L'EXPLORATION RADIO ET DU RÉSEAU CÂBLÉ ET LE SECRET PROFESSIONNEL DE L'AVOCAT

JÉRÔME GURTNER*
Docteur en droit, greffier au Tribunal administratif fédéral, St-Gall

Mots-clés: exploration, surveillance, secret professionnel de l'avocat

L'auteur présente l'exploration radio et l'exploration du réseau câblé prévues par la LRens, ainsi que l'ATF 147 I 280. Il discute ensuite des perspectives de l'exploration, notamment sous l'angle du secret professionnel de l'avocat.

I. Introduction

Le 1.12.2020, le Tribunal fédéral (ci-après: TF) a rendu un arrêt intéressant. Il portait sur une requête qui tendait à faire cesser l'exploration radio et l'exploration du réseau câblé pratiquées par le Service de renseignement de la Confédération (SRC)[1]. Avant de présenter cet arrêt (ch. III), quelques remarques concernant l'exploration radio et du réseau câblé s'imposent (ch. II). Nous discuterons ensuite des perspectives de l'exploration, notamment sous l'angle du secret professionnel de l'avocat (ch. IV).

II. L'exploration radio et du réseau câblé

L'exploration radio et du réseau câblé est régie par la loi fédérale du 25.9.2015 sur le renseignement (LRens; RS 121) qui a été acceptée par référendum le 25.9.2016 avec 65,5 % de voix. La loi est entrée en vigueur le 1.9.2017. L'exploration radio (art. 38 LRens) et l'exploration du réseau câblé (art. 39 à 43 LRens) permettent de rechercher des informations sur des événements se produisant à l'étranger. Comme l'explique le Message du 19.2.2014 concernant la loi sur le renseignement, «cette exploration n'est pas axée sur les raccordements de télécommunications des particuliers, mais sur les informations importantes du point de vue de la politique de sûreté issues d'émetteurs radio ou de transmissions du réseau câblé provenant de l'étranger» (ci-après: Message relatif à la LRens)[2]. L'exploration radio couvre l'enregistrement des ondes électromagnétiques émanant de systèmes de télécommunication qui se trouvent à l'étranger (art. 38 al. 1 LRens), tandis que l'exploration du réseau câblé couvre l'enregistrement des signaux transmis par réseau filaire qui traversent la frontière suisse (art. 39 al. 1 LRens), à savoir principalement le trafic Internet.

III. L'ATF 147 I 280

1. En fait

L'association «Société Numérique» et sept personnes, parmi lesquelles un avocat et des journalistes, ont adressé une requête au SRC en 2017. Ils demandaient à ce dernier et au Centre des opérations électroniques de l'armée (COE) de mettre fin aux activités d'exploration radio et du réseau câblé, et de les informer si et de quelle manière leurs communications faisaient ou avaient fait l'objet d'une exploration. Ils demandaient en outre de constater que l'exploration pratiquée par le SRC et le COE portait atteinte à leurs droits fondamentaux. Le SRC a répondu qu'il ne pouvait pas donner suite à leur demande. L'association et les sept particuliers (ci-après: les recourants) ont déposé un recours au Tribunal administratif fédéral (ci-après: TAF). Ce dernier est arrivé à la conclusion que les recourants n'avaient pas droit au traitement matériel de leurs demandes. Le 1.12.2020, le TF a admis leur recours et a renvoyé l'affaire au TAF.

2. En droit

Selon le TF, le droit à un recours effectif au sens de l'art. 13 de la Convention du 4.11.1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH; RS 0.101) peut être limité ou différé lors de mesures de surveillance secrètes aussi longtemps que des intérêts prépondérants justifient le maintien du secret et que le système de surveillance est dans l'ensemble compatible avec l'art. 8 CEDH

* Cette contribution n'engage que son auteur.
1 ATF 147 I 280.
2 FF 2014 2029, 2095.

