Revue générale du droit. Chronique de droit administratif français et comparé, 2021

CE French Data Network et autres, 21 avril 2021 – Perspectives pénales –

Julien Walther[1]

Citer cette publication : Julien Walther, « CE French Data Network et autres, 21 avril 2021 – Perspectives pénales – », Revue générale du droit, Chronique de droit administratif français et comparé, 2021.

[1] Maître de conférences HDR en droit privé et sciences criminelles à l'Université de Lorraine.

Si la décision du Conseil d'Etat French Data networks et autres du 21 avril 2021[2] a attiré l'attention des administrativistes et les constitutionnalistes pour ses enjeux de hiérarchie des normes (et la prudence dont a pu faire montre la haute juridiction administrative face aux tentations de l'*ultra vires more germanico*), il présente également un intérêt certain pour le pénaliste. Cette décision s'inscrit dans un contexte de redéfinition de concepts centraux et de précision de nombreux aspects techniques de la procédure pénale. Partant de la problématique de la conservation des données, elle contribue à analyser le corpus plus général de règles relatives à l'utilisation de celles-ci. Se pose ici d'emblée, la question de la nature des données collectées conservées et échangées. Selon les conclusions du rapporteur public[3], il s'agit des données de connexion ou « métadonnées » à distinguer de celles qui portent sur le contenu des échanges – cette dernière catégorie étant bien connue des juristes pénalistes depuis les années 1990.[4] Elles recouvrent des données d'identité relatives à un numéro de téléphone, un numéro de carte SIM (IMSI), un identifiant de téléphone (IMEI), un numéro d'abonné, une adresse IP ou encore une adresse mail ; d'autres données sont relatives au trafic et portent sur les contacts par téléphone ou SMS (factures détaillées ou « fadettes »), les appareils et cartes SIM utilisés. Enfin pour les échanges via Internet, les données de trafic portent notamment sur l'adresse IP, la liste des sites consultés à partir de cette adresse ou encore l'historique de l'envoi et de la réception de mails. On y compte encore les données de localisation permettent de connaître les zones d'émission et de réception d'une communication passée avec un téléphone mobile identifié, d'obtenir la liste des appels ayant transité par la même antenne relais et même de localiser un portable en veille. Ces métadonnées présentent un intérêt direct pour les enquêteurs en matière

[2] M.-C. de Montecler, Conservation des données : la guerre des juges n'aura pas lieu, *Dalloz actualité,* 26 avril 2021 ; *idem*, Conservation des données : la Cour constitutionnelle belge donne sa lecture, *Dalloz actualité,* 28 avril 2021. Le Conseil d'État maintient la conservation généralisée et indifférenciée des données personnelles par les opérateurs pour les besoins des enquêtes, *Acualités lexisnexis*, 26 avril 2021.

[3] V. Conclusions rapporteur public A. Lallet, p. 2.

[4] V. les arrêts CEDH *Kruslin* et *Huvig* (24 avril 1990) et ses suites en droit national français, la loi du 10 juillet 1991 pour le régime des « écoutes téléphoniques » et ses évolutions ultérieures vers le régime des interceptions de correspondances émises par la voie des communications électroniques (art. 100 et s. CPP)

pénale en ce qu'ils permettent d'identifier les auteurs d'infractions et d'établir la réalité d'infractions pénales dans un nombre croissant de procédures. Il est indiscutable qu'outre les infractions de cybercriminalité au sens strict, des infractions d'autre nature n'ont pu être élucidées sans le recours de plus en plus fréquent à ces techniques.[5] C'est une révolution probatoire qui dépasse celle qu'a pu être en son temps l'ADN.

La décision du Conseil d'Etat donne des indications précieuses sur les obligations de conservation des données en amont de leur utilisation par les autorités pénales (I) et souligne l'application du critère « d'infractions graves » forgé par la CJUE tout en revoyant au juge judiciaire le soin de le préciser (II).

