Campagne contre la surveillance globale

20 avril 2005

Campagne contre la surveillance globale

L'attaque sans précédent contre le droit à la vie privée, à la liberté d'expression et à la liberté de mouvement qui sévit à travers le monde exige une réplique elle aussi sans précédent de la part de la société civile du monde entier.

La *Coalition pour la surveillance internationale des libertés civile*, représentant une trentaine d'organisations, s'est jointe à des groupes de défense des droits humains bien connus à travers le monde -- American Civil Liberties Union (US), Statewatch (G-B), et Focus on the Global South (Philippines) -- pour lancer la ***Campagne internationale contre la surveillance globale***, qui demande aux gouvernements de mettre fin à la surveillance massive et au fichage de populations entières.

Inspirée par la campagne internationale qui a mené à l'interdiction des mines antipersonnel, la ***Campagne internationale contre la surveillance globale*** cherche à bâtir un mouvement de résistance des populations à ces mesures en faisant circuler un document de fond, un résumé de celui-ci et une déclaration à endosser.

Vous pouvez consulter les documents, voir la liste des groupes et organisations qui ont endossé la campagne à ce jour et signer la déclaration en ligne en allant sur le site de la campagne. Si vous voulez endosser la campagne, mais n'avez pas accès à internet, veuillez contacter la Ligue des droits et libertés au 514-849-7717.

Les dix balises décrites dans le résumé qui suit sont examinées en détail dans le rapport intitulé « The Emergence of a Global Infrastructure for Mass Registration and Surveillance », disponible en anglais seulement.

Site web de la Campagne : www.i-cams.org

DÉVELOPPEMENT D'UN VASTE SYSTÈME DE FICHAGE ET DE SURVEILLANCE À GRANDE ÉCHELLE

Résumé

La sécurité mondiale et la « guerre contre le terrorisme » dominent aujourd'hui le programme politique au niveau international. Sous la poussée des États-Unis, un nombre croissant de mesures « antiterroristes » et de « sécurité » sont adoptées par des pays du monde entier. Ce nouveau paradigme « sécuritaire » sert à restreindre les libertés et à accroître les pouvoirs policiers de façon à exercer un contrôle toujours plus grand sur les personnes et les populations.

Dans ce contexte, les gouvernements ont lancé plusieurs initiatives visant à mettre en place une infrastructure mondiale de fichage et de surveillance. Cette infrastructure permettra de « ficher » des citoyens, partout dans le monde, de surveiller les déplacements à l'échelle de la planète, de suivre et d'intercepter facilement les communications et les transactions électroniques, et de conserver les renseignements recueillis dans des bases de données publiques et privées sur des individus, de coupler ces renseignements, de les analyser et de les mettre à la disposition des agents des services de sécurité.

L'objectif qui sous-tend la mise en place de cette infrastructure n'est pas de faciliter le travail régulier de la police, mais bien de permettre la surveillance globale de populations entières. La capacité technologique et la portée mondiale de cette infrastructure en font un projet de contrôle social sans précédent. À l'heure actuelle, les États-Unis et d'autres pays se servent déjà sans détours des renseignements ainsi recueillis et échangés entre eux pour réprimer l'opposition, fermer les frontières aux réfugiés et aux militants, ainsi que pour arrêter et détenir des gens sans motif valable.

Tout cela se produit alors que les États-Unis et leurs alliés maintiennent un réseau de prisons secrètes et extra-territoriales partout dans le monde, dans lesquelles des personnes, dont le nombre demeure inconnu, sont détenues arbitrairement pendant des périodes de temps indéfinies et soumises à la torture.

Il est grand temps que le public prenne conscience des dangers parsemant la voie que les gouvernements veulent nous imposer avec ces nouvelles initiatives de fichage et de surveillance. Les dix « balises » décrites ici montrent à quel point nous sommes déjà engagés sur cette voie et les dangers qui nous guettent tous si nous n'obligeons pas nos gouvernements à faire demi-tour.