(consid. 7.1). L'ensemble du système doit pouvoir être examiné au moins une fois par une instance indépendante au niveau national, avant que les personnes concernées puissent saisir la Cour européenne des droits de l'Homme (CourEDH) d'une requête individuelle (consid. 7.2). Pour se prétendre victime d'une violation des droits reconnus dans la CEDH selon l'art. 34 CEDH, il est en principe exigé que l'auteur de la requête soit directement atteint par un acte d'exécution. Il existe des exceptions. Lorsqu'il n'est pas possible ou qu'il ne peut pas être exigé qu'un recours soit formé contre des mesures concrètes, le TF rappelle la jurisprudence de la CourEDH selon laquelle il suffit, pour admettre la «qualité de victime» au sens de l'art. 34 CEDH, de faire l'objet d'une surveillance secrète avec une vraisemblance suffisante (consid. 7.2.2).

En l'espèce, le TF considère que les recourants font valoir de manière soutenable une possible violation de leurs droits fondamentaux garantis par les art. 8 CEDH et 13 Cst. (y compris le droit à l'autodétermination informationnelle). Comme l'exploration radio et du réseau câblé permet de saisir de larges flux de signaux et de données, il existe une vraisemblance suffisante («probabilité raisonnable») que des données des recourants soient concernées par les mesures secrètes en question, raison pour laquelle leur «qualité de victime» selon les art. 13 et 34 CEDH doit en principe être admise (consid. 8.3). Le TF constate que les recourants n'ont pas la possibilité de prendre connaissance des mesures les concernant (consid. 9.2); il est donc indispensable pour eux de pouvoir faire contrôler en Suisse la constitutionnalité et la conformité avec la CEDH du système d'exploration radio et du réseau câblé (consid. 9.3).

Le TF précise que cet examen ne constitue pas un contrôle abstrait des normes. Il ne porte pas sur la loi en tant que telle, mais sur la saisie présumée des données des recourants dans le cadre de l'exploration radio et du réseau câblé. La question est de savoir si le traitement (présumé) des données des recourants viole leurs droits fondamentaux. Il ajoute à cet égard qu'il convient de prendre en considération non seulement les bases légales, mais aussi les éventuelles directives et instructions internes, la pratique effective du SRC et du COE, et les contrôles effectivement effectués par les autorités de surveillance (consid. 9.3).

Certaines restrictions de la protection juridique en cas de mesures de surveillance secrètes sont admissibles; cela suppose toutefois que le système dans son ensemble soit conforme aux exigences des art. 8 CEDH et 13 Cst. (consid. 9.4).

3. Commentaire

Malgré son importance, cet arrêt a été très peu discuté par la doctrine. AXEL TSCHENTSCHER relève que cette décision est un premier pas pour combler le manque de protection face à la pratique du SRC[3]. MAYA HERTIG RANDALL et JULIEN MARQUIS considèrent que cette jurisprudence est «pleinement justifiée, puisqu'elle constitue la seule possibilité d'éviter que la protection conventionnelle de la sphère privée ne se trouve vidée de sa substance»[4]. De notre point de vue, la solution retenue par le TF doit être saluée. Le TAF devra examiner si le traitement des données des recourants dans le système de l'exploration radio et du réseau câblé est conforme à la CEDH. Qu'adviendrait-il si le TAF arrivait à la conclusion que ce n'est pas le cas? Le considérant 10.1 de l'arrêt du TF 1C_377/2019, non publié à l'ATF 147 I 280, apporte un élément de réponse. Il précise, en ce qui concerne la demande des recourants tendant à mettre fin aux activités d'exploration, que leur intérêt digne de protection se limite à la protection de leurs propres données et, s'agissant des journalistes et de l'avocat concernés, éventuellement des données de leurs sources et de leur clientèle. Le TF ajoute que la question se pose de savoir s'il est techniquement possible d'exclure les données de certaines personnes de l'exploration. Cela semble douteux d'après lui, en raison de la grande quantité de données extraites et fouillées, et du fait qu'elles ne sont attribuées à des personnes déterminées que dans une phase tardive. Il en conclut ainsi qu'il ne peut pas d'emblée être exclu que la suspension de l'exploration puisse être le seul moyen d'assurer une protection efficace des droits fondamentaux des recourants.

