HUMAN RIGHTS WATCH

# Les algorithmes de la répression en Chine

## Rétro-ingénierie d'une application de surveillance de masse utilisée par la police du Xinjiang

Résumé et recommandations

# Résumé

Depuis fin 2016, le gouvernement chinois a soumis les 13 millions de membres de l'ethnie ouïghoure et d'autres musulmans turciques de la province du Xinjiang à des détentions arbitraires massives, à des séances d'endoctrinement politique forcé, à des restrictions de déplacement et à une oppression religieuse. Dans le cadre de cette répression accrue, un nombre de personnes pouvant aller jusqu'à un million sont détenues dans des camps d'« *éducation politique* », selon des estimations crédibles. La campagne « Frapper fort contre le terrorisme violent » (« Strike Hard Campaign against Violent Terrorism » du gouvernement a fait du Xinjiang un des plus importants laboratoires de Chine pour l'utilisation de technologies innovantes de contrôle des populations.

Le présent rapport fournit une description et une analyse détaillées d'une application mobile que la police et d'autres responsables utilisent pour communiquer avec la Plateforme intégrée d'opérations conjointes (Integrated Joint Operations Platform, IJOP, 一体化联合作战平台), l'un des principaux systèmes que les autorités chinoises utilisent pour effectuer une surveillance de masse au Xinjiang. Human Rights Watch a informé pour la première fois sur l'IJOP en février 2018, notant que ce programme de surveillance policière agrège des données concernant des personnes et signale aux autorités celles qu'il considère comme potentiellement dangereuses ; certaines des personnes visées sont arrêtées et envoyées dans les camps d'éducation politique et dans d'autres établissements. Mais après avoir effectué une « *rétro-ingénierie* » de cette application mobile, nous savons maintenant précisément le type de comportement et de personne qui est visé par ce système de surveillance de masse.

Ces constatations ont une signification plus large, en ce qu'elles offrent pour la première fois un aperçu de la manière dont la surveillance de masse fonctionne dans la réalité au Xinjiang, car le système de l'IJOP est au centre d'un plus vaste écosystème de surveillance et de contrôle social dans la région. Elles mettent également en lumière la façon dont la surveillance de masse fonctionne en Chine. Quoique les systèmes utilisés au Xinjiang soient particulièrement intrusifs, ils sont semblables, par leurs structures de base, à ceux que la police est en train de mettre au point et d'appliquer dans tout le pays.

Un grand nombre — peut-être même la totalité — des pratiques de surveillance de masse décrites dans ce rapport semblent être en contradiction avec les lois chinoises. Elles violent des droits garantis internationalement comme le droit à la confidentialité de la vie privée, celui d'être présumé innocent jusqu'à ce que la culpabilité soit prouvée, ainsi que les libertés d'association et de déplacement. Leur impact sur d'autres droits, comme les libertés d'expression et de culte, est profond.

Human Rights Watch constate que les autorités utilisent l'application de l'IJOP pour accomplir trois fonctions principales : recueillir des informations personnelles, signaler des activités ou des situations considérées comme suspectes, et déclencher des enquêtes sur les personnes que le système signale comme posant un problème potentiel.

L'analyse de l'appli de l'IJOP révèle que les autorités collectent d'énormes quantités d'informations personnelles — allant de la couleur de la voiture d'une personne à sa taille au centimètre près — et les injectent dans le système central de l'IJOP, reliant ces données au numéro de carte d'identité nationale de la personne. Notre analyse montre également que les autorités du Xinjiang considèrent de nombreux types de comportement légal, quotidien et non violent — tels que « *ne pas avoir de relations sociales avec ses voisins, éviter souvent d'entrer et de sortir par l'entrée principale* » — comme suspects. L'application considère également comme suspecte l'utilisation de 51 outils de réseaux, dont de nombreux Réseaux privés virtuels (Virtual Private Networks, VPN) et des outils de communication codée, tels que WhatsApp et Viber.

L'application de l'IJOP démontre que les autorités chinoises considèrent comme suspectes certaines activités religieuses pacifiques, comme faire des dons à des mosquées ou prêcher le Coran sans autorisation. Mais la plupart des autres comportements que l'appli considère problématiques n'ont rien à voir avec l'ethnie ou la religion. Nos constatations laissent penser que le système de l'IJOP surveille et recueille des données sur tout le monde au Xinjiang. Le système permet de connaître les déplacements des personnes en suivant à la trace les données relatives à la « *trajectoire* » et à la localisation de leurs téléphones, de leurs cartes d'identité et de leurs véhicules ; il permet aussi d'observer l'utilisation de stations d'électricité et d'essence par tout le monde dans la région. Ceci est cohérent avec les déclarations du gouvernement local du Xinjiang soulignant que les autorités doivent recueillir des données pour l'IJOP de « *manière exhaustive* » et concernant « *chaque membre de chaque foyer* ».

