme, un enjeu, une protection, un rapport de force, un pouvoir latent. C'est un processus menacé et maintenu à grand effort. Sa définition la plus cohérente est : "une information que son détenteur rend délibérément inaccessible."

On insiste généralement sur les caractères positifs de l'information (le fait qu'elle est immatérielle, innovante, qu'elle peut être partagée etc.). Du point de vue qui nous intéresse, la "lutte" entre le détenteur et celui qui veut s'emparer de l'information, le prédateur, elle présente deux particularités remarquables :

1. L'information se conserve inscrite. Dans l'instant, elle se communique en empruntant des supports évanescents et éphémères, voix ou ondes. Mais pour perdurer, pour cesser d'être une simple connaissance dans la mémoire d'un individu, elle doit être physiquement stockée. En dépit de tout ce qui se dit sur la « dématérialisation », une mémoire d'ordinateur garde l'information sous forme de disposition de cristaux de silicium quelque part dans un disque dur. L'information n'est donc pas réellement dématérialisée. Elle requiert des surfaces et des réceptacles. L'histoire de l'humanité est pour une large part celle de la façon dont elle a déchargé sa mémoire (ses capacités cérébrales) sur des supports extérieurs de transmission, archivage, etc...

En clair : l'histoire du secret dépend de celle des moyens physiques de transmission des biens symboliques, donc des technologies d'une époque. Une idée, un savoir, pour vaincre le temps (se conserver) ou l'espace (atteindre son destinataire) requiert un support matériel, mais aussi un traitement, une mise en ordre, donc un code.

2. L'information se transporte également codée (fut-ce par le simple code de la langue naturelle). Selon une définition classique, un code est un système de signaux qui, par convention préalable est destiné à représenter et à transmettre l'information entre la source

(ou émetteur) des signaux et le point de destination ou récepteur. Encoder, qu'il s'agisse de transmettre ou de dissimuler, consiste à ordonner des éléments physiques capables d'emprunter un canal et correspondant à des représentations mentales. Les signaux physiques en question peuvent être des sons, des lettres, un dessin, un vêtement, etc... Ils déterminent un répertoire et une combinatoire.

La protection du secret ne repose plus seulement sur le silence des acteurs (silence que renforcent censure, pressions morales ou pénales), ni sur des barrières physiques, clefs, gardes ou coffres, ni la dissimulation d'un objet, mais aussi sur des moyens sémantiques, des techniques sophistiquées d'identification, de contrôle d'accès, sur le chiffre et la cryptologie. Garder une chose, cacher un sens.

MACHINES À SECRETS

Toutes ces notions prennent un sens tout particulier à l'époque des nouvelles technologies de l'information et de la communication. Ainsi, l'informatique a montré que le secret débordait largement la confidentialité pour toucher également l'intégrité et l'authenticité, des notions dont se préoccupent de plus en plus les juristes. La confidentialité est le caractère d'une information qui n'est connue que d'un nombre restreint de personnes. Sur ce point, les nouvelles technologies ont quelque peu compliqué les choses : la gestion d'un système d'autorisations permettant d'accéder à divers niveaux de confidentialité devient un vrai casse-tête pour les institutions et les entreprises.

Le souci de l'intégrité est plus nouveau. À toute époque, les stratèges ont dû se méfier de l'intoxication ou des divers procédés par lesquels un adversaire essayait de leur fournir une information fautive de nature à altérer leur perception de la réalité et/ou à leur faire prendre des décisions inadaptées.

S'y ajoute désormais la possibilité d'altérer physiquement des informations/données dans une mémoire et/ou d'y introduire des instructions ou algorithmes qui fassent échapper la machine au contrôle de son maître, et ce parfois à son insu, anonymement, à distance.

La question de l'authenticité est tout aussi déroutante : Qui est qui ? Qui propage cette information ? Qui est celui qu'il prétend ? Que vaut cette signature (numérique par exemple) ? Qui est débité ? Il devient possible, notamment par vol de code et connexion à distance, d'emprunter des identités et de réaliser par des moyens purement informationnels (transmission et collecte de données) des opérations non autorisées voire délictueuses. Songez à ce que fait la petite délinquance avec un simple numéro de carte de crédit.

Ces fragilités et complications techniques changent le statut du secret.

- La question du secret se sépare de celle de la vérité. Autrefois avoir un secret c'était avoir le monopole d'une information vraie (ou que l'on croyait telle). Désormais conserver un secret, c'est aussi l'accès à ses bases de données, s'assurer contre le risque de l'intoxication, de la fautive information ou de l'information désorganisatrice ou nocive par exemple contre les virus informatiques ou les sabotages via Internet. C'est enfin s'assurer de la non-

propagation d'une information nocive, contrôler des passages et des flux, plutôt que connaître des contenus.

- La valeur du secret est de plus en plus relative dans le temps. Avoir un secret c'est savoir avant et savoir pour quelque temps. L'information est du temps concentré (un procédé qui permet d'économiser du temps et des ressources pour obtenir un résultat). Le secret est du temps garanti.

- Le secret se médiatise : il concerne de moins en moins des connaissances que l'on pourrait résumer en quelques phrases, mémoriser ou inscrire sur un bout de papier conservé dans un tiroir. Il réside sous forme de 0 et de 1 dans des mémoires, dans des processus comme des algorithmes et des logiciels, sous une forme tellement abstraite que nous ne pouvons même pas nous le représenter. Et certainement pas le savoir au sens traditionnel.

En résumé, le secret se réduit de moins en moins à une connaissance déniée à certains et ressemble de plus en plus à un processus, à la manifestation d'un rapport de force, un pouvoir d'interdire et de contrôler.

S'ajoutent d'autres facteurs nouveaux régissant la lutte autour du secret :

- La valeur commerciale ou pratique de connaissances, recettes, inventions, que certains possèdent et d'autres non s'accroît considérablement.

- Le « taux de renouvellement » des secrets augmente parallèlement. Il y a urgence à savoir vite et à exploiter avant les autres. Affaire d'avance plutôt que de silence. L'économie dite de l'immatériel augmente la désidérabilité de l'information, la valeur financière de son monopole ou de son antériorité, la dureté de la concurrence par la globalisation. Elle offre un champ d'action à des acteurs menant une stratégie économique planétaire par des moyens dits de guerre de l'information.

- Parmi les messages qui circulent et données conservées, il devient de plus en plus difficile de distinguer ce qui doit rester secret, ce qui est bénin, ce qui est disponible, ce qui est dangereux, etc. Que signifie le secret quand il touche, comme aux États-Unis, plusieurs millions de documents officiels classifiés ? L'inflation du secret prend des proportions inédites.

- Dans la mesure où nous confions le traitement de ces opérations à des machines sophistiquées, notre maîtrise sur eux diminue en même temps que se multiplient les possibilités de fraude, trucage, par des moyens technologiques invisibles.

- La question du secret est inséparable des grands enjeux de nos sociétés : la puissance politique voire militaire repose est proportionnelle à la capacité de voir et tout savoir. Le secret économique ne borne plus à quelques plans ou brevets qu'il suffirait d'enfermer dans un coffre, mais suppose l'exclusivité de milliers d'informations et de données. Le secret, autrefois rare, marginal, réservé à quelques groupes ou à quelques sphères de l'État, devient une revendication de simples citoyens, un élément de la défense de la sphère privée.

- La démocratie suppose une forme particulière de publicité et de transparence. Mais de manière quelque peu contradictoire, elle implique aussi la distinction entre les affaires privées qui ne concernent que l'individu et les affaires publiques. Cette contradiction risque de devenir dramatique au moment où les moyens de surveillance et de « traçage » prennent une telle ampleur.

La transformation de la pratique du secret sous l'effet de la technologie nous éloigne de toute vision romantique : mystère, silence, conspiration, aveu, tourments de l'individu chargé du secret... Pour autant la question du secret n'est pas devenue rationnelle et technique. Au contraire, elle est affaire de valeurs et de croyances. Elle suscite des réponses différentes mais passionnées dans des discours idéologiques contradictoires professés par des groupes opposés. Il y a un discours sécuritaire réclamant une action plus énergique contre les révisionnistes, pédophiles ou cyberterroristes, un discours étatique/technocratique justifiant un contrôle accru des flux de données ou une implication plus forte dans la quête de la « dominance informationnelle ». Mais on voit aussi des techno-libertaires ou des cyberpunks revendiquer la conquête de zones d'autonomie sur l'Internet, mener une lutte cybernétique contre toute forme d'État ou d'institution qui prétendrait au monopole de l'information. Bref on se déchire sur le thème du droit à l'anonymat et au secret.

SECRETS POSTMODERNES

La lutte pour et autour du secret a pris trois dimensions inédites ; elles concernent la publicité, la disponibilité et la lisibilité de l'information.

La publicité est une notion relative. Il y a toujours des « initiés » : ce peuvent être des conspirateurs qui ont juré silence sur leur vie, mais aussi le Tout-Paris médiatique qui se répète dans les dîners en ville quelques confidences qui n'aboutiront pas dans les journaux. À l'inverse, il existe des informations parfaitement disponibles mais si discrètement diffusées par rapport à leur gravité que cela équivaut presque à un secret. L'étouffement de l'information significative ou dérangeante sous le flux de ce que les médias répètent et signalent comme débat, événement, fait de société, question « qui nous interpelle », est infiniment plus efficace que toute forme de censure.

