PREMIER CONCOURS D'ACCÈS

À L'ÉCOLE NATIONALE DE LA MAGISTRATURE

SESSION 2024

Jeudi 30 mai 2024

Quatrième épreuve d'admissibilité : 5h (coefficient 3)

NOTE DE SYNTHÈSE À PARTIR DE DOCUMENTS SE RAPPORTANT À DES PROBLÈMES JUDICIAIRES, JURIDIQUES OU ADMINISTRATIFS

Rédigez, à partir des documents joints, une note de synthèse de quatre pages environ sur la protection des données personnelles de connexion

Tournez la page S.V.P.

Liste de documents :

Document n° 1 : Règlement général sur la protection des données du 24 mai 2016 (extraits)

Document n° 2 : Loi du 20 juin 2018 relative à la protection des données personnelles, *site vie publique le 22 juin 2018*

Document n° 3 : Arrêt rendu par la Cour de cassation, Chambre criminelle, 12 juillet 2022, 21-83.820, Publié au bulletin

Document n° 4 : Protection des données dans l'Union Européenne, *site internet de la Commission européenne, 05 avril 2024*

Document n° 5 : La protection des données personnelles dans les relations internes à l'Union européenne par Céline CASTETS-RENARD, Professeur de droit privé, Université Toulouse-I-Capitole, Membre de l'Institut Universitaire de France (IUF), Codirectrice de l'IRDEIC Centre d'Excellence Jean-Monnet, Directrice du Master Droit du Numérique, Visiting Professor, Fordham Law School (NY) in Répertoire de droit européen, octobre 2018

Document n° 6 : Communiqué de presse n° 29/21 de la Cour de justice de l'Union européenne, Luxembourg, le 2 mars 2021 - Arrêt dans l'affaire C-746/18 H. K/Prokuratuur

Document n° 7 : Communiqué de presse de la Cour de cassation du 12 juillet 2022
Enquêtes pénales : conservation et accès aux données de connexion

Document n° 8 : Recueil Lebon - Recueil des décisions du Conseil d'Etat 2021, Données de connexion : validation de l'obligation de conservation, décision du Conseil d'Etat – Assemblée, n° 21-04-2021, n° 393099 394922 397844 397851 424717 424718

Document n° 9 : Accès et conservation des données de téléphonie soumis à des conditions strictes pendant la phase d'enquête, par Jean-Baptiste Thierry – Maître de conférences à l'Université de Lorraine

Document n° 10 : Articles du code des postes et communications électroniques

Document n° 11 : Article 15 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 (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009

Document n° 12 : Données téléphoniques : le diable est dans la facture détaillée, Chronique de Stéphanie Marteau, *le Monde* 20 juillet 2022

Document n° 1 : Règlement général sur la protection des données du 24 mai 2016 (extraits)

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Modifié par : Rectificatif au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) JOUE L127 2 du 23/05/2018 [...]

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

(2)

Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. Le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques.

(3) [...]

Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.

(5)

L'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation substantielle des flux transfrontaliers de données à caractère personnel. Les échanges de données à caractère personnel entre acteurs publics et privés, y compris les personnes physiques, les associations et les entreprises, se sont intensifiés dans l'ensemble de l'Union. Le droit de l'Union appelle les autorités nationales des États membres à coopérer et à échanger des données à caractère personnel, afin d'être en mesure de remplir leurs missions ou d'accomplir des tâches pour le compte d'une autorité d'un autre État membre.

(6)

L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

Tournez la page S.V.P.

(7)
Ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. La sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques.
(8)
Lorsque le présent règlement dispose que le droit d'un État membre peut apporter des précisions ou des limitations aux règles qu'il prévoit, les États membres peuvent intégrer des éléments du présent règlement dans leur droit dans la mesure nécessaire pour garantir la cohérence et pour rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent.
(9) [...]
Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. En ce qui concerne le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées «données sensibles»). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite.
(11)
Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, ainsi que de prévoir, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations.
(12) [...]
La protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel. Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale.
(15) [...]
Le présent règlement ne s'applique pas à des questions de protection des libertés et droits fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale. Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.
(17) [...]
Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de

réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.
(19)
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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union. Le présent règlement ne devrait dès lors pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, les données à caractère personnel traitées par des autorités publiques en vertu du présent règlement devraient, lorsqu'elles sont utilisées à ces fins, être régies par un acte juridique de l'Union plus spécifique, à savoir la directive (UE) 2016/680 du Parlement européen et du Conseil. Les États membres peuvent confier à des autorités compétentes au sens de la directive (UE) 2016/680 des missions qui ne sont pas nécessairement effectuées 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 les menaces pour la sécurité publique et la prévention de telles menaces, de manière à ce que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du présent règlement.
En ce qui concerne le traitement de données à caractère personnel par ces autorités compétentes à des fins relevant du champ d'application du présent règlement, les États membres devraient pouvoir maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement. Ces dispositions peuvent déterminer plus précisément les exigences spécifiques au traitement de données à caractère personnel par ces autorités compétentes à ces autres fins, compte tenu de la structure constitutionnelle, organisationnelle et administrative de l'État membre concerné. Lorsque le traitement de données à caractère personnel par des organismes privés relève du champ d'application du présent règlement, celui-ci devrait prévoir la possibilité pour les États membres, sous certaines conditions, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir des intérêts spécifiques importants tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cela est pertinent, par exemple, dans le cadre de la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique.
(20) [...]
Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;
[...] (36) [...]
Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.
(39)
Tout traitement de données à caractère personnel devrait être licite et loyal. Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient

Tournez la page S.V.P.

être transparents à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement. Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel. Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. Il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées. Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement.

(40) [...]

L'autorité de contrôle devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel, afin d'assurer que le traitement prévu respecte le présent règlement et, en particulier, d'atténuer le risque qu'il comporte pour la personne concernée.

(97)

Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres, et les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel.

(105)

Outre les engagements internationaux pris par le pays tiers ou l'organisation internationale, la Commission devrait tenir compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en ce qui concerne la protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. Il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel. Lorsqu'elle évalue le niveau de protection offert par des pays tiers ou des organisations internationales, la Commission devrait consulter le comité.

(106) [...]
La mise en place d'autorités de contrôle dans les États membres, habilitées à exercer leurs missions et leurs pouvoirs en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les États membres devraient pouvoir mettre en place plusieurs autorités de contrôle en fonction de leur structure constitutionnelle, organisationnelle et administrative.
(118) [...]
Lorsqu'un État membre met en place plusieurs autorités de contrôle, il devrait établir par la loi des dispositifs garantissant la participation effective de ces autorités au mécanisme de contrôle de la cohérence. Il devrait en particulier désigner l'autorité de contrôle qui sert de point de contact unique, permettant une participation efficace de ces autorités au mécanisme, afin d'assurer une coopération rapide et aisée avec les autres autorités de contrôle, le comité et la Commission.
(120) [...]

Tournez la page S.V.P.

<u>Document n° 2</u> : Loi du 20 juin 2018 relative à la protection des données personnelles, *site vie publique le 22 juin 2018*

Loi du 20 juin 2018 relative à la protection des données personnelles

La loi a été promulguée le 20 juin 2018. Elle a été publiée au Journal officiel du 21 juin 2018.

L'essentiel de la loi

La loi adapte la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au cadre juridique européen entré en vigueur le 25 mai 2018.

Le texte définit le champ des missions de la Commission nationale de l'informatique et des libertés (CNIL), conformément au Règlement général sur la protection des données (RGPD). La CNIL devient l'autorité nationale de contrôle pour l'application du RGPD. Celle-ci prend en charge la publication de référentiels, de codes de bonne conduite et de règlements types sur les nouvelles obligations des opérateurs. Elle peut certifier des organismes et des services. Elle peut être consultée par le Parlement sur les questions de données personnelles.

Pour les acteurs économiques, le texte remplace le système de contrôle a priori, basé sur les régimes de déclaration et d'autorisation préalables, par un système de contrôle a posteriori, fondé sur l'appréciation par le responsable de traitement des risques en matière de protection des données. En contrepartie, les pouvoirs de la Commission nationale de l'informatique et des libertés (CNIL) sont renforcés, et les sanctions encourues pourront atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial consolidé.

Les formalités préalables sont maintenues pour les données les plus sensibles, telles que les données biométriques nécessaires à l'identification ou au contrôle de l'identité des personnes, les données génétiques, les données utilisant le numéro d'inscription au répertoire national d'identification des personnes physiques ou les données de santé.

La loi renforce les droits des personnes en créant un droit à l'information de la personne concernée par les données personnelles traitées en matière pénale et l'exercice direct des droit d'accès, de rectification et d'effacement des données. Le traitement de données personnelles relatives à la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale est interdit. Il est également interdit de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne.

Pour les mineurs de moins de quinze ans, le consentement des titulaires de l'autorité parentale sera nécessaire pour le traitement des données personnelles sur les réseaux sociaux. C'est à partir de l'âge de quinze ans qu'un mineur pourra s'inscrire sur des réseaux sociaux sans autorisation parentale (le texte initial prévoyait seize ans).

Document n° 3 : Cour de cassation, Chambre criminelle, 12 juillet 2022, 21-83.820, Publié au bulletin

M. [F] [U] a formé un pourvoi contre l'arrêt de la chambre de l'instruction de la cour d'appel de Fort-de-France, en date du 8 juin 2021, qui, dans l'information suivie contre lui des chefs d'importation et exportation de stupéfiants en bande organisée, infractions à la législation sur les stupéfiants, associations de malfaiteurs, a prononcé sur sa demande d'annulation de pièces de la procédure. [...]

Faits et procédure

1. Il résulte de l'arrêt attaqué et des pièces de la procédure ce qui suit.

2. A la suite de l'interception dans les eaux territoriales au large de la Martinique d'une embarcation dans laquelle étaient découvertes plusieurs dizaines de kilogrammes de cocaïne, une information judiciaire a été ouverte.

