COUR DE CASSATION

Note explicative relative aux arrêts de la chambre criminelle du 12 juillet 2022 (pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652)

Conservation des données de connexion et accès

Par plusieurs arrêts publiés, la chambre criminelle de la Cour de cassation tire les conséquences des décisions rendues par la Cour de justice de l'Union européenne relatives à la conservation des données de connexion et à l'accès à celles-ci dans le cadre de procédures pénales.

Il résulte de ces décisions les principes suivants :

S'agissant de la conservation des données

Les dispositions de l'article L. 34, III du code des postes et communications électroniques (CPCE), dans sa version issue de la loi n° 2013-1168 du 18 décembre 2013, n'étaient conformes au droit de l'Union qu'en ce qu'elles imposaient aux opérateurs de services de télécommunications électroniques de conserver de façon généralisée et indifférenciée :

- pour les infractions, quelle que soit leur gravité, les données relatives à l'identité civile, aux informations relatives aux comptes et aux paiements ;

- en matière de criminalité grave, les adresses IP attribuées à la source d'une connexion ;

- les données de trafic et de localisation, aux fins de la recherche, de la constatation et de la poursuite des infractions portant atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, incriminés aux articles 410-1 à 422-7 du code pénal, qui poursuivent l'objectif de sauvegarde de la sécurité nationale. Dans les cas qui lui étaient soumis, la chambre criminelle a constaté, à partir des pièces régulièrement produites par le procureur général de la Cour de cassation relatives aux attentats commis en France depuis décembre 1994, qu'une menace grave et réelle à la sécurité nationale était caractérisée antérieurement à la date des faits.

Les réquisitions prévues aux articles 60-1 et 60-2, 77-1-1 et 77-1-2, 99-3 et 99-4 du code de procédure pénale valent injonction de conservation rapide, au sens de la Convention du Conseil de l'Europe signée à Budapest le 23 novembre 2001.

Les données conservées par les opérateurs, soit pour leurs besoins propres, soit au titre de l'obligation de conservation générale imposée aux fins de sauvegarde de la sécurité nationale, peuvent donc l'être également, à la demande des enquêteurs, par voie de réquisitions, pour la répression d'une infraction grave déterminée.

Il appartient à la juridiction saisie d'un moyen de nullité critiquant la régularité de ces réquisitions de vérifier :

- que les éléments de fait justifiant la nécessité d'une telle mesure d'investigation répondent à un critère de criminalité grave,

- que la conservation rapide des données de trafic et de localisation et l'accès à celles-ci respectent les limites du strict nécessaire.

S'agissant de l'accès aux données

Les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale sont contraires au droit de l'Union uniquement en ce qu'ils ne prévoient pas un contrôle préalable par une juridiction ou une entité administrative indépendante.

En revanche, le juge d'instruction est habilité à contrôler l'accès aux données de connexion.

S'agissant de la sanction de cette non-conformité, la juridiction doit rechercher si l'irrégularité a occasionné un grief au requérant. Un tel préjudice ne peut être établi que si le requérant démontre une ingérence injustifiée dans sa vie privée et la protection de ses données à caractère personnel, parce que :

- les données ne pouvaient être régulièrement conservées au titre de la conservation rapide,

- la ou les catégories de données visées, ainsi que la durée pour laquelle l'accès à celles-ci a eu lieu, n'étaient pas, au regard des circonstances de l'espèce, limitées à ce qui était strictement justifié par les nécessités de l'enquête.

Table des matières

I - Les exigences du droit de l'Union en matière de conservation des données de connexion et d'accès à ces données conservées

I.1. - S'agissant de la conservation des données

Dans son arrêt du 6 octobre 2020 (La Quadrature du Net e.a, French Data Network e.a, C- 511/18, C- 512/18, C- 520/18), la Cour de justice de l'Union européenne (ci-après CJUE) a dit pour droit que le droit de l'Union européenne[1] **s'oppose à une conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation aux fins de lutte contre la criminalité, quel que soit son degré de gravité.** Seule est admise une conservation généralisée et indifférenciée de ces données, en cas de menace grave, réelle et

[1] résultant de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil 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, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, tels qu'interprétés par la CJUE.

actuelle ou prévisible pour la sécurité nationale, sur injonction faite aux fournisseurs de services de télécommunications électroniques, pouvant faire l'objet d'un contrôle effectif par une juridiction ou une autorité administrative indépendante, dont la décision est dotée d'un effet contraignant, chargée de vérifier l'existence d'une telle menace et le respect des conditions et garanties devant être prévues, injonction ne pouvant être émise que pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

