Projet OSSNR

Dossier INSET# 2022-123

Dossier PPSC #: F22-004

Canada

Province d'Ontario

COUR SUPÉRIEURE DE JUSTICE

(Région de l'Est)

DANS L'AFFAIRE DES demandes de :

Une autorisation d'intercepter des communications privées en vertu des dispositions des articles 185 et 186 du *Code criminel* ;

Mandats généraux en vertu de l'article 487.01 du *Code criminel* ;

Un mandat d'enregistrement de données de transmission en vertu de l'article 492.2(1) du *Code criminel*;

Un mandat de localisation en vertu de l'article 492.1 (2) du *Code criminel* ; Une ordonnance d'assistance en vertu de l'article 487.02 du *Code criminel* ; et

Une ordonnance de mise sous scellés de tous les documents non visés par l'article 187 du *Code criminel*.

L'HONORABLE

JUSTICE Bertha Wilson) Mercredi, le 1er jour du mois de juin

) 2022.

AUTORISATION D'INTERCEPTER LES COMMUNICATIONS ET ORDONNANCES ET MANDATS CONNEXES

SUR LA DEMANDE écrite, faite le 31e jour de mai 2022, par Sandra O'Connor, un agent spécialement désigné par écrit aux fins des sections 185,487. 01 (4) et (5) du *Code criminel* par le ministre de la Sécurité publique et de la Protection civile pour obtenir une ordonnance autorisant l'interception de communications en vertu des articles 185 et 186 du *Code criminel* ; un mandat général autorisant des observations au moyen d'une caméra de télévision ou d'un autre dispositif électronique en vertu de l'article 487.01 du *Code criminel* ; et une ordonnance d'assistance en vertu de l'article 487.02 du *Code criminel* ;

ET SUITE À LA DEMANDE écrite faite à la même date par le sergent Tom Erdely, agent de la paix, en vue d'obtenir des mandats généraux en vertu de l'article 487.01 du *Code criminel* ; des mandats autorisant l'utilisation d'un enregistreur de données de transmission en vertu de l'article 492.2(1) du *Code criminel*; des mandats de localisation en vertu de l'article 492.1(2) du *Code criminel* ; une ordonnance d'assistance en vertu de l'article 487.02 du *Code criminel*; et une ordonnance de mise sous scellés de tous les documents non visés par les articles 187 du *Code criminel* ;

APRÈS AVOIR LU les demandes, ainsi que les renseignements à l'appui et l'affidavit de Tom Erdely, daté du 29e jour de mai 2022 ;

APRÈS AVOIR ÉTÉ SATISFAIT que les exigences des articles 185, 186(1)(a) et (b), 492.1(2), 492.2(1), 487.01 et 487.02 du *Code criminel* ont été satisfaites ;

IL EST ORDONNÉ QUE :

Tout agent de la paix, et toute personne agissant sous sa direction, est autorisé à intercepter des communications conformément aux conditions de la présente autorisation.

De plus, tout agent de la paix est autorisé à observer au moyen d'une caméra de télévision ou d'un autre dispositif électronique similaire, conformément aux conditions de la présente autorisation.

INFRACTIONS

1. Les infractions pour lesquelles des communications peuvent être interceptées et des observations peuvent être faites sont :

    a. Possession d'explosifs avec l'intention de causer des dommages à la propriété, contrairement à l'article 81(1)(a) du *Code criminel*;

b. Possession d'explosifs avec l'intention de causer des dommages à la propriété, contrairement à l'article 81(1)(c) du *Code criminel*;

c. Participation à l'activité d'un groupe terroriste en contravention de l'article 83.18(1) du *Code criminel*;

d. Facilitation d'une activité terroriste en contravention de l'article 83.19 (1) du *Code criminel*;

f. La participation à une activité d'un groupe terroriste en violation de l'article 83.18 (1) du *Code criminel*; et

e. Conspiration en vue de commettre ou de tenter de commettre l'une des infractions susmentionnées, ou complicité après coup dans la perpétration de l'une de ces infractions, ou conseils relatifs à l'une de ces infractions, en violation de l'article 465 (1)(c) du *Code criminel.*

TYPES DE COMMUNICATIONS ET D'OBSERVATIONS

2. Les types de communications qui peuvent être interceptés sont toutes les communications et télécommunications orales privées, ainsi que toutes les communications téléphoniques par radio. Les observations qui peuvent être faites concernent les activités dans des circonstances où les personnes ont des attentes raisonnables en matière de vie privée.