I. Les obligations de conservation des données et leur contexte normatif

Pour une utilisation pratique de ces données se pose la question de leur collecte et de leur conservation, ainsi que de la mise en place de fichiers et la communication de ces données entre les autorités de police et les autorités judicaires, y compris les Etats membres de l'Union européenne.

Les textes applicables aux données utilisées dans le cadre de la procédure pénale sont d'une architecture assez complexe et se trouvent pour le droit national français dans le code de procédure pénale (CPP) ainsi que dans le Code de la Sécurité Intérieure (CSI) et dans le Code des postes et des communications électroniques (CPCE). Ils s'articulent, et c'est l'objet de la décision du Conseil d'Etat commentée, avec des dispositions de droit de l'Union européenne. La question qui nous intéresse est en particulier celle de l'obligation de conservation généralisée et indifférenciée portant sur différentes catégories de (méta)données qui pourrait s'imposer aux fournisseurs sur le fondement des dispositions de l'article 15 de la directive 2002/58 (directive vie privée et communications électroniques ou e-privacy)[6]. C'est ce qui avait été demandé par le Conseil d'Etat à titre

[5] L'on donnera pour exemples récents les développements récents dans les affaires *Noyer*, *Le Tan* ou le bornage des téléphones portables des mis en examen a été un élément clef…

[6] Dir. 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 électroniques

préjudiciel et tranché par la CJUE dans une décision 6 octobre 2020[7]. La CJUE y a précisé en outre que cette directive 2002/58 s'applique aux fournisseurs d'accès à Internet et aux opérateurs de téléphonie mobile, mais non aux hébergeurs, c'est-à-dire aux prestataires qui assurent le stockage sur leurs serveurs des données nécessaires au fonctionnement des sites Internet. Le RGPD s'applique à ces différents acteurs privés.

La directive au cœur de la décision du CE et de la CJUE ne régit pas les traitements subséquents par les autorités publiques qui ont recueilli les données. Il n'y a pas non plus application du RGPD pour les autorités en charge de la procédure pénale.[8] Des dispositions européennes spécifiques existent quant à l'utilisation et au traitement des données personnelles par les autorités judiciaires.[9]

De la même manière, les dispositions règlementaires nationales au cœur de la décision du CE ne concernent pas directement les modalités d'accès

(directive vie privée et communications électroniques). « 1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, **ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales** ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive [95/46]. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

[7] CJUE *La Quadrature du Net*, 6 oct. 2020, aff. C-511/18, *Dalloz actualité*, 13 oct. 2020, obs. C. Crichton ; *AJDA* 2020, p. 1880 ; *D.* 2021, p. 406, et les obs., note M. Lassalle ; *ibid.* 2020. 2262, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *AJ pénal* 2020, p. 531 ; *Dalloz IP/IT* 2021, p. 46, obs. E. Daoud, I. Bello et O. Pecriaux ; *Légipresse* 2020. 671, étude W. Maxwell ; *RTD eur.* 2021, p. 175, obs. B. Bertrand ; *ibid.,* p. 181, obs. B. Bertrand.

[8] Art. 2 d. 2. « Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué : [...] d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. »

[9] Directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

à ces données par l'autorité judiciaire lato sensu, lesquelles ressortent du code de procédure pénale, c'est-à-dire le droit des réquisitions par des OPJ prévu par les articles 60-2, 77-1-2 et 99-4 du CPP pour respectivement l'enquête de flagrance, l'enquête préliminaire et l'instruction – auquel on rajoutera les règles sur la géolocalisation ainsi que celles sur les techniques spéciales d'enquêtes (voir infra). De même pour ce qui est de la structure spécifique pour le traitement des données ainsi obtenues, la Plateforme nationale des interceptions judiciaires ou PNIJ, régie par les articles 230-45 et R. 40-42 à R. 40-56 du CPP.[10] Mais il est évident que ces autorités judiciaires lato sensu ne pourraient opérer efficacement sans une conservation préalable des données par les opérateurs privés.