1ère balise : Le fichage des populations

La *première balise* de cette voie que veulent emprunter les gouvernements est illustrée par les initiatives lancées par les États-Unis après le 11 septembre en vue de ficher les personnes de sexe masculin, originaires de certains pays et n'ayant pas la citoyenneté américaine, ainsi que tous les étrangers se rendant aux États-Unis. L'Union européenne a mis en place des mesures similaires visant à ficher les immigrants et les voyageurs.

Aux États-Unis, ces mesures se sont inscrites dans le cadre de deux programmes, NSEERS et US-VISIT.

- **NSEERS.** En vertu du NSEERS (*National Security Entry-Exit Registration System*), les hommes âgés de plus de 16 ans originaires de pays désignés (principalement des pays musulmans), et n'ayant pas la citoyenneté, ont été obligés de se rapporter au gouvernement fédéral. Parmi les 80 000 individus qui se sont présentés, plusieurs ont fait état de harcèlement, d'insultes et de mauvais traitements. Comme conséquence de la mise en place du NSEERS, plus de 13 000 personnes ont dû comparaître à des audiences d'expulsion et plusieurs milliers d'autres ont décidé de fuir le pays par peur.
- **US-VISIT.** Le NSEERS a éventuellement été abandonné, mais cela n'a pas mis fin au fichage des étrangers. Ce système a en effet été remplacé par un autre programme appelé US-VISIT, en vertu duquel *tous* les visiteurs (excepté quelques Mexicains et la plupart des Canadiens) doivent se faire photographier (photo numérique) et prendre leurs empreintes digitales au moment de leur entrée aux États-Unis. Ces données ne seront pas seulement utilisées à des fins de contrôle d'identité, mais elles seront reliées à plus de 20 bases de données du gouvernement fédéral américain ainsi qu'à d'autres sources de renseignements. Combinées à ces données, les données biométriques du programme US-VISIT formeront la base d'un nouveau et vaste système de constitution de dossiers sur les voyageurs internationaux.

En Europe, on constate un fichage et des recoupements de données du même type dans la foulée de la création du nouveau « EU Visa Information System (VIS) » et un registre des étrangers à l'échelle de l'UE.

- **EU-VIS.** Conformément au nouveau programme « EU VIS », les renseignements sur chaque demande de visa présentée aux 25 pays membres, y compris les photographies et les empreintes digitales, seront stockés dans une base de données centrale. Ces fichiers seront mis à la disposition des organismes chargés de l'application de la loi et de sécurité dans toute l'UE.

- **Registre des étrangers à l'échelle de l'UE.** De plus, des fichiers seront constitués sur tous les citoyens de pays tiers qui ont des permis de résidence grâce à « l'harmonisation » des permis de résidence des États membres de l'UE. Ces renseignements seront stockés dans une base de données centrale de l'UE. Une procédure automatique reliera cette base de données et la nouvelle base de données « EU VIS » aux autres bases de données de l'UE.

2e balise : La création d'un système d'identification mondial

La *deuxième balise*, la création d'un système international de cartes d'identité pour les citoyens, est l'équivalent national du fichage des étrangers.

Les cartes d'identité nationales et, plus important encore, les bases de données qui leur sont reliées, représentent non seulement un moyen de ficher les populations nationales, mais aussi un moyen centralisé et uniformisé de suivre les personnes dans leurs activités quotidiennes. Dans plusieurs démocraties, l'idée même d'une carte d'identité nationale a provoqué une levée de boucliers, tellement elle est étroitement associée à un État policier. Certes, plusieurs démocraties ont une carte d'identité nationale, mais, dans la plupart des cas, les renseignements qu'elle contient sont restreints, et seules les autorités du pays y ont accès pour des fins précises.

Depuis septembre 2001, bon nombre de pays ont lancé ou intensifié des initiatives pour mettre en place des bases de données nationales d'identification des citoyens; dans les pays qui ont déjà des documents d'identité nationaux, les autorités examinent des façons d'élargir leur capacité et l'usage qui en est fait.

