

CJUE, 06 OCTOBRE 2020, Données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle

Affaire C-623/17 et Affaires jointes C-511/18, C-512/18 et C-520/18

Conformité au droit de l'Union Européenne de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation

Synthèse : Par deux arrêts adoptés en grande chambre le 06 octobre 2020¹, la Cour de Justice de l'Union Européenne a confirmé que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation.

I. La règle : garantir la confidentialité des communications électroniques et des données afférentes

Ces arrêts confirment la position de la Cour de Justice de l'Union Européenne (ci-après « **CJUE** ») sur la protection des libertés individuelles en matière d'exploitation des données et particulièrement des métadonnées utilisées à des fins de lutte contre la criminalité. A cette occasion, elle a rappelé les principes et solutions dégagés dans son arrêt fondamental rendu le 21 décembre 2016 « **Tele2 Sverige et Watson e.a.** » (ci-après l'arrêt « **Tele2** », voir *infra*).

Pour la bonne compréhension des deux arrêts du 06 octobre 2020, il convient de rappeler que la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite « e-Privacy » (ci-après la « **directive** »), avait pour objet d'harmoniser les dispositions des Etats membres nécessaires pour assurer un niveau de protection des droits et libertés fondamentaux en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques. Toutefois, la directive laissait une marge de manœuvre aux Etats membres, lesquels pouvaient, conformément à l'article 15, adopter des mesures législatives limitant la confidentialité des communications et des données de trafic, sous réserve que cela soit nécessaire, approprié et proportionné, pour sauvegarder « la sécurité nationale ».

Dans ce contexte, et au regard de la marge de manœuvre qui leur était laissée, les Etats membres ont développé des législations (pour la France, les articles L.31-1 du Code des postes et des communications électroniques et 6 de la Loi du 21 juin 2004 pour la confiance dans l'économie numérique – dite « **LCEN** ») permettant, pour des besoins de constatation et de poursuite des infractions pénales, la conservation et la communication aux autorités nationales des métadonnées détenues par les fournisseurs de services de communications électroniques (ci-après « **FSCE** »).

¹ [Communiqué de presse n° 123/20 du 06 octobre 2020, CJUE](#)

Dès 2016, la CJUE a veillé à délimiter cette exception, en indiquant que la directive avait vocation à s'appliquer aux FSCE, contraints de conserver les données de leurs abonnés et de permettre aux autorités publiques d'y accéder, et alors même que les Etats membres invoquaient un motif de sécurité nationale.

Dans l'arrêt précité, la cour s'est opposée à une « *réglementation nationale prévoyant à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* », réaffirmant ainsi l'exigence de proportionnalité des mécanismes nationaux d'accès aux métadonnées détenues par les FSCE.

Pour autant, et dans un contexte accentué de menaces contre leur sécurité nationale, certains Etats membres, dont la France, ont interprété cette décision « Tele2 » comme leur permettant de procéder néanmoins à une collecte massive des métadonnées dans le cadre d'enquêtes policières, administratives et judiciaires.

II. L'exception : encadrer l'utilisation des données relatives au trafic et à la localisation

La CJUE a été saisie, en 2016, par les juridictions belge, britannique et française, concernant l'interprétation de l'article 15 de la directive, et par analogie, leurs transpositions respectives.

La Cour, dans ses arrêts rendus le 6 octobre 2020 en grande chambre, réitère sa jurisprudence « Tele2 » : les Etats ne peuvent pas faire de l'exception de l'article 15 de la directive une règle générale au nom de la sécurité nationale. Elle déduit de la lettre de l'article et de sa décision précédente qu'une dérogation à l'obligation de garantir la confidentialité de ces données n'est possible que si les critères cumulatifs suivants sont réunis :

- Respect des principes généraux du droit de l'Union ;
- Respect du principe de proportionnalité ; et
- Respect des droits fondamentaux garantis par la Charte des Droits Fondamentaux de l'Union Européenne.

