GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 237

Document de travail 01/2016 sur la justification des ingérences dans les droits fondamentaux à la vie privée et à la protection des données découlant de mesures de surveillance lors du transfert de données à caractère personnel (garanties essentielles européennes)

Adopté le 13 avril 2016

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant dans le domaine de la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site web: http://ec.europa.eu/justice/data-protection/index_en.htm

Table des matières

1. INTRODUCTION 3

2. INGERENCES DANS LES DROITS FONDAMENTAUX..... 4

3. LES GARANTIES ESSENTIELLES EUROPEENNES..... 6

4. GARANTIE A – LE TRAITEMENT DEVRAIT REPOSER SUR DES REGLES CLAIRES, PRECISES ET ACCESSIBLES 7

5. GARANTIE B – LA NECESSITE ET LA PROPORTIONNALITE AU REGARD DES OBJECTIFS LEGITIMES POURSUIVIS DEVRAIENT ETRE DEMONTREES 8

6. GARANTIE C – IL DEVRAIT EXISTER UN MECANISME INDEPENDANT DE CONTROLE 9

7. GARANTIE D – LES PARTICULIERS DEVRAIENT DISPOSER DE VOIES DE RECOURS EFFECTIVES..... 11

8. OBSERVATIONS FINALES 13

ANNEXE 1 – JURISPRUDENCE 14

1. Introduction

Le 6 octobre 2015, la Cour de justice de l'Union européenne (ci-après la «CJUE») a publié son arrêt de principe dans l'affaire *Maximillian Schrems/Data Protection Commissioner*[1]. À la suite d'une demande de décision préjudicielle introduite par la High Court (Haute Cour de justice) irlandaise, la CJUE a décidé d'annuler la «décision relative à la sphère de sécurité» au motif qu'il n'en ressortait pas assez clairement que la législation des États-Unis offrait des garanties suffisantes au regard de la protection des données à caractère personnel provenant de l'Union européenne (ci-après l'«UE»).

Avec l'invalidation de la décision relative à la sphère de sécurité, de nombreux transferts de données vers les États-Unis sont immédiatement devenus illégaux, car un très grand nombre d'entreprises se fondaient sur les dispositions d'une décision qui n'existait plus pour transmettre des données aux États-Unis. La CJUE a soulevé des questions quant à l'ampleur des possibles ingérences liées à la sécurité nationale et au respect des lois dans les droits fondamentaux[2] des personnes dont les données sont transférées depuis l'Union européenne vers les États-Unis. Étant donné que ces ingérences possibles ne se limitent pas aux données transférées en application de la décision relative à la sphère de sécurité, des doutes ont aussi été émis quant à la question de savoir si d'autres outils de transfert [clauses contractuelles ad hoc, clauses contractuelles types (ci-après «CCT»), règles d'entreprise contraignantes (ci-après «REC») et dérogations en vertu de l'article 26, paragraphe 1, de la directive 95/46/CE (ci-après la «directive»)] offraient des garanties suffisantes lors du transfert de données vers les États-Unis.

Par conséquent, le GT 29 a décidé, lors de sa réunion du 16 octobre 2015, d'évaluer les implications de l'arrêt Schrems pour tous les transferts de données vers les États-Unis. À cette fin, il a inventorié et analysé la jurisprudence de la CJUE en rapport avec les articles 7, 8 et 47 de la charte des droits fondamentaux (ci-après la «charte») et la jurisprudence de la Cour européenne des droits de l'homme (ci-après la «CEDH») en rapport avec l'article 8 de la convention européenne des droits de l'homme (ci-après la «convention») traitant des questions de surveillance dans les États parties à la convention. Considérée dans son ensemble, cette jurisprudence fournit des indications sur ce qui peut et ce qui ne peut pas être considéré comme une ingérence justifiée dans les droits fondamentaux dans une société démocratique. L'analyse a débouché sur ce que le GT 29 appelle les quatre garanties essentielles européennes (ci-après les «garanties»).