3. Le 6 novembre 2020, M. [F] [U] a été mis en examen des chefs précités.

4. Le 20 avril 2021, il a déposé une requête en nullité visant notamment les réquisitions des enquêteurs portant sur les données de trafic et de localisation de la téléphonie et les actes d'exploitation de ces données.

Examen des moyens

Sur les premier et deuxième moyens

5. Ils ne sont pas de nature à permettre l'admission du pourvoi au sens de l'article 567-1-1 du code de procédure pénale.

Sur le troisième moyen

Enoncé du moyen

6. Le moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en nullité portant sur les réquisitions des enquêteurs portant sur les données de trafic et de localisation de la téléphonie et des actes d'exploitation de ces données, alors :

« 1°/ que l'article 15, paragraphe 1 de la directive 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, 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, s'oppose à des mesures législatives prévoyant, aux fins de protection de la sécurité nationale ou de lutte contre les infractions graves, à titre préventif, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation des communications par les fournisseurs des services de communication électronique ; que, dans son mémoire, le mis en examen invoquait la nullité de l'ensemble des opérations d'identification de personnes, dont lui-même, en lien avec les personnes soupçonnées par les enquêteurs d'avoir commis les infractions dont ils étaient saisis, par l'utilisation des données de trafic et de localisation des communications électroniques que les fournisseurs de services de communications électroniques, en l'espèce, les fournisseurs de téléphonie, sont tenus de conserver pendant un an, en application des articles L. 34-1 et R. 10-13 du code des postes et communications électroniques et des articles 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numériques imposant aux fournisseurs de communications électronique la conservations de toutes les données notamment de trafic et de localisation et l'article 1er du décret du 25 février 2011 pris pour son application, en ce que ces dispositions violaient le droit de l'Union européenne, et en particulier l'article 15 de la directive 2002/58/CE précitée ; qu'en considérant, pour rejeter le moyen de nullité, que le trafic de stupéfiants entrait dans la catégorie des infractions graves justifiant un stockage massif et indifférencié des données de trafic et de localisation gérées par les fournisseurs de communication électronique dans les conditions prévues par l'article 15 de la directive 2002/58, quand les dispositions légales et réglementaires précitées n'ont précisé ni quelles infractions graves justifiaient une obligation de conservation, ni les catégories de données à conserver, ni les personnes concernées, ni les autorités habilitées à définir les cas dans lesquels ce stockage s'impose, la chambre de l'instruction a méconnu l'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52 de la Charte des droits fondamentaux de l'Union européenne et 88-1 de la Constitution ;

2°/ qu'en vertu de l'article 8, § 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit à la vie privée et au respect des correspondances que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la

Tournez la page S.V.P.

sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ; qu'en estimant que la conservation en vue de leur exploitation dans le cadre des enquêtes pénales des données de trafic et de localisation des utilisateurs des moyens de communication électroniques étaient justifiées pour la recherche des infractions graves, quand le législateur n'a pas défini les catégories d'infractions graves justifiant une telle ingérence, ni l'autorité habilitée à se prononcer sur l'obligation de conserver de telles données, la cour d'appel a violé l'article 8, §2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ;

3°/ qu'en vertu de l'article 15 de la directive 2002/52/CE de la directive 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, les données de trafic et de localisation ne peuvent être exploitées que pour la fin qui a autorisé la conservation ; qu'en se référant à l'arrêt du Conseil d'Etat du 21 avril 2021, ayant jugé que l'obligation de conservation des données de connexion et de localisation pendant un an prévue par la législation et la réglementation nationale, était justifiée par les impératifs de protection de la sécurité nationale que constitue la lutte contre le terrorisme, conservation pourtant non subordonnée à une autorisation d'une juridiction ou d'une autorité indépendante, la chambre de l'instruction, qui a jugé que l'accès à ces données par les enquêteurs agissant sur commission rogatoire était justifié dans le cadre de la recherche des auteurs des infractions visées aux poursuites, pourtant sans lien avec le terrorisme, a violé l'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52 de la Charte des droits fondamentaux de l'Union européenne ;

4°/ qu'en vertu de l'article 15 de la directive 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, l'accès des autorités nationales compétentes aux données de trafic et de localisation conservées est subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative, tiers par rapport à l'autorité de poursuite, et à la condition que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de cette autorité de poursuite ; que, par ailleurs, en vertu de l'article 8, paragraphe 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, l'exploitation de données de trafic et de connexion pour les besoins d'une enquête répressive ne peut intervenir que sur décision d'un juge indépendant et impartial ; que, dans son mémoire, le mis en examen contestait l'accès par les enquêteurs, agissant sur commission rogatoire, aux données de trafic et de localisation concernant différentes personnes, conservées par les fournisseurs de communication électronique, en ce que cet accès n'avait pas été autorisé par une juridiction ; que la chambre de l'instruction qui ne s'est pas prononcée sur ce moyen de nullité, a privé sa décision de base légale en violation des articles 198 et 593 du code de procédure pénale. »

Réponse de la Cour

7. Par arrêt de ce jour, la Cour de cassation a énoncé les principes suivants (Crim., 12 juillet 2022, pourvoi n° 21-83.710, publié au Bulletin).

8. L'article L. 34-1, III, du code des postes et des communications électroniques, dans sa version issue de la loi n° 2013-1168 du 18 décembre 2013, mis en œuvre par l'article R. 10-13 dudit code, tel qu'il résultait du décret n° 2012-436 du 30 mars 2012, est contraire au droit de l'Union européenne en ce qu'il imposait aux opérateurs de services de télécommunications électroniques, aux fins de lutte contre la criminalité, la conservation généralisée et indifférenciée des données de connexion, à l'exception des données relatives à l'identité civile, aux informations relatives aux comptes et aux paiements, ainsi qu'en matière de criminalité grave, de celles relatives aux adresses IP attribuées à la source d'une connexion.

9. En revanche, la France se trouvant exposée, depuis décembre 1994, à une menace grave et réelle, actuelle ou prévisible à la sécurité nationale, les textes précités de droit interne étaient conformes au droit de l'Union en ce qu'ils imposaient aux opérateurs de services de télécommunications électroniques de conserver de façon généralisée et indifférenciée les données de trafic et de localisation, aux fins de la recherche, de la constatation et de la poursuite des infractions portant atteinte aux intérêts fondamentaux de la Nation et des actes de terrorisme, incriminés aux articles 410-1 à 422-7 du code pénal.

10. Les articles 60-1 et 60-2, 77-1-1 et 77-1-2, 99-3 et 99-4 du code de procédure pénale, dans leur version antérieure à la loi n° 2022-299 du 2 mars 2022, lus en combinaison avec le sixième alinéa du paragraphe III de l'article préliminaire du code de procédure pénale, permettaient aux autorités compétentes, de façon conforme au droit de l'Union, pour la lutte contre la criminalité grave, en vue de

l'élucidation d'une infraction déterminée, d'ordonner la conservation rapide, au sens de l'article 16 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, des données de connexion, même conservées aux fins de sauvegarde de la sécurité nationale.

11. Il appartient à la juridiction, lorsqu'elle est saisie d'un moyen en ce sens, de vérifier, d'une part, que les éléments de fait justifiant la nécessité d'une telle mesure d'investigation répondent à un critère de criminalité grave, dont l'appréciation relève du droit national, d'autre part, que la conservation rapide des données de trafic et de localisation et l'accès à celles-ci respectent les limites du strict nécessaire.

12. S'agissant de la gravité des faits, il appartient au juge de motiver sa décision au regard de la nature des agissements de la personne poursuivie, de l'importance du dommage qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue.

13. Les articles 60-1 et 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 préalablement à l'accès aux données un contrôle par une juridiction ou une entité administrative indépendante. En revanche, le juge d'instruction est habilité à contrôler l'accès aux données de connexion.

14. Une personne mise en examen n'est recevable à invoquer la violation de l'exigence précitée que si elle prétend être titulaire ou utilisatrice de l'une des lignes identifiées ou si elle établit qu'il aurait été porté atteinte à sa vie privée, à l'occasion des investigations litigieuses.

15. L'existence d'un grief pris de l'absence d'un tel contrôle est établie si l'accès aux données de trafic et de localisation a méconnu les conditions matérielles posées par le droit de l'Union. Tel est le cas si l'accès a porté sur des données irrégulièrement conservées, s'il a eu lieu, hors hypothèse de la conservation rapide, pour une finalité moins grave que celle ayant justifié la conservation, n'a pas été circonscrit à une procédure visant à lutter contre la criminalité grave et a excédé les limites du strict nécessaire.

16. En l'espèce, M. [U] ne justifie ni même n'allègue qu'il aurait été porté atteinte à sa vie privée par les réquisitions délivrées aux opérateurs durant l'enquête ou sur commission rogatoire et tendant à obtenir les facturations détaillées et les géolocalisations des lignes téléphoniques dont il n'était ni titulaire ni utilisateur. Il n'a dès lors pas qualité pour en solliciter la nullité.

17. En revanche, il est recevable à solliciter la nullité des réquisitions portant sur les lignes téléphoniques dont il était l'utilisateur, auxquelles les enquêteurs n'ont eu accès que sur commission rogatoire du juge d'instruction.

18. C'est à tort que, pour ne pas faire droit à la nullité des procès-verbaux d'exploitation de facturations détaillées et de données géolocalisées concernant le requérant, l'arrêt énonce en substance que les articles L. 34-1 et R. 10-13 du code des postes et des communications électroniques, dans leur version en vigueur au moment des faits, prévoyaient une conservation ciblée des données de connexion.

