Titre VII

Les cahiers du Conseil constitutionnel

DOSSIER

N° 2 - avril 2019

La protection des données à caractère personnel, domaine emblématique des interactions jurisprudentielles entre cours européennes et Conseil constitutionnel

Écrit par

Hélène SURREL

Professeure, Sciences Po Lyon, CEE-EDIEC, EA 4185

RÉSUMÉ

Les modalités actuelles de la protection constitutionnelle des données à caractère personnel attestent certainement de la réception implicite par le Conseil constitutionnel des jurisprudences européennes. Alors que les Cours de Strasbourg et de Luxembourg requièrent l'existence de garanties exigeantes entourant les traitements de données personnelles, ce dernier a, en effet, progressivement renforcé l'intensité de son contrôle. Ce constat d'une élévation du standard constitutionnel vaut tout particulièrement pour la constitution de fichiers et la mise en œuvre de mesures de surveillance des communications.

Résolument placée sous l'influence de la jurisprudence des cours européennes, l'appréhension de la protection des données à caractère personnel par le Conseil constitutionnel a connu des évolutions majeures. Ce domaine est, en effet, particulièrement emblématique des interactions jurisprudentielles qui contribuent à un renforcement de l'effectivité de la protection des droits des individus. L'arrêt *Tele2 Sverige AB* du 21 décembre 2016 de la Cour de justice de l'Union européenne (CJUE) illustre bien cette dynamique favorable à une élévation des standards de protection. Alors que, confrontée à un dispositif prévoyant, aux fins de lutter contre la criminalité, la conservation généralisée de données transmises par voie électronique, laquelle impliquait nécessairement un traitement de données personnelles, la Cour avait pris appui sur la jurisprudence strasbourgeoise [(1)], tandis que le Service juridique du Conseil constitutionnel pointe l'élévation du niveau de protection garanti par ce dernier en la mettant en perspective avec l'« élévation du niveau d'exigence en matière d'accès aux données de connexion (...) au niveau communautaire » [(2)].

Il est vrai aussi que des législations permettant des traitements de données personnelles, dont certains déclarés conformes à la Constitution, ont valu à la France des condamnations par la Cour européenne [(3)]. Mais, toujours est-il qu'il existe bien désormais une réelle proximité des jurisprudences européennes et constitutionnelle, convergence qui ne manque pas de faire écho à l'existence d'un consensus international et européen concernant les principes fondamentaux de la protection des données personnelles et les garanties que les Etats sont tenus de mettre en place, relevée par la Cour EDH dans l'affaire *Surikov c/ Ukraine* (26 janvier 2017, § 74).

© Source : Conseil constitutionnel

Prenant place dans le cadre d'une organisation pionnière pour ce qui est de la protection des données personnelles c'est-à-dire « toute information concernant une personne identifiée ou identifiable » [4], la Cour européenne a, très tôt, garanti le droit à leur protection au regard du droit au respect de la vie privée et imposé la fixation de « règles claires et détaillées » régissant les traitements de données et l'existence de « garanties suffisantes contre les risques d'abus et d'arbitraire » [5]. A ses yeux, ces traitements appellent un contrôle « rigoureux » [6]. Toutefois, l'étendue de la marge nationale d'appréciation varie principalement en fonction du caractère plus ou moins sensible des données concernées [7] mais aussi du but poursuivi Elle est ainsi étroite dans certains cas ou, au contraire, mais plus rarement, large [8].

S'inscrivant résolument dans le sillage de la jurisprudence strasbourgeoise, la Cour de justice a d'abord garanti cette protection *via* les principes généraux du droit, puis, à la suite de l'entrée en vigueur du traité de Lisbonne, au regard des articles 7 - sur le droit au respect de la vie privée - et 8 - sur le droit à la protection des données à caractère personnel - de la Charte des droits fondamentaux, les deux droits étant mobilisés conjointement. Mais il faut aussi rappeler que la protection des données personnelles s'inscrit, ici, dans le contexte particulier de leur libre circulation, le fait d'assurer un niveau de protection élevé et uniforme - *via* la directive 95/46/CE du 24 octobre 1995 puis le règlement (UE) 2016/679 du 27 avril 2016 (RGPP) - devant permettre d'éviter des entraves à la liberté de circulation au sein du marché intérieur.