Ces garanties sont à distinguer du «niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive [européenne sur la protection des données], lue à la lumière de la Charte» auquel la CJUE fait référence. La CJUE place la barre à ce niveau substantiellement équivalent pour ce qui est de

[1] Les références de toute la jurisprudence citée dans la présente analyse figurent à l'annexe 1.
[2] Dans le présent document de travail, l'expression «droits fondamentaux» est tirée de la charte des droits fondamentaux de l'UE. Elle est toutefois également utilisée pour faire référence aux «droits de l'homme» tels que visés dans la convention européenne des droits de l'homme. De l'avis du GT 29, leur respect devrait être assuré de manière similaire.

l'obtention d'une décision constatant le caractère adéquat du niveau de protection telle que prévue à l'article 25, paragraphe 6, de la directive européenne sur la protection des données, tandis que les garanties essentielles européennes fournissent des indications pour évaluer si une ingérence dans un droit fondamental peut se justifier et s'appliquer à toutes les opérations de traitement de données, y compris aux transferts effectués en application des articles 25 et 26 de la directive.

Le présent document de travail replace les quatre garanties essentielles européennes dans leur contexte. Le GT 29 tient à souligner que ces garanties reposent principalement sur la jurisprudence de la CJUE et de la CEDH. Il convient toutefois de les lire en liaison avec l'interprétation que le GT 29 a donnée à divers éléments du cadre juridique de l'UE en matière de protection des données dans ses avis précédents. En ce qui concerne les transferts de données vers les États-Unis, le GT 29 renvoie à son avis 01/2016 sur le niveau de protection assuré par le bouclier de protection des données UE-États-Unis, qui comprend une analyse des garanties essentielles européennes pour ce qui est des transferts de données vers les États-Unis.

2. Ingérences dans les droits fondamentaux

Les droits fondamentaux à la vie privée et familiale et à la protection des données sont inscrits aux articles 7 et 8 de la charte et s'appliquent à tous. L'article 8 fournit en outre des orientations de base en matière de traitement des données: il exige notamment la limitation des finalités, le contrôle indépendant par une autorité de contrôle et la disponibilité d'une base juridique prévue par la loi, et prévoit des droits d'accès et de rectification. Dans l'arrêt Schrems, la CJUE rappelle qu'«une réglementation de [l'UE] comportant une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte doit, selon la jurisprudence constante de la Cour, prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données»[3]. Il convient d'assurer ce niveau de protection des droits fondamentaux contre les ingérences arbitraires lorsque des données sont transférées vers un pays considéré comme offrant un niveau de protection adéquat sur la base de l'article 25 de la directive. Un régime similaire devrait s'appliquer aux transferts de données fondés sur l'article 26 de la directive, ne serait-ce que parce que les droits fondamentaux s'appliquent de manière générale et pas uniquement en fonction de la base juridique du transfert de données. En outre, il est à noter que l'article 4 des CCT, en application de l'article 26, paragraphe 4, de la directive, requiert des autorités chargées de la protection des données qu'elles évaluent si le droit d'un pays tiers oblige l'importateur de données «à déroger au droit applicable à la protection des données au-delà des limitations nécessaires dans une

[3] Arrêt Schrems, point 91.

société démocratique»[4]. Le résultat de l'évaluation du respect des droits fondamentaux dans un cas précis peut cependant être différent de ce qu'il serait aux fins de l'approbation générale des transferts de données vers un pays tiers.

La protection des droits fondamentaux offerte en Europe en ce qui concerne les données à caractère personnel ne repose pas seulement sur le droit de l'UE, mais également sur les dispositions de la convention[5]. Récemment, la CEDH, dans l'affaire Zakharov, a réitéré sa position au sujet des ingérences dans le droit fondamental à la vie privée. Celles-ci ne peuvent se justifier que si elles sont prévues par la loi, visent un but légitime et sont nécessaires, dans une société démocratique, pour atteindre ce but[6].

Tant la charte que la convention soumettent les limitations des droits dont elles assurent la protection à des critères de nécessité et de proportionnalité[7]. L'article 52, paragraphe 1, de la charte précise la portée de la limitation possible des articles 7 et 8 en indiquant que «[t]oute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.»

Dans le même temps, la clause de limitation figurant à l'article 8, paragraphe 2, de la convention dispose également qu'«[i]l ne peut y avoir ingérence d'une autorité publique dans l'exercice [du droit au respect de la vie privée et familiale] 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 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».

