Illicéité de la surveillance par exploration du réseau câblé

Marc Løebekken, le 29 janvier 2026

Le TAF considère que le régime de surveillance par exploration du réseau câblé opéré par le service de renseignement de la Confédération n'offre pas des garanties juridiques suffisantes pour protéger les droits fondamentaux et doit être revu.

ATAF A-6444/2020, du 19 novembre 2025

Nota bene : La présente contribution fait partie d'une série de deux contributions consacrées à l'arrêt du TAF A-6444/2024 rendu le 19 novembre 2025 concernant l'illicéité de la surveillance par exploration du réseau câblé (cf. swissprivacy.law/392 pour un état des lieux de la surveillance de masse, en comparant cette décision à l'ATF 144 I 126 rendu en 2018). Cette première contribution vise à analyser l'arrêt du TAF et son impact.

Contexte

La Suisse, comme de nombreux autres États, s'efforce d'adopter des normes afin de lutter efficacement contre les menaces à la sécurité nationale et internationale. Dans ce contexte, différentes formes de surveillance des communications à grande échelle ont été instituées par la loi, allant de la rétention de données (*Vorratsdatenspeicherung*), qui consiste à requérir des fournisseurs de services électroniques de conserver des métadonnées de communications pour une durée déterminée (encadrée par la Loi sur la Surveillance de la correspondance par poste et télécommunication ; LSCPT), jusqu'à la surveillance par exploration du réseau câblé (*Kabelaufklärung*), qui implique l'interception en masse des communications transfrontalières (encadrée par la Loi sur le renseignement ; LRens). Ces mesures doivent être conciliées avec les droits fondamentaux à la vie privée, au secret des communications et à une protection effective contre les abus garantis par la Constitution fédérale suisse et la Convention européenne des droits de l'homme (CEDH). Si ces deux types de surveillance ont été le sujet de nombreuses critiques depuis la révision du cadre juridique LSCPT/LRens (entrée en force en 2018), c'est l'exploration du réseau câblé qui a récemment fait l'objet d'un arrêt de principe du TAF.

Qu'est-ce que la surveillance par exploration du réseau câblé

La surveillance par exploration du réseau câblé fait référence aux activités menées par le Service de renseignement fédéral (SRC) visant à capter et analyser des communications électroniques qui transitent par des câbles ou par voie hertzienne à des fins de renseignement en application de la Section 7 de la LRens. Dans sa forme actuelle, ce système permet la capture de vastes flux de données de communication transfrontalière, en se fondant sur des paramètres de recherche pour identifier des communications potentiellement pertinentes pour la sécurité nationale.

Bien que les mandats d'exploration du réseau câblé soient soumis à l'autorisation du TAF, ce type de surveillance s'apparente à ce que l'on appelle souvent l'interception de masse (*bulk interception*), dans laquelle de larges volumes de trafic sont saisis sans qu'il existe nécessairement de soupçon concret à l'égard d'une personne déterminée. Les contenus captés et analysés peuvent potentiellement inclure des données privées de personnes qui ne sont pas suspectées de participer à une activité répréhensible. La surveillance couvre notamment les communications dites « transfrontalières » (même si l'expéditeur et le destinataire sont en Suisse, leur trafic peut transiter par des réseaux étrangers), ce qui fait que des données personnelles de citoyens et résidents ordinaires peuvent être interceptées sans lien direct avec un soupçon individuel.

L'invalidation de la surveillance par exploration du réseau câblé (A-6444/2020)

Dans son arrêt A-6444/2020, le TAF s'est prononcé pour la première fois de manière approfondie sur la compatibilité de la surveillance par exploration du réseau câblé avec les droits fondamentaux. L'affaire portait non pas sur un cas individuel de surveillance mais sur la légalité structurelle du système lui-même, tel qu'il est prévu par la LRens et mis en œuvre en pratique. L'arrêt conclut une longue procédure initiée en 2017 par la Société Numérique (*Digitale Gesellschaft*).

Dans son analyse, le TAF ne nie pas que la surveillance du trafic transfrontalier puisse, en principe, poursuivre un objectif légitime de sécurité nationale. Le cœur du litige porte sur la question de savoir si le cadre légal et les mécanismes de contrôle entourant cette surveillance satisfont aux exigences constitutionnelles (art. 13 Cst.) et conventionnelles (art. 8 CEDH).

Analyse juridique à l'aune des huit critères de la CEDH

Le TAF procède à une évaluation systématique du régime suisse de surveillance du réseau câblé à l'aune des huit critères dégagés par la Grande Chambre de la CEDH dans les arrêts

Big Brother Watch et *Centrum för rättvisa*. Cette grille d'analyse vise à déterminer si le système comporte, dans son ensemble, des garanties « de bout en bout » suffisantes contre les abus.