Quand le système de l'IJOP détecte des irrégularités ou des déviations par rapport à ce qu'il considère comme normal, par exemple lorsqu'une personne utilise un téléphone qui n'est pas enregistré à son nom, lorsqu'elle consomme plus d'électricité que la « *normale* », ou lorsqu'elle quitte sans autorisation de la police le secteur où elle est enregistrée comme y ayant son domicile, le système signale ces « *micro-indices* » aux autorités comme étant suspectes et déclenche une enquête.

Un autre élément clé de l'IJOP est la surveillance des relations personnelles. Les autorités semblent considérer certaines de ces relations comme étant intrinsèquement suspectes. Par exemple, l'application de l'IJOP donne instruction à des agents d'enquêter sur les personnes dont un membre de la famille a obtenu un nouveau numéro de téléphone ou a des relations à l'étranger.

Les autorités ont cherché à justifier la surveillance de masse au Xinjiang comme étant un moyen de lutter contre le terrorisme. Mais si l'application donne effectivement instruction aux responsables de rechercher les indices de « *terrorisme* » et les « *contenus audio-visuels violents* » quand ils effectuent des contrôles de téléphones et de logiciels, ces termes sont définis de façon large dans la législation chinoise. L'application donne également instruction de repérer les « *adhérents au Wahhabisme* », terme évoquant une forme radicale de l'Islam, et les « *familles d'individus … qui ont fait exploser [des engins] dans des attaques-suicide.* » Mais de nombreux comportements — voire la totalité — auxquels le système de l'IJOP accorde une attention toute spéciale n'ont aucun rapport clair avec le terrorisme ou l'extrémisme. Nos analyses du système de l'IJOP laissent penser que la collecte d'informations afin de lutter contre le véritable terrorisme ou la violence extrémiste n'est pas l'objectif central du système.

L'application sert également à noter les responsables gouvernementaux sur la manière dont ils s'acquittent de leurs tâches et est un instrument permettant aux cadres des échelons supérieurs de confier des tâches à ceux des échelons inférieurs et de suivre de près leurs performances. L'application de l'IJOP vise, en partie, à contrôler les fonctionnaires pour s'assurer qu'ils exécutent efficacement les ordres répressifs du gouvernement.

En créant le système de l'IJOP, le gouvernement chinois a bénéficié de la coopération de compagnies chinoises qui lui fournissent leurs technologies. Si le gouvernement chinois est le principal responsable des violations des droits humains qui sont commises au Xinjiang, il incombe également à ces compagnies, aux yeux du droit international, de respecter les droits humains, d'éviter de se rendre complices d'abus et de remédier à ceux-ci de manière adéquate quand ils se produisent.

Comme nous le détaillons ci-dessous, le système de l'IJOP et certains points de contrôle de la région fonctionnent ensemble pour former une série de clôtures invisibles ou virtuelles. Les autorités les décrivent comme étant une série de « *filtres* » ou de « *tamis* » disposés dans toute la région et permettant de repérer les éléments indésirables. En fonction du niveau de la menace perçue par les autorités — déterminé par des facteurs programmés dans le système de l'IJOP — la liberté de déplacement de l'individu est réduite à des degrés divers. Certains sont détenus dans les prisons et les camps d'éducation politique du Xinjiang ; d'autres sont assignés à résidence, avec interdiction de quitter la localité où ils sont enregistrés, interdiction de pénétrer dans des lieux publics ou interdiction de quitter la Chine.

Le contrôle exercé aujourd'hui par le gouvernement sur les déplacements au Xinjiang présente des similitudes avec l'ère Mao Zedong (1949-1976), quand les gens étaient contraints de vivre dans les lieux où ils avaient été recensés et la police pouvait arrêter quiconque s'aventurait hors de sa localité. Après le lancement de la libéralisation économique en 1979, la plupart de ces contrôles étaient devenus largement obsolètes. Mais l'État policier moderne du Xinjiang — qui se sert d'un ensemble de systèmes technologiques et de contrôles administratifs — habilite les autorités à réimposer un degré de contrôle ressemblant à celui de l'ère Mao, mais d'une manière graduelle qui permet également de satisfaire le besoin pour l'économie d'une main d'œuvre essentiellement libre de ses mouvements.

