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

14/FR
WP 228

Document de travail sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale

Adopté le 5 décembre 2014

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 sur 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 de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

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

Synthèse

Le présent document de travail contient l'analyse juridique de l'*Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale* du groupe de travail «article 29», adopté le 10 avril 2014. Cet avis porte essentiellement sur le suivi à mettre en place à la suite des révélations de Snowden. À cette fin, il contient plusieurs recommandations sur la manière de rétablir le respect des droits fondamentaux à la protection de la vie privée et des données par les services de sécurité et de renseignement, et sur la manière d'améliorer la surveillance des activités menées par ces entités tout en préservant la sécurité nationale. Le présent document de travail expose les conclusions des discussions et de l'analyse juridique sur lesquelles les recommandations du groupe de travail sont fondées.

Il est important de noter avant tout qu'il ne convient pas de prendre uniquement en considération le droit de l'Union européenne lorsque les débats traitent de questions de surveillance et de sécurité nationale du point de vue de la protection des données. Tout aussi importants sont les principes fixés dans la Déclaration universelle des droits de l'homme et dans le pacte international relatif aux droits civils et politiques, ainsi que les principes consacrés dans la convention européenne des droits de l'homme et dans la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[1]. L'ingérence dans de tels droits ne peut être envisagée que si elle est conforme à la loi, nécessaire et proportionnée et que si elle répond à un besoin social impérieux. Cela présuppose également que d'autres options, moins intrusives, ne sont pas disponibles.

En l'absence d'une définition claire du terme «sécurité nationale», le groupe de travail a examiné de quelle manière il convient d'interpréter cette notion, d'autant plus que la ligne ténue séparant répression et sécurité nationale semble parfois s'estomper. En tout état de cause, il est nécessaire de distinguer la sécurité nationale non seulement de la sécurité de l'Union européenne mais également de la sûreté de l'État, de la sécurité publique et de la défense. Toutes ces notions sont évoquées séparément dans les traités de l'UE et dans la législation sous-jacente, bien qu'elles soient liées de manière indissociable. C'est pourquoi des arguments d'ordre strictement juridique ne peuvent justifier à eux seuls que certains éléments relèvent ou non de la dérogation au titre de la sécurité nationale. Il peut toutefois être affirmé que, même si les activités menées par des services de sécurité et de renseignement sont communément acceptées comme relevant de la dérogation au titre de la sécurité nationale, tel n'est pas nécessairement le cas lorsque des autorités répressives générales accomplissent des tâches analogues.

[1] Le respect de ces principes est obligatoire pour tous les États parties, dont les pays de l'UE.

Le document de travail examine également la question de savoir si l'intérêt d'un pays tiers en matière de sécurité nationale peut être invoqué. Le groupe de travail souligne le fait que les dérogations prévues dans les traités n'offrent pas la possibilité d'invoquer la sécurité nationale d'un pays tiers comme argument permettant à lui seul d'exclure l'applicabilité de la législation de l'UE. Il reconnaît toutefois que, dans certains domaines, l'intérêt en matière de sécurité nationale d'un État membre de l'UE puisse coïncider avec celui d'un pays tiers. Le cas échéant, il appartient à l'État membre de l'UE de justifier dûment cette situation auprès des autorités concernées, au cas par cas.

Une grande partie du document de travail examine l'applicabilité du mécanisme de transfert des données visé par la directive 95/46/CE. Bien que de nombreuses informations concernant les programmes de surveillance manquent toujours de clarté, il semble probable que les autorités de surveillance d'un pays tiers accèdent généralement aux données après que celles-ci ont été transférées par un responsable du traitement relevant de la juridiction de l'UE vers un lieu situé en dehors de cette juridiction. De tels transferts se produiront en principe conformément aux procédures prévues dans la directive et dans les dispositions d'application nationales correspondantes, en faisant éventuellement appel à des clauses contractuelles types, à des règles d'entreprise contraignantes ou à l'accord sur la sphère de sécurité. Cependant, aucun de ces instruments ne comporte de dispositions autorisant des transferts de données massifs, structurels ou illimités. Il y a lieu pour les autorités publiques d'un pays tiers souhaitant obtenir un accès direct à des données à caractère personnel relevant de la juridiction de l'UE de recourir aux mécanismes de coopération officiels dans la mesure où la législation de l'UE ne prévoit explicitement aucune possibilité de transférer des données à caractère personnel détenues par des responsables du traitement du secteur privé vers les autorités répressives ou les services de sécurité d'un pays tiers. Dans un souci d'efficacité, le présent document de travail illustrera son analyse à l'aide de différents scénarios. En guise de conclusion, le document de travail formulera un certain nombre d'observations concernant des pistes envisageables pour la suite.

Table des matières

.

1. Introduction

Le 10 avril 2014, le groupe de travail «article 29» (ci-après le «groupe de travail») a adopté l'avis sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale[4], donnant ainsi une première réponse aux révélations relatives à une surveillance massive de la part des services de renseignement du monde entier, sur la base de documents transmis pour l'essentiel par Edward Snowden. Cet avis contient également plusieurs recommandations adressées à la communauté internationale ainsi qu'aux législateurs de l'Union européenne et des États membres, sur la manière d'améliorer la protection des données à caractère personnel des personnes dans le contexte de la surveillance.

Bien que l'avis porte essentiellement sur le suivi à mettre impérativement en place à l'égard des conséquences que les révélations de Snowden entraînent pour la protection des données, les membres du groupe de travail ont également longuement débattu du cadre juridique régissant les opérations de surveillance massive, notamment en ce qui concerne l'applicabilité du droit européen aux activités de surveillance dévoilées. Le présent document de travail expose les conclusions de ces discussions. Qui plus est, le groupe de travail est convaincu de la nécessité d'un débat plus large, associant différentes parties prenantes. Le présent document de travail se veut donc essentiellement une contribution à ce type de débat. Il présente également plusieurs scénarios de transferts de données vers les services de sécurité et de renseignement de pays tiers. Le groupe de travail souligne que l'analyse effectuée dans ce document de travail n'apporte pas, et ne saurait apporter, de solution satisfaisante à l'ensemble des opérations de traitement de données transfrontières concernées susceptibles d'être menées: l'analyse juridique finale de la légitimité d'un traitement de données sera toujours fonction des spécificités de chaque situation.

2. Programmes de surveillance

Depuis la mi-2013, un grand nombre de programmes de surveillance auparavant secrets ont été dévoilés par les médias, essentiellement *The Guardian*[5] et *The Washington Post*[6]. Nombre de ces programmes semblent porter sur la collecte massive de données à caractère personnel provenant de diverses sources en ligne et concernent des données relatives aussi bien au contenu qu'au trafic. Selon les rapports, la plupart des programmes ne font pas de distinction entre les personnes, que celles-ci soient suspectées ou non. Il en ressort également que des services de renseignement prenant part à des programmes de surveillance dans d'autres pays collaborent de manière intensive.

---

[4] WP215 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf.

[5] http://www.theguardian.com/world/the-nsa-files.

[6] http://www.washingtonpost.com/nsa-secrets/.

La surveillance électronique dans le cadre d'une veille automatique[7] est devenue une technique communément utilisée par les services de renseignement au cours des dernières décennies et doit respecter les conditions réglementaires relatives à l'interception des communications afin de pouvoir être utilisée en toute légalité. Depuis les révélations de Snowden, il apparaît toutefois clairement que les limites de la légalité ont été atteintes et, par moments, également franchies.[8] Il est probable que des programmes de surveillance soient menés dans toutes les parties du monde.

L'aperçu général présenté aux points 2.1 et 2.2 ci-dessous vise à fournir des informations factuelles et se fonde essentiellement sur les informations communiquées dans les comptes rendus des médias, dans le rapport du groupe d'experts UE-USA[9] ainsi que sur les informations pour lesquelles les autorités des États-Unis ont levé le secret à la suite de la divulgation publique de plusieurs programmes de surveillance. Ce bref aperçu ne constitue pas une position du groupe de travail, même si le point de vue du groupe de travail est exprimé dans les points abordés ultérieurement. À ce jour, les gouvernements européens n'ont fourni publiquement que très peu d'informations ayant trait à l'existence et au fonctionnement des programmes de surveillance évoqués, notamment en ce qui concerne la collaboration des services de renseignement respectifs avec les autorités chargées de ces programmes. Il apparaît cependant clairement que la surveillance électronique massive ne concerne pas uniquement les États-Unis mais constitue un phénomène d'envergure mondiale présent dans de nombreux pays. L'exemple des États-Unis présenté ci-dessous vise à illustrer certaines des questions qui se sont posées dans la mesure où les États-Unis constituent sans doute à ce jour l'exemple d'implication d'un pays tiers le plus largement débattu. Cependant, des cas similaires ont été relevés également dans d'autres pays, comme expliqué au point 2.2.

---

[7] La veille automatique (ou SIGINT) est un terme généralement utilisé pour évoquer la collecte d'informations sur les communications entre personnes ainsi que la collecte de signaux électroniques en provenance, par exemple, des systèmes de radar et d'armement. Les informations sur les communications peuvent contenir aussi bien des données relatives au contenu que des données «autour» du contenu, ce qui aux États-Unis correspond aux «métadonnées».

[8] Voir en particulier les évolutions en la matière contenues dans les rapports du conseil américain de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, PCLOB) – disponibles à l'adresse: http://www.pclob.gov/

[9] Rapport sur les conclusions des coprésidents de l'UE du groupe de travail ad hoc UE-USA sur la protection des données accompagnant la communication de la Commission au Parlement européen et au Conseil intitulée «Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique» [COM(2013) 846 final] - http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf - *Ce groupe de travail UE-USA examine les différentes dimensions de la relation UE-USA en matière de surveillance, dont le Patriot Act, l'Executive Order 12333 et les fonctions de supervision au niveau exécutif, législatif et judiciaire . La communication de la Commission traite davantage des modifications potentielles à apporter aux accords en matière de transfert des données conclus par l'UE et les USA, tels que l'accord sur les données des dossiers passagers (PNR), l'accord TFTP, l'accord-cadre relatif à la coopération en matière pénale et l'accord sur la sphère de sécurité.*

2.1. Surveillance de la part des États-Unis

Aux États-Unis, la plupart des programmes de surveillance sont menés par la NSA. En fonction des programmes, la NSA, la CIA et/ou le FBI peuvent accéder aux bases de données ainsi créées pour y effectuer des recherches. La plupart des programmes de surveillance sont menés au titre des lois «Patriot Act» et «Foreign Intelligence Surveillance Act» (FISA) mais également sur la base de l'«Executive Order 12333» (ordre présidentiel).

À la suite du débat public déclenché par les révélations de Snowden, le président des États-Unis a institué un comité d'examen des technologies du renseignement et des communications (Review Group on Intelligence and Communications Technologies). Le rapport du groupe a été remis le 12 décembre 2013 et contient des recommandations sur les modifications susceptibles d'être apportées à la politique de sécurité nationale des États-Unis.[10] Le président a tenu compte de ces recommandations dans l'élaboration de sa nouvelle directive de politique générale relative aux activités de veille automatique, laquelle a été présentée lors d'une conférence de presse organisée le 17 janvier 2014.

