_swissprivacy.law

2e révision des ordonnances de la LSCPT : vers une surveillance de tout un chacun toujours plus intrusive pour l'internet suisse

Marc Løebekken, le 8 avril 2025

Le Conseil fédéral a récemment ouvert une seconde consultation relative à la révision partielle des ordonnances liées à la Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Sous couvert de clarifier les définitions des fournisseurs et de leurs obligations, le projet cherche à largement étendre les obligations de rétention de données aux fournisseurs de service de communication dérivés en Suisse.

I. Contexte

La rétention indiscriminée de données secondaires a toujours été au cœur de débats juridiques et sociétaux houleux, en Suisse comme ailleurs. La notion, qui exige des fournisseurs de conserver sans distinction certaines données de tous les utilisateurs de leurs services aux fins de futures hypothétiques enquêtes pénales, bien qu'interdite dans l'UE par la CJUE (Digital Rights Ireland e.a.), avait été considérée comme conforme au droit pour les services de télécommunication suisses par le TF en 2018 (ATF 144 I 126).

Fort de cette victoire d'étape, l'administration avait étendu l'application des obligations de surveillance des fournisseurs de services de télécommunication (FST) — soit les fournisseurs opérant des réseaux pour transmettre de l'information, tels que les fournisseurs d'accès internet ou de téléphonie — aux fournisseurs de services de communication dérivés (FSCD) — soit tout opérateur de service de communication utilisant internet pour fournir son service — par le biais de la nouvelle LSCPT en 2018. Ainsi, la volonté affichée de l'administration depuis 2018 a été d'imposer ces obligations au secteur technologique suisse, à contre-courant de nos voisins européens.

L'administration, sous couvert de clarification des différentes questions juridiques soulevées par les recours et les postulats subséquents à l'entrée en force de la LSCPT, cherche aujourd'hui à considérablement étendre un régime d'obligations étant déjà considéré comme l'un des plus intrusifs au sein des démocraties occidentales. Pendant ce temps, la décision du TF de 2018 est toujours en attente de jugement par la CEDH à Strasbourg, afin de trancher sur la légalité du principe de rétention indiscriminée de données dans la LSCPT (Glättli et al.

Contre Suisse).

II. Modification du champ d'application pour les obligations étendues des FSCD

L'OSCPT dans sa forme actuelle fonctionne avec différents niveaux d'obligation pour les FST et les FSCD en fonction de leur importance. En effet, afin de respecter le principe de proportionnalité, il est admis que les petits fournisseurs ne devraient pas se voir imposer des obligations intrusives et coûteuses.

Les FST, ayant des obligations de surveillance étendues par défaut, peuvent s'en voir exonérer sur requête (système de « *downgrade* ») s'ils n'offrent que des services dans le domaine de la recherche ou de l'éducation ou n'atteignent aucune des valeurs suivantes : (1) un chiffre d'affaires annuel en Suisse de 100 millions de francs pendant deux exercices consécutifs ; ou (2) des mandats de surveillance (émis par un tribunal des mesures de contrainte) portant sur dix cibles différentes au cours de douze derniers mois (art. 26 al. 6 LSCPT / art. 51 OSCPT).

Les FSCD, à l'inverse, ne sont soumis qu'à des obligations très limitées par défaut (art. 50 OSCPT a contrario/at. 18a OSCPT). Dès lors qu'ils atteignent certains seuils, ces derniers se voient imposer des obligations supplémentaires (système d'« *upgrade* »). Sous le système actuel, si un FSCD reçoit plus de 100 demandes de renseignements — soit des demandes d'informations simples sur un utilisateur spécifique (non soumis à un ordre d'un tribunal des mesures de contrainte) — au cours des douze derniers mois, celui-ci se voit imposer des obligations étendues en matière de renseignement (art. 22 OSCPT). S'il reçoit des mandats de surveillance sur plus de cibles différentes au cours des douze derniers mois, celui-ci se voit imposer des obligations étendues en matière de surveillance (art. 52 OSCPT). Si un FSCD réalise un chiffre d'affaires en Suisse de plus de 100 millions de francs suisses pendant deux exercices consécutifs et fournit ses services à plus de 5000 usagers, celui-ci se voit imposer les obligations des deux catégories simultanément.