La CJUE a précisé la nature de son contrôle au regard de la Charte dans l'arrêt précité *Volker Schecke GbR und Markus et a.*, dans lequel elle affirme que les limitations apportées au droit à la protection des données à caractère personnel « correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH » (pt 52) et ne manque pas de rappeler le caractère strict de son contrôle, s'accompagnant d'une marge d'appréciation réduite du législateur de l'Union, comme dans l'affaire *Digital Rights Ireland Ltd.* Renvoyant à la jurisprudence européenne, notamment l'arrêt *S. et Marper*, elle vérifie pareillement, au regard du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, l'existence de garanties contre les risques d'abus s'agissant de la conservation de données relatives à des communications électroniques qui, « prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes » [9].

Dans ce contexte, l'examen de la constitutionnalité des traitements de données personnelles, au regard de la liberté personnelle puis du droit au respect de la vie privée [10], a profondément évolué. La perméabilité de la jurisprudence constitutionnelle à l'influence des corpus prétoriens européens s'est notamment traduite par une modification générale des modalités du contrôle au regard de l'article 2 de la Déclaration. A compter de la décision n° 2012-652 DC, du 22 mars 2012, « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à l'objectif poursuivi » (cons. 8).

Le Conseil a également renforcé son contrôle des mesures de surveillance des individus, notamment lorsqu'elles sont susceptibles de donner accès à des données personnelles, rejoignant, dès lors, la jurisprudence de la CJUE sur les données de connexion et les métadonnées. Et s'il pratique encore, dans certains cas, un contrôle limité à l'absence de disproportion manifeste, cela n'emporte pas *ipso facto* un niveau de protection inférieur au standard européen. Les garanties européennes - substantielles et procédurales - entourant les traitements de données ont, en effet, été progressivement intégrées dans le cadre du contrôle de constitutionnalité.

Deux sortes de traitements de données sont ainsi particulièrement révélateurs des fortes interactions jurisprudentielles entre les cours européennes e le Conseil constitutionnel : la constitution de fichiers qui fait, dès lors, l'objet, d'un réel encadrement (I) et les mesures de surveillance de communications qui sont désormais strictement conditionnées (II).

I. La constitution de fichiers réellement encadrée

L'encadrement de la constitution de fichiers contenant des données personnelles concerne à la fois la mémorisation et l'accès aux données (A) et leur conservation (B).

A. La délimitation exigeante des conditions de mémorisation et d'accès aux données

Pour la Cour de Strasbourg, la protection des données à caractère personnel joue un « rôle fondamental » pour l'exercice du droit au respect de la vie privée. Aussi des « garanties appropriées » pour empêcher toute utilisation de ces données qui ne serait pas conforme aux garanties prévues dans l'article 8 doivent-elles être prévues [11], *a fortiori* s'agissant de données soumises à un traitement automatique et utilisées à des fins policières [12]. Dans cette perspective, leur conservation, dans un fichier, constitue une ingérence dans le droit au respect de la vie privée qui est jugée proportionnée au but légitime poursuivi seulement si les motifs la justifiant sont « pertinents et suffisants » [13].

Les données en jeu doivent être « pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées », l'existence d'un lien entre la finalité de leur traitement et leur consultation étant vérifiée. Le droit interne doit ainsi « contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs » [14].

© Source : Conseil constitutionnel

Ainsi, dans l'affaire *M. K. c/ France*, du 18 avril 2013, la Cour relève-t-elle les défaillances concernant le fichier automatisé des empreintes digitales. Ce dernier vise non seulement à faciliter la recherche et l'identification des auteurs de crimes et de délits mais aussi « la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie dont il n'est pas clairement indiqué qu'elle se limiterait aux crimes et délits ». Dans la mesure où le décret pertinent vise également « les personnes, mises en cause dans une procédure pénale, dont l'identification s'avère nécessaire », « il est susceptible d'englober de facto toutes les infractions » (§ 41). En outre, « aucune distinction fondée sur l'existence ou non d'une condamnation par un tribunal, voire même d'une poursuite par le ministère public » n'est opérée (§ 42). Or, le juge européen est particulièrement attentif au « risque de stigmatisation » de personnes qui n'ont été reconnues coupables d'aucune infraction et doivent bénéficier de la présomption d'innocence [(15)].

