CONCOURS EXTERNE DE CONTRÔLEUR
STAGIAIRE DU TRÉSOR PUBLIC

ANNÉE 2006

ÉPREUVE N°2 A OPTION

Durée : 3 heures – Coefficient : 4

---

*Toute note inférieure à **6/20** est* **ÉLIMINATOIRE**

<u>TRÈS IMPORTANT</u> :

Le candidat traitera celui des trois sujets ci-après qui correspond à l'option qu'il a choisie lors de son inscription au concours : CE CHOIX NE PEUT PAS ÊTRE MODIFIÉ.

Sous peine d'annulation de leur copie, les candidats ne doivent porter aucun signe distinctif (nom, prénom, lieu, etc.) sur la partie réservée à la rédaction.

Les candidats ne peuvent quitter la salle moins d'une heure après le début des épreuves.

L'utilisation de tout document et matériel est interdite.

Tournez la page S.V.P.

ATTENTION INTERNET VOUS SURVEILLE !

(2 952 mots)

****

Tout ce que vous faites sur le net pourra être utilisé contre vous. Parce que chaque connexion laisse ici et là des empreintes indélébiles. Les entreprises ne se gênent pas pour les collecter, à des fins de marketing. Les Etats de même : des dictatures, comme la Chine, exercent sur le Réseau un contrôle étroit ; des démocraties, comme la France, se dotent au nom de la lutte contre le terrorisme ou la pédophilie, de législations autorisant toutes les dérives.

Dans les films policiers des années 1950-1960, parmi les scènes obligées du genre, il y avait celle où l'on voyait l'ennemi public n°1 ou le vilain kidnappeur appeler la police d'une cabine téléphonique plantée au milieu d'une banlieue déserte, et proférer des menaces ou poser ses conditions ; puis, coupant court au dialogue que ses interlocuteurs tentaient de lui imposer, raccrocher le combiné et détaler. Une légende voulait en effet, à l'époque, que la police fût capable de localiser un appel ; mais, pour que la procédure réussisse, celui-ci devait durer au moins trente secondes....

Devrons-nous bientôt, nous aussi, abréger nos consultations au minimum lorsque nous surfons, le dimanche après-midi chez nous, sur des sites Internet reflétant des penchants sexuels, politiques ou autres ? Si la question se pose, c'est qu'en matière d'intimité et de respect de la vie privée, on a vraiment fait mieux, dans l'histoire, que le Web.

De fait, le réseau ressemble désormais à une illustration du célèbre Panopticon de Jeremy Bentham, ce projet de prison modèle imaginé à la fin du XVIII^{ème} siècle par l'un des fondateurs anglais du libéralisme, où un seul homme pouvait observer tous les autres sans lui-même être vu. Le philosophe Michel Foucault y vit le symbole du pouvoir de surveillance installé par nos sociétés modernes. Nos appels Internet transitant par des opérateurs agréés, les fournisseurs d'accès, tous nos actes peuvent être retracés à la fraction de seconde près grâce au numéro d'identification de notre poste, notre adresse IP (pour Internet Protocol), enregistrés et conservés. Avec possibilité de les utiliser un jour, au besoin, comme élément de preuve.

On peut ainsi, potentiellement, déterminer non seulement quels sites nous avons visités, mais aussi quels éléments de leurs pages nous avons téléchargés. Pour accéder aux logs, aux traces électroniques que laissent derrière eux nos ordinateurs quand ils se connectent avec des sites, rien de plus simple : il suffit de s'adresser aux opérateurs, lesquels connaissent de surcroît notre état civil, notre adresse et, last but not least, nos coordonnées bancaires.

Et ils ne sont pas les seuls dans ce cas. Les sites à qui nous refusons de donner notre adresse mail, croyant ainsi rester de parfaits anonymes, peuvent aussi connaître nos habitudes, nos marottes, qu'expriment nos consultations. Avec des méthodes d'analyse mathématiques très banales, on peut ainsi dresser de loin notre « profil » de consommateur pour nous proposer telle ou telle offre spéciale de promotion d'un nouveau produit, avec l'espoir que nous l'adopterons.