D'après les deux juridictions, toute limitation des droits fondamentaux à la vie privée et à la protection des données ou toute ingérence dans ces droits (c'est-à-dire la collecte, la conservation, l'accès ou l'utilisation et la diffusion de données à caractère personnel concernant un particulier à des fins autres que celles pour lesquelles les données ont été transférées initialement, relevant de la sécurité nationale ou du renseignement) ne peut se justifier que si elle est «strictement nécessaire dans une société démocratique».[8] Dans leurs arrêts et leurs décisions, les juridictions ont décrit de manière relativement détaillée ce

[4] Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 96/46/CE du Parlement européen et du Conseil (2010/87/UE).
[5] Le GT 29 rappelle l'article 6, paragraphe 3, du traité UE, selon lequel «[l]es droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux».
[6] CEDH, arrêt Zakharov, paragraphe 227.
[7] Pour en savoir plus, voir http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15%281997%29.pdf.
[8] CEDH, arrêt Klass, paragraphes 42 et 48; CEDH, arrêt Malone, paragraphe 81; etc.

qu’elles considèrent être nécessaire dans une société démocratique, notamment l’exigence que toute mesure prise soit prévue par la loi et offre «un minimum de garanties contre les abus»[9].

Par ailleurs, lorsqu'elle évalue la nécessité d'une mesure, la CEDH dit invariablement que les États parties disposent «d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale»[10]. Naturellement, ce droit qu'ont les États d'adopter une législation destinée à préserver la sécurité nationale ou de collecter des données à des fins de renseignement est également reconnu par le GT 29. En outre, la collecte de renseignements peut constituer un but parfaitement légitime au regard du traitement de données à caractère personnel, comme l'a également souligné la CEDH, notamment dernièrement dans l’affaire Szabó[11]. Elle peut même comporter le recours à des mesures de surveillance secrète, pour autant que des garanties adéquates et suffisantes contre les abus soient en place et empêchent que cette surveillance «sap[e], voire [...] détrui[se], la démocratie au motif de la défendre»[12].

En principe, toutes les opérations de traitement de données, y compris les mesures de surveillance[13], constituent une ingérence, en particulier lorsque des données relatives à la vie privée d’un particulier sont mémorisées par une autorité publique[14] et/ou lorsque des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication sont obligés de conserver des données relatives à la vie privée d’une personne et à ses communications[15]. L’accès d’une autorité (répressive) compétente aux données constitue une ingérence supplémentaire[16]. Pour établir l'existence d'une ingérence, «il importe peu [...] que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d’éventuels inconvénients»[17].

Tant la CJUE que la CEDH ont indiqué clairement dans leurs arrêts et leurs décisions qu’il leur appartenait en dernier ressort de déterminer si des ingérences dans un droit fondamental pouvaient se justifier. Cependant, en l’absence d’un tel arrêt ou d'une telle décision et en vertu de la jurisprudence constante, les autorités chargées de la protection des données sont habilitées à examiner des cas individuels, soit d’office, soit à la suite d’une plainte, afin de décider si un transfert de données peut (continuer d') avoir lieu si elles constatent une ingérence dans les droits fondamentaux à la vie privée et à la protection des données.

3. Les garanties essentielles européennes

Le GT 29 s’est fondé sur la jurisprudence pour définir ce qu’il appelle les *garanties essentielles européennes* qui devraient être en place pour faire en sorte que les ingérences

[9] CJUE, arrêt Schrems, point 91 et jurisprudence citée.
[10] CEDH, décision Weber et Saravia, paragraphe 106.
[11] CEDH, arrêt Szabó, paragraphe 57.
[12] CEDH, arrêt Szabó, paragraphe 57.
[13]CEDH, arrêt Malone, paragraphe 64.
[14] CEDH, arrêt Amman, paragraphe 70.
[15] CJUE, arrêt Digital Rights Ireland, point 34.
[16] CEDH, arrêt Leander, paragraphe 48; CEDH, arrêt Rotaru, paragraphe 46; CJUE, arrêt Digital Rights Ireland, point 35.
[17] CJUE, arrêt Schrems, point 87 et jurisprudence citée.

n'aillent pas au-delà de ce qui est nécessaire dans une société démocratique. Les garanties essentielles européennes reposent principalement sur la jurisprudence de la CJUE et de la CEDH dans des affaires liées à l'application des droits à la vie privée et à la protection des données en Europe. Cela signifie qu'elles s'appliquent avant tout dans les États membres de l'Union européenne et du Conseil de l'Europe et à ces États membres lorsque ceux-ci appliquent une législation européenne ou nationale qui implique une ingérence dans ces droits. Puisque les données transférées en dehors de l'UE devraient bénéficier d'une protection constante contre toute ingérence arbitraire, les garanties essentielles européennes devront également être dûment prises en considération dans le cadre de tous les transferts vers des pays tiers.