Le juge constitutionnel procède à un contrôle analogue dans la décision précitée n° 2012-652 DC, en jugeant des dispositions de la loi prévoyant le recueil et la conservation des données requises pour la délivrance du passeport et de la carte d'identité contraires à la Constitution « eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation » (cons. 11).

Alors même qu'il « est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française » et que les données biométriques enregistrées sont « particulièrement sensibles », la loi permet, en effet, que ce dispositif soit utilisé « à d'autres fins de police administrative ou judiciaire » (cons. 10) [(16)].

Le Conseil vérifie également si les autorités habilitées à consulter un fichier ont été précisément définies, comme dans la décision n° 2014-690 DC, du 13 mars 2014, à propos d'un registre national recensant des crédits à la consommation et visant à prévenir des situations de surendettement. Au regard de la nature des données, de l'ampleur du traitement en jeu, de la fréquence de son utilisation, du très grand nombre de personnes susceptibles d'y avoir accès et de l'insuffisance des garanties relatives à l'accès au registre, l'atteinte portée au droit au respect de la vie privée s'avère, ici, disproportionnée (cons. 52 et 57) [(17)].

L'absence d'une telle garantie peut aussi être sanctionnée sur le terrain de l'incompétence négative comme dans la décision n° 2018-765 DC, du 12 juin 2018, lorsque le législateur s'est borné à reproduire les termes du RGPD « sans déterminer lui-même ni les catégories de personnes susceptibles d'agir sous le contrôle de l'autorité publique, ni quelles finalités devraient être poursuivies par la mise en œuvre d'un tel traitement de données » (§ 45).

A contrario, le traitement automatisé de données personnelles par les organisateurs de manifestations sportives à but lucratif, en cause dans la décision n° 2017-637 QPC, du 16 juin 2017, est bien entouré de garanties suffisantes. Non seulement celles prévues par la loi n° 78-17 du 6 janvier 1978 sont applicables mais, en outre, le fichier ne peut recenser qu'une catégorie de personnes déterminée - celles « qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité de ces manifestations » - et ne peut être utilisé à d'autres fins que leur identification de façon à leur refuser l'accès aux manifestations sportives en cause (§ 14) [(18)].

B. Les garanties inhérentes à la conservation des données

Non seulement les données doivent être conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées mais, pour apprécier le caractère proportionné de leur durée de conservation au regard de l'objectif poursuivi par leur mémorisation, la Cour européenne tient aussi compte de l'existence ou non d'un contrôle indépendant de la justification de leur conservation, qui doit être fondé sur des critères précis, et donc des caractéristiques de la procédure d'effacement. Il s'agira, pour des traitements à des fins policières, de la gravité de l'infraction ou des arrestations antérieures [(19)]. En outre, comme cela a été souligné, le « risque de stigmatisation » de personnes qui n'ont été reconnues coupables d'aucune infraction fait l'objet d'une attention particulière. L'examen des traitements de données, par le Conseil, au regard de l'article 9 de la DDHC fait d'ailleurs écho à cette exigence [(20)].

La première garantie fait bien défaut pour le fichier national automatisé des empreintes génétiques en cause dans l'affaire *Aycaguer c/ France* (22 juin 2017). La conservation des profils ADN n'offre pas, en effet, une protection suffisante parce que la durée maximale de 40 ans est en pratique la norme (§ 42). En outre, la Cour européenne pointe l'absence de différenciation en fonction de la nature et de la gravité de l'infraction commise en dépit de la grande diversité des situations entrant dans le champ d'application de l'article 706-55 du CPP et alors même que le Conseil avait formulé une réserve d'interprétation, dans la décision n° 2010-25 QPC, du 16 septembre 2010, en jugeant les articles 706-54 à 706-56 du CPP conformes à la Constitution à condition « de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées » (cons. 18).