La collecte intrusive et massive d'informations personnelles grâce à l'application de l'IJOP aide à comprendre les affirmations de musulmans turciques du Xinjiang selon lesquels les fonctionnaires du gouvernement leur ont posé – à eux-mêmes ou à des membres de leurs familles – un éventail déconcertant de questions personnelles. Quand les agents du gouvernement effectuent des visites intrusives aux domiciles ou aux bureaux de musulmans, par exemple, ils demandent généralement si les résidents possèdent des

équipements de culture physique et comment ils communiquent avec des familles vivant à l'étranger ; il semble que ces agents répondent ainsi à des exigences qui leur sont transmises via des applications telles que celle de l'IJOP. L'appli de l'IJOP ne requiert pas que les fonctionnaires du gouvernement informent les gens dont la vie quotidienne est ainsi examinée à la loupe et archivée de l'objectif d'une telle collecte intrusive de données ou de la façon dont leurs informations sont utilisées ou stockées, et encore moins qu'ils obtiennent leur accord pour une telle collecte.

La campagne « Frapper fort » a fait preuve d'un mépris total pour les droits des musulmans turciques à la présomption d'innocence jusqu'à preuve de culpabilité. Au Xinjiang, les autorités ont créé un système qui considère des individus comme suspects sur la base de critères généraux et contestables, puis génère des listes de personnes devant être évaluées par les fonctionnaires en vue d'une éventuelle mise en détention. Des documents officiels affirment que les individus « *qui devraient être saisis, doivent l'être* », ce qui laisse entendre que le but est de maximiser le nombre de personnes considérées comme « *indignes de confiance* » qui sont placées en détention. Ces personnes sont alors soumises à des interrogatoires de police sans bénéficier des protections procédurales de base. Elles n'ont pas droit à l'assistance d'un avocat et certaines sont soumises à des tortures et à de mauvais traitements, pour lesquels elles n'ont aucun moyen d'obtenir réparation, comme nous l'avons documenté dans notre rapport de septembre 2018. Il en résulte que les autorités chinoises, s'appuyant sur la technologie, placent massivement en détention, arbitrairement et indéfiniment, des musulmans turciques du Xinjiang, pour des actes et des comportements qui ne constituent pas des crimes aux yeux de la législation chinoise.

Et pourtant les autorités chinoises continuent de prétendre, de manière radicalement inexacte, que leurs systèmes « *sophistiqués* » servent à maintenir la sécurité au Xinjiang en permettant de « *cibler* » les terroristes « *avec précision.* » En Chine, l'absence d'un système judiciaire indépendant et d'une presse libre, s'ajoutant à l'hostilité farouche du gouvernement vis-à-vis des organisations indépendantes de la société civile, signifie qu'il n'y a aucun moyen de faire rendre des comptes au gouvernement ou aux entreprises qui coopèrent avec lui pour leur comportement, notamment pour les conséquences dévastatrices pour la vie des gens de l'utilisation de ces systèmes.

Le gouvernement chinois devrait immédiatement fermer l'IJOP et effacer toutes les données qu'il a recueillies sur les habitants du Xinjiang. Il devrait mettre fin à sa campagne « Frapper fort », y compris à tous les programmes contraignants visant à surveiller et contrôler les musulmans turciques. Toutes les personnes détenues dans les camps d'éducation politique devraient être remises en liberté sans conditions et les camps fermés. Le gouvernement devrait également ouvrir une enquête sur le Secrétaire du Parti communiste du Xinjiang, Chen Quanguo, et sur d'autres responsables de haut rang impliqués dans des violations des droits humains, notamment des violations du droit à la confidentialité de la vie privée, et accorder l'accès au Xinjiang, comme l'ont réclamé le Haut-Commissariat des Nations Unies aux droits de l'homme et les experts de l'ONU en matière de droits humains.

Les gouvernements étrangers soucieux de cette situation devraient imposer des sanctions ciblées, à l'exemple de la Loi Magnitsky à portée mondiale (Global Magnitsky Act) des États-Unis, incluant des refus de visas et des gels d'avoirs, au Secrétaire du Parti Chen et à d'autres responsables de haut rang liés aux abus commis dans le cadre de la campagne « Frapper fort ». Ils devraient également imposer des mécanismes appropriés de contrôle des exportations afin d'empêcher le gouvernement chinois d'obtenir des technologies utilisables pour violer les droits humains fondamentaux.

# Recommandations

## Au gouvernement de la République populaire de Chine :

- Fermer la Plateforme intégrée d'opérations conjointes (Integrated Joint Operations Platform, IJOP) au Xinjiang et effacer toutes les données qu'elle a recueillies ;
- Suspendre la collecte et l'utilisation de données biométriques au Xinjiang jusqu'à l'adoption d'une loi nationale exhaustive qui protège la vie privée ;
- Cesser immédiatement la campagne « Frapper fort contre le terrorisme violent » (« Strike Hard Campaign against Violent Terrorism » au Xinjiang, y compris tous les programmes contraignants visant à surveiller et contrôler les musulmans turciques ;
- Enquêter de manière impartiale sur le comportement du Secrétaire du Parti communiste de la région, Chen Quanguo, et d'autres responsables de haut rang impliqués dans de présumées pratiques abusives de surveillance de masse liées à la campagne « Frapper fort », et faire rendre des comptes de manière appropriée à leurs auteurs ; et
- Accorder l'accès au Xinjiang, comme le réclament le Haut-Commissaire de l'ONU aux droits de l'homme et plusieurs experts de l'ONU.