Les principales modifications annoncées concernent les programmes de surveillance menés au titre de la section 215 du PATRIOT Act américain, plus particulièrement le programme baptisé «business records programme» qui permet aux fournisseurs de télécommunications de collecter des données sur le trafic (métadonnées téléphoniques). Malgré les conclusions du conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, PCLOB) concernant la section 215 du Patriot Act des États-Unis, et plus particulièrement le programme appelé «business records programme» autorisant la collecte de métadonnées téléphoniques, selon lesquelles la collecte de métadonnées «est dénuée de fondement juridique viable»[11], il ne sera pas mis un terme aux programmes de surveillance massive. Cependant, le président des États-Unis a également annoncé un contrôle plus strict des activités de renseignement menées par les États-Unis, y compris une modification de la procédure instaurée devant la FISA Court, laquelle permettra «la mise en place d'une commission d'avocats extérieure au gouvernement et chargée de fournir un point de vue indépendant dans des affaires importantes».[12] En outre, bien que le président des États-Unis ait souligné l'importance d'un rétablissement de la confiance avec les partenaires étrangers, les

---

[10] Liberté et sécurité dans un monde en évolution - rapport et recommandations du comité présidentiel chargé de l'examen des technologies du renseignement et des communications (Liberty and Security in a Changing World – Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies), p. 11, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. (consulté en dernier lieu le 20 novembre 2014).

[11] Rapport sur le programme d'enregistrements téléphoniques mené au titre de la section 215 du Patriot Act des États-Unis et sur les opérations du tribunal de surveillance du renseignement extérieur, p. 1616, http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf. (consulté en dernier lieu le 20 novembre 2014).

[12] Discours du président des États-Unis, disponible à l'adresse http://www.whitehouse.gov/blog/2014/01/17/president-obama-discusses-us-intelligence-programs-department-justice. (consulté en dernier lieu le 20 novembre 2014).

modifications proposées pour la collecte d'informations aux fins du renseignement extérieur ont une portée relativement limitée. La collecte de données dans le cadre de la veille automatique à des fins de sécurité nationale se poursuivra de manière massive, la différence étant simplement que les données seront conservées par les fournisseurs de télécommunications et non par le gouvernement. Le président a ajouté que l'utilisation des données devra néanmoins se conformer aux objectifs de sécurité nationale.

Le PCLOB a publié, en juillet 2014, un rapport supplémentaire sur la section 702 du Patriot Act des États-Unis. Ce rapport n'est pas aussi critique à l'égard des pratiques existantes qu'un précédent rapport concernant la section 215 (publié en janvier 2014). Il reconnaît que «*certains aspects du programme relevant de la section 702 poussent le programme à la limite de ce qui est raisonnablement constitutionnel*», en faisant référence à des aspects tels que le champ d'application inconnu et potentiellement vaste de la collecte fortuite des communications de ressortissants américains, l'utilisation des métadonnées collectées afin d'accéder à des communications internet qui ne sont ni à l'origine ni la cible des opérations de surveillance, ainsi que le recours à des requêtes informatiques afin de retrouver dans les informations collectées les communications de ressortissants américains spécifiques. Le rapport recommande que les programmes PRISM et Upstream (relevant tous deux de la section 702 du Patriot Act) deviennent plus «raisonnables» eu égard aux limites imposées par la constitution américaine.

2.2. Surveillance de la part des États membres de l'Union européenne et d'autres pays tiers

Les révélations de Snowden ainsi que celles qui ont vu le jour parallèlement à l'affaire Snowden ne se limitent pas uniquement aux activités de surveillance des États-Unis mais concernent également les opérations de surveillance menées par les services de renseignement d'États membres de l'UE, que ce soit sur le territoire européen ou à l'étranger. Celles-ci revêtent une importance particulière dans la mesure où il est à présent confirmé que plusieurs services de renseignement établis en Europe collaborent étroitement avec leurs homologues américains[13]. Les informations partagées en vertu du principe de réciprocité seront d'autant plus nombreuses que les relations avec les États-Unis sont étroites. Cela démontre que la sécurité nationale est moins «nationale» que son nom ne le laisse supposer: des données, dont certaines à caractère personnel, sont partagées et échangées à grande échelle par les services de renseignement.

Les programmes de surveillance menés par les services de renseignement européens englobent, semble-t-il, aussi bien la collecte de métadonnées sur le trafic issues de diverses sources que la surveillance de forums en ligne et la mise sur écoute de réseaux câblés. À ce

[13] Déclaration de Charles Farr devant le tribunal d'enquête (Investigatory Powers Tribunal), 16 mai 2014.

jour, cependant, l'existence de pratiquement aucun de ces programmes n'a été confirmée par les gouvernements eux-mêmes[14].

En dehors de l'Union européenne également, les gouvernements sont réticents lorsqu'il s'agit de confirmer l'existence de programmes de surveillance menés par les services de renseignement respectifs. Il apparaît cependant clairement qu'à tout le moins l'Australie[15], la Chine[16], l'Inde[17] et la Russie[18] recourent à de tels programmes. Le fonctionnement des activités révélées devrait toutefois être semblable à ce qui a été divulgué à ce jour: les services de renseignement collectent des données à caractère personnel à une très grande échelle et coopèrent à l'échelon mondial en partageant des informations dans le cadre de diverses alliances. Parfois, la préoccupation d'un pays en matière de sécurité nationale semble être devenue la préoccupation de nombreux autres pays.

Sur le plan de la protection des données, cette situation soulève plusieurs questions. L'utilisation (le traitement) de données à caractère personnel par les services de renseignement est-elle licite? De quelle manière les données ont-elles été recueillies et sur quelle base juridique? L'accès à des données à caractère personnel provenant d'entreprises privées de l'UE peut-il être réalisé sans difficulté de l'étranger, sans que la personne concernée n'en soit consciente et sans même qu'elle sache que cette possibilité existe? Dans quelle mesure le droit fondamental à la protection des données reconnu dans toute l'Europe continue-t-il de s'appliquer (réellement) à notre époque, alors que les données à caractère personnel sont apparemment si aisément accessibles pour les services gouvernementaux?

Ces questions ont été largement débattues au sein du groupe de travail. À ce stade, seules quelques conclusions ont pu être tirées étant donné qu'une évaluation complète dépend dans une large mesure des spécificités de chaque situation: l'existence éventuelle de suspicions, le cadre juridique applicable, le caractère plus ou moins spécifique et ciblé de la collecte de données, etc. Dans le même temps, un débat devrait avoir lieu sur la question de savoir dans quelle mesure le cadre juridique international et européen régissant la protection des données est, et devrait être, applicable.

---

[14] Voir en particulier les paragraphes 3, 4 et 5 du rapport du Haut-Commissariat des Nations unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, publié le 30 juin 2014 et accessible en suivant le lien suivant: https://www.ccdcoe.org/sites/default/files/documents/UN-140730-RightToPrivacyReport.pdf

[15] http://www.theguardian.com/world/2014/oct/13/australias-defence-intelligence-agency-conducted-secret-programs-to-help-nsa

[16] Par exemple, en Chine: http://www.theguardian.com/world/2011/jul/26/china-boosts-internet-surveillance (consulté en dernier lieu le 20 novembre 2014).

[17] Par exemple, en Inde: https://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

[18]http://www.theguardian.com/world/2014/sep/24/strasbourg-court-human-rights-russia-eavesdropping-texts-emails-fsb-

3. Cadre juridique général

L'examen du cadre juridique applicable aux activités de surveillance ne peut faire abstraction de la dérogation au titre de la sécurité nationale prescrite par l'article 4, paragraphe 2, du traité sur l'Union européenne (TUE). Cependant, ces activités sont soumises à un éventail de législations plus large. S'inspirant des normes internationales originelles, lesquelles sont largement admises et ont influencé le droit européen, les instruments juridiques des Nations unies accordent aux personnes le droit universel de ne pas faire l'objet d'immixtions arbitraires ou illégales dans leur vie privée. Les instruments du Conseil de l'Europe ainsi que la jurisprudence de la Cour européenne des droits de l'homme (ci-après «la Cour») garantissent ensuite, au niveau européen, une compréhension commune de la portée de ce droit et des ingérences dont il est susceptible de faire l'objet.

3.1. Instruments juridiques des Nations unies

Le groupe de travail rappelle que la législation internationale sur les droits de l'homme fournit le cadre universel au regard duquel doit être appréciée toute ingérence dans le droit à la vie privée des personnes.

Le droit de l'homme à la vie privée, droit internationalement reconnu, est codifié dans la Déclaration universelle des droits de l'homme des Nations unies (1948) ainsi que dans le pacte international relatif aux droits civils et politiques[19].

L'article 12 de la Déclaration ainsi que l'article 17 du pacte international disposent que nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée.

Les États assujettis à la Charte des Nations unies ont l'obligation de favoriser le respect universel et effectif des droits de l'homme et des libertés fondamentales[20]. En outre, les États parties au pacte s'engagent à prendre, en accord avec leurs procédures constitutionnelles et avec les dispositions du pacte, les arrangements devant permettre l'adoption de telles mesures d'ordre législatif ou autre, propres à donner effet aux droits reconnus dans le pacte. Cette obligation prévoit que soit mis à disposition un recours utile, en ce y compris le développement de possibilités de recours juridictionnel en cas de violation des droits consacrés par le pacte, et que soit garantie la bonne suite donnée à tout recours.

[19] Pacte International relatif aux droits civils et politiques, résolution de l'Assemblée générale 2200A du 16 décembre 1966.

[20] Charte des Nations unies, article 55, point c).

3.1.1. Résolution de l'Assemblée générale des Nations unies n° 68/167 de janvier 2014

La résolution de l'Assemblée générale des Nations unies n° 68/167[21] réaffirme les droits consacrés dans le pacte et:

- reconnaît l'équilibre des intérêts en jeu tant au niveau de la vie privée que de la sécurité, notant que si le souci de la sécurité publique peut justifier la collecte et la protection de certaines données sensibles, il ne dispense pas les États de respecter pleinement les obligations que leur impose le droit international des droits de l'homme;

- affirme que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, en particulier le droit à la vie privée et invite les États à protéger ces droits sur toutes les plateformes numériques;

- invite les États à prendre des mesures pour faire cesser les violations de ces droits et à créer en outre des conditions qui permettent de les prévenir; et à revoir leurs procédures, leurs pratiques et leur législation nationales (relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle) en veillant à ce que la législation nationale applicable ne permette plus la violation des droits consacrés par le pacte; et invite les parties à veiller à respecter pleinement toutes leurs obligations au regard du droit international des droits de l'homme.

Cette résolution invite également les États parties au pacte à créer des mécanismes nationaux de contrôle indépendants qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent. La résolution des Nations unies coïncidait donc avec les démarches (décrites dans l'avis WP215 du groupe de travail adopté le 10 avril 2014) que le groupe travail a entreprises afin d'examiner les pratiques existantes mises en place dans les États membres de l'UE pour garantir la supervision des services nationaux de renseignement. À la suite des révélations de 2013 relatives aux activités de surveillance, le groupe de travail a relevé la nécessité de dresser un tableau des mécanismes de contrôle existant au niveau national au sein de l'UE et portant sur les activités menées par les services de renseignement et de sécurité nationale. De l'avis du groupe de travail, ces mécanismes ont souvent une incidence sur l'efficacité de la protection des données et du respect de la vie privée au niveau de l'UE.

