LE TEMPS

récit Samedi8 décembre 2012

Hacker vaillant rien d'impossible

Par Yves Eudes, Le Monde

Christopher Soghoian est un expert en ordinateurs et il a le sens du scandale. Ses actions coups de poing, aux Etats-Unis, à la limite de la légalité, visent à lutter contre la surveillance électronique généralisée de la population par la police et l'Etat

Pour ne pas laisser de traces avec sa carte bancaire, Christopher Soghoian règle presque tous ses achats en liquide. Pour éviter que sa vie privée soit étalée sur Internet, il n'a pas de compte Facebook. Il utilise un téléphone mobile, mais avec précaution: «Quand j'ai un rendez-vous important, je l'éteins, et en plus j'enlève la batterie.» Il dit pourquoi: «Quand un téléphone est piraté, il peut être remis en marche à distance et enregistrer ce qui se passe dans la pièce.» Et puisqu'on ne peut pas enlever la batterie des iPhones, il n'a pas d'iPhone.

L'Américain Christopher Soghoian, 30 ans, militant infatigable de la protection de la vie privée sur les réseaux électroniques, mène une vie hors norme, parfois à la lisière de la légalité. Armé d'un simple ordinateur, il se bat à visage découvert contre l'adversaire le plus puissant du monde: le gouvernement des Etats-Unis – plus précisément, la nébuleuse des agences fédérales chargées de la surveillance électronique de la population, et les sociétés privées qui leur fournissent les équipements et services nécessaires.

Né à San Francisco de père américain et de mère franco-britannique, il passe son enfance à Londres, puis rentre aux Etats-Unis à l'adolescence et se plonge dans Internet. Son seul capital est une connaissance approfondie de l'informatique, acquise dès l'enfance grâce à son père ingénieur. Il a un autre talent: il sait expliquer, convaincre, animer un débat, fabriquer un scandale, créer l'événement autour de lui.

Sa première action d'éclat date de 2006, alors qu'il est étudiant. Un incident avec des policiers dans un aéroport le décide à prouver l'absurdité de leurs procédures. Après quelques jours de recherches, il trouve une faille et publie sur Internet un mode d'emploi pour fabriquer un jeu de fausses cartes d'embarquement permettant à n'importe qui de franchir les contrôles. Pour attirer l'attention, il affiche sur son site une carte prête à imprimer, au nom d'Oussama Ben Laden. Mission accomplie, le FBI fonce chez lui: «Mais ils n'avaient pas de mandat de perquisition. Ils sont revenus à deux heures du matin, avec un mandat. Pas contents du tout.» Christopher n'est pas arrêté, mais ses ordinateurs sont saisis. L'affaire tourne court quand les autorités s'aperçoivent qu'il n'est pas un terroriste, mais un citoyen astucieux qui les a alertés sur une faille de sécurité. Christopher a trouvé sa voie, et son mode opératoire.

Tout en étant high-tech, le combat de Soghoian est ancré dans une tradition intellectuelle aussi vieille que les Etats-Unis: la doctrine du «small government». Fuyant les tyrannies du «vieux monde», les émigrants européens rêvent de bâtir en Amérique une société fondée sur la liberté individuelle, où l'Etat jouerait un rôle minime. Avec Internet, ce courant de pensée a été renforcé par une armée de jeunes hyperactifs et ultra-compétents: les geeks et les hackers qui, depuis vingt ans, mènent une guérilla acharnée pour essayer d'empêcher l'Etat et les grandes entreprises d'imposer leur loi et leurs

contraintes dans le cyberespace. Pour défendre leurs idéaux, ils ont créé des associations réunissant des juristes, des militants de la gauche alternative et des informaticiens -les plus actives sont l'*Electronic Frontier Foundation* et l'*Electronic Privacy Information Center*.