19. En effet, une telle conservation n'existait pas en droit français.

20. L'arrêt n'encourt néanmoins pas la censure pour les motifs qui suivent.

21. D'une part, la chambre de l'instruction a, à juste titre, énoncé que les faits d'importation et d'exportation de plusieurs centaines de kilogrammes de cocaïne d'une grande pureté, en bande organisée, par une structure criminelle de dimension internationale, entrent dans le champ de la criminalité grave.

22. D'autre part, elle a également relevé que l'ingérence dans la vie privée du requérant constituée par les réquisitions aux opérateurs téléphoniques et l'exploitation des données d'identité, de trafic et de géolocalisation apparaissait tout à la fois nécessaire et proportionnée à la poursuite d'infractions pénales relevant de la criminalité grave.

23. Il s'ensuit qu'agissant sur commission rogatoire du juge d'instruction, les enquêteurs pouvaient, sans méconnaître les dispositions conventionnelles invoquées au moyen, accéder aux données de trafic et de localisation régulièrement conservées pour la finalité de la sauvegarde de la sécurité nationale.

24. Le moyen ne peut dès lors être accueilli.

25. Par ailleurs l'arrêt est régulier en la forme.

PAR CES MOTIFS, la Cour : REJETTE le pourvoi. [...]

Tournez la page S.V.P.

Document n° 4 : Protection des données dans l'Union Européenne, *site internet de la Commission européenne, 05 avril 2024*

Droits fondamentaux

La charte des droits fondamentaux de l'UE dispose que les citoyens de l'Union européenne ont droit à la protection de leurs données à caractère personnel.

Protection des données à caractère personnel

Législation

Le train de mesures sur la protection des données adopté en mai 2016 vise à adapter l'Europe à l'ère numérique. Plus de 90 % des Européens veulent les mêmes droits en matière de protection des données dans toute l'UE, où que soient traitées ces données.

Règlement général sur la protection des données (RGPD)

Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Ce texte inclut le rectificatif publié au Journal officiel de l'UE du 23 mai 2018.

Ce règlement est une étape essentielle pour renforcer les droits fondamentaux des personnes à l'ère du numérique et stimuler l'activité économique en clarifiant la réglementation du marché unique numérique pour les entreprises et les organismes publics. Une législation unique permettra également de mettre fin à la fragmentation juridique actuelle entre les différents systèmes nationaux et aux charges administratives inutiles pesant sur les entreprises.

Le règlement est entré en vigueur le 24 mai 2016 et s'applique depuis le 25 mai 2018. Plus d'informations pour les entreprises et les particuliers.

Informations sur l'intégration du règlement général sur la protection des données (RGPD) dans l'accord EEE.

Notifications des États membres de l'UE à la Commission européenne au titre du RGPD

Directive en matière de protection des données dans le domaine répressif

Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en lien avec des infractions pénales ou l'exécution de sanctions pénales, ainsi qu'à la libre circulation de ces données.

Cette directive protège le droit fondamental des citoyens à la protection des données les concernant lorsque ces données sont utilisées par les services répressifs à des fins répressives. Elle garantit notamment la protection des données à caractère personnel des victimes, des témoins et des suspects et facilite la coopération transfrontière dans la lutte contre la criminalité et le terrorisme.

La directive est entrée en vigueur le 5 mai 2016 et les pays de l'UE étaient tenus de la transposer en droit national avant le 6 mai 2018.

Autorités nationales de protection des données

Les pays de l'UE ont mis en place des instances nationales chargées de la protection des données à caractère personnel, conformément à la charte des droits fondamentaux de l'Union européenne (article 8, paragraphe 3).

Comité européen de la protection des données

Le comité européen de la protection des données est un organe européen indépendant qui veille à l'application cohérente des règles en matière de protection des données dans l'ensemble de l'Union européenne. Il a été institué par le règlement général sur la protection des données (RGPD).

Le comité européen de la protection des données est composé de représentants des autorités nationales chargées de la protection des données des pays de l'UE/EEE et du Contrôleur européen de la protection des données (CEPD). La Commission européenne participe aux activités et aux réunions du comité sans droit de vote. Le secrétariat du comité, assuré par le CEPD, accomplit ses tâches sous l'autorité exclusive du président du comité.

Les tâches du comité européen de la protection des données consistent principalement à fournir des orientations générales sur les concepts clés du RGPD et de la directive en matière de protection des données dans le domaine répressif, à conseiller la Commission européenne sur les questions liées à la protection des données à caractère personnel et aux nouvelles propositions législatives dans l'UE, et à adopter des décisions contraignantes en cas de différends entre autorités de contrôle nationales.
Protection des données dans les institutions et organes de l'UE
Législation

Le règlement (UE) 2018/1725 définit les règles applicables au traitement des données à caractère personnel par les institutions, organes et organismes de l'UE. Il est conforme au règlement général sur la protection des données et à la directive relative à la protection des données dans le domaine répressif. Ce règlement est entré en vigueur le 11 décembre 2018.

Contrôleur européen de la protection des données

Le règlement (UE) 2018/1725 a mis en place un Contrôleur européen de la protection des données (CEPD). Le CEPD est une autorité européenne indépendante chargée de surveiller l'application des règles relatives à la protection des données au sein des institutions européennes et d'examiner les plaintes.

Délégué à la protection des données de la Commission européenne

La Commission européenne a désigné un délégué à la protection des données, qui est chargé de la surveillance et de l'application des règles relatives à la protection des données au sein de la Commission. Le délégué à la protection des données veille de manière indépendante à l'application interne des règles de protection des données, en coopération avec le Contrôleur européen de la protection des données.

Clauses contractuelles types

À la suite de l'adoption, en juin 2021, de deux ensembles de clauses contractuelles types [l'une devant être utilisée entre les responsables du traitement et les sous-traitants au sein de l'Espace économique européen (EEE) et l'autre pour le transfert de données à caractère personnel vers des pays hors EEE], la Commission européenne a publié, le 25 mai 2022, des questions et réponses pour fournir des orientations pratiques sur l'utilisation de ces clauses et aider les parties prenantes à se conformer au règlement général sur la protection des données (RGPD). Ces questions-réponses sont fondées sur les retours d'information des différents acteurs concernant leur expérience de l'utilisation des nouvelles clauses contractuelles types au cours des premiers mois qui ont suivi leur adoption. Elles sont destinées à servir de source d'information «dynamique» et seront mises à jour à mesure que de nouvelles questions se poseront.

Document n° 5 : La protection des données personnelles dans les relations internes à l'Union européenne par Céline CASTETS-RENARD, in Répertoire de droit européen, octobre 2018

[...] Section 2 - Les principes de la directive [en matière pénale (directive 2016/680/UE) adoptée le 27 avril 2016]

223. Principes directeurs du traitement. - L'article 4, § 1, pose des principes directeurs communs au RGPD. Ainsi, les États membres doivent respecter des principes de licéité, de loyauté (art. 4, § 1, a), de finalité (art. 4, § 1, b), de pertinence (art. 4, § 1, c), d'exactitude et, si possible, d'actualisation (art. 4, § 1, d), ainsi que de conservation limitée (art. 4, § 1, e) et de sécurité des données (art. 4, § 1, f). Le principe de licéité précisé à l'article 8 est celui selon lequel le traitement n'est licite que si, et dans la mesure où : il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, § 1 ; il est fondé sur le droit de l'Union ou le droit d'un État membre. En outre, le droit de l'État membre doit préciser au moins les objectifs du traitement, les données à caractère personnel concernées et les finalités (art. 8, § 2). Les exigences d'exactitude et d'actualisation sont souples, puisqu'il est simplement prévu que les données doivent être exactes et « si nécessaire » tenues à jour. En outre, « toutes les mesures raisonnables » doivent être prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées « sans tarder » (art. 4, § 1, d). Le principe de nécessité consacré par le GDPR n'est pas repris en tant que tel dans la directive. Est cependant consacré un principe de modération ou de minimisation des données, eu égard aux finalités poursuivies (art. 4, § 1, c). Le principe de conservation suppose que les données soient conservées « pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » (art. 4, § 1, e). Selon le principe de sécurité, les données sont « traitées de façon à garantir leur sécurité, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées » (art. 4, § 1, f). Ce principe est essentiel, eu égard à la sensibilité des informations se rapportant aux infractions pénales.

224. Principe de finalité : finalités larges et réutilisations autorisées. - Le principe de finalité impose que les données soient collectées « pour des finalités déterminées, explicites et légitimes » et ne soient pas traitées « d'une manière incompatible avec ces finalités » (art. 4, § 1, b). En outre, les données collectées doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées » (art. 4, § 1, c). Cependant, les finalités prévues par la directive, telle la « protection contre les menaces pour la sécurité publique », sont larges ; aussi, il pourrait s'avérer difficile de donner une interprétation stricte de ce principe et de lui trouver des limites claires. La notion de « sécurité publique » est particulièrement diluée aujourd'hui, à l'heure où la menace terroriste reste omniprésente. Au demeurant, le paragraphe 2 reconnaît un changement possible de finalité. Il prévoit que le traitement, par le même ou par un autre responsable du traitement, pour une finalité autre que celles pour lesquelles les données ont été collectées, est autorisé. Cette autorisation est cependant soumise au respect de trois conditions : la seconde finalité doit être conforme à celles énoncées à l'article 1er, § 1 ; le responsable du traitement doit être autorisé à traiter ces données pour une telle finalité ; ce traitement doit être nécessaire et proportionné à cette autre finalité. On le voit, ces finalités sont peu exigeantes. En résumé, les mêmes données pourront être utilisées pour des finalités différentes, dès lors que leur traitement reste dans le cadre de la directive. Il pourra notamment s'agir d'un traitement des données à des fins d'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, mais non pas exclusivement. Plus encore, l'article 9 autorise à ce que les données collectées soient traitées à des fins autres, si un tel traitement est autorisé par le droit de l'Union ou le droit d'un État membre. Dans ce cas, le RGPD s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du droit de l'Union. Cette souplesse facilite la réutilisation des données, mais remet substantiellement en cause la vigueur du principe de finalité, pourtant pierre angulaire de la protection des données.

