Article de M. Junior-Jack AVRIL,
juriste, stagiaire au sein de notre cabinet

CE., 30 juin 2023, n°469712

Le Gouvernement a adopté un décret « portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion ».

Il était fait grief au décret pris par le Premier ministre une atteinte disproportionnée aux libertés fondamentales et, plus précisément, au droit au respect de la vie privée. Ce faisant, pour les requérants, le décret aurait méconnu l'article 41 de la charte des droits fondamentaux de l'Union européenne et le principe général de motivation des actes des autorités nationales pris dans le champ du droit de l'Union. Par suite, le décret n'ayant prévu un dispositif de réexamen périodique de l'obligation de conservation des donnée, un contrôle administratif ou encore juridictionnel, il irait à l'encontre de la directive 2002/58, telle que le commanderait l'interprétation de la Cour de justice de l'Union européenne.

Les requérants estimaient aussi que l'adoption de ce nouveau décret aurait du être soumis à la constation d'une menace de nature ou d'intensité différente de celle précédemment invoquée. De ce fait, le Premier ministre aurait méconnu la directive 2002/58 et le règlement du 27 avril 2016, lus à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union et des dispositions de l'article L34-1 du code des postes et des communications électroniques.

Plus généralement, était soulevé, aussi, le moyen tiré d'une prétendue erreur d'appréciation sur l'existence d'une menace grave et actuelle contre la sécurité nationale justifiant qu'ordre soit fait aux opérateurs de communications électroniques, aux fournisseurs et hébergeurs de contenus de conserver ces données.

Etait-il réellement attentatoire au droit au respect de la vie privée de porter injonction au regard de la menace grave et actuelle contre la sécurité nationale de la conservation de certaines catégories de données pour une durée d'un an renouvelable ?

Les juges administratifs du Palais-Royal répondent à cette question par la négative. Effectivement ils considèrent, d'une part, que l'existence d'une menace grave et actuelle contre la sécurité nationale est justifiée aux termes de l'article III de l'article L34-1 du code des postes et des communications et que, en ce sens le Premier ministre a suffisamment motivé le décret attaqué.

La durée maximale d'un an, d'autre part, ne peut être renouvelée que si les conditions prévues pour son édiction sont réunies. A l'inverse lorsque que ces conditions ne sont plus réunies, il peut être mis fin avant le terme prévu.

Il n'est nullement avéré, du reste, que l'adoption d'un nouveau décret portant injonction de conservation de certaines données de connexion, soit subordonnée à la constatation d'une menace différente de nature ou d'intensité de celles précédemment invoquées. Les requérants infondés à demander l'annulation du décret attaqué, les Hauts magistrats administratifs rejettent la requête.

Si la solution du Conseil d'État est la manifestation d'une conciliation complexe entre des impératifs de sécurités nationales et la protection des libertés individuelles (I), elle marque une singularité certaine au regard de la jurisprudence de la Cour du Luxembourg (II).

I. La délicate conciliation entre des impératifs de sécurité nationale et de protection des libertés individuelles

Dans sa solution, le Conseil d'État juge d'une conservation des données conforme aux impératifs de sécurité nationale (A), tout en recherchant un certain équilibre (B).

A. Une conservation des données conforme aux impératifs de sécurité nationale

Le juge de l'excès de pouvoir avalise l'analyse gouvernementale c'est-à-dire une conservation des données conforme aux impératifs de sécurité nationale. En effet, dans un premier temps, les conseillers d'État ont jugé que le Premier ministre « a suffisamment motivé le décret attaqué ». En l'espèce, le Premier ministre se bornait seulement à dire que l'édiction du décret résultait « *de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion* ». Le motif se retrouvant au III de l'article L34-1 du Code des postes et des communications électroniques.

Pour autant, il ressort de la jurisprudence de la Cour de Justice de l'Union européenne un principe général de motivation des actes, pendant d'une protection juridictionnelle opérationnelle (CJCE, 15 octobre 1987, Unectef contre Georges Heylens et autres, Aff. 222/86, Rec. 4097). L'article 41 de la Charte des Droits Fondamentaux de l'Union européenne pose aussi l'exigence de motivation des actes. Cependant, à la différence des institutions de l'Union, l'obligation de motivation est applicable seulement aux actes individuels et non aux actes de portée générale (CJCE, 17 juin 1997, Sodemare SA, Anni Azzurri Holding SpA et Anni Azzurri Rezzato Srl contre Regione Lombardia, Aff. C-70/95, Recueil I-3395).

Le Conseil Constitutionnel comme le Conseil d'État à l'occasion de plusieurs décisions conviennent des rapports entre droits de l'Union et droit interne. Ce sont notamment les décisions du 10 juin 2004, loi pour la confiance dans l'économie numérique n°2004-496 DC du Conseil constitutionnel ou du Conseil d'État du 8 février 2007, Société Arcelor n°287110. En tout état de cause, les deux juridictions s'accordent sur le fait que lorsqu'est en cause l'intérêt national, le droit interne prime.

Le Conseil d'État avalise, ainsi, une conservation des données conforme à des impératifs de sécurité nationale, toutefois, un équilibre est recherché.

