_swissprivacy.law

État des lieux de la surveillance de masse

Marc Løebekken, le 29 janvier 2026

La récente décision du TAF rendue sur la question spécifique de l'exploration du réseau câblé, prend le contrepied d'une décision antérieure du TF sur un autre régime de surveillance de masse : la rétention indiscriminée des métadonnées.

ATF 144 I 126, du 2 mars 2018

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/391 pour une analyse de l'arrêt au fond). Cette deuxième contribution vise à faire un état des lieux de la surveillance de masse, en revenant sur l'ATF 144 I 126.

La validation de la rétention indiscriminée des métadonnées (1C-598/2016)

Par le passé, dans l'arrêt 1C_598/2016 du 2 mars 2018, le TF a examiné une action constitutionnelle (également menée par la Société Numérique) contre la rétention indiscriminée des métadonnées par les fournisseurs de service électronique sous l'ancienne Loi sur la Surveillance de la correspondance par poste et télécommunication ; LSCPT (alors en révision). La procédure faisait suite à un recours dirigé contre l'obligation imposée aux fournisseurs de services de conserver, pendant une durée déterminée, certaines données de trafic et de localisation relatives aux communications électroniques.

La question centrale était de savoir si l'obligation généralisée de conserver des métadonnées affectant l'ensemble des utilisateurs concernés constituait une violation inadmissible des droits fondamentaux, en particulier du droit au respect de la vie privée et à la protection contre l'utilisation abusive des données personnelles (art. 13 Cst.). Les données en cause incluaient notamment les informations relatives aux connexions (adresses IP, numéros appelés, date, heure et durée des communications, données de localisation approximative), mais pas le contenu des communications.

Dans l'arrêt 1C_598/2016, le TF a reconnu explicitement que la conservation généralisée des données secondaires de télécommunication constituait une ingérence dans la sphère privée

et dans le droit à l'autodétermination informationnelle garanti par l'art. 13 Cst. Il a admis que ces données, bien qu'elles ne portent pas sur le contenu des communications, permettent néanmoins de tirer des conclusions sur les habitudes de vie, les contacts sociaux et l'environnement personnel des individus, et qu'elles peuvent être combinées pour établir des profils de personnalité. Le TF ne niait donc pas la portée intrusive du mécanisme, mais en proposait une appréciation nuancée quant à son intensité.

Il a considéré en particulier que l'ingérence était d'une nature différente et moins grave que celle résultant de la surveillance du contenu des communications. En se référant à sa propre jurisprudence ainsi qu'à celle de la CEDH, il a opéré une distinction entre données de contenu et données périphériques, ces dernières étant perçues comme révélant indirectement des informations sensibles, mais ne donnant pas accès immédiat aux échanges eux-mêmes. Cette distinction a joué un rôle central dans l'évaluation de la proportionnalité.

S'agissant de la base légale, le TF a estimé que la LSCPT définissait de manière suffisamment précise l'obligation de conservation, en particulier quant aux catégories de données concernées et à la durée de conservation de six mois. Il a souligné que cette obligation reposait sur une réglementation formelle adoptée par le législateur fédéral et complétée par des dispositions d'exécution, ce qui satisfaisait aux exigences de légalité et de prévisibilité.

L'élément déterminant du raisonnement du TF a résidé toutefois dans l'importance accordée aux garanties procédurales entourant l'accès aux données. Le TF mettait en avant le fait que les autorités de poursuite pénale ne disposaient d'aucun accès direct et libre aux données conservées par les fournisseurs. L'obtention de ces informations supposait la mise en œuvre des mécanismes de surveillance prévus par le Code de procédure pénale, notamment l'art. 273 CPP, qui exige l'existence d'un soupçon grave, le respect du principe de proportionnalité et l'autorisation d'un tribunal indépendant. Il relevait également que les mesures de surveillance devaient être motivées, limitées dans le temps, contrôlées par le tribunal des mesures de contrainte et, en principe, notifiées ultérieurement aux personnes concernées, lesquelles disposaient de voies de recours. Ces mécanismes ont été considérés comme des freins institutionnels significatifs aux abus.

Enfin, le TF a souligné que le législateur avait prévu des mesures de sécurité techniques et organisationnelles imposées aux fournisseurs de services de télécommunication. Ceux-ci sont tenus de conserver les données de manière sécurisée, de les effacer irrévocablement à l'expiration du délai légal, et de mettre en œuvre des mécanismes destinés à prévenir les accès non autorisés. Le TF a considéré que ces obligations de protection des données

faisaient partie intégrante du dispositif légal et contribuaient à réduire les risques d'abus ou de détournement, participant ainsi à l'appréciation globale de la proportionnalité.

