La jurisprudence sur la conservation des données des communications électroniques et son impact sur la législation nationale et les procédures pénales

Andres Parmas, Procureur général d'Estonie

Situation actuelle et questions soulevées dans le droit interne estonien :

- Ces dernières années, l'Estonie a été confrontée à une série de problèmes aigus et critiques concernant la collecte de preuves obtenues par la conservation de données de communications électroniques et l'utilisation de ce type de preuves dans le cadre de procédures pénales.

- En juin 2021, la Cour suprême d'Estonie a décidé que les données de communication électronique, que les entreprises de télécommunication étaient tenues de collecter et de conserver en vertu de l'article 1111 de la loi sur les communications électroniques, ne pouvaient être demandées à des fins d'enquête criminelle, car la procédure de stockage et d'utilisation des données en vigueur en Estonie est contraire au droit de l'Union européenne, compte tenu de l'arrêt préjudiciel de la Cour de justice de l'Union européenne du 2 mars 2021.

o Plus précisément, la Cour Suprême a conclu que l'Art 15(1) de la Directive E-Privacy (2002/58/EC), en conjonction avec les Articles 7, 8, 11 et 52(1) 11 de la Charte des Droits Fondamentaux de l'UE doivent être interprétés comme étant en contradiction avec les dispositions légales nationales selon lesquelles les compagnies de télécommunication sont obligées de collecter et de conserver proactivement de manière générale et indiscriminée les données de communication et le Bureau du Procureur a le droit d'effectuer des enquêtes pour obtenir ces données.

o La Cour suprême a décidé que les dispositions susmentionnées du droit communautaire sont en contradiction avec la réglementation nationale estonienne qui autorise le bureau du procureur à adresser des demandes aux entreprises de télécommunications afin d'obtenir des données relatives au trafic des appels téléphoniques, ainsi que des données de localisation, qui sont stockées pour les procédures pénales en vertu de la loi sur les communications électroniques, dans le but d'enquêter sur les crimes.

- Le changement de paradigme concernant la légalité de la conservation des données des communications électroniques à des fins d'enquête criminelle a conduit à une situation juridiquement floue et imprévisible.

o Les entreprises de télécommunications continuent actuellement à conserver certaines données de communication à des fins commerciales. En outre, la norme obligeant les télécoms à collecter et à conserver les données est toujours en vigueur et, pour l'instant, il semble que les télécoms doivent

conserver les données à des fins autres que l'enquête criminelle (notamment à des fins de sécurité interne ou externe).

o Le bureau du procureur s'est abstenu de demander des données conservées sur la base de l'obligation annulée de l'article 1111 de la loi sur les communications électroniques, mais a demandé les mêmes données que les télécoms possèdent nonobstant cette obligation à des fins de facturation (sur la base de l'article 102 de la loi sur les communications électroniques).

 D'un point de vue statistique, le nombre de demandes a toutefois considérablement diminué depuis la décision de la Cour suprême :

 Entre le 01.10.2020 et le 30.04.2021, le bureau du procureur a accordé environ 1024 autorisations de demander des données de communication.

 En 2022, le bureau du procureur a soumis moins de 350 demandes d'accès aux données de communication au juge de la mise en état. En 2023, le nombre de demandes est resté à peu près le même.

- L'approche d'enquête alternative à l'obtention de preuves en demandant l'accès aux données de communication est l'obtention de données à l'aide de mesures d'enquête secrètes. Alors que la première consiste à accéder à des métadonnées telles que les journaux d'appels ou l'historique de localisation avec une précision de mât téléphonique, la seconde implique des mesures beaucoup plus invasives telles que les écoutes téléphoniques, la surveillance secrète ou l'accès à l'intégralité du contenu de l'appareil de communication. Malgré l'intrusion nettement plus importante dans les droits de la personne qu'implique la surveillance, la pratique actuelle des tribunaux suggère paradoxalement une tendance à favoriser cette approche.