## Au Comité permanent du Congrès national du peuple :

- Rédiger et adopter une législation pertinente en ce qui concerne les données biométriques et personnelles, pour faire en sorte que leur collecte soit conforme aux normes internationales en matière de droits humains :
    - Les normes définies dans cette législation devraient faire partie d'un cadre juridique plus large garantissant que toute collecte, utilisation, consultation, dissémination et conservation de telles données est absolument nécessaire ; que des mesures moins intrusives ne sont pas disponibles ; et que la collecte et l'utilisation de telles données soient étroitement et proportionnellement ajustées à un objectif légitime, tel que la sécurité publique.

- Pour assurer que ces normes soient appliquées, tout programme de données biométriques devrait inclure : une autorisation indépendante de collecte et d'utilisation des données, la notification du public que les autorités recueillent ces données, la mise en place de moyens de supervision indépendante du programme, ainsi que des voies de recours pour que les citoyens puissent contester les éventuels abus et obtenir réparation.
- Le comité permanent devrait également faire en sorte que les autorités compétentes publient des informations sur la collecte et l'utilisation de technologies d'identification basées sur la biométrique, y compris sur les bases de données ainsi créées et sur la manière dont elles sont utilisées.

## Aux gouvernements étrangers :

- Imposer des sanctions ciblées, à l'image de la Loi Magnitsky à portée mondiale (Global Magnitsky Act) des États-Unis et d'autres protocoles, incluant des refus de visas et des gels d'avoirs, au Secrétaire du Parti communiste du Xinjiang, Chen Quanguo, et à d'autres responsables de haut rang liés aux abus commis dans le cadre de la campagne « Frapper fort » ;
- Imposer des mécanismes appropriés de contrôle des exportations pour dénier au gouvernement chinois — et aux entreprises chinoises qui facilitent les abus du gouvernement — l'accès aux technologies utilisées pour violer les droits fondamentaux, y compris en ajoutant la CETC et d'autres compagnies nommées dans ce rapport sur les listes déjà existantes des entreprises visées par cette mesure ;
- S'assurer que les institutions étatiques, y compris les universités, ne s'engagent pas dans une coopération avec la police du Xinjiang et les compagnies chinoises de haute technologie qui sont liées aux violations des droits humains commis à l'encontre des musulmans turciques au Xinjiang ; et
- Pousser à la création d'une mission internationale d'établissement des faits pour évaluer la situation au Xinjiang et faire rapport au Conseil des droits de l'homme de l'ONU.

## Aux Nations Unies :

- Le Secrétaire général de l'ONU, Antonio Guterres, et d'autres responsables de haut rang de l'organisation devraient aborder publiquement et en privé avec le gouvernement chinois les préoccupations suscitées par les violations des droits humains occasionnées par la campagne « Frapper fort » ;
- Les hauts responsables de l'ONU devraient agir pour s'assurer que les activistes de la société civile puissent transmettre en toute sécurité des informations sur les abus commis par le gouvernement chinois au Xinjiang et ailleurs aux mécanismes onusiens de défense des droits humains ; et
- Les hauts responsables de l'ONU devraient apporter un soutien aux organisations de la société civile chinoises, en résistant aux tentatives du gouvernement chinois au sein du Département des affaires économiques et sociales (DESA) de l'ONU d'empêcher l'accréditation d'organisations plaidant pour les droits des musulmans turciques au Xinjiang.

## Aux entreprises chinoises et internationales actives au Xinjiang, dont la CETC, HBFEC, Baidu, Face++ et Hikvision :

- S'assurer que leurs opérations commerciales ne favorisent pas la campagne « Frapper fort », en particulier les systèmes de surveillance de masse et de profilage biométrique gérés par le Bureau de la Sécurité publique du Xinjiang ;
- S'assurer que leurs relations d'affaires avec la police du Xinjiang ou avec d'autres forces de sécurité ne contribuent pas aux abus et agir sans retard pour mettre fin à de telles relations lorsqu'il existe des preuves que c'est le cas ;
- Adopter des politiques soutenant explicitement les droits humains et établir des procédures pour s'assurer que les opérations de la compagnie n'aient pas pour résultat, ou ne contribuent pas à, des violations des droits humains ; et
- Analyser les impacts en termes de droits humains de propositions d'investissements ou d'opérations et appliquer des stratégies visant à prévenir et à atténuer de tels impacts négatifs. De telles « *évaluations d'impacts en termes de droits humains* » devraient être effectuées en coordination avec les organisations de la société civile et les experts en matière de droits humains.