Mais cette tendance est aggravée par l'émergence d'un nouvel outil d'identification en voie d'être adopté partout dans le monde : le « passeport biométrique à interopérabilité mondiale », qui est fondé sur une norme internationale créée à la demande des États-Unis. Les différents pays du monde en sont à différents stades dans l'adoption de passeports contenant des données biométriques, telles que des photographies numériques et des empreintes digitales numériques, ainsi que des puces d'identification par radiofréquence (« radio frequency identification » ou RFID) capables de transmettre des renseignements à quiconque dispose d'un lecteur RFID. Les États-Unis ont annoncé à leurs alliés que s'ils n'adoptent pas ces passeports, leurs citoyens ne seront plus admis aux États-Unis sans visa.

Ainsi, partout dans le monde, de plus en plus de personnes ont des documents d'identité informatisés, avec comme conséquence, que les renseignements les concernant se retrouvent dans des bases de données d'identité, à la fois dans leur propre pays et à l'étranger. Ceci ouvre la voie à la surveillance routinière des déplacements des personnes à l'échelle du monde.

<u>3e balise</u> : La création d'une infrastructure de surveillance mondiale des déplacements

La *troisième balise* renvoie à la création d'une infrastructure mondiale de surveillance des déplacements. Non seulement les autorités de plusieurs pays sont-elles bien engagées dans la mise en place de points de contrôle et de bases de données pour suivre les déplacements des individus à l'aide de leurs documents d'identité nationaux et/ou leurs passeports à données biométriques, mais elles cherchent également à avoir un accès direct aux dossiers des passagers (« passager name records » ou PNR) des compagnies aériennes.

Les PNR sont des fichiers conservés dans les systèmes de réservation du transport aérien. Ils peuvent comprendre plus de 60 champs d'informations, dont le nom et l'adresse du voyageur, l'adresse de la personne chez qui le voyageur se rendra, l'itinéraire, la date à laquelle le billet a été acheté, les renseignements de la carte de crédit, le numéro du siège, les choix de repas (ce qui peut révéler l'appartenance religieuse ou ethnique), des renseignements médicaux, des informations sur le comportement et des données sur les voyageurs assidus.

Le gouvernement des États-Unis, notamment, a demandé l'accès à ces renseignements et il cherche à obliger les compagnies aériennes à lui remettre ces dossiers même si cela est susceptible de contrevenir aux lois sur la protection de la vie privée protégeant les passagers de l'Union européenne et d'autres pays. À l'issue de longues négociations, les États-Unis ont réussi à convaincre les représentants de l'UE de violer leurs propres principes en matière de respect de la vie privée et de conclure un accord leur donnant accès aux PNR européens. De son côté, l'Union européenne a décidé de mettre en place son propre système de PNR pour suivre les déplacements de quiconque pénètre sur son territoire ou en ressort.

L'Organisation de l'aviation civile internationale (OACI), une institution des Nations Unies, examine la possibilité de créer un format harmonisé pour les PNR. L'OACI encourage les États à établir leurs propres systèmes PNR et à échanger les données à l'échelle mondiale. Ainsi, les renseignements sur la destination des voyageurs, la fréquence de leurs déplacements (ainsi que d'autres renseignements de nature personnelle, comme l'origine ethnique et l'hôtel où se rendra un voyageur), feront l'objet d'une analyse et seront conservés et échangés entre différents pays, dans le but de réguler et de contrôler les déplacements transfrontaliers.

4e balise : La création d'une infrastructure pour la surveillance mondiale des communications électroniques et des transactions financières

La *quatrième balise* constitue la création d'une infrastructure visant la surveillance à l'échelle mondiale des communications électroniques et des transactions financières. Cette initiative comprend plusieurs aspects :

- **Des pouvoirs accrus d'interception des communications :** Par des mesures, comme la promulgation du « Patriot Act », les États-Unis et d'autres pays ont réagi au 11 septembre en accordant au gouvernement de plus larges pouvoirs d'interception des courriels, des conversations et des autres communications électroniques, tout en limitant le contrôle judiciaire sur ces pouvoirs.

- **De nouvelles exigences pour le secteur privé :** Les gouvernements imposent également de nouvelles exigences aux entreprises et autres entités du secteur privé afin de faciliter l'aspect technique de la surveillance. Les gouvernements affirment qu'ils doivent introduire ces obligations pour se conformer à la *Convention sur la cybercriminalité*–un traité, adopté à l'insistance des États-Unis après le 11 septembre, qui accorde aux autorités une gamme de nouveaux pouvoirs pour enquêter sur les délits cybernétiques au-delà des frontières nationales.