- Le véritable problème posé par la jurisprudence estonienne réside dans le fait qu'elle est imprévisible et souvent incohérente. En outre, une décision récente du tribunal de district datant de la mi-mai de cette année, bien qu'elle ne soit pas encore entrée en vigueur, a conclu que, puisque l'obligation légale de conservation proactive générale et indiscriminée des données de communication a été annulée, l'utilisation de ces données obtenues auprès des sociétés de télécommunications est illégale et n'est pas admissible en tant que preuve. Cependant, le tribunal de district n'a absolument pas tenu compte du fait que, récemment, seules les données de communication que les sociétés de télécommunications possèdent à des fins de facturation ont été demandées. La question reste donc ouverte. La situation est d'autant plus complexe que les télécoms ne disposent pas de bases de données différentes pour les données stockées sur des bases juridiques différentes. Par conséquent, la différenciation de la source des données n'est de toute façon qu'imaginaire.

- Un autre problème est que, dans de nombreux cas, le déclenchement de l'utilisation de mesures secrètes est basé sur les preuves recueillies à partir des données de communication. Par conséquent, si les données de communication sont déclarées irrecevables en tant que preuves, les preuves recueillies par des mesures secrètes le sont également. Cette situation est très préoccupante pour de nombreuses procédures pénales en cours, car elle menace gravement la poursuite de nombreux types de crimes.

- Dans le même temps, il est profondément paradoxal que le cadre juridique permette aux entreprises de médias sociaux de fonctionner, en les autorisant à stocker de grandes quantités de données personnelles. Ces modèles commerciaux sont conçus pour capitaliser sur les données des utilisateurs. À l'inverse, les États ne peuvent pas utiliser ces données pour remplir leurs objectifs et obligations fondamentaux en matière d'enquête et de dissuasion des crimes, ainsi que d'aide aux victimes. Cette contradiction soulève des questions cruciales sur l'équilibre entre la protection de la vie privée et la sécurité, et met en lumière la controverse que suscite le fait d'autoriser l'exploitation commerciale des données tout en limitant leur utilisation à des fins de sécurité publique et de justice.

La voie à suivre :

- Les recommandations de la CJCE concernant la collecte sélective de données sont irréalisables, en particulier en ce qui concerne les limitations géographiques proposées. En ce qui concerne les télécommunications, l'intensité de la couverture du signal et la question de savoir si l'appareil de télécommunication se trouve dans le rayon d'action d'un mât particulier sont influencées par les conditions météorologiques, ce qui complique encore le problème. La recommandation de la CJCE de cibler des individus spécifiques équivaut à un profilage de masse, qui est intrinsèquement discriminatoire et, en ce sens, incompréhensible. Outre les préoccupations éthiques que de telles pratiques soulèvent, elles pourraient avoir des conséquences désastreuses pour les membres des groupes ciblés (tels que les pédophiles présumés) en cas de violation d'une base de données. Il est donc préférable de traiter tout le monde de la même manière et de trouver un moyen de stocker les métadonnées des communications sans discrimination.

- Dans le contexte européen actuel, l'approche prônée par la CJCE peut s'avérer dangereuse en raison de l'évolution des défis en matière de sécurité, tels que la guerre en cours en Europe, la multiplication des actes de sabotage et le terrorisme. Dans ce contexte, le ministère estonien de l'intérieur travaille sur un projet de législation qui vise à justifier davantage un régime indiscriminé de conservation des données sous le couvert de considérations de sécurité. Cependant, cela n'atténuerait pas les préoccupations des enquêtes criminelles dans la plupart des cas qui ne sont pas directement liés à la sécurité nationale.

- Pour aller de l'avant, si l'Union européenne est consciente des risques associés, il serait plus efficace de mettre en œuvre des réglementations au niveau de l'UE. La Commission européenne pourrait introduire un nouveau règlement pour répondre à ces préoccupations de manière globale. En outre, la voie à suivre ne devrait pas se limiter à la poursuite du débat sur la conservation et l'utilisation des données de télécommunications, telles que les données relatives aux appels téléphoniques et aux messages SMS. Nous devons plutôt nous concentrer sur les méthodes de communication contemporaines, telles que les appels par internet (par exemple, WhatsApp) et les services de messagerie, qui comprennent principalement des plateformes comme FaceTime. Ces formes de communication sont fondamentalement différentes en termes d'exigences et de réglementations relatives au stockage des données, pour lesquelles il n'existe actuellement aucune règle globale. Nos cadres existants, liés à l'infrastructure téléphonique traditionnelle, sont dépassés. Nous devrions

donner la priorité à l'élaboration de nouveaux cadres réglementaires pour l'obtention de preuves dans les procédures pénales, qui tiennent compte du paysage actuel de la communication numérique.