Certes, ces méthodes appartiennent à cette déjà vieille pseudo-science qu'est le marketing. Mais elles sont désormais pratiquées en temps réel, actualisant les résultats en permanence et sans avoir à se lancer dans de ruineuses enquêtes avec constitution de panels et de questionnaires. C'était au départ un service rendu par ces sites, un « bon mouvement » de leur part, afin que nous puissions les consulter avec un meilleur confort de connexion, qui leur sert à « tracer », comme l'on dit, nos comportements.

Les cookies, ces courtes lignes de programme qui se déposent à notre insu dans la mémoire de nos disques durs la première fois que nous visitons certains sites, sont devenus aujourd'hui

Tournez la page S.V.P.

presque inoffensifs. La plupart des navigateurs actuels nous les signalent et nous pouvons aisément les effacer, ou ordonner à notre ordinateur de les rejeter systématiquement. Mais des procédures plus sophistiquées leur ont succédé, tels ces *spywares* ou logiciels espions, que nous implantons souvent à notre insu sur nos disques durs quand nous téléchargeons des logiciels gratuits, supposés là aussi nous aider, mais qui permettent d'épier tous nos gestes.

C'est paradoxalement le raffinement même de nos techniques de communication que nous a apporté l'Internet qui permet ce contrôle accru et si efficace sur nos vies. Elles nous aident à mieux correspondre entre nous, mais rendent en même temps plus aisée notre surveillance - le bouquet en ce domaine étant remporté haut la main par nos mails.

Ces derniers sont à peu près aussi confidentiels que des cartes postales. S'ils ne sont pas cryptés, ces messages peuvent être lus à chaque étape de leur acheminement. On les duplique en un éclair de seconde ; et personne ne peut s'en rendre compte. A l'aide d'un scan, il est également possible d'y repérer certains mots-clés. Cette procédure permet de les trier, de mettre à part ceux que l'on juge dignes d'intérêt, afin de les examiner plus tard, à tête reposée.
« Conserver chaque courrier envoyé par la poste nécessiterait une infrastructure énorme, résume l'Américain Ben Edelman, un juriste consultant pour l'American Civil Liberties Union (ACLU), association de défense des libertés politiques individuelles. *Dans le monde électronique, quelques gros ordinateurs peuvent faire le même travail, mieux que les êtres humains et pour un coût réduit. Cette simplification permet aux gouvernements d'envisager des types de surveillance qu'ils n'auraient sans doute pas pratiqués auparavant. »*

Blocage de certaines pages ; listes noires de mots-clés tels que « démocratie », « droits de l'homme », etc., qui enrayent les recherches lorsqu'on tape ces mots ; pages-miroirs, aussi vraies que les originales, qui déroutent les trop curieux vers des sites-pièges, etc. ; les gouvernements rêvant de contrôler la navigation de leurs sujets sur la Toile n'ont que le choix des moyens. Et tous sont d'une simplicité et d'une économie désarmantes. Il suffit parfois de débrancher un modeste câble ou de fermer un seul des quelque 60 000 ports de communication pour rompre le contact avec un pan entier du Net. Certains pays, comme la Tunisie, ne font pas dans la demi-mesure, exigeant des fournisseurs d'accès qu'ils connectent leurs serveurs à un superordinateur central installé dans les locaux du ministère de l'intérieur. D'autres, plus subtils, comme l'Arabie Saoudite, font disparaître de certaines pages les éléments qui les dérangent ! Staline, c'est sûr, aurait adoré le Net…

Et on aurait tort de croire que l'usage de ces procédés de filtrage est l'apanage des dictatures. Depuis le 11 septembre 2001 - et sans doute avant, car les attentats de New York n'ont fait que précipiter une tendance déjà existante, comme en témoigne le projet Carnivore du FBI, censé, dès 2000, scruter les mails des américains - , nos démocraties ne sont pas en reste. Mieux : c'est avec notre bénédiction qu'elles pratiquent ce contrôle sous le couvert de la sécurité intérieure, comme l'a montré le récent vote du projet de loi antiterroriste Sarkozy. Servitude volontaire, avez-vous dit ?