PERSONNES

3. Les personnes dont les communications peuvent être interceptées et qui peuvent être observées sont:

a. Principales personnes désignées :

i. Nom : Charlie BLACK Date de naissance : 1er octobre 1999

Adresse : 123 rue Main, Ottawa, Ontario

Profession : Développeur Web

ii. Nom : Sam WHITE Date de naissance : 1er décembre 1989

Adresse : 234, rue First, Ottawa, Ontario

Profession : Adjoint administratif

iii. Nom : Jordan RED Date de naissance : 1er septembre 2000

Adresse : 345 Avenue Second, Ottawa, Ontario

Profession : Spécialiste en informatique

c. Personnes inconnues :

i. Toute autre personne interceptée ou observée en tout lieu visé au paragraphe 4 ou par l'entremise de tout système informatique ou service de télécommunication visé au paragraphe 5.

LIEUX

4. Les communications des personnes visées au paragraphe 3 peuvent être interceptées à :

a. Lieux de garde

i. Tout lieu fixe ou mobile, où une personne du paragraphe 3a est détenue légalement.

b. Lieux à microphones activés

i. Tout endroit, fixe ou mobile, situé à portée audible d'un système informatique visé au paragraphe 5a.

c. Autres endroits

i. Tout autre endroit, fixe ou mobile, dont il y a des motifs raisonnables de croire qu'il est ou sera utilisé par une personne visée au paragraphe 3a.

Et où les personnes visées au paragraphe 3a peuvent être observées :

d. **Lieux d'observation**

i. Tout lieu, fixe ou mobile, où une personne visée au paragraphe 3a est détenue légalement.

SYSTÈMES INFORMATIQUES ET SERVICES DE TÉLÉCOMMUNICATION

5. Les communications des personnes visées au paragraphe 3 peuvent être interceptées lorsqu'elles sont effectuées à l'aide des systèmes informatiques ou des services de télécommunication suivants :

a. Dispositif mobile ou service de télécommunication associé à :

i. Le numéro de téléphone 613-555-2345, et le numéro d'identité mobile international (IMEI) 345898779877989877 utilisé par Charles BLACK ; et

ii. Le numéro de téléphone 613-555-3456 et le numéro international d'identité mobile (IMEI) 341214711471147114711471 qui y est associé, utilisés par Charles BLACK.

Il est entendu que l'interception en vertu du paragraphe 5a peut se poursuivre sur tout appareil mobile associé au numéro de téléphone, au IMEI, au numéro IMSI ou à tout autre appareil mobile ou identificateur de service de télécommunication unique qui ont été associés ensemble par le fournisseur de services de télécommunication à la date à laquelle cette autorisation a été accordée ;

b. tout autre système informatique ou service de télécommunication dont on a de bonnes raisons de penser qu'il est utilisé par une personne visée au paragraphe 3a. L'interception en vertu du présent alinéa peut se poursuivre sur tout dispositif ou identifiant de service de télécommunication associé au numéro de téléphone, au numéro IMEI, au numéro IMSI ou à tout autre système informatique ou identifiant de service de télécommunication unique qui étaient associés ensemble par le fournisseur de services de télécommunication au moment où l'interception a commencé en vertu du présent alinéa ; et

c. toute fonction de transfert d'appel, de renvoi d'appel ou de messagerie vocale associée à tout téléphone en tout lieu visé au paragraphe 4, ou à tout système informatique ou service de télécommunication visé au paragraphe 5.