- **L'obligation de « conserver des données » :** Les gouvernements, plus particulièrement ceux des pays européens, font également pression pour créer « l'obligation de conservation des données ». En vertu de cette obligation, les fournisseurs de services de communication seraient tenus de conserver et de stocker des données relatives à leurs clients, données qu'ils doivent aujourd'hui supprimer pour se conformer aux lois sur la protection des renseignements personnels. L'UE est en train de débattre un projet de loi qui aurait pour effet d'obliger les fournisseurs à conserver pendant trois ans les données concernant le trafic des conversations téléphoniques, des courriels, des télécopies et d'Internet.

- **L'expansion d'ECHELON :** Échelon, un programme de surveillance international géré dans l'ombre, s'intéresse à la majeure partie des communications électroniques mondiales. Ce partenariat entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande, permet à chacun de ces pays d'éviter le contrôle judiciaire en demandant aux pays partenaires d'épier leurs propres citoyens. En raison des nouvelles exigences adoptées dans plusieurs pays en matière de collecte et de conservation des données, Échelon pourra disposer d'une quantité de renseignements beaucoup plus vaste dans un proche avenir.

- **Le suivi et le signalement des transactions financières :** De nouvelles lois adoptées dans plusieurs pays ont pour objet d'enrôler les institutions financières et les entreprises ordinaires dans une infrastructure de surveillance financière, sous prétexte de mettre fin au blanchiment d'argent et au financement du terrorisme. Voici quelques exemples :

    - Une résolution du Conseil de sécurité de l'ONU, adoptée après le 11 septembre 2001, oblige tous les États à interdire à leurs citoyens de mettre à la disposition des terroristes des fonds ou de leur fournir des services, un mandat qui revient à exiger la surveillance de l'activité économique à l'échelle mondiale.

    - Aux États-Unis, le *Patriot Act* a mis en place un vaste dispositif juridico-bureaucratique visant la collecte et l'analyse systématiques des transactions financières.

    - Le FATF (« Financial Action Task Force »), Groupe de travail sur les transactions financières, un organe multilatéral responsable de l'élaboration des politiques qui est composé de 31 pays membres, a élargi son mandat pour s'attaquer aussi au financement des activités terroristes (en plus du blanchiment d'argent). L'Organisation de coopération et de développement économiques (OCDE) en a fait de même.

Grâce à ces initiatives, les agents de l'État partout dans le monde vont rapidement obtenir l'accès direct et gratuit à tous les courriels, tous les appels téléphoniques, tous les sites Web visités et à toutes les transactions financières réalisées. Les organismes de charité et les ONG qui œuvrent en zone de conflit, ou qui travaillent auprès de collectivités arabes ou musulmanes, subissent déjà les contrecoups de cette nouvelle infrastructure.

5e balise : La convergence des bases de données nationales et internationales

La *cinquième balise* tourne autour d'un aspect nouveau qui alimente les autres balises : l'intégration de diverses bases de données gouvernementales et du secteur privé, tant au niveau national qu'international. Cette tendance se fait sentir à plusieurs égards, notamment :

- L'initiative des États-Unis visant à assurer l'interconnexion de plus de 20 bases de données gouvernementales différentes au sein du système US-VISIT;

- La compilation et l'intégration de renseignements au sujet de citoyens américains et étrangers par des méga-courtiers de données aux États-Unis, qui vendent ces données à des dizaines d'organismes gouvernementaux américains;

- Des programmes, tels que le système américain « The Matrix », qui amalgament de nombreuses sources de données gouvernementales et du secteur privé en un tout, qui est ensuite mis à la disposition de la police partout au pays.

L'intégration des données provenant de différentes sources en une base de données unique et centralisée (ou des bases de données multiples mais accessibles de façon centralisée) transforme la collecte de données en une opération de surveillance totale qui fournit des registres toujours plus complets des activités des particuliers à travers le temps. Il en résulte un réseau mondial de bases de données dont se serviront les États-Unis et d'autres pays (en même temps que les systèmes de surveillance des déplacements dans le monde et des transactions électroniques et financières) pour créer des dossiers détaillés sur tous les particuliers.