225. Conservation et effacement des données. - S'agissant de la conservation et de l'effacement des données, une marge de manœuvre est laissée aux États membres qui doivent « fixer des délais appropriés pour l'effacement des données ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel ». En outre, les États doivent instaurer des règles procédurales, afin de garantir le respect de ces délais (art. 5). Ces dispositions sont importantes, car l'effacement des

données est très peu souvent réalisé en pratique. Les États sont donc censés revoir leurs procédures et modèles organisationnels. Mais il faudra suivre concrètement la mise en œuvre pratique pour s'assurer du respect des droits des personnes concernées.

226. Identification des personnes concernées. - L'article 6 de la directive identifie quatre catégories de personnes concernées par les traitements de données à caractère personnel que le responsable de traitement doit distinguer. Il s'agit : des personnes suspectées d'avoir commis ou d'être sur le point de commettre une infraction pénale ; des personnes reconnues coupables d'une infraction pénale ; des victimes d'une infraction pénale ; des tiers à une infraction pénale, spécialement les témoins. Ces quatre catégories correspondent à des situations bien différentes qu'il est important de bien distinguer. Or, le texte précise qu'il faut distinguer ces catégories seulement « dans la mesure du possible ». On regrettera que l'exigence de distinction ne soit pas marquée plus fermement et clairement. Il y a là un risque d'atteinte aux droits fondamentaux des personnes concernées qui n'est pas justifié par une réelle difficulté technique ou pratique.

227. Qualité non garantie des données transmises. - Par ailleurs, l'article 7, § 1, distingue les données à caractère personnel fondées sur des faits et celles fondées sur des « appréciations personnelles ». Là encore, ces deux catégories doivent être différenciées « dans la mesure du possible ». Cette réserve réduit la protection des intérêts des personnes concernées. En effet, les appréciations personnelles peuvent conduire à des suspicions et à profilages erronés. Si on comprend l'utilité d'une certaine souplesse sur la façon dont les personnes doivent être appréhendées par les autorités compétentes, plus ou moins liées à des intuitions ou à des expériences des officiers de police par exemple, il y a là des risques importants pour la protection des individus. De même, le paragraphe 2 dispose que les États membres doivent prévoir que les autorités compétentes prennent « toutes les mesures raisonnables » pour garantir que les données à caractère personnel inexactes, incomplètes ou périmées ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, « dans la mesure du possible », la qualité des données avant leur transmission ou leur mise à disposition. Il n'y a donc pas d'obligation réelle de vérifier la qualité des données avant transmission. On comprend bien que, sur le terrain, il n'est pas toujours possible de procéder à des vérifications, notamment en situation d'urgence ou pour des raisons de coûts. Néanmoins, la transmission et la diffusion de données erronées sur des individus constituent des risques d'atteinte aux intérêts des individus particulièrement importants. Également, lors de toute transmission de données à caractère personnel sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, de la fiabilité des données et de leur niveau de mise à jour, « dans la mesure du possible ». Cependant, le paragraphe 3 prévoit que s'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite le destinataire doit être informé « sans retard », et les données à caractère personnel doivent être rectifiées ou effacées, ou leur traitement est limité. Il est absolument nécessaire d'imposer une réactivité la plus grande possible pour éviter que les informations fausses se répandent.

228. Licéité du traitement. - L'article 8, § 1, dispose que les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1, § 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement (art. 8, § 2). Ce n'est donc qu'à ses conditions, définies par les États membres, que le traitement est licite.

229. Conditions spécifiques applicables au traitement. - L'article 9, § 1, prévoit des hypothèses de changement de finalité des traitements, révélant une grande souplesse. En effet, lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres que celles exécutées pour les finalités énoncées à l'article 1er, paragraphe 1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union (art. 9, § 2). Les États membres prévoient que, lorsque le droit de l'Union ou le droit d'un État membre applicable à l'autorité compétente qui transmet les données soumet le traitement à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter (art. 9, § 3). L'autorité compétente ne doit alors pas poser des conditions différentes de celles applicables aux transferts de

Tournez la page S.V.P.

données similaires à l'intérieur de l'État membre dont relève l'autorité compétente qui transmet les données (art. 9, § 4).

230. Données sensibles peu spécifiquement protégées. - L'article 10 encadre l'utilisation des données sensibles. Si l'énumération est identique à celle du RGPD, le régime juridique est totalement différent, puisque le principe n'est pas l'interdiction d'utiliser de telles données, mais l'autorisation « en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée ». Cette autorisation n'est donc valable que pour trois cas limitativement énumérés : lorsque les traitements sont autorisés par le droit de l'Union ou le droit d'un État membre ; pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. Ces deux derniers cas sont, par ailleurs, des exceptions au principe d'interdiction dans le règlement. La première hypothèse n'est pas prévue en tant que telle, mais plusieurs exceptions du règlement s'en rapprochent, si bien que cette différence de régime n'est probablement pas si importante qu'il y paraît au premier abord.

231. Décision individuelle automatisée. - L'article 11, § 1, dispose que les États membres prévoient que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis et qui fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement. La marge de manœuvre laissée aux États membres leur permettant de ne pas respecter l'interdiction de traitement leur donne une grande liberté, ce qui risque d'entraîner une grande disparité législative. Quoi qu'il en soit, les décisions ne doivent pas être fondées sur des données sensibles, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place (art. 11, § 2). En d'autres termes, l'utilisation des données sensibles est rendue possible. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des données sensibles est interdit, conformément au droit de l'Union (art. 11, § 3). Dès lors seul est interdit le profilage basé en tant que tel sur les données sensibles. Ces dispositions se rapprochent de celles prévues à l'article 22 du RGPD. Mais le législateur est moins protecteur en matière pénale et laisse la liberté aux États de recourir à des dispositifs automatisés, tels les algorithmes déjà utilisés par exemple à des fins de police et de justice prédictive. Or, ces outils peuvent non seulement être attentatoires aux droits fondamentaux des personnes concernées, mais peuvent aussi s'avérer discriminants et biaisés, comme l'a prouvé l'étude menée par l'ONG Propublica sur le logiciel COMPAS Propublica (https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm), couramment utilisé aux États-Unis pour aider à la prise de décision de libération conditionnelle et à l'évaluation du risque de récidive. L'étude a révélé des biais raciaux dans les résultats, dès lors que les données utilisées pour alimenter la base de données étaient elles-mêmes biaisées. Au demeurant, les garanties apportées par le législateur de l'Union peuvent paraître bien faibles. La référence classique à « la sauvegarde des droits, des libertés et des intérêts légitimes de la personne concernée » n'apporte pas une protection concrète et effective et risque d'être vide de sens. Certes, le droit d'obtenir une intervention humaine est prévu, mais il risque de simplement donner l'illusion d'un « contrôle » ou d'une « explication », alors même qu'une telle explication ne peut être donnée pour les dispositifs complexes, tels les procédés de *machine learning*. L'homme est alors le plus souvent dans l'incapacité de comprendre la décision prise par la machine qui ne suit pas un raisonnement humain d'apprentissage.

<u>Document n° 6</u> : Cour de justice de l'Union européenne COMMUNIQUE DE PRESSE n° 29/21, Luxembourg, le 2 mars 2021 - Arrêt dans l'affaire C-746/18 H. K/Prokuratuur

L'accès, à des fins pénales, à un ensemble de données de communications électroniques relatives au trafic ou à la localisation, permettant de tirer des conclusions précises sur la vie privée, n'est autorisé qu'en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

Le droit de l'Union s'oppose par ailleurs à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique à ces données afin de mener une instruction pénale.

Une procédure pénale a été engagée en Estonie contre H. K. des chefs de vol, d'utilisation de la carte bancaire d'un tiers et de violence à l'égard de personnes participant à une procédure en justice. H. K. a été condamnée pour ces infractions par un tribunal de première instance à une peine privative de liberté de deux ans. Cette décision a ensuite été confirmée en appel.
Les procès-verbaux sur lesquels s'appuie la constatation de ces infractions ont été établis, notamment, sur la base de données à caractère personnel générées dans le cadre de la fourniture de services de communications électroniques. La Riigikohus (Cour suprême, Estonie), devant laquelle un pourvoi en cassation a été introduit par H. K., a émis des doutes quant à la compatibilité avec le droit de l'Union[1] des conditions dans lesquelles les services d'enquête ont eu accès à ces données.
Ces doutes concernent, en premier lieu, la question de savoir si la durée de la période pour laquelle les services d'enquête ont eu accès aux données constitue un critère permettant d'évaluer la gravité de l'ingérence que constitue cet accès dans les droits fondamentaux des personnes concernées. Ainsi, lorsque cette période est très brève ou que la quantité de données recueillies est très limitée, la juridiction de renvoi s'est interrogée sur le fait de savoir si l'objectif de lutte contre la criminalité en général, et pas seulement de lutte contre la criminalité grave, est susceptible de justifier une telle ingérence. En second lieu, la juridiction de renvoi a nourri des doutes quant à la possibilité de considérer le ministère public estonien, compte tenu des différentes missions qui lui sont confiées par la réglementation nationale, comme une autorité administrative « indépendante » au sens de l'arrêt Tele2 Sverige et Watson e.a.[2], susceptible d'autoriser l'accès de l'autorité chargée de l'enquête aux données concernées.
Par son arrêt, prononcé en grande chambre, la Cour juge que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose à une réglementation nationale permettant l'accès des autorités publiques à des données relatives au trafic ou à des données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique. Selon la Cour, la durée de la période pour laquelle l'accès à ces données est sollicité et la quantité ou la nature des données disponibles pour une telle période n'ont pas d'incidence à cet égard. En outre, la Cour considère que cette même directive, lue à la lumière de la Charte, s'oppose à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de mener une instruction pénale.