En revanche, le droit de l'Union ne s'oppose pas à des mesures législatives prévoyant, aux fins de la lutte contre la criminalité grave :

- une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments 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 ;

- une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

- une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ;

- le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, 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, dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

Ces principes peuvent être ainsi schématisés :

	données relatives à l'identité civile des utilisateurs	**adresses IP attribuées à la source d'une connexion**	**données relatives au trafic et à la localisation**
En cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée
Lutte contre la criminalité grave	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée pour une période temporellement limitée au strict nécessaire	Pas de conservation généralisée et indifférenciée Mais Conservation ciblée pour une période temporellement limitée au strict nécessaire **et**

			Injonction pour conservation rapide
Infractions ne relevant pas de la criminalité grave	Conservation généralisée et indifférenciée	Pas de conservation	Pas de conservation

La conservation rapide, qui a pour fondement l'article 16 de la Convention sur la cyber-criminalité, signée à Budapest le 23 novembre 2001, **peut porter sur les données que détiennent les opérateurs de télécommunications électroniques, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale.**

Cette conservation rapide des données de trafic et de localisation ne peut avoir lieu qu'à des fins de lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, dans le respect des conditions matérielles et procédurales prévues en droit européen (CJUE, arrêt du 6 octobre 2020, La Quadrature du Net e.a, French Data Network e.a, C-511/18, C-512/18, C-520/18). Elle a pour effet, en réalité, de cibler et limiter dans le temps, une conservation qui, sinon, serait généralisée et indifférenciée.

Par ailleurs, elle **peut être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave**, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction, telles les données de la victime et celles de son entourage social ou professionnel (CJUE, arrêt du 5 avril 2022, Commissioner of An Garda Siochana , C-140/20).

I.2. - S'agissant de l'accès aux données régulièrement conservées

La CJUE juge que l'accès aux données de connexion ne peut être autorisé que :

- si ces données ont été conservées conformément aux exigences du droit européen ;

- s'il a eu lieu pour la finalité ayant justifié la conservation ou une finalité plus grave, sauf conservation rapide;

- s'il est limité au strict nécessaire ;

- s'agissant des données de trafic et de localisation, s'il est circonscrit aux procédures visant à la lutte contre la criminalité grave et soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante.

Pour la CJUE, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, susceptible d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité grave, et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données de caractère personnel.

Dans son arrêt du 2 mars 2021, Prokuratuur, C-746/18, la CJUE a précisé que le droit de l'Union s'oppose à une réglementation nationale donnant compétence au ministère public, qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique, pour autoriser l'accès d'une autorité publique aux données relatives

au trafic et aux données de localisation. Il en est de même pour un fonctionnaire de police, qui ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises (CJUE, arrêt du 5 avril 2022, Commissioner of An Garda Siochana, C-140/20).

II. - Application par la chambre criminelle de ces principes

L'adhésion à l'Union européenne emporte l'obligation, pour le juge national, d'assurer la primauté du droit de l'Union.

La CJUE en déduit qu'afin de garantir l'effectivité de l'ensemble des dispositions du droit de l'Union, le principe de primauté impose aux juridictions nationales d'interpréter, dans toute la mesure du possible, leur droit interne de manière conforme au droit de l'Union. A défaut de pouvoir procéder à une telle interprétation, le juge national a l'obligation d'assurer le plein effet des dispositions du droit de l'Union en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel (CJCE, arrêt du 9 mars 1978, Simmenthal, 106/77).

II.1. - Constat de la conformité partielle au droit de l'Union des dispositions des articles L.34, III et R.10-13 du code des postes et des communications électroniques, dans leur version en vigueur à la date des faits

L'article L. 34-1, III, du code des postes et des communications électroniques, dans sa version en vigueur au moment des faits[2], imposait aux opérateurs de services de télécommunications électroniques la conservation généralisée et indifférenciée, pour une durée maximale d'un an, des données de connexion énumérées à l'article R. 10-13 dudit code[3], pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Dans les affaires enregistrées sous les n° 21-83.710, 21-83.820 et 21-84.096, la Cour de cassation relève d'abord que les atteintes aux intérêts fondamentaux de la Nation et le terrorisme, dont la répression poursuit l'objectif de sauvegarde de la sécurité nationale, sont incluses dans les « infractions pénales » visées à l'article L.34-1, III précité.

