

La réglementation en France

Pendant longtemps, la cryptographie a été considérée comme une arme ; son usage était réglementé, aussi bien pour la fourniture et l'exportation que pour l'utilisation à titre personnel.

En février 1998, toutefois, l'État français a autorisé tout procédé nécessaire à l'authentification de données ou d'entités (intégrité, signature numérique et contrôle d'accès), ainsi que le chiffrement des communications, en limitant, dans ce dernier cas, la clé secrète à 40 bits. Une telle taille de clé ne garantissait pas un niveau de confidentialité suffisant pour des applications «sérieuses» : à raison d'un million d'essais par seconde, une station de travail trouve la clé en moins de 15 jours.

Comment accroître la sécurité ? En augmentant la taille de la clé et en déposant alors la clé secrète auprès d'un tiers de confiance. Ce dépôt permettait alors aux instances judiciaires d'obtenir, de ce tiers de confiance, la clé secrète nécessaire au déchiffrement de communications chiffrées, en cas de besoin justifié.

Le 19 janvier 1999, le premier ministre, Lionel Jospin, annonçait une proche libéralisation de l'usage de la cryptographie. Après avoir interrogé les acteurs, les experts et les partenaires internationaux, le gouvernement a retenu les orientations suivantes : libéraliser complètement la cryptographie ; supprimer le recours obligatoire aux tiers de confiance pour le dépôt des clés secrètes de chiffrement ; compléter le dispositif juridique afin d'obliger la remise aux autorités judiciaires de la

transcription en clair des documents chiffrés, lors de leur demande. De telles modifications législatives nécessiteront plusieurs mois.

Pour lever rapidement les principales entraves au développement du commerce électronique et pour assurer la confidentialité des communications, des décrets, parus le 19 mars 1999, relèvent le seuil de la cryptographie libre de toute autorisation de 40 bits à 128 bits. Plus précisément, ces décrets stipulent que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à 40 bits sont totalement libres» et que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur supérieure 40 bits et inférieure ou égale 128 bits sont libres sans condition pour un usage privé, et soumis à déclaration dans les autres cas».

Ces décrets représentent l'étape essentielle, car des clés de 128 bits garantissent une sécurité plus que suffisante : une attaque par recherche exhaustive (essai de toutes les clés) nécessiterait plusieurs siècles, même avec tous les ordinateurs de la planète réunis. Une autre étape importante, sera «d'assurer, avec toutes les garanties nécessaires, la valeur probante du document sous forme numérique et des signatures électroniques. Les obstacles juridiques qui demeurent au développement des transactions dématérialisées seront ainsi levés».

David POINTCHEVAL, École normale supérieure, Paris

Ces systèmes ne satisferont personne, car ils sont faciles à détourner. Les espions et les criminels peuvent modifier les logiciels de chiffrement pour empêcher la recherche de la clé ou utiliser d'autres logiciels disponibles sur le réseau Internet. De surcroît, avec ces solutions, la recherche des clés serait très onéreuse et le coût du recouvrement des clés n'a pas été envisagé : qui paiera ? Enfin, la confiance dans le gouvernement risquerait de s'éroder, et la procédure serait très compliquée : imaginez qu'à chaque achat de gants vous soyez légalement tenus de coudre des copies en latex de vos empreintes digitales aux doigts de ces gants !

Les systèmes de recouvrement de clés seraient également dangereux. La procédure secrète utilisée par le FBI pour déchiffrer les messages pourrait être détournée au profit de criminels, d'intrus, d'espions ou même d'employés mécontents du FBI. En volant une super clé secrète, ces indélégats pourraient déchiffrer toutes les communications. Des millions de secrets appartenant à des sociétés, à des personnes privées ou au gouvernement seraient brusquement vulnérables.

En 1993, le Congrès américain a réclamé une étude de ces problèmes. Après deux années de travail, la commission réunie pour l'occasion a estimé que la libéralisation de la cryptographie était plus avantageuse que son interdiction. Aucune loi ne devrait limiter la fabrication, la vente et l'utilisation des systèmes cryptographiques à l'intérieur des États-Unis.

Les membres de la commission ont également estimé que l'État ne pourrait pas faire respecter une interdiction de la cryptographie. Pourtant, le FBI et la NSA prônent tou-

jours la mise en place d'un service de recouvrement des clés ; ils s'opposent au relâchement des contrôles à l'exportation, tant que la possibilité de retrouver les clés secrètes n'est pas incorporée dans les logiciels exportés.