---

1 Plus précisément, avec 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 (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive "vie privée et communications électroniques" »), 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 (ci-après la « Charte »).

2 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15 point 120 ; voir également communiqué de presse n°145/16.

Tournez la page S.V.P.

Appréciation de la Cour

S'agissant des conditions dans lesquelles l'accès aux données relatives au trafic et aux données de localisation conservées par les fournisseurs de services de communications électroniques peut, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, être accordé à des autorités publiques, en application d'une mesure prise au titre de la directive « vie privée et communications électroniques »[3] , la Cour rappelle ce qu'elle a jugé dans son arrêt La Quadrature du Net e.a.[4]. Ainsi, cette directive n'autorise les États membres à adopter, entre autres à ces fins, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic[5], que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte[6]. Dans ce cadre, la directive s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, poursuivi par la réglementation en cause, conformément au principe de proportionnalité, la Cour considère que seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée des personnes concernées, sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès.

S'agissant de la compétence donnée au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de diriger une instruction pénale, la Cour rappelle qu'il appartient au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données dont ils disposent. Toutefois, pour satisfaire à l'exigence de proportionnalité, une telle réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et indiquer en quelles circonstances et sous quelles conditions matérielles et procédurales une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire.

Selon la Cour, aux fins de garantir, en pratique, le plein respect de ces conditions, 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 et que la décision de cette juridiction ou de cette entité intervienne 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. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais. À cet égard, la Cour précise que le contrôle préalable requiert, entre autres, que la juridiction ou l'entité chargée d'effectuer ce contrôle dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause.

S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure 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 et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès. Lorsque ce contrôle est effectué non par une juridiction mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui

---

3 Article 15, paragraphe 1, de la directive « vie privée et communications électroniques ».

4 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, points 166 à 169 ; [...]

5 Article 5, paragraphe 1, de la directive « vie privée et communications électroniques ».

6 En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

permettant d'agir, lors de l'exercice de ses missions, de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure.
D'après la Cour, il en résulte que l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique 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, tel n'est pas le cas d'un ministère public qui, comme c'est le cas du ministère public estonien, dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. Il s'ensuit que le ministère public n'est pas en mesure d'effectuer le contrôle préalable susmentionné.

Tournez la page S.V.P.

Document n° 7 : Communiqué de presse de la Cour de cassation du 12 juillet 2022 Enquêtes pénales : conservation et accès aux données de connexion

Droit de l'Union européenne : protection de la vie privée, des données personnelles et de la liberté d'expression

La règle

Les États membres de l'Union européenne ne peuvent imposer aux opérateurs de communications électroniques, fournisseurs d'accès à internet et hébergeurs, une conservation généralisée et indifférenciée de l'ensemble des données de trafic et de localisation.

Des exceptions

Cette conservation peut avoir lieu, sous certaines conditions, en cas de menace grave et actuelle pour la sécurité nationale.

Afin d'élucider une infraction déterminée relevant de la criminalité grave, les États membres peuvent également imposer aux opérateurs et fournisseurs de procéder à la conservation « rapide » des données, s'ils entourent cette obligation d'un certain nombre de garanties.

L'accès aux données conservées doit, en tout état de cause, être autorisé par une juridiction ou une entité administrative indépendante.

De quelles données de connexion parle-t-on ici ?

Il s'agit des :

- données de trafic, qui établissent les contacts qu'une personne a eus par téléphone ou SMS / la date et l'heure de ces contacts / la durée de l'échange ;
- données de localisation, qui permettent de : connaître les zones d'émission et de réception d'une communication passée avec un téléphone mobile identifié / obtenir la liste des appels ayant borné à la même antenne relais.

Ces données sont accessibles sur les « *fadettes* ».

Repère :

Selon la Cour de justice de l'Union européenne (CJUE), ces données sont « susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé [...].
Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. »

Les faits et la procédure

Dans plusieurs affaires, notamment de meurtre ou de trafic de stupéfiants, des personnes mises en examen ont demandé l'annulation des réquisitions portant sur leurs données de trafic et de localisation, délivrées par des enquêteurs agissant en enquête de flagrance sous le contrôle du procureur de la République ou sur commission rogatoire du juge d'instruction, ainsi que des actes d'exploitation de ces données.

Selon les requérants, ces données avaient fait l'objet :
- d'une conservation irrégulière car la législation française alors en vigueur imposait aux opérateurs de conserver pendant un an l'ensemble des données de connexion pour la recherche de toutes les infractions pénales ;
- d'un accès irrégulier car ces données personnelles ont été obtenues par les enquêteurs avec l'autorisation du procureur de la République ou du juge d'instruction, qui ne sont ni une juridiction ni une entité administrative indépendante.

Les principes

Repère :
Afin de garantir l'effectivité du droit de l'Union au sein des différents États membres, le juge national doit interpréter le droit français de manière conforme au droit de l'Union.
À défaut de pouvoir procéder à une telle interprétation conforme, le juge national est tenu de laisser inappliquées les règles de droit français contraires au droit de l'Union.
Si le juge ne respecte pas la législation de l'Union européenne, il expose l'État à un recours en manquement.

Conservation générale des données de trafic et de localisation (régime antérieur à la loi du 30 juillet 2021)

La sauvegarde de la sécurité nationale permettait une conservation générale et indifférenciée des données.
La réglementation française en ce qu'elle prévoyait la conservation générale des données de connexion pour la protection des intérêts fondamentaux de la Nation et la lutte contre le terrorisme était conforme au droit de l'Union, sous réserve d'un réexamen périodique de l'existence d'une menace grave pour la sécurité nationale.
Dans les affaires examinées, une menace pour la sécurité de la Nation existait avant les faits : c'est ce qui ressort des pièces produites par le procureur général près la Cour de cassation relatives aux attentats commis en France depuis décembre 1994. La durée de conservation pendant un an est jugée strictement nécessaire à la sauvegarde de la sécurité nationale.
En revanche, la conservation générale à d'autres fins était contraire au droit de l'Union.
Il était possible de procéder, par voie de réquisitions, à la conservation « rapide » des données pour élucider une infraction grave et dans les limites de la stricte nécessité : le juge saisi d'une contestation doit s'assurer de cette nécessité.
Les données conservées par les opérateurs pour leurs besoins propres ou au titre de sauvegarde de la sécurité nationale, peuvent l'être également, à la demande des enquêteurs, par voie de réquisitions, pour la répression d'une infraction grave déterminée.
Les réquisitions valent alors injonction de conservation « rapide ».
Afin de s'assurer du respect du droit de l'Union, lorsqu'il est saisi d'un moyen de nullité critiquant la régularité des réquisitions, le juge doit vérifier que :
- les faits en cause relèvent de la criminalité grave ;
- la conservation « rapide » des données de connexion et l'accès à celles-ci respectent les limites du strict nécessaire.

Accès aux données de trafic et de localisation
Le juge d'instruction, qui est une juridiction, peut contrôler l'accès aux données ; le procureur de la République, qui n'est pas un tiers dans les enquêtes, ne peut y procéder.
La loi en ce qu'elle permet au procureur de la République, ou à un enquêteur, d'accéder aux données est contraire au droit de l'Union car elle ne prévoit pas un contrôle préalable par une juridiction ou une entité administrative indépendante.
Le procureur de la République dirige la procédure d'enquête et exerce, le cas échéant, l'action publique : il est ainsi impliqué dans la conduite de l'enquête pénale et n'a pas une position de neutralité vis-à-vis des parties à la procédure pénale, comme l'exige le droit de l'Union.
En revanche, le juge d'instruction est habilité à exercer ce contrôle, puisqu'il n'est pas une partie à la procédure mais une juridiction et qu'il n'exerce pas l'action publique.

Tournez la page S.V.P.

Par conséquent, la personne mise en examen peut, sous certaines conditions, invoquer la violation de l'exigence de contrôle indépendant de l'accès à ses données de connexion.
L'acte ayant permis d'accéder aux données ne peut être annulé par le juge que s'il a été porté atteinte à la vie privée de la personne mise en examen et si celle-ci a subi un préjudice. La Cour de cassation précise les conséquences d'un accès irrégulier aux données de connexion sur la validité des actes d'enquête :
La loi donne à la personne mise en examen la possibilité de contester efficacement la pertinence des preuves tirées de ses données, en particulier dans le cadre d'une demande d'expertise.
Le droit de l'Union cherche à protéger la vie privée : ne pas le respecter revient à porter atteinte à un intérêt privé.
Dès lors, la personne mise en examen ne peut invoquer la violation des exigences en matière de contrôle de l'accès aux données que si elle prétend être titulaire ou utilisatrice d'une ligne identifiée ou si elle démontre qu'à l'occasion de ces investigations, il a été porté atteinte à sa vie privée.
Le juge pénal ne peut annuler les actes ayant permis d'accéder aux données que si l'irrégularité constatée a occasionné un préjudice à la personne mise en examen. Ce préjudice est établi :
lorsque les données ne pouvaient être conservées au titre de la conservation « rapide » ;
ou lorsque les catégories de données visées et la durée pendant laquelle il a été possible d'y avoir accès n'étaient pas limitées à ce qui était strictement nécessaire au bon déroulement de l'enquête en cause.

