« IL SUFFIT QUE LES GENS PENSENT QUE ÇA EXISTE »

SOCIÉTÉ CIVILE, CULTURE DU SECRET ET SURVEILLANCE AU BÉLARUS

AMNESTY INTERNATIONAL

Amnesty International est un mouvement mondial réunissant plus de sept millions de personnes qui agissent pour que les droits fondamentaux de chaque individu soient respectés.

La vision d'Amnesty International est celle d'un monde où chacun peut se prévaloir de tous les droits énoncés dans la Déclaration universelle des droits de l'homme et dans d'autres textes internationaux relatifs aux droits humains.

Essentiellement financée par ses membres et les dons de particuliers, Amnesty International est indépendante de tout gouvernement, de toute tendance politique, de toute puissance économique et de tout groupement religieux.

Première publication en 2016
par Amnesty International Ltd
Peter Benenson House, 1 Easton Street
Londres WC1X 0DW, Royaume-Uni

Index : EUR 49/4306/2016
Original : anglais.

amnesty.org

Photo de couverture : *Minsk, Bélarus*
© Maxim Sarychau

AMNESTY INTERNATIONAL

1. SYNTHÈSE

Le cadre juridique dans lequel s'exerce la surveillance secrète au Bélarus ne comporte pas de garanties suffisantes et permet aux pouvoirs publics de se livrer à de multiples activités d'espionnage de la population sans avoir, la plupart du temps, à se justifier. N'importe qui ou presque peut faire l'objet d'une surveillance, mais il est quasiment impossible à un individu de savoir s'il est surveillé ou non. Cette incertitude a un effet dissuasif pour les défenseurs des droits humains, les membres de l'opposition politique, les avocats et les militants en général, et elle limite leur capacité à exercer leurs droits humains, notamment leur droit au respect de la vie privée et à la liberté d'association, de réunion pacifique et d'expression.

La surveillance secrète peut être légitime dans le cadre des missions des services chargés de l'application des lois, mais lorsqu'elle n'est pas assortie de garanties ou de contrôles suffisants, ou lorsque, plus généralement, elle ne respecte pas la législation et les normes internationales, elle constitue une violation des droits humains. Le présent rapport passe en revue les conséquences de la surveillance secrète illégitime au Bélarus sur les droits humains et sur la manière dont fonctionne la société civile dans ce pays. Il a été rédigé à partir d'entretiens que nous avons eus avec plus d'une cinquantaine de militants de la société civile, majoritairement au Bélarus, mais également auprès de personnes vivant en exil. Il est également fondé sur un examen approfondi du cadre juridique bélarussien et international réglementant les activités de surveillance.

Le système de surveillance mis en place au Bélarus est problématique à bien des égards. Le système SORM, qui regroupe un ensemble de moyens techniques normalisés permettant d'intercepter les communications, pose tout particulièrement problème. Il permet en effet aux pouvoirs publics d'accéder directement et à distance à toutes les communications des usagers et aux données afférentes, sans en informer les fournisseurs d'accès. La législation bélarussienne exige des fournisseurs proposant des services de télécommunications sur le territoire national qu'ils fassent en sorte que leur matériel soit compatible avec le système SORM. Ce système permet un suivi des communications en temps réel, ainsi que l'accès aux données, que les services de télécommunications sont tenus de conserver pendant une durée pouvant atteindre cinq ans. Il permet l'accès au contenu des communications et aux métadonnées associées (telles que l'heure, le mode ou les lieux d'émission et de réception).

Ce dispositif de surveillance préoccupant fonctionne avec l'aide d'entreprises, comme les compagnies de téléphone ou les fournisseurs d'Internet, qui, aux termes de la loi bélarussienne, doivent veiller à ce que les autorités puissent avoir directement accès aux données de leurs clients. Ces entreprises bélarussiennes, ainsi que les multinationales dont elles sont les filiales ou qui en sont des actionnaires majeurs, s'abstiennent (en contradiction avec les obligations qui sont les leurs) de relever les violations des droits humains commises en conséquence de leurs activités ou en raison des partenariats commerciaux qu'elles ont conclus, de les prévenir et d'y remédier. Elles se mettent en cela en contravention avec les normes internationales relatives à la responsabilité des entreprises en matière de droits humains. Les entreprises doivent prendre des mesures afin d'assumer les responsabilités qui sont les leurs en matière de droits humains, quel que soit l'endroit où elles décident d'exercer leurs activités. Ces mesures doivent être proportionnées au préjudice que les personnes sont susceptibles de subir en conséquence de leurs opérations.