Le GT 29 souligne que les garanties sont fondées sur les droits fondamentaux qui s'appliquent à tous, indépendamment de la nationalité.

À la suite de l'analyse de la jurisprudence, le GT 29 est parvenu à la conclusion que les exigences pouvaient être résumées en quatre garanties essentielles européennes:

A. le traitement devrait reposer sur des règles claires, précises et accessibles;
B. la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis devraient être démontrées;
C. il devrait exister un mécanisme indépendant de contrôle;
D. les particuliers devraient disposer de voies de recours effectives.

4. Garantie A – le traitement devrait reposer sur des règles claires, précises et accessibles

Pour être justifiée, une ingérence doit tout d'abord être prévue par la loi. Les conséquences de l'ingérence pour le particulier doivent être prévisibles, de sorte que celui-ci bénéficie d'une protection adéquate contre toute ingérence arbitraire. Dès lors, le traitement doit reposer sur une base juridique précise, claire et accessible (c'est-à-dire publique)[18]. Cette base juridique devrait dans tous les cas être inscrite dans la loi, laquelle devrait notamment renfermer la nature des infractions susceptibles de donner lieu à un mandat d'interception ou de surveillance, la définition des catégories de personnes susceptibles de faire l'objet d'une surveillance, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies et les précautions à prendre pour la communication des données à d'autres parties[19]. Elle doit également contenir les circonstances et les conditions matérielles et procédurales afférentes à l'accès des autorités compétentes.[20] Enfin, la Cour «ne voit aucune raison de soumettre les règles gouvernant l'interception de communications individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents»[21].

[18] CEDH, arrêt Malone, paragraphes 65, 66 et 70.
[19] CEDH, décision Weber et Saravia, paragraphe 95.
[20] CJUE, arrêt Digital Rights Ireland, point 61.
[21] CEDH, arrêt Liberty, paragraphe 63.

La CEDH a rappelé dans l'affaire Zakharov que, «en matière d'interception de communications, la "prévisibilité" ne pouvait se comprendre de la même façon que dans beaucoup d'autres domaines». Elle a précisé que, dans le contexte des mesures de surveillance secrète, telle l'interception de communications, «la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence». Cependant, étant donné que le risque d'arbitraire apparaît avec netteté dans ce type de situation, «[l']existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît [...] indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes.[22]»

5. Garantie B – la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis devraient être démontrées

Tout traitement de données par des autorités publiques est, par définition, constitutif d'une ingérence dans le droit à la vie privée et à la protection des données[23]. Cela vaut également pour le traitement de données par des autorités publiques à des fins de renseignement, qui peut néanmoins être justifié, à la condition qu'il soit nécessaire et proportionné par rapport à un objectif légitime.

Dans l'arrêt Schrems, la CJUE a indiqué ce qui suit: «Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données[24].»

Dans l'arrêt Szabó, une chambre de la CEDH indique que «face à ces progrès, la Cour doit examiner la question de savoir si la mise au point de méthodes de surveillance impliquant la collecte massive de données s'accompagne de la mise en place simultanée de garanties juridiques assurant le respect des droits dont les citoyens jouissent en vertu de la convention. [...] En effet, les mesures prises par les pouvoirs publics pour tenir le terrorisme en échec et rétablir ainsi la confiance des citoyens dans leurs capacités à maintenir la sécurité publique perdraient tout leur sens si la menace terroriste était paradoxalement remplacée par la perception d'une menace d'ingérence illimitée du pouvoir exécutif dans la sphère privée des citoyens au moyen de techniques et de prérogatives de surveillance de grande envergure ne faisant l'objet d'aucune restriction. [...] Cette menace pour la vie privée doit être soumise à un

[22] CEDH, arrêt Zakharov, paragraphe 229.
[23] Voir, par exemple, CJUE, arrêt Digital Rights Ireland, point 36.
[24] CJUE, arrêt Schrems, point 93.

contrôle très approfondi à la fois sur le plan intérieur et dans le cadre de la convention. [...] L'examen de cette question ne se justifie cependant pas en l'espèce.[25]»