IV. Les perspectives

1. Rôle et importance du secret professionnel de l'avocat

Le secret professionnel de l'avocat protège d'abord un intérêt privé, celui du client. Il est en effet institué pour inspirer au justiciable une confiance absolue en la discrétion de son défenseur. Il protège ensuite un intérêt public, à savoir la protection de l'ordre juridique et de l'accès à la justice[5]. Il n'a en revanche pas pour fonction de protéger les intérêts de l'avocat. Il n'est en effet pas destiné à le protéger des conséquences de ses propres erreurs, ce qui signifie qu'il doit en principe s'effacer lorsque c'est l'avocat lui-même qui fait l'objet d'une procédure judiciaire[6]. Il convient également de garder à l'esprit que seules les activités typiques de l'avocat sont protégées par le secret[7].

Dans sa mission, l'avocat est susceptible de représenter des mandants dont les intérêts sont opposés à l'État: des lanceurs d'alerte, des terroristes ou encore des gouvernements étrangers dans des affaires sensibles. Ainsi, une surveillance de masse, sans motif, secrète, insuffisamment encadrée, mettrait en péril le secret professionnel de l'avocat, compromettrait sa mission, et remettrait en question les fondements de l'État de droit.

3 AXEL TSCHENTSCHER, in: ZBJV 157/2021 p. 565, 580–581.
4 MAYA HERTIG RANDALL/JULIEN MARQUIS, in: MARTENET/DUBEY (édit.), *Commentaire romand de la Constitution fédérale*, 2021, N 58 ad art. 13 Cst.
5 BENOÎT CHAPPUIS/JÉRÔME GURTNER, *La profession d'avocat*, 2021, N 664 ss.
6 *Idem*, N 855 ss.
7 *Idem*, N 96 ss.

Les communications entre un avocat et son client sont protégées par l'art. 8 par. 1 CEDH, qui dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. La relation entre cette disposition et le secret professionnel de l'avocat n'est pas évidente à cerner, et rarement abordée. Dans l'affaire *Michaud c. France,* la CourEDH a apporté une précision importante à ce sujet[8]: l'art. 8 CEDH accorde une «protection renforcée» aux échanges entre les avocats et leurs clients.

Les droits conférés à l'art. 8 CEDH ne sont pas absolus. Selon l'art. 8 par. 2 CEDH, une ingérence dans les droits garantis par cette disposition ne peut se justifier que si elle est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

L'avocat peut enfin se prévaloir de l'art. 6 CEDH. Dans l'affaire *Kadura et Smaliy c. Ukraine,* la CourEDH a retenu qu'une atteinte au secret professionnel des avocats peut avoir des répercussions sur la bonne administration de la justice et sur les droits garantis par l'art. 6 CEDH, ajoutant que les autorités doivent avoir une raison impérieuse pour s'immiscer dans le secret des communications d'un avocat ou dans ses documents de travail[9].

2. Étapes du processus de l'interception en masse et cadre juridique selon la CourEDH

Dans l'affaire *Centrum för rättvisa c. Suède,* la CourEDH a relevé que le recours à un régime d'interception en masse, afin de repérer les menaces pesant sur la sécurité nationale ou sur des intérêts nationaux essentiels est une décision qui relève de la marge d'appréciation des États[10]. Elle a ensuite jugé que l'interception en masse est «un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmente au fur et à mesure que le processus avance»[11].

Les différentes étapes du processus d'interception en masse (qui peuvent varier d'un régime à l'autre) peuvent être décrites comme suit[12]:

a) interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées);
b) application de sélecteurs spécifiques aux communications retenues et aux données de communication associées;
c) examen par des analystes des communications sélectionnées et des données de communication associées; et
d) rétention subséquente des données et utilisation du «produit final», notamment partage de ces données avec des tiers.

Selon la CourEDH, le contrôle et la supervision des mesures de surveillance secrète peuvent intervenir à trois stades: lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé[13]. Afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, elle a retenu que le processus doit être «encadré par des ‹garanties de bout en bout›, c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*»[14].

Enfin, toujours selon la CourEDH, les États doivent rechercher si le cadre juridique national définit clairement[15]:

1. les motifs pour lesquels l'interception en masse peut être autorisée;
2. les circonstances dans lesquelles les communications d'un individu peuvent être interceptées;
3. la procédure d'octroi d'une autorisation;
4. les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés;
5. les précautions à prendre pour la communication de ces éléments à d'autres parties;
6. les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits;
7. les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement;
8. les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

C'est en principe à l'aune des critères précités que le système de l'exploration radio et du réseau câblé devra être examiné par le TAF.