Entre-temps, la cryptographie s'est développée, les utilisateurs se sont familiarisés avec les programmes de cryptographie, et le contrôle deviendra inéluctablement difficile. Les entreprises adoptent des standards publics de cryptographie que même des lycéens peuvent convertir en programmes. De surcroît, il existe de nouvelles techniques qui ne chiffrent pas le message, mais permettent la confidentialité en le cachant dans un fouillis de données aléatoires. D'où la difficulté d'un contrôle !

Je maintiens que les citoyens doivent avoir le droit d'avoir des conversations privées. La démocratie repose sur la possibilité que possède chaque citoyen de partager librement ses façons de voir, sans crainte de surveillance ou de représailles. Ce principe doit être appliqué au «cyberespace», comme il l'est au monde réel. Si les États-Unis restreignaient le droit d'utiliser la cryptographie, ce serait un recul de la démocratie et une victoire de *Big Brother*.

Donald RIVEST est l'un des inventeurs de la méthode de chiffrement RSA. Il enseigne à l'Institut de technologie du Massachusetts.

Whitfield DIFFIE et Susan LANDAU, *Privacy on the Line : The Politics of Wiretapping and Encryption*, MIT Press, 1998.

Les galets, outils du Paléolithique

SOPHIE A. DE BEAUNE

Des galets non taillés révèlent l'invention de gestes techniques avant la fabrication d'outils spécialisés.

Les silex taillés sont parmi les vestiges les plus impressionnants et les plus abondants laissés par les hommes de la Préhistoire. Des images et des récits ont popularisé la vision de l'«homme des cavernes» taillant un silex ou le brandissant pour chasser. C'est aussi par la typologie de cet outillage de pierre taillée et de l'outillage en os façonné que les grands ensembles culturels ont été définis : l'Aurignacien, le Gravettien, le Solutréen, le Magdalénien...

Toutefois, nos ancêtres ne taillaient pas la pierre plus que nécessaire : pour la plupart des outils en roche non cassante utilisés pour leurs besoins domestiques et techniques courants, ils

ménageaient leur peine et choisissaient des blocs, des plaquettes ou des galets dont la forme naturelle était proche de celle qu'ils recherchaient. Ainsi, pour obtenir des récipients en roche dure, ils ramassaient des galets ronds ou ovales dont ils n'avaient plus qu'à creuser l'une des faces. Ils utilisaient aussi fréquemment des galets bruts, pourvu qu'ils aient la taille, la forme, la dureté et la densité voulues. Ils en faisaient alors des enclumes, des broyeurs, des molettes, des pilons-broyeurs, des maillets, des lissoirs, des polissoirs... Bien que rudimentaires, ces outils étaient conservés et exploités très longtemps.

Ces outils «naturels», ou façonnés par des techniques autres que la taille

(piquetage, martelage, raclage, plus rarement polissage), ont été longtemps négligés. Les préhistoriens du XIX^e siècle et de la première moitié du XX^e siècle les abandonnaient le plus souvent dans les déblais. Dans le meilleur des cas, ils les conservaient sous une rubrique «divers».

Heureusement, quelques sites font exception, telles les grottes pyrénéennes de La Vache, fouillée de 1866 à 1940, et d'Isturitz, de 1912 à 1954, dont l'intégralité du matériel a été conservée : les galets utilisés y sont si abondants (presque 500 pour chaque site) que leur



1. DES MOLETTES, ou meules à main, étaient utilisées pour le broyage, de végétaux par exemple, par un mouvement de bascule d'avant en arrière et de droite à gauche.

De nombreuses formes naturelles des galets se prêtent à cet usage. Le plus ancien témoignage en est un galet de roche volcanique (à droite, hauteur réelle : 7,5 centimètres), manipulé par des Néandertaliens il y a 70 000 à 40 000 ans dans le Petit Abri de Laussel, en Dordogne. L'usure a légèrement aplati sa face inférieure. De même, le frottement répété a poli les deux faces et le pourtour d'un petit galet de quartzite quasi circulaire, découvert dans la grotte d'Isturitz, dans les Pyrénées-Atlantiques, et daté de 28 000 à 22 000 ans (au milieu, diamètre réel : 6,5 centimètres).

classement, respectivement par Dominique Buisson, alors au Musée des antiquités nationales, et par moi-même, a permis de constituer des collections utilisables pour des comparaisons au fur et à mesure des nouvelles découvertes. Aujourd'hui, les fouilleurs récupèrent l'intégralité du matériel archéologique.