Dans l'arrêt Digital Rights Ireland, la CJUE laisse entendre qu'une législation couvrant «toute personne et tous les moyens de communication électronique» devrait comporter une «différenciation, limitation [ou] exception»[26]. En outre, la CJUE considère que le législateur doit prévoit un «critère objectif permettant de délimiter l'accès [...] aux données et leur utilisation ultérieure». [27]

Dans le même temps, dans l'arrêt Zakharov, la Grande Chambre de la CEDH précise que «l'existence d'un soupçon raisonnable à l'égard de la personne concernée»[28], qui doit être clairement désignée au moyen de ses nom, adresse, numéro de téléphone ou d'autres informations pertinentes[29], doit être vérifiable, ce qui semble indiquer que seule la collecte ciblée de données devrait être autorisée.

Les juridictions ne semblent pas s'être prononcées définitivement sur la légalité de la collecte massive et non sélective (c'est-à-dire la collecte de masse non ciblée) de données à caractère personnel et de l'utilisation ultérieure de ces données ni, en particulier, sur les circonstances dans lesquelles une telle collecte et une telle utilisation de données à caractère personnel pourraient avoir lieu. La CJUE devrait aborder cette question, au moins dans une certaine mesure, au cours de l'année 2016, dans les affaires jointes Tele2 Sverige AB/Post- och telestyrelsen et Secretary of State for the Home Department/Davis e.a.[30] et dans l'avis à rendre sur la validité de l'accord UE-Canada sur les données des dossiers passagers (PNR)[31].

Pour ce qui est du contenu des données de communication, la CJUE est plus claire. Elle a indiqué dans l'arrêt Schrems que les autorités publiques ne devraient pas être autorisées à accéder de manière généralisée au contenu de communications électroniques[32]. Une réglementation permettant aux autorités publiques d'avoir un tel accès doit en effet être considérée comme portant atteinte non seulement au droit, mais «au contenu essentiel du droit fondamental au respect de la vie privée»[33]. Toutefois, la Cour ne précise pas ce qu'elle entend par «de manière généralisée».

6. Garantie C – il devrait exister un mécanisme indépendant de contrôle

Depuis les années 1970, la CEDH estime que toute ingérence dans le droit à la vie privée et à la protection des données devrait être soumise à un système de contrôle effectif, indépendant et impartial, prévu par un juge ou par un autre organe indépendant[34] (par exemple, une

[25] CEDH, arrêt Szabó, paragraphes 68 à 70.
[26] CJUE, arrêt Digital Rights Ireland, point 57.
[27] CJUE, arrêt Digital Rights Ireland, point 60.
[28] CEDH, arrêt Zakharov, paragraphe 260.
[29] CEDH, arrêt Zakharov, paragraphe 264.
[30] CJUE, affaires jointes C-203/15 et C-698/15.
[31] CJUE, affaire A-1/15.
[32] CJUE, arrêt Schrems, point 94.
[33] CJUE, arrêt Schrems, point 94.
[34] CEDH, arrêt Klass, paragraphes 17 et 51.

autorité administrative ou un organe parlementaire). Quelle que soit la forme du contrôle indépendant, l'existence d'autorités de contrôle constitue «un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel»[35]. Le GT 29 rappelle qu'une ingérence a lieu au moment de la collecte des données, mais également au moment où une autorité publique accède à ces données en vue de leur traitement ultérieur à des fins de renseignement.

La CEDH considère qu'un contrôle indépendant peut être exercé à différents stades du cycle de vie d'une opération de traitement de données: lorsqu'on ordonne la surveillance, pendant qu'on la mène et/ou après qu'elle a cessé[36]. Compte tenu de la nature particulière du traitement de données à des fins de renseignement, il est admis que le traitement ait lieu sans que la personne concernée en soit informée, en tout cas lors du lancement et au cours de l'opération de surveillance. La CEDH a précisé ce qui suit: «Concernant les deux premières phases, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. [...] En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le pouvoir judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière.[37]»

La CJUE précise que «[...] l'accès aux données conservées [...] [devrait être] subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales[38]».

Il convient de noter que la CEDH semble avoir tiré ses conclusions dans des affaires concernant des écoutes téléphoniques, dans lesquelles il serait difficile de distinguer l'autorisation préalable de collecter les données de l'accès ultérieur aux données. En revanche, la citation de la CJUE provient de l'affaire Digital Rights Ireland relative à la conservation des données, qui portait sur des métadonnées, ce qui, en vertu de la législation concernée, implique la collecte massive de données non ciblées.