En menant une telle enquête, le groupe de travail souhaitait présenter un tableau plus clair des différentes modalités adoptées en Europe à cet égard. Cet exercice consistait à identifier dans quel pays l'autorité chargée de la protection des données était compétente pour superviser les services de renseignement et à découvrir s'il existait des limites à cette compétence. De l'avis du groupe de travail, la conclusion significative à tirer de l'enquête est que les autorités chargées de la protection des données contribuent à contrôler de façon plus étroite, d'une part,

---

[21] Résolution de l'Assemblée générale des Nations unies n° 68/167 de janvier 2014 - http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=/english/&Lang=F (consulté en dernier lieu le 20 novembre 2014).

la manière dont les États membres maintiennent un système juridique cohérent pour les services de renseignement et, d'autre part, les dispositions que les cadres juridiques nationaux doivent comporter pour garantir in fine aux personnes le respect du droit à la protection des données[22]. L'avis mentionné ci-dessus présente en détail les résultats de cette enquête[23].

Enfin, la résolution des Nations unies prie également le Haut-Commissaire des Nations unies aux droits de l'homme de présenter, à l'Assemblée générale ainsi qu'au Conseil des droits de l'homme, un rapport sur la protection et la promotion du droit à la vie privée dans le contexte de la surveillance et/ou de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle.

Bien que ce type de résolution ne soit pas juridiquement contraignant, il adresse aux États parties un message important selon lequel il convient de mener une réflexion ultérieure et sérieuse et de prendre des mesures tant collectives qu'individuelles conformément aux objectifs des Nations unies, tels qu'énoncés à l'article 1er de la Charte des Nations unies[24]. La résolution vise également à étendre aux communications électroniques et à la vie privée la protection consacrée dans le pacte international relatif aux droits civils et politiques.

3.1.2. Rapport des Nations unies sur le droit à la vie privée à l'ère du numérique

Ce rapport[25] a été adopté en juillet 2014[26], à la suite des événements décrits ci-dessus. Il souligne dans ses recommandations et ses conclusions qu'«*il existe manifestement un besoin*

---

[22] Dans son avis WP215 (p. 13), le groupe de travail appelle entre autres à «*une supervision externe efficace, solide et indépendante, assurée soit par un organe spécialisé avec la participation des autorités chargées de la protection des données, soit par l'autorité chargée de la protection des données elle-même*».

[23] Il n'est pas pertinent d'examiner plus avant cette enquête dans le cadre de ce document de travail, lequel cible d'autres considérations juridiques importantes en la matière.

[24] La Charte des Nations unies, en son article 1er, paragraphes 3 et 4, énonce ses buts comme suit: «3. Réaliser la coopération internationale en résolvant les problèmes internationaux d'ordre économique, social, intellectuel ou humanitaire, en développant et en encourageant le respect des droits de l'homme et des libertés fondamentales pour tous, sans distinctions de race, de sexe, de langue ou de religion; et

4. Être un centre où s'harmonisent les efforts des nations vers ces fins communes.»

Lors des débats de novembre 2013 relatifs au rapport des Nations unies, une question pertinente appelant à une réflexion ultérieure a été posée en ces termes par l'ambassadeur allemand , l'un des coauteurs de la résolution: «Mais tout ce qui est techniquement possible doit-il pour autant être autorisé?» Site internet: http://www.dw.de/germany-brazil-introduce-anti-spying-resolution-at-un-general-assembly/a-17213179 'Germany. Brazil introduce anti-spying resolution'. Deutsche Welle (consulté en dernier lieu le 20 novembre 2014)

[25] Rapport du Haut-Commissaire des Nations unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique. Distribué le 30 juin 2014. Site internet: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (consulté en dernier lieu le 20 novembre 2014).

[26] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (consulté en dernier lieu le 20 novembre 2014).

urgent de vigilance en garantissant la conformité de toute politique ou pratique de surveillance avec le droit international des droits de l'homme, y compris du droit à la vie privée, par la conception de mesures de protection efficaces contre les abus»[27]. Le rapport déplore les circonstances qui, dans de nombreux pays, ont contribué à un manque de responsabilisation en cas d'ingérence arbitraire ou illégale dans le droit à la vie privée. Il s'agit notamment du manque de transparence autour des pratiques de surveillance et des cadres juridiques applicables. Le groupe de travail attire l'attention sur la déclaration figurant dans le rapport des Nations unies, selon laquelle: «*Comme mesure immédiate, il y a lieu pour les États de revoir leurs propres législations, politiques et pratiques au niveau national aux fins de garantir une totale conformité avec le droit international des droits de l'homme.*»

Le rapport des Nations unies souligne également la nécessité de veiller à ce que les processus de révision juridique prévoient un dialogue associant toutes les parties intéressées, parmi lesquelles les États membres, la société civile, les communautés scientifique et technique, le secteur des affaires, le monde universitaire et des experts des droits de l'homme. Le groupe de travail sera particulièrement intéressé par ce point et s'efforcera de nourrir le débat en Europe à l'occasion d'une conférence spéciale organisée à la fin 2014, comme expliqué dans son avis 04/2014.

Par ailleurs, le groupe de travail observe également que la Conférence internationale de 2013 des commissaires à la protection des données et de la vie privée a adopté une résolution[28] faisant suite à ses précédents appels en faveur du développement plus détaillé dans le droit international du droit à la vie privée et, plus spécifiquement, du droit à la protection des données. Les commissaires ont résolu d'«*inviter les gouvernements à plaider en faveur de l'adoption d'un protocole supplémentaire se rapportant à l'article 17 du pacte international relatif aux droits civils et politiques (PIDCP), lequel devrait être fondé sur les normes qui ont été élaborées et approuvées par la Conférence internationale ainsi que sur les dispositions figurant dans l'observation générale n° 16 relative au pacte*».

En résumé, malgré certaines initiatives récentes, la notion de droit à la protection de la vie privée n'a pas encore été traduite, au niveau des Nations unies, sous la forme de dispositions[29] nouvelles et plus étoffées. En Europe, cependant, le droit au respect de la vie privée – de même que le droit à la protection des données – a été défini de manière beaucoup plus

---

[27] Rapport du Haut-Commissaire des Nations unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, distribué le 30 juin 2014, p. 16, point 50.

[28] Résolution sur l'ancrage de la protection des données et de la protection de la vie privée dans le droit international, 35e Conférence internationale des commissaires à la protection des données et de la vie privée, septembre 2014. Site internet: https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf (consulté en dernier lieu le 20 novembre 2014).

[29] L'observation générale n° 16 du comité des droits de l'homme relative à l'article 17 du PIDCP, adoptée le 8 avril 1988, fournit une interprétation détaillée du droit ainsi qu'au point 10, certains principes concernant la protection des données.

détaillée, ce qui a permis de prendre les premières mesures propres à assurer la garantie collective de certains droits énoncés dans la Déclaration universelle.

3.2. Instruments du Conseil de l'Europe

Les deux principaux instruments juridiquement contraignants ayant trait aux droits fondamentaux et à la protection des données au niveau du Conseil de l'Europe sont la Convention européenne des droits de l'homme[30] (ci-après CEDH) ainsi que la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [31] (ci-après la convention 108).

3.2.1. La CEDH

L'article 1er de la CEDH impose aux parties de reconnaître à toute personne relevant de leur juridiction[32] les droits et libertés définis dans la Convention. Cette disposition implique que les parties ont des obligations non seulement négatives mais également positives, lesquelles «*exigent des autorités nationales qu'elles prennent les mesures nécessaires à la sauvegarde d'un droit*[33] *ou, plus précisément encore, d'adopter des mesures raisonnables et adéquates pour protéger les droits de l'individu*»[34],[35]. Dans des circonstances exceptionnelles, la jurisprudence de la Cour a conclu que la notion de juridiction et les obligations des États parties ne peuvent se limiter au territoire national de l'État partie. Dans la jurisprudence

---

[30] Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales - Rome, 4 novembre 1950.

[31] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Strasbourg, 28 janvier 1981 – STCE n° 108.

[32] La notion de juridiction visée à l'article 1er de la CEDH n'a pas été définie dans la convention ni dans les travaux préparatoires. Cependant, lorsqu'elle envisage la notion de juridiction en lien avec l'article 1er, la jurisprudence de la Cour prend en considération le concept de contrôle effectif exercé par l'État. Ainsi, dans l'arrêt rendu dans l'affaire Loizidou c. Turquie du 23 mars 1995, la Cour a rappelé que, si l'article 1er (obligation de respecter les droits de l'homme) fixe des limites au domaine de la CEDH, la notion de «juridiction» au sens de cette disposition ne se circonscrit pas au territoire national des Hautes Parties contractantes. En particulier, un État peut également voir engager sa responsabilité lorsque, par suite d'une action militaire - légale ou non -, il exerce en pratique le contrôle sur une zone située en dehors de son territoire national. L'obligation pour l'État d'assurer dans une telle région le respect des droits et libertés garantis par la CEDH découle du fait de ce contrôle, qu'il s'exerce directement, par l'intermédiaire des forces armées de l'État concerné ou par le biais d'une administration locale subordonnée. À cet égard, voir également l'arrêt rendu par la Cour dans l'affaire Al-Skeini et autres c. Royaume-Uni, 7 juillet 2011.

En droit international public, la juridiction se définit comme le pouvoir d'un État souverain à déterminer, juger et faire appliquer les dispositions auxquelles ses justiciables sont tenus.

[33] Arrêt de la Cour dans l'affaire Hokkanen c. Finlande, 24 août 1994.

[34] Arrêt de la Cour dans l'affaire Lopez-Ostra c. Espagne, 9 décembre 1994.

[35] Jean-François Akandji-Kombe, *Les obligations positives en vertu de la Convention européenne des droits de l'homme*, Précis sur les droits de l'homme n° 7, Conseil de l'Europe, 2007.

traitant de cette question, la Cour a tenu compte de la notion de «contrôle effectif» de la part de l'État partie pour déterminer si ce dernier exerce sa juridiction.

À cet égard, le rapport ECHELON du Parlement européen déclare à propos des instruments du Conseil de l'Europe que *«[Les États membres] conservent la responsabilité de leur territoire ainsi que leurs obligations vis–à–vis du justiciable européen dès lors que l'exercice de la puissance publique est assuré par le service de renseignements d'un autre pays»*.[36]

3.2.1.1. Champ d'application de la CEDH

Outre au champ d'application territorial défini à l'article 1er, la CEDH s'applique aux territoires dont les parties assurent les relations internationales pour autant qu'elles aient notifié cette information conformément à l'article 56, paragraphe 1, de la CEDH.

Des restrictions générales au champ d'application matériel de la CEDH ne sont pas autorisées. Cependant, au moment de la signature et de la ratification, les parties ont eu la possibilité de formuler des réserves au sujet d'une disposition particulière de la Convention, dans la mesure où une loi alors en vigueur sur leur territoire n'était pas conforme à cette disposition[37]. En ce qui concerne les États membres de l'UE, aucune des réserves ne porte sur l'article 8 de la CEDH relatif au droit à la vie privée et familiale[38].

