**L’industrie de la surveillance et les droits humains**

**Réponse de la Suisse – 11.02.2019**

1. **Renseignements concernant les cadres réglementaires nationaux qui peuvent s’appliquer au développement, à la commercialisation, à l’exportation, au déploiement ou à la facilitation de technologies de surveillance par des entreprises privées, par exemple:**
2. **Lois, règlements administratifs, décisions judiciaires ou autres politiques et mesures qui imposent des règlements sur l’exportation, l’importation ou l’utilisation de technologies de surveillance à double usage;**

La loi du 13 décembre 1996 sur le contrôle des biens (LCB; RS *946.202*) règle les conditions d’importation, d’exportation, de transit et de courtage des biens à double usage (civil et militaire), des biens militaires spécifiques et des biens stratégiques.

En décembre 2013, les États parties à l’Arrangement de Wassenaar ont convenus d’élargir les listes de biens destinés à la surveillance d’internet et des communications mobiles qui sont soumis au contrôle à l’exportation, pour y inclure notamment des biens des technologies de l’information, comme les logiciels d’intrusion, les systèmes de surveillance de protocole internet et les appareils servant à capter l’identité internationale d’abonné mobile (intercepteurs d’IMSI). En Suisse, ces biens figurent à l’annexe 2 de l’ordonnance du 3 juin 2016 sur le contrôle des biens (OCB; RS *946.202.1*) en tant que biens à double usage (civil et militaire) et sont de ce fait soumis au régime du permis.

Pour ces raisons, le 13 mai 2015, le Conseil fédéral a édicté l’ordonnance sur l’exportation et le courtage de biens destinés à la surveillance d’internet et des communications mobiles (OSIC, RS *946.202.3*). Cette ordonnance permet de refuser le permis s’il y a des raisons de penser que les biens qui doivent être exportés ou faire l’objet d’un courtage seront utilisés par le destinataire final comme moyens de répression. Il s’agit d’une ordonnance basée directement sur la Constitution, dont la durée de validité est limitée à 4 ans.

L’OSIC ayant fait ces preuves, le Conseil fédéral a pour cette raison approuvée le 27 juin 2018 le message au Parlement correspondant. La proposition concrète a pour but de créer la base légale permettant d’intégrer le contenu de l’ordonnance dans le droit ordinaire.

Le 17 avril 2018, le Tribunal administratif fédéral s’est occupé d’une décision de refus sur la base de l’OSIC. Le permis d’exportation a été refusé car il y avait des raisons de supposer que

« les biens qui doivent être exportés ou faire l'objet d'un courtage seront utilisés par le destinataire final comme moyens de répression » (OSIC, art. 6, al.1 let a). Le Tribunal administratif fédéral a confirmé la décision de l’autorité des contrôles à l’exportation suisse et a rejeté le recours du demandeur (B-7184/2017).

1. **Recours possibles en cas d’exportation illicite ou d’utilisation de technologies de surveillance privées ;**

Les dispositions pénales sont ancrées dans l’art. 9 de l’OSIC:

1. Est puni d’une peine privative de liberté de trois ans au plus ou d’une peine pécuniaire quiconque, intentionnellement:
	1. sans être titulaire d’un permis, exporte ou se livre au courtage des biens destinés à la surveillance d’Internet et des communications mobiles qui sont mentionnés en annexe;
	2. sans être titulaire d’un permis, transfère des biens immatériels, y compris le savoir-faire, et la concession de droits y afférents à des destinataires à l’étranger ou se livre à leur courtage;
	3. n’observe pas les conditions et les charges assorties à un permis;
	4. dans une demande, donne des indications fausses ou incomplètes alors qu’elles sont essentielles pour l’octroi d’un permis, ou utilise une telle demande faite par un tiers;
	5. ne déclare pas ou déclare de manière inexacte l’exportation ou le courtage des biens matériels ou immatériels;
	6. fait ou fait faire le courtage des biens matériels ou immatériels, les livre ou les fait livrer, les transfère ou les fait transférer à un destinataire final ou vers un lieu de destination autre que celui qui figure dans le permis;
	7. fait parvenir des biens matériels ou immatériels à un tiers, dont il sait ou doit présumer qu’il les transmettra, directement ou indirectement, à un utilisateur final auquel ils ne doivent pas être livrés.
2. En cas d’infraction grave, la peine est une peine privative de liberté de un à cinq ans.
3. Si l’auteur a agi par négligence, la peine est une peine pécuniaire de 180 jours-amende au plus.
4. **Si les lois, règlements ou politiques identifies sont conformes aux obligations des Etats en vertu de l’article 19 du Pacte internationale relative aux droits civils et politiques, de l’articles 19 de la Déclaration universelles des droits de l’homme et d’autre normes pertinents relatives aux droits de l’homme.**