3. Présentation et discussion du système de l'exploration

Les lois sur le renseignement établissent souvent des régimes juridiques différents pour la surveillance intérieure et extérieure. Alors que la première fait l'objet d'un plus grand contrôle et de garanties procédurales plus solides, la seconde ne bénéficie que de peu, voire d'aucune protec-

8 Arrêt de la CourEDH *Michaud c. France* du 6. 12. 2012, N 118 et 119.
9 Arrêt de la CourEDH *Kadura et Smaliy c. Ukraine* du 21. 1. 2021, N 142 et les réf. cit.
10 Arrêt de la CourEDH *Centrum för rättvisa c. Suède* du 25. 5. 2021, N 254 et 261.
11 *Idem*, N 239.
12 *Idem*, N 239.
13 *Idem*, N 250.
14 *Idem*, N 264.
15 *Idem*, N 275.

tion[16]. La Suisse n'a pas dérogé à cette règle. L'exploration radio et du réseau câblé est régie par la section 6 du chapitre 3 de la LRens intitulée «Recherche d'informations sur des événements se produisant à l'étranger». Les mandats d'exploration radio ne sont soumis à aucune autorisation. L'exploration radio et du réseau câblé (art. 36 à 43 LRens) ne prévoit aucune obligation d'informer *a posteriori* les personnes surveillées, contrairement aux mesures de recherche soumises à autorisation au sens de l'art. 26 LRens (art. 33 LRens). Le Message relatif à la LRens justifie ce choix en raison du fait «que cette exploration n'est pas axée sur les raccordements de télécommunications des particuliers, mais sur les informations importantes du point de vue de la politique de sûreté issues d'émetteurs radio ou de transmissions du réseau câblé provenant de l'étranger», ajoutant que «ce ne sont pas les personnes ou leur vaste trafic de télécommunications qui sont le but de la recherche d'informations»[17]. La loi prévoit certaines restrictions. Dans le cadre de l'exploration du réseau câblé, si tant l'émetteur que le récepteur se trouvent en Suisse, il est interdit d'utiliser les signaux enregistrés en vertu de l'art. 39 al. 1 LRens (art. 39 al. 2 LRens). Il est en outre interdit d'utiliser des indications relatives à des ressortissants ou à des personnes morales suisses comme mots-clés de recherche (art. 39 al. 3 LRens). Les mandats d'exploration du réseau câblé sont soumis à l'autorisation du TAF et l'aval du chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS) (art. 40 al. 1 et 2 LRens). Dans le cadre de sa mise en œuvre, le service chargé de l'exploration du réseau câblé ne transmet au SRC des informations relatives à des personnes qui se trouvent en Suisse que si elles sont nécessaires à la compréhension d'un événement se produisant à l'étranger et qu'elles ont été anonymisées (art. 42 al. 2 LRens). Cette règle connaît toutefois une exception: lorsque les données contiennent des informations sur des événements se produisant en Suisse ou à l'étranger qui peuvent constituer une menace concrète pour la sûreté intérieure au sens de l'art. 6 al. 1 let. a LRens, le service chargé de l'exploration du réseau câblé les transmet telles quelles au SRC (art. 42 al. 3 LRens). Il existe un organe de contrôle indépendant, interne à l'administration, pour l'exploration radio et du réseau câblé (ci-après: OCI) (art. 79 LRens). Ses activités sont définies à l'art. 10 de l'ordonnance sur la surveillance des activités de renseignement (OSRens; RS 121.3). Quelques remarques s'imposent.