AUTRES MODALITÉS ET CONDITIONS

6. Il est en outre ordonné que :

Les communications avocat-client

a. Aucune communication ne peut être interceptée au bureau ou à la résidence d'un avocat, ou à tout autre endroit habituellement utilisé par les avocats pour consulter leurs clients ;

b : Lorsqu'un contrôleur croit raisonnablement qu'un avocat est partie à une communication, interceptée en tout lieu ou par tout dispositif, le contrôleur doit interrompre l'interception. À des intervalles raisonnables, le contrôleur peut reprendre l'interception dans le but de déterminer si l'avocat reste partie à la communication. Lorsque des communications ont été interceptées alors qu'elles sont sous surveillance automatique, le surveillant qui examine ultérieurement la communication doit cesser de l'examiner dès qu'il a des raisons de croire qu'un avocat est partie à la communication, mais il peut surveiller la communication en l'examinant à intervalles raisonnables afin de déterminer si l'avocat reste partie à la communication. Nul ne peut accéder à une communication à laquelle un avocat fait partie et qui est enregistrée conformément à la présente autorisation, sauf si la Cour l'autorise ;

Toutefois, si une ou plusieurs communications ont été interceptées et que l'accès a été refusé conformément au présent paragraphe, et s'il est raisonnable de penser qu'une communication peut être soumise au secret professionnel de l'avocat, la ou les communications peuvent être soumises à la Cour pour déterminer ex-parte si l'accès à l'une ou l'autre des communications sera autorisé.

Surveillance en direct

c. L'interception dans les lieux visés au paragraphe 4a s'accompagne d'une surveillance visuelle en direct ou d'une surveillance audio en direct. L'interception d'une communication est interrompue dès qu'il a été établi qu'aucune des personnes visées au paragraphe 3a n'y est partie. Toutefois, l'interception peut être reprise à intervalles raisonnables pour déterminer si une telle personne est devenue partie à la communication. Si tel est le cas, l'interception peut se poursuivre.

Il est entendu que les communications traitées conformément au présent paragraphe qui sont interceptées au moyen d'un système de livraison différée sont réputées de faire l'objet d'une écoute en direct.

Il est entendu que le paragraphe 6c ne s'applique pas à l'interception au moyen d'un outil d'enquête sur dispositif (un programme informatique connu sous le nom d'outils d'enquête embarqués (OEE) et ne s'applique pas à l'interception de télécommunications non orales.

Interceptions au moyen d'un outil d'enquête embarqués (OEE)

d. Lorsque des communications orales ont été interceptées à l'aide d'un OEE, le moniteur qui examine ensuite la communication doit cesser de l'examiner dès qu'il détermine qu'aucune personne visée au paragraphe 3a n'est partie à la communication ou, lorsque l'interception est effectuée par micro activé à un endroit visé au paragraphe 4b, qu'aucune personne visée au paragraphe 3a n'est à portée audible du système informatique visé au paragraphe 5a. Le contrôleur peut examiner la communication à intervalles raisonnables afin de déterminer si une personne visée au paragraphe 3a devient partie à la communication ou se trouve à portée audible du système informatique visé au paragraphe 5a, auquel cas l'examen peut se poursuivre. Nul ne peut accéder à une communication à laquelle aucune personne visée au paragraphe 3a n'est partie, ou qui se trouve à portée audible du dispositif visé au paragraphe 5a, sauf autorisation de la Cour.

Observations

f. En ce qui concerne les observations aux endroits mentionnés au paragraphe 4d, toutes les observations décrites au paragraphe 2 ne peuvent être faites que par un agent de la paix. En ce qui concerne les lieux d'observation, aucune observation ne sera faite au bureau ou à la résidence d'un avocat, ou à tout autre endroit habituellement utilisé par les avocats pour consulter leurs clients, ou dans une chambre à coucher ou une salle de bain.

Les observations dans les lieux visés au paragraphe 4d ne sont entreprises que s'il existe des motifs raisonnables de croire qu'une personne visée au paragraphe 3a se trouve ou est sur le point de se trouver dans ce lieu. Lorsqu'il y a de bonnes raisons de croire qu'aucune des personnes visées au paragraphe 3a ne se trouve dans ce lieu, les observations sont interrompues.

MODALITÉS D'INTERCEPTION ET D'OBSERVATION

7. Dispositifs électromagnétiques, acoustiques, mécaniques ou autres, y compris les moyens d'un OEE. Les observations qui peuvent être faites le sont au moyen d'une caméra de télévision ou d'un autre dispositif électronique similaire.

