

La justice européenne retoque la collecte massive des données permise par la France

Fin du suspens dans la bataille opposant l'Etat français et des associations de lutte pour la confidentialité des données. La Cour de justice européenne vient d'interdire les textes nationaux obligeant les hébergeurs et les FAI à conserver les données de manière généralisée et indifférenciée, sauf exceptions encadrées.

Temps de lecture : minute

6 octobre 2020

C'est une petite victoire pour la Quadrature du Net, la Fédération des fournisseurs d'accès à internet et les associations qui se battent pour la confidentialité des données. La Cour de justice de l'Union européenne (CJUE) vient de confirmer ses décisions prises dès 2016 et réitérées en 2018 concernant la possibilité pour les États d'obliger les hébergeurs et les fournisseurs d'accès à internet (FAI) à conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation. La réponse de la justice européenne est franche mais nuancée : ces mesures sont en principe interdites mais peuvent être modulées en fonction des circonstances.

La protection des données, cheval de bataille de l'UE

Sujet sensible pour les consommateurs·rices comme les autorités de sûreté, la confidentialité des données est au coeur des débats des instances juridiques françaises depuis quelques années déjà. À tel point

qu'en juillet 2019, le Conseil d'État décidait de saisir la Cour de justice de l'Union européenne pour mettre un terme définitif à une querelle qui est loin d'être anodine. Les services de renseignements français admettent clairement miser sur ces données pour élucider des infractions et anticiper des menaces. Afin de les aider dans leur mission, le gouvernement français a pris, dans plusieurs textes législatifs (notamment la loi sur la confiance dans l'économie numérique), la décision d'obliger les intermédiaires techniques que sont les FAI et les hébergeurs, à conserver les données de connexion de manière généralisée et indifférenciée pendant un an.

Plusieurs voix se sont alors élevées, dont celles de la Quadrature du Net ou encore de la fédération des fournisseurs d'accès à internet (FDN) pour critiquer l'entrave à la confidentialité engendrée par ce type de texte.

La Cour de justice européenne vient de leur donner raison, écartant ainsi la possibilité de mettre en oeuvre ce type de législation, jugée contraire à la "*directive vie privée et communication électronique*" et trop disproportionnée. La Charte de l'Union européenne repose sur le principe de proportionnalité des décisions prises entre la limite des libertés et la sécurité.

Des dérogations soumises à vérification

Malgré ce revers pour la législation française, la CJUE a émis quelques dérogations à son obligation de garantir la confidentialité des communications électroniques et des données y afférentes. En cas de menace réelle ou prévisible grave pour la sécurité nationale, la "*directive vie privée et communication électronique*" ne s'oppose pas à ce qu'un État ordonne la conservation des données relatives au trafic et à la localisation de manière généralisée et indifférenciée. À condition que celle-ci soit effectuée par une période limitée au strict nécessaire et qu'elle fasse l'objet d'un contrôle effectif par une juridiction ou une entité

administrative indépendant dont la décision est dotée d'un effet contraignant.

La Cour ajoute également que ce type de demande devra être effectuée sur la base d'éléments objectifs et non discriminatoires, en fonction de la catégorie de personnes concernées ou au moyen d'un critère géographique. La conservation des données s'appliquera également aux adresses IP, de manière limitée dans le temps ainsi qu'aux données relatives à l'identité civile des utilisateurs des moyens de communication électroniques, sans limite de durée cette fois-ci.

Afin de permettre l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, la conservation des données au delà des délais légaux établis pourra également être demandée à condition que les infractions aient déjà été constatées ou que leur existence soit raisonnablement soupçonnable.

Le dernier point abordé par la Cour concerne la recueil en temps réel des données lorsque des personnes sont soupçonnées d'être impliquées de près ou de loin dans des actes de terrorisme. Une dérogation est encore possible à condition qu'un contrôle soit rapidement réalisé.

Si toutefois les autorités d'un État décidait d'utiliser des preuves obtenues hors du cadre de réglementation posé par la CJUE, celle-ci exige que le juge national les écarte.