6e balise : La généralisation d'un modèle « d'évaluation des risques »

La *sixième balise* est la généralisation du paradigme « d'évaluation des risques » qui est à l'origine de la collecte, du stockage et du croisement de cette masse de renseignements. Selon cette approche de la sécurité, d'énormes quantités de renseignements personnels sont recueillis afin de pouvoir évaluer si des personnes sont « dignes de confiance » ou si elles posent une menace pour la sécurité. Plutôt que d'avoir recours à des techniques éprouvées, qui consistent à s'en tenir aux faits connus et à s'intéresser d'abords aux personnes soupçonnées d'être des malfaiteurs, la démarche de l'évaluation des risques cherche à soumettre *tout le monde* à l'examen dans l'espoir d'identifier les personnes fautives parmi la masse.

L'approche « high-tech » consiste à effectuer un triage dans la mer de renseignements recueillis par la surveillance à grande échelle dans l'espoir de détecter le « risque », en utilisant des programmes « d'exploration des données » (data mining) qui cherchent des profils d'activités suspects. Cela revient à chercher une aiguille dans une multitude de bottes de foin… Il n'est guère surprenant que ces programmes engendrent un taux d'erreurs alarmant – non seulement parce qu'ils signalent des personnes innocentes comme étant « dangereuses », mais aussi parce qu'ils laissent filer des personnes dangereuses. Avec l'approche « low-tech », ce sont des êtres humains qui évaluent sur-le-champ si un individu pose une « menace » pour la société. Mais comme les agents pêchent par un excès de prudence, sans trop se soucier du bien-être des individus signalés, on ne compte plus le nombre de cas de citoyens qui ont été considérés à tort comme une menace.

L'évaluation des risques entraîne des conséquences véritablement kafkaïennes car les critères employés pour évaluer le risque sont vagues ou tenus secrets, et les renseignements utilisés sont souvent imprécis et incomplets. Les innocents qui sont identifiés comme posant un risque à la sécurité, selon le modèle d'évaluation des risques, ne savent généralement pas pourquoi on leur a apposé cette étiquette, et encore moins comment s'en débarrasser.

7e balise : L'intégration des forces de sécurité et l'effritement du contrôle exercé par des institutions souveraines

La *septième balise* est illustrée par l'intégration poussée de la police, du renseignement et du militaire coïncidant avec la renonciation des pouvoirs publics à exercer leur souveraineté et un contrôle national. En voici quelques exemples :

- Le nombre croissant « d'ententes d'assistance mutuelle » assurant la coopération entre les services de maintien de l'ordre et les organismes de renseignements de différents pays. Récemment, des fonctionnaires américains ont invoqué ce type d'accord lorsqu'ils ont saisi, à Londres, des serveurs hébergeant les sites Web du Centre des médias indépendants (*Indymedia*) d'une vingtaine de pays, soi-disant à la demande de la police suisse et italienne.

- Des équipes d'enquête mixtes sont en train d'être mises sur pied par les États-Unis et le Canada, et par les États-Unis et 25 États membres de l'UE. Ces équipes échangeront des renseignements sans qu'il leur faille présenter des demandes officielles d'État à État au titre d'ententes d'assistance mutuelle, et elles pourraient ne pas avoir à répondre de leurs actions en territoire étranger. Ces équipes peuvent comprendre des agents des douanes, de la police et des services d'immigration, ainsi que des agents des services de sécurité et de renseignements.

- En Europe, un accord conclu entre Europol et les États-Unis, sans aucun contrôle des institutions démocratiques, donnera accès aux renseignements d'Europol à un nombre incalculable d'organes américains, y compris des renseignements de nature délicate sur l'origine ethnique, l'opinion politique, les croyances religieuses, la santé et la vie sexuelle des particuliers. L'entente a été signée même si elle est contraire à la *Convention Europol* et à la *Directive sur la protection des données* de l'Union européenne.