Les télécommunications ne constituent pas le seul domaine dans lequel les autorités du Bélarus se livrent à une surveillance abusive des citoyens. La législation accorde à l'État de larges pouvoirs en matière de surveillance physique des personnes, qui peuvent, par exemple, être mises sur écoute. Ces dispositions, de même que la pratique qui consiste à saisir les ordinateurs, les téléphones portables ou d'autres appareils appartenant à des particuliers, les privant ainsi de certaines données personnelles, menacent le droit au respect de la vie privée. Face au manque de transparence concernant les capacités de l'État en matière de surveillance, personne ne sait finalement quels sont les outils et les techniques dont disposent les autorités.

Exercée par toute une série d'organismes de l'État, la surveillance secrète est autorisée par la loi pour divers motifs aussi vagues que généraux. Les autorités peuvent y recourir, au titre de la législation nationale, pour surveiller des personnes qui ne sont soupçonnées d'aucune infraction. Les garanties d'autorisation et de contrôle ne sont pas suffisantes et relèvent généralement de l'autorité des procureurs, et non pas d'une instance judiciaire indépendante.

Lorsque la surveillance débouche sur des violations des droits humains, il est extrêmement difficile, dans la pratique, d'exercer un recours, d'autant plus que les pouvoirs publics ne sont pas tenus d'informer les personnes qu'elles ont fait l'objet d'une surveillance, une fois celle-ci terminée, même lorsqu'il n'y a aucun risque qu'une telle information compromette la bonne marche d'une enquête. Les citoyens disposent donc rarement d'éléments qui leur permettraient d'étayer une plainte. Un nombre infime de militants estimant avoir fait l'objet d'une surveillance illégale a été en mesure de porter plainte. Les rares qui l'ont fait ne se faisaient généralement aucune illusion sur les chances de voir leur recours aboutir et n'avaient entamé une procédure que pour éviter d'être eux-mêmes poursuivis.

Si le cadre juridique du Bélarus empêche presque toujours de savoir avec certitude si l'on a été mis sous surveillance, l'histoire récente du pays donne à de nombreux militants des raisons de croire qu'ils le sont.

La répression exercée par les autorités au lendemain des élections présidentielles de 2010 a été marquée par l'arrestation et l'emprisonnement de nombreux membres de l'opposition, à qui il était reproché d'avoir exercé leurs droits fondamentaux. Largement médiatisés, les procès intentés contre eux ont très souvent été marqués par l'usage prépondérant de relevés de communications privées et de données associées. La presse a très largement fait état du fait que les autorités s'étaient servies d'informations permettant de localiser les téléphones portables pour identifier les participants aux manifestations organisées au lendemain des élections (manifestations non autorisées, mais qui s'étaient déroulées pour l'essentiel dans le calme).

Les militants qui ont accepté de parler avec Amnesty International se disaient par conséquent tous convaincus qu'ils étaient soumis à une surveillance secrète, sous une forme ou sous une autre, en raison de leurs activités civiques ou politiques. La crainte d'être surveillé est exacerbée par les restrictions juridiques qui pèsent sur la société civile au Bélarus. Les activistes font régulièrement l'objet de sanctions, pour avoir simplement voulu exercer leurs droits humains (participer à une manifestation non violente, par exemple) et des limites de plus en plus draconiennes sont imposées à l'exercice des libertés fondamentales sur Internet. Ce climat général a un effet dissuasif, qui incite de nombreuses personnes à s'autocensurer et à s'abstenir dans bien des cas d'exercer leurs droits les plus fondamentaux.

Les militants avec qui Amnesty International a pu s'entretenir ont expliqué qu'ils s'abstenaient généralement d'aborder au téléphone des sujets sensibles, tels que le financement d'une organisation non reconnue officiellement ou l'organisation d'une manifestation, activités susceptibles de donner lieu à des poursuites. Les actes les plus banals, comme le fait d'organiser une réunion, impliquent de recours à des systèmes sophistiqués de langage codé et obligent généralement les gens à se voir en personne, souvent à l'extérieur, en l'absence de tout téléphone portable susceptible d'enregistrer les conversations ou de signaler les déplacements des uns et des autres. De peur que leurs communications en ligne soient surveillées, les militants sont contraints de recourir à des outils de cryptage, comme le logiciel PGP, qui permet de crypter les courriels, à des programmes de discussion cryptés et au codage des données figurant sur les disques durs.