La disponibilité est une autre facette de cette lutte : elle renvoie à la possibilité concrète d'accéder à un système ou une base où résident des informations. Internet offre des moyens de pénétrer dans des mémoires de tout point. L'espace ne semble plus un obstacle, ni le temps : le violeur de secrets peut agir en temps réel mais aussi à retardement comme le font les « chevaux de Troie » introduits dans les systèmes informatiques pour en prendre le contrôle ultérieurement. L'identité de l'attaquant est assez bien protégée. Du coup, se développent de catégories inattendues d'agresseurs, agissant à faible risque, soit par goût de l'exploit gratuit (hackers), ou par ressentiment et goût du vandalisme (crackers).

L'effraction est invisible et indolore et la pénétration immatérielle : parfois la victime ne réalisera jamais que le secret a été violé. Ou, dans le cas de marquage, de « chips » etc. elle

ignorera qu'il existe un moyen de reconstituer vos activités : il subsiste toujours une trace de tout ce que l'on a reçu et émis, un indice de tous ses mouvements physiques ou virtuels (connexions).

Ceci fonctionne dans les deux sens : "prélèvement" d'informations, mais aussi pénétration. Cookies, chevaux de Troie, virus, bombes à retardement, etc. introduisent frauduleusement des machines de guerre (qui opèrent destruction, désorganisation, falsification, etc.) et des machines de contrôle (qui permettront de prélever de l'information ou d'exécuter des instructions) dans les systèmes informatiques.

Corollairement, les techniques de défenses changent, elles deviennent topologiques ou sémantiques. Dans le premier cas, il ne faut pas laisser de points de passages aux signaux hostiles. Dans ce second cas, il faut les discriminer, et que l'information protège contre l'information. Dans le monde virtuel plus que dans le réel, distinguer l'ami de l'ennemi devient un problème vital et plus seulement pour les soldats.

De là découle le caractère crucial de l'identification (authentification et signature).

L'impératif du "prouve qui tu es" forme le pendant de la revendication d'anonymat du citoyen. La valeur probante du document numérique et de la signature électronique soulève des questions de liberté publique autant que d'économie. En l'absence physique de l'individu accrédité, reste à faire appel à l'emploi de symboles : prouver que l'on sait A, pour démontrer que l'on est X et avoir le droit de savoir B ou de rentrer en Y. Le tout en laissant une signature, une empreinte, une preuve de son passage.

Ultime aspect du secret, dernier terrain de lutte : la lisibilité. Une guerre sans fin oppose codeur et décodeur, cryptologue et cryptanalyste, camouflage et repérage, l'art sophistiqué de compliquer la forme du message, et l'analyse subtile des indices et ressemblances. Mais là encore l'informatique change les règles. Le codage est désormais délégué à des puces et logiciels : les éléments du texte clair deviennent des séries de 0 et de 1 qui, elles-mêmes, sont comme "brassées" suivant un ordre. La capacité de briser (ou de préserver) de tels n'a plus rien à voir avec l'ingéniosité, mais repose sur la puissance informatique, sur une notion de nombre de tentatives. Un service secret (telle la National Security Agency américaine, dont a dit cent fois que c'est le premier employeur de mathématiciens au monde) ou un groupe de pirates informatiques peut ou ne peut pas casser une clef de tant de bits, dans un délai de tant d'heures ou de jours. Garder ou découvrir un secret devient un problème de force de calcul comme gagner une guerre est une question de puissance de feu.

Qu'on l'examine sous ses trois aspects, publicité, disponibilité, lisibilité, le secret a changé de statut : pour le garder, il ne suffit plus de se taire, pour le vaincre, il faut bien davantage que des indicateurs ou des espions. Maîtrise du secret et viol du secret reflètent un rapport de force militaire, politique, économique, technique et idéologique. Il se pourrait que la puissance se confonde désormais avec la faculté de savoir ou de dissimuler et que la part du secret s'accroisse à mesure que les techniques dites de l'intelligence et de la connaissance prédominent.

Le secret entre transmission et rétention

Le mot « secret » souffre d'abord d'inflation médiatique : le secret des médecines douces, des cadres qui réussissent, des amours d'un peuple, du prochain feuilleton de TF1, cela signifie en réalité : scoop, nouveau et excitant, une « nouvelle » peut-être connue de milliers de gens, mais pas encore été publié à des millions d'exemplaires. À l'inverse, le Secret avec majuscule devient facilement système d'explication global. C'est le cas pour toutes les formes d'hermétisme : elles supposent partout des correspondances occultes. Pour elles, Secret est l'autre nom du Monde et toute apparence recèle un sens.

Les variantes séculières de la théorie du complot ne font pas autrement : une conspiration des puissants (gouvernements, groupes occultes) dissimule sous une « vérité officielle » et force manipulations médiatiques un plan en cours de réalisation. Plan que révèle l'interprétation suspicieuse des fausses apparences. Voir la littérature de type « Da Vinci code » ou les théories pour qui le Onze Septembre est un leurre du complexe militaro-industriel. Aucun avion ne s'étant écrasé sur le Pentagone, et rien n'étant ce qu'il semble la vérité est forcément ailleurs

Une obsession comparable du décryptage nourrit la conviction de ceux qui pensent comme Guy Debord que « le secret domine le monde, et d'abord comme secret de la domination »¹ (il serait donc ce que dissimule le spectacle, le mécanisme ignoré de l'aliénation de l'idéologie et de l'obéissance)..

Même si nous le distinguons bien de l'inconnu, de l'ineffable ou du mystère et de tout ce qui excède nos possibilités cognitives, même si nous nous méfions de la paranoïa qu'il encourage ou du délire d'interprétation qu'il favorise, le secret nous provoque par son omniprésence. Il est le processus par lequel le détenteur d'une information la rend délibérément inaccessible. L'étymologie latine, le verbe *secernere* qui implique l'idée de séparer, mettre à part, impliquait déjà cette idée.

¹ Guy Debord *Nouveaux commentaires sur la société du spectacle*, aphorisme 21. Voir aussi Olivier Jacquemond *Les 3 secrets en hommage à Guy Debord* Sens et Tonka 2006

La forme du secret, les procédés ou procédures par lesquels il perdure, sont donc au moins aussi significatifs que son contenu. La langue anglaise, pour une fois plus précise que la notre, distingue «secret » (l'information dissimulée, cachée, confidentielle, codée, non reproductible, inaccessible...) et « secrecy », le processus par lequel l'information est gardé secrète.

Secret, croyances et luttes

Le secret un phénomène religieux ou, du moins, il est lié à l'existence des communautés de croyance. Les dogmes tendent à susciter une lecture ésotérique. Les églises à subir la concurrence de formes sectaires et initiatiques ? La foi – et pas seulement monothéiste – à nourrir une forme de gnose (qui prétend accéder à travers les secrets des textes sacrés à une connaissance salvatrice). Ou des mystères par lesquels un savoir mystique mène au salut à condition de ne pas être profané par sa révélation. Le point commun de ces pratiques et de leurs équivalents « laïcs », maçonniques ou autres, n'est pas seulement la discrétion, l'usage de rites, mots de passe et cérémonies cachées, bref, le besoin de se dissimuler aux yeux du monde. Il est le statut de la connaissance « secrète » : elle ne peut se divulguer sous peine d'être profanée ou mal interprétée par des esprits non préparés. Il faut donc que celui qui détient le secret – et le garde pour le transmettre – en devienne un digne réceptacle. Il s'est transformé en méritant la révélation et devient gardien du secret à son tour. À moins que la proposition ne se retourne et que ce soit afin d'atteindre un certain statut, celui d'initié, qu'il faille pratiquer une ascèse, gagner puis garder le secret. Les rites d'initiation des jeunes mâles, pratique commune à de multiples cultures, obligent le plus souvent les impétrants à se cacher pendant et se taire après l'initiation. Les nouveaux membres forment ainsi volontairement une sociétés fraternelle où les liens sont renforcés par la double force de la foi partagée et du secret juré. Tout ce qui rend difficile la communication de la croyance en facilite la transmission et la durée.

Mais le politique aussi est par excellence domaine du secret. Il rend le stratège impénétrable et imprévisible : dissimuler ses desseins ou ses ressources est un art de Prince et de Général. Machiavel ou Gracian ne font en ce domaine que

répéter ce que disaient Sun Zi ou Énée le Tacticien² quelques siècles avant notre ère. Le « qui ne sait dissimuler ne sait régner » de Louis XI fait écho au « Le Prince a perdu son mystère/ Des tigres s'attachent à ses pas » du livre de Han Fei³, classique chinois et à son éloge du souverain qui «ne révèle point ses ressorts».

Le secret vaut menace : l'opposant ou l'adversaire est dans l'incertitude, et comme paralysé, ne sachant ce que l'on sait de lui. Dans un régime totalitaire, où, par définition, le secret est réservé au Parti ou au Chef et tous les autres exposés, le citoyen ignore ce que sait la police (elle-même souvent secrète). Souvent aussi, il ignore aussi ce qu'il peut dire sans risque, même des faits notoires que chacun connaît mais que nul n'ose proclamer (il y a des camps..., le plan quinquennal ne sera pas réalisé..., le roi est nu... Big Brother a changé de politique...).

