

Le Monde 2

TÉLÉPHONES,
ORDINATEURS,
CAMÉRAS, CARTES
ÉLECTRONIQUES :
IL DEVIENT DE PLUS
EN PLUS DIFFICILE
DE SE SOUSTRAIRE
À LA SURVEILLANCE
DES TECHNOLOGIES
MODERNES. NON
SANS DOMMAGE
POUR LA VIE PRIVÉE.

PEUT-ON ENCORE DISPARAÎTRE ?

CINÉMA Entretien exclusif avec Martin Scorsese **PHOTO** Des guides de voyage à voir

ARCHIVES Nouvelle-Calédonie : vingt ans après la prise d'otages d'Ouvéa

le grand entretien

NOS TÉLÉPHONES PORTABLES SONT DES MOUCHARDS, NOS ORDINATEURS DES BALANCES. LES LIBERTÉS INDIVIDUELLES SE RÉDUISENT AU RYTHME DU DÉVELOPPEMENT DES NOUVELLES TECHNOLOGIES. POURTANT, LOIN DE NOUS EN INQUIÉTER, NOUS FAVORISONS CETTE SURVEILLANCE EN DÉVOILANT NOS VIES SUR INTERNET OU EN UTILISANT DES PASSES ÉLECTRONIQUES. SACRIFIER SA LIBERTÉ POUR LE CONFORT, LE DIVERTISSEMENT OU LA SÉCURITÉ : THIERRY ROUSSELIN, COAUTEUR DE « SOUS SURVEILLANCE », NOUS MET EN GARDE CONTRE CE MARCHÉ DE DUPES. PROPOS RECUEILLIS PAR JÉRÔME FENOGLIO – PHOTOS DESIREE PALMEN

« Streetwise ». Arrêt de bus, Rotterdam, 2002.

Peut-on échapper à la surveillance?

Satellites d'observation, caméras de vidéosurveillance, passeports biométriques, fichiers administratifs, policiers ou commerciaux, puces à radiofréquence,

GPS, téléphones portables, Internet : le citoyen moderne est au centre d'un réseau de technologies de plus en plus perfectionnées, et de plus en plus indiscretes. Chacun de ces outils, censé nous apporter sécurité et confort, nous en demande chaque jour un peu plus sur nous-même, nous classe, voire nous observe. A la fois complices et inconscients, nous avons basculé dans une société de surveillance. Est-il encore possible d'échapper à ces multiples dispositifs qui nous environnent ? Nous l'avons demandé à Thierry Rousselin, consultant en observation spatiale, ancien directeur de programme d'armement à la Délégation générale pour l'armement, qui publie avec Françoise de Blomac, spécialiste des nouvelles technologies d'information, *Sous surveillance* (Les Carnets de l'Info), un très utile tour d'horizon de ces technologies, qui tente de faire la part entre fantasmes et vrais risques de dérives.

Quels sont aujourd'hui les grands domaines de la surveillance technologique ?

On pourrait tracer des cercles concentriques. Le premier, ce sont les « morceaux » de nous-mêmes, tout ce qui concerne la biométrie. On donne progressivement un certain nombre d'éléments qui nous appartiennent, qui nous identifient. Cela a commencé avec nos empreintes digitales. C'est maintenant au tour de notre ADN, notre iris, la paume de notre main, bientôt notre manière de marcher ou nos tics. Notre identité est en train de se confondre avec notre biologie et nos comportements physiques. Le second cercle, ce sont tous les capteurs qui nous entourent : ceux qui nous regardent avec la vidéosurveillance, les webcams, les drones, les avions, les hélicoptères, les satellites. Il y a aussi l'écoute, dans tous les sens du terme. Il ne faut jamais oublier que le premier moyen d'écoute, c'est une personne à côté de nous. On peut aussi utiliser nos propres outils, le téléphone notamment. On m'a vu, on m'a écouté, sait-on également où je suis ou qui je suis par le

biais de mes propres objets ? Je me suis payé un GPS ou un téléphone portable. Est-ce qu'on est capable de me suivre à cause de ces appareils ? Les multiples cartes – de paiement, de fidélité, d'abonnement – que j'ai dans mon portefeuille racontent-elles des choses de moi en temps réel à chaque fois que je les emploie ? Les formulaires que j'ai remplis depuis trente ans dessinent-ils une image de moi plus précise que mes propres souvenirs ?