B. Une volonté recherchée d'équilibre du Conseil d'État avec un contrôle « normal » de l'existence d'une « menace grave, actuelle ou prévisible »

Malgré la conformité de la mesure prononcée par le Conseil d'État, ce dernier souligne l'équilibre de la mesure dans plusieurs de ses aspects.

En premier lieu, et c'est le ***point principal à retenir de cette décision du Conseil d'Etat,*** le ***Le juge de l'excès de pouvoir exerce un contrôle normal sur l'existence d'une menace grave, actuelle ou prévisible, contre la sécurité nationale, justifiant l'injonction faite aux opérateurs de communications électroniques de conserver certaines catégories de données de trafic et de localisation*** sur le fondement du III de l'article L. 34-1 du code des postes et des communications électroniques (CPCE).

En second lieu, la mesure est doublement encadrée.

D'abord, la mesure est encadrée par son motif ; elle « *ne peut être renouvelée que si les conditions prévues pour son édiction continuent d'être réunies* ». En d'autres termes, dès lors que les conditions de menace grave et actuelle contre la sécurité nationale ne sont plus réunies, un recours pour excès de pouvoir peut être formé en vue de suspendre l'effet de la mesure.

Ensuite, l'injonction est « *d'une durée maximale d'un an* [et elle] *ne peut être renouvelée que si les conditions prévues pour son édiction continuent d'être réunies* ». De ce fait, l'injonction faite aux opérateurs de communications électroniques est circonscrite dans le délai d'un an « *si les conditions prévues pour son édiction continuent d'être réunies* ».

Sur ces points, le Conseil d'État tache de trouver un certain équilibre entre des exigences de sécurité et de liberté. De ce fait, la décision se conforme au cadre dérogatoire énoncé par la Cour de Justice de l'Union européenne. Effectivement, dans plusieurs de ses décisions en date du 6 octobre 2020, la Cour de Justice de l'Union Européenne permet, « *une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace* » ; des lors qu'un « *État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle, actuelle ou prévisible* ».

En dépit, d'une volonté d'équilibre recherchée, la décision, bien qu'elle soit conforme à la jurisprudence du Conseil d'État marque une certaine singularité au regard de la jurisprudence de la Cour de Justice de l'Union Européenne. Une jurisprudence de la Cour de Justice de l'Union Européenne, pour le moins protectrice des libertés fondamentales. Ce faisant, la décision du Conseil d'État pour l'interrogation fondamentale, de l'ouverture à un aménagement perpétuel au regard de la menace des impératifs de sécurités nationales.

II. Un arrêt singulier au regard de la jurisprudence de la Cour de Justice de l'Union Européenne

Si la décision du Conseil d'État s'avère être dans la droite lignée de ses précédentes jurisprudences (A), elle ouvre, par la même, la voie à un aménagement perpétuel (B).

A. Un arrêt s'inscrivant dans la droite lignée de décisions précédemment rendues

Selon le Conseil d'État et découlant de ce que dit précédemment, les requérants « *ne sont pas fondés à demander l'annulation du décret attaqué* ». La décision de la Haute juridiction de l'ordre administratif n'est en réalité guère surprenante sur ce point. A l'évidence, c'est une décision qui est l'héritière de celles rendues précédemment.

Les conseillers d'État se sont, ainsi résolus, dans leur arrêt du 21 avril 2021, French Data Network et autres au fait que ne pouvait être écarté une règle nationale, si cela en revenait à priver de garantie des exigences constitutionnelles qui ne bénéficient pas d'une protection équivalente en droit de l'Union européenne. Il convient de rappeler que les premiers jalons de ce type de jurisprudence sont posés par l'arrêt du Conseil d'État du 8 février 2007, Société Arcelor. Il est à noter, toutefois que Le Conseil d'État s'est, par le passé refusé au contrôle de l'*ultra vires* de la CJUE, alors que le Gouvernement le lui demandait.

D'après la Cour de Justice de l'Union européenne, le principe reste que le droit de l'Union ne saurait permettre de « *conservation généralisée et indifférenciée de données relatives au trafic et à la localisation* ».

Cet arrêt, marque une continuité voulue par le Conseil d'État, ce qui interroge sur un aménagement à vocation perpétuel.

B. L'ouverture à un aménagement perpétuel aux motifs de la menace à des impératifs de sécurité nationale

Le Conseil d'État a entériné, la conservation de données de connexion au regard d'impératif de sécurité nationale. Parmi lesquels, « *la menace islamiste sunnite* », des risques « *d'ingérence et d'espionnage* » ou une recrudescence de « *l'activité de groupes radicaux et extrémistes de l'ultra-droite et de l'ultra-gauche* ». Autant de menaces hétéroclites, qui de fait, ouvrent la voie à un aménagement sans borne temporelle dans l'hypothèse ou préexistent toujours ces menaces. Ce dernier considérant est source d'interrogations. A l'évidence, la France, aujourd'hui plus qu'hier, est confronté à des menaces de types multifactorielles. Néanmoins, dès lors que ces menaces ont vocation à durer, il convient de s'interroger sur la vocation perpétuelle de la mesure.

Du reste, contrairement à l'arrêt du Conseil d'État en date du 21 avril 2021, French Data Network et autres, les juges administratifs n'ordonnent pas au Gouvernement une réévaluation régulière de la menace qui pèse sur le territoire.