- Il est de plus en plus fréquent que les gouvernements n'arrivent même pas à assurer la protection de leurs citoyens quand ils sont pris par erreur dans les mailles du filet mondial de sécurité. C'est ce que l'on a pu constater lorsque le gouvernement canadien a tenté d'obtenir la libération de Maher Arar, que les autorités américaines avaient refoulé en Syrie. Un autre exemple est celui du gouvernement suédois qui a dû négocier avec les États-Unis lorsqu'il a demandé que les noms de certains de ses citoyens soient enlevés de la liste de terroristes établie par les Nations Unies.

8e balise : Le complexe industriel-sécuritaire

La *huitième balise* passe par la création d'un nouveau « complexe industriel-sécuritaire ». À l'ère de l'informatique, une part toujours plus importante de nos activités est suivie et enregistrée par des entreprises privées, et ces renseignements sont de plus en plus souvent mis à la disposition des gouvernements. Les pouvoirs des gouvernements d'exiger l'accès à de telles données sont élargis, mais bon nombre d'entreprises vendent de leur propre gré des bases de données à des organismes gouvernementaux.

Pour les entreprises d'informatique et de technologie, la « guerre contre le terrorisme » a ouvert de nouveaux marchés gouvernementaux. Les services de renseignements et de sécurité, qui devaient justifier leur existence après la fin de la guerre froide, ont trouvé dans la « guerre contre le terrorisme » une occasion sans précédent d'augmenter leurs pouvoirs d'enquête et de surveillance. Ce nouveau complexe industriel-sécuritaire est devenu un puissant moteur du projet de surveillance globale.

Des multinationales établies aux États-Unis, en Europe occidentale et en Asie vont engranger d'énormes bénéfices grâce à la vente de bases de données, de lecteurs de données biométriques, de programmes d'exploration des données et d'autres technologies nouvelles en matière de surveillance et de contrôle.

L'Union européenne a lancé un nouveau programme de « recherche en matière de sécurité », dans le but de concurrencer les États-Unis dans le domaine des technologies liées à la sécurité. L'un des objectifs de ce programme est de lever le cloisonnement entre la recherche civile et la recherche militaire, afin que toutes deux servent à des fins militaires, économiques et de politique étrangère. Le Canada a lui aussi injecté des milliards de dollars dans les technologies de la sécurité et de la surveillance. Les grands projets de surveillance entrepris par les États-Unis, tels que US VISIT, MATRIX, CAPPS II et les programmes de *Terrorism Information Awareness*, sont une véritable mine d'or pour les entreprises de technologies. Ces sociétés ont rapidement cherché à créer des liens avec les appareils de sécurité de ces pays dans l'espoir de vendre des technologies de contrôle de plus en plus envahissantes.

9e balise : L'érosion des valeurs démocratiques

La *neuvième balise* signale la trahison consternante des valeurs démocratiques par le gouvernement des États-Unis et de certaines autres démocraties, dans leur volonté de mettre en œuvre le projet de surveillance globale. Pour parvenir à leurs fins, les gouvernements n'ont pas hésité à :

- suspendre le contrôle exercé par les tribunaux sur les activités des agents de l'application de la loi et des fonctionnaires

- concentrer des pouvoirs sans précédent entre les mains de l'exécutif

- contourner le contrôle démocratique et le débat par la branche législative du gouvernement, en imposant des politiques par le truchement d'organes transnationaux non-élus qui ne rendent de comptes à personne

- passer outre à des mesures fermement établies de protection de la vie privée des citoyens

- ignorer les garanties constitutionnelles et faire reculer les principes de droit pénal ainsi que les principes de justice fondamentale dans l'application de la loi, qui protègent les droits des citoyens face aux pouvoirs de l'État (telles que la présomption d'innocence, l'*habeas corpus*, le secret professionnel de l'avocat, le droit à un procès public, le droit de connaître la preuve et de la réfuter, les motifs raisonnables de perquisition ou de saisie, le droit de garder le silence)

- saper la liberté d'expression et la liberté d'association

Lorsque des régimes répressifs ont adopté des mesures de surveillance et de fichage de la population, ils ont maintenu ou aggravé le statu quo. L'exemple donné par les pays occidentaux permet aux gouvernements des pays moins démocratiques d'affermir leur emprise sur le pouvoir; il agit comme un feu vert pour toutes les atteintes aux droits de la personne et d'autres formes de violations.