Les conséquences dans les affaires examinées

Dans les affaires pour lesquelles les personnes mises en examen n'avaient aucun droit sur les lignes téléphoniques, les requêtes en nullité sont jugées irrecevables.
Dans les affaires pour lesquelles les personnes mises en examen avaient un droit sur les lignes téléphoniques, les pourvois sont rejetés car :
1. Les données de connexion ont été régulièrement conservées dès lors que les faits relevaient bien de la criminalité grave (meurtre en bande organisée, destruction par moyen dangereux, importations et exportations de centaines de kilos de stupéfiants par organisation criminelle de dimension internationale etc.), et que les réquisitions aux opérateurs des données de connexion (identité, trafic, localisation) et leur exploitation étaient nécessaires au bon déroulement des enquêtes.
2. L'accès par des enquêteurs ayant agi sur commission rogatoire du juge d'instruction a été régulièrement accordé.
3. Bien que des enquêteurs ont eu irrégulièrement accès aux données de trafic et de localisation dans le cadre d'une enquête de flagrance menée sous le contrôle du procureur de la République, la chambre de l'instruction a valablement pu rejeter les demandes de nullité, car, en l'espèce, les catégories de données visées et la durée pendant laquelle il a été possible d'y avoir accès étaient limitées à ce qui était strictement nécessaire au bon déroulement de l'enquête.

<u>Document n° 8</u> : Recueil Lebon - Recueil des décisions du conseil d'Etat 2021, Données de connexion : validation de l'obligation de conservation, Décision du Conseil d'Etat – Assemblée, n° 21-04-2021, n° 393099 394922 397844 397851 424717 424718

Sommaire : La contrariété d'une disposition législative aux stipulations d'un traité international ou au droit de l'Union européenne ne peut être utilement invoquée à l'appui de conclusions dirigées contre un acte réglementaire que si ce dernier a été pris pour son application ou si en elle constitue la base légale.

Le respect du droit de l'Union constitue une obligation tant en vertu du traité sur l'Union européenne (TUE) et du traité sur le fonctionnement de l'Union européenne (TFUE) qu'en application de l'article 88-1 de la Constitution.

Il emporte l'obligation de transposer les directives et d'adapter le droit interne aux règlements européens. En vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne (CJUE), le juge national, chargé d'appliquer les dispositions et principes généraux du droit (PGD) de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif.

Toutefois, tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique interne, dans les conditions mentionnées au point précédent, l'article 88-1 confirme la place de la Constitution au sommet de ce dernier.

Il appartient au juge administratif, s'il y a lieu, de retenir de l'interprétation que la CJUE a donnée des obligations résultant du droit de l'Union la lecture la plus conforme aux exigences constitutionnelles autres que celles qui découlent de l'article 88-1, dans la mesure où les énonciations des arrêts de la Cour le permettent.

Dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la CJUE, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige.

En revanche, il n'appartient pas au juge administratif de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la CJUE elle-même, de la répartition des compétences entre l'Union européenne et les Etats membres. Il ne saurait ainsi exercer un contrôle sur la conformité au droit de l'Union des décisions de la CJUE et, notamment, priver de telles décisions de la force obligatoire dont elles sont revêtues, rappelée par l'article 91 de son règlement de procédure, au motif que celle-ci aurait excédé sa compétence en conférant à un principe ou à un acte du droit de l'Union une portée excédant le champ d'application prévu par les traités.

Il en résulte, d'une part, que, dans le cadre du contrôle de la légalité et de la constitutionnalité des actes réglementaires assurant directement la transposition d'une directive européenne ou l'adaptation du droit interne à un règlement et dont le contenu découle nécessairement des obligations prévues par la directive ou le règlement, il appartient au juge administratif, saisi d'un moyen tiré de la méconnaissance d'une disposition ou d'un principe de valeur constitutionnelle, de rechercher s'il existe une règle ou un PGD de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité du respect de la disposition ou du principe constitutionnel invoqué.

Dans l'affirmative, il y a lieu pour le juge administratif, afin de s'assurer de la constitutionnalité de l'acte réglementaire contesté, de rechercher si la directive que cet acte transpose ou le règlement auquel cet acte adapte le droit interne est conforme à cette règle ou à ce PGD de l'Union. Il lui revient, en l'absence de difficulté sérieuse, d'écarter le moyen invoqué, ou, dans le cas contraire, de saisir la CJUE d'une question préjudicielle, dans les conditions prévues par l'article 167 du TFUE.

Tournez la page S.V.P.

En revanche, s'il n'existe pas de règle ou de PGD de l'Union garantissant l'effectivité du respect de la disposition ou du principe constitutionnel invoqué, il revient au juge administratif d'examiner directement la constitutionnalité des dispositions réglementaires contestées.

D'autre part, lorsqu'il est saisi d'un recours contre un acte administratif relevant du champ d'application du droit de l'Union et qu'est invoqué devant lui le moyen tiré de ce que cet acte, ou les dispositions législatives qui en constituent la base légale ou pour l'application desquelles il a été pris, sont contraires à une directive ou un règlement européen, il appartient au juge administratif, après avoir saisi le cas échéant la CJUE d'une question préjudicielle portant sur l'interprétation ou la validité de la disposition du droit de l'Union invoquée, d'écarter ce moyen ou d'annuler l'acte attaqué, selon le cas.

Toutefois, s'il est saisi par le défendeur d'un moyen, assorti des précisions nécessaires pour en apprécier le bien-fondé, tiré de ce qu'une règle de droit national, alors même qu'elle est contraire à la disposition du droit de l'Union européenne invoquée dans le litige, ne saurait être écartée sans priver de garanties effectives une exigence constitutionnelle, il appartient au juge administratif de rechercher s'il existe une règle ou un PGD de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité de l'exigence constitutionnelle invoquée. Dans l'affirmative, il lui revient, en l'absence de difficulté sérieuse justifiant une question préjudicielle à la CJUE, d'écarter cette argumentation avant de faire droit au moyen du requérant, le cas échéant.

Si, à l'inverse, une telle disposition ou un tel PGD de l'Union n'existe pas ou que la portée qui lui est reconnue dans l'ordre juridique européen n'est pas équivalente à celle que la Constitution garantit, il revient au juge administratif d'examiner si, en écartant la règle de droit national au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties effectives l'exigence constitutionnelle dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

Gouvernement soutenant en défense que les dispositions du droit national relatives aux conditions de conservation des données de connexion par les opérateurs de communications électroniques, qui sont contestées au motif qu'elles seraient contraires au droit de l'Union européenne, ne sauraient être écartées sans priver de garanties effectives les objectifs de valeur constitutionnelle (OVC) de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infraction pénale et de lutte contre le terrorisme.

Il ressort en effet de l'article 12 de la Déclaration des droits de l'Homme et du citoyen de 1789 que la garantie des droits de l'homme et du citoyen, sans laquelle une société n'a point de constitution selon l'article 16 de la même Déclaration, nécessite une force publique. La sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales constituent des OVC, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée.

Selon le paragraphe 2 de l'article 4 du TUE, il appartient à l'Union, y compris à la CJUE, de respecter l'identité nationale des Etats membres, "inhérente à leurs structures fondamentales politiques et constitutionnelles", ainsi que "les fonctions essentielles de l'Etat, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale", cette dernière restant "de la seule responsabilité des Etats membres".

Il ressort de la jurisprudence de la CJUE, d'une part, que les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, qui contribuent à la protection des droits et des libertés d'autrui, sont au nombre des objectifs d'intérêt général reconnus par l'Union, comme tels susceptibles de justifier des limitations aux droits garantis par la Charte en vertu de son article 52, et, d'autre part, que si l'article 6 de la Charte, qui garantit le droit à la sûreté, ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer des infractions pénales, il découle de ses articles 3, 4 et 7, qui garantissent le droit au respect de l'intégrité

de la personne, l'interdiction de la torture et des peines et traitements inhumains ou dégradants et le respect de la vie privée et familiale, des obligations positives à la charge de l'Etat, incluant la mise en place de règles permettant une lutte effective contre certaines infractions pénales.

Toutefois, les exigences constitutionnelles mentionnées ci-dessus, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des Etats membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution.

Par suite, il revient au juge administratif d'examiner si, en écartant la règle de droit national contestée au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties effectives ces exigences constitutionnelles dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

Par son arrêt du 6 octobre 2020 La Quadrature du Net et autres (C-511/18, C-512/18, C-520/18), la Cour de justice de l'Union européenne (CJUE) a dit pour droit que la directive 2002/58/CE du 12 juillet 2002 ne s'opposait pas à ce que des mesures législatives permettent, aux fins de sauvegarde de la sécurité nationale, d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et des données de localisation, sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, pour une durée limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

Il ressort en outre du point 135 de cet arrêt que la responsabilité des Etats membres en matière de sécurité nationale, au sens du droit de l'Union, correspond à l'intérêt primordial de protéger les fonctions essentielles de l'Etat et les intérêts fondamentaux de la société, et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'Etat en tant que tel, telles que notamment des activités de terrorisme.

Ni l'article L. 34-1 du code des postes et des communications électroniques (CPCE) ni l'article 6 de la loi n° 2004-575 du 21 juin 2004 ne prévoient un réexamen périodique, au regard des risques pour la sécurité nationale, de la nécessité de maintenir l'obligation faite aux personnes concernées de conserver les données de connexion. Ces articles, ainsi, par suite, que l'article R. 10-13 du CPCE et le décret n° 2011-219 du 25 février 2011, en tant qu'ils ne subordonnent pas le maintien en vigueur de cette obligation au constat, à échéance régulière, qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible, pour la sécurité nationale sont, dans cette mesure, contraires au droit de l'Union européenne.

Il résulte de ce qui précède que, s'agissant de l'objectif de sauvegarde de la sécurité nationale, le refus d'abroger l'article R. 10-13 du CPCE et l'article 1er du décret du 25 février 2011 doit être annulé en tant seulement que leurs dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, s'agissant des données qu'elles mentionnent autres que celles afférentes à l'identité civile, aux comptes et aux paiements des utilisateurs et aux adresses IP.

Il y a lieu d'enjoindre au gouvernement de compléter ces dispositions dans un délai de six mois à compter de la présente décision.

Il ressort des pièces du dossier que la France est, à la date de la présente décision, confrontée à une menace grave, réelle et non seulement prévisible mais actuelle pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure (CSI) qui, par son intensité, revêt un caractère grave et réel. Cette menace est, à la date de la présente décision, non seulement prévisible mais aussi actuelle.