GARANTIE DE L'ENREGISTREUR DE DONNÉES DE TRANSMISSION (art. 492.2(1))

8. Il est ordonné que les agents de la paix soient autorisés à obtenir des données de transmission au moyen d'enregistreurs de données de transmission, y compris les OEE, et à installer, activer, utiliser, entretenir, surveiller et retirer, secrètement ou autrement, des enregistreurs de données de transmission en relation avec les lieux mentionnés au paragraphe 4 lorsqu'ils sont utilisés par les personnes désignées au paragraphe 3a et les systèmes informatiques et services de télécommunication visés au paragraphe 5.

GARANTIE GÉNÉRALE D'OBTENTION DE CARACTÈRES COMPOSÉS (art. 487.01)

9. Il est ordonné que les agents de la paix soient autorisés à obtenir et à enregistrer tous les caractères composés qui ne sont pas autrement autorisés par le paragraphe 2 de la présente autorisation en relation avec les lieux du paragraphe 4 lorsqu'ils sont utilisés par les personnes nommées au paragraphe 3a et les systèmes informatiques et services de télécommunication énumérés au paragraphe 5.

GARANTIE GÉNÉRALE D'INTERCEPTION DES FONCTIONS D'ORDINATEUR ET D'UTILISATION DES OEE (art. 487.01)

10. Il est ordonné que les agents de la paix soient autorisés à faire ce qui suit :

a. "Intercepter" toutes les "fonctions" (telles qu'elles sont définies à l'article 342.1 (2) du *Code criminel*), y compris, mais sans s'y limiter, la navigation sur le Web et les données ou les renseignements qui aideront à accéder à un OEE, à l'installer, à le maintenir ou à le retirer, sur tout système informatique à un endroit visé au paragraphe 4 et de tout système informatique ou service de télécommunication visé au paragraphe 5, ou en acquérir la substance, le sens ou la portée, non autrement autorisé par les paragraphes 2 ou 8 de la présente autorisation. L'interception des fonctions décrites dans le présent paragraphe n'est pas soumise à une surveillance en direct.

b. Accéder secrètement, à distance ou autrement, aux systèmes informatiques visés au paragraphe 5a et les modifier afin d'installer, d'activer, de maintenir ou de supprimer par tout moyen un OEE dans ou sur le système informatique.

c. Copier à partir des systèmes informatiques visés au paragraphe 5a, à l'aide d'un OEE, toute donnée aux fins de l'installation, de la maintenance et de la suppression de l'OEE, y compris mais sans s'y limiter :

i. Les mots de passe, les codes de passe et les clés de chiffrement ; et

ii. L'utilisation de l'ordinateur, l'identité de l'utilisateur de l'ordinateur, ou la configuration des fonctions et des programmes du système informatique.

d. Copier, à partir des systèmes informatiques visés au paragraphe 5a, à l'aide d'un OEE, toute donnée stockée dans le système informatique ou accessible à celui-ci, quel que soit l'endroit où les données sont physiquement enregistrée, qui peut constituer une preuve des infractions visées au paragraphe 1, notamment

i. Les télécommunications, y compris les communications privées reçues, envoyées et non envoyées, datées après et y compris le 1er janvier 2021, mais avant la date de délivrance de la présente autorisation, y compris les données relatives à l'identité de l'initiateur ou du récepteur de ces communications.

ii. Les données comprenant :

a. Les dates et heures, y compris les décalages (fuseau horaire), si disponibles, pour tous les types de données suivants ;

b. Système de positionnement global (GPS) et données de géolocalisation ;

c. Les journaux d'appels téléphoniques, y compris ceux composés, manqués ou reçus ;

d. Les fichiers multimédias, y compris les photographies, les fichiers vidéo, les fichiers audio ou toute autre image et les métadonnées associées ;

e. Documents et notes électroniques, y compris les copies numérisées ou les images de fichiers texte, les documents de traitement de texte, le format de document portable (PDF), les feuilles de calcul, les bases de données, les rappels de tâches, les événements de calendrier, les documents de voyage tels que les itinéraires et les cartes de voyage, les informations de passeport et/ou les cartes d'embarquement électroniques ;