Le dernier point concerne l'ordinateur. Est-ce qu'en l'utilisant, je lui transmets des informations au-delà de ce que je suis en train de taper ? Depuis un certain nombre d'années, on voit bien que, dans chaque instruction judiciaire, les policiers embarquent l'ordinateur. C'est bien qu'il peut raconter des choses sur nos activités. Après, il y a Internet. Là, on s'inquiète que des gens soient capables de passer par le réseau pour nous subtiliser de l'information. Est-ce que ma soif de me ►

La photographe

• Desiree Palmen est née aux Pays-Bas en 1963. Après des études d'art spécialisées dans la sculpture, à Maastricht, elle participe à de nombreuses expositions d'art contemporain en France, en Allemagne ou en Israël...
• En 2001, quand la police de Rotterdam décide d'installer des caméras de surveillance dans les rues, elle a l'idée de créer des « vêtements de camouflage » pour les citoyens qui veulent se cacher de ces regards indiscrets. Desiree Palmen ne retouche aucune de ses images : elle photographie des endroits et peint des vêtements avant de se mettre elle-même en scène dans l'environnement choisi. Elle ne sélectionne pas les lieux de ses clichés au hasard : ils sont pour la plupart l'objet de la surveillance des caméras policières, à l'image de Jérusalem où des caméras installées dans la vieille ville en 2000 pour la venue du pape n'ont jamais été retirées. www.desireepalmen.nl

REMERCIEMENTS : RISK HAZEKAMP ET JUTTA TRANKLE POUR LA SÉRIE DE JÉRUSALEM



« Interior camouflage ». Bibliothèque, 2004.



« Old city suit ». Surveillance policière dans le quartier chrétien, Jérusalem, 2006.

► faire des amis, de me faire connaître ne me conduit pas à raconter trop de choses qui pourraient être, un jour, utilisées contre moi ? Les domaines de surveillance touchent donc aujourd'hui quasiment toutes nos interactions avec le monde extérieur, presque tous nos sens.

Les inquiétudes sont d'autant plus vives que l'on voit bien que l'on aurait beaucoup de mal à se passer de nombre de ces technologies.

Oui, nous sommes en grande partie complices de la progression de la surveillance. D'abord, cela nous simplifie la vie. Nous préférons avoir une carte qu'un ticket pour entrer dans le bus, cela nous évite de composer. Le passe Navigo, que la RATP est en train de substituer à la carte Orange, contient une puce RFID [à radiofré-

déplacements contenues dans le boîtier électronique du véhicule. Les clients ont échangé une économie substantielle contre la perte de la confidentialité de leurs allers et venues. À l'inverse, protéger son anonymat peut coûter plus cher. La CNIL a demandé à la RATP de proposer une carte sans informations personnelles. C'est le passe Navigo Découverte : il existe, mais il est plus onéreux que le passe classique.

Beaucoup de maires français se sont lancés dans la vidéosurveillance, sur le modèle de la Grande-Bretagne où est déjà déployé le total de 25 millions de caméras. À quoi est dû cet engouement ?

C'est très irrationnel. En novembre, Michèle Alliot-Marie, ministre de l'intérieur, a affirmé que « l'efficacité

« Très souvent derrière les systèmes technologiques de surveillance, il y a l'incapacité du pouvoir à apporter de vraies réponses aux problèmes posés »

quence], sur laquelle sont chargées des données personnelles qui permettent de reconstituer tous vos déplacements sur deux jours. En l'utilisant, vous ne vous déplacez donc plus tout à fait anonymement. Mais la carte a permis de gagner du temps aux guichets et aux portillons, et de fluidifier les flux de voyageurs. La plupart des usagers la considèrent donc avant tout comme une amélioration du service.

Aux États-Unis, une société commercialise une carte spéciale pour éviter les longues files d'attente dues aux contrôles dans les aéroports. Pour l'obtenir, il faut répondre à un questionnaire très détaillé en ligne et fournir des éléments d'identification biométriques. Récemment, un des premiers abonnés commentait le service en ces termes : « En m'inscrivant, je me suis mis à penser : j'espère qu'ils ont un putain de système de sécurité vu la quantité d'informations que je leur fournis... Mais je n'y penserai plus quand je passerai en sifflotant dans ma voie réservée, en regardant la queue des cent couillons qui attendent. » C'est tout à fait typique de notre ambivalence sur ces questions. Nous sentons bien que nous confions des éléments éminemment intimes, parfois à des sociétés qui n'existaient pas l'année précédente. Mais elles fournissent des services tellement pratiques que nous préférons oublier les risques que cela fait courir. C'est aussi le cas des solutions RFID et GPS destinées aux enfants ou aux malades d'Alzheimer. Nous acceptons la surveillance parce qu'elle concerne nos proches les plus fragiles. Mais pour les industriels, ces techniques mettent aussi en place les conditions d'un marché. Nous avons commencé à les accepter pour les gens auxquels nous tenons le plus, et cela ouvre la voie à un usage de masse.