Le dispositif litigieux ne prévoit pas non plus de possibilité d'effacement des données pour les personnes condamnées, seules les personnes soupçonnées pouvant en bénéficier. La durée de conservation est donc disproportionnée par rapport à la nature des infractions et aux buts des restrictions.

Dans la droite ligne de cette jurisprudence, le Conseil estime, dans la décision précitée n° 2017-646/647 QPC, que l'impossibilité pour certaines

© Source : Conseil constitutionnel

personnes mises en cause dans une procédure pénale d'obtenir l'effacement de données figurant dans les fichiers d'antécédents judiciaires (art. 230-8, al. 1, du CPP) viole la Constitution.

Pouvant contenir « les informations recueillies au cours d'une enquête ou d'une instruction concernant une personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer à la commission de certaines infractions » c'est-à-dire des « données particulièrement sensibles », ces fichiers sont « susceptibles de porter sur un grand nombre de personnes dans la mesure où y figurent des informations concernant toutes les personnes mises en cause pour un crime, un délit et certaines contraventions de la cinquième classe » (§§ 9-11). Or, la durée maximale de conservation des données n'a pas été fixée par le législateur, le pouvoir réglementaire ayant prévu qu'elles puissent être conservées, en fonction de l'âge de l'individu concerné et de la nature de l'infraction, pendant une durée comprise entre cinq ans et quarante ans (article R. 40-27 du CPP) [(21)].

Par ailleurs, l'existence d'un contrôle indépendant est requise, ce qu'illustre l'affaire précitée *Brunet*, dans laquelle était en cause le fichier STIC.

Attentive au risque de stigmatisation précédemment évoqué, la Cour européenne estime que le requérant, ayant bénéficié d'un classement sans suite, ne devait, dès lors, pas être traité de la même façon qu'une personne condamnée (§ 39). Alors que la durée de conservation des données de 20 ans est importante au regard de l'absence de condamnation, le procureur n'avait pas compétence pour vérifier la pertinence du maintien des informations dans le STIC « au regard de la finalité de ce fichier, ainsi que des éléments de fait et de personnalité », ce qui ne répond pas à l'exigence d'effectivité requise (§ 42). Sa décision n'était, en outre, susceptible d'aucun recours. Partant, même si la conservation des données était limitée dans le temps, le requérant « n'a pas disposé d'une possibilité réelle de demander l'effacement des données le concernant » et, dans son cas, la durée prévue était « en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum » (§ 43).

A contrario, la procédure judiciaire d'effacement des données du fichier judiciaire national automatisé des auteurs d'infractions sexuelles assure un contrôle indépendant de la justification de la conservation des données dans l'affaire *Gardel c/ France* (17 décembre 2009), comme l'avait constaté le Conseil dans la décision précitée 2004-492 DC (notamment cons. 82).

L'« alignement » de la jurisprudence constitutionnelle sur le standard européen est donc bien réel.

II. Les mesures de surveillance strictement conditionnées

Si les juridictions européennes admettent très tôt l'existence de mesures de surveillance secrète nécessaires à la sécurité nationale ou à la prévention des infractions pénales [(22)], le développement des techniques de surveillance, notamment dans le cadre de la lutte contre le terrorisme, s'accompagne cependant, d'un renforcement concomitant des garanties octroyées aux individus [(23)]. Confrontées à des dispositifs de surveillance et d'interception des communications, elles ont donc non seulement affirmé qu'ils devaient répondre à une stricte nécessité [(24)] mais ont aussi déterminé la nature des garanties requises contre les abus qui, pour le juge de Strasbourg, doivent être « adéquates et suffisantes » [(25)].

Dans une approche analogue, la CJUE a précisé, de manière novatrice, les garanties assortissant la conservation et l'accès aux données de connexion, garanties d'autant plus importantes lorsqu'est en cause un traitement automatique des données. Exigeant des « règles claires et précises » et des « garanties suffisantes », elle impose l'existence d'un lien entre la conservation des données et la menace en cause et une délimitation de l'accès aux données et de leur utilisation comme des modalités de leur conservation. Elle se montre aussi très attentive à l'existence d'un contrôle indépendant [(26)].

La grille d'analyse progressivement façonnée par le juge constitutionnel s'avère très proche de celle des juridictions européennes. Les garanties portent à la fois sur le champ d'application des mesures de surveillance (A) et sur leur mise en œuvre (B).

