LA FRANCE PEUT- ELLE S'AFFRANCHIR DES DECISIONS DE LA COUR DE JUSTICE DE L'UNION EUROPEENNE

C'est un nouveau rebondissement qui s'est produit le 3 mars dernier dans la bataille, bien connue des spécialistes, mais pas assez du grand public, que se livrent les autorités françaises et la justice européenne depuis plusieurs années. L'objet est fondamental : l'équilibre entre liberté et sécurité, à travers des pratiques hautement sensibles, dont celles de la collecte et la conservation des données par les fournisseurs de services de communication électronique (donc les fournisseurs d'accès à Internet, FAI). L'enjeu est capital, puisqu'il s'agit de la possibilité pour l'Etat de donner accès aux autorités de sûreté dans le cadre d'enquêtes pour lesquelles Internet est une source d'information indispensable.

Reprenons le long fil de ce bras de fer engagé par l'Etat français pour s'affranchir du cadre légal imposé par la CJUE, et ce à travers plusieurs actions successives qui ne lui ont pas jusqu'ici donné entièrement raison. La dernière en date, celle du 3 mars est cependant de loin la plus déconcertante : le gouvernement a demandé au Conseil d'État de rejeter la jurisprudence européenne sur la conservation générale des données télécoms par les opérateurs, sans limite de temps, au nom de la sécurité nationale et du maintien de l'ordre public.

A l'origine de cette bataille : la mise en œuvre de la directive européenne 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 privées, dite « e-Privacy » (elle devait être révisée en 2017 mais est restée bloquée au Conseil européen, faute d'accord entre les États membres). Cette directive « e-privacy » de 2002 donc, traite de nombreux enjeux essentiels encadrant la navigation des internautes que nous sommes, comme la confidentialité des informations, le traitement des données relatives au trafic, les spams ou encore les cookies. Dans son article 15, la directive prévoit que les États membres peuvent 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* ». Après le drame du 11 septembre 2001, cela avait un sens et la directive se devait de prévoir et encadrer une telle possibilité. Après des débats houleux et difficiles mais lucides un accord fut cependant trouvé entre les Etats Membres.

Les États membres ont donc pu intégrer dans leur droit national cette notion de « sécurité nationale » en s'appuyant sur l'article 15 de cette directive « e-Privacy » : c'est ainsi qu'en France fut adoptée la Loi du 21 juin 2004 sur « la Confiance dans l'Economie Numérique », dont l'article 6 traite de cette question, en lien avec l'article L.31-1 du code des postes et des communications électroniques. Tout semblait donc aller pour le mieux : le principe de protection de nos données de navigation était solidement établi par le droit européen, et un régime dérogatoire permettait aux États membres d'exiger leur conservation et d'y accéder dans le cadre d'enquêtes pour des infractions pénales. Un juste équilibre entre liberté et sécurité.

Cet équilibre fragile s'est fissuré sous les coups de butoir de plusieurs États membres qui ont établi des législations nationales utilisant la marge de manœuvre laissée par l'article 15 de la directive « e-Privacy » pour l'interpréter de façon maximaliste, en termes de spectre de la

collecte des données mais aussi de durée de leur conservation. La France s'est particulièrement illustrée à ce sujet, dans un contexte sécuritaire sensible et difficile qui l'a souvent mise sous la pression légitime de l'opinion publique et des élus confrontés à des drames qui ont endeuillé la nation et à des menaces dont la gravité devait justifier des actions fermes et rapides en matière de sécurité nationale.

Dans un arrêt fondamental du 21 décembre 2016, dit « Tele2 », la CJUE a toutefois confirmé l'exigence de proportionnalité des mesures et considéré comme illicite toute « *règlementation 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* ».

Loin de mettre fin aux controverses, cet arrêt, qui ne condamne pas la conservation des données en soi, avait relancé en France la bataille autour de plusieurs dispositions de la Loi « Renseignement » de 2015 et conduit le Conseil d'État à saisir la CJUE de trois questions préjudicielles, pour en particulier justifier et sauver la pratique de conservation indifférenciée des données qu'il estime d'une « *utilité sans précédent* » et permettre ainsi «*à l'autorité judiciaire d'accéder aux données relatives aux communications qu'un individu a effectuées avant d'être suspecté d'avoir commis une infraction pénale* ».

Plus surprenant, le Conseil d'État interrogeait également la CJUE sur la légalité de l'encadrement européen de telles pratiques, dès lors qu'elles relèvent des exigences de la sécurité nationale – dont il précise que la « *responsabilité incombe aux seuls États-membres en vertu de l'article 4 du Traité sur l'Union européenne* ». Le Conseil d'Etat considérant que cette ingérence « *est justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne* ». Ce faisant, il écornait sérieusement la hiérarchie des normes et tentait d'ouvrir dans le droit européen des brèches au profit du droit français – rejoint en cela par d'autres États membres, dont la Belgique et le Royaume-Uni.