L'intérêt financier peut-il également jouer ?

Bien sûr ! Si je prends une carte de fidélité, je vais avoir des cadeaux en échange de quelques données personnelles. En Grande-Bretagne, plusieurs compagnies proposent des assurances moins chères pour des automobilistes qui s'engagent à ne pas rouler certaines heures de jours « à risques ». Pour vérifier, les sociétés ont le droit de récupérer toutes les informations sur les

de la vidéosurveillance pour améliorer de façon significative la sécurité quotidienne n'est plus à démontrer ». Pourtant, il n'existe pas de travail de recherche qui confirme l'efficacité des caméras. Très souvent derrière les systèmes technologiques de surveillance, il y a l'incapacité du pouvoir à apporter de vraies réponses aux problèmes posés. On installe des caméras parce que c'est très visible et que cela coûte moins cher que d'embaucher des gens et de conduire un véritable travail de terrain. Tout le monde s'y met donc alors qu'au Royaume-Uni la plupart des bilans sont très mitigés. L'effet est très faible en matière de prévention, de dissuasion, surtout sur les atteintes aux personnes (bagarres, viols...) souvent dues à des gens au comportement impulsif qui se fichent bien de savoir s'ils sont filmés. C'est pareil pour le terrorisme : les « fous de Dieu » ou d'une cause quelconque seraient même heureux de passer ainsi à la postérité. Quant aux petits délits comme ceux pratiqués par ►

| Agir contre la surveillance |

- Privacy International (www.privacyinternational.org), qui milite depuis 1990 contre la surveillance et pour la défense de la vie privée, est sans doute l'ONG qui a la plus grande influence internationale dans ce domaine. Elle publie un classement annuel des pays où la vie privée est la plus menacée : dans le dernier, la France est classée parmi les « pays de surveillance développée ». Les Big Brother Awards, émanations de Privacy International, sont décernés chaque année, dans une vingtaine de pays, pour « distinguer les prédateurs de la surveillance ». En France, ils viennent notamment de sanctionner, le 21 mars, les sociétés fabriquant des drones de surveillance et Google (bigbrotherawards.eu.org).
- Une équipe mixte de chercheurs juristes et informaticiens présente en ligne ses travaux sur le droit et la sécurité informatique (www.asphales.cnrs.fr).
- La CNIL permet de visualiser sur son site les traces laissées par chaque internaute sur le web (www.cnil.fr, rubrique « découvrir » puis « vos traces »).
- Dans le domaine artistique, parmi de nombreuses initiatives, le cinéaste Adam Rifkin a réalisé un film entièrement tourné avec des caméras placées juste à côté d'authentiques caméras de surveillance ou dans des lieux où l'on peut en trouver. *Look* vient de sortir aux États-Unis.
- En Grande-Bretagne le Manifesto for CCTV Filmmakers (Manifeste de réalisateurs de films de vidéosurveillance) regroupe des artistes qui exploitent des vidéos tournées avec des caméras de surveillance. Ils récupèrent ces images en vertu de la loi qui permet aux personnes filmées de se faire remettre les enregistrements qui portent atteinte à leur vie privée.

► les pickpockets dans le métro, ils sont trop rapides pour être repérés et leurs auteurs passent à l'acte dans des lieux souvent étendus aux multiples issues. La vidéosurveillance est surtout une aide précieuse dans la résolution d'enquêtes a posteriori.

Etant donné cette généralisation des moyens de surveillance, est-il encore possible de « disparaître » dans nos sociétés, d'échapper au contrôle de la technologie ?