Elle en déduit que **les dispositions de ce dernier texte, mises en œuvre par celles de l'article R.10-13 du même code, ne sont conformes au droit de l'Union qu'en ce qu'elles imposent une obligation de conservation des données de trafic et de localisation pour la recherche, la constatation et la poursuite des infractions incriminées aux articles 410-1 à 422-7 du code pénal.**

Toutefois, dans la mesure où ces dispositions ne subordonnaient pas le maintien de cette obligation de conservation à un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, la Cour de cassation énonce que *« cette obligation de conservation ne vaut injonction au sens où l'entend la CJUE et cette conservation n'est régulière que si le juge saisi du contentieux*

[2] Antérieurement à l'entrée en vigueur de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

[3] Dans sa version antérieure à la promulgation du décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du code des postes et des communications électroniques.

constate, sous le contrôle de la Cour de cassation, l'existence d'une menace [grave, réelle et actuelle ou prévisible pour la sécurité nationale] ».

Il appartient ainsi à la juridiction saisie d'une requête ou d'une exception de nullité, sous le contrôle de la Cour de cassation, de vérifier si, à la date de la conservation des données litigieuses, il existait une telle menace pour la sécurité nationale.

Dans les cas qui lui étaient soumis, la chambre criminelle de la Cour de cassation, à partir des pièces régulièrement produites par le parquet général de la Cour de cassation relatives aux attentats commis en France depuis décembre 1994, a constaté qu'**une telle menace était caractérisée antérieurement à la date des faits.**

S'agissant de la durée de conservation de ces données, l'article L. 34-1, III, précité, mis en œuvre par celles de l'article R.10-13 du même code, dans leur version en vigueur à la date des faits, précisait, notamment pour les activités de téléphonie, que les données relatives au trafic et celles permettant d'identifier l'origine et la localisation de la communication devaient être conservées pour une durée d'un an.

La chambre criminelle retient que cette durée de **conservation de ces données, pour une année, apparaît comme strictement nécessaire aux besoins de la sauvegarde de la sécurité nationale.**

Dans les affaires enregistrées sous les n° 21-83.710, 21-83.820 et 21-84.096, la chambre criminelle de la Cour de cassation constate que l'obligation faite aux opérateurs de télécommunications électroniques de conserver de façon généralisée et indifférenciée aux fins de sauvegarde de la sécurité nationale les données de connexion énumérées à l'article R. 10-13 du code précité qui ont fait l'objet des réquisitions litigieuses, était conforme au droit de l'Union.

A retenir : L'obligation de conservation généralisée et indifférenciée des données de connexion prévue par l'article L.34, III du CPCE, antérieurement à l'entrée en vigueur de la loi n° 2021-998 du 30 juillet 2021, n'est conforme au droit de l'Union que s'agissant de la répression des atteintes aux intérêts fondamentaux de la Nation et du terrorisme, incriminées aux articles 410-1 à 422-7 du code pénal et qui poursuivent l'objectif de sauvegarde de la sécurité nationale.

II.2. - Conformité des dispositions qui autorisent la conservation rapide des données régulièrement détenues par les opérateurs de télécommunications électroniques aux fins de sauvegarde de la sécurité nationale

La chambre criminelle relève que le rapport explicatif de de la Convention de Budapest précise que l'injonction de conservation rapide peut résulter d'une injonction de produire.

Elle constate qu'en droit interne, les données de trafic ou de localisation conservées par les opérateurs de télécommunication sont communiquées en raison de l'émission de réquisitions lors d'une enquête en flagrant délit, en application des articles 60-1 et 60-2 du code de procédure pénale, par un officier de police judiciaire ou par un agent de police judiciaire agissant sous son contrôle, lors d'une enquête préliminaire, sur le fondement des articles 77-1-1 et 77-1-2 dudit code, sur autorisation du procureur de la République, enfin, en cas d'ouverture d'une information, en application des articles 99-3 et 99-4 de ce code, par un officier de police judiciaire autorisé par commission rogatoire du juge d'instruction[4].

[4] Dans leur version applicable antérieurement à la loi n°2022-299 du 2 mars 2022.

En outre, aux termes du sixième alinéa du paragraphe III de l'article préliminaire du code de procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction.

La régularité des réquisitions précitées peut d'ailleurs être contestée devant la chambre de l'instruction ou la juridiction de jugement, sous le contrôle de la Cour de cassation.

