SECURITE NATIONALE ET PROTECTION DE LA VIE PRIVEE

Quand les juges dialoguent au sujet de la conservation des données numériques : l'arrêt du Conseil d'Etat du 21 avril 2021

« Le dialogue des juges », c'est par cette expression que les cours européennes et les cours suprêmes des Etats membres désignent communément leurs échanges sur des questions juridiques qui peuvent se révéler délicates, particulièrement lorsqu'elles portent sur les droits fondamentaux, en raison de l'étroite imbrication des ordres juridiques nationaux et européens.

Le dialogue peut être rude, comme en témoigne l'arrêt du Conseil d'Etat du 21 avril 2021 sur la conservation des données numériques de connexion qui clôt provisoirement sur ce sujet un échange d'une intensité inédite, les juridictions nationales ayant interrogé la Cour de justice de l'Union Européenne (CJUE) à cinq reprises, le Conseil d'Etat étant lui-même à l'origine de deux saisines.

Les développements techniques qui nourrissent les trente-neuf pages de l'arrêt le rendent peu accessible au grand public. Et pourtant, la recherche d'une solution équilibrée entre respect de la vie privée et sauvegarde de la sécurité nationale, à laquelle se sont livrés les grands juges, fait écho aux mêmes préoccupations contrastées du commun des mortels.

En effet, le citoyen qui, chaque jour, fait l'expérience de la puissance des algorithmes des géants du net et s'inquiète de ce qu'il advient de ses données personnelles sur la toile, adhère avec d'autant plus d'enthousiasme à la jurisprudence européenne que celle-ci lui est présentée comme prohibant de façon péremptoire, au nom du principe du respect de la vie privée, la collecte et la conservation généralisée et indifférenciée des données numériques au profit de la puissance publique.

D'un autre côté, observateur fasciné des progrès de la police scientifique au travers d'affaires criminelles au retentissement médiatique, le citoyen exprime sa satisfaction que les données de connexion et de localisation, conjuguées aux techniques d'identification par ADN, puissent contribuer à laisser de moins en moins de chance au crime.

Et après la longue série d'effroyables attentats terroristes, il ne s'interroge guère sur le fait qu'à la suite du dernier en date, à Rambouillet, le gouvernement envisage de « pérenniser l'usage d'algorithmes pour scruter l'ensemble des

communications téléphoniques et des sites web pour traquer les signaux faibles passés sous les radars ».

Au sein de l'Union européenne, la plupart des législations nationales tentent de concilier les impératifs de la vie privée et de la sécurité publique, dans le respect des principes posés par la directive « ePrivacy » 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.

Le vaste lac des données

Les dispositions du Code des postes et des communications électroniques, et de la loi récente sur la confiance dans l'économie numérique (LCEN), qui étaient contestées devant le Conseil d'Etat au regard du droit de l'Union européenne, énumèrent très précisément les données numériques que doivent conserver pendant un an les fournisseurs de services de communications électroniques. Il s'agit, en substance, des données d'identification (adresse mail, adresse IP…), des données de trafic et des données de localisation.

Il est illusoire de croire que cette mesure de conservation des données pourrait atteindre ses objectifs affichés d'identification des criminels et de lutte contre le terrorisme si elle n'était pas généralisée à l'ensemble de la population et si elle ne concernait pas toutes les données numériques utiles à cette fin, même celles qui sont les plus intrusives dans la vie privée, telle que l'adresse IP, qui permet de connaître les sites consultés par une personne, ou les données de trafic ou de localisation.

Une telle collecte généralisée et indifférenciée aboutit inévitablement, pour reprendre la métaphore du rapporteur public, à la constitution d' «un vaste lac de données »

On relèvera toutefois, en continuant de filer la métaphore, que l'eau de ce vaste lac est régulièrement renouvelée, ce qui est essentiel.

En effet, l'effacement automatique des données numériques au bout d'un an, comme le prévoit la directive de 2002, constitue une protection majeure de la vie privée, notamment en contemplation des difficultés rencontrées par l'internaute pour faire valoir son « droit à l'oubli » et obtenir l'effacement d'informations le concernant apparaissant sur certains sites.

Il reste qu'à ce vaste lac de données un nombre croissant d'autorités administratives ont, au fil du temps, selon le rapporteur public, été autorisées à

s'abreuver (services fiscaux, douanes, Hadopi, Autorité de la concurrence, organismes de sécurité sociale… Une affaire étant actuellement pendante devant la CJUE en ce qui concerne l'AMF).

