La conservation et l'accès aux métadonnées dans le cadre des enquêtes judiciaires: vers un bouleversement dans la procédure pénale française ?

Matthieu Audibert

Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales, Assemblée nationale, 29 avril 2014, p. 77 [en ligne].
[31] Circulaire du 23 mai 2014, *op. cit.*, p. 9, note de bas de page n° 15.
[32] Commission relative aux droits de la défense dans l'enquête pénale et au secret professionnel de l'avocat, « Le renforcement de l'équilibre des enquêtes préliminaires et du secret professionnel de l'avocat », 29 p.

Procédure pénale

[Jurisprudence] La conservation et l'accès aux métadonnées dans le cadre des enquêtes judiciaires : vers un bouleversement dans la procédure pénale française ?

Réf. : CJUE, 2 mars 2021, aff. C-746/18, Prokuratuur (N° Lexbase : A49864II)

N6851BYE

par Matthieu Audibert, officier de gendarmerie et doctorant en droit privé et sciences criminelles (Université Paris Nanterre – CDPC – EA 3982)
Le 24-03-2021

Mots-clés : Cour de justice de l'Union européenne (CJUE) • métadonnées, proportionnalité • preuve numérique • vie privée • procureur de la République • juge d'instruction • enquêtes judiciaires

Dans la continuité de ses arrêts rendus depuis 2014 [1], la CJUE poursuit l'encadrement des dispositifs juridiques liés à la conservation [2] et maintenant à l'accès, à des fins pénales, aux données de localisation et de trafic (métadonnées) des utilisateurs. La CJUE pose ensuite un certain nombre de garanties liées à cet accès qui mettent à mal les prérogatives du procureur de la République et, par ricochet, certaines prérogatives du juge d'instruction au regard de la Directive n° 2002/58/CE, du Parlement européen et du Conseil (N° Lexbase : L6515A43), du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne (UE).

H.K, ressortissante estonienne, a été condamnée en première instance à une peine privative de liberté pour avoir commis plusieurs vols, escroqueries et exercé des actes de violences. Pour la déclarer coupable, la juridiction de jugement s'est fondée sur différents actes réalisés par les services d'enquête et notamment l'obtention de données relatives aux communications électroniques (métadonnées) sur autorisation du parquet. En effet, le droit estonien impose aux opérateurs de communications électroniques que les métadonnées relatives à la téléphonie mobile et fixe soient conservées de manière généralisée et indifférenciée pendant une durée d'un an. Ces données sont accessibles par les autorités publiques pour prévenir, rechercher, détecter et poursuivre les auteurs d'infractions pénales.

Condamnée en première instance et en appel, H.K introduit alors un pourvoi en cassation contre cette décision auprès de la Cour suprême de son pays. Cette dernière va alors demander à la CJUE son interprétation de l'article 15, § 1 de la Directive n° 2002/58, du 12 juillet 2002, concernant le traitement et l'accès aux métadonnées au regard de la protection de la vie privée.

La CJUE va préciser que cet accès doit être « circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention des menaces graves contre la sécurité publique [3] » (**I**).

La CJUE va également indiquer que le droit de l'Union[4] s'oppose à ce que le ministère public puisse autoriser l'accès aux enquêteurs aux métadonnées. Cet aspect de l'arrêt implique de nombreuses conséquences pour le parquet français mais également par ricochet le juge d'instruction (**II**).

I . La notion de criminalité grave ou de menace grave contre la sécurité publique comme seul critère autorisant l'accès aux autorités publiques aux métadonnées

Ce nouvel arrêt de la CJUE reprend une solution qui n'est pas nouvelle (**A**). Toutefois, combiné à l'arrêt « Quadrature du Net », ce nouvel arrêt est susceptible d'entraîner de lourdes conséquences dans la réussite de nombreuses enquêtes judiciaires (**B**).

A . Une confirmation de la jurisprudence « Quadrature du Net » s'agissant de la conservation des métadonnées pour en préciser les modalités d'accès

La CJUE commence par rappeler sa jurisprudence antérieure. Tout d'abord, elle subordonne l'accès à ces données à leur conservation de manière conforme au droit de l'Union [5]. Ce dernier s'oppose à des législations nationales prévoyant à des fins pénales, à titre préventif, la conservation généralisée et indifférenciée des métadonnées [6] [7].