Tournez la page S.V.P.

Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés.

Par ailleurs, la France est particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique.

La France est également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes.

Dans la mesure où il résulte de la présente décision que la réalité et la gravité de la menace pesant sur la sécurité nationale justifient l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion à cette fin, les opérateurs ne sauraient, avant l'expiration du délai de six mois laissé au Gouvernement pour compléter les dispositions litigieuses, se soustraire à cette obligation et aux sanctions dont sa méconnaissance est assortie au motif que la durée de l'injonction qui leur est faite n'a pas été limitée dans le temps par le pouvoir réglementaire.

Les articles L. 851-1, L. 851-2, L. 851-4 et le IV de l'article L. 851-3 du code de la sécurité intérieure (CSI) relatifs aux modalités d'accès des services de renseignement aux données de connexion méconnaissent le droit de l'Union européenne, faute pour la Commission nationale de contrôle des techniques de renseignement (CNCTR) de disposer d'un pouvoir d'avis conforme.

L'annulation des décrets attaqués en tant qu'ils permettent l'application de ces dispositions sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée, ne saurait toutefois avoir pour conséquence d'entacher d'illégalité, pour le passé, l'usage par les services de renseignement des techniques prévues par ces articles que dans les hypothèses où le Premier ministre les aurait mises en œuvre, en dehors des cas d'urgence dûment justifiée, malgré un avis défavorable de la commission.

Or, il ressort des rapports publics de la commission que l'avis rendu par celle-ci préalablement à la mise en œuvre de ces techniques de renseignement, bien qu'étant dépourvu d'effet contraignant, a été, dans les faits, systématiquement suivi par le Premier ministre.

Il suit de là que l'annulation rétroactive des décrets attaqués, qui n'impliquerait par elle-même la suppression d'aucune donnée recueillie par les services de renseignement sur leur fondement, n'emporterait pas de conséquences manifestement excessives.

Par ailleurs, l'annulation des décrets attaqués, compte tenu de sa portée, implique seulement, dans l'attente de l'intervention des textes nécessaires à la mise en conformité du droit national avec le droit de l'Union européenne, qu'en cas d'avis défavorable de la CNCTR, le Premier ministre ne pourra légalement autoriser la mise en œuvre des techniques de renseignement mentionnées aux articles L. 851-1, L. 851-2, L. 851-4 et au IV de l'article L. 851-3 du CSI avant l'intervention de la décision du Conseil d'État, qu'il appartiendra alors à la commission de saisir en application de l'article L. 833-8 du même code.

Dans ces conditions, il n'y a pas lieu de différer dans le temps les effets de l'annulation ainsi prononcée.

<u>Document n° 9</u> : Accès et conservation des données de téléphonie soumis à des conditions strictes pendant la phase d'enquête, par Jean-Baptiste Thierry – Maître de conférences à l'Université de Lorraine

Mardi 12 juillet [2022], la Cour de cassation s'est notamment prononcée sur les conditions dans lesquelles les procureurs de la République pouvaient accéder et conserver les données de trafic et de localisation de personnes pendant une enquête. Ces arrêts ont donné à lieu à une réaction inédite et indignée de la Conférence nationale des procureurs de la République qui dénonce dans un communiqué « *un obstacle majeur à l'identification de délinquants et criminels* ».

Que contestaient les requérants devant la Cour de cassation et comment y répond-elle ?

Dans les quatre arrêts, les individus mis en examen contestaient le refus de différentes chambres de l'instruction d'avoir écarté les requêtes en nullité qu'ils avaient formées relatives aux conditions de conservation et d'accès à leurs données de trafic et de localisation (les données d'identité n'étaient pas en cause). Ils invoquaient pour cela la jurisprudence de la Cour de justice de l'Union européenne relative à l'interprétation de l'article 15 de la directive « vie privée » du 12 juillet 2002, lu à la lumière des dispositions de la Charte des droits fondamentaux de l'Union européenne. La CJUE a en effet une jurisprudence fournie sur cette question, qu'elle a progressivement précisée dans ses arrêts *Ministerio Fiscal*, *Quadrature du Net*, *Prokuratuur*, et *Commissioner of An Garda Siochana*.

La Cour de cassation rappelle en premier lieu le cadre de cette jurisprudence, pour constater que l'article L. 34-1 du Code des postes et des communications électroniques, dans sa version alors applicable, qui prévoyait une conservation généralisée et indifférenciée des données de connexion était conforme au droit de l'Union européenne en raison de la nécessité d'assurer la sauvegarde de la sécurité nationale. Ce raisonnement reprend celui que le Conseil d'État avait utilisé dans sa décision *French Data Network et autres* du 21 avril 2021. Elle relève ensuite que la « conservation rapide » des données est autorisée par la jurisprudence de la CJUE et qu'elle correspond en droit interne aux réquisitions informatiques prévues dans le code de procédure pénale. Toutefois, et comme l'exige le droit de l'Union, pour être régulière cette conservation rapide ne peut concerner que des faits relevant de la « criminalité grave » et être strictement nécessaire.

La Cour de cassation examine en deuxième lieu la question de l'accès à ces données et relève que les dispositions relatives aux réquisitions informatiques intervenant pendant l'enquête sont contraires au droit de l'Union. En effet, la CJUE exige que l'accès à ces données soit préalablement autorisé par une autorité indépendante. Cette indépendance – qui se rapproche plutôt de l'impartialité – suppose que l'autorité qui contrôle l'accès aux données de connexion ait la qualité de tiers par rapport à celle qui demande l'accès aux données. Or, dans sa décision *Prokuratuur*, la CJUE avait relevé que « *tel n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. En effet, le ministère public a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale* ». La Cour de cassation en déduit logiquement que la possibilité reconnue par le code de procédure pénale au procureur de la République d'autoriser l'accès aux données de connexion est contraire au droit de l'Union. En revanche, tel n'est pas le cas du 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, [et] doit être regardé comme étant habilité à contrôler l'accès aux données de connexion* ».

En dernier lieu, la Cour de cassation applique ces différents principes aux situations dont elle était saisie. De manière très pragmatique, elle précise les conditions de la nullité de réquisitions d'accès aux données de connexion. D'abord, il n'y a que la personne concernée qui peut l'invoquer : elle doit être titulaire ou utilisatrice de la ligne concernée. Ensuite, la nullité en cause est une cause de nullité d'ordre privé, c'est-à-dire qu'elle est soumise à la preuve d'un grief subi par la personne qui l'invoque. Or, « *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* ». Cette précision est particulièrement

Tournez la page S.V.P.

restrictive car la nullité ne pourra être prononcée que si les données auxquelles il a été accédé ont été conservées irrégulièrement – ce qui est hypothétique en ces temps de risque pour la sécurité nationale – et qu'il a été accédé à des données non strictement nécessaires à l'enquête. On le voit, cette précision de la Cour de cassation limitera considérablement les chances de succès des requêtes en nullité.

Concrètement, de quels pouvoirs se trouvent privés les procureurs et à quelles conditions pourront-ils désormais accéder aux données de connexion et de géolocalisation ?

Les procureurs étaient déjà privés factuellement de l'accès aux données de connexion pour les infractions les moins graves. Depuis la décision du Conseil constitutionnel du 3 décembre 2021, l'accès général et indifférencié aux données de connexion pendant l'enquête préliminaire avait déjà été réduit, pour des raisons différentes du droit de l'Union. En revanche, l'accès aux mêmes données pendant l'enquête de flagrance ne méconnaît pas les exigences constitutionnelles, pas plus que pendant l'information judiciaire.

Depuis la loi n° 2022-299 du 2 mars 2022, les conditions dans lesquelles il est possible d'avoir accès aux données de connexion pendant l'enquête (phase menée par le procureur de la République) ont été resserrées. Ainsi, seuls sont concernés les crimes et délits punis d'au moins trois ans d'emprisonnement, les délits punis d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques, les délits punis d'une peine d'emprisonnement lorsque l'accès concerne les équipements terminaux de la victime et intervient à la demande de celle-ci, ou les enquêtes permettant de retrouver une personne disparue.

Dans le cadre d'une enquête, l'accès aux données de connexion reste possible, mais il est conditionné par deux critères : celui de la criminalité grave, d'une part, et celui de la stricte nécessité, d'autre part. Il n'est exclu que pour les infractions les moins graves. Il sera donc indispensable que les procureurs de la République exercent un réel contrôle lors de la délivrance de l'autorisation d'accès à ces données. Jusqu'alors, la Cour de cassation avait une appréhension très compréhensive, pour ne pas dire permissive, de l'autorisation délivrée par le procureur de la République. En effet, elle jugeait de manière constante que cette autorisation n'est soumise à aucune forme particulière et qu'il n'est pas nécessaire que figure à la procédure « *la formalisation écrite et préalable d'une demande d'autorisation ou de cette autorisation elle-même ni l'indication de la forme sous laquelle cette autorisation a été donnée* ». Elle a également approuvé des juges du fond qui avaient refusé d'annuler des réquisitions qui « *s'inscrivent dans la logique de la première autorisation et s'enchaînent dans un ensemble cohérent, compte tenu des renseignements recueillis* ».

La Cour de cassation a en outre donné des indications pour apprécier le critère de la « criminalité grave » justifiant la conservation rapide des données : il faut prendre en compte la nature des agissements, l'importance du dommage qui en résulte, les circonstances de commission des faits et la durée de la peine encourue. Il s'agit donc d'une appréciation factuelle qui sera opérée par les juges du fond : aux procureurs de la République d'anticiper ces aspects pour réserver les réquisitions aux hypothèses les plus indiscutables.

Cela constitue-t-il à votre sens un obstacle à la lutte contre l'identification des délinquants et le critère de la criminalité grave vous parait-il opportun ?