Sur cette base, le TF a conclu que, malgré son caractère généralisé et préventif, la rétention de métadonnées reposait sur une base légale suffisante, poursuivait un intérêt public important lié à la poursuite des infractions graves, et était entourée de garanties jugées aptes à contenir l'atteinte aux droits fondamentaux dans des limites admissibles. La Société Numérique a recouru contre l'arrêt auprès de la CEDH et le recours est actuellement pendant (Glättli et al. Contre Suisse).

Critique de l'écart entre les décisions

La divergence entre l'arrêt du TAF sur la surveillance du réseau câblé et le jugement du TF sur la rétention des métadonnées soulève des critiques importantes, car bon nombre des défauts structurels et des risques d'atteinte aux droits fondamentaux identifiés dans l'arrêt A-6444/2020 sont également présents dans le régime de rétention indiscriminée des métadonnées, toujours existant dans l'actuelle LSCPT, mais n'ont pas conduit à une invalidation similaire du de ce régime lorsqu'analysé en 2018 par le TF.

Similitude des ingérences

Les deux régimes impliquent une surveillance massive et préventive sans lien avec un soupçon individuel : la rétention indiscriminée des métadonnées capture des informations sur toutes les personnes concernées pendant une période prolongée, tandis que la surveillance par câble capture des flux entiers de communication. Dans le cas de la rétention indiscriminée de métadonnées, l'État dispose de grandes quantités de données personnelles sans qu'une autorisation préalable indépendante ne soit requise au moment de la collecte initiale par les fournisseurs.

Garanties procédurales et supervision

Le TAF fonde une grande partie de son constat d'illicéité sur l'insuffisance des garanties contre les abus dans la surveillance du réseau câblé. Il insiste sur l'absence d'un contrôle indépendant suffisamment fort sur l'ensemble du processus, sur la protection insuffisante des communications sensibles (avocats, journalistes, etc.) et sur le manque de mécanismes permettant de vérifier concrètement que seules les données pertinentes sont exploitées.

Or, ces critiques peuvent intégralement être transposées à la rétention indiscriminée des

métadonnées. Certes, l'accès aux données conservées est soumis à des autorisations et à des procédures, mais la collecte elle-même, c'est-à-dire la conservation systématique des données de toute la population concernée par les fournisseurs contraints, intervient sans contrôle individuel préalable. De plus, la supervision porte surtout sur l'accès par les autorités, et non sur la logique globale d'une conservation massive et indifférenciée.

Ainsi, si l'on applique le raisonnement du TAF, on peut se demander si le régime de rétention indiscriminée offre réellement des garanties structurelles plus solides que celles jugées insuffisantes pour la surveillance par câble. La différence semble davantage tenir à la qualification juridique du dispositif qu'à une divergence fondamentale dans les risques pour les droits fondamentaux.

Proportionnalité

Dans l'arrêt 1C_598/2016, le TF a jugé la rétention généralisée des métadonnées proportionnée en se fondant surtout sur l'intérêt public à la poursuite des infractions graves et sur le fait que l'accès aux données est encadré par des procédures. L'analyse repose donc principalement sur une pesée abstraite des intérêts entre sécurité et vie privée.

Le TAF adopte, dans l'arrêt A-6444/2020, une approche plus stricte. Pour lui, la proportionnalité ne dépend pas seulement du but poursuivi, mais aussi de la structure du système de surveillance. Un dispositif qui collecte des données de manière massive et sans soupçon individuel doit intégrer des garanties fortes dès le départ (limitations techniques, contrôle indépendant, protection des communications sensibles, voies de recours).

Appliqué à la rétention des métadonnées, ce standard plus exigeant soulève des doutes : ce régime aussi est général, préventif et non ciblé. Le fait qu'il s'agisse de métadonnées ne supprime pas le caractère intrusif du dispositif. La différence de résultat entre les deux décisions peut donc donner l'impression que deux niveaux de proportionnalité ont été appliqués.

Absence de recours effectif

L'un des éléments centraux du raisonnement du TAF dans l'arrêt A-6444/2020 est le déficit de voies de recours effectives pour les personnes concernées par la surveillance du réseau câblé. Le TAF souligne que, dans un système de surveillance secrète et de masse, les individus ignorent en principe si leurs communications ont été interceptées ou analysées. Sans mécanisme clair permettant, a posteriori, d'être informé, de demander des explications ou de contester la légalité du traitement de leurs données, le droit à un contrôle juridictionnel effec-

tif reste largement théorique.