Ensuite, la Cour se livre à un contrôle de proportionnalité s'agissant de l'accès à ces données entre, d'une part, la gravité de l'ingérence dans les droits fondamentaux et, d'autre part, l'objectif d'intérêt général poursuivi [8] [9]. Ainsi « seule la lutte contre la criminalité et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés [par la Charte] [10] ». Ces ingérences sont notamment celles qui « impliquent la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée. [11]»

La CJUE conclut que « seules des ingérences ne présentant pas un caractère grave peuvent être justifiées par l'objectif [...] de prévention, de recherche, de détection et de poursuite d'infractions pénales en général [12]». Il est intéressant de noter qu'elle opère ensuite une distinction avec les données relatives à l'identité civile des utilisateurs non associées aux métadonnées. Pour les premières, celles-ci ne permettant pas, à elles seules, de connaitre les usages de l'utilisateur ou encore sa localisation, la CJUE considère que leur conservation n'est pas en contradiction avec le droit de l'Union [13]. On retrouve la même solution dans la jurisprudence de la Cour européenne des droits de l'Homme (CEDH) [14] [15].

Dans la suite de son raisonnement, la CJUE considère l'accès restreint à une quantité limitée de données de connexion comme étant un critère inopérant pour justifier une telle ingérence [16].

S'agissant des conséquences procédurales, le juge doit exclure les éléments de preuve si les personnes poursuivies « 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 [17]».

Pour conclure, la CJUE écarte donc les critères liés à la durée de l'accès aux données et à la nature des données disponibles pour conclure que le droit de l'Union [18] n'autorise l'accès, dans le cadre des enquêtes judiciaires, aux métadonnées, permettant de tirer des conclusions sur la vie privée des personnes visées par les investigations, que dans le cadre de la lutte contre la criminalité grave ou pour prévenir des menaces graves contre la sécurité publique [19].

Enfin, dans l'argumentaire du Gouvernement estonien, il est intéressant de souligner que l'accès aux données conservées en vertu du droit national estonien peut être sollicité pour tout type d'infraction pénale [20]. Ce qui est également le cas du droit français [21].

B. Quelles implications pour les enquêtes judiciaires ?

Avant tout, il convient de distinguer données de contenu et métadonnées. Les premières contiennent les paroles prononcées ou écrites et les secondes les informations relatives à la connexion des appareils aux réseaux téléphoniques ou à Internet.

Les interceptions de correspondances émises par la voie des communications électroniques[22] sont possibles dans le cadre d'une information judiciaire en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement [23]. S'agissant de l'enquête de flagrance et de l'enquête préliminaire, les interceptions de correspondances sont possibles pour l'une des infractions entrant dans le champ d'application des articles 706-73 (**N° Lexbase : L2154LHA**) et 706-73-1 du Code de procédure pénale (**N° Lexbase : L8161LS3**) [24]. Il y a donc un critère lié à la gravité, soit en raison de la typologie de l'infraction soit en raison de la peine encourue.

En revanche, que ce soit en enquête de flagrance[25], en enquête préliminaire[26] ou dans le cadre d'une information judiciaire [27], aucun seuil n'est exigé s'agissant de la possibilité de requérir les opérateurs de communications électroniques aux fins de récupérer des métadonnées. Il est donc possible de solliciter ces métadonnées aussi bien pour une contravention que pour un délit ou un crime. Cette différence de traitement entre ces deux types de données se justifie aisément. Les premières portent sur les propos ou écrits échangés et les secondes sur les informations techniques

relatives à la connexion des appareils aux différents réseaux. Le niveau d'intrusion dans la vie privée de la personne objet des investigations est donc sensiblement différent.

L'apport de l'arrêt du 2 mars 2021 réside dans la limitation de l'accès aux métadonnées à des fins pénales dans les seuls objectifs de lutte contre la criminalité grave ou de prévention des menaces graves contre la sécurité publique. Or réduire l'accessibilité de ces données aux seules infractions pénales graves est difficilement concevable pour les services d'enquête notamment parce que la notion « d'infraction grave » exclut de nombreuses possibilités d'investigations alors que plus de 85 % des enquêtes judiciaires s'appuient sur ces données [28]. Le recours aux métadonnées est aujourd'hui un acte d'investigation ordinaire auquel les enquêteurs ont recours pour toutes les affaires, qu'il s'agisse de l'identification du mis en cause, la démonstration de sa participation à l'infraction ou encore l'identification de complices.