En ce qui concerne le contrôle a posteriori, il est essentiellement lié aux voies de recours dont disposent les particuliers. Cet aspect est abordé dans le cadre de la garantie D. Il est souligné que, dans certaines situations, des contrôles a posteriori pourraient également être réalisés d'office afin de vérifier la conformité des mesures de surveillance avec la législation

[35] CJUE, arrêt Commission/Allemagne, point 23.
[36] CEDH, arrêt Klass, paragraphes 55 et 56; CEDH, arrêt Zakharov, paragraphe 233.
[37] CEDH, arrêt Zakharov, paragraphe 233.
[38] CJUE, arrêt Digital Rights Ireland, point 62. La Cour l'a indiqué clairement en déclarant que la directive sur la conservation des données était invalide car elle ne répondait pas à ces exigences.

applicable. À la connaissance du GT 29, les juridictions n'ont pas fixé de critères spécifiques afférents à de tels contrôles réalisés d'office et a posteriori.

En ce qui concerne l'indépendance des mécanismes de contrôle des mesures de surveillance, la Cour de Strasbourg a indiqué préférer qu'un juge soit chargé du contrôle. Il n'est toutefois pas exclu qu'un autre organe puisse en être chargé, «à condition que cet organe soit suffisamment indépendant à l'égard de l'exécutif»[39] et «des autorités qui procèdent à la surveillance [et qu'il soit] invest[i] de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent»[40]. La CEDH ajoute que «le mode de désignation et le statut juridique des membres de l'organe de contrôle»[41] doivent être pris en compte dans l'appréciation de l'indépendance. Elle considère comme indépendantes les «personnes possédant les qualifications requises pour accéder à la magistrature et nommées soit par le parlement soit par le Premier ministre. En revanche, elle a jugé insuffisamment indépendant un ministre de l'Intérieur qui non seulement était nommé par le pouvoir politique et membre de l'exécutif, mais de plus était directement impliqué dans la commande de moyens spéciaux de surveillance.[42]» De plus, «il est essentiel selon la [CEDH] que l'organe de contrôle ait accès à tous les documents pertinents, y compris à des informations confidentielles»[43]. Enfin, la CEDH tient compte de la question de savoir «si les activités de l'organe de contrôle sont ouvertes à un droit de regard du public»[44].

En ce qui concerne spécifiquement les autorités chargées de la protection des données, la CJUE a, dans trois affaires, donné son avis sur ce que suppose l'indépendance à la lumière de la directive. Étant donné que certaines autorités chargées de la protection des données sont également compétentes pour contrôler les opérations de traitement de données à des fins de renseignement, la norme fixée par la CJUE pourrait être utile dans ces situations particulières. Tout d'abord, l'indépendance signifie que les autorités doivent exercer leurs missions sans être soumises à une influence extérieure. «[L']indépendance exclut notamment toute injonction et toute autre influence extérieure sous quelque forme que ce soit, qu'elle soit directe ou indirecte, qui seraient susceptibles d'orienter leurs décisions [...].[45]» La Cour rappelle également que «[l']indépendance fonctionnelle ne suffit pas, à elle seule, à préserver ladite autorité de contrôle de toute influence extérieure»[46].

7. Garantie D – les particuliers devraient disposer de voies de recours effectives

La dernière garantie essentielle européenne a trait aux droits de recours dont bénéficient les particuliers. Ces derniers doivent disposer d'une voie de recours effective pour faire valoir leurs droits s'ils estiment que ceux-ci ne sont pas respectés. Dans l'arrêt Schrems, la CJUE a expliqué qu'«une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer

[39] CEDH, arrêt Zakharov, paragraphe 258.
[40] CEDH, arrêt Klass, paragraphe 56.
[41] CEDH, arrêt Zakharov, paragraphe 278.
[42] CEDH, arrêt Zakharov, paragraphe 278.
[43] CEDH, arrêt Zakharov, paragraphe 281.
[44] CEDH, arrêt Zakharov, paragraphe 283.
[45] CJUE, arrêt Commission/Hongrie, point 51 et jurisprudence citée.
[46] CJUE, arrêt Commission/Autriche, point 42.

des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article.[47]»