Ces règles sont suffisamment claires et précises pour permettre le respect des conditions matérielles de la conservation des données et procédurales y afférentes. Elles offrent aux personnes concernées des garanties effectives contre les risques d'abus.

La chambre criminelle en déduit que **les dispositions des articles 60-1 et 60-2, 77-1-1 et 77-1-2, 99-3 et 99-4 du code de procédure pénale peuvent être interprétées, de façon conforme au droit de l'Union, comme permettant, pour la lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, la conservation rapide des données de connexion stockées, même conservées aux fins de sauvegarde de la sécurité nationale.**

La criminalité grave n'est pas définie en droit de l'Union. Il appartient en conséquence à la juridiction, lorsqu'elle est saisie d'un moyen ou d'une exception de nullité, de **vérifier que les éléments de fait justifiant la nécessité d'une telle mesure d'investigation répondent à un critère de criminalité grave** au regard de la nature des agissements de la personne poursuivie, du montant du préjudice qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue.

En outre, elle doit **s'assurer que la conservation rapide des données de trafic et de localisation et l'accès à celles-ci respectent les limites du strict nécessaire**.

En résumé : La réquisition judiciaire aux fins de communication des données de connexion, prévue aux articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 et 99-4 du code de procédure pénale, dans leur version applicable antérieurement à l'entrée en vigueur de la loi n°2022-299 du 2 mars 2022, permet, pour la lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, la conservation rapide des données de connexion stockées par les opérateurs de communications électroniques, y compris aux fins de sauvegarde de la sécurité nationale.

La juridiction, saisie d'une requête ou d'une exception de nullité, doit s'assurer que les faits ayant pu justifier la délivrance d'une telle réquisition judiciaire relèvent de la criminalité grave, au regard de la nature des agissements de la personne poursuivie, du montant du préjudice qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue.

II.3. - Non-conformité des dispositions qui donnent compétence au procureur de la République pour autoriser l'accès aux données de connexion et conformité de celles qui donnent une telle compétence au juge d'instruction

Dans l'affaire enregistrée sous le n° 21-83.710, la chambre criminelle constate que **les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale sont contraires au droit de l'Union uniquement en ce qu'ils ne prévoient pas un contrôle préalable par une juridiction ou une autorité administrative indépendante.**

En effet, comme il a été vu, le droit de l'Union impose que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale. Or, le procureur de la République, quel que soit son statut, dirige la procédure d'enquête et exerce, le cas échéant, l'action publique.

En revanche, dans les affaires enregistrées sous les n°21-83.820 et 21-84.096, la chambre criminelle écarte toute irrégularité, après avoir relevé que les enquêteurs n'ont eu accès aux données de trafic et de localisation du requérant que sur commission rogatoire du juge d'instruction.

En effet, selon elle, ***« le juge d'instruction**, qui n'est pas une partie à la procédure mais une juridiction, n'exerce pas l'action publique et statue de façon impartiale sur le sort de celle-ci, mise en mouvement par le ministère public ou, le cas échéant, la partie civile, **doit être regardé comme étant habilité à contrôler l'accès aux données de connexion ».***

A retenir : les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale ne sont pas conformes au droit de l'Union en ce que les réquisitions sont délivrées, en enquête de flagrant délit, par un officier de police judiciaire ou par un agent de police judiciaire agissant sous son contrôle, ou lors d'une enquête préliminaire, sur autorisation du procureur de la République, sans contrôle préalable par une juridiction ou une autorité administrative indépendante.

En revanche, les articles 99-3 et 99-4 du même code sont conformes en ce qu'ils prévoient l'intervention du juge d'instruction.

III. - Incidences sur la procédure de la non-conformité au droit de l'Union des articles 60-1, 60-2, 77-1-1 et 77-1-2 du CPP

III.1. - Le principe d'autonomie procédurale en droit de l'Union européenne

La CJUE juge qu'il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (CJUE, arrêt du 6 octobre 2020 précité).

Le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (CJUE, arrêt du 6 octobre 2020 précité).

Le principe d'équivalence commande que l'ensemble des règles de procédure nationales s'appliquent indifféremment aux recours fondés sur la violation du droit de l'Union et aux recours fondés sur la méconnaissance du droit interne ayant un objet et une cause semblables.