En novembre 2001, surfant sur la vague de psychose née des attentats de New York, la loi française sur la sécurité quotidienne (LSQ) impose aux fournisseurs d'accès de conserver les logs (les traces de connexion des internautes) pendant un an. Le décret d'application ne verra jamais le jour… En 2002, la loi sur la sécurité de l'information (LSI) pérennise les dispositions adoptées un an plus tôt. Mais le décret d'application une fois encore n'a pas été publié… En 2005, le projet de loi relatif à la lutte contre le terrorisme, dit « projet Sarkozy », revient sur la question initiale des logs. Il élargit (aux cybercafés, notamment) la liste des organismes qui doivent les conserver et évince le judiciaire, traditionnel garant des libertés publiques, de la procédure, afin de permettre aux policiers d'accéder directement à eux. Le projet de loi a été avalisé par les deux chambres du Parlement. Se dissociant de leurs collègues députés, qui

Tournez la page S.V.P.

s'étaient abstenus, les sénateurs socialistes ont saisi le Conseil constitutionnel. En pure perte : celui-ci vient de juger le texte conforme à la Constitution.

Devant cette accumulation de mesures rarement suivies d'effets, force est de se demander à quoi peuvent servir toutes ces annonces. Il est certes plus facile de promulguer une loi que de s'attaquer à un problème. Dans le cas d'Internet, ce « prurit législatif », selon les mots du juriste Sébastien Canevet, a peut-être pour vertu essentielle de produire de la confusion. Pas mal d'internautes en viennent à croire qu'il est illégal de consulter certains sites « dangereux », alors que ce délit n'existe pas. Et le fin du fin du contrôle ne réside-t-il pas dans l'autocensure ?

La morale peut aussi opportunément venir à la rescousse. En Thaïlande par exemple, la lutte contre les sites pédophiles sert, par ricochet, à censurer l'expression des revendications sécessionnistes de certaines régions du Sud. Et qui peut assurer qu'un tel comportement ne nous atteindra jamais ? Google tente ainsi depuis quelques semaines de résister au département américain de la justice qui, réactivant une loi de protection contre la pornographie en ligne datant de 1998 (mais jamais appliquée en raison de l'opposition de la Cour suprême), lui demande de fournir toutes les données sur les recherches des particuliers à ce propos sur son site. Des informations qu'America Online, Yahoo ! et MSN auraient en revanche données sans problème…

L'Internet menace aujourd'hui de se transformer en une immense centrale de contrôle politique, économique et moral. Quel contraste avec les espoirs levés au milieu des années 1990 ! A entendre certains, il ouvrait un espace de liberté totale, hors de toute censure, délivré du poids de l'économie marchande. Bref, le rêve d'une autogestion généralisée, grâce à laquelle nous allions devenir, enfin, des individus libres et autonomes ne s'autorisant que d'eux-mêmes.

Mais cessons là les lamentations ! Ce qu'il y a de rassurant et même de passionnant, dans l'affaire, c'est que l'Internet lui-même offre des parades aux mécanismes de contrôle qu'il permet. Et vice versa, pourrait-on ajouter. A toute technique de contrôle correspond une technique d'anticontrôle. A moins de se trouver dans un pays comme la Chine, qui a su construire une Grande Muraille numérique infranchissable, contourner l'interdiction de consulter un site est le plus souvent un jeu d'enfant.