3.2.1.2. Le droit au respect de la vie privée

Conformément à l'article 8, paragraphe 1, de la CEDH, *«Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance»*.

Les notions de «vie privée» et de «correspondance» comprennent les données relatives à la téléphonie et aux télécommunications[39]. La jurisprudence de la Cour précise que la portée de la protection de ce droit fondamental couvre non seulement le contenu de la communication mais également, entre autres, «*la date et la durée des conversations téléphoniques*» ainsi que «*les numéros composés*», dans la mesure où de telles informations «*font partie intégrante des communications téléphoniques*»[40]. En d'autres termes, la portée de la protection recouvre non seulement le contenu de la communication mais également ce que l'on appelle les «données relatives au trafic» ou «métadonnées».

---

[36] Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) – A5-0264/2001, p. 88.

[37] Voir l'article 57 de la CEDH.

[38] Les notifications et les déclarations sont disponibles à l'adresse http://www.conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?CL=FRE&CM=8&NT=005&DF=29/07/2014&VL=1. (consultée en dernier lieu le 20 novembre 2014).

[39] Voir l'arrêt de la Cour dans l'affaire Klass et autres c. Allemagne, 6 septembre 1978, point 41.

[40] Voir l'arrêt de la Cour dans l'affaire Malone c. Royaume-Uni, 2 août 1984, point 84.

3.2.1.3. Ingérences possibles dans le droit au respect de la vie privée

Conformément à l'article 8, paragraphe 2, de la CEDH, il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée que si cette restriction:

- est prévue par la loi (laquelle doit avoir des conséquences prévisibles et être accessible de manière générale)[41]; et

- constitue une mesure qui, au sein d'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.

Il découle de la première condition que la seconde condition se réfère aux intérêts des parties à la convention et non aux intérêts d'États tiers, que ces intérêts coïncident ou non.

Selon la jurisprudence de la Cour, «*une exception à un droit garanti par la Convention appelle une interprétation étroite*» [42].Dans l'affaire Klass, la Cour a en outre précisé que: «*Caractéristique de l'État policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques*»[43].

Il convient dès lors de démontrer que toute ingérence dans le droit au respect de la vie privée (en l'espèce, tout accès d'une autorité gouvernementale aux données à caractère personnel relatives aux communications) est une mesure strictement nécessaire, au sein d'une société démocratique, à l'un des objectifs énoncés à l'article 8, paragraphe 2.

Selon la Cour, une telle ingérence peut être considérée comme nécessaire si elle répond à un besoin social impérieux, si elle est proportionnée au but poursuivi et si les motifs invoqués par les autorités publiques pour la justifier apparaissent pertinents et suffisants[44].

À cet égard, dans l'affaire S. et Marper c. Royaume-Uni[45], la Cour a précisé que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales et des données

---

[41] Voir l'arrêt de la Cour dans l'affaire Malone c. Royaume-Uni, 2 août 1984, points 83 et suivants.

[42] Voir l'arrêt de la Cour dans l'affaire Klass et autres c. Allemagne, 6 septembre 1978, point 42. Voir également l'affaire Youth Initiative for Human Rights c. Serbie, 25 juin 2013 , points 24-26, qui confirme que les agences de renseignement sont tenues également de respecter les droits fondamentaux de même que les mesures d'application nationales correspondantes.

[43] Voir l'affaire Klass, citée supra, également point 42.

[44] Voir, entre autres, l'arrêt de la Cour dans l'affaire S. et Marper c. Royaume-Uni, 4 décembre 2008, point 101.

[45] Voir l'arrêt de la Cour dans l'affaire S. et Marper c. Royaume-Uni, 4 décembre 2008, notamment le point 125. «En conclusion, la Cour estime que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte

ADN des requérants soupçonnés d'avoir commis des infractions mais non condamnés ne se justifiait pas au titre de l'article 8, paragraphe 2, de la convention.

Dans le contexte de l'UE, la Cour de justice de l'Union européenne (ci-après la «CJUE») a également affirmé qu'une ingérence ne peut être jugée proportionnée que s'il est démontré que d'autres méthodes moins intrusives n'étaient pas disponibles[46].

Dans le contexte particulier de la sécurité nationale, la Cour a observé que les modalités régissant les exigences de prévisibilité peuvent être différentes selon les domaines mais que les dispositions juridiques doivent en tout état de cause définir dans quelles circonstances et sous quelles conditions l'État est habilité à mener des activités d'ingérence secrètes et, partant, potentiellement dangereuses, dans l'exercice du droit au respect de la vie privée[47].

Ce qui précède est particulièrement pertinent et applicable à toute activité de surveillance impliquant une partie à la CEDH, que ce soit en collaboration ou non avec un pays tiers[48]. Par ailleurs, le droit au respect de la vie privée est accordé à toutes les personnes relevant de la juridiction d'une partie contractante, indépendamment de leur nationalité ou de leur lieu de résidence.

Ce raisonnement est étayé par l'arrêt Loizidou c. Turquie[49] dans lequel la Cour a déclaré que *«...la notion de juridiction au sens de cette disposition ne se circonscrit pas au territoire national des Hautes Parties contractantes [...]. La responsabilité des Parties contractantes peut entrer en jeu à raison d'actes émanant de leurs organes, se produisant sur ou en dehors de leur territoire et produisant des effets en dehors de leur propre territoire»*, en référence à l'arrêt rendu par la Cour dans l'affaire Drozd et Janousek[50].

---

disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique. Cette conclusion dispense la Cour d'examiner les critiques formulées par les requérants à l'encontre de certains points précis du régime de conservation des données litigieuses, tels l'accès, trop large selon eux, à ces données et la protection, insuffisante à leurs yeux, offerte contre les usages impropres ou abusifs de ces données.»

[46] Voir l'arrêt de la CJUE dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke GbR et Hartmut Eifert/Land Hessen, 9 novembre 2010, point 81.

[47] Voir l'arrêt de la Cour dans l'affaire Rotaru c. Roumanie, 4 mai 2000, points 50, 52 et 55;. et dans l'affaire Amann c. Suisse, 16 février 2000, points 50 et suivants.

[48] Dans ce cas, la responsabilité du pays partie à la CEDH serait engagée, et non celle du pays tiers.

[49] Voir l'arrêt de la Cour dans l'affaire Loizidou c. Turquie, 23 mars 1995, point 62, en référence à l'affaire Drozd et Janousek; voir l'arrêt de la Cour dans l'affaire Drozd et Janousek c. France et Espagne, 26 juin 1992, point 91.

[50] Voir l'arrêt de la Cour dans l'affaire Drozd et Janousek c. France et Espagne, 26 juin 1992, point 91.

3.2.2. Convention 108

Le but de la Convention est «*de garantir, sur le territoire*[51] *de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ("protection des données")*».

L'adhésion à la convention est également ouverte aux États non-membres du Conseil de l'Europe[52]. La ratification de la convention indique qu'un pays prend l'engagement ferme de protéger les données à caractère personnel et qu'il souhaite adhérer de manière explicite à des normes internationales communes. Aussi le groupe de travail se féliciterait-il de l'adhésion effective à la convention de la part de pays non européens.

3.2.2.1. Champ d'application de la convention 108

En principe, la convention 108 et son protocole additionnel s'appliquent «*aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé*»[53] à moins que les parties ne fassent connaître qu'elles n'appliqueront pas la convention à certaines catégories de fichiers conformément à l'article 3, paragraphe 2, point a). Cette liste sera déposée et ne peut inclure des catégories de fichiers assujetties selon le droit interne de la partie concernée à des dispositions de protection des données[54].

C'est pourquoi la législation nationale transposant les dispositions de la convention s'appliquera aux fichiers ayant trait à la «sécurité nationale» d'une partie à la convention à moins que la partie en question n'ait expressément opté en faveur d'une dérogation et qu'elle ait fait connaître sa décision en déposant dûment la liste correspondante. À ce jour, seule une minorité de parties ont déposé des déclarations invoquant une dérogation au titre de la «sécurité de l'État» ou de «secrets d'État»[55].

Certaines parties ont également décidé d'appliquer la convention à des fichiers de données à caractère personnel ne faisant pas l'objet de traitements automatisés, conformément à l'article 3, paragraphe 2, point c), ou à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique [voir l'article 3, paragraphe 2, point b).

---

[51] Le territoire peut être désigné ultérieurement par les parties conformément à l'article 24 de la convention.

[52] Voir l'article 23 de la convention.

[53] Voir l'article 3, paragraphe 1, de la convention.

[54] Voir l'article 3, paragraphe 2, point a), de la convention.

[55] Dix parties ont présenté ce type de déclaration, dont des États membres de l'UE, en l'occurrence l'Irlande, la Lettonie, Malte et la Roumanie.

3.2.2.2. Principes régissant la protection des données dans le cadre de la convention 108

Le chapitre II de la convention énonce les «principes de base pour la protection des données». Le principe de qualité des données (article 5) prévoit l'obligation selon laquelle les données sont obtenues et traitées loyalement et licitement; enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités; adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées; exactes et si nécessaire mises à jour; conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.

L'article 6 dispose que des «catégories particulières de données» (les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle) de même que les données à caractère personnel concernant des condamnations pénales ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées.

L'article 7 contient l'obligation de prendre des mesures de sécurité appropriées tandis que l'article 8 fixe les droits de la personne concernée à l'information, à l'accès, à la rectification et à l'effacement, ainsi que le droit de disposer d'un recours si ces droits ne sont pas respectés.

Selon l'article 10, les parties s'engagent à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet à ces principes. L'article 11 permet aux parties d'accorder une protection plus étendue que celle prévue par la convention.

3.2.2.3. Exceptions

L'article 9 de la convention prévoit des exceptions aux dispositions concernant l'obligation de respecter les principes de qualité (article 5), les garanties particulières pour les données sensibles (article 6) et les droits des personnes concernées (article 8)[56] lorsqu'une telle dérogation:

- est prévue par la loi de la partie; et
- constitue une mesure nécessaire dans une société démocratique à la protection de la personne concernée et des droits et libertés d'autrui, ainsi qu'à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales.

Une fois de plus, il convient de rappeler que la Cour accorde dans sa jurisprudence une grande importance à l'interprétation des dérogations visées à l'article 8 de la CEDH. Ce raisonnement peut, a fortiori, s'appliquer à l'interprétation des dérogations contenues dans la convention

[56] Voir l'article 9 de la convention.

108[57]. La Cour interprète les droits fondamentaux d'une manière très large, en vertu du principe d'efficacité, lequel exige que ces droits soient interprétés dans le sens qui protège au mieux la personne[58]. Il en découle de même du protocole additionnel aux termes duquel «*Les Parties possèdent une marge d'appréciation pour déterminer les dérogations au principe de niveau adéquat. Les règles pertinentes de droit interne doivent néanmoins respecter le principe de droit inhérent à l'ordre juridique européen qui consiste à interpréter les clauses d'exception de manière restrictive afin que l'exception ne devienne pas la règle*»[59].

3.2.2.4. Le protocole additionnel n° 181[60] et les règles relatives aux transferts

Un protocole additionnel à la convention 108, non ratifié par l'ensemble des États membres de l'UE, fixe les règles relatives aux flux transfrontières de données ainsi que l'obligation de se doter d'autorités de contrôle indépendantes dans le domaine de la protection des données.

