Cour fédérale  Federal Court

Ottawa, le 28 novembre 2017 – Dans les demandes présentées en vertu des articles 12 et 21 de la Loi sur le *Service canadien du renseignement de sécurité*, le juge en chef a rendu des motifs de jugements confidentiels le 27 septembre 2017. Après avoir pris en compte les représentations de la part des avocats, incluant deux *amici curiae* nommés par la Cour, des versions caviardées de ces motifs publics ont été conclues par la Cour. Ces motifs publics sont émis aujourd'hui.

Résumé (2017 CF 1047): Dans cette décision, la question centrale à être tranchée par la Cour porte sur la légalité de l'utilisation d'un émulateur de station de base (ESB) sans mandat par le Service canadien du renseignement de sécurité (SCRS). Entre autre, la Cour a dû déterminer si cette activité menée par le SCRS constituait une violation des droits de la cible d'enquête contre les fouilles, les perquisitions et les saisies abusives qui lui sont garantis par l'article 8 de la *Charte canadienne des droits et libertés* (Charte)

Le SCRS se sert d'ESB afin d'obtenir les caractéristiques distinctives d'appareils mobiles des cibles spécifiques de ces enquêtes dont l'identité internationale de l'abonné mobile (*International Mobile Subscriber Identity* ou IMSI) et l'identité internationale d'équipement mobile (*International Mobile Equipment Identity* ou IMEI).

Suite à son examen de la preuve, la Cour conclu que, bien que les droits de la cible protégés par l'article 8 de la Charte étaient atteints, ces derniers n'ont pas été violés. Bref, la cueillette d'identificateurs IMSI et IMEI par le SCRS était une « fouille » au sens de l'article 8 de la Charte car ces numéros ont aidé le Service à mieux comprendre certains aspects des renseignements biographiques d'ordre personnel relativement auxquels la cible avait une attente raisonnable en matière de vie privée. Par contre, la fouille sans mandat n'était pas « abusive ». La raison en est que cette fouille était étroitement ciblée, très précise et minimalement envahissante, principalement grâce aux mesures mises en œuvre par le SCRS dans le cadre de ses opérations fondées sur les ESB. Entre autres, lors des opérations d'ESB, le matériel ne garde le contact avec les appareils mobiles que pendant quelques secondes et il ne nuit d'aucune manière perceptible à l'expérience de l'utilisateur d'un appareil mobile. De plus, les opérations du SCRS fondées sur des ESB n'ont pas d'incidence sur la capacité de l'utilisateur de l'appareil mobile de composer le 911, et le Service n'a pas recueilli le contenu des communications ou les données qui y sont rattachées. Enfin, le SCRS supprime très rapidement les IMSI et le IMEI tirées d'appareils mobiles de tiers, et elles ne font l'objet d'aucune analyse. En autant que le Service continue d'exécuter ces opérations ESB de la même façon à l'avenir, la Cour a conclu que si ces mesures essentielles sont en tout temps respectées, ces activités ne constituent pas une fouille abusive eu égard à l'article 8 de la Charte. Par contre, la Cour a remarqué que l'utilisation de la technologie relative aux ESB pour recueillir en « lots » les IMSI et les IMEI des appareils mobiles du public ne serait pas permise car une telle fouille ne satisferait pas au critère d'une fouille sans mandat.

**

Résumé (2017 CF 1048): Le SCRS a déposé plusieurs demandes de mandats dans le cadre de ses enquêtes sur deux ensembles distincts d'activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Ces demandes ont soulevé trois questions relatives à l'autorisation demandée par le SCRS d'obtenir des données d'identification de base (DIB) auprès des fournisseurs de services de communication (FSC). Les DIB comprennent le nom et l'adresse de l'abonné à un compte de communications, et, dans certains cas, l'information concernant l'adresse IP. Les trois questions soulevées en l'espèce étaient :

1. La Cour peut-elle autoriser le SCRS à obtenir des DIB auprès des FSC liées à des comptes de personnes non-identifiées dont les numéros de téléphone ou les identificateurs électroniques pourront éventuellement attirer l'attention du SCRS?

2. La Cour peut-elle autoriser le SCRS à obtenir les DIB liées aux comptes de personnes qui ont été identifiées?

3. La Cour peut-elle autoriser le SCRS à obtenir les DIB liées à un compte de communications lorsqu'un « chef » au sein du SCRS détermine que ce compte a été découvert lors d'une enquête et que les DIB faciliteraient cette enquête et cela?

La Cour a conclu qu'avant qu'elle ne puisse accorder à un agent de l'État l'autorisation de mener une activité envahissante, elle doit être satisfaite qu'il existe un lien suffisant entre l'enquête et la personne dont les droits en matière de vie privée seraient enfreints.

Puisqu'un tel lien n'a pas été démontré dans les circonstances entourant la première question, la Cour a déterminé que les autorisations demandées ne satisfaisaient pas aux exigences de base nécessaires pour autoriser des agents de l'État à mener une activité envahissante. Quant à la deuxième question, la Cour a accordé l'autorisation d'obtenir les DIB car un lien suffisant avait été établi. Enfin, quant à la troisième question, la Cour a conclu que l'autorisation demandée ne pouvait être accordée, car elle constituerait une délégation inacceptable de fonctions judiciaires qui doivent être exercés par la Cour elle-même.

**

Vous pouvez obtenir les deux décisions sur le site Internet de la Cour fédérale : http://cas-ncr-nter03.cas-satj.gc.ca/portal/page/portal/fc_cf_fr/Index

****

Andrew Baumberg
Media Contact / Liaison avec les Médias
Federal Court / Cour fédérale
Tel. / Tél. : (613) 947-3177