Plutôt qu'un obstacle, il s'agit d'un changement de pratique. On passe d'une situation où il était possible d'accéder à toutes les données pour n'importe quelle infraction à une situation où un contrôle va devoir s'exercer sur la nécessité de l'accès aux données de trafic et de localisation. Il ne devient pas impossible, mais plus restreint, ce dont on ne peut que se féliciter au regard de la protection des droits. L'avocat général Frédéric Desportes mentionnait 1 726 144 réquisitions en 2021 aux fins d'obtention de données de connexion : on peut légitimement se demander si elles étaient toutes strictement nécessaires et l'idée qu'un contrôle s'opère sur l'accès n'apparaît pas saugrenue. La facilité d'accès et la grande tolérance dont la jurisprudence judiciaire faisait preuve jusqu'alors allaient à l'encontre du caractère très attentatoire à la vie privée que représentent la conservation et l'accès aux données de connexion. Sauf à aller expressément à l'encontre du droit européen, en mobilisant un principe inhérent à l'identité constitutionnelle de la France, la décision de la Cour de cassation était inéluctable. Elle n'a en revanche pas été anticipée, ce qui est regrettable.

Quant au critère de la criminalité grave, il ne paraît pas constituer un obstacle insurmontable pour les services d'enquête. Il est au contraire suffisamment souple pour justifier l'accès aux données de connexion. Les critères donnés par la Cour de cassation sont plus larges qu'une référence au seul quantum de la peine encourue. Dans les affaires ayant donné lieu aux arrêts du 12 juillet, la gravité ne faisait guère de doute : des faits de trafic de stupéfiants, d'enlèvement et séquestration en bande organisée, de meurtre et tentative de meurtre en bande organisée... Ce que les procureurs de la République ont regretté dans la prise de position – peu commune et critiquable – de la conférence nationale des procureurs de la République est la malléabilité du critère. On pourrait aisément répondre que cette malléabilité permettra justement de justifier l'accès aux données de connexion.

Les procureurs et enquêteurs doivent donc changer de culture de l'investigation. Les réactions sur la jurisprudence relative aux données de connexion ne sont pas sans rappeler celles qui étaient intervenues lors des décisions européennes et nationales sur l'absence de l'avocat pendant les interrogatoires d'une personne gardée à vue. Les craintes qui étaient alors exprimées ne se sont pas concrétisées : le grand pragmatisme de la Cour de cassation sur l'accès aux données de connexion devrait produire les mêmes effets. Si la téléphonie constitue un outil important, il faut tout de même se rappeler que ce n'est pas le seul et qu'il est, finalement, assez récent. Il ne s'agit pas de faire sans, mais de faire différemment.

Les décisions de la Cour de cassation, après celles de la CJUE, du Conseil constitutionnel et du Conseil d'État, parachèvent donc la construction jurisprudentielle de la protection des données de connexion. C'est désormais au législateur qu'il appartient de faire un choix permettant de prendre en compte ces exigences en confiant, par exemple, au juge des libertés et de la détention le soin d'opérer le contrôle de l'accès aux données. Ce qui n'est qu'une manière de revenir, une fois encore, sur la question des moyens de l'institution judiciaire.

Tournez la page S.V.P.

Document n° 10 : Articles du code des postes et communications électroniques

Article L.34-1 du code des postes et télécommunications

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonymes, sous réserve des II bis à VI, les données relatives aux communications électroniques.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II bis.- Les opérateurs de communications électroniques sont tenus de conserver :

1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

3° Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux.

III.-Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'État.

L'injonction du Premier ministre, dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées au premier alinéa du présent III.

III bis.-Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données.

IV. – Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le VI, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'État pris après avis de la

Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

V. – Sans préjudice des dispositions du III et du IV, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

VI. – Les données conservées et traitées dans les conditions définies aux II bis à V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, détermine, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II bis et III ainsi que les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Article R.10-13 du code des postes et communications électroniques (avant le 21 octobre 2021)

I. – En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ;

b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

e) Les données permettant d'identifier le ou les destinataires de la communication.

II. – Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

Tournez la page S.V.P.

III. – La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

IV. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

Article R.10-13 du code des postes et communications électroniques (après le 21 octobre 2021)

I.-Les informations relatives à l'identité civile de l'utilisateur, au sens du 1° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont :

1° Les nom et prénom, la date et le lieu de naissance pour une personne physique ou la raison sociale, ainsi que les nom, prénom, date et lieu de naissance de la personne agissant en son nom, lorsque le compte est ouvert au nom d'une personne morale ;

2° La ou les adresses postales associées ;

3° La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ;

4° Le ou les numéros de téléphone.

II.-Les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte, mentionnées au 2° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont :

1° L'identifiant utilisé ;

2° Le ou les pseudonymes utilisés ;

3° Les données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier, le cas échéant par l'intermédiaire d'un double système d'identification de l'utilisateur, dans leur dernière version mise à jour.

III.-Les informations relatives au paiement mentionnées au 2° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, pour chaque opération de paiement, lorsque la souscription du contrat ou la création du compte est payante, sont :

1° Le type de paiement utilisé ;

2° La référence du paiement ;

3° Le montant ;

4° La date, l'heure et le lieu en cas de transaction physique.

IV.-Les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, mentionnées au 3° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont :

1° L'adresse IP attribuée à la source de la connexion et le port associé ;

2° Le numéro d'identifiant de l'utilisateur ;

3° Le numéro d'identification du terminal ;

4° Le numéro de téléphone à l'origine de la communication.

V.-Les données de trafic et de localisation mentionnées au III de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver sur injonction du Premier ministre, sont :

1° Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

2° Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

3° Les données techniques permettant d'identifier le ou les destinataires de la communication, mentionnées aux 1° à 4° du IV du présent article ;

4° Pour les opérations effectuées à l'aide de téléphones mobiles, les données permettant d'identifier la localisation de la communication.

VI. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

Tournez la page S.V.P.

<u>Document n° 11</u> : Article 15 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 (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009

(15) Une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau.

<u>Document n° 12</u> : Données téléphoniques : le diable est dans la facture détaillée - Chronique de Stéphanie Marteau, *le Monde* 20 juillet 2022

Le recours aux fameuses « fadettes » par les policiers est désormais strictement encadré par une décision de la Cour de cassation. Privant magistrats et enquêteurs d'une pièce maîtresse de leurs procédures.

Au nom des libertés publiques

Les factures détaillées de téléphone portable (ou « fadettes »), très utilisées par la police judiciaire, vont-elles disparaître des procédures ? Pour se conformer au droit européen, la Cour de cassation a rendu, le 13 juillet, quatre arrêts encadrant le recours aux données de connexion par les enquêteurs. Les relevés d'appels et de SMS, ainsi que les données de géolocalisation, adresses IP et listes des sites Internet consultés, transmis aux policiers par les opérateurs téléphoniques, font désormais l'objet d'un contrôle très strict. Même si le téléphone est un facteur central d'élucidation des affaires judiciaires, le procureur de la République ne pourra plus, sans validation d'une autorité indépendante, ordonner de telles mesures d'investigation, considérées comme attentatoires aux libertés publiques.

Au cœur des procédures

Mises sur le devant de la scène par l'affaire Bettencourt, popularisées à ses dépens par Nicolas Sarkozy dans l'affaire dite « Paul Bismuth », le nom utilisé par l'ancien président pour son téléphone portable d'emprunt, les fadettes sont un incontournable de la procédure judiciaire. Si elles ne donnent pas accès au contenu des conversations (à la différence des écoutes), elles permettent de savoir qui appelle qui et quand, mais aussi de lire des échanges de SMS ou de savoir quand un suspect a acheté un billet d'avion en ligne et avec quel moyen de paiement. Les policiers les plus aguerris se souviennent qu'autrefois elles recensaient déjà les appels passés sur des lignes de téléphone fixe (comme dans l'affaire Grégory) et des fax. Les réquisitions que les enquêteurs adressent aux opérateurs téléphoniques et aux fournisseurs d'accès à Internet sont payantes, ce qui occasionne des frais de justice considérables.

Le parquet sous contrôle

La chambre criminelle de la Cour de cassation prévoit tout de même des exceptions pour les affaires de terrorisme, la haute criminalité organisée et pour « les infractions les plus graves ». Reste à définir ces dernières, ce que le droit européen ne fait pas. Les parquetiers, très remontés, attendent donc que la direction des affaires criminelles et des grâces traduise dans une circulaire les applications concrètes de ces arrêts. « Nous avons commencé à écrire aux officiers de police judiciaire pour leur dire de lever le pied sur les données de connexion », déplore le procureur d'Ajaccio, Nicolas Septe.

Enquêteurs désarmés

« *Ça va être un énorme problème. L'immense majorité des dossiers comporte des réquisitions téléphoniques* », prévient déjà Frédéric Lagache, du syndicat de police Alliance. C'est surtout la lutte contre la « délinquance du quotidien » (cambriolages, enlèvements d'enfants, trafic de stupéfiants, harcèlement, violences conjugales…) qui risque d'être entravée par ces mesures : « *Sur mon ressort, nous avons énormément de vols de voitures. Pas une enquête ne tient sans la téléphonie et le bornage ! Et puis, dans les dossiers de violences conjugales, où l'on manque souvent d'éléments de preuve, la téléphonie est cruciale et les SMS souvent décisifs* », plaide Jean-Baptiste Bladier, procureur de Senlis et président de la Conférence nationale des procureurs de la République, qui s'attend à voir déferler les requêtes en nullité. « *Le système judiciaire français n'est pas du tout en capacité d'appliquer ce que demande la Cour de cassation, prévient Nicolas Septe. Ce seront des centaines de réquisitions à faire auprès du juge de la liberté et de la détention !* » Voire des milliers chaque année, dans les plus grosses juridictions. Or les bras manquent toujours, dans les palais de justice.

* * * * *