
Garanties et limites de la protection des données personnelles de connexion

Description

CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18.

La primauté du droit européen sur les droits nationaux impose que ceux-ci soient conformes au premier. Il en est ainsi des dispositions relatives à la protection des données personnelles et de la vie privée à l'égard de l'usage des techniques de communications électroniques et de la possibilité, pour les autorités nationales, d'imposer, aux prestataires techniques, de prêter, de conserver et, en certaines circonstances, de mettre à la disposition de la police et de la justice les données de connexion des utilisateurs de ces services.

La Cour de justice de l'Union européenne (CJUE) avait été saisie, notamment par la juridiction administrative française, de questions préjudicielles relatives à la conformité de différentes dispositions du droit français (code de la sécurité intérieure ; code des postes et des communications électroniques ; loi du 21 juin 2004 pour la confiance dans l'économie numérique¹) aux exigences du droit européen (Charte des droits fondamentaux de l'Union européenne ; cinq directives² dont la directive sur le commerce électronique et la directive dite vie privée et communications électroniques, ainsi que le règlement général sur la protection des données ou RGPD).

Sur la base de ces différents textes, rappelant le principe du droit à la protection des données personnelles et de la vie privée, l'arrêt du 6 octobre 2020 envisage cependant des situations et des circonstances, notamment de garantie de la sécurité nationale et de prévention et de poursuite d'infractions, dans lesquelles les prestataires techniques des services de communications électroniques peuvent, à titre d'exception, être contraints de conserver les données de connexion des utilisateurs desdits services et de les mettre à la disposition des autorités de police et de justice nationales.

L'article 15 de la directive 2002/58/CE du 12 juillet 2002 constitue la principale disposition à laquelle se réfère la Cour de justice dans le présent arrêt. Il y est posé que *« les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévues à »* par de précédents articles relatifs à la confidentialité des communications, à l'exploitation des données relatives au trafic, à l'identification de la ligne appelante et de la ligne connectée et aux données de localisation, *« lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale »* « -dire la » *« de l'État »* « la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou utilisation non autorisée du système de communications »

Électroniques ». En pareille circonstance, est notamment envisagée la possibilité, pour les États membres, d'adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée ».

L'arrêt se prononce sur les mesures législatives nationales prévoyant le recueil et la conservation préventive des données relatives au trafic, des données de localisation, des adresses IP et des données relatives à l'identité civile, aux fins de lutte contre la criminalité et de la sauvegarde de la sécurité nationale et de la sécurité publique ; l'analyse automatisée des données relatives au trafic et des données de localisation ; l'information des personnes dont les données ont été recueillies et analysées.

En l'issue d'une longue comparaison des dispositions européennes et nationales visées, il arrive à la conclusion que l'article 15, § 1 de la directive 2002/58/CE « s'oppose à des mesures législatives prévoyant, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic des données et des données de localisation ».

L'arrêt pose, en revanche, que ledit article « ne s'oppose pas à des mesures législatives permettant, aux fins de sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où un État membre fait face à une menace grave pour la sécurité nationale qui soit réelle et actuelle ou prévisible » ; « prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée de données relatives au trafic et des données de localisation qui soit limitée, sur la base d'objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable », ou « une conservation généralisée et indifférenciée des adresses IP » ou « des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques » ; « permettant, aux fins de lutte contre la criminalité grave et, a fortiori, de sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services ».

Il est ajouté que le même article 15 de la directive 2002/58/CE « ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés », en cas de situations constitutives d'une « menace grave pour la sécurité nationale ».

À et À condition que cela ne concerne que des « personnes À l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées dans des activités de terrorisme ».

Dans une société démocratique, aucun droit ne peut être absolu. Au principe de protection des données personnelles de connexion aux services de communications électroniques, contre l'usage que pourraient en faire les prestataires techniques et les autorités publiques, le droit européen admet bien nécessairement que les droits nationaux y apportent des dérogations aux fins de sauvegarde de la sécurité nationale, de lutte contre le terrorisme, ou pour assurer la prévention ou la poursuite d'infractions pénales. Il appartient aux autorités des États membres de l'Union européenne, ainsi qu'il est clair sur la signification et la portée du droit européen, de veiller à la conformité de leurs dispositions nationales à son égard.

¹ Et divers décrets d'application n^{os} 2015-1185, 2015-1211, 2015-1639 et 2016-67.

² Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; directive 97/66/CE du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ; directive 2000/31/CE du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur, dite directive sur le commerce électronique ; directive 2002/21/CE du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques ; 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 directive vie privée et communications électroniques.

Sources :

- « Stockage des données. Le coup de frein de la justice européenne », Amaëlle Guiton, *Libération*, 8 octobre 2020.
- « Données de connexion : la justice européenne s'oppose à une collecte généralisée », Elise Vincent, *Le Monde*, 8 octobre 2020.

Categorie

1. Droit

date création

19 janvier 2021

Auteur

emmanuelderieux