S'agissant d'abord des motifs pour lesquels une surveillance de masse peut être autorisée, le TAF considère que le droit suisse, bien que formulé de manière relativement ouverte, définit de façon suffisamment prévisible les finalités poursuivies. La surveillance par câble vise l'obtention d'informations sur des événements importants pour la politique de sécurité extérieure, notamment en lien avec le terrorisme, la prolifération des armes de destruction massive ou d'autres menaces graves. Ces buts relèvent des intérêts légitimes reconnus par les art. 8 par. 2 et 10 par. 2 CEDH. Le TAF admet ainsi que, sur ce premier point, l'atteinte aux droits fondamentaux peut être justifiée en principe.

Concernant ensuite les circonstances dans lesquelles des communications peuvent être surveillées, le TAF estime que le cadre légal fournit des balises suffisantes. La surveillance est formellement limitée aux flux transfrontaliers, et la loi interdit l'utilisation de communications purement internes à la Suisse. Même si le TAF reconnaît qu'il n'est pas toujours techniquement possible d'exclure ces communications au stade de la captation, il attache une importance particulière à l'interdiction d'utilisation et à la séparation organisationnelle entre l'entité chargée de la collecte technique et celle responsable de l'exploitation du renseignement. Sur ce point également, le régime est jugé globalement compatible avec les exigences de prévisibilité.

La situation est plus nuancée en ce qui concerne la procédure d'autorisation préalable. Le TAF relève positivement que les mandats de surveillance par câble sont soumis à l'autorisation d'un tribunal indépendant (en l'occurrence, le TAF lui-même), ce qui constitue une garantie centrale. Toutefois, il identifie des lacunes importantes, notamment en lien avec certaines formes de surveillance et avec l'utilisation de termes de recherche particulièrement précis, qui ne sont pas toujours soumis à un contrôle préalable suffisamment strict. Le critère de l'autorisation indépendante n'est ainsi rempli que partiellement.

En revanche, le TAF adopte une appréciation nettement critique des procédures de sélection, d'évaluation et d'utilisation des données interceptées. Il constate l'absence d'obligation d'implémenter en permanence les capacités techniques visant à exclure les communications purement suisses, le manque de garanties assurant que seules des données pertinentes et exactes sont traitées, ainsi qu'une traçabilité et une documentation incomplètes des différentes étapes du traitement. De plus, la possibilité de recherches rétrospectives n'apparaît

pas suffisamment prévisible au regard du cadre légal.

S'agissant des précautions à prendre lors de la transmission des informations à d'autres parties, notamment à des États étrangers ou à des organisations internationales, le TAF se réfère aux exigences élevées posées par la jurisprudence européenne. Il estime que le droit suisse ne structure pas de manière suffisamment précise et contraignante les conditions et les garanties entourant ces transmissions, en particulier en ce qui concerne la prévention des usages abusifs ultérieurs.

En ce qui concerne les limites relatives à la durée de conservation et à la destruction des données, le TAF relève l'existence de règles formelles prévoyant des délais et des obligations d'effacement. Toutefois, replacées dans le contexte d'une collecte massive, de possibilités de recherches rétrospectives et d'un contrôle imparfait des traitements, ces règles ne suffisent pas, selon le TAF, à assurer une protection effective contre les atteintes disproportionnées. Les garanties apparaissent ainsi fragilisées dans le fonctionnement global du système.

Le TAF se montre également critique quant à la supervision indépendante continue du système. S'il reconnaît l'existence d'organes de contrôle, il estime que ceux-ci ne disposent pas de moyens suffisants pour assurer une surveillance fine, technique et permanente de l'ensemble de la chaîne de traitement. L'absence d'une traçabilité exhaustive et de contrôles approfondis affaiblit le rôle de ces mécanismes institutionnels, qui ne compensent pas les lacunes structurelles identifiées.

Enfin, s'agissant de la possibilité de recours effectif pour les personnes concernées, le constat du TAF est clairement négatif. Le système d'information différée et de recours indirect ne permet pas, en pratique, un contrôle *a posteriori* effectif de la légalité de la surveillance. Les individus concernés n'ont que très rarement la possibilité de savoir si leurs communications ont été traitées et de faire valoir leurs droits devant une instance indépendante. Cette insuffisance constitue un élément déterminant dans l'appréciation globale.

Conséquences juridiques

Pour ces raisons, le TAF a conclu que la surveillance du réseau câblé telle qu'exercée ne dispose pas des garanties nécessaires et doit être adaptée. Il a toutefois accordé au législateur un délai de cinq ans pour remédier aux lacunes légales avant que la pratique ne doive être stoppée. Plus récemment, le SRC a annoncé renoncer à un recours contre le jugement et œuvrer à l'adaptation du cadre juridique dans le cadre de la refonte du « paquet de base » de la LRens, comprenant notamment les dispositions relatives aux mesures de recherche, à la

conservation des données et à la surveillance. Des développements sont attendus courant 2026.

Proposition de citation : Marc L□EBEKKEN, Illicéité de la surveillance par exploration du réseau câblé, 29 janvier 2026 *in* www.swissprivacy.law/391

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.