L'article 2, paragraphe 1, du protocole additionnel prévoit que les flux transfrontières de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas partie à la convention ne peuvent être effectués que si cet État ou cette organisation destinataire assure un niveau de protection adéquat pour le transfert considéré.

Cependant, par dérogation à cette disposition, l'article 2, paragraphe 2, dispose que les parties peuvent autoriser un transfert de données à caractère personnel (a) si le droit interne le prévoit pour des intérêts spécifiques de la personne concernée ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants; ou (b) si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne.

---

[57] Il peut être avancé que la Cour se réserve le droit d'examiner la convention 108 par le biais des dispositions de l'article 8 de la CEDH.

[58] Jean-François Akandji-Kombe, *Les obligations positives en vertu de la Convention européenne des droits de l'homme*, Précis sur les droits de l'homme n° 7, Conseil de l'Europe, 2007.

[59] Voir le rapport explicatif sur le protocole additionnel à la convention 108 concernant les autorités de contrôle et les flux transfrontières de données, article 2, paragraphe 2, point a).

[60] Protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STCE n°: 181), Strasbourg, 8.11.2001.

3.2.2.5. Recommandation n° (87)15[61] sur le traitement des données à caractère personnel dans le secteur de la police

Outre les instruments juridiquement contraignants mentionnés ci-dessus, le Comité des ministres a adopté plusieurs recommandations à l'intention des membres du Conseil de l'Europe concernant le traitement des données à caractère personnel. Ces recommandations ont été à la base de la promulgation de législations nationales dans plusieurs États membres et certaines d'entre elles sont mentionnées et mises en œuvre dans des instruments contraignants de l'UE.

La recommandation n° (87)15 vise à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Elle fournit aux États membres une orientation sur la base de l'article 8 de la CEDH, de la convention 108 et des dérogations autorisées au titre de l'article 9 de cette dernière. Elle couvre «*l'ensemble des tâches incombant aux autorités de police pour la prévention et la répression des infractions pénales et le maintien de l'ordre public*»[62]. Elle n'est donc pertinente que dans la mesure où les tâches relevant de la sécurité nationale sont effectuées par les autorités de police régulières et non par des services de sécurité ou de renseignement.

3.2.3. Conclusion

En conclusion, dans la mesure où l'ensemble des États membres de l'UE sont également parties à la CEDH et à la convention, ils ont l'obligation positive, également développée dans la jurisprudence des cours européennes, de garantir la protection efficace des droits fondamentaux de toutes les personnes relevant de leur juridiction.

Toute restriction à ces droits fondamentaux ne peut être acceptée que si elle remplit les conditions fixées par la Cour et se limite donc à des situations spécifiques, bien définies et prévisibles. Aussi le groupe de travail fait-il observer que, si la conformité avec les instruments du Conseil de l'Europe doit être jugée effective, aucune collecte de données massive, non ciblée et secrète ayant trait à des personnes relevant de la juridiction de l'UE ne saurait être tolérée par les États parties à la CEDH.

4. Le droit de l'Union européenne

En ce qui concerne la législation applicable au niveau de l'Union européenne, le présent point examine la portée de la dérogation au titre de la sécurité nationale de même que les textes pertinents tels que l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE) ainsi que l'article 7, l'article 8 et l'article 52, paragraphe 1, de la Charte des droits fondamentaux. En ce qui concerne le droit dérivé, il examine le cadre au regard duquel la

[61] Recommandation n° (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, 17.9.1987.

[62] Voir le point «Champ d'application et définitions» de la recommandation n° R (87)15.

directive 95/46/CE[63,64] et la directive «vie privée et communications électroniques» sont évaluées, avec une attention particulière accordée au mécanisme de transfert des données au titre de la directive 95/46/CE.

4.1 Dérogation au titre de la sécurité nationale

Avant d'aborder les particularités de la législation de l'Union européenne, il y a lieu de s'attarder sur la signification de la dérogation au titre de la sécurité nationale prescrite par l'article 4, paragraphe 2, du traité sur l'Union européenne (TUE). Cet article stipule que «*L'Union respecte l'égalité des États membres (...) ainsi que leur identité nationale (...). Elle respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet (...) de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre*.» C'est pourquoi le droit de l'UE, dont la Charte des droits fondamentaux de l'Union européenne (ci-après la Charte)[65], ne s'applique pas aux matières ayant trait à la sécurité nationale des États membres. Il s'agit d'une importante dérogation à l'applicabilité du droit de l'UE, qui se révèle également particulièrement pertinente pour de nombreuses questions soulevées dans le présent document de travail, dans la mesure où les services de sécurité et de renseignement sont généralement censés s'acquitter de leurs tâches au nom de la sécurité nationale des États membres.

4.1.1. Absence de définition claire concernant la notion de sécurité nationale

En résumé, l'UE n'est pas compétente pour légiférer sur des matières afférentes à la sécurité nationale des États membres. Il n'existe cependant pas de définition claire, dans la législation de l'UE, de ce que recouvre la notion de «sécurité nationale». Au contraire, les traités de l'UE contiennent des notions auxquelles ils font référence et qu'il est particulièrement difficile de distinguer de la sécurité nationale, ou qui sont à tout le moins étroitement liées à cette dernière, et pour lesquelles l'UE est néanmoins habilitée à légiférer.

Tout d'abord, l'article 75 du traité sur le fonctionnement de l'Union européenne (TFUE) prévoit, dans le titre traitant de l'«Espace de liberté, de sécurité et de justice» (ELSJ) la compétence pour l'UE d'établir un cadre de mesures destinées à prévenir et à combattre le terrorisme et les activités criminelles connexes. Cette disposition soulève la question de savoir comment la lutte contre le terrorisme peut se distinguer de la protection de la sécurité nationale. Des mesures spécifiques prises dans le cadre de la lutte contre le terrorisme illustrent davantage ce propos.

---

63 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

64 Dans ce chapitre, toute référence à la directive doit s'entendre comme englobant la législation nationale portant application de celle-ci dans les États membres, même si ladite législation n'est pas mentionnée de manière explicite.

65 Journal officiel C 364 du 18 décembre 2000.

L'UE et ses États membres coopèrent étroitement avec les États-Unis dans la lutte contre le terrorisme, par exemple en échangeant des informations sur les transactions financières à analyser dans le cadre du programme de surveillance du financement du terrorisme (TFTP). Le champ d'application de l'accord TFTP2 sous-jacent[66] comprend la prévention, l'examen, la détection et la poursuite d'actes susceptibles de déstabiliser gravement ou de détruire les structures fondamentales d'un pays. En outre, toute piste découverte au départ de données partagées par l'UE dans le cadre de ce programme et utile pour les efforts de lutte antiterroriste déployés par les États membres doit être partagée par les États-Unis. De l'avis du groupe de travail, le traitement de données à caractère personnel à de telles fins du moins s'apparente étroitement à ce qui peut être généralement perçu comme un objectif de sécurité nationale et peut apparemment être soumis aux règles approuvées par l'UE.

Qui plus est, l'article 24, paragraphe 1, du TUE ainsi que l'article 2, paragraphe 4, du TFUE prévoient que la compétence de l'Union dans les matières relevant de la politique étrangère et de sécurité commune (PESC) «*couvre ... l'ensemble des questions relatives à la sécurité de l'Union*». En conséquence, «*la sécurité de l'Union*» relève du droit de l'UE et doit également se distinguer de la sécurité nationale des États membres, laquelle – selon l'article 4, paragraphe 2, du TUE – échappe au champ d'application du droit de l'UE.

En ce qui concerne le droit dérivé, l'article 3 de la directive 2000/31/CE[67] dispose que «*Les États membres peuvent prendre, à l'égard d'un service donné de la société de l'information, des mesures qui dérogent ... si les conditions suivantes sont remplies: (a) les mesures doivent être ... nécessaires pour une des raisons suivantes: ... la sécurité publique, y compris la protection de la sécurité et de la défense nationales…»*. Une formulation analogue est proposée à l'article 3, paragraphe 2, premier tiret, de la directive 95/46/CE relative à la protection des données: *«La présente directive ne s'applique pas au traitement de données à caractère personnel - mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, ... et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal»*. Aux termes de ces dispositions, la sécurité nationale, la sûreté de l'État, la sécurité publique et la défense sont autant de notions qu'il convient de distinguer les unes des autres.

La jurisprudence de la CJUE n'apporte pas non plus de définition claire de la notion de «sécurité nationale». Dans l'affaire Promusicae[68], la CJUE a estimé que «*[ces exceptions]*

[66] Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, 27 juin 2010.

[67] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).

[68] CJUE, Productores de Música de España (Promusicae) contre Telefónica de España SAU (C-275/06, arrêt du 29 janvier 2008), point 51.

concernent en effet, d'une part, la sécurité nationale, la défense et la sécurité publique, qui constituent des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers…».

Dans les conclusions formulées dans l'affaire C-120/94[69], l'avocat général Jacobs renvoie à une jurisprudence antérieure de la Cour européenne des droits de l'homme. La Cour avait ainsi déclaré qu'«*Il incombe d'abord à chaque État contractant, responsable de "la vie de (sa) nation", de déterminer si un "danger public" la menace et, dans l'affirmative, jusqu'où il faut aller pour essayer de le dissiper*».

En résumé, ni les dispositions applicables du droit de l'UE ni la jurisprudence de la CJUE n'offrent une définition claire de ce que revêt le terme «sécurité nationale». En outre, l'UE et ses États membres utilisent des notions diverses relativement semblables en rapport avec la sécurité sans pour autant les définir: sécurité intérieure, sécurité nationale, sûreté de l'État et défense sont autant de notions qu'il convient de distinguer mais qui, de l'avis du groupe de travail, sont reliées de manière indissociable. C'est pourquoi des arguments d'ordre strictement juridique ne peuvent justifier à eux seuls que certains éléments relèvent ou non de la dérogation au titre de la sécurité nationale. En réalité, il apparaît nécessaire de tenir compte de la situation politique en vigueur au moment de faire ce «choix», ainsi que des acteurs concernés. On peut toutefois affirmer que, même si les activités menées par des services de sécurité et de renseignement sont communément acceptées comme relevant de la dérogation au titre de la sécurité nationale, il n'en va pas toujours de même lorsque des autorités répressives générales accomplissent des tâches analogues.

La CJUE est la seule institution en mesure d'apporter une plus grande sécurité juridique quant à ce qu'il convient de considérer ou non comme relevant de la dérogation au titre de la sécurité nationale. Seule la CJUE peut définir davantage le champ d'application du droit de l'Union et – partant – l'applicabilité de la Charte. Jusqu'à ce que la CJUE ait apporté de nouveaux éclaircissements sur la portée de la dérogation au titre de la sécurité nationale, le groupe de travail attend des États membres qu'ils s'en tiennent à la jurisprudence établie[70], laquelle exige que tout recours à ladite dérogation soit dûment justifié. Ainsi, dans le premier arrêt Kadi, la CJUE a clairement affirmé que les obligations imposées par un accord international ne peuvent porter atteinte aux principes consacrés par les traités de l'UE, dont le principe selon lequel tous les actes de l'UE doivent respecter les droits fondamentaux.