A. La nécessaire détermination du champ d'application des mesures

Les cours européennes contrôlent la finalité et l'objet des mesures et censurent la surveillance généralisée. Ainsi en est-il de la CJUE, dans l'affaire précitée *Tele2 Sverige AB*, relative à l'obligation faite à des fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation concernant tous les abonnés et utilisateurs et tous les moyens de communication électronique et consistant donc en une « conservation généralisée et indifférenciée » de données permettant d'établir le profil des personnes concernées (pts 97 et 99)

Une telle ingérence, « particulièrement grave », ne peut être justifiée que par la seule lutte contre la criminalité grave mais un tel objectif n'est pas, à lui seul, de nature à la considérer comme nécessaire dans une société démocratique (pt 100). Et alors que la directive 2002/58/CE du 12 juillet 2002 postule que la conservation de données est l'exception, le système litigieux excède bien « les limites du strict nécessaire » dans la mesure où il ne prévoit « aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi » et « ne requiert aucune relation entre les données dont la

© Source : Conseil constitutionnel

conservation est prévue et une menace pour la sécurité publique » (pts 105-107).

Evidemment, un système de surveillance généralisée et indifférenciée, comme dans l'affaire *Mustafa Sezgin Tanrikulu c/ Turquie* (18 juillet 2017), viole aussi la CEDH. Était en cause, ici, une décision autorisant les services de renseignement à intercepter les communications téléphoniques et électroniques de toute personne se trouvant en Turquie dans le but d'identifier des personnes suspectées de participer à des activités terroristes.

Le Conseil constitutionnel vérifie pareillement que les catégories de personnes susceptibles d'être soumises à une mesure de surveillance ont bien été définies. La décision n° 2017-648 QPC, du 4 août 2017, relative à la constitutionnalité de l'article L. 851-2, § I, du code de la sécurité intérieure (CSI) permettant le recueil en temps réel, sur les réseaux des opérateurs et de certaines personnes, d'informations ou documents, en fournit une illustration

Ici, le législateur a opéré une conciliation équilibrée entre les intérêts concurrents lorsque la mesure de surveillance concerne « une personne préalablement identifiée susceptible d'être en lien avec une menace » (§ 10). La finalité poursuivie est, en effet, précisée - les besoins de la prévention du terrorisme - et l'objet délimité puisque ne peuvent « être recueillis que les informations ou documents traités ou conservés par les opérateurs de télécommunication, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service » (§ 7). En revanche, tel n'est pas le cas lorsque la procédure est appliquée aux personnes appartenant à l'entourage de la personne concernée par l'autorisation lorsqu'il y a des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations (§ 11).

La décision n° 2016-590 QPC, du 21 octobre 2016, atteste également de la qualité du contrôle opéré à propos de mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne obéissant à une procédure dérogatoire (art. L. 811-5 du CSI).

Se prononçant, comme la Cour européenne, au regard à la fois du droit au respect de la vie privée et du droit au secret des correspondances lorsqu'un accès au contenu des communications est rendu possible [(27)], le juge constitutionnel relève que si les mesures en jeu peuvent « être prises aux seules fins de défense des intérêts nationaux », leur utilisation « à des fins plus larges » n'est, cependant, pas exclue (§ 7). En outre, non seulement leur nature n'est pas définie mais la décision d'y recourir n'est entourée d'« aucune condition de fond ni de procédure » (§ 8).

De façon à s'assurer du respect effectif de ces conditions, la CJUE exige en principe que le déclenchement de la surveillance soit précédé d'un contrôle par une entité indépendante [(28)]. Le Conseil constitutionnel vérifie également l'existence d'une telle garantie comme dans la décision précitée n° 2017-648 QPC, dans laquelle il relève que les mesures de surveillance en jeu sont autorisées après avis préalable d'une autorité indépendante, la commission nationale de contrôle des techniques de renseignement (CNCTR). *A contrario*, la procédure dérogatoire de mise en œuvre de dispositifs de localisation en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement, instituée par la loi relative au renseignement, porte une atteinte disproportionnée au droit au respect de la vie privée et au secret des correspondances, en n'exigeant ni l'autorisation préalable du Premier ministre ou de l'un de ses collaborateurs directs habilités au secret de la défense nationale, ni la délivrance préalable d'un avis de la CNCTR (décision n° 2015-713 DC, 23 juillet 2015, cons. 29).