Plusieurs militants disent avoir vécu des expériences indiquant, selon eux, qu'ils étaient suivis via leur téléphone portable (contrôle par des policiers qui semblaient manifestement savoir où les trouver, par exemple). Étant donné le cadre juridique mis en place au Bélarus, ils ne sont toutefois pas en mesure de confirmer leurs soupçons et doivent le plus souvent se contenter de supposer qu'on les surveille dans leurs déplacements.

Certains militants craignent que leurs bureaux, voire leur domicile, ne soient truffés de micros ou de caméras. Ils évitent donc d'y traiter certaines questions sensibles, ce qui les gêne considérablement dans leur action.

Amnesty International s'est entretenue avec trois activistes, qui pensaient que leur boîte de courrier électronique ou leur compte sur certains réseaux sociaux avait été piraté. Ils soupçonnaient les autorités d'être derrière ces attaques, soupçons qui ont été renforcés lorsque les pouvoirs publics ont produit des données personnelles les concernant pour les menacer ou engager des poursuites contre eux. Plus fréquemment, les autorités n'hésitent pas à saisir les ordinateurs et autres appareils appartenant à des militants, qui ne peuvent plus, dès lors, s'en servir, y compris lorsque ceux-ci leur sont rendus, de peur qu'un logiciel espion n'y ait été installé.

L'utilisation d'Internet a beaucoup augmenté ces dernières années au Bélarus. Elle concernait 59 p. cent de la population en 2014, contre 39,6 p. cent en 2011[1]. Les risques de surveillance des communications et l'incertitude qui règne à ce sujet compliquent néanmoins fortement les activités des militants bélarussiens. Ils ne profitent pas de la croissance de la connectivité constatée. La peur de la surveillance est dissuasive. Elle ralentit les communications, limite les flux d'informations, bloque les velléités d'organisation et sape la confiance.

Le cadre juridique qui régit la surveillance au Bélarus est tel que chacun vit comme s'il était surveillé, ce qui a bien sûr des conséquences préjudiciables pour l'exercice des droits fondamentaux. S'il est impossible de connaître exactement l'ampleur actuelle des activités de surveillance, l'impact des abus commis dans ce domaine est évident. Pour expliquer la peur qu'ils ont d'être surveillés, les personnes interrogées citent aujourd'hui encore les procès très médiatisés intentés au lendemain des élections de 2010, au cours desquels les autorités avaient produit les données relatives aux communications personnelles d'un certain nombre d'opposants et de défenseurs des droits humains pour les incriminer. Les exemples cités par des militants rencontrés par Amnesty International montrent bien que ceux-ci restent soumis à une surveillance secrète.

Les autorités du Bélarus doivent de toute urgence revoir les lois relatives à la surveillance secrète, afin de les mettre en conformité avec les normes internationales. Elles doivent par exemple veiller à ce que la surveillance ne puisse s'exercer que lorsqu'elle est dûment autorisée (ou contrôlée) par un magistrat indépendant, sur la foi de motifs suffisamment précis, à partir de l'existence de soupçons raisonnablement fondés pesant sur un individu, et en respectant les obligations de nécessité et de proportionnalité. Le système SORM doit être remplacé par un autre dispositif, ne permettant pas l'accès direct aux données de communications. Les procureurs ne doivent pas chercher à soumettre des personnes à une surveillance parce que celles-ci exercent leurs droits fondamentaux, comme celui d'organiser une manifestation non violente. Les procureurs et les services chargés de la surveillance doivent communiquer de manière plus transparente sur le nombre de cas de surveillance autorisés et réalisés. Les personnes ayant fait l'objet de mesures de surveillance doivent en être informées et pouvoir avoir effectivement accès à des recours en cas de violations des droits humains liées auxdites mesures. Les entreprises privées qui aident à la mise en œuvre de la surveillance au Bélarus doivent contester les pratiques illégales des pouvoirs publics en la matière, insister pour que des réformes soient faites et pour plus de transparence concernant la législation et les pratiques gouvernant l'accès aux données des usagers au Bélarus.