Disparaître est encore possible : plusieurs milliers de personnes le font volontairement chaque année en France sans que les impôts ou l'Urssaf ne les retrouvent. Mais il faut savoir ce que cela représente comme efforts, surtout si vous restez dans la légalité, sans

« Disparaître est encore possible : plusieurs milliers de personnes le font volontairement chaque année, sans que les impôts ou l'Urssaf ne les retrouvent »

fausse identité ou chirurgie esthétique. L'option « île déserte » est en apparence la plus simple à réaliser. Vous vous retirez dans une zone rurale dans laquelle vous pourrez pratiquer un mode de vie minimalisant les échanges commerciaux – sans ordinateur ni téléphone portable –, il en existe encore en France. Vous fermez votre compte en banque et payez tout en liquide. Il faudra vous astreindre à ne plus voyager à

À LIRE
Sous surveillance
de Françoise de Blomac et Thierry Rousselin, Les Carnets de l'info, 224 p., 16 €.

l'étranger, a fortiori aux Etats-Unis, pour éviter de vous faire établir des papiers faisant appel à la biométrie. Il faudra rester avec votre vieille carte d'identité qui est valable, en France, tant que vous êtes reconnaissable sur la photo. Bien sûr, pas question de scolariser vos enfants dans le système officiel. Et la vraie limite concernera la santé, car à partir du moment où vous avez besoin du système de soins français, vous faites obligatoirement partie des fichiers.

Le problème, c'est que cette mise en retrait de la société va surtout ressembler à un voyage vers le passé, à un retour vers des formes anciennes de contrôle social. Dans votre petit hameau perdu, il n'y aura presque personne, mais tout le monde à dix kilomètres à la ronde saura tout de vos habitudes de vie courante, de vos particularités. Les siècles précédant la technologie moderne étaient loin d'être des époques sans surveillance. Pour éviter cela, vous pouvez préférer vous fondre dans la jungle urbaine. La foule des villes peut encore garantir l'anonymat. Mais dans ce cas, la marge entre sortie du système et exclusion est dangereusement étroite. Vous passerez inaperçu, mais avec un mode de vie de plus en plus proche de celui d'un sans-abri.

Sans aller aussi loin, peut-on encore au moins contrôler les informations qu'on laisse sur soi ?

Si vous décidez de rester dans la société, des informations circulent nécessairement sur vous. Vous payez vos impôts au fisc qui par conséquent sait des choses sur vous, de même que votre employeur, etc. Vous n'en êtes pas mort jusqu'à présent et vous n'en mourrez pas. En

revanche, vous pouvez éviter de donner sur vous-même des renseignements que personne ne vous oblige à révéler. Vous pouvez éviter de remplir tous les questionnaires auxquels vous ne faites même pas attention, généralement sous prétexte de bénéficier de cadeaux de pacotille. On peut très bien survivre sans cartes de fidélité et sans avoir donné son état civil complet pour l'achat d'un grille-pain. Certes on y gagne, mais c'est surtout le droit à ce que l'ensemble de nos achats soient analysés, identifiés. Les cartes de fidélité alimentent consciencieusement des bases de données qui mémorisent toutes les transactions. Progressivement, on laisse donc se constituer une mine d'informations sur soi-même. Certains de ces fichiers circulent librement, si

vous avez oublié de cocher la petite case en bas à droite interdisant à votre interlocuteur de céder vos coordonnées à des « partenaires ». Donc lorsque vous remplissez des questionnaires non obligatoires, vous n'êtes absolument pas forcé de donner des informations réelles. Rien ne vous empêche de vous tromper sur votre adresse ou votre numéro de téléphone.

Les téléphones portables sont de plus en plus souvent considérés comme des mouchards potentiels. Peut-on encore limiter ce risque ?

A partir du moment où votre appareil est allumé ou en veille, votre opérateur, sur demande d'un surveillant, peut effectivement mettre en route tout un tas de mécanismes d'espionnage. Pour la localisation, il existe différentes procédures qui permettent de vous situer à cinquante mètres près, en se servant, par triangulation, des trois antennes-relais les plus proches de votre téléphone. C'est ce qui a été utilisé pour repérer le commando qui avait assassiné le préfet Erignac. Les téléphones de nouvelle génération, qui constituent aujourd'hui le haut de gamme, contiennent une puce GPS et seront localisables beaucoup plus facilement, et plus précisément.

Pour l'écoute, cela ne se limite pas à la possibilité d'intercepter une conversation, ce qui est devenu très simple. Un opérateur a aussi la capacité de déclencher un portable comme micro d'ambiance. Juridiquement, les services de police peuvent, sous certaines conditions, demander à l'opérateur de transformer le téléphone en micro et d'écouter tout ce qui se dit autour de la personne qui le porte. Mais dans tous ces cas, pour la localisation comme pour l'écoute, il faut que le portable en question ne soit pas éteint. S'il l'est, plus rien n'est possible, contrairement à ce qu'ont affirmé nombre d'articles qui ont confondu éteint et en veille. Donc, si vous voulez éviter d'être repérables en permanence, faites comme les policiers ou les truands, coupez votre portable dès que vous ne vous en servez pas. Evidemment, au passage, vous perdrez l'un des grands intérêts de l'appareil, celui de pouvoir être joint en permanence. ►



« Interior camouflage ». Porte ouverte dans le studio de l'artiste, Rotterdam, 2004.