f. Les métadonnées et les données EXIF qui font partie d'un fichier et qui comprennent les dates et heures de création/modification, le modèle d'appareil photo, l'auteur, le titre, le sujet, les attributs de fichiers *Windows*, *Mac* et *Linux*, l'adresse, l'emplacement, le statut de cryptage, les données supprimées, la langue, le format, le sujet et/ou la taille du fichier ;

g. Toutes les données énumérées dans le présent document qui peuvent être trouvées sur les services en réseau qui sont disponibles et contenues dans les extractions de données ;

h. Toutes les données énumérées dans les présentes qui peuvent être trouvées sur des applications de médias sociaux (applications) ou un enregistrement *Cloud* sur internet qui sont disponibles et contenues dans les extractions de données ;

i. L'OEE n'obtient initialement que les données d'identification du système informatique ;

ii. Les collecteurs de l'OEE ne peuvent être activés qu'après qu'il a été déterminé que l'OEE se trouve sur un système informatique du paragraphe 5a. L'OEE doit être retiré de tout autre système informatique ; et

iii. Toutes les données d'identification obtenues à partir d'un système informatique ne relevant pas du paragraphe 5a doivent être stockées en toute sécurité et ne pas être communiquées aux enquêteurs ou utilisées à d'autres fins sans une nouvelle ordonnance de la Cour. Ces données doivent être détruites à la fin de l'enquête si aucune accusation n'est portée, ou lorsque toutes les accusations découlant de l'enquête sont définitivement tranchées, y compris tous les appels.

i. L'équipe d'accès secret et d'interception (EASI) ou l'unité spéciale "I" s'efforcera raisonnablement de séparer toutes les données copiées conformément au paragraphe 10d qui ne se trouvent pas dans la période définie. Les données isolées ne peuvent être utilisées par l'EASI ou le "Spécial I" qu'aux fins décrites au paragraphe 10c, et ne doivent pas être partagées avec les enquêteurs ou utilisées à d'autres fins sans une nouvelle ordonnance du tribunal. Les données isolées sont détruites à la fin de l'enquête si aucune accusation n'est portée, ou lorsque toutes les accusations découlant de l'enquête sont définitivement tranchées, y compris tous les appels.

j. Si, après examen, on peut raisonnablement penser que l'une des données copiées et transmises aux serveurs de la police en vertu du présent mandat général constitue une communication privée à laquelle un avocat est partie, cette communication est soumise aux conditions énoncées au paragraphe 6b.

k. Il n'y a pas de limite au nombre de fois que les agents de la paix peuvent faire les choses décrites dans le présent mandat général.

l. L'interception de fonctions informatiques à l'aide d'un OEE n'est pas soumise à une surveillance en direct.

m. Conformément à l'article 487.01 (5.1) du *Code criminel*, un avis d'accès à un système informatique visé au paragraphe 5a en vertu du présent mandat général doit être donné à la personne qui a fait l'objet du déploiement et de l'activation de l'OEE. Le délai dans lequel l'avis doit être donné conformément à l'article 487.01 (5.1) du *Code criminel* est de quatre-vingt-dix jours au plus tard après l'expiration du présent mandat général, sous réserve de toute prolongation accordée en vertu de l'article 487.01 (5.2) du *Code criminel*, et tout système informatique auquel on accède plus d'une fois ne nécessite qu'un seul avis à la personne qui a fait l'objet de la technique.

GARANTIE GÉNÉRALE D'OBTENTION DE RENSEIGNEMENTS SUR L'ABONNÉ (art. 487.01)

11. Il est ordonné que les agents de la paix soient autorisés à obtenir des fournisseurs de services de télécommunication les renseignements de base sur l'abonné (nom et adresse du client) pour toute adresse de protocole internet qui sera identifiée par le mandat d'enregistrement des données de transmission ou le mandat général d'interception des fonctions informatiques.

MANDAT POUR UN DISPOSITIF DE LOCALISATION (art. 492.1 (2))

12. Il est ordonné que les agents de la paix soient autorisés à obtenir des données de repérage au moyen d'un dispositif de localisation, y compris un OEE, et à, secrètement ou autrement, installer, activer, utiliser, entretenir, surveiller et retirer des dispositifs de repérage dans ou sur les systèmes informatiques ou les services de télécommunication mentionnés au paragraphe 5.