Un certain nombre de recommandations supplémentaires figurent en fin de rapport.

[1] http://data.worldbank.org/indicator/IT.NET.USER.P2

2. RECOMMANDATIONS

2.1 AUX POUVOIRS EXÉCUTIF ET LÉGISLATIF DU BÉLARUS :

1. Modifier les lois relatives à la surveillance, et notamment la Loi sur les recherches opérationnelles (Loi n°307-Z du 15 juillet 2015) et le Code de procédure pénale, afin de mettre le régime juridique de la surveillance et les pratiques afférentes en conformité avec le droit international relatif aux droits humains et les normes en la matière.
2. Veiller à ce que le public ait accès aux informations relatives à la législation et aux pratiques de surveillance dans une mesure au moins égale à celle prévue par *les nouveaux Principes de Tshwane sur la sécurité nationale et le droit à l'information*.
3. Des mesures doivent notamment être prises pour que :

    - les pouvoirs publics, lorsqu'ils souhaitent obtenir des données auprès de prestataires de services de télécommunications, soient tenus de leur soumettre des demandes avalisées par le pouvoir judiciaire, et qu'ils ne puissent pas avoir accès à ces données directement et à distance ;
    - les fournisseurs de services de télécommunications ne soient pas tenus de conserver les données relatives aux communications en dehors du cadre d'enquêtes pénales en cours et de l'existence d'un mandat émis par une autorité judiciaire précisant qu'il existe des soupçons spécifiques et raisonnables d'infraction ;
    - l'interception et la consultation de communications (et des données afférentes) ne puissent se faire qu'à condition que la demande en ait été exprimée (ou renouvelée) par une instance judiciaire indépendante chargée de vérifier le bien-fondé de soupçons spécifiques et raisonnables d'infraction par la personne visée par la surveillance, dans le respect des exigences de nécessité et de proportionnalité ;
    - les motifs juridiques justifiant la surveillance secrète, et notamment la définition de la notion de « sécurité nationale », soient indiqués dans la loi, de manière suffisamment claire et précise pour que les citoyens aient une idée exacte des circonstances dans lesquelles une surveillance peut être mise en place ;
    - les pouvoirs en matière de surveillance soient contrôlés par une autorité véritablement indépendante, disposant de moyens suffisants, fonctionnant de

manière transparente, ayant accès à toutes les informations et habilitée à détecter les atteintes aux droits humains liées à des activités de surveillance secrète, à enquêter sur ces atteintes, à agir pour y mettre un terme et à proposer des recours ;

- la loi soit modifiée afin de limiter clairement la durée de la surveillance secrète dans tous les cas ;
- la loi définisse clairement les conditions dans lesquelles l'ensemble des données relatives à la surveillance doit être détruit ;
- les personnes ayant fait l'objet d'une surveillance secrète en soient informées, dans tous les cas où une telle information ne compromet pas ou plus l'objet légitime d'une enquête en cours ;
- les personnes puissent avoir accès à des recours efficaces et soient autorisées à saisir un tribunal indépendant fournissant toutes les garanties de procédure régulière, afin de contester la légitimité des mesures de surveillance ou de dénoncer les violations de leurs droits éventuellement engendrées par la surveillance dont elles ont été l'objet ;
- des informations suffisantes concernant les caractéristiques techniques des systèmes de surveillance, y compris des outils de piratage, soient rendues publiques.

2.2 AUX PROCUREURS :

En attendant que la décision d'autoriser une surveillance secrète relève de la compétence d'un magistrat indépendant, les procureurs doivent :

1. veiller à ce que les demandes de surveillance secrète ne soient acceptées qu'à condition qu'elles soient fondées sur des soupçons raisonnables et spécifiques d'infraction de la part de la personne visée, et dans le respect des conditions de nécessité et de proportionnalité nécessaires ;

2. publier régulièrement des rapports indiquant, au minimum, le nombre de demandes de surveillance secrète déposées, acceptées et rejetées, en ventilant les données selon les services demandeurs et les motifs juridiques invoqués ;

3. veiller à n'accorder aucune autorisation lorsque le motif invoqué relève de l'exercice des droits fondamentaux de la personne (participation aux activités d'un groupe non officiellement reconnu ou à un rassemblement non violent, notamment) ;

4. exercer leurs pouvoirs de contrôle de la mise en œuvre des mesures de surveillance et, lorsqu'il existe des éléments indiquant que des atteintes à la législation ou aux droits humains ont été commises, veiller à ce qu'il soit mis un terme à la surveillance et à ce que les responsables rendent des comptes.