La question des seuils d'application des obligations étendues pour les FSCD a fait l'objet de nombreuses discussions et débats entre l'administration, les tribunaux et le secteur technologique suisse. En effet, la base légale de la LSCPT mentionne que les FSCD peuvent se voir imposer par le Conseil fédéral des obligations similaires aux FST uniquement sur la base de (1) leur importance économique et/ou (2) de leur nombre d'utilisateurs (art. 27 al. 3 LSCPT). Sous cet angle, le secteur technologique suisse avait vivement critiqué le critère du nombre de demandes de renseignements et ordres de surveillance reçus par un fournisseur, dans la mesure où celui-ci était la plupart du temps entièrement décorrélé de l'importance écono-

mique d'un fournisseur ou de son nombre d'utilisateurs.

La bonne nouvelle, c'est que l'administration semble avoir entendu cette critique et supprimé ce critère dans le présent projet de révision (toutefois uniquement pour les FSCD, les FST étant toujours soumis à ce critère). La mauvaise, c'est que le second critère désormais proposé par l'administration pour les FSCD, à savoir le critère du nombre d'utilisateurs, aurait pour conséquence d'affecter un nombre beaucoup plus conséquent de FSCD avec des obligations supplémentaires. En effet, l'administration propose de remplacer le système existant par un système graduel à trois niveaux :

- Les FSCD ayant des obligations complètes, ayant un chiffre d'affaires en Suisse d'au moins 100 millions de francs au cours de deux exercices consécutifs ou ayant une moyenne d'un million d'utilisateurs sur l'ensemble des services dérivés qu'ils offrent au cours de douze derniers mois (16 g rev-OSCPT)
- Les FSCD ayant des obligations restreintes, n'atteignant pas les seuils précédemment mentionnés, mais ayant une moyenne de 5000 utilisateurs sur l'ensemble des services dérivés qu'ils offrent au cours des douze derniers mois (16f rev-OSCPT)
- Les FSCD ayant des obligations minimales, n'atteignant aucun des seuils précédemment mentionnés (16e rev-OSCPT)

L'introduction de cette catégorie intermédiaire, les FSCD ayant des obligations restreintes, est une des propositions principales de cette révision. À défaut d'avoir des obligations aussi lourdes et intrusives que la catégorie supérieure (qui correspond à l'ancienne catégorie des FSCD avec obligations étendues), cette catégorie se voit proposer un nombre conséquent d'obligations, qui seront détaillées dans la prochaine section. Avec un seuil d'application extrêmement bas (5000 utilisateurs), c'est tout le secteur technologique suisse opérant sur internet qui entrera dans cette catégorie, introduisant un système de surveillance généralisé de l'internet suisse.

Pour le surplus, on peut s'inquiéter de la proposition de l'administration de considérer les seuils comme déterminants de manière globale et sur la base de tous les services fournis par un FSCD de manière cumulée, s'éloignant de sa pratique précédente de considérer différents services fournis par un même fournisseur de manière isolée. Ainsi un FSCD ayant des obligations restreintes ou complètes sur la base d'un de ses services à large adoption se verrait soumis aux obligations correspondantes pour tous ses autres services, aussi mineurs soient-ils. Il est garanti que ce système présente une entrave significative à l'innovation, en augmentant notamment considérablement les coûts liés à la conformité de nouveaux services.

III. Obligations de rétention de données : mécanismes juridiques

Dans l'OSCPT actuelle, il existe trois sources principales susceptibles d'imposer des obligations de conservation de données d'utilisateurs aux fournisseurs : (1) l'obligation en matière de surveillance ; (2) l'obligation en matière de renseignement et (3) l'obligation d'identifier les utilisateurs selon des « moyens appropriés ».