D'abord, pour faire échec à l'interdiction prévue à l'art. 39 al. 2 LRens, il suffit que l'émetteur ou le récepteur se trouve à l'étranger, ce qui n'est pas rare dans le cadre de communications[18]. Par ailleurs, dans le cadre des communications par câble, à savoir principalement le trafic Internet, la distinction entre les communications en Suisse et à l'étranger n'a guère de sens, lorsque l'on sait qu'une communication entre deux personnes, dans la même ville, peut faire le tour du monde avant d'atteindre son destinataire[19]. Ainsi, en raison du mélange des communications intérieures et extérieures et des difficultés techniques de les distinguer, des communications entre des personnes se trouvant en Suisse seront interceptées par le COE[20]. Malgré le texte de l'art. 39 al. 2 LRens, la loi n'exclut pas que de telles données soient transmises au SRC lorsque les conditions prévues aux art. 42 al. 2 ou 3 LRens sont remplies. Enfin, l'application de règles différentes pour la surveillance intérieure et extérieure est discutable et mériterait de faire l'objet d'un examen plus poussé. Dans un arrêt du 19. 5. 2020, la Cour constitutionnelle fédérale allemande a jugé que le Service fédéral du renseignement allemand est lié par les droits fondamentaux garantis par la loi fondamentale («Grundgesetz») lorsqu'il procède à la surveillance des télécommunications passées par des étrangers se trouvant hors du territoire allemand[21]. Cette solution est justifiée: on ne comprendrait pas que les droits de l'homme, réputés universels, s'arrêtent à la frontière d'un pays. Il serait p. ex. choquant que le secret professionnel de l'avocat dont l'art. 8 CEDH accorde une «protection renforcée» (cf. ch. IV. 1 *supra*) soit ignoré, au motif qu'un avocat se trouve à l'étranger, étant précisé qu'un avocat suisse peut également être concerné lorsqu'il envoie un message à un destinataire en Suisse depuis l'étranger.

4. *Protection du secret professionnel de l'avocat dans la LRens et l'ORens*

La LRens et l'ordonnance du 16. 8. 2017 sur le Service de renseignement (ORens; RS 121.1) prévoient quelques dispositions concernant la protection de secrets professionnels. L'art. 23 ORens dispose que si une personne appartenant à l'un des groupes professionnels mentionnés aux art. 171 à 173 du code de procédure pénale est surveillée en vertu de l'art. 27 LRens, il convient de s'assurer que le SRC n'entre pas en possession d'informations liées à un secret professionnel et sans relation avec le motif de la surveillance, étant précisé que le SRC signale dans la procédure d'autorisation au sens de l'art. 29 LRens que les informations doivent être triées conformément à l'art. 58 al. 3 LRens. Selon la disposition précitée, les données qui ne présentent aucun lien spécifique avec la menace justifiant la décision doivent être triées et détruites sous la direction du TAF si la mesure de recherche soumise à autorisation concerne une personne qui relève de l'une des catégories professionnelles citées aux art. 171 à 173 CPP, étant précisé que si cette mesure concerne d'autres personnes, les données au sujet desquelles une personne citée aux art. 171 à 173 CPP pourrait refuser de témoigner doivent elles aussi être détruites. Cependant, l'art. 58 al. 4 LRens prévoit encore que le SRC peut, dans un cas particulier et en tenant compte de l'art. 5 al. 5 à 8 LRens, verser au surplus des données personnelles dans le système d'information prévu à cet effet à l'art. 47 al. 1 LRens, si ces données contiennent des informations dont il a besoin pour accomplir des tâches visées à l'art. 6 al. 1 LRens.

D'un point de vue systématique, les art. 58 LRens et 23 ORens s'appliquent aux mesures de recherche soumises à autorisation (chapitre 4, section 3 de la LRens; chapitre 2, section 3 de l'ORens). Ils ne devraient ainsi en principe pas s'appliquer à l'exploration radio qui n'est soumise à aucune autorisation. Il devrait en aller de même pour l'exploration du réseau câblé, qui est certes soumise à une procédure d'autorisation (art. 41 LRens), mais qui n'est pas conçue comme une mesure de recherche soumise à autorisation au sens de l'art. 26 LRens. L'art. 58 al. 1 LRens se réfère en effet aux données provenant d'une mesure de recherche soumise à autorisation au sens de l'art. 26 LRens, alors que la disposition précitée n'est pas applicable à la procédure d'autorisation dans le cadre de l'exploration du réseau câblé (art. 41 al. 2 LRens qui renvoie aux art. 29 à 32 LRens). Certes, l'art. 36 al. 5 LRens précise que le SRC peut enregistrer dans des systèmes d'information distincts des données provenant de l'étranger comparables à celles obtenues par des mesures de recherche d'informations soumises à autorisation lorsque l'ampleur des données, le secret ou la sécurité le requièrent. Il ne ressort cependant pas de cette disposition, non contraignante, comme l'indique l'utilisation du mot «peut», que l'art. 58 LRens serait applicable à l'exploration radio et du réseau câblé, même par analogie. Les art. 58 LRens et 23 ORens ne sont ainsi en principe pas applicables à l'exploration radio et du réseau câblé. Le même constat s'impose en ce qui concerne l'art. 28 al. 2 LRens. Même si ces dispositions ne sont *a priori* pas adaptées à des interceptions non ciblées, comme le permet l'exploration, il s'agit d'une importante lacune. En effet, le secret professionnel de l'avocat doit également être protégé dans le cadre de l'exploration radio et du réseau câblé (cf. ch. IV. 5, 3e remarque *infra*). Cette protection doit inclure les données couvertes par le secret des avocats et de leurs clients, que ces derniers se trouvent en Suisse ou à l'étranger.

