AMNESTY INTERNATIONAL

Index AI : POL 40/6154/2022

VERS UN MORATOIRE MONDIAL SUR LES TECHNOLOGIES DE SURVEILLANCE CIBLÉE

INTRODUCTION

Les attaques numériques contre les défenseur·e·s des droits humains, les journalistes et les membres de la société civile sont en augmentation. Des éléments toujours plus nombreux viennent prouver que des gouvernements et des entreprises commettent des violations des droits humains en surveillant de manière ciblée et illégale des militant·e·s, des journalistes, des avocat·e·s, etc. De trop nombreux États à travers le monde ferment les yeux et autorisent les exportations de technologies de surveillance vers des pays ayant un lourd passif de recours à des logiciels espions pour violer les droits humains. Ces violations ne peuvent plus être ignorées.

C'est David Kaye, rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, qui a été le premier à proposer à la communauté internationale l'idée d'un moratoire sur les exportations de technologies de surveillance. « Les États devraient imposer un moratoire immédiat sur l'exportation, la vente, le transfert, l'utilisation et la maintenance des technologies de surveillance conçues par le secteur privé et le lever uniquement lorsqu'un régime de garanties conforme aux droits de l'homme aura été établi », recommandait-il dans son rapport de 2019[1]. Depuis, des États[2], des spécialistes des droits humains[3] et de nombreux membres de la société civile se sont fait l'écho de cette proposition.

QU'EST-CE QUE LA SURVEILLANCE CIBLÉE ILLÉGALE ?

Une surveillance ciblée peut être considérée comme illégale pour deux motifs principaux. C'est le cas, d'une part, si des personnes sont ciblées parce qu'elles exercent leurs droits humains ou par discrimination, à cause de leur identité. Les exemples de ce genre sont nombreux : des journalistes sont la cible d'une surveillance pour avoir critiqué un gouvernement, des militant·e·s pour avoir organisé des manifestations, et des personnes sont ciblées de manière discriminée sur la base de critères ethniques ou raciaux, ou en raison de leur orientation sexuelle, de leur religion ou d'autres aspects de leur identité qui font qu'on les considère comme des criminel·le·s avérés ou potentiels.

Exercer une surveillance ciblée pour ces raisons est toujours contraire au droit relatif aux droits humains.

D'autre part, la surveillance ciblée peut être illégale dans des cas où elle pourrait être fondée sur des motifs légitimes – par exemple lorsqu'il existe des charges suffisantes pour suspecter une personne d'avoir commis un délit –, mais où le système permettant cette surveillance est en soi illégal parce qu'il ne prévoit pas de garanties suffisantes (notamment des voies de recours) contre les abus.

Cela s'explique surtout par l'effet paralysant (*chilling effect*) qu'une telle surveillance peut avoir. Dans ce contexte, la notion d'effet paralysant désigne le phénomène selon lequel des personnes renoncent à exercer leurs droits par peur d'être surveillées. Autrement dit, « la possibilité qu'une information relative à des communications soit interceptée constitue même à elle seule une immixtion dans la vie privée et peut être attentatoire à des droits, y compris ceux relatifs à la liberté d'expression et d'association[4]. »

Des études ont confirmé que les militantes et militants qui craignent – même sans preuve – de faire l'objet d'une

---

[1] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, doc ONU A/HRC/41/35 (2019), p. 22.

[2] https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/.

[3] "Spyware Scandal: UN experts call for moratorium on sale of 'life-threatening' surveillance tech", 12 août 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379.

[4] Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, Le droit à la vie privée à l'ère du numérique, doc ONU A/HRC/27/37, 30 juin 2014, § 20.

surveillance sont moins susceptibles de critiquer ouvertement leur gouvernement, d'organiser des manifestations, de se réunir librement avec des collègues, voire de parler au téléphone ou d'envoyer des courriels, car ces personnes ignorent comment ces activités pourront être utilisées contre elles[5].