ENTRÉE

13. Afin d'exécuter les termes de la présente autorisation et des ordonnances et mandats connexes, les agents de la paix sont autorisés à pénétrer, secrètement ou non, dans les lieux mentionnés au paragraphe 4 et dans leurs environs immédiats, à l'exception de toute résidence, afin d'installer, d'entretenir ou de retirer tout dispositif électromagnétique, acoustique, mécanique ou autre, toute caméra de télévision ou autre dispositif électronique similaire, et tout dispositif de repérage.

ORDONNANCE D'ASSISTANCE (art. 487 .02)

14. Conformément à l'article 487.02 du *Code criminel*, il est ordonné que *Synergy Communications*, Bell Canada, Bell Mobilité Inc., *Rogers Communications Canada Inc*., *Telus Communications Inc*., *Freedom Mobile Inc*. et toute autre personne au Canada qui fournit des services téléphoniques ou de télécommunication fournissent l'assistance raisonnablement requise pour donner effet à la présente autorisation et aux ordonnances et mandats connexes. Sans restreindre la généralité de ce qui précède, cette assistance comprendra ce qui suit :

a. Fournir les renseignements et les installations nécessaires à l'installation, à l'entretien, à la surveillance et au retrait de tout dispositif électromagnétique, acoustique, mécanique ou autre, ou d'une caméra de télévision ou d'un dispositif électronique similaire pour intercepter des communications, ou pour faire des observations.

b. Faire tous les efforts raisonnables pour permettre l'accès à la messagerie vocale d'une manière qui ne puisse pas être détectée par l'abonné.

c. Fournir les informations et les installations nécessaires à l'installation, à l'entretien, à l'activation, à l'utilisation, à la surveillance et au retrait d'un enregistreur de données de transmission, et fournir les données de transmission.

d. Fournir les informations de base publiées et non publiées sur l'abonné (nom et adresse du client) et toutes les informations d'identification du fournisseur de services (IIFS), y compris tous les fournisseurs de services de télécommunications et leurs revendeurs, associés aux numéros de téléphone, aux numéros IMEI et IMSI identifiés par le mandat de l'enregistreur de données de transmission. Nonobstant le paragraphe 15, l'obligation de produire des informations reste en vigueur jusqu'à ce que les informations aient été produites.

e. Fournir toutes les informations de base sur l'abonné (nom et adresse du client) décrites au paragraphe 11.

f. Fournir les informations et les installations nécessaires à l'installation, à l'activation, à l'utilisation, à l'entretien, à la surveillance et au retrait des dispositifs de suivi, et fournir les données de suivi.

g. Activer secrètement toute fonction d'un système informatique ou d'un service de télécommunication du paragraphe 12 et prendre toutes les mesures nécessaires pour permettre l'obtention des informations sur la position géographique actuelle à partir du système informatique ou du service de télécommunication.

h. Aucune personne fournissant une assistance, y compris ses employés, préposés et agents, ne peut directement ou indirectement divulguer ou permettre la divulgation de toute assistance fournie, ou du contenu, l'existence ou le fonctionnement de la présente autorisation, ainsi que des ordonnances et mandats connexes, à quiconque, sauf si cela s'avère nécessaire aux fins de l'exécution de l'ordonnance d'assistance ou de l'obtention de l'avis ou de l'assistance d'un conseiller juridique, sauf ordonnance contraire d'un tribunal compétent.

DURÉE

15. La présente autorisation et les ordonnances et mandats connexes sont valables pour une période n'excédant pas 60 jours, à compter de la date de délivrance, inclusivement.

ORDONNANCE DE SCELLEMENT

16. Tous les documents relatifs à la présente autorisation et aux ordonnances et mandats connexes doivent être mis sous scellés à l'abri de la vue du public dans le même paquet et traités conformément aux articles 187 et 487.3 du *Code criminel*.

FAIT à Ottawa, Ontario, le 1er jour de juin 2022.

L'honorable juge

_____

Bertha Wilson

de la Cour supérieure de justice