Ainsi, la majorité des métadonnées exploitées par les services d'enquête le sont dans le cadre de la lutte contre la criminalité et surtout contre la délinquance par opposition à la notion de « criminalité grave » énoncée par la CJUE mais non définie en droit français. En droit interne, cette notion de gravité est déterminée en fonction de la classification crime, délit, contravention avec pour chacune des infractions une échelle de sanctions spécifiques [29]. Ainsi, un crime est par nature nécessairement grave. Or s'agissant des délits, la liste des infractions potentiellement concernées par un accès prohibé aux métadonnées est extrêmement longue.

C'est le cas par exemple des infractions pouvant être exclusivement commises par la voie des communications électroniques : infractions relatives à la vie privée [30], cyberharcèlement [31], provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance à une ethnie, une nation, une race ou à une religion déterminée [32], la provocation à la haine ou à la violence à raison du sexe ou de l'orientation sexuelle, de l'identité de genre ou du handicap et provocation à des discriminations les concernant [33].

Ces infractions sont-elles graves ? Les sanctions prévues pour celles-ci varient entre un an et deux d'emprisonnement. L'application stricte de l'arrêt de la CJUE empêcherait donc le recours aux métadonnées pour enquêter sur des infractions de haine en ligne. Or ces données sont absolument essentielles pour élucider de tels faits. Ainsi « l'inquiétude pèse tant sur les procédures en cours que sur l'avenir des moyens d'enquêtes [34]».

Réserver l'accès aux métadonnées à certaines infractions présuppose une dichotomie entre infractions graves et infractions mineures, alors même qu'il y a rarement d'étanchéité entre les infractions et que les analyses de données téléphoniques réalisées à l'occasion d'infractions mineures permettent souvent de dévoiler des faits graves ou de caractériser la criminalité organisée [35]. Une réduction drastique du champ de conservation des métadonnées et des possibilités d'y accéder méconnaît donc les processus d'investigations.

De plus, au début d'une enquête, il est impossible de déterminer une zone délimitée qui pourrait être celle de l'auteur des faits et de ses éventuels complices. Il est impossible pour les magistrats et les enquêteurs de connaître à l'avance les données dont ils auront besoin pour élucider les enquêtes qu'ils mènent. Enfin comment déterminer à l'avance l'identité des personnes qui feront l'objet d'investigations [36], à charge comme à décharge ? Ainsi « plus que le dispositif national, ce sera peut-être la méthodologie d'enquête qui devra être revue [37] ».

Enfin, l'arrêt de la CJUE faisant suite à une question préjudicielle[38], il appartient à la juridiction nationale qui a saisi la Cour de résoudre l'affaire conformément à la décision de la CJUE. En outre, cette décision lie les autres juridictions nationales des pays de l'Union européenne qui seraient saisies d'un problème similaire. La combinaison des arrêts « Quadrature du Net » et « Prokuratuur » est donc susceptible de remettre profondément en cause les méthodes actuelles d'enquêtes judiciaires [39] [40].

II. L'exclusion du ministère public dans le contrôle préalable de certains actes d'enquêtes : un bouleversement à venir dans la procédure pénale française ?

Au regard de l'article 15, paragraphe 1, de la Directive n° 2002/58 et de l'arrêt « Tele2 » du 21 décembre 2016, le ministère public est-il compétent pour autoriser l'accès aux métadonnées ? Par sa réponse, la CJUE remet en cause le ministère public français (**A**) et indirectement les pouvoirs d'enquête du juge d'instruction (**B**).

A. Une remise en cause du ministère public français

S'agissant du ministère public estonien, la CJUE relève qu'il est « tenu d'agir de manière indépendante », il doit « examiner les éléments à charge et à décharge lors de la procédure d'instruction, l'objectif de cette procédure [étant] la collecte d'éléments de preuve ainsi que la réunion des autres conditions nécessaires à la tenue d'un procès », il « représente l'action publique lors du procès et [...] serait donc également partie à la procédure ». Enfin, il « est organisé de manière hiérarchique » [41].