Dans les entreprises, on appelle *firewalls* (pare-feu) ces systèmes destinés à prévenir l'accès par des internautes extérieurs à des informations privées, telles celles qui circulent sur l'intranet. C'est un système de cet ordre, mais étendu au niveau d'un pays tout entier, que la Chine a dressé face à l'Internet étranger. On ne connaît que peu de chose sur la façon dont fonctionne d'un point de vue technique ce « grand firewall ». On sait seulement qu'il filtre l'accès aux sites jugés indésirables et permet de voir ce qui circule sur le réseau. Des mots-clés font par ailleurs fonction d'alerte lorsqu'ils sont utilisés par les internautes chinois. Bâtir un tel système de protection est une prouesse technologique ; et plusieurs organisations de défense des libertés, Reporters sans frontières et Human Rights Watch, suspectent certaines firmes occidentales, Sun Microsystems, Nokia, Motorola, Cisco, Microsoft et AOL, d'avoir aidé, contre des garanties de parts de marché, à sa mise en place. Depuis plusieurs années, Yahoo ! filtre de lui-même le contenu renvoyé aux visiteurs de son portail chinois. En 2005, le moteur de recherche a même communiqué aux autorités des informations concernant le journaliste Shi Tao, qui furent utilisées comme pièces à conviction à son procès, à l'issue duquel il fut condamné à dix ans de prison. Et il y a deux semaines, on apprenait que Google, l'entreprise « rebelle », avait elle aussi accepté de filtrer l'accès à certains sites interdits par les autorités chinoises. « *Je n'aime pas cela*, a déclaré Jerry Yang, le cofondateur de Yahoo !, *mais nous devons suivre la loi.* » Celle de la liberté ou celle du marché ?

L'Internet étant un réseau mondial, il suffit parfois de passer tout simplement par un moteur de recherche étranger. On peut aussi adresser sa demande à un serveur relais, localisé lui aussi à l'étranger et échappant donc au contrôle. Les *proxies* - en anglais juridique, le mot désigne les procurations qu'on donne à une personne dans une affaire - servent à cela. La demande vers un certain site semblera, grâce à eux, émaner d'un autre poste que le nôtre. Les logiciels dits « anonymiseurs » ne font que systématiser cette idée. Ils nous épargnent la tâche d'avoir à rechercher ces sites sanctuaires, renvoyant nos demandes sur des proxies préétablis. Pour rendre plus difficile l'identification, on mélange ces méthodes, en recourant de plus en plus au téléphone pour demander, via Singapour ou Rio de Janeiro, tel ou tel site.

Pour briser les velléités de contrôle d'un Etat, on peut également songer à les désorganiser selon le principe des grèves du zèle d'antan, par le trop plein. C'est ce qu'essaya de faire en 1999 ADM, un collectif international de hackers, en tentant de bloquer le système Echelon de la National Security Administration (NSA) américaine, conçu pour écouter tout ce qui transite par le mail, le téléphone, le fax, les satellites, etc... Les activistes élaborèrent un programme engendrant des mails qui véhiculaient les mots-clés censés alerter Echelon. Le but était de submerger le système de filtrage jusqu'à ce qu'il demande grâce. L'entreprise échoua. Le nombre de mails n'était sans doute pas suffisant pour saturer Echelon, qui traite déjà un bon milliard de communications par jour émanant en priorité des entreprises et des gouvernements, moins des particuliers. Mais, depuis le 11 septembre, la donne pourrait avoir changé, et la méthode s'avérer efficace au cas où la tentation totalitaire saisirait nos démocraties sous l'effet de la lutte contre le terrorisme. Donald Rumsfeld ne vient-il pas de reconnaître que la NSA menait des opérations de surveillance de citoyens américains depuis plusieurs années ?

