

La rétention indiscriminée de métadonnées en Suisse : chronologie et développements

Nicolas Sacroug et Marc Løebekken, le 14 avril 2022

Le Conseil fédéral a récemment ouvert une première 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) afin de les adapter à l'arrivée de la technologie 5G. Une seconde consultation suivra notamment pour clarifier la catégorisation des entités soumises à ces obligations.

La surveillance en Suisse et en Europe

À l'heure actuelle, la surveillance des postes et télécommunications est régie par la LSCPT, dont la version actuellement en force a été entièrement révisée en 2013 et est entrée en vigueur en 2018.

L'ancienne LSCPT, adoptée en 2000 et entrée en vigueur en 2002, était la première loi unifiant à la fois la surveillance des services postaux et des fournisseurs de télécommunications (FST). Ainsi, au niveau des communications électroniques, seuls les services de télécommunication entrant dans le champ d'application de la Loi fédérale sur les télécommunications (LTC), et donc soumis à enregistrement, faisaient face aux obligations de surveillance et de rétention d'informations de la LSCPT (art. 1 al. 2 A-LSCPT).

Avec sa révision totale en 2013, son champ d'application a été largement étendu par l'inclusion, notamment, des fournisseurs de communication dérivés (FSCD), à savoir « les fournisseurs de services qui se fondent sur des services de télécommunication et qui permettent une communication unilatérale ou multilatérale » (art. 2 let. c LSCPT). Par cet ajout, presque tous les fournisseurs suisses proposant un service de communication sur Internet se retrouvent soumis à des obligations en matière de surveillance ou de fourniture de renseignements.

L'ordonnance principale d'application de cette loi, l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT), soumet les FSCD à des obligations similaires à celles applicables aux FST, dont les plus notables sont l'obligation de rétention générale et indiscriminée des données secondaires de télécommunication (à savoir, les

données indiquant avec qui, quand, combien de temps et d'où les usagers ont été ou sont en communication ainsi que les caractéristiques techniques des communications en question), ou métadonnées, pendant six mois (art. 21 OSCPT) ainsi que l'obligation d'identification des utilisateurs « par des moyens appropriés » (art. 19 OSCPT). L'imposition de telles obligations à potentiellement tous les fournisseurs de services suisses sur Internet met à mal la notion d'un Internet privé et sûr et pose d'importantes questions sur le modèle sociétal choisi par la Suisse.

De telles velléités ont d'ailleurs été observées chez nombre de nos voisins européens jusqu'à ce que la CJUE rappelle (à plusieurs reprises dont la dernière en date du mois d'avril) l'incompatibilité avec le droit européen d'une législation nationale imposant la rétention générale et indiscriminée de métadonnées et de données de localisation à des fins de lutte contre les infractions en général ou de préservation de la sécurité nationale, en raison de sa grave ingérence aux droits fondamentaux, et particulièrement au respect de la vie privée des individus (affaires Digital Rights Ireland e.a., Tele2 Sverige AB e.a., La Quadrature du Net e.a. et G.D.). Celle-ci a en effet estimé que seule la lutte contre la criminalité grave était susceptible de justifier une telle rétention de données, à condition d'être ciblée, proportionnée et limitée au strict nécessaire. Exit donc la rétention indiscriminée de métadonnées à des fins préventives.

Appelé à trancher une question similaire, le Tribunal fédéral a estimé que la rétention systématique de données secondaires de tous les usagers pendant six mois n'était pas contraire à la Constitution fédérale ni à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales aux motifs que l'intensité de l'ingérence aux droits fondamentaux des utilisateurs était proportionnée et que l'accès à ces données par les autorités pénales était soumis aux conditions du CPP, rappelant au passage qu'il n'était pas lié par la jurisprudence de la CJUE.

Le Tribunal fédéral semble donc arriver à des conclusions diamétralement opposées à celles de la CJUE, dont les conclusions s'inquiétaient d'un sentiment des justiciables « que leur vie privée [fasse] l'objet d'une surveillance constante » (Digital Rights Ireland e.a.). Les requérants, insatisfaits par ce résultat décevant, ont porté la cause devant la Cour européenne des droits de l'Homme, toujours pendante à ce jour.