5. *Identification de quelques faiblesses et recommandations*

Sur la base des informations librement accessibles, nous avons identifié, de manière non exhaustive, les faiblesses suivantes et formulé quelques recommandations.

Premièrement, les mandats d'exploration radio, contrairement aux mandats d'exploration du réseau câblé, ne sont soumis à aucune autorisation initiale par un organe de contrôle indépendant, ce qui représente une importante faiblesse pour une mesure de surveillance secrète. À notre avis, des garanties similaires devraient s'appliquer à l'exploration radio et à l'exploration du réseau câblé.

Deuxièmement, les mandats d'exploration du réseau câblé sont soumis à l'autorisation du TAF et l'aval du chef du DDPS. Si cette autorisation représente une garantie importante, elle ne permet pas, à elle seule et dans le cadre d'une interception non ciblée, d'éviter que des communications protégées par le secret professionnel de l'avocat soient interceptées, notamment par inadvertance. Un contrôle judiciaire initial ne permet pas d'éviter tous les abus. Le processus doit être encadré par des garanties de bout en bout (cf. ch. IV. 2 *supra*). C'est après le contrôle judiciaire initial, soit pendant et après la phase d'interception, que du contenu protégé par le secret professionnel de l'avocat pourra être examiné. Dans l'affaire *Big Brother Watch et autres c. Royaume-Uni,* le Juge Paulo Pinto de Albuquerque, dans une opinion séparée, avait relevé, à juste titre, ce qui suit: «Le contrôle judiciaire ne doit pas s'arrêter à la phase initiale du processus d'interception. Si le fonctionnement réel du système d'interception était caché au juge, l'intervention initiale de celui-ci pourrait être aisément mise à mal et privée de tout effet utile, ce qui en ferait une garantie virtuelle et illusoire. Le juge doit au contraire encadrer l'ensemble du processus en examinant de manière régulière et vigilante la nécessité et la proportionnalité du mandat d'interception, au regard des données qui ont été interceptées. Faute de recevoir en permanence des remontées d'information de la part de l'autorité interceptrice, le juge qui a délivré l'autorisation ne peut pas savoir comment celle-ci est utilisée en pratique»[22]. En Suisse, le contrôle ultérieur n'est pas effectué par un organe judiciaire, comme le TAF, mais par l'OCI, ce qui n'est *a priori* pas exclu par la CourEDH. Cet organe doit être indépendant et «investi de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent»[23]. À cet égard, la loi ne prévoit aucune règle exigeant de l'OCI qu'il vérifie si le COE et le SRC traitent des informations protégées par le secret professionnel de l'avocat. D'une manière générale, les vérifications effectuées par l'OCI mentionnées à l'art. 10 al. 1 OSRens sont très vagues et non contraignantes («l'OCI *peut* [...] procéder aux vérifications [...]»). En revanche, la vérification de l'exécution des mandats d'exploration du réseau câblé dans les six mois qui suivent le début de l'exploration, voire au moins une fois par année (art. 10 al 2 OSRens), semble obligatoire («il contrôle [...]»), mais demeure insuffisante si aucun contrôle plus régulier n'est effectué. Les investigations et les recomman-

16 ASAF LUBIN, *«We Only Spy on Foreigners»: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,* in: Chicago Journal of International Law, Vol. 18, N° 2, Article 3, 2018, p. 507.