---

[69] Commission des Communautés européennes contre République hellénique; conclusions du 6 avril 1995, point 55.

[70] Dont l'affaire C-387/05, Commission européenne contre République italienne, arrêt du 15 décembre 2009, point 45: «*Il ne saurait en être déduit qu'il existerait une réserve générale, inhérente au traité, excluant du champ d'application du droit communautaire toute mesure prise au titre de la sécurité publique. Reconnaître l'existence d'une telle réserve, en dehors des conditions spécifiques des dispositions du traité, risquerait de porter atteinte au caractère contraignant et à l'application uniforme du droit communautaire.*»

Dans l'affaire Rotaru c. Roumanie[71], la Cour a établi de la même manière que les données collectées doivent être pertinentes aux fins poursuivies en matière de sécurité nationale et que, même dans un cadre relevant de la sécurité nationale, la loi doit définir le genre d'informations pouvant être consignées, les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, les circonstances dans lesquelles peuvent être prises ces mesures ou la procédure à suivre. De même, ladite loi doit fixer des limites quant à l'ancienneté des informations détenues et à la durée de leur conservation. Elle doit également renfermer des dispositions explicites et détaillées sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues.

Au moment d'apprécier si la dérogation au titre de la sécurité nationale est applicable, il convient également d'examiner s'il s'agit d'une dérogation générale, comme celle fixée dans les traités et à l'article 3, paragraphe 2, de la directive 95/46/CE, ou s'il s'agit d'une dérogation s'inscrivant dans le cadre d'une disposition qui exclut certaines garanties pour des raisons de sécurité nationale, par exemple lorsque des États membres sont autorisés à imposer des limitations au droit d'accès d'une personne concernée pour des raisons de sécurité nationale, tel que prévu à l'article 13, paragraphe 1, point a), de la directive 95/46/CE.

4.1.2. L'intérêt d'un pays tiers en matière de sécurité nationale

L'analyse proposée jusqu'ici appréhende la dérogation au titre de la sécurité nationale dans le cadre de la relation entre l'Union européenne et les États membres. Dans ce contexte, la sécurité nationale permet de distinguer les compétences de l'Union de celles des États membres. Cependant, le fait que les activités menées par les États membres au titre de la sécurité nationale soient exclues du champ d'application du droit de l'UE ne signifie pas pour autant que le droit de l'UE cesse de s'appliquer dès lors que des pays tiers accèdent au nom de leur propre sécurité nationale à des données soumises à la législation de l'UE en matière de protection des données.

Le groupe de travail interprète l'article 4 du TUE comme une tentative visant à définir les compétences de l'Union à l'égard des États membres. Ces derniers font valoir leur souveraineté quand il est question de leur propre sécurité nationale. Cette situation diffère toutefois de l'obligation de respecter la législation de l'UE afférente à la protection des données imposée aux responsables du traitement même lorsque ces derniers sont soumis à la législation d'un pays tiers en matière de sécurité nationale. C'est pourquoi le groupe de travail souligne que la dérogation au titre de la sécurité nationale doit être interprétée de manière à refléter la compétence de l'UE à l'égard des États membres et non comme une dérogation générale aux exigences de l'UE en matière de protection des données accordée à toutes les activités dont l'exécution est sollicitée par des pays tiers au nom de la sécurité nationale.

---

[71] Voir notamment les points 53 à 63 de l'arrêt rendu par la Cour dans l'affaire Rotaru c. Roumanie» , 4 mai 2000, accessible à l'adresse http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:[%22001-58586%22]} (consultée en dernier lieu le 20 novembre 2014).

En outre, le groupe de travail est d'avis qu'il est important d'évaluer de manière critique si la surveillance est effectivement réalisée aux fins de la sécurité nationale. Il convient de noter que, bien que les activités de surveillance américaines objet des révélations puissent sembler de prime abord destinées à préserver la sécurité nationale, il semble en réalité que les intérêts visés soient bien plus larges. Ainsi, le FISA Act autorise les interceptions dès lors que les informations «*concernent (...) la conduite des affaires extérieures des États-Unis*»[72]. Il est très peu probable qu'une quelconque définition de la dérogation au titre de la sécurité nationale prévue dans les instruments de l'UE, même si elle est étendue au-delà de son champ d'application initial, puisse couvrir un objectif aussi large. En outre, le groupe de travail observe que la ligne séparant les objectifs de sécurité nationale des objectifs de répression est extrêmement ténue, comme le démontre également la participation de différentes agences (telles que le FBI, la CIA et la NSA) dans les programmes de surveillance des États-Unis. Aussi le respect du principe de limitation de la finalité est-il essentiel.

Le groupe de travail craint que la législation de l'UE (relative à la protection des données) puisse être contournée dans la pratique en faisant simplement valoir que le traitement des données soit exigé à des fins de sécurité nationale[73]. Il s'agit d'une évolution dangereuse d'autant plus si ce n'est pas la sécurité nationale d'un État membre qui est en jeu mais la prétendue sécurité nationale d'un pays tiers. Le groupe de travail souligne le fait que les dérogations prévues dans les traités n'offrent pas la possibilité d'invoquer la sécurité nationale d'un pays tiers comme argument permettant à lui seul d'exclure l'applicabilité de la législation de l'UE.

Il convient toutefois de noter qu'un État membre peut alléguer qu'une menace envers la sécurité nationale d'un pays tiers (partenaire ou allié) constitue également une menace pour sa propre sécurité nationale, ce qui rend dès lors inapplicable le droit de l'UE. Le groupe de travail reconnaît qu'il peut exister des domaines dans lesquels un État membre de l'UE et un pays tiers partagent un même intérêt en matière de sécurité nationale et que, le cas échéant, il se peut que les frontières de la sécurité nationale d'un État membre de l'UE ne soient pas toujours claires. L'argument selon lequel l'intérêt d'un pays tiers en matière de sécurité nationale coïncide avec celui d'un État membre de l'UE ne doit être accepté que s'il est dûment justifié auprès des autorités compétentes au cas par cas. Si l'État membre ne procède pas de la sorte, il devra se conformer au droit de l'UE. Ce raisonnement est étayé par l'arrêt de la CJUE dans l'affaire Commission européenne contre République italienne, lequel dispose que la seule invocation de la dérogation au titre de la sécurité nationale ne suffit pas pour déclarer la non-applicabilité du droit de l'UE[74]. Cela est d'autant plus vrai si l'État membre

[72] 50 U.S. Code § 1801, point (e)(2)(B)

[73] Il convient de rappeler que, selon la jurisprudence de la CJUE, notamment dans l'affaire ZZ contre Secretary of State (C-300/11), toute limitation d'un droit fondamental doit notamment respecter le contenu essentiel du droit fondamental en cause et requiert, en outre, que, dans le respect du principe de proportionnalité, elle soit nécessaire et réponde effectivement à des objectifs d'intérêt général reconnus par l'Union européenne (point 51) et soit soumise à un contrôle juridictionnel (point 58).

[74] Affaire C-387/05, point 45 (cité supra).

soutient qu'il partage avec un pays tiers un même intérêt en matière de sécurité nationale. En conséquence, la base juridique permettant d'invoquer l'intérêt d'un pays tiers en matière de sécurité nationale doit être clairement établie dans la législation nationale ainsi que, le cas échéant, dans des accords politiques internationaux juridiquement contraignants conclus par les gouvernements des États membres[75].

4.2. Légifération de la protection des données

L'article 16, paragraphe 1, du TFUE établit le droit à la protection des données à caractère personnel, lequel s'applique à «toute personne».

Afin de garantir l'application de ce droit, l'article 16, paragraphe 2, prévoit une nouvelle base juridique pour l'adoption de la réglementation européenne relative à la protection des données à l'égard du traitement de ces données par les institutions, organes et organismes de l'UE, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et des règles relatives à la libre circulation de ces données. Cela exige également que le respect de ces règles soit soumis au contrôle d'autorités indépendantes.

La déclaration 21 indique que, dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, des règles spécifiques peuvent s'avérer nécessaires. Cependant, ces règles seront également adoptées sur la base de l'article 16 du TFUE.

En ce qui concerne la sécurité nationale, la déclaration 20 indique que chaque fois que doivent être adoptées, sur la base de l'article 16, des règles relatives à la protection des données à caractère personnel qui pourraient avoir une incidence directe sur la sécurité nationale, il devra en être dûment tenu compte**.** Elle rappelle également que la législation actuellement applicable (voir en particulier la directive 95/46/CE) prévoit des dérogations spécifiques à cet égard.

4.3. La Charte des droits fondamentaux de l'Union européenne

4.3.1. Le champ d'application de la Charte de l'UE

As a result of the national security exemption addressed above and contrary to Council of Europe instruments, the scope of application of the Charter is limited. Still, as far as national security of EU Member States is not concerned, the principles enshrined in the Charter, in particular in Articles 7 and 8, apply to EU institutions and bodies and all the activities of Member States when they implement Union law.

---

[75] Le groupe de travail «article 29» est parfaitement conscient du fait que certains instruments internationaux juridiquement contraignants tels que des traités d'entraide judiciaire (TEJ) renferment également des dispositions permettant aux États membres de déroger à ces instruments. Cette mesure n'est toutefois autorisée que lorsqu'elle permet de prévenir tout préjudice aux intérêts essentiels de l'État membre concerné (et non aux intérêts essentiels d'un pays tiers qui n'est pas partie à cet instrument). C'est à l'État membre de l'UE qu'il appartient de justifier clairement en quoi consistent ses propres intérêts essentiels.

4.3.2 Le droit au respect de la vie privée et à la protection des données tel que prévu dans la Charte

L'article 7 de la Charte, comparable à l'article 8 de la Convention européenne des droits de l'homme (CEDH), prévoit un droit général au respect de la vie privée et familiale, du domicile et des communications, et protège les personnes contre l'ingérence des autorités publiques. L'article 8, paragraphe 1, établit le droit de toute personne à la protection des données à caractère personnel la concernant: les données à caractère personnel ne peuvent faire l'objet d'un traitement que si certaines exigences essentielles sont respectées. Ces dernières sont fixées à l'article 8, paragraphes 2 et 3, de la Charte, lesquels spécifient que ces données doivent être traitées «*loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi*». Cet article prévoit également le droit de toute personne à accéder aux données collectées la concernant et d'en obtenir la rectification, et soumet le respect de ces règles au contrôle d'une autorité indépendante.

Dans son arrêt annulant la directive sur la conservation des données[76], la CJUE a déclaré que «*l'obligation (...) de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications (...) constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte. En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental. (...) De même, [la conservation des données] est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel*»[77]. La Cour fait valoir en outre qu'étant donné, entre autres, qu'aucune limitation au stockage et à l'accès des données concernant les télécommunications n'est imposée dans la législation et que des droits restreints ont été prévus en faveur des personnes, la directive sur la conservation des données «*comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire*»[78].

Même si l'affaire relative à la conservation des données a trait à l'applicabilité de dispositions réglementaires, le raisonnement de la CJUE est particulièrement pertinent, notamment pour les programmes dans lesquels la finalité du traitement des données comprend la lutte contre le terrorisme et/ou les actes criminels graves (deux domaines considérés comme relevant de la

[76] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

[77] Voir l'arrêt de la CJUE dans l'affaire Digital Rights Ireland et Seitlinger et autres (affaires jointes C-293/12 et C-594/12), 8 avril 2014, points 34-36.