Le secret (son monopole, à certains égards, remplace celui de la violence légitime) est un objectif géostratégique majeur. Aujourd'hui, les USA, où plus de dix millions de documents sont classés top secret, comptent sur la « communauté de l'intelligence », treize agences fédérales avec un budget d'environ 47 milliards de dollars, pour percer les secrets de tous les adversaires États ou terroristes et pour conserver les siens. La doctrine militaire américaine de la « Révolution dans les affaires militaires » repose sur l'avantage cognitif : dans les futurs conflits, l'US Army verra, écouterait et saura tout, tandis que l'ennemi sera plongé dans le « brouillard de la guerre ». En principe du moins, car, qu'il s'agisse d'anticiper le 11 Septembre ou d'arrêter les jihadistes, le système ne se révèle pas à la hauteur de la théorie.

Le secret remplit aussi des fonctions moins inquiétantes. La loi l'alloue et le répartit entre administration et citoyens. Au moins dans les démocraties, elle tient la balance entre la transparence de l'action gouvernementale, pour en permettre le contrôle par le peuple et la défense des intérêts du souverain par le secret d'État ou le secret défense. Elle garantit des secrets professionnels, de fabrication ou des affaires, d'autres qui garantissent l'intimité, la

² Sun Zi (L'Art de la guerre) et Enée le Tacticien (Poliorcétique) ont respectivement écrit les plus anciens manuels de stratégie chinoise et grecque. Tous deux donnent une large place au secret (à la dissimulation, à la déception et désinformation, aux agents secrets, aux messages chiffrés etc.) dans la pratique militaire.

liberté ou l'égalité (correspondance, vote, secret fiscal, des examens...), le secret des archives, celui de la procédure,... Bref, les droits de savoir, de dire, de conserver, de rechercher l'information suscitent un jeu complexe d'obligations et de limitations entre des intérêts contradictoires. L'esprit du temps réclame de plus en plus de transparence de la machine étatique à la mesure que se développe le souci de défendre la vie privée, y compris sur Internet .

Le secret est aussi affaire de rareté donc d'économie. Jouir de la connaissance exclusive d'une formule, d'un brevet, de l'emplacement d'une ressource, de la réalité d'un marché, d'une future opération boursière, d'un danger ou d'une opportunité pour l'entreprise c'est à l'évidence un avantage dans la compétition. Savoir ce que d'autres ignorent, défendre ses secrets, le cas échéant espionner le concurrent : tout cela n'est pas nouveau, même si une discipline moderne, l'intelligence économique, rajeunit ces pratiques. Mais ce n'est pas tout. À l'ère numérique, l'information est devenue vulnérable (elle peut être perdue, dérobée, falsifiée en dépit du secret qui était censé la protéger...). Elle est aussi redoutable (un virus informatique ou une rumeur électronique peut infliger un dommage ou assurer une domination, de façon clandestine). Elle est surtout désirable : l'information rare et pertinente au moment juste représente un gain de temps, une économie de force, une liberté d'action supérieure et constitue une valeur marchande.

Secret et histoire des techniques

Le secret est aujourd'hui plus que jamais cette « forme sociologique universelle qui recouvre de façon tout à fait neutre la valeur de ses contenus » que décrivait George Simmel⁴, son premier grand théoricien. Il considérait l'existence de zones de secret la contrepartie de la confiance sur laquelle reposent la plupart de nos relations. De fait, il n'y a pas de société sans secret ...

Il peut porter sur le passé (des événements honteux ou inavouables, par exemple) ou sur le futur (projets, plans dont un adversaire ou un concurrent pourrait tirer profit s'ils étaient

⁴ Simmel G. *Secret et sociétés secrètes*, Paris, Circé, 1996

révélés)... Mais le secret dissimule aussi de façon intemporelle des informations qui permettent à quelqu'un de faire quelque chose: une recette, une invention, ou encore un sésame. Deleuze opposait avec raison les anciennes sociétés d'autorité caractérisées par le mot d'ordre à nos sociétés de contrôle caractérisées par le mot de passe⁵.

Il arrive que le secret ne recouvre rien, ou rien que l'on ne sache en vérité. Il peut ne servir qu'à assurer le prestige de son détenteur, à identifier et rapprocher les membres d'une communauté, ou à entretenir la crainte et la passivité de ceux qui ne le partagent pas. Parfois encore, c'est une pure forme vide, avec pour unique fonction d'être secret. Il ne recouvre rien, aucune vérité présumée, aucune énonciation, aucune description du monde ou des intentions de quelqu'un, rien de significatif... De tels signes conventionnels seront mémorisés et révélés dans un cadre opérationnel précis. Le secret sert seulement à prouver que l'on possède le secret. C'est un marqueur ou un identifiant qui autorise à faire : réaliser des opérations, pénétrer dans un lieu, accéder à des documents, activer des commandes depuis son ordinateur. Sous une forme simplifiée, c'est le digicode qui nous permet d'ouvrir la porte de notre immeuble. Dans une version sophistiquée, cela devient la clé d'un système de haute technologie régi par un protocole. Ainsi un standard informatiques comme IPSEC garantit non seulement la confidentialité sur un réseau, mais aussi l'authentification de l'origine, l'intégrité des données, le masquage des adresses Internet, la traçabilité ou la preuve des transactions. Et tout cela par des secrets et des codes. ... Sans compter que quelqu'un possède le secret du secret (comment sa marche) pour nous garantir que le secret est bien secret.

Le secret sépare les détenteurs et les exclus. Il faut une stratégie pour empêcher que l'information secrète soit révélée, dupliquée, anticipée... Il trace une frontière à défendre avec ses adversaires, au moins potentiels, ceux qui pourraient le mettre en danger. Il est toujours lié à un pouvoir et à un conflit.

Car il a une double fonction : il transmet et il protège. Il préserve et il interdit. Il sépare ceux qui partagent une certaine connaissance et ceux qui pourraient l'exploiter, la profaner, en faire un usage dangereux, ou, tout simplement, ceux qui n'en ont pas le droit... Toujours

⁵ Deleuze G. *Pourparlers*, Minuit 1990

menacé par le double péril de l'aveu (la révélation, la trahison) et du viol (que ce soit de vive force, ou par astuce et décryptage) le secret se défend avec peine et effort. Les armes du défenseur sont l'ignorance qu'il entretient (il est seul à savoir que la connaissance, chose, l'action ou la société secrètes existent ou ont existé), l'incertitude (personne ne peut lire son message ou deviner ses actions), l'impénétrabilité (on sait bien où est le secret mais on ne peut par le voir, l'apprendre ou le publier).

Or ceci ne peut se faire que suivant quatre stratégies.

La stratégie du coffre consiste à enfermer un objet conservant la trace d'une information— par exemple un document confidentiel ou un exemplaire d'une invention— et à confier à des murs, à des serrures ou des gardiens et douaniers, la tâche de le rendre physiquement inaccessible. Il faut alors rendre une chose secrète ou inviolable. Des secrets comme celui de la soie ont ainsi été conservés pendant des siècles⁶.

La stratégie de l'interdit présume une forme de menace (la loi, la honte, les règles du conseil de l'ordre, l'omerta...) pour empêcher de dire, de diffuser l'information secrète ou d'y accéder. Elle suppose toujours une contrainte. La moindre n'est pas que l'on exerce sur soi-même et qu'étudie la psychanalyse pour ne pas se trahir par un aveu, une confiance ou en un indice. Cette stratégie agit sur les gens et non plus sur les choses par l'intermédiaire d'une peur ou d'une croyance.

Mais il existe deux autres méthodes, qui agissent sur les images et sur les signes pour les rendre invisibles ou illisibles: celle du masque et celle du code. La première recouvre l'image contenant le secret sous une autre destinée qui la cache comme un écran. Se camoufler, c'est devenir soi-même l'information secrète en échappant à la perception. La forme d'un visage, d'un corps, d'un véhicule, d'un bâtiment ne contraste plus avec le fond. Elle est rendue indiscernable La stéganographie (d'un verbe grec signifiant « recouvrir »,

⁶ Nous avons nous-même décrit une douzaine de ces secrets historiques et techniques dans E. et FB Huyghe *Histoire des secrets*, Hazan 2000

l'art de dissimuler un message, par exemple avec une encre sympathique ou sur un micropoint) est une autre manière de rendre imperceptible⁷.

Mais l'utilisation du code brouille, elle, des symboles lettres ou bits informatiques, pour dissimuler un sens.

Cette seconde méthode agit sur signes qui permettent de lire l'information. secrète : il faut remplacer des signes clairs par des signes incompréhensibles et surajouter un code arbitraire à celui de la langue. Bref il faut produire délibérément un pseudo hasard, fabriquer un maximum d'entropie (une répartition des signaux qui semble totalement aléatoire) pour empêcher de retrouver ordre et sens dans le message.

De là deux disciplines adverses : la cryptologie, art de faire des messages secrets et la cryptanalyse, art de deviner le sens d'un texte chiffré sans en connaître la clef. Aujourd'hui toutes deux mobilisent une énorme puissance de calcul informatique et requièrent des connaissances scientifiques de pointe. Ce n'est pas par hasard que la National Security Agency américaine, dont la fonction est précisément de violer tous les secrets de transmission et de casser tous les codes, est le premier employeur de mathématiciens du monde.