B. Les garanties entourant la mise en œuvre des mesures

La jurisprudence européenne requiert également l'existence de garanties au stade de la mise en œuvre des mesures de surveillance, que ce soit en ce qui concerne la détermination de leur durée ou un possible contrôle par une instance indépendante. Or, dans un nombre de cas non négligeable, le Conseil ne peut que constater l'absence totale de garanties entourant la mise en œuvre de procédures de réquisition de données comme dans la décision précitée n° 2016-590 QPC à propos de la surveillance des transmissions empruntant la voie hertzienne en vue de la défense des intérêts nationaux. Il en est de même du droit d'accès à des données de connexion conféré aux agents des services d'instruction de l'Autorité de la concurrence dans la décision n° 2015-715 DC, du 5 août 2015 (cons. 137), ou encore du dispositif prévu par le code monétaire et financier (art. L. 621-10, alinéa 1, seconde phrase) qui prévoit que les enquêteurs de l'Autorité des marchés financiers peuvent se faire communiquer certaines données conservées et traitées par les opérateurs de télécommunications, dans la décision précitée n° 2017-646/647 QPC [(29)].

Ici, le législateur n'a manifestement pas assuré une conciliation équilibrée entre le droit au respect privée et la prévention des atteintes à l'ordre public et la recherche des auteurs [] d'infractions. Se limitant à réserver l'exercice de ce droit à des agents habilités soumis au respect du secret professionnel sans leur conférer un pouvoir d'exécution forcée, il n'a prévu « aucune autre garantie » (§ 9).

Par ailleurs, le juge constitutionnel estime aussi, en se plaçant sur le terrain de l'incompétence négative, que la procédure de surveillance des communications émises ou reçues à l'étranger est contraire à la Constitution, dans la décision précitée n° 2015-713 DC. Le législateur n'a, en effet, défini « ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre » (cons. 78).

© Source : Conseil constitutionnel

Il relève, en revanche, l'existence de garanties suffisantes dans la décision précitée n° 2017-648 QPC. Le recueil de données, effectué par des agents qualifiés, est réalisé sous le contrôle de la CNCTR dont la composition et l'organisation consacrent l'indépendance, la définition de ses missions garantissant le caractère effectif de son contrôle (art. L. 833-1 à 11 du CSI). En outre, toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la CNCTR peut saisir le Conseil d'Etat à cette fin (§ 9) [(30)].

La procédure relative aux mesures de surveillance des communications électroniques internationales, en cause dans la décision n° 2015-722 DC du 26 novembre 2015, fournit aussi des garanties suffisantes, le législateur ayant « précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectés ainsi que celles du contrôle exercé par la commission nationale de contrôle des techniques de renseignement » (cons. 15).

On le voit, en réceptionnant implicitement les jurisprudences européennes qui prohibent le fichage et la surveillance généralisés, le Conseil constitutionnel a renforcé, de manière bienvenue, l'intensité du contrôle des atteintes susceptibles d'être portées au droit à la protection des données personnelles.

(1) La CJUE se réfère aux arrêts *Zakharov c/ Russie* (Gr., 4 déc. 2015) et *Szabo et Vissy c/ Hongrie* (12 janv. 2016), Gr. Ch., aff. C-203/15 et C-698/15, pts 119 et 120.

(2) Commentaire de la déc. n° 2017-646/647 QPC, 17 juill. 2017, Cons. const., site Internet, p. 14.

(3) Cour EDH, 18 sept. 2014, *Brunet c/ France* ; Cons. const., déc. n° 2003-467 DC, 13 mars 2003 et déc. n° 2011-625 DC, 10 mars 2011.

(4) Cour EDH, 16 février 2000, *Amann c/ Suisse*, § 65. Dans le même sens, CJUE, 9 nov. 2010, *Volker und Markus Schecke GbR et a.*, aff. C-92 et 93/09, pt 52.