III.2. - Application par la chambre criminelle de ces principes

III.2.1. - Le principe d'équivalence

- *Un moyen de nullité qui relève de l'article 802 du code de procédure pénale*

En droit interne, la chambre criminelle distingue les nullités d'ordre public, qui touchent à la bonne administration de la justice, de celles qui sanctionnent la violation d'une formalité substantielle ou prescrite à peine de nullité, qui a pour objet de préserver un droit ou un intérêt qui est propre au requérant (Crim., 7 septembre 2021, pourvoi n° 21-80.642, publié au Bulletin).

Déclinant sa méthodologie à l'espèce, la chambre criminelle de la Cour de cassation relève que **les exigences européennes en matière de conservation et d'accès aux données de connexion ont pour objet la protection du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et du droit à la liberté d'expression** (CJUE, arrêt du 6 octobre 2020 précité).

Il en est ainsi en particulier de l'exigence d'un contrôle préalable par une juridiction ou une entité administrative indépendante qui vise à garantir, en pratique, le plein respect des conditions d'accès aux données à caractère personnel, et notamment que l'ingérence aux droits précités est limitée à ce qui est strictement nécessaire (CJUE, arrêt du 2 mars 2021 précité ; CJUE, arrêt du 5 avril 2022 précité).

Il en résulte que **les dispositions invoquées sont édictées dans le seul intérêt de la personne concernée.**

Par voie de conséquence, la chambre criminelle juge, dans l'affaire n° 20-86.652, qu'un tel moyen doit avoir été soumis aux juges du fond pour être recevable devant la Cour de cassation.

En outre, dans les affaires n°21-83.820 et 21-84.096, la chambre criminelle en déduit que la personne mise en examen est irrecevable à invoquer la violation des exigences européennes en matière d'accès aux données de connexion dans la mesure où elle n'est ni le titulaire ou l'utilisateur de l'une des lignes identifiées ni n'a établi qu'il aurait été porté atteinte à sa vie privée, à l'occasion des investigations litigieuses.

- *Examen du grief*

En application des dispositions de l'article 802 du code de procédure pénale, le juge pénal ne peut prononcer la nullité que si l'irrégularité elle-même a occasionné un préjudice au requérant, lequel ne peut résulter de la seule mise en cause de celui-ci par l'acte critiqué (Crim., 7 septembre 2021, précité).

Pour la chambre criminelle, l'irrégularité fait nécessairement grief au requérant, lorsque la méconnaissance de la règle a irrévocablement affecté les droits de celui-ci.

Tel est le cas lorsque l'acte attentatoire à la vie privée a été accompli par une autorité qui n'était pas compétente, à défaut d'y avoir été autorisée, conformément à la loi. Tel est également le cas lorsque l'acte

n'a pas été motivé par l'autorité compétente pour l'ordonner alors qu'il devait l'être (Crim., 8 juillet 2015, pourvoi n° 15-81.731, Bull. crim. 2015, n° 174).

A défaut, il appartient au requérant de justifier d'une atteinte à ses intérêts. La Cour de cassation juge qu'il en est ainsi notamment lorsque l'acte attentatoire à la vie privée a été accompli par un agent compétent mais sans le contrôle d'un tiers alors que celui-ci était prévu par la loi (Crim., 7 décembre 2021, pourvoi n° 20-82.733, publié au Bulletin). C'est le cas du procureur de la République ou de l'officier de police judiciaire compétent en vertu du droit national pour accéder aux données de connexion, mais qui agit sans le contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

La chambre criminelle en déduit que **l'absence de contrôle indépendant préalable ne peut faire grief au requérant que s'il établit l'existence d'une ingérence injustifiée au respect de sa vie privée et à la protection de ses données à caractère personnel, de sorte que cet accès aurait dû être prohibé**.

En conséquence, **il appartient, dès lors, à la chambre de l'instruction de s'assurer que, d'une part, l'accès a porté sur des données régulièrement conservées, d'autre part, que la ou les catégories de données visées, ainsi que la durée pour laquelle l'accès à celles-ci a eu lieu, étaient, au regard des circonstances de l'espèce, limitées à ce qui était strictement justifié par les nécessités de l'enquête.**

Dans l'affaire enregistrée sous le n°21-83.710, la chambre criminelle de la Cour de cassation relève que l'accès des enquêteurs a eu lieu dans le cadre d'une enquête de flagrance, en l'absence d'un contrôle indépendant préalable. Cependant, elle rejette le pourvoi, après avoir approuvé la chambre de l'instruction qui a constaté que l'accès des enquêteurs aux informations litigieuses a porté sur des données régulièrement conservées et qu'il a eu lieu en vue de la poursuite d'infractions relevant de la criminalité grave, dans des conditions limitant cet accès à ce qui était strictement justifié par les nécessités de l'enquête.