L'obligation en matière de surveillance, la plus lourde des trois, requiert notamment d'être en mesure d'exécuter ou de faire exécuter par des tiers les surveillances selon les sections 8 à 12 de l'OSCPT (art. 50 al. 1 OSCPT). En matière de rétention de données, cette obligation doit être comprise à la lueur des ordres de surveillance HD (« Historical Data » ou *données historiques*) mentionnés dans la section 11 de l'OSCPT, qui détaillent le type de données à transmettre pour chaque type d'ordre de surveillance rétroactive. À défaut d'obligations en matière de surveillance, un fournisseur ne doit fournir pour un ordre HD que les données dont il dispose dans l'usage normal de son service. « Être en mesure d'exécuter » l'ordre en question requiert dès lors du fournisseur de conserver toutes les données listées dans l'ordre HD du service correspondant, indépendamment de leur utilité pratique pour la fourniture du service. Un fournisseur de courrier électronique soumis à l'obligation de surveillance devrait par conséquent conserver pendant une durée de 6 mois l'ensemble des données listées sous ordre HD_30_EMAIL (art. 62 OSCPT), à savoir une copie de tous les courriels envoyés et reçus par l'utilisateur (contenu exclu), le journal de connexion à la boîte mail, ainsi que les adresses IP de connexion pour chacun de ces événements. Il s'agit là d'une quantité absolument massive de données desquelles la conservation représente un risque conséquent.

L'obligation en matière de renseignement, bien que plus légère, propose notamment d'être étendue à cette nouvelle catégorie de FSCD avec des obligations restreintes, qui doivent désormais « conserver et être en mesure de fournir pendant toute la durée de la relation commerciale, ainsi que six mois après celle-ci, les indications relatives aux services » (art. 21 al. 1 let a. rev-OSCPT). Celle-ci doit être comprise à la lueur des requêtes de renseignement IR (« Information Request » ou *demande de renseignement*) mentionnées aux sections 4 à 6 de l'OSCPT. Les requêtes IR ne sont, contrairement aux ordres HD, pas soumises à une décision du tribunal des mesures de contrainte et peuvent être ordonnées par les autorités de poursuite pénale de manière autonome.

À défaut d'obligations en matière de renseignement, un fournisseur ne doit fournir pour une requête IR reçue que les données dont il dispose dans l'usage normal de son service. S'il est sujet à l'obligation en matière de renseignement, le fournisseur devra conserver les données

nécessaires afin de pouvoir exécuter pleinement la requête IR correspondant au service qu'il opère. Si un type de service n'est pas spécifiquement catégorisé dans l'OSCPT (par exemple, les services de messagerie tels que Threema ou Session), celui-ci entre dans la catégorie « COM », dite des autres services de communication. La création d'une nouvelle requête d'information telle que la requête IR_60_COM_LAST (art. 43a rev-OSPCT), qui requiert notamment de conserver la date et l'heure de la dernière connexion à un service, ainsi que l'adresse IP et le numéro de port du client, créera de facto un système de surveillance généralisé de tous les accès aux services fournis par les FSCD de plus de 5 000 utilisateurs basés en Suisse.

Nous sommes bien loin des promesses faites par le conseiller fédéral Guy Parmelin lors de la procédure de révision de la LSCPT selon laquelle il n'y aurait pas de surveillance généralisée. On pourrait pour le surplus se demander si ce type de données de connexion, incluant les données de géolocation (adresses IP) ne devrait pas requérir un ordre du tribunal des mesures de contrainte sur la base de l'art. 273 CPP, et si dès lors l'introduction de ce nouveau type de renseignement ne représente pas une tentative de soustraire la réquisition de certains types de données au contrôle judiciaire censé les protéger.