C'est ici que le bât blesse et que la vigilance s'impose.

L'accès aux données conservées ne saurait en effet être autorisé en dehors du cadre strict des recherches criminelles et de la sauvegarde de la sûreté nationale qui ont justifié la mesure de conservation et les atteintes à la vie privée auxquelles elle conduit.

Les enquêtes criminelles

L'utilisation des données de connexion et de localisation pour la recherche des auteurs de crimes n'est pas de nature à susciter de grands débats au regard de la protection de la vie privée, tant paraît légitime une telle utilisation, par ailleurs entièrement soumise aux exigences de la procédure pénale qui présente les garanties que l'on sait.

Dans ce contexte en effet, non seulement l'utilisation des données numériques est limitée à l'acte criminel, commis ou en préparation, mais elle intervient sous le contrôle de l'autorité judiciaire.

Faut-il néanmoins, comme l'a dit pour le droit la CJUE, réserver l'accès aux données de connexion et de localisation numériques aux infractions les plus graves ? Sans aucun doute. Mais c'est toutefois avec raison que le Conseil d'Etat a retenu que la CJUE n'exigeait pas de dresser à cette fin la liste des infractions les plus graves, et qu'il a pu estimer que « *le principe de proportionnalité entre gravité de l'infraction et importance des mesures d'enquête mises en œuvre, qui gouverne la procédure pénale* » relève, dans chaque affaire, de l'appréciation du juge pénal.

Ce pouvoir d'appréciation pourrait conduire le juge pénal à interroger la CJUE afin de donner à celle-ci l'occasion, au regard de cas concrets dont il est saisi, de préciser ce qu'il faut entendre par criminalité grave au sens de sa jurisprudence.

La lutte antiterroriste et les atteintes à la sûreté nationale

Ici le débat se focalise sur la prévention et les activités de renseignement qui lui sont consubstantielles.

Il ne peut y avoir de lutte anti-terroriste efficace sans une intense activité de renseignement.

Mais permettre aux services de renseignement de scruter les activités de l'ensemble de la population en puisant dans la masse des données numériques conservées par les fournisseurs de services de communications électroniques constitue incontestablement une ingérence profonde dans la vie privée des citoyens qui ne peut être justifiée que par des circonstances particulièrement graves et passagères.

C'est ce que la CJUE a jugé dans son arrêt du 6 octobre 2020. Après avoir affirmé que le stockage général et indifférencié des données de connexion et de localisation est contraire, en principe, à la Charte des droits fondamentaux de l'Union européenne et à la directive « ePrivacy », elle admet des exceptions dès lors que cela « *constitue une mesure nécessaire, appropriée et proportionnée* […] *pour sauvegarder la sécurité nationale, la défense et la sécurité publique* », en précisant qu'il doit exister des « *circonstances suffisamment concrètes permettant de considérer que l'Etat membre concerné fait face à une menace grave*,[…]*réelle et actuelle ou prévisible* », et que la mesure ne peut être ordonnée que pour « *une période limitée* » et à condition que soit mis en place « *un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant* »

Au regard de ces exigences, le Conseil d'Etat a censuré les dispositions gouvernementales réglementaires en vigueur qui :

- *Ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée de certaines données à la sauvegarde de la sécurité nationale*,
- *Ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale*,

Il a également censuré les dispositions qui autorisent les services de renseignement à puiser dans les données numériques *sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée*.

Il en résulte que l'avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui jusqu'ici n'était que consultatif, sera désormais conforme. En d'autres mots, les services de renseignement ne pourront pas avoir accès aux données conservées sans l'accord de la CNCTR.

Par ailleurs, il paraît raisonnable que les services de renseignement puissent avoir les mains libres en cas d'urgence justifiée, le contrôle dans ce cas se faisant a posteriori.

En conclusion de ce rapide survol, on retiendra que le « dialogue des juges » au sujet de la question de la conservation des données numériques, pour « rugueux » qu'il ait pu paraître, n'en a pas moins été fructueux. L'arrêt du Conseil d'Etat du 21 avril 2021, en tirant toute la substance des décisions de la CJUE, est parvenu à concilier de manière heureuse des impératifs contraires. Mais s'il est déjà considéré par certains comme historique, c'est moins par son important apport à la protection de la vie privée dans le secteur des communications électroniques que par ce qu'il dit de la hiérarchie des normes et de l'articulation des ordres juridiques national et européen.

Roger Grass
Magistrat honoraire
Membre du Comité-Europe iDFrights