Dans l'intervalle, un certain nombre d'incertitudes et de défauts du cadre juridique suisse a été contesté par différentes associations et fournisseurs suisses de services électroniques. Les problématiques liées à la rétention de données découlant des ordonnances d'application

de la LSCPT ont fait l'objet de trois recours devant les Tribunaux administratif fédéral et fédéral (arrêts du TAF A-5373/2020, A-550/2019 et du TF 2C_544/2020) et de quatre objets parlementaires (postulat 19.4031, heure des questions 19.5273, interpellation 19.3267, motion 18.3507) depuis l'entrée en force de l'intégralité de leurs dispositions en 2018.

Si le Conseil fédéral a systématiquement défendu l'application des ordonnances, le bilan devant les tribunaux est quant à lui considérablement plus mitigé, tous les recours ayant été *a minima* partiellement admis sur leurs conclusions principales.

La pratique montre que la LSCPT laisse une marge de manœuvre inquiétante au Conseil fédéral et que celle-ci a servi à maintes reprises à étendre son application bien au-delà de la volonté du législateur. À titre d'exemple, les simples définitions et délimitations des différents types de fournisseurs, de prime abord réglées de manière équivoque dans la loi, mais en pratique faisant l'objet d'une décision du Service de Surveillance de la correspondance par poste et des télécommunications (Service SCPT), ont été intensément discutées devant les tribunaux.

Les exemples des sociétés Threema GmbH et Proton AG, fournisseurs respectivement de messagerie instantanée et de courriers électroniques cryptés de bout en bout, sont parlants à eux seuls. Ces dernières avaient effectivement été considérées comme des FST par le Service SCPT, les soumettant à de plus lourdes obligations en matière de surveillance et de fourniture de renseignements qu'auparavant. Le Tribunal fédéral, respectivement le Tribunal administratif fédéral, en a décidé autrement et a renvoyé la cause au Service SCPT pour nouvelle(s) décision(s), ce dernier devant désormais requalifier les fournisseurs concernés de FSCD.

Le projet de révision des ordonnances n'améliore guère la situation. En effet, les potentielles clarifications de catégorisation des fournisseurs feront l'objet d'une révision subséquente à celle-ci. Ainsi, les fournisseurs sont amenés aujourd'hui à se prononcer sur des obligations sans être capables d'identifier lesquelles de celles-ci s'appliqueront à eux demain. La plupart des révisions envisagées dépassent en réalité la simple adaptation de la surveillance à la technologie 5G annoncée par le Conseil fédéral en renforçant des mesures de surveillance existantes.

Parmi celles-ci, l'on peut citer la possibilité donnée aux autorités de poursuite pénale d'obtenir les données de potentiellement plusieurs milliers d'utilisateurs grâce à une seule adresse IP sans contrôle préalable du tribunal des mesures de contrainte (art. 38 al. 1 P-OSCPT) et l'obligation faite aux fournisseurs de traiter les demandes de renseignements

sans aucune intervention humaine ([art. 18 al. 2 P-OSCPT](#)). Ce dernier projet de révision, combiné à l'actuelle incapacité pratique des fournisseurs de contester les décisions rendues en matière de surveillance ([art. 42 al. 2 LSCPT](#)), contribue à rendre la surveillance générale toujours plus aisée, sans contreparties adaptées pour les fournisseurs et la société civile. Il augmente considérablement le risque posé à la sécurité des usagers.

Constat

L'Internet suisse se trouve aujourd'hui pris dans une procédure de révision incertaine, qui semble procéder d'une logique chronologique difficilement compréhensible. Par ailleurs, nombre de propositions de modification (et investissements financiers et techniques y correspondant) reposent sur l'admission par le Tribunal fédéral de la licéité de la rétention indiscriminée de métadonnées et pourraient se voir entièrement invalidées à tout moment par une décision défavorable de la CourEDH.

Dans l'intervalle et au vu de la pratique des autorités d'exécution, de plus en plus d'opérateurs suisses se retrouvent contraints de collecter toujours davantage de données de leurs utilisateurs, dont la grande majorité s'avère bien souvent inutile en pratique, alors que leurs concurrents européens ne font face pour la plupart à aucune obligation analogue.

Une situation bien loin d'être idéale pour la sécurité – des données et du droit – dans un secteur toujours plus stratégique au sein d'un pays pourtant réputé pour avoir su rester, au fil de son histoire, à la pointe des développements technologiques.

Proposition de citation : Nicolas SACROUG / Marc LEBEKKEN, La rétention indiscriminée de métadonnées en Suisse : chronologie et développements, 14 avril 2022 *in* www.swissprivacy.law/135

 Les articles de [swissprivacy.law](http://www.swissprivacy.law) sont publiés sous licence creative commons CC BY 4.0.