Les hackers constatent pourtant que l'appareil de surveillance de masse, surtout après le 11 septembre 2001, s'intensifie. La police et les services de renseignement exploitent les possibilités de surveillance offertes par les connexions Internet, les mobiles, les réseaux sociaux et les GPS. La police peut retracer précisément la vie d'un citoyen pour un coût dérisoire. Sa vie 24 heures sur 24, ce qu'il mange, ses idées politiques... Pour cela, le pouvoir américain a tissé des liens informels mais solides avec les sociétés comme Google ou Facebook, qui ont d'ailleurs embauché des ex-policiers pour gérer les demandes d'écoute et d'interception de leurs anciens collègues. Or, ces professionnels de la surveillance ont les mains libres, car les textes encadrant leurs activités, rédigés il y a des dizaines d'années, sont obsolètes.

Face à cette montagne, les défenseurs des libertés numériques se fixent des objectifs réalistes: obliger les pouvoirs publics à établir des règles et bonnes pratiques pour limiter la liberté de la police et des services de renseignement en matière de surveillance électronique. La lutte a lieu dans les médias, à Washington, où les militants comptent sur des élus libéraux et, surtout, devant les tribunaux, lors d'affaires qui semblent banales, dont les jugements sont appelés à faire jurisprudence.

Le combat contre la surveillance de masse a aussi besoin de francs-tireurs comme Soghoian. Il agit en marge du système, sans tomber dans l'illégalité. Ce qu'il traque n'est pas interdit, mais est annonciateur d'atteintes aux libertés. Après l'affaire des cartes d'embarquement, il s'installe à Washington et fréquente les politiciens, les fonctionnaires et les lobbyistes, dans le but de les éduquer, ou de les défier. Il ne leur ressemble guère: barbu, chevelu, habillé comme un étudiant fauché, il partage un appartement avec quatre colocataires, se déplace à vélo et suit un strict régime végétalien – ni viande, ni poissons, ni œufs.

Malgré son look, en 2009, il décroche un travail temporaire à la Commission fédérale du commerce (FTC) en tant qu'expert en matière de protection de la vie privée. Il profite de son badge officiel pour assister à une conférence réservée à la police, aux services de renseignements et aux sociétés de Télécom. Avec son portable, il enregistre en cachette les orateurs, dont un dirigeant de la compagnie de téléphone Sprint: «Il a expliqué qu'en un an les services de police avaient effectué huit millions d'interceptions. J'avais enfin un chiffre sur l'ampleur de la surveillance électronique.» Puis, le responsable de Sprint annonce que sa société va créer un site sur lequel les agents de l'Etat pourront obtenir en temps réel la localisation de n'importe quel téléphone mobile. Aussitôt, Christopher publie l'enregistrement sur son blog: «Tous les médias en ont parlé, des extraits ont même été diffusés à la télévision.» Le contrat de Christopher à la FTC n'est pas renouvelé.

Toujours à Washington, il apprend l'art de la négociation et s'initie au droit public et administratif: «J'analyse les questions juridiques et politiques sous l'angle de la technologie. Je suis un des seuls dans cette ville à posséder cette double compétence.»

Soghoian se démarque des militants généralistes qui dénoncent une politique globale ou prétendent avoir une solution à tous les problèmes de la société: «Je suis enregistré comme démocrate, mais comme des millions d'électeurs je suis obsédé par une seule question. Pour certains, c'est l'avortement ou le droit de porter une arme, pour moi, c'est la surveillance des citoyens.» En tant qu'informaticien, et aussi en tant que militant ayant eu affaire au FBI, il a pu se faire une idée de ce que serait une société sans aucune vie privée: «Ce n'est pas beau à voir.» Quand on lui demande qui sont ses maîtres à penser, il ne cite pas un philosophe des libertés mais Philip Zimmermann, l'inventeur d'un logiciel gratuit permettant au grand public de crypter les messages Internet.

L'une de ses tactiques préférées consiste à exiger du gouvernement des documents confidentiels en vertu de la loi sur la liberté de l'information. Travail ingrat. Car les administrations font tout pour la contourner. «Souvent, je reçois des pages de textes entièrement noircies, censurées au nom de la sécurité nationale. Mais de temps en temps, ils oublient de noircir une phrase intéressante, ça me permet d'ouvrir une nouvelle piste et d'envoyer une nouvelle demande.» La piste la plus facile est de suivre les paiements: «A chaque fois qu'une société effectue une interception ou une écoute pour l'Etat, elle envoie une facture. 25 dollars pour Google, 20 dollars pour Yahoo – 20 dollars plus le timbre pour la réponse.»