Dès que l'on sort domaine du « petit » secret individuel ou familial, celui qui se conserve simplement en n'en parlant pas, dès que la transmission du secret implique davantage d'acteurs ou de plus grands enjeux, intervient une organisation complexe. Organisations matérialisées (dont les moindres ne sont pas les sociétés dites secrètes) et matière organisée (notamment par les techniques cryptologiques) contribuent aux stratégies ébauchées plus haut. Les premières semblent proliférer dans nos sociétés qui se voudraient vouées à la transparence. Mais les secondes évoluent plus vite encore

⁷ Art de rendre invisible le support physique du message, par opposition avec la cryptographie qui consiste à transposer un message clair en un ensemble de signes incompréhensibles aux non-initiés, et ce par l'usage d'un code ou chiffré. C'est la différence entre la lettre volée d'Edgar Poe et son Scarabée d'or. On notera que l'informatique a donné une nouvelle jeunesse à la stéganographie, par exemple pour insérer un message invisible ou un filigrane indécélable dans les pixels d'une image d'écran.

Pendant des siècles, les cryptologues recourent à des méthodes purement sémantiques : substituer une lettre (ou un mot, ou un signe) à un autre et/ ou de les brasser dans un certain ordre. Encoder, qu'il s'agisse de transmettre ou de dissimuler, consiste à ordonner des éléments physiques pouvant emprunter un canal et correspondant à des représentations mentales. Les signaux physiques en déterminent un répertoire et une combinatoire. Il suffit de la changer par une convention connue du seul émetteur et du destinataire.

Dès les années 1930, la cryptologie subit cependant une première révolution : elle passe à l'âge mécanique. On confie à des machines comme la fameuse Enigma de la Wehrmacht cette fonction de substitution et mutation des lettres des messages, par des rouages et connexions électriques. La machine à produire du hasard (ou les apparences du hasard) en somme... Pour briser le secret d'Enigma (et accessoirement gagner la seconde guerre mondiale) les Alliés devront eux-mêmes inventer des machines à décrypter, réalisant un très grand nombre d'opérations par essais et erreurs, machines qui seront les ancêtres des ordinateurs.

Aujourd'hui le code est bien entré dans l'hypersphère. L'informatique a transformé la nature du code et lui a découvert des usages inédits.

Pouvoirs et usages du code

Le codage est délégué à des puces et logiciels : les éléments du texte clair deviennent des séries de 0 et de 1 qui, elles-mêmes, sont comme "brassées" suivant une procédure déterminée par un algorithme. La capacité de briser (ou de préserver) de tels codes n'a plus rien à voir avec l'ingéniosité, mais repose sur la puissance informatique, et sur le nombre de tentatives. Un service secret ou un groupe de pirates peut ou ne peut pas casser une clef de tant de bits, dans un délai de tant d'heures ou de jours. Garder ou découvrir un secret devient un problème de force de calcul comme gagner une guerre est une question de puissance de feu.

- Parallèlement, la technologie numérique multiplie les usages quotidiens du secret pour produire un unique (image, message ou logiciel), non imitable
- télédiffuser aux seuls abonnés (TV),
- certifier une transaction,
- réserver une commande à distance aux acteurs autorisés,
- faire voter électroniquement,
- déclarer en laissant une signature opposable à son auteur,
- sécuriser la transmission de données et en protéger les bases,
- assurer la traçabilité d'un document numérique,
- limiter l'accès à une partie d'un système informatique
- etc.

Nous sommes des centaines de millions à utiliser des systèmes cryptographiques complexes pour téléphoner, connecter notre ordinateur ..., sans la moindre conscience de tous ces secrets qui tapissent les niches de notre environnement informationnel. Ce secret conventionnel, banal et utilitaire contraste le caractère romantique et excitant dans les histoires d'espions ou de conspirateurs, mais il met en jeu des mécanismes techniques importants. L'accroissement des flux de données numériques, notre recours à des prothèses numériques pour conserver nos mémoires et réaliser nos transactions obligent à multiplier ces zones de connaissance réservée, pour garantir les opérations symboliques à distance. Parallèlement, la question du secret s'est séparée de celle de la vérité de l'information qu'elle recouvre.

Du coup, le secret, ne protège plus seulement la confidentialité de messages et documents, il garantit la disponibilité constante de données ou de logiciels, et aussi l'intégrité des stocks et flux d'information. Surtout, il permet l'identification. L'impératif "prouve qui tu es" répond à la revendication d'anonymat du citoyen. La valeur probante du document numérique et de la signature électronique soulève des questions de liberté publique autant qu'économiques. En l'absence physique d'un contrôleur, l'acteur accrédité emploie des signes. Il prouve qu'il sait A, pour

démontrer qu'il est bien X et a le droit de savoir B ou de rentrer en Y. Le tout en laissant une signature, une empreinte, une preuve de son passage. C'est ce que nous faisons tous les jours en pénétrant sur Internet ou en payant par carte. Par la gestion du secret s'instaure la confiance : on peut croire que les gens et les choses sont ce qu'ils prétendent être.

Sous tous ses aspects, publicité, disponibilité, lisibilité, le secret a changé de statut : pour le garder, il ne suffit plus de se taire, pour le vaincre, il faut davantage que des indicateurs ou des espions. Maîtrise du secret et viol du secret reflètent un rapport de force politique, économique, technique. La puissance se confond désormais avec la faculté de savoir ou de dissimuler et la part du secret s'accroît à la mesure des techniques qui étaient censées répandre savoir et transparence.

De l'électrum à l'électron, le secret de l'argent.

Quoi de plus éloquent que l'argent ? Il ne sert que si tous l'identifient, l'acceptent et en savent les propriétés. Il lui faut une reconnaissance collective pour être efficace en privé. Chacun peut décider que le jeton rouge vaudra dix et le vert cent. Mais le boulanger ne donnera pas de baguette en échange. L'argent n'est rien en soi ; il est tout par ce qu'il représente. Pour faire accepter cela, il a besoin d'être persuasif.

Pas d'usage universel de l'argent sans publicité. Pas d'universalité sans anonymat de la monnaie divisible en unités. Pour que fonctionnent des conventions si complexes, la monnaie s'explique clairement. L'argent médiateur de l'échange est d'abord un médium. Il enregistre et garantit un savoir préalable : des informations si possible publiques, authentiques, vérifiables. Nous verrons qu'elles reposent sur d'autres inimitables ou inaccessibles.

Pour le dire autrement, si la monnaie remplit ses trois fonctions canoniques, compter, thésauriser, échanger, cela requiert un accord sur ce que l'on mesure (donc sur le barème), sur la constance de la valeur, et sur la validité des transactions. Et cet accord repose lui-même sur des connaissances résumées par la monnaie (voire sur la monnaie) de la façon la plus visible et la moins ambiguë. Du coup, elle ne se contente pas d'exprimer de la valeur, elle commente.

Quand la monnaie bavarde

L'argent est un opérateur bavard, fier de ses pouvoirs, parfois vantard. Conformément à son étymologie (monere), la monnaie avertit.

Elle nous renseigne sur :

- sa nature et son nom d'espèce (je suis un sesterce, un dollar..)
- sa quantité (je suis dix, cent...)
- l'autorité qui lui confère cette valeur (l'Empereur, la République)

et, implicitement, elle renouvelle sa promesse : par moi, tu pourras acheter des choses voire des gens.

Ce faisant, la monnaie rappelle des vérités qui lui permettent d'être à la fois intermédiaire, mesure et réserve donc stock :

- sa rareté (si elle se multipliait sans limites, l'inflation lui retirerait toute valeur)
- son intégrité (elle est bien telle qu'elle a été créée et persévérera dans son être)
- son origine (elle émane de la bonne source)

La monnaie fournit souvent d'autres indications :

Acte de foi : *Nous avons confiance en Dieu. La République est une et indivisible.*

Proclamation. *César règne. La Révolution est en marche.*

Admiration. *Voilà une chef d'œuvre de l'architecture, élément majeur de notre patrimoine national. Untel est un grand homme.*

Message idéologique et politique. Ici, règne tel souverain. Une nouvelle République a été proclamée. Notre pays est devenu indépendant. Le peuple a brisé ses chaînes. L'avenir est radieux.

Allégorie. *L'Industrie appuyée sur la Science et le Travail apportera la Prospérité à l'Humanité.*

La monnaie peut faire sa propre apologie. Ainsi, en 1295, les Ilkhanides, (i.e. la dynastie qui dirigeait la Perse comme « délégués des grands Khans », leurs cousins Yuan régnant en Chine) impriment des billets bilingues en chinois et en arabe, datés de l'Hégire. Comme d'autres jusqu'au vingtième siècle (dont feu le billet en francs) celui-ci avertit aussi les faussaires des châtiments qui les attendent. Ils assure aux honnêtes gens que la pauvreté disparaîtra et que les prix baisseront grâce à la facilité croissante des échanges. Le pronostic est mauvais : en quelques semaines la surabondance de billets provoque un chaos économique. Mais ce bout de papier résume un cours d'Histoire, d'ethnologie, de religion et d'économie (avec éloge du fiduciaire) voire de communication politique⁸.