Tout d'abord, la CJUE relève que la loi estonienne donne au parquet un accès général à toutes les données sans préciser l'objectif poursuivi [42], ces dispositions ne respectant pas l'exigence de proportionnalité[43]. Ensuite, elle indique « que l'accès des autorités nationales compétentes aux données conservées [doit être] subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité [doit intervenir] à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales [44] ». Elle précise enfin que la juridiction ou l'entité de contrôle « [doit disposer] de toutes les attributions et [doit présenter] toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause [45] ». Dès lors cette juridiction ou entité de contrôle doit avoir « une position de neutralité vis-à-vis des parties à la procédure pénale [46] ».

Dans la mesure où le ministère public estonien dirige l'enquête mais est également susceptible d'exercer l'action publique, la CJUE en conclut que celui-ci ne peut être considéré comme indépendant : il n'a pas la qualité de tiers à la procédure, notamment vis-à-vis des enquêteurs qui demandent l'accès aux données, et il peut faire l'objet d'une influence extérieure [47]. Enfin, la CJUE insiste pour rappeler qu'un contrôle de l'accès postérieur n'est pas suffisant car il doit intervenir dans les plus brefs délais, « préalablement à tout accès, sauf cas d'urgence dûment justifié [48] ».

À la lumière de cet arrêt de la CJUE, il convient d'examiner les caractéristiques du parquet français. En France, la police judiciaire est exercée sous la direction du procureur de la République [49]. Il exerce l'action publique dans le respect du principe d'impartialité [50], il ne prend donc pas parti dans les enquêtes. Toutefois, c'est lui qui dispose du principe de l'opportunité des poursuites [51] et peut le cas échéant mettre en œuvre l'action publique et requérir une condamnation [52]. Enfin, le procureur de la République est placé sous l'autorité du procureur général près la cour d'appe[53].

Sur ces points, la CJUE a fait preuve de clarté[54] : le droit de l'Union s'oppose à une législation nationale qui donne compétence au ministère public, qui dirige l'enquête judiciaire et exerce, le cas échéant, l'action publique, pour autoriser l'accès aux enquêteurs aux données de connexion.

Or, en droit français, dans le cadre de l'enquête de flagrance, le procureur de la République ou l'officier de police judiciaire et l'agent de police judiciaire sous le contrôle de ce dernier peuvent, par réquisition, récupérer les métadonnées intéressant une enquête en cours [55]. En enquête préliminaire, le procureur et, sur autorisation de celui-ci, l'officier ou l'agent de police judiciaire, peuvent également récupérer ces métadonnées, toujours par réquisition [56]. Le contrôle préalable n'existe donc que dans le cadre de l'enquête préliminaire. En pratique, il existe aussi en enquête de flagrance dans la mesure où il s'agit de réquisitions facturées au titre des frais de justice [57].

Ainsi en enquête de flagrance ou préliminaire, aucun tiers à la procédure, tel un juge des libertés et de la détention, n'intervient pour autoriser cet accès. Seul le procureur de la République exerce ce contrôle. Or du fait de son positionnement, il y a, d'une part, une problématique s'agissant du contrôle préalable [58] tel qu'exigé par la CJUE et, d'autre part, une question d'indépendance dans la mesure où c'est le procureur qui exerce le cas échéant l'action publique à l'issue de l'enquête qu'il dirige.

Le parquet français est donc clairement menacé par l'arrêt de la CJUE du 2 mars 2021, tant en raison de son positionnement dans la procédure qu'en raison de ses attributions propres.

B. Un impact indirect mais réel sur les pouvoirs d'enquête du juge d'instruction

A priori, le juge d'instruction ne semble pas impacté par cet arrêt de la CJUE. Toutefois, certains points de l'arrêt sont susceptibles de le concerner.

Il ne représente pas l'action publique. Son rôle est d'instruire à charge et à décharge et de procéder à tous les actes d'enquête qu'il juge utile à la manifestation de la vérité [59]. Il peut procéder lui-même à ces actes ou les déléguer aux officiers de police judiciaire par le biais de commissions rogatoires [60]. À cet effet, les officiers de police judiciaire exercent, dans les limites de la commission rogatoire, tous les pouvoirs du juge d'instruction [61].