17 FF 2014 2029, 2095.

18 Lors de l'audience publique dans l'affaire *Big Brother Watch et autres c. Royaume-Uni* (requêtes nos 58170/13, 62322/14 et 24960/15), le Juge Paulo Pinto de Albuquerque avait demandé au Gouvernement britannique s'il pouvait garantir qu'un message confidentiel envoyé par la CourEDH à un avocat à Londres ne serait pas intercepté par les services de renseignement britannique, question à laquelle le Gouvernement avait répondu par la négative.

19 Privacy International, How Bulk Interception Works, le 30. 9. 2016, disponible sur: https://privacyinternational.org/long-read/827/how-bulk-interception-works.

20 Dans ce sens également: TANIA CHENAUX, *L'exploration du réseau câblé (art. 39 ss LRens): analyse à la lumière de l'art. 13 Cst.*, in: QFLR 2/16 p. 12–14, p. 12 et 13 et les réf. cit. En ce qui concerne l'exploration radio, cf. FF 2014 2029, 2101.

21 *Bundesverfassungsgerichts,* arrêt du 19. 5. 2020, 1 BvR 2835/17.

22 Arrêt de la CourEDH *Big Brother Watch et autres c. Royaume-Uni* du 25. 5. 2021, opinions séparées, N 26.

23 Arrêt de la CourEDH *Roman Zakharov c. Russie* du 4. 12. 2015, N 275 et la réf. cit.

dations de l'OCI devraient être documentées et rendues publiques, au moins de manière résumée, ce qui n'est pas le cas (art. 10 al. 3 OSRens *a contrario*). Enfin, l'OCI n'est pas compétent pour mettre un terme à une mission d'exploration par câble (art. 79 al. 3 LRens *a contrario*), alors qu'il est compétent pour analyser les résultats obtenus (art. 10 al. 1 let. d OSRens). Une question de coordination se pose donc entre le TAF et l'OCI, qui n'est pas réglée dans la loi, étant précisé qu'un organe de contrôle doit être compétent pour mettre un terme à une telle mission,[2] et que des recommandations formulées à la fin d'un mandat ne sont pas suffisantes (art. 79 al. 3 LRens).

Troisièmement, le secret professionnel de l'avocat doit être protégé dans le cadre de l'exploration radio et du réseau câblé. La principale difficulté réside dans le fait que des communications protégées par le secret professionnel seront interceptées, notamment par inadvertance. Au Royaume-Uni, l'*Investigatory Powers Act* de 2016 (ci-après: IPA) et le Code de conduite concernant l'interception des communications (ci-après: le Code de conduite; version 3.2018) prévoient certaines règles à ce sujet (art. 55 et 153 IPA, ainsi que par. 9.59 à 9.73 du Code de conduite). Nous pouvons nous en inspirer et les adapter pour formuler la proposition suivante. Le COE ou le SRC devrait rapidement identifier les informations protégées par le secret professionnel de l'avocat qu'il traite. Une fois identifiées, elles devraient être marquées en tant que telles, isolées et leur accès restreint. Une autorité indépendante, qui pourrait être le TAF ou l'OCI, devrait être informée de leur existence. À ce stade, elles ne devraient être conservées que pour être supprimées dans un délai raisonnable, avec confirmation de leur suppression notifiée au TAF ou à l'OCI. Exceptionnellement, si ces informations n'étaient pas supprimées dans le délai fixé, une autorité indépendante devrait autoriser leur conservation ou leur utilisation à la condition suivante: l'intérêt public à conserver ces éléments devrait l'emporter sur l'intérêt privé et public à préserver leur confidentialité, et leur conservation devrait être nécessaire dans l'intérêt de la sécurité nationale ou dans le but de prévenir la mort ou un préjudice important. Cet examen, qui implique une pesée des intérêts délicate, devrait être confié à une autorité judiciaire, dans l'idéal au TAF. Compte tenu de l'importance du secret professionnel de l'avocat (cf. ch. IV. 1 *supra*), il s'agit de garanties minimales. Enfin, il est clair que les données protégées par un secret professionnel et destinées à être détruites pour ce motif ne sauraient être proposées par le SRC aux Archives fédérales aux fins d'archivages, l'art. 68 LRens prévoyant notamment pour les données archivées un délai de protection de 50 ans durant lequel le SRC peut les consulter. Si le secret professionnel de l'avocat n'est pas suffisamment protégé, c'est l'ensemble du système de l'exploration qui pourrait être remis en question (cf. ch. III. 3 *supra*).