[78] Idem, point 6**5**.

compétence de l'Union européenne[79]). En d'autres termes, pour être jugés conformes au cadre juridique de l'UE en matière de protection des données, ces programmes doivent être précisément encadrés par des dispositions permettant de garantir qu'ils sont effectivement limités au strict nécessaire. L'article 52, paragraphe 1, de la Charte précise ces garanties.

4.3.3 Le champ d'application des restrictions au droit fondamental au respect de la vie privée et à la protection des données

L'article 52, paragraphe 1, de la Charte permet que des limitations soient apportées à l'exercice des droits et libertés reconnus par la Charte pour autant que ces limitations:

- soient nécessaires et proportionnées;
- répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui;
- soient prévues par la loi;
- respectent le contenu essentiel desdits droits et libertés.

Dans l'affaire ZZ contre Secretary of State for the Home department, la CJUE a rappelé que *«si, certes, l'article 52, paragraphe 1, de la Charte admet des limitations à l'exercice des droits consacrés par celle-ci, cette disposition exige toutefois que toute limitation doit notamment respecter le contenu essentiel du droit fondamental en cause et requiert, en outre, que, dans le respect du principe de proportionnalité, elle soit nécessaire et réponde effectivement à des objectifs d'intérêt général reconnus par l'Union»*[80].

En outre, elle a confirmé qu'il devait être démontré que les limitations spécifiques en cause étaient effectivement nécessaires pour garantir la sûreté de l'État. Le fait qu'un État membre invoque une telle dérogation n'est pas à lui seul suffisant: *«Il incombe à l'autorité nationale compétente d'apporter, conformément aux règles de procédure nationales, la preuve que la sûreté de l'État serait effectivement compromise par une communication à l'intéressé des motifs précis et complets qui constituent le fondement d'une décision prise (...). Il en découle qu'il n'existe pas de présomption en faveur de l'existence et du bien-fondé des raisons invoquées par une autorité nationale»*[81].

---

[79] Voir le point 4.1.1.

[80] Voir l'arrêt de la CJUE dans l'affaire ZZ contre Secretary of State for the Home department, affaire C-300/11, 4 juin 2013, point 51.

En outre, dans l'affaire Unitrading, la CJUE a précisé que les dispositions nationales ne devaient pas «rendre pratiquement impossible ou excessivement difficile l'exercice des droits conférés par l'ordre juridique communautaire (principe d'effectivité)». CJUE, Unitrading ltd contre Staatssecretaris van Financiën, affaire C-437/13, 23 octobre 2014.

[81] Idem, point 61.

Quand bien même la nécessité d'une telle limitation serait démontrée, une dérogation généralisée à l'obligation de respecter les droits fondamentaux ne serait pas pour autant admise: «*S'il s'avère que la sûreté de l'État s'oppose effectivement à la communication à l'intéressé desdits motifs, le contrôle juridictionnel (...) doit (...) être effectué dans le cadre d'une procédure qui met en balance de manière appropriée les exigences découlant de la sûreté de l'État et celles du droit à une protection juridictionnelle effective tout en limitant les ingérences éventuelles dans l'exercice de ce droit au strict nécessaire*»[82]

4.3.4. Interaction entre la Charte et la CEDH

Les champs d'application de la Charte de l'UE et de la CEDH ne sont pas identiques: comme exposé ci-dessus, la sécurité nationale des États membres de l'UE est exclue du champ d'application du droit de l'UE, et donc de la Charte, tandis que la CEDH exige des parties signataires qu'elles garantissent à toute personne relevant de leur juridiction une série de droits et de libertés, dont le droit au respect de la vie privée, et ne comporte pas de dérogation générale pour les matières relevant de la sécurité nationale. Cependant, la CEDH autorise tout de même l'ingérence des États membres dans l'exercice du droit au respect de la vie privée conformément à la législation nationale applicable, pour autant que cette mesure soit nécessaire, au sein d'une société démocratique, à la sécurité nationale.

L'article 52, paragraphe 3, de la Charte précise que, dans la mesure où celle-ci contient des droits correspondant à des droits garantis par la CEDH, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Les principes fondamentaux développés dans les deux textes sont donc parfaitement cohérents. L'article en question spécifie également que cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

4.4. Directive 95/46/CE[83,84]

4.4.1. Champ d'application de la directive

La directive 95/46/CE ne s'applique pas aux «*traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et [aux] activités de l'État relatives à des domaines du droit pénal*». Cette limitation du champ d'application est énoncée à l'article 3, paragraphe 2, de la directive. Elle reflète le partage des compétences entre l'UE et les États membres, notamment avant l'entrée en vigueur du traité de Lisbonne. Cette directive

[82] Idem, point 64.

[83] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[84] Dans ce chapitre, toute référence à la directive doit s'entendre comme englobant la législation nationale transposant cette dernière dans les États membres, même si ladite législation n'est pas mentionnée de manière explicite.

ne doit toutefois pas être considérée comme dénuée de pertinence dans le contexte de la répression et dans les questions relevant de la sécurité nationale. Au contraire, bien que la directive ne réglemente pas le traitement des données par les autorités de répression et les services de renseignement, les législations nationales transposant cette directive régissent quant à elles la transmission de données à caractère personnel par les responsables du traitement et les sous-traitants lorsque ceux-ci reçoivent l'injonction de communiquer ces informations aux autorités de répression et aux services de renseignement. L'article 13 de la directive permet – dans certaines conditions – que le législateur national prenne des mesures législatives visant à limiter la portée de certains droits et obligations, en autorisant par exemple que soit modifiée la finalité du traitement des données.

Comme expliqué au point 4.1, la dérogation au titre de la sécurité nationale renvoie à la sécurité nationale des États membres de l'UE, laquelle «*reste de la seule responsabilité de chaque État membre*»[85]. En conséquence, si le traitement concerne la sécurité nationale d'un pays tiers et non celle de l'UE ou des États membres de l'UE, celui-ci n'échappe pas au champ d'application de la directive. Celle-ci s'appliquera pour autant que chacun des critères du droit applicable décrits ci-dessous soit respecté. Ensuite, les responsables du traitement devront s'y conformer et pourraient faire l'objet de mesures répressives.

En ce qui concerne le champ d'application spécifique/territorial de la directive, l'article 4, paragraphe 1, prévoit que les dispositions d'application nationales s'appliquent au traitement de données à caractère personnel lorsque:

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement situé sur le territoire d'un État membre de l'UE.

L'avis du groupe de travail sur le droit applicable propose un certain nombre de critères permettant d'identifier plus facilement ce que revêt la notion d'établissement pertinent. Il prône une approche fonctionnelle, en tenant compte davantage du cadre dans lequel les activités de l'établissement sont menées et du degré de participation de ce dernier dans le traitement des données à caractère personnel que de la localisation des données ou du lieu d'établissement du responsable du traitement[86]. La CJUE a précisé ultérieurement que l'article 4, paragraphe 1, point a), de la directive n'exige pas que «*le traitement de données à caractère personnel en question soit effectué "par" l'établissement concerné lui-même*»[87]. Elle estime en outre que cette disposition ne saurait être interprétée de manière restrictive, au vu de l'objectif de la directive d'«*assurer une protection efficace et complète des libertés et des droits fondamentaux (...)*»[88].

[85] Article 4, paragraphe 2, du TUE.

[86] Avis 8/20**10** du groupe de travail «article 29» sur le droit applicable, adopté le 16 décembre 2010.

[87] Arrêt de la CJUE dans l'affaire Google contre Espagne,13 mai 2014, point 52.

[88] Idem, point 5**3**.

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;

c) le responsable du traitement n'est pas établi sur le territoire de l'UE et recourt, à des fins de traitement de données à caractère personnel, à des moyens[89], automatisés ou non, situés sur le territoire d'un État membre de l'UE (sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté).

Dans ce cas, l'article 4, paragraphe 2, exige du responsable du traitement qu'il désigne un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

Le groupe de travail salue le fait que le champ d'application territorial des législations de l'UE sur la protection des données fasse l'objet d'une définition plus explicite dans le cadre de la proposition de règlement général sur la protection des données: en effet, l'article 3, paragraphe 2, de la proposition de la Commission européenne[90] dispose que le règlement s'applique au traitement des données à caractère personnel appartenant à des personnes concernées ayant leur résidence sur le territoire de l'Union par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées (a) à l'offre de biens ou de services à ces personnes concernées dans l'Union ou (b) à l'observation de leur comportement.

Bien que la proposition soit en cours d'examen au Parlement européen et au Conseil de l'UE, les deux colégislateurs approuvent largement le champ d'application proposé par la Commission. Le Conseil de l'UE soutient expressément le champ d'application territorial de la proposition de règlement et a insisté sur la nécessité de garantir dans une large mesure l'application des règles de l'Union aux responsables du traitement non établis dans l'UE lors du traitement de données à caractère personnel appartenant à des personnes concernées relevant de la juridiction de l'Union[91]. Le Parlement européen s'est également prononcé en faveur du champ d'application proposé et a même élargi ce dernier[92].

Dans l'arrêt de 2009 relatif à la conservation des données, la CJUE a conclu que l'article 95 de l'ancien traité CE (rapprochement des législations concernant le marché intérieur) constituait

---

[89] L'avis du groupe de travail «article 29» sur le droit applicable, cité supra, apporte des indications supplémentaires sur la notion de «moyens».

[90] Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données).

[91] Conseil de l'Union européenne, communiqué de presse, 3319e session du Conseil «Justice et affaires intérieures» des 5 et 6 juin 2014, ainsi que le document 2012/0011 (COD).

[92] Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données).

la base juridique appropriée pour l'imposition d'une obligation en matière de conservation des données. Dans sa motivation, la Cour a estimé que la directive 2006/24/CE visait les activités des fournisseurs de services dans le marché intérieur, modifiait les obligations de ces derniers en matière de protection des données[93], avait des implications économiques importantes pour ces fournisseurs de services et ne comportait aucune réglementation des activités menées par les autorités publiques à des fins répressives. L'argument avancé par l'Irlande selon lequel l'obligation ne pouvait être imposée que conformément au titre VI de l'ancien traité UE (justice et affaires intérieures) a été rejeté.

Dans l'affaire relative à la conservation des données, la conservation obligatoire des données à caractère personnel par les fournisseurs de services, même à des fins de répression, est considérée comme un traitement soumis aux dispositions nationales portant application de la réglementation de l'UE relative à la protection des données (en particulier, la directive «vie privée et communications électroniques»[94]). En conséquence, la directive sur la conservation des données constituait une dérogation spécifique de certaines dispositions de la directive «vie privée et communications électroniques»[95].

De même, les dispositions nationales portant application de la directive 95/46/CE s'appliquent au traitement de données par des acteurs privés à des fins commerciales, y compris au transfert de données provenant de ces acteurs privés. Elles s'appliquent également au traitement de données par les autorités publiques des États membres de l'UE couvert par la directive, c.-à-d. non exclu au titre de l'article 3, paragraphe 2.