L'information peut être plus technique : valeur intrinsèque de la monnaie métallique (elle pèse tant), valeur représentative (elle est là à la place de tant de métal qui est conservé quelque part), valeur conventionnelle (l'État a décidé qu'elle valait tant).

Elle indique aussi sa date de fabrication, lieu de la fabrique ... Sous Charles VI, dès 1389, les écus frappés dans divers ateliers du royaume portent un « point secret » par atelier. Il est caché sous une lettre bien précise dans la légende de la pièce.

Même si l'artiste signe parfois la gravure d'un billet, l'argent n'a pas à proprement parler d'auteur mais une autorité.

Il peut pourtant être personnalisé. Pour reprendre un autre exemple chinois, Marco Polo décrit comment, à la fin du XIII^e siècle, se fabriquent des billets xylographiés sur papier léger à base d'écorce de mûrier. Une fois imprimé, chacun est signé par le fonctionnaire local accrédité et revêtu de son sceau. Puis le sceau de l'Empereur Yuan est apposé en grande pompe et à l'encre vermillon, parachevant cette œuvre semi artisanale. Chaque billet ainsi certifié est relativement traçable.

La monnaie scripturale, le chèque qui nous permet d'émettre des euros « privés » d'un simple gribouillis, répond aux mêmes impératifs de publicité et de certification : pour qu'il soit accepté, il est indispensable soit que nous soyons connus, soit que nous prouvions notre identité voire l'approvisionnement de notre compte. D'où d'évidents problèmes de confidentialité et de données personnelles.

⁸ Les exemples pris dans cet article ont été développés dans E. et F.B. Huyghe, *Histoire des secrets*, Hazan 2001

Lorsque nous effectuons une transaction électronique à distance, nous dialoguons avec une machine à la fois maternelle (es-tu certain de vouloir réaliser cette opération ?) et méfiante (ton code ?).

Quand un transfert de fonds se fait transit de signes volatils (dont nous ne savons plus trop s'ils représentent une promesse ou la chose même), l'échange est pure messagerie.

Le secret du multiple

Comme d'autres le disent ici, la monnaie se fluidifie au cours du temps⁹. Métallique d'abord, donc gravée dans une matière rare, puis fiduciaire par impression d'un message sur un papier (demeurant encore une chose), scripturale par des jeux de signature, électronique enfin, réduite à des bits.

À la question « où est l'argent ? » il est facile de répondre qu'il est dans notre paume (métal), dans les réserves de la Banque nationale quand le billet le représente... C'est déjà plus abstrait pour un chèque : l'argent est-il « sur » le compte d'Untel, « à » la banque ? Et quand l'argent devient électronique (c'est-à-dire quand il est possible de transférer de l'argent d'écran à écran sans transport de support) notre logique vacille.

À l'occasion de l'affaire de la Société Générale, nous avons vu comment Jérôme Kerviel créait cinquante milliards « occultes » en quelques clics pour finalement en « perdre » cinq un matin. Le tout par la magie d'un identifiant secret qui lui permettait de créer de la richesse à volonté. Je défie le lecteur de ne pas avoir pensé une seconde : « Mais où était l'argent en réalité ? ».

L'histoire de la monnaie, envisagée comme triomphe des conventions publiques ou comme victoire du signe sur la matière, en recouvre une autre : la saga des secrets conservés et violés.

En effet, pour que la monnaie manifeste sa puissance, il n'y a pas seulement besoin d'y croire, il faut se persuader que c'en est et de la bonne. Pour la première condition, il suffit que tous les autres croient comme nous : si tout le monde est prêt à accepter mon billet de dix euros, pourquoi m'inquiéter ?

Pour la seconde, l'utilisateur peut soulever d'autres questions :

Cette monnaie est-elle ce qu'elle prétend ? (est-ce bien de l'euro ?)

Émane-t-elle de qui elle devrait ? En quelle quantité ?

Qui me prouve sa valeur ?

La connaissance ou reconnaissance publique de la « bonne » monnaie suppose le monopole et le contrôle d'informations par des pouvoirs.

⁹ Voir aussi *La vaporisation de la valeur* de Paul Soriano, Medium n°7

Dès l'apparition de la monnaie frappée, la question naît : « Qui sait quoi ? Qui possède le secret de cet argent ? ».

L'électrum, (alliage naturel de trois parts d'or pour une d'argent qui se trouve dans le fleuve Pactole) est le premier métal employé pour frapper des pièces en Lydie vers 590 580 avant notre ère. Cette monnaie a sans doute facilité les échanges entre ce royaume et les cités ioniennes en remplaçant des gouttes de métal, lingots ou autres moyens d'échange pesés mais pas encore frappés, ni identifiés à un pouvoir d'émission poinçonné, portant une figure ou un emblème, l'électrum est la première monnaie qui parle par elle-même et d'elle-même (elle se nomme et dit ce qu'elle représente).

Or l'électrum naturel ou artificiel présente un inconvénient : difficile de connaître la proportion d'or. L'émetteur est au courant mais pas l'utilisateur. D'où l'idée, attribuée à Crésus, de séparer monnayage d'or et d'argent. La nature du métal poinçonné peut se vérifier à la pierre de touche. La monnaie dont l'existence repose sur les notions de poids, d'écriture, de mathématiques et comptabilité, requiert aussi deux innovations techniques : le raffinement de l'or, stade sophistiqué de la métallurgie, et la pierre de touche. Sans instrument de vérification, pas de monnaie : le mode de preuve précède la chose.

Une monnaie métallique peut ne pas contenir tout le métal qu'il faudrait, mais elle peut aussi le contenir sans être ce qu'elle devrait. Sous l'Empire romain, sur les côtes indiennes, des commerçants locaux refondent pour les besoins du négoce des monnaies à l'imitation des deniers, des aurei et solidi romains. Au XIII^e siècle de la «fausse monnaie sarrasine» sert pour le commerce avec les pays d'Islam. Il ne s'agit pas à proprement parler d'escroquerie (le poids de métal y est) mais d'imitations à des fins pratiques. Un souverain peut rogner sa monnaie ou en mêler le métal. Philippe IV le Bel a une réputation de roi faux-monnayeur qui le met en délicatesse avec le pape et lui vaut d'être stigmatisé dans la Divine Comédie¹⁰.

On peut donc feindre la quantité (poids), la qualité (pureté du métal) et l'authenticité (émaner de qui de droit) .

Le rôle du secret s'accroît avec le billet. L'idée de remplacer des choses par des signes remonte à Babylone. Au deuxième millénaire avant notre ère, les marchands se passent déjà par écrit des ordres et promesses. La Mésopotamie qui a inventé la comptabilité et sa fille, l'écriture, en a compris le pouvoir. Mais qui dit confiance dit initiés : les systèmes de lettre de change fonctionnent par limitation du nombre d'acteurs, identification et confidentialité.

Le passage à la monnaie scripturale vraie, c'est-à-dire au billet anonyme, interchangeable, universel est long et compliqué.

¹⁰ Voir les vers de Dante : "Li si vedrà il duol che sovra Senna induce, falseggiando la moneta, quel che morrà di colpo di cotenna" (Là se verra la désolation qu'amène sur la Seine, en falsifiant la monnaie, celui qui mourra blessé par un sanglier)

Les premiers billets chinois datant du VIII^e siècle sont des effets à vue certifiant que tel marchand possède telle quantité de métaux précieux ; ils sont utilisés comme lettres de change. Puis le billet devient un « bon pour » émis par un fonctionnaire et pouvant payer les impôts. L'émission par la première banque d'État chinoise date de 1023, mais ses billets ont encore une durée de vie limitée : il faut s'en servir dans les trois ans.

En Europe, le processus est long qui mène des lettres de change des orfèvres italiens au XV^e siècle, au certificat de dépôt des banques d'Amsterdam (XVII^e siècle), puis au système de Law. Celui-ci reposait tout à la fois sur des encaisses métalliques et sur des actions de la Compagnie Perpétuelle des Indes fusionnée avec la banque. Law produisait des billets eux-mêmes garantis par le roi. Avoir confiance dans le billet c'était avoir confiance certes en une promesse d'échange, mais aussi dans la connaissance que possédaient ceux qui étaient dans le secret des Compagnies. La banqueroute de Law et la mauvaise réputation de l'assignat nourriront une résistance bien française envers le « papier » : c'est seulement peu avant la guerre de 14-18 que la valeur de la masse des billets dépassera celle des pièces dans notre pays.

Le faussaire à l'ère de la reproductibilité technique

Mais le billet de banque est un objet produit à de multiples exemplaires, fils de l'imprimerie. D'où le souci d'éviter la contrefaçon : comment éviter que ce qui est par nature reproductible ne soit multiplié de façon illégitime ?

Le problème s'est posé aux Etats-Unis au XIX^e siècle, lorsque 1.600 banques privées émettent jusqu'à 700 types de billets différents. Résultat : des abus (une banque émet 5.700 fois ce qu'aurait autorisé son encaisse métal), des tirages illégaux (notamment chez les imprimeurs) et de vrais faux billets. D'où l'institution du Greenback fabriqué par le Département du Trésor : sa protection contre les faux-monnayeurs est confiée à un bureau du service secret en 1865.