S'agissant des métadonnées, le juge d'instruction ou l'officier de police judiciaire commis par lui peut, par réquisition, récupérer les métadonnées intéressant une enquête en cours [62]. Or ce pouvoir d'enquête précis va rentrer en contradiction avec l'arrêt de la CJUE. Celle-ci explique en substance que l'autorité qui exerce le contrôle préalable ne peut être la même que celle qui sollicite l'accès aux métadonnées. L'autorité de contrôle ne doit pas être impliquée dans la conduite de l'enquête pénale [63].

Lorsque le juge d'instruction ou l'officier de police judiciaire requiert en vertu de l'article 99-3 du Code de procédure pénale (**N° Lexbase : L4947K8Q**), aucune entité ne contrôle préalablement sa réquisition. Seule une nullité nécessairement postérieure pourra, le cas échéant, être soulevée [64]. Par-dessus tout, le juge d'instruction est impliqué dans l'enquête car c'est justement son rôle d'informer à charge et à décharge [65]. La CJUE indiquant que le droit de l'Union « s'oppose à une réglementation nationale donnant compétence au ministère public dont la mission est de diriger

la procédure d'instruction pénale [...] pour autoriser l'accès d'une autorité publique aux données [de connexion] aux fins d'une instruction pénale [66] », nous pouvons donc en déduire que l'article 99-3 du Code de procédure pénale semble contraire au droit de l'Union.

Par extension, le raisonnement pourrait également s'appliquer aux interceptions de correspondances bien que non concernées par cet arrêt. En effet, en enquête de flagrance et en enquête préliminaire, celles-ci sont autorisées par le juge des libertés et de la détention (JLD) [67]. Toutefois, dans le cadre de l'information judiciaire, le JLD n'intervient pas [68]. Il serait paradoxal que les métadonnées fassent l'objet d'un traitement plus strict et plus protecteur pour la vie privée que les données de contenu, objets des interceptions. Pour ces raisons, cet arrêt de la CJUE menace par ricochet les pouvoirs d'enquête du juge d'instruction.

Enfin, il convient de se demander si la jurisprudence de la CJUE n'a pas pour objet d'inciter les États membres à tendre vers la création d'un juge de l'enquête : magistrat non impliqué dans la procédure qui serait uniquement chargé, à la demande des enquêteurs, du procureur de la République ou du juge d'instruction pourtant indépendant, d'autoriser certains actes attentatoires à des droits ou libertés. Il s'agirait alors d'un basculement majeur dans notre procédure pénale et dans notre organisation judiciaire. Cela soulèverait de nombreuses questions capacitaires considérant d'une part les flux de réquisitions à absorber et d'autre part la nécessité de les traiter rapidement eu égard aux impératifs opérationnels.

---

[1] CJUE, 8 avril 2014, aff. C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e.a. (**N° Lexbase : A7603MIG**) ; CJUE, 21 décembre 2016, aff. C-203/15 et C-698/15, Tele2 Sverige (**N° Lexbase : A7089SXT**) ; CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a. c/ Premier ministre e.a. (**N° Lexbase : A78303WW**).
[2] M. Lassalle, *Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE,* D., 2021, p. 406
[3] Point 60, 1.
[4] Directive (CE) n° 2002/58 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, art. 15 §1 (**N° Lexbase : L6515A43**) ; Charte des droits fondamentaux, art. 7, 8, 11 et 52 (**N° Lexbase : L8117ANX**).
[5] Point 29. Voir aussi CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., point 167.
[6] Point 30. Voir aussi CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., point 168.
[7] M. Lassalle, *Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE,* D., 2021, p.406
[8] Points 31 et 32.
[9] CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., point 131.
[10] Points 33.
[11] *Ibid*.
[12] *Ibid*. Voir aussi CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., points 140 et 146.
[13] Point 34. Voir aussi CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., points 157 et 158.
[14] CEDH, 30 janvier 2020, Req. 50001/12, Brayer c/ Allemagne, 30 janvier 2020.
[15] M.-C. de Montecler, *Protection des données : la CJUE infléchit sa jurisprudence*, AJDA, 2020, p.1880.
[16] Point 40.
[17] Point 44.
[18] Directive (CE) n° 2002/58 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, art. 15, § 1 ; Charte des droits fondamentaux, art. 7, 8, 11 et 52.
[19] Point 45.
[20] Point 28.
[21] CPCE, art. L. 34-1 (**N° Lexbase : L0413IZC**) et R. 10-13 (**N° Lexbase : L6792ISD**) et dispositions du Code de procédure pénale, voir par exemple C. proc. pén., art. 60-1 (**N° Lexbase : L7424LPN**).
[22] Données de contenu.
[23] C. proc. pén., art. 100 (**N° Lexbase : L7405LPX**).
[24] Infractions relatives à la criminalité et à la délinquance organisées.
[25] C. proc. pén., art. 60-1.
[26] C. proc. pén., art. 77-1-1 (**N° Lexbase : L5533LZX**).
[27] C. proc. pén., art. 99-3 (**N° Lexbase : L4947K8Q**).
[28] A. Vitard, *Pourquoi la France entame-t-elle un bras de fer avec l'Europe sur la conservation des métadonnées ?,* L'Usine digitale, 16 mars 2021 [en ligne].
[29] C. pén., art. 111-1 (**N° Lexbase : L1759AM4**).
[30] C. pén., art. 226-1 et s. (**N° Lexbase : L8546LXS**).