2.3 AUX SERVICES CHARGÉS DES « RECHERCHES OPÉRATIONNELLES » :

Dans l'attente des réformes recommandées plus haut :

1. Publier régulièrement des rapports indiquant, au minimum, le nombre de demandes de surveillance secrète déposées, acceptées et rejetées, en ventilant les données selon les motifs juridiques invoqués.

2. Publier des informations concernant le nombre de fois où le système SORM a été utilisé pour accéder à des données, ainsi que les fondements juridiques de ces usages.

3. S'abstenir de demander une autorisation lorsque le motif invoqué relève de l'exercice des droits fondamentaux de la personne (participation aux activités d'un groupe non officiellement reconnu ou à un rassemblement non violent, notamment).

2.4 AUX ENTREPRISES DE TÉLÉCOMMUNICATIONS

1. Procéder à des examens en diligence requise destinés à détecter les conséquences de leurs activités, ou de celles de leurs filiales, sur l'exercice des droits humains au Bélarus et ailleurs, à prévenir ces conséquences, à les atténuer et à les prendre en compte, en adoptant notamment et au moins les mesures suivantes :

    - Contester les obligations légales qui ne sont pas conformes au droit international relatif aux droits humains et aux normes dans ce domaine.
    - Publier régulièrement des données sur le nombre de demandes et d'occurrences d'accès aux communications des usagers et aux données afférentes Lorsque cela n'est pas possible, publier des informations détaillées et accessibles concernant le cadre juridique et les pratiques relatives à la communication aux services de l'État de données propres aux usagers.
    - Insister pour que les conditions imposant la mise en œuvre du système SORM soient renégociées et pour que les obligations, légales ou autres, de communication des données propres aux usagers, selon des modalités contraires à la législation et aux normes internationales, soient revues.

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL DE DÉFENSE DES DROITS HUMAINS. LORSQU'UNE PERSONNE EST VICTIME D'INJUSTICE, NOUS SOMMES TOUS CONCERNÉS.

CONTACTEZ-NOUS

info@amnesty.org

+44 (0)20 7413 5500

PRENEZ PART A LA CONVERSATION

www.facebook.com/AmnestyGlobal

@AmnestyOnline

«IL SUFFIT QUE LES GENS PENSENT QUE ÇA EXISTE»

SOCIÉTÉ CIVILE, CULTURE DU SECRET ET SURVEILLANCE AU BÉLARUS

La législation du Bélarus permet aux autorités de l'État de se livrer à de vastes activités de surveillance sous n'importe quel prétexte ou presque et en dehors de tout contrôle indépendant. Ce système de surveillance secrète a un effet paralysant sur la société civile bélarussienne, dont l'action est déjà fortement compromise par la menace de sanctions pénales ou administratives pesant sur ceux et celles qui entendent simplement exercer leurs droits fondamentaux, comme le droit de participer à une manifestation.

Dans un tel contexte, la crainte de la surveillance a un effet dissuasif, qui complique et rend périlleux les actes les plus banals du quotidien, comme le fait de passer un coup de téléphone ou d'organiser une réunion ou une manifestation publique. Les téléphones portables peuvent espionner les conversations privées, suivre les déplacements de leurs propriétaires et indiquer qui ils ont rencontré. Les informations privées contenues dans les courriels ou les comptes des réseaux sociaux peuvent, une fois ceux-ci piratés, exposer certains militants à des représailles judiciaires.

Dans la pratique, le dispositif en place au Bélarus ne prévoit guère de recours pour celles et ceux dont les droits sont violés par des activités de surveillance. Ce dispositif est conforté par la coopération des entreprises de télécommunications bélarussiennes et étrangères, qui accordent aux pouvoirs publics un accès direct aux communications et aux données de leurs clients, via le système SORM.

Ce rapport comporte des recommandations au gouvernement du Bélarus, ainsi qu'aux entreprises de télécommunications bélarussiennes et internationales, pour que cessent les violations des droits humains commises au Bélarus en raison des activités de surveillance qui y sont menées.

Index : **EUR 49/4306/2016**
Juillet 2016
Langue : français.

amnesty.org

AMNESTY INTERNATIONAL