Pour la CEDH, la question du recours effectif est inextricablement liée à la notification de la mesure de surveillance à la personne concernée une fois la surveillance terminée. «La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure.[48]»

En l'absence de notification, la CEDH a précisé dans l'affaire Kennedy qu'elle considérait qu'une juridiction offrait des possibilités de recours suffisantes si celle-ci remplissait une série de critères: être un organe indépendant et impartial, qui a édicté son propre règlement de procédure et dont les membres exercent ou ont exercé de hautes fonctions judiciaires ou sont des juristes chevronnés. Lorsqu'elle examine les griefs d'un justiciable, la juridiction devrait avoir accès à toutes les informations pertinentes[49], y compris les informations confidentielles. Enfin, elle devrait avoir le pouvoir de remédier à la non-conformité[50].

La question est de savoir si une voie de recours effective ne peut être fournie que par une juridiction ordinaire ou si elle peut l'être également par un autre organe qui est suffisamment indépendant et dispose de pouvoirs suffisants pour remédier à la non-conformité. L'article 47 de la charte fait référence à un tribunal, alors que, dans des versions linguistiques autres que le français et l'anglais, la préférence est donnée au terme «juridiction»[51]. Dans le même temps, la convention oblige seulement les États membres à garantir que «[t]oute personne dont les droits et libertés [...] ont été violés [...] a droit à l'octroi d'un recours effectif devant une instance nationale.[52]» Il ne doit pas nécessairement s'agir d'une institution judiciaire, comme la CEDH l'a précisé dans l'arrêt Klass[53]. Néanmoins, la Cour de Strasbourg a de fortes attentes à l'égard de l'organe octroyant le recours effectif, ainsi qu'elle l'a clairement fait savoir dans l'arrêt Kennedy.

---

[47] CJUE, arrêt Schrems, point 95.
[48] CEDH, arrêt Zakharov, paragraphe 234.
[49] Le GT 29 souligne que le commissaire aux droits de l'homme du Conseil de l'Europe considère que la règle dite du «tiers service» – selon laquelle les agences de renseignement d'un pays qui fournissent des données aux agences de renseignement d'un autre pays peuvent leur imposer de ne pas divulguer ces données à des tiers – ne devrait pas s'appliquer aux organes de contrôle afin de ne pas compromettre la possibilité d'un recours effectif (document thématique sur la surveillance démocratique et effective des services de sécurité nationale).
[50] CEDH, arrêt Kennedy, paragraphe 167.
[51] Le terme «tribunal» a par exemple été traduit par «Gericht» en allemand et par «gerecht» en néerlandais.
[52] Article 13 de la convention.
[53] CEDH, arrêt Klass, paragraphe 67.

8. Observations finales

Les quatre garanties essentielles européennes qui sont décrites dans le présent avis ne sont pas des garanties inconditionnelles. De plus, compte tenu de la manière dont elles sont formulées, il devrait être clair qu'elles nécessitent toutes les quatre un certain degré d'interprétation.

Si un pays tiers permet des ingérences allant au-delà de ce qu'il convient de considérer comme strictement nécessaire dans une société démocratique, un particulier peut faire appel à son autorité chargée de la protection des données pour l'aider à examiner la question et à protéger ses droits fondamentaux. Le GT 29 souligne que les autorités chargées de la protection des données procéderont à une analyse sur une base individuelle ou en vue d'approuver (ou d'évaluer) des transferts de données massifs, structurels ou répétitifs sur la base de l'un des outils de transfert. Le résultat de cette analyse pourra varier et les mesures d'exécution pourront consister, entre autres, à interdire ou à suspendre des transferts de données au cas par cas.

Le GT 29 fait observer que l'interprétation de la garantie essentielle européenne B (l'obligation de démontrer la nécessité et la proportionnalité) pourrait faire l'objet d'une mise à jour dans le courant de l'année 2016, lorsque la CJUE aura publié ses décisions dans les affaires PNR Canada, Tele2 Sverige et Davis. Dans l'intervalle, le GT 29 rappelle qu'il a toujours estimé que la collecte massive et non sélective (ou collecte de masse non ciblée) de données ne pouvait en aucun cas être considérée comme proportionnée[54].