En 2011, le ministère de la justice envoie aux procureurs fédéraux une circulaire pour leur présenter de nouveaux outils de surveillance électronique. Soghoian l'apprend et envoie une demande pour se la procurer. Refus. Il n'hésite pas à porter plainte devant un tribunal fédéral: «J'ai rédigé le dossier, avec l'aide bénévole de juristes. Pour payer les 1 000 dollars de frais de justice, j'ai lancé une souscription sur Indiegogo.com, site de financement collectif de projets; ça a marché, j'ai reçu la somme, par dons de 5 ou 10 dollars. Puis j'ai plaidé devant le tribunal. J'ai perdu.» Parfois, il reçoit des documents sans demander. «Des fonctionnaires désapprouvent ce que leurs chefs leur font faire. Ils m'envoient anonymement des comptes rendus de réunions secrètes, des contrats avec des sociétés de surveillance, des listes d'achats de matériel...»

Soghoian s'attaque aussi au Center for Copyright Information (CCI), organisme chargé de rappeler à l'ordre les téléchargeurs illicites de musique et de films. «Ils veulent obliger les fournisseurs d'accès à conserver les données de connexion de leurs abonnés, sinon, ils n'attraperont personne. Or, si ces fichiers existent, la police et les services de renseignement y auront accès, tôt ou tard, pour d'autres usages.» Dans cette bataille, Soghoian affronte un homme qu'il connaît bien: Jules Polonetsky, ex-responsable du respect de la vie privée des consommateurs dans des sociétés Internet, aujourd'hui directeur du think tank *Future of Privacy Forum*. En outre, celui-ci va siéger au conseil du CCI. Avant, il faisait équipe avec Soghoian pour inciter des sociétés ou des administrations à sécuriser leurs systèmes informatiques. Il en garde un très bon souvenir: «Quand un patron affirme qu'il est impossible de pénétrer son réseau, Christopher prouve le contraire.» L'ex-tandem a fait corriger des failles de sécurité dans des entreprises: «Pour Christopher, seul le résultat compte. S'il faut faire un scandale, il n'hésite pas, mais si tout peut être réglé discrètement, c'est mieux.»

Christopher Soghoian a aussi des liaisons plus dangereuses. A l'automne 2011, il aide WikiLeaks, qui s'apprête à publier des documents sur des sociétés occidentales vendant des systèmes de surveillance à des gouvernements dictatoriaux: «Ils m'ont demandé de contacter les médias pour leur expliquer le contenu des documents techniques. J'ai accepté.» Par ailleurs, il est intervenu dans une procédure opposant Twitter au ministère de la justice. Twitter avait refusé de livrer les données de connexion de Julian Assange et de trois de ses collaborateurs. Soghoian a tenté – en vain – de démontrer au juge que les utilisateurs des réseaux sociaux restent juridiquement propriétaires de leurs données personnelles.

Christopher considère Julian Assange comme le personnage le plus influent de la dernière décennie dans le domaine de l'information, à égalité avec Mark Zuckerberg, fondateur de Facebook. «Assange veut que toute l'information étatique soit publiée, Zuckerberg veut que toute l'information privée soit publiée. Tous deux à leur façon sont persuadés que le monde serait meilleur s'il était plus transparent. Or, la grande nouveauté est que, grâce à Internet, certains informaticiens ont les moyens d'imposer leur vision du monde au reste de la population. Au lieu d'écrire des essais philosophiques dans l'espoir d'influencer les générations futures, ils réalisent leur projet de société. Le fait d'être ou non d'accord avec eux est sans objet, car ils ont déjà rapproché le monde de leur idéal.»