[31] C. pén., art. 222-33-2-2 (N° Lexbase : L6228LLA).
[32] Loi du 29 juillet 1881 relative à la liberté de la presse, art. 24 (N° Lexbase : L7589AIW).
[33] *Ibid*.
[34] B. Nicaud, *CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données*, AJ pénal, 2020, p.531.
[35] F. Molins, *La protection des citoyens européens dans un monde ultra-connecté,* Fondation Robert Schuman, Question d'Europe n° 510, 8 avril 2019 [en ligne].
[36] *Ibid*.
[37] B. Nicaud, *CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données*, AJ pénal, 2020, p.531.
[38] TUE, art. 267 (N° Lexbase : L2581IPB).
[39] E. Daoud, I. Bello, O. Pecriaux, *Données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle,* Dalloz IP/IT, 2021, p.46.
[40] B. Nicaud, *CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données*, AJ pénal, 2020, p.531.
[41] Point 47. Voir également C. Crichton, *Précisions sur l'accès aux métadonnées lors du procès pénal*, Dalloz actualité, 5 mars 2021 [en ligne].
[42] Points 49 et 50.
[43] *Ibid*.
[44] Point 51. Voir également CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a, point 189.
[45] Point 52.
[46] Point 54.
[47] Points 54-57.
[48] Point 58.
[49] C. proc. pén., art. 12 (N° Lexbase : L7228A4H) et 41 (N° Lexbase : L7391LPG).
[50] C. proc. pén., art. 31 (N° Lexbase : L4927IXR).
[51] C. proc. pén., art. 40 (N° Lexbase : L5531DYI).
[52] C. proc. pén., art. 40-1 (N° Lexbase : L7457LBS).
[53] C. proc. pén., art. 35 (N° Lexbase : L4928IXS) à 37 (N° Lexbase : L5530DYH).
[54] Point 60, 2).
[55] C. proc. pén., art. 60-1.
[56] C. proc. pén., art. 77-1-1 (N° Lexbase : L5533LZX).
[57] C. proc. pén., art. A. 43-9 (N° Lexbase : L8850LUC).
[58] Pour l'enquête de flagrance considérant la rédaction de l'article 60-1 du Code de procédure pénale.
[59] C. proc. pén., art. 81 (N° Lexbase : L9490LP8).
[60] C. proc. pén., art. 151 (N° Lexbase : L3525AZL).
[61] C. proc. pén., art. 152 (N° Lexbase : L5551DYA).
[62] C. proc. pén., art. 99-3 (N° Lexbase : L4947K8Q).
[63] Point 54.
[64] C. proc. pén., art. 170 (N° Lexbase : L0918DYN).
[65] C. proc. pén., art. 81.
[66] Point 59.
[67] C. proc. pén., art. 706-95 (N° Lexbase : L0578LTL).
[68] C. proc. pén., art. 100 (N° Lexbase : L7405LPX).

Procédure pénale

[Brèves] Géolocalisation : la Chambre criminelle juge l'appréciation de l'existence d'une localisation en temps réel sur un territoire étranger

Réf. : Cass. crim., 2 mars 2021, n° 20-84.004, F-P+I (N° Lexbase : A49964IU)

N6945BYU