En conséquence, la Cour rappelle que deux situations ne peuvent être considérées comme répondant à ces exigences :

- Une réglementation nationale imposant aux FSCE la transmission généralisée et indifférenciée des données relatives au trafic et à la localisation (ci-après les « **données en cause** ») aux services de sécurité et de renseignement, pour des motifs de sauvegarde de la sécurité nationale ; et
- Une réglementation nationale imposant aux FSCE, à titre préventif, une conservation généralisée et indifférenciée de telles données.

Plus spécifiquement, la Cour fait preuve de pédagogie en fournissant aux Etats membres un « guide » des critères impératifs à respecter, lequel illustre particulièrement bien tant le critère « d'exception » de l'article 15 de la directive, que la grande attention portée par la Cour à la protection de la vie privée. Partant, les mesures présentant le plus de risques pour les personnes concernées sont soumises à des exigences plus strictes.

Ainsi, une législation nationale ne peut prévoir **d'enjoindre aux FSCE de conserver de manière généralisée et indifférenciée les données en cause pour des motifs de sécurité nationale que si :**

- Il existe une menace grave pour la sécurité nationale ;
- La menace est réelle et actuelle ou prévisible ;
- L'injonction ne porte que sur une période temporellement limitée au strict nécessaire ; et
- L'injonction fait l'objet d'un contrôle effectif (juridictionnel ou par une entité administrative indépendante dont la décision est contraignante).

Une législation nationale **ne peut prévoir l'analyse automatisée des données en cause de l'ensemble des utilisateurs de moyens de communications électroniques que si :**

- Il existe une menace grave pour la sécurité nationale ;
- La menace est réelle et actuelle ou prévisible ;
- L'analyse ne porte que sur une période temporellement limitée au strict nécessaire ; et
- L'analyse fait l'objet d'un contrôle effectif (juridictionnel ou par une entité administrative indépendante dont la décision est contraignante).

Une législation nationale **ne peut prévoir la conservation ciblée des données en cause pour des motifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique ou de sauvegarde de la sécurité nationale, que si :**

- La conservation ne porte que sur une période temporellement limitée au strict nécessaire ;
- La conservation est délimitée en fonction des catégories de personnes concernées ou au moyen d'un critère géographique ; et
- La conservation est fondée sur la base d'éléments objectifs et non discriminatoires.

Une législation nationale **ne peut imposer aux FSCE de recueillir en temps réel les données en cause que si :**

- Le recueil est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées dans des activités de terrorisme ;
- Le recueil n'est autorisé que dans la limite de ce qui est strictement nécessaire ; et
- L'injonction est soumise au contrôle préalable d'une juridiction ou d'une entité administrative indépendante dont la décision est contraignante.

Une législation nationale **ne peut prévoir le recours à la conservation rapide des données en cause dont disposent les FSCE pour une durée excédant les délais légaux de conservation, à des fins d'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, que si :** les infractions ou atteintes ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée.

Une législation nationale ne peut prévoir la conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication électronique que si la durée de conservation est limitée au strict nécessaire.

Enfin, une législation nationale peut prévoir la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs des moyens de communication électronique, et ce sans restriction ou condition particulière.

En conséquence, la réitération de la décision « Tele2 » ainsi que la démarche pédagogique de la Cour réduisent dès lors significativement la marge de manœuvre d'interprétation de l'article 15 de la directive laissée jusqu'alors aux Etats membres.

A toutes fins utiles, la Cour précise aux Etats membres qu'elle n'entend pas différer l'effet de ses décisions, et qu'aucune disposition interne, législative ou juridictionnelle, ne pourrait valablement différer ces effets. Toutefois, elle ne précise pas les conditions dans lesquelles les Etats doivent prendre acte de ces décisions, ni comment ceux-ci peuvent les transposer efficacement dans les contentieux en cours.

Cette décision, particulièrement attendue après quatre ans de procédure, pourrait ainsi remettre en cause les méthodes actuelles d'enquête (policière, administrative et judiciaire).

Emmanuel DAOUD, Avocat au barreau de Paris, associé du Cabinet Vigo, membre du réseau international d'avocats GESICA

Océane PECRIAUX, élève-avocate à l'IXAD, Cabinet Vigo