Longtemps, la contrefaçon demande trois choses : la capacité purement « artistique » d'imiter le dessin des billets à la taille douce, celle de reproduire le filigrane (et/ou d'autres signes plus ou moins discrets laissés par les ateliers d'État) et enfin le bon papier dont la formule est, comme se doit, confidentielle et la détention réglementée. La bonne équation est une forme, plus des signes (discrets ou cachés), plus une matière.

La riposte implique complexité et confidentialité. Complexité : il faut rendre de plus en plus difficile l'exploit qui consisterait à reproduire le dessin à l'identique (par exemple en surajoutant des détails presque indécélables à l'œil). Confidentialité : c'est celle de plusieurs formules (elle est souvent renforcée par la garde armée de supports de l'information : plaques pour gravure, stocks de papier...).

Ceci n'empêche pas quelques exploits remarquables. Pendant la Seconde Guerre Mondiale, les Allemands produisent de fausses livres afin de ruiner l'économie britannique en inondant le pays de faux, mais leur papier est trop bon : celui qu'utilise la banque de sa Majesté n'est pas de la même qualité. Le faussaire Bojarski réalise dès 1951 et jusqu'en

1963, de l'ancien au nouveau franc, de si bonnes reproductions qu'il introduit une microscopique erreur délibérée (un pétale de fleur) pour s'y retrouver lui-même.

De nos jours, la protection contre les faussaires ne repose plus sur la qualité du dessin (n'importe quel scanner le reproduit sans peine), mais sur une pluralité de petits secrets de fabrication : un euro comporte 63 points de contrôle dont une dizaine ne sont pas révélés au public : fil incorporé et bande métallique, hologramme, encre apparaissant aux rayons ultra violets ou changeant de couleur selon les angles de vision. En principe, l'imiter représente tant de performances que soit le faussaire n'y parvient pas sur tous les points soit cela lui coûte plus cher qu'un vrai billet.

La séparation entre connaissance publique et connaissance cachée prend son importance avec la monnaie électronique, ou plus exactement les transactions électroniques réalisant un transfert de monnaie.

Au début, les cartes de crédit sont simples. Ces rectangles de plastique certifient qu'Untel a bien un compte auprès de la banque Y (ou auprès du magasin qui lui accorde le droit de payer en différé). Elles servent d'élément de preuve (Oui, Untel a bien du crédit chez Y) en conjonction avec des papiers d'identité qu'il faut parfois présenter au commerçant (je suis bien Untel) voire avec une vérification téléphonique (Je confirme : Untel a bien droit à un crédit chez Y). De ce point de vue, la carte première manière rappelle encore un chéquier classique, à part le report dans le temps du paiement, et la procédure d'enregistrement.

La piste magnétique a un rôle pratique (retirer de l'argent dans un distributeur) mais aussi symbolique : pour la première fois l'argent porte un message en un langage non humain. La bande, qui ne parle plus de Dieu, de César, de Cézanne ni des travaux forcés, porte un message invisible à l'œil nu : "oui je suis bien la carte tant du compte tant qui a droit a tel crédit".

La carte à mémoire (la « puce » inventée par Moreno) est introduite parallèlement à d'autres modes d'identification, de complication, de secrets (hologrammes, inscriptions laser...). L'argent devient trace et témoigne de sa propre histoire. La carte ne se contente plus de dire son identité, comme un numéro d'immatriculation, elle stocke, elle compte, et elle raconte. Elle mémorise des dépenses hors ligne et dialogue en ligne avec des terminaux, elle échange des données. C'est un palimpseste toujours réécrit. De l'argent comme signe à l'argent comme témoignage, le changement n'est pas mince.

D'où un énorme problème de protection de données. Il faut prévenir le viol bigbrotherien de l'intimité du consommateur, mais aussi se garantir contre les escrocs qui voleraient l'identité du propriétaire ou fabriquaient des cartes ne correspondant à aucun compte véritable, etc., D'où un nouveau partage à réaliser entre l'information nécessaire à la transaction et l'information à cacher.

Nous ne donnons plus tant d'unités de compte, ni ne certifions plus de notre dette par une signature, nous appuyons sur cinq touches, les quatre de notre code, et celle de la

validation. Nous faisons des choses dans un ordre convenu pour prouver que nous possédons un secret.

L'argent ainsi réduit à des suites de 1 et de 0, ce numéraire numérisé, est-il encore une chose ou un événement ? Pourtant, sa dématérialisation repose sur une infrastructure très lourde : sans des administrations, sans l'État pour construire des lignes téléphoniques et fournir de l'électricité, sans des dizaines d'employés et des tonnes de ferraille ou de circuits fabriqués à Taiwan, rien de tout cela n'existerait. De même, si l'opération se traduit par une transmission immédiate de signaux, elle a pour contrepartie un système lourd de sécurité, de contrôle, et donc de dissimulation.

De l'électrum à l'électron

Ceci vaut davantage encore avec le règlement électronique sur Internet. Il supprime le dernier lien physique qui rattachait encore l'acte de payer à une expérience séculaire (aller, prendre, donner en échange). Il rompt le rapport entre la possession d'argent et la détention d'une chose, fut-ce un rectangle de plastique. L'envoi correct de données – traduction du fait qu'un ordinateur communique légitimement une certaine information – suppose la preuve que l'on détient une information réservée, le plus souvent un numéro- mais sans divulguer celui-ci ni aucune donnée sensible. Tout est rendu possible par les avancées spectaculaires de la cryptologie¹¹.

Il peut exister des raffinements dont le système dit du « tiers de confiance ». Ce dernier fournit à distance soit des certificats attestant de l'identité d'une personne qui signe par code, soit des outils de signature électronique fiables, soit enfin l'infrastructure technique nécessaire pour garantir le tout. Dans tous les cas, la transaction se fractionne en deux : la relation entre acheteur et vendeur (ou créancier et débiteur) et une relation avec le tiers qui assure la bonne marche ; l'argent existe, a bien été versé, les signataires sont qui ils prétendent, personne ne peut interférer ou s'infiltrer dans le circuit. Et ceci est crédible parce que ce tiers possède certaines informations sur l'un ou l'autre mais pas nécessairement sur la transaction même. En fractionnant ainsi mode de connaissance et mode de preuve, l'utilisateur ne livre que le strict nécessaire. Tout un édifice combinant algorithmes, mots de passe et bases de données protégées, assure le fonctionnement fluide au prix d'une divulgation minimale..

La confiance indispensable aux systèmes monétaires présuppose une assurance sur l'ignorance.

Il faut tout à la fois que le monopole de certaines connaissances (savoirs techniques, accès à des données numériques) permette de restreindre la prolifération incontrôlée des moyens de paiement.

Il faut ensuite qu'un stock (compte, réserve, base de données) ne puisse être altéré, saboté, prélevé, reproduit, publié, surtout numériquement...

¹¹ Voir notre article *Le code paradoxal*, Cahiers de Médiologie n °9

Enfin le secret sert à prouver. En démontrant que l'on détient une information dont l'unique rôle est d'être unique, on peut démontrer qui l'on est ou ce que l'on est autorisé à faire.

De l'électrum à l'électron, il faut ces arcanes garantissant rareté, intégrité, confidentialité, authenticité..., pour que l'argent règne sur la scène publique.

De l'électrum à l'électron, le secret de l'argent.

Quoi de plus éloquent que l'argent ? Il ne sert que si tous l'identifient, l'acceptent et en savent les propriétés. Il lui faut une reconnaissance collective pour être efficace en privé. Chacun peut décider que le jeton rouge vaudra dix et le vert cent. Mais le boulanger ne donnera pas de baguette en échange. L'argent n'est rien en soi ; il est tout par ce qu'il représente. Pour faire accepter cela, il a besoin d'être persuasif.

Pas d'usage universel de l'argent sans publicité. Pas d'universalité sans anonymat de la monnaie divisible en unités. Pour que fonctionnent des conventions si complexes, la monnaie s'explique clairement. L'argent médiateur de l'échange est d'abord un medium. Il enregistre et garantit un savoir préalable : des informations si possible publiques, authentiques, vérifiables. Nous verrons qu'elles reposent sur d'autres inimitables ou inaccessibles.

Pour le dire autrement, si la monnaie remplit ses trois fonctions canoniques, compter, thésauriser, échanger, cela requiert un accord sur ce que l'on mesure (donc sur le barème), sur la constance de la valeur, et sur la validité des transactions. Et cet accord repose lui-même sur des connaissances résumées par la monnaie (voire sur la monnaie) de la façon la plus visible et la moins ambiguë. Du coup, elle ne se contente pas d'exprimer de la valeur, elle commente.

Quand la monnaie bavarde

L'argent est un opérateur bavard, fier de ses pouvoirs, parfois vantard. Conformément à son étymologie (*monere*), la monnaie avertit.