Christopher Soghoian s'est fait des amis inattendus, dont Stephanie Pell, 43 ans, qui fut procureur fédéral pendant quinze ans. Chargée d'affaires de terrorisme, elle a mené l'accusation contre José

Padilla, le «taliban américain», condamné à dix-sept ans de prison. En 2011, elle démissionne et devient consultante pour des sociétés de sécurité informatique qui ont besoin de savoir ce qui se passe à Washington. Mis en contact par des amis communs, Christopher et Stephanie décident d'écrire un article très pointu proposant un cadre juridique à l'utilisation par la police des données de localisation des mobiles. «Nous avons trouvé des compromis raisonnables qui respectent nos convictions respectives», explique Stephanie Pell.

Tout en restant éloignée du radicalisme de son ami, elle aime son pragmatisme. «Dans son monde idéal, le gouvernement n'aurait accès à aucune information sur les gens, c'est excessif et naïf. Mais nous avons besoin d'idéalistes comme lui.» Cela dit, elle mesure la complexité de l'époque: «D'un côté, je suis bien placée pour comprendre les besoins de la justice en matière de surveillance et de dépistage des délinquants. Mais je vois que l'Etat a désormais des outils si puissants, efficaces et faciles à utiliser que l'équilibre avec le reste de la société est rompu. Un policier peut suivre n'importe qui à la trace et tout savoir sur sa vie, sans bouger de son bureau. Il faut des lois pour rétablir l'équilibre au profit des libertés publiques.»

Pour elle, le problème va bien au-delà de la chasse aux délinquants. «Si les Etats-Unis le voulaient, le monde entier serait sous surveillance et toutes ces données pourraient être stockées pour l'éternité. Nous n'en sommes pas là, mais cela pourrait se produire grâce aux smartphones. Les intérêts de la police et des sociétés Internet sont identiques.»

Stephanie Pelle et Christopher Soghoian veulent se pencher sur une nouvelle menace: IMSI Catcher (attrapeur d'identifiant de carte SIM), un appareil qui tient dans un sac à dos et qui est capable d'identifier tous les téléphones mobiles présents dans une zone donnée et d'intercepter leurs communications à la volée. Selon Soghoian, ils sont utilisés par des hackers et des escrocs, mais aussi par les polices de nombreux pays, dont les Etats-Unis et la France. Pour lui, la prolifération de ces engins illustre un problème plus vaste. «Les réseaux pourraient être mieux sécurisés, ce qui protégerait les usagers contre les pirates. Mais les gouvernements ne veulent pas que ces failles soient colmatées, car ils utilisent les mêmes méthodes pour surveiller leurs citoyens.»

Quand il ne bataille pas contre l'Etat, Christopher Soghoian s'en prend aux entreprises. Il est à l'origine de la campagne d'opinion qui a obligé Google à crypter systématiquement les courriers électroniques de son service Gmail. Il est aussi l'inventeur de la technologie DNT (Do not Track), une application intégrée dans les navigateurs Internet, qui envoie aux sites Web commerciaux un message indiquant que le propriétaire de l'ordinateur ne veut être ni fiché ni pisté par les régies publicitaires. Le DNT a déclenché une bataille juridique et politique acharnée car si les sites commerciaux étaient obligés de le respecter, la publicité ciblée sur Internet serait en danger de mort. Ses joutes avec le secteur privé ont une autre fonction: «Quand on se bat contre l'Etat, tout est long, pénible, les victoires sont rarissimes et souvent éphémères. C'est épuisant. Les sociétés privées sont plus vulnérables, elles cèdent parfois à mes exigences. J'ai besoin de victoires de temps en temps, c'est bon pour le moral.»

Depuis septembre, Christopher Soghoian travaille pour l'*American Civil Liberties Union* (ACLU), une vénérable institution qui défend les droits civiques des Américains depuis 1920. Il y est à l'aise et s'est emparé de plusieurs dossiers. Il travaille notamment sur une nouvelle menace: l'apparition de sociétés privées qui découvrent des failles de sécurité dans les logiciels grand public, comme le font les pirates, et qui les revendent très cher aux polices de différents pays pour les aider à espionner les citoyens. Il ne dit pas s'il va rentrer dans le rang et adopter la démarche légaliste de l'ACLU ou s'il prépare de nouvelles actions spectaculaires qui le replaceront en position de franc-tireur.