Cette conservation est prévue à l'article L 34-1 III CPCE ; il s'agit d'une exception à un « principe de non-conservation » des données qui s'impose aux opérateurs de communications électroniques (dont les fournisseurs d'accès Internet et les opérateurs téléphoniques) – plus exactement d'effacement ou d'anonymisation – exception qui repose sur la constatation et la poursuite des infractions pénales. Plus qu'une exception, il s'agit de poser une obligation inverse de conserver ces données dans ces cas précis. Le non-respect de cette obligation est pénalement sanctionné.[11] Le volet règlementaire détaillant cette conservation précise à l'article R 10-3 CPCE quelles sont les données à conserver et la durée de cette conservation. C'est ce volet réglementaire (en plus d'autres dispositions concernant les services de renseignement) qui a fait l'objet du recours pour excès de pouvoir de la part des requérants.

Le Conseil d'Etat a choisi de ne pas mettre en péril le fondement technique et textuel de ces méthodes d'investigation en maintenant la conservation généralisée et indifférenciée de certaines données personnelles par les

[10] La PNIJ est mise en œuvre par l'Agence nationale des techniques d'enquêtes numériques judiciaires. Articles instaurés par décret n° 2014-1162 du 9 oct. 2014 portant création d'un traitement automatisé de données à caractère personnel, dénommé « PNIJ ». V. M. Imbert-Quaretta, *AJ pénal* 2017, p. 318. M. Touillier, Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre, *AJ pénal* 2017, p. 312, T. Lebreton, Investigations et téléphonie mobile, *Gaz. Pal.*, 12 mars 2019, n° 10, p. 15.

[11] L 39-3 CPCE I. « Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents : (…) 2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi. »

opérateurs pour les besoins des enquêtes pénales à partir du moment où des éléments objectifs démontrent qu'existe un lien au moins indirect avec des actes de criminalité grave. Le Conseil d'Etat préserve ainsi les techniques modernes d'investigation qu'il juge indispensables et « sans alternative » réelle – l'exemple des infractions dématérialisées le prouvant aisément (pt. 50). Il applique ici ce que rapporteur public avait décrit comme un « tableau de concordance » posé par la CJUE et contrôle la proportionnalité entre le degré d'ingérence en termes de conservation des données et le seuil de gravité des infractions visées. En conséquence pour le Conseil d'Etat :

-La conservation générale et indifférenciée des données relative à la seule identité civile, aux paiements, aux contrats et aux comptes de l'abonné est possible pour la recherche de toutes les infractions pénales. Cette conservation est possible sans délai particulier (pts. 34 et s.).

-Une obligation de conservation généralisée et indifférenciée des adresses IP peut ainsi être imposée aux opérateurs, dès lors que les conditions d'accès à ces données par les services d'enquête sont fixées en fonction de la gravité des infractions susceptibles de le justifier, dans le respect du principe de proportionnalité et sous le contrôle des juridictions compétentes. L'article R 10-3 du CPCE prévoit une durée de conservation d'un an – ce qui serait compatible avec la condition d'une durée strictement nécessaire posée par la Cour (pts. 37 et s.).

-La question la plus délicate est celle de la conservation généralisée et indifférenciée des données de trafic de localisation autres que les adresses IP. Le cahier des charges de la CJUE est ici plus restrictif. La conservation de telles données serait possible pour lutter contre la criminalité grave en application d'éléments objectifs et non discriminatoires en fonction de catégories de personnes concernées ou de critères géographiques mais le CE souligne la difficulté technique et opérationnelle de la mise en œuvre de cette « conservation ciblée » (et les discriminations qui pourraient poindre). Le Conseil d'Etat met donc en avant et valide la technique de la « conservation rapide » (*quick freeze*) des donnés de trafic et des données de localisation mentionnée à l'article 16 de la Convention du Conseil de l'Europe sur la cybercriminalité (dite de Budapest) du 23 novembre 2001

(technique validée sous conditions par la CJUE dans son arrêt de 2020 pour les infractions graves). Dans l'hypothèse d'une infraction suffisamment grave et sur injonction faite par l'autorité judiciaire aux opérateurs de communications électroniques, la conservation rapide des données de trafic et de localisation est possible. Le délai de conservation est selon les termes de la Convention de Budapest limitée à 90 jours au maximum (renouvelables). La conservation des données de connexion n'est pas permise pour d'autres motifs, notamment pour la recherche des infractions ne relevant pas de la criminalité grave (pts. 32 et 55).