III.2.2. - Le principe d'effectivité

En premier lieu, la chambre criminelle relève qu'il résulte des articles 156 et suivants du code de procédure pénale que toute personne mise en examen peut solliciter du juge d'instruction une expertise et, le cas échéant, une contre-expertise, sous le contrôle de la chambre de l'instruction, lorsque se pose « une question d'ordre technique ». Il en est de même devant la juridiction de jugement.

Elle en déduit que la législation française offre ainsi à toute personne mise en examen ou poursuivie la possibilité de contester efficacement la pertinence des éléments de preuve résultant de l'exploitation des données de connexion.

En second lieu, la chambre criminelle de la Cour de cassation rappelle que le principe d'effectivité impose que les parties aient une véritable possibilité de soulever un moyen fondé sur le droit de l'Union européenne devant une juridiction nationale.

Or, dans l'affaire enregistrée sous le n° 20-86.652, le requérant avait la possibilité de soulever, devant les juges du fond, le moyen pris de la violation de l'article 15, paragraphe 1, de la directive 2002/58/CE du 12 juillet 2002, telle que modifiée par la directive 2009/136/CE du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne par la Cour de justice de l'Union européenne.

Elle conclut donc à l'irrecevabilité d'un tel grief, invoqué devant elle pour la première fois.

ANNEXE - VADE-MECUM POUR LES CHAMBRES DE L'INSTRUCTION

Saisie d'un moyen de nullité pris de la violation des exigences européennes, la chambre de l'instruction vérifie :

1/ si le requérant est recevable à contester la régularité de la conservation et de l'accès à ses données de trafic et de localisation : Est irrecevable à invoquer la violation des exigences européennes en matière d'accès aux données de connexion la personne mise en examen qui n'est ni le titulaire ou l'utilisateur de l'une des lignes identifiées ni n'a établi qu'il aurait été porté atteinte à sa vie privée, à l'occasion des investigations litigieuses.

2/ si les données en cause ont été régulièrement conservées.

En premier lieu, la chambre de l'instruction doit constater que **les données de connexion ont été valablement conservées au titre de la sauvegarde de la sécurité nationale,** la Cour de cassation ayant relevé, dans les affaires enregistrées sous les n° 21-83.710, 21-83.820 et 21-84.096, que depuis décembre 1994, la France se trouve exposée, en raison du terrorisme et de l'activité de groupes radicaux et extrémistes, à une menace grave et réelle, actuelle ou prévisible à la sécurité nationale.

En second lieu, il lui appartient de **rechercher si les données pouvaient faire l'objet d'une conservation rapide au titre de la lutte contre la criminalité grave**.

Pour ce faire, la chambre de l'instruction doit vérifier que :

- **les faits en cause relèvent de la criminalité grave :** elle doit motiver sa décision au regard de la nature des agissements de la personne poursuivie, du montant du préjudice qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue. Il s'agit d'une appréciation *in concreto ;*

- **les réquisitions étaient tout à la fois nécessaires et proportionnées à la poursuite des infractions** objet de la procédure dont elle est saisie.

3/ si l'accès a fait l'objet d'un contrôle indépendant préalable.

S'il s'agit d'une réquisition faite sur commission rogatoire du juge d'instruction, l'accès est régulier au regard des exigences du droit de l'Union.

S'il s'agit d'une réquisition faite dans le cadre d'une enquête de flagrance ou en préliminaire, l'acte a été accompli en méconnaissance de ces exigences. Le requérant doit alors justifier de l'existence d'un grief pour obtenir le prononcé de la nullité.

4/ si l'accès aux données de trafic et de localisation autorisé par le procureur de la République ou l'officier de police judiciaire a occasionné un grief au requérant.

Il appartient à la chambre de l'instruction de s'assurer que, d'une part, l'accès a porté sur des données régulièrement conservées, d'autre part, que la ou les catégories de données visées, ainsi que la durée pour laquelle l'accès à celles-ci a eu lieu, étaient, au regard des circonstances de l'espèce, limitées à ce qui était strictement justifié par les nécessités de l'enquête.

Si l'accès aurait dû être refusé, la chambre de l'instruction doit prononcer la nullité des réquisitions en cause et des actes subséquents.

A défaut, elle doit constater l'absence d'atteinte aux intérêts de l'intéressé.