Elle nous renseigne sur :

- sa nature et son nom d'espèce (*je suis un sesterce, un dollar..*)
- sa quantité (*je suis dix, cent...*)
- l'autorité qui lui confère cette valeur (l'Empereur, la République)

et, implicitement, elle renouvelle sa promesse : *par moi, tu pourras acheter des choses voire des gens.*

Ce faisant, la monnaie rappelle des vérités qui lui permettent d'être à la fois intermédiaire, mesure et réserve donc stock :

- sa rareté (si elle se multipliait sans limites, l'inflation lui retirerait toute valeur)
- son intégrité (elle est bien telle qu'elle a été créée et persévérera dans son être)
- son origine (elle émane de la bonne source)

La monnaie fournit souvent d'autres indications :

Acte de foi : *Nous avons confiance en Dieu. La République est une et indivisible.*
Proclamation. *César règne. La Révolution est en marche.*

Admiration. *Voilà une chef d'œuvre de l'architecture, élément majeur de notre patrimoine national. Untel est un grand homme.*

Message idéologique et politique. *Ici, règne tel souverain. Une nouvelle République a été proclamée. Notre pays est devenu indépendant. Le peuple a brisé ses chaînes. L'avenir est radieux.*

Allégorie. *L'Industrie appuyée sur la Science et le Travail apportera la Prospérité à l'Humanité.*

La monnaie peut faire sa propre apologie. Ainsi, en 1295, les Ilkhanides, (i.e. la dynastie qui dirigeait la Perse comme « délégués des grands Khans », leurs cousins Yuan régnant en Chine) impriment des billets bilingues en chinois et en arabe, datés de l'Hégire. Comme d'autres jusqu'au vingtième siècle (dont feu le billet en francs) celui-ci avertit aussi les faussaires des châtiments qui les attendent. Ils assure aux honnêtes gens que la pauvreté disparaîtra et que les prix baisseront grâce à la facilité croissante des échanges. Le pronostic est mauvais : en quelques semaines la surabondance de billets provoque un chaos économique. Mais ce bout de papier résume un cours d'Histoire, d'ethnologie, de religion et d'économie (avec éloge du fiduciaire) voire de communication politique¹².

L'information peut être plus technique : valeur intrinsèque de la monnaie métallique (*elle pèse tant*), valeur représentative (*elle est là à la place de tant de métal qui est conservé quelque part*), valeur conventionnelle (*l'État a décidé qu'elle valait tant*).

Elle indique aussi sa date de fabrication, lieu de la fabrique ... Sous Charles VI, dès 1389, les écus frappés dans divers ateliers du royaume portent un « point secret » par atelier. Il est caché sous une lettre bien précise dans la légende de la pièce.

Même si l'artiste signe parfois la gravure d'un billet, l'argent n'a pas à proprement parler d'auteur mais une autorité.

Il peut pourtant être personnalisé. Pour reprendre un autre exemple chinois, Marco Polo décrit comment, à la fin du XIII^e siècle, se fabriquent des billets xylographiés sur papier léger à base d'écorce de mûrier Une fois imprimé,

¹² Les exemples pris dans cet article ont été développés dans E. et F.B. Huyghe, *Histoire des secrets*, Hazan 2001

chacun est signé par le fonctionnaire local accrédité et revêtu de son sceau. Puis le sceau de l'Empereur Yuan est apposé en grande pompe et à l'encre vermillon, parachevant cette œuvre semi artisanale. Chaque billet ainsi certifié est relativement *traçable*.

La monnaie scripturale, le chèque qui nous permet d'émettre des euros « privés » d'un simple gribouillis, répond aux mêmes impératifs de publicité et de certification : pour qu'il soit accepté, il est indispensable soit que nous soyons connus, soit que nous prouvions notre identité voire l'approvisionnement de notre compte. D'où d'évidents problèmes de confidentialité et de données personnelles.

Lorsque nous effectuons une transaction électronique à distance, nous dialoguons avec une machine à la fois maternante (*es-tu certain de vouloir réaliser cette opération ?*) et méfiante (*ton code ?*).

Quand un transfert de fonds se fait transit de signes volatils (dont nous ne savons plus trop s'ils représentent une promesse ou la chose même), l'échange est pure messagerie.

Le secret du multiple

Comme d'autres le disent ici, la monnaie se fluidifie au cours du temps¹³. Métallique d'abord, donc gravée dans une matière rare, puis fiduciaire par impression d'un message sur un papier (demeurant encore une chose), scripturale par des jeux de signature, électronique enfin, réduite à des bits.

À la question « où est l'argent ? » il est facile de répondre qu'il est dans notre paume (métal), dans les réserves de la Banque nationale quand le billet le représente... C'est déjà plus abstrait pour un chèque : l'argent est-il « sur » le compte d'Untel, « à » la banque ? Et quand l'argent devient électronique (c'est-à-dire quand il est possible de transférer de l'argent d'écran à écran sans transport de support) notre logique vacille.

À l'occasion de l'affaire de la Société Générale, nous avons vu comment Jérôme Kerviel créait cinquante milliards « occultes » en quelques clics pour finalement en « perdre » cinq un matin. Le tout par la magie d'un identifiant secret qui lui permettait de créer de la richesse à volonté. Je défie le lecteur de ne pas avoir pensé une seconde : « Mais où était l'argent *en réalité* ? ».

L'histoire de la monnaie, envisagée comme triomphe des conventions publiques ou comme victoire du signe sur la matière, en recouvre une autre : la saga des secrets conservés et violés.

¹³ Voir aussi *La vaporisation de la valeur* de Paul Soriano, Medium n°7

En effet, pour que la monnaie manifeste sa puissance, il n'y a pas seulement besoin d'y croire, il faut se persuader que c'en est et de la bonne. Pour la première condition, il suffit que tous les autres croient comme nous : si tout le monde est prêt à accepter mon billet de dix euros, pourquoi m'inquiéter ?

Pour la seconde, l'utilisateur peut soulever d'autres questions :

Cette monnaie est-elle ce qu'elle prétend ? (*est-ce bien de l'euro ?*)

Émane-t-elle de qui elle devrait ? En quelle quantité ?

Qui me prouve sa valeur ?

La connaissance ou reconnaissance publique de la « bonne » monnaie suppose le monopole et le contrôle d'informations par des pouvoirs.

Dès l'apparition de la monnaie frappée, la question naît : « Qui sait quoi ? Qui possède le secret de cet argent ? ».

L'électrum, (alliage naturel de trois parts d'or pour une d'argent qui se trouve dans le fleuve Pactole) est le premier métal employé pour frapper des pièces en Lydie vers 590 580 avant notre ère. Cette monnaie a sans doute facilité les échanges entre ce royaume et les cités ioniennes en remplaçant des gouttes de métal, lingots ou autres moyens d'échange pesés mais pas encore frappés, ni identifiés à un pouvoir d'émission poinçonné, portant une figure ou un emblème, l'électrum est la première monnaie qui parle par elle-même et d'elle-même (elle se nomme et dit ce qu'elle représente).

Or l'électrum naturel ou artificiel présente un inconvénient : difficile de connaître la proportion d'or. L'émetteur est au courant mais pas l'utilisateur. D'où l'idée, attribuée à Crésus, de séparer monnayage d'or et d'argent. La nature du métal poinçonné peut se vérifier à la pierre de touche. La monnaie dont l'existence repose sur les notions de poids, d'écriture, de mathématiques et comptabilité, requiert aussi deux innovations techniques : le raffinement de l'or, stade sophistiqué de la métallurgie, et la pierre de touche. Sans instrument de vérification, pas de monnaie : le mode de preuve précède la chose.

Une monnaie métallique peut ne pas contenir tout le métal qu'il faudrait, mais elle peut aussi le contenir sans être ce qu'elle devrait. Sous l'Empire romain, sur les côtes indiennes, des commerçants locaux refondent pour les besoins du négoce des monnaies à l'imitation des deniers, des *aurei* et *solidi* romains. Au XIII^e siècle de la « fausse monnaie sarrasine » sert pour le commerce avec les pays d'Islam. Il ne s'agit pas à proprement parler d'escroquerie (le poids de métal y est) mais d'imitations à des fins pratiques. Un souverain peut rogner sa monnaie ou en mêler le métal.

Philippe IV le Bel a une réputation de roi faux-monnayeur qui le met en délicatesse avec le pape et lui vaut d'être stigmatisé dans la Divine Comédie¹⁴.

On peut donc feindre la quantité (poids), la qualité (pureté du métal) et l'authenticité (émaner de qui de droit) .

Le rôle du secret s'accroît avec le billet. L'idée de remplacer des choses par des signes remonte à Babylone. Au deuxième millénaire avant notre ère, les marchands se passent déjà par écrit des ordres et promesses. La Mésopotamie qui a inventé la comptabilité et sa fille, l'écriture, en a compris le pouvoir. Mais qui dit confiance dit initiés : les systèmes de lettre de change fonctionnent par limitation du nombre d'acteurs, identification et confidentialité.

Le passage à la monnaie scripturale vraie, c'est-à-dire au billet anonyme, interchangeable, universel est long et compliqué.

Les premiers billets chinois datant du VIII^e siècle sont des effets à vue certifiant que tel marchand possède telle quantité de métaux précieux ; ils sont utilisés comme lettres de change. Puis le billet devient un « bon pour » émis par un fonctionnaire et pouvant payer les impôts. L'émission par la première banque d'État chinoise date de 1023, mais ses billets ont encore une durée de vie limitée : il faut s'en servir dans les trois ans.