Mais selon le Conseil d'État, le législateur n'est pas obligé d'énumérer par avance les infractions en cause. Le critère de la gravité est donc central et doit être précisé.

II. La gravité des infractions - contours et jalons

Le critère fondamental pour que soient applicables ces constructions est - avec la sécurité nationale - tout d'abord celui de la recherche et de la poursuite d'une infraction pénale. Ce concept d'infraction lui-même n'est pas uniforme et varie d'un Etat-membre à l'autre. La notion d'infraction pénale peut être en conséquence entendue comme une notion autonome du droit de l'Union conforme à l'interprétation de la Cour de justice de l'Union européenne.[12]

Dans quatre décisions du 21 décembre 2016, *Tele2* (C-203/15 et C-698/15), 2 octobre 2018, *Ministerio fiscal* (C-207/16), 6 octobre 2020 précitée ainsi que 2 mars 2021, *H. K. c/ Prokuratuur*, (C-746/18) la CJUE retient au regard de la Charte des droits fondamentaux de l'UE, un critère supplémentaire de gravité qui n'apparait pas dans les textes visés. La directive « vie privée » 2002/58 mentionne simplement « la prévention, la recherche, la détection et la poursuite d'infractions pénales ». Il en va de même pour le RGPD dans son article 23 §1d. Selon la CJUE dans Tele2 (pt. 102), « eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de

[12] C'est ce qui est précisé dans la directive 2016/680, cons. 13.

données relatives au trafic et de données de localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure ». Et la Cour réitère cette affirmation le 6 octobre 2020 (pt. 140) : « Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave…[est] de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation ».

Ce critère supplémentaire « qualitatif » de la gravité des infractions est poreux et nécessitera un travail de définition de la part du juge national.[13] Le Conseil d'Etat reprend ce critère comme clef de voûte de l'articulation de la portée des obligations de conservation des données sans plus le détailler, précisant juste que la qualification se fera sous le contrôle du juge pénal : « le rattachement d'une infraction à la criminalité grave a donc vocation à s'apprécier de façon concrète sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce » (pt. 38). Ce faisant, le juge administratif opère de la même façon qu'a pu le faire le juge constitutionnel en matière de cumul des sanctions fiscales et pénales – une autre zone de contact privilégiée entre le droit administratif et le droit pénal.[14] Ainsi, le cumul est réservé au cas de fraudes fiscales les plus graves et au-delà de quelques critères généraux posés par la Conseil constitutionnel, la Chambre criminelle de la Cour de cassation y a ajouté le jeu des circonstances aggravantes prévues à l'article 1741 CGI.[15]

---

[13] La notion de criminalité grave (*serious crime*) ou d'infraction grave *(serious offence)* est selon les avocats généraux Saugmandsgaard Øe et Giovanni Pitruzzella laissée à l'appréciation des Etats (pt. 93 des conclusions *Ministerio fiscal* et pt. 91 conclusions *HK*).

[14] Cons. const. 24 juin 2016, n° 2016-545 QPC *Dalloz actualité*, 27 juin 2016, obs. J. Gallois ; *D.* 2016, p. 2442, note O. Décima ; *ibid*., p. 1836, obs. C. Mascala ; *ibid.* 2017, p. 1328, obs. N. Jacquinot et R. Vaillant ; *AJ pénal* 2016, p. 430, obs. J. Lasserre Capdeville ; *Constitutions* 2016, p. 361, Décision ; *ibid*., p. 436, chron. C. Mandon ; *RSC* 2016, p. 524, obs. S. Detraz ; 22 juill. 2016, n° 2016-556 QPC, *D.* 2016, p. 1569 ; 23 nov. 2018, n° 2018-745 QPC*, Dalloz actualité*, 4 déc. 2018, obs. P. Dufourq ; *D.* 2018, p. 2237, et les obs. ; *ibid.* 2019, p. 439, point de vue J. Roux ; *Constitutions* 2018, p. 465, Décision.