Cette autocensure se produit lorsque les États n'adoptent pas de garanties suffisantes. Il est alors impossible de savoir qui fait l'objet d'une surveillance, ni comment ou pourquoi. Dans ces cas-là, « les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance secrète ne sont pas injustifiés […]. Dans ces circonstances, on est fondé à alléguer que la menace de surveillance restreint par elle-même la liberté de communiquer au moyen des services des postes et télécommunications et constitue donc, pour chaque usager ou usager potentiel, une atteinte directe au droit [au respect de la vie privée et familiale[6]]. »

Autrement dit, lorsque les garanties sont insuffisantes, ce ne sont pas seulement les droits des personnes visées qui sont touchés, mais ceux de la population dans son ensemble.

UN MORATOIRE POUR RENFORCER LES DROITS

Des organisations de la société civile et des médias ont démontré que ces deux types de ciblage illégal étaient extrêmement répandus, mais il ne fait pas de doute que la surveillance ciblée rendue illégale par un manque de garanties est pratiquement universelle. Comme l'a si bien résumé l'ancien rapporteur spécial David Kaye, « [d]ire que le mécanisme global de contrôle de l'utilisation des technologies de surveillance ciblée ne fonctionne pas est un euphémisme. En réalité, ce mécanisme est pratiquement inexistant[7]. » En l'absence de moratoire immédiat, l'utilisation illégale de technologies de surveillance continuera d'avoir des effets dévastateurs sur les droits humains des personnes visées, mais aussi de la population en général.

Ce moratoire sur les logiciels espions aurait deux grands objectifs : mettre fin à la vente, au transfert et à l'utilisation des technologies d'espionnage numérique, mais surtout renforcer les garanties en matière de droits humains.

Il convient donc peut-être d'imaginer ce moratoire comme une consolidation du droit au respect de la vie privée (et d'autres droits touchés par la surveillance illégale). Cela permettrait de réaffirmer l'interdiction de la surveillance illégale en vigueur et de renforcer les droits humains.

MODÈLES POSSIBLES

Un moratoire sur les logiciels espions devrait prendre la forme d'une liste des garanties relatives aux droits humains que les États auraient l'obligation de mettre en pratique avant de pouvoir vendre, transférer ou utiliser des technologies de surveillance ciblée.

Le droit international relatif aux droits humains donne de nombreux exemples de manières d'y parvenir. Le Traité sur le commerce des armes[8], par exemple, tout comme les propositions de traités visant à réglementer les systèmes d'armes létaux autonomes (ou « robots tueurs[9] ») ou le commerce des « instruments de torture[10] » comportent tous des critères

---

[5] Amnesty International, *Bélarus. « Il suffit que les gens pensent que ça existe ». Société civile, culture du secret et surveillance au Bélarus*, EUR 49/4306/2016, https://www.amnesty.org/fr/documents/eur49/4306/2016/fr/?msclkid=a728523ac7b611ec83ec6bce36b64552.

[6] *Roman Zakharov c. Russie*, Cour européenne des droits de l'homme, § 171.

[7] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, doc. ONU A/HRC/41/35 (2019), § 46.

[8] Traité sur le commerce des armes, adopté le 2 avril 2013, doc. ONU A/RES/ 67/234B, entré en vigueur le 14 décembre 2014, art. 7.

[9] Human Rights Watch, *New Weapons, Proven Precedent: Elements of and Models for a Treaty on Killer Robots*, octobre 2020, https://www.hrw.org/report/2020/10/20/new-weapons-proven-precedent/elements-and-models-treaty-killer-robots.

[10] Amnesty International, *Mettre fin au commerce de la torture. Vers des mesures de contrôle des « instruments de torture » au niveau mondial*, https://www.amnesty.org/fr/documents/act30/3363/2020/fr/.

imposant aux États d'adopter des garanties concernant des outils ou des technologies pouvant autant être utilisés de manière légitime qu'illégitime afin d'éviter les violations des droits engendrées par leur fabrication, leur utilisation ou leur transfert.

CONCLUSION

La nécessité d'un moratoire mondial sur la vente, le transfert et l'utilisation des technologies de surveillance ciblée est manifeste et urgente. En raison de l'absence de réglementation et de transparence dans la vente et l'utilisation de ces produits, nous ne connaîtrons peut-être jamais l'ampleur réelle de ce genre d'abus. Le monde ne peut plus fermer les yeux sur cette menace colossale qui pèse sur nos droits.

Des commentaires ou des questions ? Contactez rebecca.white@amnesty.org