Concernant l’exportation, l’objectif de l’OSIC est le contrôle des exportations et le courtage de biens destinés à la surveillance d’internet et des communications mobiles qui pourraient être utilisés dans le contexte de la répression. L’idée de base de l’OSIC est particulièrement de respecter le droit à la liberté d’opinion et d’expression.

1. **Information concernant l’utilisation de ces technologies de surveillance:**
2. **La mesure dans laquelle des sociétés privées de surveillance offrent des services aux Etats et à d’autres acteurs pour déployer leurs technologies dans des circonstances spécifiques et la mesure dans laquelle les entreprises sont au courant de l’utilisation finale des technologies qu’elles commercialisent.**

La loi fédérale sur les prestations de sécurité privées fournies à l’étranger (LPSP) est entrée en vigueur le 1er septembre 2015. Selon la loi, les entreprises qui entendent fournir depuis la Suisse des prestations de sécurité privées à l’étranger sont tenues de le déclarer préalablement à l’autorité compétente (art. 10, LPSP). Des prestations de sécurité privées, telles que le soutien opérationnel ou logistique à des forces armées ou de sécurité ou le conseil ou la formation du personnel de forces armées ou de sécurité étrangères, sont également soumises à l’obligation de déclarer. Elles peuvent par ailleurs être liées aux marchés passés avec l’étranger dans le domaine des biens destinés à la surveillance d'internet et des communications mobiles.

La formation relative à l’utilisation de ces biens et de ces technologies, l’entretien, la réparation et le développement de ces biens et de ces technologies (soutien logistique) constituent des exemples de prestations relevant du champ d’application de la loi. Au-delà des dispositions légales liées à l’exportation de biens et de technologies de surveillance, la LPSP permet un contrôle sur l’utilisation de ces biens et de ces technologies par des États étrangers, pour autant que des prestations de services selon la LPSP soient présentes et les destinataires de ces prestations soient des forces armées ou de sécurité étrangères. Lors de la soumission d’une déclaration, l’autorité compétente analyse en effet en détail les activités planifiées et vérifie dans quelle mesure ces activités respectent les objectifs de la loi, parmi lesquels figure la garantie du respect du droit international, en particulier des droits de l’homme et du droit international humanitaire (art. 1, LPSP). L’autorité ouvre une procédure d’examen lorsque des indices font penser que ces activités pourraient être contraires aux buts de la loi. Dans ce cas, elle interdit l’activité. L’autorité a plusieurs fois été saisie de cas d’entreprises offrant des prestations dans le domaine des technologies de surveillance (formation, soutien logistique). Ce type de prestations a également fait l’objet d’interdictions.

Les prestations liées aux activités d’intelligence privée sont également soumises à l’obligation de déclarer selon la LPSP. Dans ce domaine, les entreprises doivent communiquer à l’autorité compétente l’identité du mandant ou du destinataire de la prestation lorsque celui-ci est un État étranger ou l’un de ses organes, un organisme qui se considère comme un gouvernement ou comme un organe étatique, ou lorsqu’il s’agit d’une organisation internationale (art. 5 de l’Ordonnance sur les prestations de sécurité privées fournies à l’étranger, OPSP). L’autorité compétente n’a pas été saisie de cas d’entreprises offrant dans ce domaine des services ayant pour objet le déploiement de technologies de surveillance dans des circonstances spécifiques.