Couple sur un banc public, 2001.

► La plus grosse brèche dans notre vie privée reste tout de même l'ordinateur connecté à Internet ?

C'est certain. La plupart des ordinateurs nous sont livrés avec des systèmes d'exploitation qui donnent juridiquement le droit à Microsoft ou Apple de placer des espions chez vous, censés être là pour de bonnes raisons. Dès le raccordement en ligne, et en dehors de toute décision autonome de notre part, tout un petit trafic va se dérouler pour proposer des mises à jour, vérifier que nous n'utilisons pas des éditions piratées et collecter des informations sur notre poste de travail. Récemment, le Land de Rhénanie-du-Nord-Westphalie a voté un texte de loi autorisant la police à mettre des virus d'écoute dans l'ordinateur de suspects. Cela a servi de révélateur en Allemagne. Les gens se sont rendu compte que tech-

niquement c'était enfantin et que des tas d'entreprises savaient le faire. Dès que je surfe en ligne, cela s'aggrave encore. A chaque fois que l'on visionne un site web, il enregistre le nombre de pages vues, leur temps de consultation, les liens suivis, l'intégralité du parcours du client avant la transaction ainsi que les sites consultés avant et après. Imaginez les mêmes méthodes appliquées au magazine que vos lecteurs ont entre les mains : sont-ils prêts à ce que vous connaissiez systématiquement le type de fauteuil dans lequel ils sont assis, le grossissement de leurs lunettes, leurs heures de lecture, le journal qu'ils ont lu avant celui-ci ? Assurément non, et pourtant c'est ce qui se passe, à notre insu, chaque fois que nous surfons. Le *New York Times* a publié une enquête en décembre dernier qui explique que lorsqu'on va sur Yahoo!, on donne 811 informations personnelles simultanées. L'ordinateur est une vraie fenêtre sur le monde, mais elle est sans rideaux.

Dès lors, si je veux être certain de passer inaperçu, je ne vais pas sur Internet. Mais cela équivaut de plus en plus à dire « je sors du jeu social ». Est-ce que cela sera possible dans quinze ou vingt ans, lorsque tout aura été dématérialisé, notamment les formalités administratives ?

Dans ce nouveau « jeu social », pourquoi êtes-vous si critique avec les réseaux sociaux ou la pratique des blogs ?

Parce que, pour moi, le risque majeur se situe là, et notamment en ce qui concerne les adolescents. Ils ont été des millions à ouvrir des blogs ou à participer à des forums où ils vont lâcher énormément d'informations sans se rendre compte des conséquences. On a déjà vu de nombreuses affaires. Des jeunes qui massacrent sur leur blog les entreprises dans lesquelles ils ont fait des stages et qui sont surpris deux ans plus tard d'apprendre que les recruteurs lisent ce genre de choses. Faire des bêtises et vouloir se montrer, c'est propre à l'adolescence. Le problème est qu'on les diffuse sur des systèmes technologiques privés qui vont en garder la mémoire.

90 % des gens qui s'inscrivent dans un réseau social n'y sont plus deux mois après. Ils ont fait tout le processus d'admission puis finissent par se lasser. Ils laissent derrière eux des tas de données personnelles. Je viens de faire une expérience édifiante sur ce point, dans le cadre professionnel. J'étais dans un centre de renseignement militaire. Pour un audit, je visitais les unités de production. Au retour, en rédigeant mon rapport, je m'aperçois que je n'ai pas pris le nom du responsable. Je suis donc allé sur un outil qui permet de chercher qui est sur quel réseau social, l'équivalent d'un métamoteur de recherche pour les réseaux sociaux. J'ai entré les informations dont je disposais (son prénom, sa nationalité et son employeur actuel). J'ai retrouvé ce gars sur LinkedIn. Figurait sur ce site sa biographie qu'il avait lui-même tapée, ainsi que toutes ses affectations militaires jusqu'à son poste actuel. J'étais effaré.