Dans le cadre de l'analyse, il convient de considérer les garanties essentielles européennes non pas séparément mais ensemble, en examinant la législation applicable à la collecte de données à des fins de surveillance, le niveau minimal de garanties pour la protection des droits des personnes concernées et les voies de recours prévues par la législation nationale du pays tiers. Comme la CEDH l'a indiqué dans l'arrêt Kennedy, «[l']appréciation de cette question dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne»[55].

Le GT 29 souligne que les garanties sont fondées sur les droits fondamentaux qui s'appliquent à tous, indépendamment de la nationalité. En outre, il convient de noter qu'elles reposent sur ce qui est exigé par la loi et pas nécessairement sur ce qui constitue la pratique actuelle dans les États membres de l'UE. Le GT 29 n'applique pas deux poids deux mesures et a donc déjà invité plusieurs fois les États membres à faire en sorte que leur législation en matière de surveillance soit conforme à la jurisprudence de la CJUE et de la CEDH.

[54] WP 215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf
[55] CEDH, arrêt Kennedy, paragraphe 153.

Annexe 1 – Jurisprudence

Tout au long du présent avis, il est fait référence à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. Les références des différentes affaires, y compris des affaires pertinentes qui ne sont pas explicitement mentionnées, mais qui ont été utilisées pour élaborer le présent avis, sont les suivantes:

- Amman c. Suisse
  Cour européenne des droits de l'homme, 16 février 2000
  Requête n° 27798/95

- Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie
  Cour européenne des droits de l'homme, 28 juin 2007
  Requête n° 62540/00

- Bucur et Toma c. Roumanie
  Cour européenne des droits de l'homme, 8 janvier 2013
  Requête n° 40238/02

- Chahal c. Royaume-Uni
  Cour européenne des droits de l'homme, 15 novembre 1996
  Requête n° 22414/93

- Commission/Autriche
  Cour de justice de l'Union européenne, 16 octobre 2012
  Affaire C-614/10

- Commission/Allemagne
  Cour de justice de l'Union européenne, 9 mars 2010
  Affaire C-518/07

- Commission/Hongrie
  Cour de justice de l'Union européenne, 8 avril 2014
  Affaire C-288/12

- Copland c. Royaume-Uni
  Cour européenne des droits de l'homme, 3 avril 2007
  Requête n° 62617/00

- Digital Rights Ireland/Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlande et the Attorney General, et Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl et autres
  Cour de justice de l'Union européenne, 8 avril 2014
  Affaires jointes C-293/12 et C-594/12

- Gillan et Quinton c. Royaume-Uni
  Cour européenne des droits de l'homme, 12 janvier 2010
  Requête n° 4158/05

- Hokkanen c. Finlande
  Cour européenne des droits de l'homme, 23 septembre 1994
  Requête n° 19823/92

- Huvig c. France
  Cour européenne des droits de l'homme, 24 avril 1990
  Requête n° 11105/84

- Klass et autres c. Allemagne
  Cour européenne des droits de l'homme, 6 septembre 1978
  Requête n° 5029/71

- Leander c. Suède
  Cour européenne des droits de l'homme, 26 mars 1987
  Requête n° 9248/81

- Liberty et autres c. Royaume-Uni
  Cour européenne des droits de l'homme, 1er juillet 2008
  Requête n° 58243/00

- López Ostra c. Espagne
  Cour européenne des droits de l'homme, 9 décembre 1994
  Requête n° 16798/90

- Malone c. Royaume-Uni
  Cour européenne des droits de l'homme, 2 août 1984
  Requête n° 8691/79

- Rotaru c. Roumanie
  Cour européenne des droits de l'homme, 4 mai 2000
  Requête n° 28341/95

- S. et Marper c. Royaume-Uni
  Cour européenne des droits de l'homme, 4 décembre 2008
  Requêtes nos 30562/04 et 30566/04

- Schrems/Data Protection Commissioner of Ireland
  Cour de justice de l'Union européenne, 6 octobre 2015
  Affaire C-362/14

- Szábo et Vissy c. Hongrie
  Cour européenne des droits de l'homme, 12 janvier 2016
  Requête n° 37138/14

- Weber et Saravia c. Allemagne
  Cour européenne des droits de l'homme, 29 juin 2006
  Requête n° 54934/00

- Zakharov c. Russie
  Cour européenne des droits de l'homme, 4 décembre 2015
  Requête n° 47143/06

- ZZ/Secretary of State for the Home Department
  Cour de justice de l'Union européenne, 4 juin 2013
  Affaire C-300/11