Cette critique peut être transposée au régime de rétention indiscriminé des métadonnées. Là aussi, les données sont collectées et conservées de manière préventive, sans que les personnes concernées en soient informées individuellement. Si l'accès par les autorités à ces données est soumis à des procédures, la conservation elle-même ne fait l'objet d'aucune possibilité de contestation concrète par les personnes dont les données sont stockées, puisque les fournisseurs tenus de conserver les données peuvent simplement leur opposer une obligation légale de le faire. En pratique, un individu ne saura généralement pas que ses métadonnées ont été utilisées dans une procédure, et encore moins qu'elles ont été conservées à titre préventif pendant des mois, les modalités de notification de la personne concernée par l'autorité étant régies par l'art. 279 CPP, qui permet notamment aux autorités de renoncer à informer si les données obtenues en surveillance ne sont pas utilisées à des fins probatoires, ce qui est souvent le cas en pratique.

Il en résulte que le contrôle juridique se concentre sur les autorités et les mécanismes institutionnels, plutôt que sur la capacité des personnes concernées à faire valoir leurs droits. Or, la logique retenue par le TAF met précisément l'accent sur la nécessité que les droits fondamentaux ne soient pas protégés uniquement de manière abstraite ou institutionnelle, mais qu'ils puissent être invoqués concrètement par les individus. Sous cet angle, la différence de traitement entre la surveillance par câble et la rétention indiscriminée des métadonnées apparaît moins nette, car dans les deux régimes, le droit au recours effectif est structurellement affaibli par le caractère secret, généralisé et préventif de la collecte de données.

Standard de protection des communications sensibles

Alors que le TAF a explicitement tenu compte de la nécessité d'un haut niveau de protection pour les communications sensibles (sources journalistiques, avocat-client), le jugement sur la rétention des métadonnées n'aborde pas aussi systématiquement cet aspect. Pourtant, les métadonnées peuvent révéler des profils extrêmement sensibles de la vie personnelle et professionnelle d'un individu (réseaux de contacts, positions géographiques, habitudes), ce qui pose des questions fondamentales de dignité et d'intimité.

Conclusion

L'arrêt A-6444/2020 du TAF constitue une remise en question importante des régimes de surveillance de masse en Suisse. Il marque un déplacement du centre de gravité de l'analyse juridique : il ne suffit plus d'invoquer un objectif légitime de sécurité nationale ou de lutte

contre la criminalité pour justifier une surveillance étendue. Le TAF insiste sur le fait que des ingérences profondes dans la vie privée ne peuvent être admises que si le système lui-même intègre des garanties structurelles solides, supervision indépendante, limitations techniques réelles, protection renforcée des communications sensibles et possibilités concrètes de recours. Ces exigences s'inscrivent clairement dans la lignée de la jurisprudence européenne récente relative à la surveillance de masse et l'on peut s'en réjouir pour l'état des droits fondamentaux.

À l'inverse, la jurisprudence en matière de rétention indiscriminée des métadonnées, telle qu'interprétée dans l'arrêt 1C_598/2016, reflète une approche plus permissive, fondée principalement sur une pesée classique des intérêts entre sécurité publique et sphère privée. La conservation généralisée est admise en raison de son utilité pour les enquêtes pénales, malgré son caractère préventif, non ciblé et étendu. Le contraste entre les deux décisions donne ainsi l'impression que des régimes extrêmement proches du point de vue de leur logique basée sur une collecte massive de données de personnes non soupçonnées sont évalués selon des standards de contrôle juridictionnel différents.

Cette divergence met en lumière un débat juridique et politique plus large sur l'équilibre entre sécurité et libertés individuelles dans l'ordre juridique suisse. Elle soulève surtout une question de cohérence : si des garanties structurelles insuffisantes rendent illicite la surveillance par exploration du réseau câblé, il devient difficile d'ignorer que des interrogations identiques existent à propos de la rétention généralisée des métadonnées. L'enjeu n'est donc pas seulement de corriger un dispositif particulier, mais de clarifier le niveau de protection attendu face aux formes contemporaines de surveillance numérique.

Dans ce contexte, une réévaluation critique des normes suisses paraît inévitable afin d'assurer une protection cohérente et effective des droits fondamentaux dans tous les régimes de surveillance. Cette réflexion pourrait notamment s'inscrire dans le cadre de la révision des ordonnances liées à la LSCPT initiée en 2025 et pourrait constituer une occasion de rapprocher le droit suisse des standards européens en matière de garanties procédurales et de contrôle des systèmes de surveillance de masse. À défaut, il est certain que le TAF soit appelé à nouveau à procéder à la même analyse après l'entrée en force des nouvelles ordonnances de la LSCPT. Un nouveau projet de l'administration, qui devrait selon toute vraisemblance initier une seconde phase de consultation, est attendu courant 2026.

Proposition de citation : Marc L□EBEKKEN, État des lieux de la surveillance de masse, 29 janvier 2026 *in* www.swissprivacy.law/392

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