[15] Crim. 11 sept. 2019, n°18-84.144 ; v. A. Rousseau, Cumul des sanctions pénales et fiscales : quel est le poids du critère de gravité ? *Lexbase Hebdo édition fiscale* n° 841, 29 octobre 2020.

Ce critère de gravité n'est pas une nouveauté au regard des normes prévues par le CPP et la Cour de cassation n'opère pas en terra incognita. Le III de l'article préliminaire du Code de procédure pénale énonce dans son alinéa 6 qu' « au cours de la 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 ». Le contrôle de l'adéquation et la proportionnalité de la mesure à la gravité sont donc posées comme un principe directeur de la procédure pénale française - même si la portée normative de ces principes de l'article préliminaire est discutée, leur rôle comme guide dans l'interprétation des autres dispositions du CPP est reconnu par certains et souligné par la jurisprudence ; pour d'autres auteurs, l'article préliminaire aurait une fonction récapitulative ou pédagogique.[16] Notons que cette disposition est expressément visée par le Conseil d'Etat dans la décision étudiée (n° 39).

Mais quelle sera l'aune pour éprouver cette gravité ? Quels jalons guident le juge pénal ? Il semble bien que le droit positif fournisse déjà bon nombre d'éléments.

Dans une perspective européenne - et de transposition en conséquence dans le système français - il est plausible que le critère de la compétence pénale de l'UE au sens de l'article 83 du TFUE puisse trouver à s'appliquer ici. Les crimes et délits mentionnés au § 1er (le terrorisme, la traite des êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée), les infractions visées dans des directives nées de l'application du § 2 et leurs déclinaisons nationales pourraient donc toujours être des infractions graves selon la logique même des textes du droit de l'UE. Dans sa communication de 2011, la Commission mentionnait expressément la gravité comme un des critères

[16] Voir pour une synthèse des différents positions, E. Vergès, Art. préliminaire - Fasc. 20 : principes directeurs du procès pénal. – Origine et force normative des principes directeurs, Jurisclasseur procédure pénale, 2019.

de la compétence pénale de l'UE.[17] Peuvent être lues en ce sens, au moins partiellement les conclusions de l'avocat général pour la décision Tele 2 Sverige « 182. Lors de la présentation de la proposition de directive ayant conduit à l'adoption de la directive 2006/24, la Commission a illustré cette utilité à l'aide de plusieurs exemples concrets d'enquêtes portant notamment sur des actes de terrorisme, de meurtre, d'enlèvement et de pédopornographie.[18]» Pour la Cour européenne des droits de l'homme, certaines mesures d'investigation sont subordonnées à des conditions de prévisibilité et de proportionnalité ; ainsi la collecte de données au moyen du GPS ont été reconnues comme conformes à l'article 8 CEDH parce que la loi allemande en limite l'usage à des « infractions extrêmement graves » (*besonders schwere Straftat*)[19] - en l'occurrence dans l'affaire Uzun de 2010, la qualification visée était celle de terrorisme. Il s'agit de dispositions introduites dans le CPP allemand par une loi de 1992 destinée à lutter contre la criminalité organisée et le trafic de stupéfiant (§ 100c StPO). On y retrouve les infractions terroristes mentionnées dans la décision du Conseil d'Etat.