Dans ses arrêts du 6 octobre 2020, rendus en grande chambre, la CJUE apporte ce qui aurait dû s'apparenter à un épilogue à plus de quinze années de litiges, procédures et controverses sur ces sujets.
La Cour réitère ainsi sa jurisprudence « Tele2 » selon laquelle les États ne peuvent invoquer la seule sécurité nationale pour faire exception aux dispositions de l'article 15 de la directive « e-Privacy ». Elle précise à l'usage des États membres les critères impératifs à respecter pour faire exception à cet article 15, et ce pour plusieurs situations auxquelles peuvent répondre les législations nationales :

- L'obligation faite aux fournisseurs de services de communication électronique de conserver de manière généralisée et indifférenciée des données pour des motifs de sécurité nationale,
- 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,

- La conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication électronique,
- L'analyse automatisée des données en cause de l'ensemble des utilisateurs de moyens de communications électroniques,
- Le recueil en temps réel les données en cause,
- Recourir à la conservation rapide des données en cause dont disposent les fournisseurs de services de communication électronique 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.

Par ces arrêts, qui fixent une liste limitative et exhaustive d'exceptions, la CJUE a souhaité mettre fin à la longue bataille l'opposant aux autorités nationales et se prémunir de futures controverses en précisant de manière pratique la portée et l'interprétation de l'article 15 de la directive « e-Privacy ». Elle est également restée constante dans l'appréciation de situations au regard des valeurs européennes, en précisant l'obligation de respecter les droits de la Charte des droits fondamentaux de l'UE.

A l'intention des autorités françaises notamment, la Cour rappelle également que « *bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union* ».

Mais, loin d'être la conclusion d'une longue histoire, il semble au contraire que cela ait relancé l'ardeur des autorités françaises à s'opposer à la Cour dont les arrêts « violeraient l'identité constitutionnelle de la France ». C'est donc dans cette nouvelle direction que semble s'orienter le combat les autorités françaises, en arguant que la sécurité nationale et le maintien de l'ordre public sont des composantes de l'identité constitutionnelle française, supérieure au droit européen.

L'Institut se pose deux questions essentielles :

1 - Peut-on conserver de manière **généralisée et indifférenciée**, l'ensemble des données relatives au trafic et des données de localisation de **tous les abonnés et utilisateurs** concernant tous leurs moyens de communication électronique ?
La réponse est : **NON, il ne peut exister une telle règlementation nationale et même en cas de lutte contre la criminalité, cette règlementation devrait être considérée comme disproportionnée au regard de l'objectif poursuivi. Il faut des limitations : catégorie de données, durée de conservation etc..**

D'ailleurs la Cour européenne juge que le droit de l'Union européenne s'oppose à une législation permettant l'accès d'autorités publiques aux données de connexion, si cet accès n'est pas « *circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique »*

2 – Les autorités compétentes peuvent-elles avoir accès sans restriction à ces données ?

La réponse est encore **: NON. Ceci ne peut être autorisé que dans les limites du strict nécessaire.**
L'accès des autorités nationales compétentes aux données conservées doit être subordonné à un contrôle préalable intervenant sur une demande motivée de ces autorités nationales compétentes.
Il faut donc une demande motivée ET un contrôle.
Or, ce contrôle ne peut être effectué que par une juridiction ou une autorité administrative indépendante, de manière objective et impartiale, et doit rester à l'abri de toute influence extérieure.
En matière de droit pénal, l'exigence d'indépendance implique que l'autorité chargée du contrôle ne soit pas impliquée dans la conduite de l'enquête pénale en cause et ait une position de neutralité vis-à-vis des parties à la procédure pénale.

Or, que dit la CJUE ? que tel n'est pas le cas lorsqu'un Ministère public qui dirige la procédure d'enquête exerce l'action publique, et que dans ces conditions le ministère public n'est pas en mesure d'effectuer ce contrôle préalable.

Au stade actuel, deux hypothèses :

Si le Conseil d'Etat suit la CJUE, alors le Parquet, qui n'est pas indépendant en France, va devoir revoir certaines affaires jugées tout dernièrement….
Si le refus d'appliquer le droit européen nous était «reconnu », d'autres Etats membres risquent de s'engouffrer dans cette brèche … par exemple la Hongrie ou le Pologne.

L'Institut suivra bien évidemment cette nouvelle affaire avec beaucoup d'intérêt et aura l'occasion de publier prochainement sur son site une analyse plus approfondie de la décision qui sera rendue par le Conseil d'Etat.

Thomas Kieffer
Président fondateur d'Europtimum
Cabinet de conseil en affaires publiques européennes
Membre du Comité d'Experts des affaires européennes

Benjamin Martin-Tardivat
Associé fondateur du Cabinet d'avocats WITETIC
Spécialisé dans la protection des données personnelles