C'est un secret de Polichinelle que, dans nombre de pays totalitaires, bien des *sites proxies* sont des leurres. Quant à l'incognito procuré par les anonymiseurs, il repose sur la confiance que leurs utilisateurs veulent bien accorder aux sociétés qui les leur ont vendus. Dirigés par des indélicats, ils pourraient devenir de parfaits instruments de chantage. Bref, la parade non seulement n'est pas absolue, mais soulève à son tour d'autres problèmes : « *le recours aux proxies et aux autres technologies assurant une protection satisfaisante de la vie privée,* remarque Ben Edelman, *reste encore réservé à quelques utilisateurs. Si leur usage devait s'imposer, nous verrions peut-être surgir un système de classes, où seule une élite technologiquement avancée d'internautes s'en sortirait. Et puis, imaginez que les gouvernements décident de mettre en place des procédures pour traquer ceux qui utilisent systématiquement des proxies ! tout serait à refaire...* »

Drôle de dialectique ! Entre les mains des hackers, les procédés de contrôle se retournent régulièrement en moyen de lutte contre la surveillance ; tandis que, dans celles du système étatique ou industriel, les innovations d'anticontrôle imaginées par les internautes se renversent tout aussi régulièrement en armes de contrôle... Comme si se déroulait un jeu de cache-cache perpétuel entre ceux qui tentent de maintenir coûte que coûte le caractère libertaire de l'Internet et ceux qui cherchent à en tirer du profit.

Entre 1999 et mars 2003, c'est une véritable guérilla électronique souterraine qui a opposé ainsi en France, un site ouvertement raciste et islamophobe, SOS-Racaille, et des hackers du bord opposé cherchant à identifier la personne se cachant derrière son hébergeur et, de fil en aiguille, l'ensemble du groupe. Grand technicien, l'individu présumé, un certain « Caméléon », avait disposé tout un réseau de *proxies*, d'anonymiseurs et de sites-miroirs, etc., que ses adversaires tentèrent de déborder afin de s'insinuer sur son serveur et de le désorganiser. Ce qui arriva finalement, Caméléon abandonnant le logiciel de cryptographie PGP qu'il utilisait au profit d'un autre, qu'il ne maîtrisait pas. Cassant ce nouveau système, les hackers réussirent à

Tournez la page S.V.P.

s'immiscer dans les conversations des membres de SOS-Racaille et à identifier la plupart d'entre eux.

Car Internet a ceci de particulier qu'il est peut-être la première technique dans l'histoire à se développer par l'initiative de ceux qui s'en servent, c'est-à-dire nous. Et c'est ce caractère d'univers en expansion permanente qui peut lui éviter de dégénérer en une technique de contrôle absolu. A l'inverse de ce qu'avait imaginé Bentham dans son Panopticon, nous détenons, autrement dit, le moyen de brouiller la vue de notre gardien. Grâce aux méthodes précédemment évoquées, mais aussi par simple effet de masse. Bref, c'est le développement même du Net qui dresse les plus sûres limites à son contrôle.

Pour qu'il reste fidèle à l'espoir originel, pour qu'il ouvre un nouveau modèle participatif de production, chacun doit donc prendre part à son évolution. *« Appelez cela comme vous voudrez, blog, vlog, photologging, etc., il n'a jamais été aussi facile de publier des idées personnelles qu'aujourd'hui sur l'Internet,* souligne l'Américain Ryan Junell, le cofondateur de Webzine, un événement réunissant tous les ans les passionnés de publication indépendante sur le Net. *Que n'importe qui, avec un peu de savoir-faire technique, puisse être présent en ligne en quelques minutes, publier une opinion accessible mondialement et à laquelle le reste des internautes soit en mesure de répondre, on peut se demander ce qu'en penserait Gutenberg... Internet ne porte aucune promesse assurée en soi. Ce n'est qu'une technologie, un médium. Et il ne tient qu'à nous d'en faire un usage émancipateur. »*

La « fracture numérique » se situe peut-être précisément là : entre ceux qui se font utiliser par le Net et ceux qui savent l'utiliser. En quoi Internet ne fait que poser un problème éternel, aussi vieux que notre présence sur Terre : pour rester libératrice, la technique doit être l'affaire de tous. Se désintéresser d'elle est le plus sûr moyen de se faire broyer par elle.

Le Monde 2 n°104
Supplément au Monde
du 11 février 2006