Enfin, l'obligation d'identifier les utilisateurs par des moyens appropriés demeure plus ou moins un mystère pour les fournisseurs (art. 19 al. 1 OSCPT). Le texte soumis à consultation ne propose pas de l'altérer fondamentalement, mais clarifie qu'elle sera désormais applicable aux FST, aux FSCD ayant des obligations restreintes, et aux FSCD ayant des obligations étendues. Cette obligation floue voudrait qu'un fournisseur soit capable d'identifier tout utilisateur de son service par des moyens appropriés, ce qui est en principe impossible et loin d'être le cas pour la majorité des fournisseurs en Suisse et dans le reste du monde. Le rapport explicatif tente, comme son prédécesseur, d'offrir des pistes qui pourraient satisfaire l'administration, mais cette liste est loin d'offrir la clarté nécessaire pour les fournisseurs qui ne peuvent raisonnablement exiger un passeport, un numéro de téléphone ou une carte de crédit pour ouvrir une relation commerciale.

Pour le surplus, la proposition semble désormais, à la lueur du rapport, mélanger l'obligation d'identification par des moyens appropriés avec l'obligation de renseignement, dans la mesure où elle désigne spécifiquement le fait de conserver les données relatives au type de requête IR_60_COM_LAST (art. 43a rev-OSCPT) — à savoir la rétention des données relatives à la dernière connexion au service avec adresse IP et port-source — comme une manière possiblement valide de s'acquitter de cette obligation. En tout état de cause, le manque de clarté sur cette obligation ne renforce pas la sécurité du droit et promet de nombreuses

discussions avec l'administration afin de comprendre ce qui est attendu des fournisseurs.

IV. Conclusion

Lorsque l'on analyse les nouvelles dispositions du projet soumis à consultation, on ne peut qu'être confus à comprendre la volonté de l'administration. Tout au contraire de ce qu'elle indique dans le message de consultation, à savoir une volonté de simplifier les obligations des PME et fournir un cadre juridique sûr pour le secteur technologique suisse, elle entreprend par ce projet de considérablement aggraver la surveillance généralisée en Suisse, laissant l'avenir du secteur, et spécifiquement des acteurs suisses réputés pour leur sécurité et leur minimisation des données, tels que Proton, Threema ou Tresorit (et plus récemment la messagerie Session, qui s'est paradoxalement installée en Suisse il y a quelques mois pour son cadre juridique favorable en la matière) incertain face à ces obligations qui menacent l'existence même de leur modèle commercial.

Enfin, pas incertain pour Proton. Car il est déjà clair pour nous que nous ne pourrons jamais entrer en conformité avec les obligations qui tentent d'être adoptées par l'administration suisse dans le présent projet. Si celles-ci devaient être imposées telles que proposées, nous n'aurions d'autre choix que de déplacer les opérations de nos services dans des juridictions ayant des régimes moins draconiens en matière de surveillance. Au-delà de la trahison de la promesse faite à nos utilisateurs qu'elles représenteraient, les obligations contemplées ne permettraient simplement pas à Proton et aux autres acteurs suisses de bénéficier de la compétitivité et de la vélocité nécessaires pour faire face aux concurrents étrangers sur le marché des services technologiques, ce qui apparaît pourtant crucial à la lueur du climat géopolitique actuel.

Avant d'en arriver là, il reste une chance d'arriver à convaincre l'administration qu'imposer une rétention indiscriminée de données pour les FSCDs similaire à celle imposée aux FST est une énorme balle dans le pied de la Suisse. Si vous êtes sensible au sujet et saisissez l'ampleur de l'enjeu, n'hésitez pas à donner votre opinion dans la procédure de consultation avant l'échéance du 6 mai 2025. Notre équipe juridique demeure disponible pour toute question ou discussion à cette adresse.

Proposition de citation : Marc L□EBEKKEN, 2e révision des ordonnances de la LSCPT : vers une surveillance de tout un chacun toujours plus intrusive pour l'internet suisse, 8 avril 2025 *in*

_swissprivacy.law

www.swissprivacy.law/347

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