En Europe, le processus est long qui mène des lettres de change des orfèvres italiens au XV^e siècle, au certificat de dépôt des banques d'Amsterdam (XVII^e siècle), puis au système de Law. Celui-ci reposait tout à la fois sur des encaisses métalliques et sur des actions de la Compagnie Perpétuelle des Indes fusionnée avec la banque. Law produisait des billets eux-mêmes garantis par le roi. Avoir confiance dans le billet c'était avoir confiance certes en une promesse d'échange, mais aussi dans la connaissance que possédaient ceux qui étaient dans le secret des Compagnies. La banqueroute de Law et la mauvaise réputation de l'assignat nourriront une résistance bien française envers le « papier » : c'est seulement peu avant la guerre de 14-18 que la valeur de la masse des billets dépassera celle des pièces dans notre pays.

Le faussaire à l'ère de la reproductibilité technique

Mais le billet de banque est un objet produit à de multiples exemplaires, fils de l'imprimerie. D'où le souci d'éviter la contrefaçon : comment éviter que ce qui est par nature reproductible ne soit multiplié de façon illégitime ?

Le problème s'est posé aux Etats-Unis au XIX^e siècle, lorsque 1.600 banques privées émettent jusqu'à 700 types de billets différents. Résultat : des abus (une banque émet 5.700 fois ce qu'aurait autorisé son encaisse métal), des tirages

¹⁴ Voir les vers de Dante : "Li si vedrà il duol che sovra Senna induce, falseggiando la moneta, quel che morrà di colpo di cotenna" (Là se verra la désolation qu'amène sur la Seine, en falsifiant la monnaie, celui qui mourra blessé par un sanglier)

illégaux (notamment chez les imprimeurs) et de vrais faux billets. D'où l'institution du *Greenback* fabriqué par le Département du Trésor : sa protection contre les faux-monnayeurs est confiée à un bureau du service secret en 1865.

Longtemps, la contrefaçon demande trois choses : la capacité purement « artistique » d'imiter le dessin des billets à la taille douce, celle de reproduire le filigrane (et/ou d'autres signes plus ou moins discrets laissés par les ateliers d'État) et enfin le bon papier dont la formule est, comme se doit, confidentielle et la détention réglementée. La bonne équation est une forme, plus des signes (discrets ou cachés), plus une matière.

La riposte implique complexité et confidentialité. Complexité : il faut rendre de plus en plus difficile l'exploit qui consisterait à reproduire le dessin à l'identique (par exemple en surajoutant des détails presque indécélables à l'œil). Confidentialité : c'est celle de plusieurs formules (elle est souvent renforcée par la garde armée de supports de l'information : plaques pour gravure, stocks de papier...).

Ceci n'empêche pas quelques exploits remarquables. Pendant la Seconde Guerre Mondiale, les Allemands produisent de fausses livres afin de ruiner l'économie britannique en inondant le pays de faux, mais leur papier est trop bon : celui qu'utilise la banque de sa Majesté n'est pas de la même qualité. Le faussaire Bojarski réalise dès 1951 et jusqu'en 1963, de l'ancien au nouveau franc, de si bonnes reproductions qu'il introduit une microscopique erreur délibérée (un pétale de fleur) pour s'y retrouver lui-même.

De nos jours, la protection contre les faussaires ne repose plus sur la qualité du dessin (n'importe quel scanner le reproduit sans peine), mais sur une pluralité de petits secrets de fabrication : un euro comporte 63 points de contrôle dont une dizaine ne sont pas révélés au public : fil incorporé et bande métallique, hologramme, encre apparaissant aux rayons ultra violets ou changeant de couleur selon les angles de vision. En principe, l'imiter représente tant de performances que soit le faussaire n'y parvient pas sur tous les points soit cela lui coûte plus cher qu'un vrai billet.

La séparation entre connaissance publique et connaissance cachée prend son importance avec la monnaie électronique, ou plus exactement les transactions électroniques réalisant un transfert de monnaie.

Au début, les cartes de crédit sont simples. Ces rectangles de plastique certifient qu'Untel a bien un compte auprès de la banque Y (ou auprès du magasin qui lui accorde le droit de payer en différé). Elles servent d'élément de preuve (*Oui, Untel a bien du crédit chez Y*) en conjonction avec des papiers d'identité qu'il faut parfois présenter au commerçant (*je suis bien Untel*) voire avec une vérification téléphonique (*Je confirme : Untel a bien droit à un crédit chez Y*). De ce point de vue, la carte première manière rappelle encore un chéquier classique, à part le report dans le temps du paiement, et la procédure d'enregistrement.

La piste magnétique a un rôle pratique (retirer de l'argent dans un distributeur) mais aussi symbolique : pour la première fois l'argent porte un message en un langage non humain. La bande, qui ne parle plus de Dieu, de César, de Cézanne ni des travaux forcés, porte un message invisible à l'œil nu : "*oui je suis bien la carte tant du compte tant qui a droit a tel crédit*".

La carte à mémoire (la « puce » inventée par Moreno) est introduite parallèlement à d'autres modes d'identification, de complication, de secrets (hologrammes, inscriptions laser...). L'argent devient trace et témoin de sa propre histoire. La carte ne se contente plus de dire son identité, comme un numéro d'immatriculation, elle stocke, elle compte, et elle raconte. Elle mémorise des dépenses hors ligne et dialogue en ligne avec des terminaux, elle échange des données. C'est un palimpseste toujours réécrit. De l'argent comme signe à l'argent comme témoignage, le changement n'est pas mince.

D'où un énorme problème de protection de données. Il faut prévenir le viol *bigbrotherien* de l'intimité du consommateur, mais aussi se garantir contre les escrocs qui voleraient l'identité du propriétaire ou fabriquaient des cartes ne correspondant à aucun compte véritable, etc., D'où un nouveau partage à réaliser entre l'information nécessaire à la transaction et l'information à cacher.

Nous ne donnons plus tant d'unités de compte, ni ne certifions plus de notre dette par une signature, nous appuyons sur cinq touches, les quatre de notre code, et celle de la validation. Nous faisons des choses dans un ordre convenu pour prouver que nous possédons un secret.

L'argent ainsi réduit à des suites de 1 et de 0, ce numéraire numérisé, est-il encore une chose ou un événement ? Pourtant, sa dématérialisation repose sur une infrastructure très lourde : sans des administrations, sans l'État pour construire des lignes téléphoniques et fournir de l'électricité, sans des dizaines d'employés et des tonnes de ferraille ou de circuits fabriqués à Taiwan, rien de tout cela n'existerait. De même, si l'opération se traduit par une transmission immédiate de signaux, elle a pour contrepartie un système lourd de sécurité, de contrôle, et donc de dissimulation.

De l'électrum à l'électron

Ceci vaut davantage encore avec le règlement électronique sur Internet. Il supprime le dernier lien physique qui rattachait encore l'acte de payer à une expérience séculaire (aller, prendre, donner en échange). Il rompt le rapport entre la possession d'argent et la détention d'une chose, fut-ce un rectangle de plastique. L'envoi correct de données – traduction du fait qu'un ordinateur communique légitimement une certaine information – suppose la preuve que l'on détient une information réservée, le

plus souvent un numéro- mais sans divulguer celui-ci ni aucune donnée sensible. Tout est rendu possible par les avancées spectaculaires de la cryptologie¹⁵.

Il peut exister des raffinements dont le système dit du « tiers de confiance ». Ce dernier fournit à distance soit des certificats attestant de l'identité d'une personne qui signe par code, soit des outils de signature électronique fiables, soit enfin l'infrastructure technique nécessaire pour garantir le tout. Dans tous les cas, la transaction se fractionne en deux : la relation entre acheteur et vendeur (ou créateur et débiteur) et une relation avec le tiers qui assure la bonne marche ; *l'argent existe, a bien été versé, les signataires sont qui ils prétendent, personne ne peut interférer ou s'infiltrer dans le circuit*. Et ceci est crédible parce que ce tiers possède certaines informations sur l'un ou l'autre mais pas nécessairement sur la transaction même. En fractionnant ainsi mode de connaissance et mode de preuve, l'utilisateur ne livre que le strict nécessaire. Tout un édifice combinant algorithmes, mots de passe et bases de données protégées, assure le fonctionnement fluide au prix d'une divulgation minimale..

La confiance indispensable aux systèmes monétaires présuppose une assurance sur l'ignorance.

Il faut tout à la fois que le monopole de certaines connaissances (savoirs techniques, accès à des données numériques) permette de restreindre la prolifération incontrôlée des moyens de paiement.

Il faut ensuite qu'un stock (compte, réserve, base de données) ne puisse être altéré, saboté, prélevé, reproduit, publié, surtout numériquement...

Enfin le secret sert à prouver. En démontrant que l'on détient une information dont l'unique rôle est d'être unique, on peut démontrer qui l'on est ou ce que l'on est autorisé à faire.

De l'électrum à l'électron, il faut ces arcanes garantissant rareté, intégrité, confidentialité, authenticité..., pour que l'argent règne sur la scène publique.

François-Bernard Huyghe



¹⁵ Voir notre article *Le code paradoxal*, Cahiers de Médiologie n °9

Le secret de l'argent