Google et Yahoo! sont ainsi devenus les principaux détenteurs d'informations sur nos comportements, sur nos habitudes de consommation. Ce sont des sociétés qui n'existaient pas il y a encore dix ou quinze ans. Qui peut dire ce qu'elles seront dans vingt ans ?

Nous venons de voir qu'il reste quelques marges de manœuvre si l'on veut échapper à la surveillance technologique. Mais qu'en sera-t-il le jour où tous ces systèmes seront interconnectés, lorsque sera installée la « convergence » des fichiers, des ordinateurs, des moyens d'observation que certains auteurs annoncent comme inéluctable avant 2050 ?

Je ne suis pas sûr que l'on puisse être si catégorique sur l'avènement d'un tel métasystème. Il y a plusieurs facteurs, difficiles à mesurer, qui peuvent retarder cette évolution, voire l'empêcher, en grippant le système. D'abord il y a l'incompétence, qu'il ne faut jamais sous-estimer. Le surveillant est, par définition, parano. Par conséquent, il a plein d'ennemis parmi ceux qui

« Lorsqu'on va sur Yahoo!, on donne 811 informations personnelles simultanées. L'ordinateur est une vraie fenêtre sur le monde, mais elle est sans rideaux »

sont censés être de son côté. Avant d'en arriver à un système qui pourra se passer des humains, il y aura encore des gens qui s'engueulent, des services qui ne se parlent pas, des responsables qui se dissimulent des informations. Le b. a.-ba de l'administration depuis cinq mille ans consiste, entre services, à se cacher mutuellement de l'information. Dans toutes les affaires liées au terrorisme, on s'aperçoit que la logique de base, c'est le FBI qui tape sur la CIA, qui elle-même tape sur la NSA, etc. C'est aussi pour cela que le mollah Omar et Ben Laden courent toujours. C'est ce que je trouve parfois excessif dans les pamphlets sur la surveillance : il y a toujours une exagération de Goliath, cette tendance à penser que le surveillant ne commet pas d'erreurs, qu'il ne se barre pas au milieu de la vidéo pour boire un café, etc. On le rend inhumain. Alors que nombre d'imperfections nuisent au potentiel d'efficacité de la surveillance.

L'autre paramètre à prendre en compte, c'est que chacune des technologies crée ses propres contre-pouvoirs. Pour l'observation (vidéosurveillance ou satellites), on voit que la grande difficulté se situe dans la trop grande quantité d'images par rapport au nombre d'analystes existant et aux capacités techniques d'analyse

disponibles. Des dizaines de milliers d'amateurs qui décryptent des images deviennent aussi puissants que des pouvoirs qui disposent de moyens limités. On l'a constaté au moment de l'ouragan Katrina, où en regardant les images à leur disposition, les internautes ont mis en lumière l'impuissance des autorités américaines. Les citoyens peuvent aussi retourner certains moyens contre leurs concepteurs et surveiller les surveillants. L'un des aspects de notre enquête qui nous a rendus optimistes est l'effervescence créatrice qui est en train de monter autour de ce sujet. De multiples formes de résistances artistiques ou associatives se mettent en place. Elles peuvent retarder ou empêcher le pire, en sensibilisant le grand public.

Plutôt que chercher à passer inaperçu, la solution serait-elle de demeurer actif pour subvertir le système ?

Oui, il reste encore beaucoup de domaines de notre vie personnelle où tout n'est pas joué. Et c'est aussi à chacun de nous de faire en sorte que la surveillance ne s'amplifie pas. On assiste à l'émergence des activistes, on voit des artistes, des gens qui ont des comportements sains. Mais voilà, on tombe sur nos propres facilités, nos petits intérêts momentanés. C'est peut-être contre cela qu'il faut lutter.

Contre nous-mêmes ?

Oui ! Parce que nous aimons bien ce qui est moderne et simple. La force de Google ou d'Apple, c'est des interfaces incroyablement faciles et intuitives, qui nous séduisent. On a tous des amis qui nous ont fait la démonstration de leur nouvel objet superhigh-tech, qui nous vantent à longueur de temps les vertus de leur nouveau téléphone, de leur nouveau PDA [assistant personnel]. Ils sont en train ni plus ni moins de promouvoir le nouvel instrument qui les surveille. Et ils en sont très fiers. Nous sommes tous un peu comme ça. Cela montre que nous sommes modernes. Par moments, il faut savoir se montrer un peu vieux jeu, et accepter que la vie nous soit un peu moins simplifiée. ●