10e balise : Renvoi extrajudiciaire, torture, mort

La *dixième balise* est constituée par la perte de repères moraux dans des pays comme les États-Unis qui se présentent comme des défenseurs des droits humains, mais qui ont adopté des pratiques de contrôle social inhumaines et exceptionnelles. On sait aujourd'hui que les États-Unis et d'autres pays pratiquent la torture, qu'ils infligent des traitements inhumains, qu'ils détiennent dans leurs propres prisons des personnes pendant des périodes indéfinies et qu'ils renvoient des suspects vers des pays tiers pour y être soumis à des traitements semblables ou pires. Les citoyens ont beaucoup plus à craindre dans le cadre de la mise en place d'un système de surveillance à l'échelle mondiale que la simple perte de leur vie privée, des libertés civiles ou de la liberté de mouvement.

Les États-Unis dirigent un système de camps de prisonniers et de centres de détention partout dans le monde, largement à l'insu du public. Certains sont administrés directement par les États-Unis, par exemple Guantanamo Bay, à Cuba, et d'autres centres de détention en Afghanistan, en Irak, au Qatar, au Pakistan, en Thaïlande et ailleurs. D'autres prisons sont administrées par des organismes collaborateurs en Jordanie, au Maroc, en Arabie Saoudite et au Pakistan – des pays où le recours à la torture lors d'interrogatoires a été documenté. Les centres de détention de Damas (Syrie), où le citoyen canadien Maher Arar a été détenu, et du Caire, sont parmi les pires.

L'administration Bush a affirmé que ni le droit criminel américain ni les Conventions de Genève et les autres traités internationaux ne s'appliquent aux personnes qui ont été jetées dans ce système de camps. En d'autres termes, les États-Unis disent que ces détenus se trouvent dans un vide juridique, une sorte de « no man's land » où les États-Unis et leurs alliés peuvent se soustraire à la loi, ou choisir les parties de la loi qu'ils appliquent. Alors même que le droit international et les lois de la plupart des nations (y compris les États-Unis) interdisent formellement l'usage de la torture contre *quelque personne que ce soit*, cette affirmation fait doublement frémir si l'on pense que bien des personnes prises dans les mailles du filet n'ont finalement pas de liens avec le terrorisme. Ce parcours sordide fait de tortures, de refoulements extrajudiciaires et même d'exécutions extrajudiciaires est une négation des valeurs démocratiques et de la civilisation en soi.

Conclusion

À l'examen des faits décrits ici, il est manifeste que la voie qui mène à un système mondial de fichage et de surveillance est dangereuse, tant pour la sécurité des particuliers que pour la sécurité collective.

Les initiatives décrites dans le présent rapport n'ont pas l'efficacité voulue pour identifier les terroristes ou faire échec à leurs plans. Elles détournent des ressources essentielles qui pourraient être investies dans des services de renseignement humain nécessaires pour nous donner des renseignements fiables sur des menaces précises, au lieu de produire des données inutiles sur la vaste majorité de la population qui ne constitue pourtant aucune menace. Ces méthodes ne font que susciter la méfiance des collectivités qui pourraient aider les services de renseignement à obtenir de l'information fiable. Elles n'aident en rien à régler les causes fondamentales du terrorisme. Au lieu d'accroître la sécurité, ces méthodes affaiblissent les institutions démocratiques et les garanties individuelles dont dépend la sécurité des citoyens. Au lieu d'accroître la sécurité dans le monde, elles exacerbent l'insécurité mondiale. Le ciblage injuste des Musulmans et le traitement brutal et hors du cadre de la loi qui est de rigueur dans le réseau mondial de camps de détention décrit ici engendrent la haine envers les pays occidentaux et leurs alliés, favorisant davantage de fanatisme et de terrorisme.

Nous ne sommes pas plus en sécurité avec le fichage et la surveillance globale, bien au contraire.

Il est temps que l'opinion se mobilise ! Les citoyens du monde doivent signifier à leurs gouvernements qu'ils font fausse route. Ajoutez votre voix à la **Campagne internationale contre la surveillance globale** en signant la **Déclaration**.