Partant du droit français, il est évident que la gravité au regard du seul droit français ne saurait relever de la simple classification tripartite telle qu'elle est posée par l'article 111-1 du CP. Le droit européen ne peut nous éclairer ici, bon nombre de pays connaissant d'autres classifications des infractions. S'il est clair que seront considérées comme graves des infractions de nature criminelle et trop bénignes les contraventions, il semble indispensable que tombent sous le coup de cette qualification certains délits. C'est là l'enjeu primordial de la classification par la gravité. Le seul jeu d'une circonstance aggravante prévue par un texte d'incrimination ne saurait justifier de la gravité suffisante au regard des exigences des cours – cela pour écarter toute tautologie ou tout raisonnement circulaire. On peut supposer que certaines circonstances

[17] Vers une politique de l'UE en matière pénale : assurer une mise en œuvre efficace des politiques de l'UE au moyen du droit pénal COM(2011) 573 final, p. 12.
[18] *Commission Staff Working Document* présenté en annexe à la proposition de directive ayant conduit à l'adoption de la directive 2006/24, SEC(2005)1131, 21 septembre 2005, n° 1.2, « The importance of traffic data for law enforcement ».
[19] CEDH, 2 sept. 2010, n° 35623/05, *Uzun c/ Allemagne*, *D.* 2011, p. 724, obs. S. Lavric, note H. Matsopoulou ; *RSC* 2011, p. 217 et s., obs. D. Roets.

aggravantes seront à leur tour écartées car trop « légères ». Il doit s'agir pour respecter le raisonnement fondé sur le contrôle de la proportionnalité, d'une gravité « qualifiée ». Quels seraient alors les délits suffisamment graves pour tomber sous le coup de l'exception visée par le CE ? Une série d'éléments permettent de donner des pistes sérieuses en ce sens.

Les infractions relatives à la sécurité nationale devraient tomber dans cette catégorie et l'on renverrait au Titre I et II du Livre IV du Code pénal puisqu'il y aurait conjonction ou adéquation avec l'objectif de fins de sauvegarde de la sécurité nationale et de lutte contre le terrorisme (en ce sens le pt. 43 de la décision étudiée). L'on peut penser que les infractions prévues par les articles 706-73 et 706-73-1 du CPP présentent également ce seuil de gravité suffisant.[20] Il est parfois question en doctrine du « cadre » ou du « répertoire ajouté » ou de la « procédure pénale bis ».[21] La liste de ces infractions[22] s'est allongée avec la loi du 28 février 2017, et d'aucuns ont remis en cause l'accessibilité et la prévisibilité de cette catégorie.[23] Ces infractions relèvent du régime procédural dérogatoire mis en place par la loi Perben II du 9 mars 2004 et dont l'arsenal n'a cessé d'être augmenté régulièrement. Elles sont, selon un auteur, "graves" par nature, « soit parce que, bien que relevant du droit commun, elles sont commises en bande organisée, soit parce qu'elles s'inscrivent "naturellement" dans une organisation comme les trafics de stupéfiants important, les faits de proxénétisme et de traite des êtres humains ».[24] Elles ressortent plus généralement de la criminalité organisée, de la criminalité économique et du terrorisme. Corrélativement, les pouvoirs d'investigations portant sur des techniques et données numériques qui sont au cœur de nos interrogations sont réservés aux procédures relatives

[20] T. Meindl, art. 706-73 à 706-106, fasc. 20 : procédure applicable à la criminalité et la délinquance organisées, *jurisclasseur procédure pénale,* 2020.
[21] Voir C. Lazerges, La dérive de la procédure pénale, *RSC* 2003, p. 644 et s. ; S. Guinchard/J. Buisson, *Procédure pénale*, LexisNexis, 2020, p. 689 et s.
[22] On dénombre vingt types d'infractions pour lesquelles la procédure dérogatoire au droit commun peut s'appliquer énumérées dans l'art. 706-73 et s'y ajoutent les infractions majoritairement économiques de 706-73-1.
[23] V. J.-C. Saint-Pau, Les investigations numériques et le droit au respect de la vie privée, *AJ pénal* 2017, p. 321.
[24] T. Meindl, réf, précitée, n° 7.