Cet outillage, que l'on retrouve sous des formes analogues chez des peuples nomades actuels, chasseurs-cueilleurs ou éleveurs, nous renseigne sur la vie quotidienne de leurs utilisateurs. Très variés, ces outils sont intervenus aussi bien dans la transformation de la matière que dans la consommation et l'acquisition de la nourriture : fabrication de l'outillage, préparation de la nourriture, stockage de divers ingrédients, préparation des colorants, éclairage, travail des peaux, chasse, pêche...

Les traces d'utilisation visibles à la surface de ces objets permettent la reconstitution des gestes exécutés. Notre connaissance des activités et des comportements des hommes du Paléolithique en est élargie. Par exemple, au Roc de Sers, en Charente, un bloc ayant servi à la fois d'enclume pour débiter du silex et de support à découper de la viande ou des peaux apporte de nombreuses informations sur la taille de la pierre, mais aussi sur les techniques de découpe et de préparation alimentaire, et sur la gestion de l'espace dans le campement. Les galets non taillés nous informent aussi sur la consommation et les modes de préparation des végétaux sauvages, dont presque toutes les traces

directes ont aujourd'hui disparu (les restes végétaux se fossilisent mal). Sur-tout, nous verrons que l'étude des gestes auxquels sont liés ces outils pose de façon nouvelle la question du progrès, du début du Paléolithique au Néolithique : de nombreuses innovations techniques résultent de la simple application de gestes anciens à un nouveau but.

Des traces à la fonction

À quelles activités les traces que nous observons aujourd'hui sur un galet correspondent-elles ? Comment pourrions-nous déterminer si elles ont été produites par la seule utilisation de l'objet ou au cours d'une éventuelle fabrication ? Dans un premier temps, nous devons retrouver le fonctionnement de ces objets : comment ont-ils été utilisés ? Nous pourrions ensuite formuler des hypothèses sur leurs fonctions.

En 1943, André Leroi-Gourhan a proposé une classification des « moyens élémentaires d'action sur la matière », qui lui a servi de base pour une classification générale de l'ensemble des techniques humaines. Sa classification des percussions suffit pour tenter d'élucider l'origine des traces visibles sur les galets préhistoriques. J'ai ainsi obtenu quatre grandes catégories d'outils, actifs ou passifs : ceux ayant exercé ou subi une percussion lancée, ceux ayant exercé

ou subi une percussion posée, ceux ayant alterné une percussion lancée et posée, enfin ceux n'ayant reçu ou exercé aucune percussion. Cette terminologie ne préjuge pas de la nature de l'activité réalisée et se limite à la description d'un geste.

J'ai ensuite défini des critères qui permettent de dire comment le geste s'est exercé. Pour cela, je tiens compte du type de support (galet ou bloc) et de l'emplacement des traces d'usage par rapport à la forme de l'objet (sur l'extrémité, la surface ou le flanc, concentrées ou éparées) pour en déterminer la spécificité. D'autres paramètres, telles la nature et les caractéristiques de la roche, facilitent le diagnostic. Cette reconstitution s'appuie sur plusieurs méthodes : la tracéologie, mais aussi l'expérimentation, la confrontation avec les vestiges voisins et l'observation ethnographique.

Lorsque nous avons ainsi retrouvé le fonctionnement d'un galet, nous pouvons nous intéresser à sa fonction, en remplaçant les gestes au sein d'une chaîne opératoire : par exemple, pour



2. LA MOUTURE était connue de certains groupes du Paléolithique, bien avant l'invention de l'agriculture. Les stries et les traces de colorant visibles sur la surface de cette grande plaque de schiste (*en bas, longueur réelle : 28 centimètres*) qui provient de l'abri du Cap Blanc, en Dordogne, attestent en effet que de l'ocre y a été broyée et moulue, il y a 14 000 à 11 000 ans. C'est l'une des rares meules entières connues au Paléolithique supérieur. Elle a été utilisée avec un broyeur semblable à ce volumineux galet de grès rose (*en haut, longueur réelle : 13,5 centimètres*), dont les faces et les flancs sont usés et striés. Celui-ci, qui provient de niveaux de 28 000 à 22 000 ans de la grotte d'Isturitz, dans les Pyrénées-Atlantiques, a fait l'objet d'un ravivage de ses surfaces, comme cela se pratiquait fréquemment à partir du Néolithique : la surface est piquetée pour être rendue à nouveau rugueuse, afin de mieux mordre la matière à moudre et à écraser.