(5) Cour EDH, 6 sept. 1978, *Klass et a. c/ Allemagne*, § 50.

(6) Cour EDH, 26 mars 1987, *Leander c/ Suède*, § 48.

(7) A la différence des « données intimes ou étroitement liées à (l') identité » d'une personne, des données bancaires ne requièrent pas une « protection accrue » (22 déc. 2015, *G.S.B. c/ Suisse*, § 93).

(8) Cour EDH, Gr. Ch., 4 déc. 2008, *S. et Marper c/ Royaume-Uni*, §§ 99, 102, 104, empreintes digitales, profils ADN et échantillons cellulaires ; déc., 11 janv. 2018, n° 38334/08, *Anchev c/ Bulgarie*, informations sur les personnes ayant collaboré avec les anciens services de sécurité.

(9) CJUE, Gr. Ch., 8 avr. 2014, aff C-293/12 et C-594/12, pt 27.

(10) Cons. const, déc. n° 91-294 DC, 25 juill. 1991, cons. 49 et déc. n° 99-416 DC, 23 juill. 1999, cons. 45.

(11) 25 févr. 1997, *Z. c/ Finlande*, § 95.

(12) *S. et Marper*, préc., § 103.

(13) *Ibid.*, § 86 et § 101.

(14) 17 déc. 2009, *B. B. c/ France*, § 61.

(15) § 36 ; *S. et Marper*, préc., § 122.

(16) Dans le même sens, déc., préc. n° 2017 - 670 QPC.

(17) Aussi Cons. const., déc. n° 2016-591 QPC, 21 oct. 2016, registre public des trusts pour lequel ni les motifs justifiant la consultation des données et ni les personnes habilitées à y accéder n'avaient été précisés.

(18) Aussi Cons. const., déc. n° 2004-492 DC, 2 mars 2004, définition stricte des personnes ayant accès au fichier automatisé des auteurs d'infractions sexuelles, cons. 83.

(19) *B.B.*, préc., § 61 ; *S. et Marper*, préc., § 119.

© Source : Conseil constitutionnel

(20) Par exemple, Cons. const., déc. préc. n° 2004-492 DC, cons. 88.

(21) Aussi Cons. const., déc. n° 2011-625, préc., disposition permettant aux enquêteurs de prolonger, au-delà de trois ans, la conservation des données personnelles révélées par l'exploitation des enquêtes réalisées au moyen de logiciels, cons. 72.

(22) Cour EDH, *Klass et a.*, préc., § 48.

(23) *Szabo et Vissy* , préc., § 68.

(24) *Klass et a* ., préc., § 42, *Szabo et Vissy*, préc., § 73 et CJUE, *Tele2 Sverige AB*, préc., pt 116.

(25) *Klass et a* ., préc., § 50.

(26) *Digital Rights Ireland Ltd* , préc. pts 54-64. Les demandes de renvoi devant la Grande chambre de la Cour EDH ayant été acceptées, les affaires *Centrum för Rättvisa c/ Suède* (19 juin 2018) et *Big Brother Watch et a. c/ Royaume-Uni* (13 sept. 2018) ne sont pas évoquées.

(27) Par exemple, *Zakharov*, préc., § 173.

(28) *Digital Rights Ireland Ltd* , préc., pt 62. Aussi art. 16 du TFUE et 8 de la Charte.

(29) Aussi Cons. const., déc. n° 2017-752 DC, 8 sept. 2017, § 59.

(30) Aussi Cons. const, déc. n°2015-478 QPC, 24 juill. 2015, réquisition administrative de données placée sous le contrôle permanent de la commission nationale de contrôle des interceptions de sécurité.

Citer cet article

Hélène SURREL. « La protection des données à caractère personnel, domaine emblématique des interactions jurisprudentielles entre cours européennes et Conseil constitutionnel », Titre VII [en ligne], n° 2, *De l'intégration des ordres juridiques : droit constitutionnel et droit de l'Union européenne*, avril 2019. URL complète : https://www.conseil-constitutionnel.fr/publications/titre-vii/la-protection-des-donnees-a-caractere-personnel-domaine-emblematique-des-interactions

© Source : Conseil constitutionnel