à ces mêmes infractions au titre des techniques spéciales d'enquête. Il en va ainsi des arts. 706-95 et s. CPP (accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique), en particulier les articles 706-95-20 et s. CPP pour le recueil de données techniques de connexion et les articles 706-102-1 et s. pour la captation des données informatiques. L'article 706-95-11 CPP limite l'application des techniques spéciales d'enquêtes aux infractions « d'une particulière gravité et complexité », selon les termes du Conseil constitutionnel dans sa décision du 21 mars 2019.[25]

Le critère de la complexité va pouvoir souvent s'agréger à celui de la gravité, allant dans le sens de la décision du Conseil d'Etat étudiée qui mentionne outre « la nature de l'infraction commise », la prise en compte de « l'ensemble des faits de l'espèce ».

Pour l'application des textes procéduraux de droit commun, la chambre criminelle a déjà eu l'occasion de se prononcer sur le critère de la gravité. En 2013, pour ce qui est de la réquisition des données de géolocalisation au titre notamment de l'article 77-1-1 CPP, la chambre criminelle jugeait dans des affaires de terrorisme et de trafic de stupéfiants que la géolocalisation constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge, et non pas seulement du procureur de la République (dans la même affaire était également visé l'art. L. 34-1 du code des postes et télécommunications, des réquisitions avaient été envoyées à des opérateurs aux fins d'obtenir des renseignements en leur possession relatifs à des adresses électroniques).[26] En conséquence était adoptée la loi du 28 mars 2014 sur la géolocalisation[27]: l'article 230-32 du CPP n'autorise ces mesures que pour les crimes et délits punis d'au moins 3 ans d'emprisonnement. On pourrait y déceler un plancher de « gravité qualifiée » dans le contexte de la collecte des métadonnées – ce seuil de 3 ans est d'ailleurs retenu pour

[25] Cons. const., 21 mars 2019, n° 2019-778 DC : JurisData n° 2019-004275.
[26] Cass. crim., 22 oct. 2013, n° 13-81945 : Bull. crim., n° 196 ; Cass. crim., 22 oct. 2013, n° 13-81949 : Bull. crim., n° 197.
[27] J. Buisson, la géolocalisation enfin prévue par une loi…, *Procédures* 2014, Étude n° 10 ; T. Lebreton, investigations et téléphonie mobile, *Gaz. Pal.* 12 mars 2019, p. 15 ; P. Valat, la loi du 28 mars 2014 relative à la géolocalisation, *Dr. pénal* 2014, Étude n° 12.

d'autres mesures d'enquête (perquisitions contraintes en enquête préliminaire et interceptions télécommunications judiciaires, articles 76 et 100 CPP). La chambre criminelle se prononçant sur des écoutes téléphoniques et une éventuelle violation de l'article 8 de la CEDH y conclut que la gravité de l'infraction est, selon un commentateur, « un critère d'importance, mais non exclusif, dans l'appréciation de la nécessité de l'ingérence et du besoin social impérieux. »[28]

S'ajoute à ces catégories un dernier élément tiré des compétences *rationae materiae* des juridictions interrégionales spécialisées (JIRS) ou du Tribunal judiciaire de Paris et du Parquet National Financier (PNF) : selon les articles 704 et 705 du CPP, les infractions d'une grande complexité sont du ressort des JIRS ou du Tribunal judiciaire de Paris et les infractions qu'on y trouve sont souvent celles que l'on retrouve dans la liste des articles 706-73 et s CPP.

En recoupant ces différents éléments, les critères de gravité et de complexité semblent déjà largement applicables et appliqués en droit positif – le renvoi au juge criminel ne devrait pas être un exercice insondable mais un travail de précision et de consolidation de l'édifice normatif existant.

[28] F. Fourment, Des écoutes en règle !? comm. ss. Cass. crim., 8 juill. 2015, n° 15-81731, *Gaz. Pal.*, 3 nov. 2015, n° 245h3, p. 40.