La CJUE a également spécifié que cette situation ne pouvait être comparée au cadre dans lequel s'inscrit l'arrêt rendu dans l'affaire Passenger Name Records (PNR: dossiers passagers)[96]. Elle a fait valoir qu'«*à la différence de la décision 2004/496 [annulée par l'arrêt PNR], qui concernait un transfert de données personnelles s'insérant dans un cadre institué par les pouvoirs publics en vue d'assurer la sécurité publique, la directive 2006/24 vise les activités des fournisseurs de services dans le marché intérieur et ne comporte aucune réglementation des activités des pouvoirs publics à des fins répressives*».

En outre, à la différence de la directive sur la conservation des données récemment annulée, les accords PNR (sur les données des dossiers passagers) conclus par l'UE comportent des garanties relatives à la protection des données[97] s'adressant aux autorités publiques qui

---

[93] Fixées par la directive 2002/58/CE (directive «vie privée et communications électroniques»).

[94] 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, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009.

[95] Voir, en particulier, les articles 5, 6 et 9 de la directive 2002/58/CE.

[96] CJUE, affaires jointes C-317/04 et C-318/04, Parlement européen contre Conseil de l'Union européenne et Commission des communautés européennes, 30 mai 2006.

[97] Jugées adéquates par le Conseil mais critiquées **par le groupe de travail «article 29» et le CEPD.**

procèdent au traitement de ces données. Ces garanties ont été jugées «adéquates» par le Conseil de l'UE[98], bien que le groupe de travail «article 29» et le contrôleur européen de la protection des données ne les aient pas considérées suffisantes[99].

Tout cela tend à démontrer que si le transfert de données à caractère personnel par des entreprises privées est imposé à des fins répressives, le cadre juridique général régissant la protection des données continuera de s'appliquer jusqu'au transfert effectif de ces données. Dans de nombreux États membres, la situation sera différente pour les services de renseignement dans la mesure où ceux-ci ne sont pas soumis à la législation générale afférente à la protection des données[100]. Néanmoins, il ressort clairement qu'une base juridique appropriée doit être mise en place également pour le transfert de données à caractère personnel aux services de renseignement ainsi que pour la collecte de ce type de données par ces services.

4.4.2. Les principes de protection des données contenus dans la directive 95/46/CE

Lorsqu'une activité de traitement relève du champ d'application de la directive, les principes, droits et obligations en matière de protection des données fixés dans celle-ci doivent être respectés:

- principes relatifs à la qualité des données: aux termes de l'article 6 de la directive, les responsables du traitement[101] doivent veiller à ce que les données à caractère personnel soient (a) traitées loyalement et licitement; (b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités; (c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement; (d) exactes et, si nécessaire, mises à jour; et (e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement[102];

- principes relatifs à la légitimation des traitements de données: l'article 7 dispose que le traitement des données à caractère personnel ne peut être effectué que si (a) la personne concernée a indubitablement donné son consentement; ou s'il est nécessaire (b) à l'exécution d'un contrat; (c) au respect d'une obligation légale à laquelle le responsable du traitement est soumis; ou (d) à la sauvegarde de l'intérêt vital de la personne concernée; (e) à l'exécution

[98] Voir entre autres l'article 19 de l'actuel accord PNR UE-USA (accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, 2011).

[99] Voir les avis du CEPD et du groupe de travail «article 29» sur les accords PNR, disponibles aux adresses www.edps.europa.eu et http://ec.europa.eu/justice/data-protection/article-29.

[100] WP215 (cité supra), p. 9.

[101] Voir l'article 6, paragraphe 2, de la directive.

[102] Voir l'article 6, paragraphe 1, de la directive.

d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées; ou (f) à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées (à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée);

• données sensibles: l'article 8 interdit en principe le traitement de catégories particulières de données (des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle), à moins que ne s'appliquent certaines exceptions[103]. Il soumet également à des garanties supplémentaires le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté;

• transparence: les articles 10 et 11 spécifient les informations à donner à la personne concernée en cas de collecte de données auprès de cette dernière et lorsque les données n'ont pas été collectées auprès de cette dernière. Conformément à l'article 18, les responsables du traitement sont également tenus de notifier aux autorités responsables de la protection des données toute activité de traitement[104]. L'article 21 prévoit la publication d'un registre des traitements notifiés.

• droits des personnes concernées: les articles 12 et 14 réglementent les droits d'accès, de rectification, d'effacement et de verrouillage des données ainsi que le droit d'opposition au traitement;

• décisions individuelles automatisées: l'article 15 vise à protéger la personne concernée contre certaines activités de profilage et établit le droit de ne pas être soumis à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.;

• confidentialité et sécurité des traitements: les articles 16 et 17 précisent les obligations que les responsables du contrôle et les sous-traitants ont de respecter la confidentialité du traitement et de mettre en œuvre les mesures de sécurité techniques et d'organisation appropriées.

La directive prévoit également le contrôle du respect de ces droits et obligations de la part d'autorités indépendantes chargées de la protection des données ainsi que des possibilités de recours administratif et juridictionnel.

---

[103] Énoncées à l'article 8, paragraphes 2 et 3.

[104] Voir également l'article 19.

4.4.3. Exceptions aux principes de protection des données

Conformément à l'article 13, paragraphe 1, les États membres de l'UE peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits garantis par les principes de qualité et de transparence des données, ainsi que des droits d'accès, de rectification, d'effacement et de verrouillage, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder (a) la sûreté de l'État; (b) la défense; (c) la sécurité publique; (d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées; (e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne; (f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e); ou (g) la protection de la personne concernée ou des droits et libertés d'autrui.

Contrairement aux exclusions générales du champ d'application de la directive énoncées à l'article 3, paragraphe 2, les dérogations aux principes, droits et obligations spécifiques visées à l'article 13, paragraphe 1, ou contenues dans d'autres dispositions de la directive[105] laissent supposer que la directive s'applique en principe au traitement en question. Comme exigé expressément par la directive[106], ces exceptions doivent être ensuite établies par les législations des États membres, lesquelles doivent également, dans de nombreux cas, fournir des garanties supplémentaires[107].

4.5 La directive «vie privée et communications électroniques»

La directive «vie privée et communications électroniques» est étroitement liée à la directive 95/46/CE en ce qui concerne l'application des principes généraux de protection des données. Cette directive prévoit des garanties supplémentaires visant à protéger les communications électroniques. Son champ d'application se limite cependant aux fournisseurs de services de communications électroniques accessibles au public.

L'article 5, paragraphe 1, de la directive 2002/58/CE protège la confidentialité des communications en ces termes: *«Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs*

[105] *Idem*

[106] Voir, entre autres, l'article 13, paragraphes 1 et 2, imposant une mesure législative de la part des États membres.

[107] Voir, entre autres, l'article 13, paragraphe 2.

concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1.»

Un scénario susceptible de déclencher l'application de l'article 5, paragraphe 1, a été décrit par la presse dans le cadre des révélations de Snowden: les services de renseignement obtiennent l'accès aux serveurs d'un fournisseur de services de communications soumis à la directive «vie privée et communications électroniques» en profitant d'une faille dans la sécurité des systèmes de ce fournisseur (plus que probablement avec la coopération confidentielle de ce dernier). Dans le cas extrême de ce scénario, les services de renseignement pourraient avoir accès à l'ensemble des données à destination ou en provenance de ces serveurs[108].

Il pourrait être allégué qu'en *ne proscrivant pas* (ou en ne garantissant pas un contrôle efficace afin de réprimer efficacement) ce type d'accès, (1) les États membres ne se conforment pas aux exigences de confidentialité que leur impose la directive «vie privée et communications électroniques» et que (2) les fournisseurs de services de communications électroniques accessibles au public ne respectent pas les dispositions nationales transposant l'obligation de confidentialité prescrite par la directive.

En outre, les articles 6 et 9 de la directive «vie privée et communications électroniques» protègent les données relatives au trafic ainsi que les données de localisation (autres que celles relatives au trafic), et prévoient leur effacement ou leur anonymisation immédiats, sauf dans des cas spécifiques, notamment lorsque les données sont utilisées à des fins de facturation ou de commercialisation et ce, moyennant des garanties strictes.

Toute autre forme de traitement ou de transfert à des tiers de communications et de données relatives au trafic serait dès lors illicite au titre de la directive «vie privée et communications électroniques», sauf dans le cadre de l'article 15, paragraphe 1. Conformément à cette disposition, toute limitation éventuelle apportée au principe de confidentialité garanti par les articles 5 et 6 doit être assortie de conditions strictes: «*toute limitation apportée à la confidentialité des données de communications doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE*».

Il convient d'interpréter ces conditions strictes à la lumière de l'arrêt rendu en 2014 par la CJUE dans l'affaire relative à la conservation des données, en vertu duquel une telle ingérence devait être «précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire»[109]. L'accès et l'utilisation de la part des autorités nationales compétentes doivent être limités au strict nécessaire tant au niveau des catégories

[108] Des faits analogues survenus dans l'affaire Belgacom ont incité l'autorité belge chargée de la protection des données à ouvrir une enquête.

[109] Cité supra, point 65.

des données que des personnes concernées, et doivent être soumis à des conditions de fond et de procédure. En outre, il y a lieu pour les législations nationales de prévoir une protection efficace contre les risques d'accès illicite et toute autre forme d'abus, y compris l'obligation de soumettre le stockage des données au contrôle d'une autorité indépendante garantissant la conformité avec la législation de l'UE en matière de protection des données.

Comme déjà mentionné, les exceptions à des fins de sécurité nationale sont admissibles au sein de l'UE aux fins de la sécurité nationale des États membres et dans des conditions strictes. Elles ne sauraient justifier l'interception ni la demande de données à caractère personnel de la part de l'autorité publique d'un pays tiers, ni l'accès à ces dernières, si ce n'est au titre d'un impératif de sécurité nationale fixé par ledit pays tiers.

5. Mécanisme de transfert des données selon la directive 95/46/CE

Le fonctionnement exact des programmes de surveillance mis en place de par le monde n'est pas encore parfaitement connu. De nouveaux faits permettant de dresser un tableau plus complet peuvent toujours se produire. Cependant, on peut raisonnablement prévoir que les autorités de surveillance d'un pays tiers ne semblent pouvoir accéder à des données qu'à la suite d'un transfert international d'une entreprise établie dans l'UE vers une autre entreprise située en dehors de l'UE.

De tels transferts devront être encadrés par l'un des outils de transfert prévus dans la directive 95/46/CE de sorte que l'entité étrangère devra respecter ses engagements chaque fois qu'elle recevra une demande de communication de données ou d'accès à des données. Il apparaît donc nécessaire d'analyser les dispositions spécifiques des outils de transfert qui pourraient être pertinents lorsqu'une autorité de surveillance d'un pays tiers accède à des données ou demande la communication de données qui, à l'origine, ont été transférées au départ de l'UE.

Cette partie de l'avis examinera dans un premier temps le cadre juridique actuel régissant les transferts internationaux et analysera ensuite les dispositions spécifiques applicables à différents scénarios.

La directive 95/46/CE ne propose pas de définition pour le terme «transfert de données». Cependant, selon le contrôleur européen de la protection des données, «On peut partir du principe que le terme est utilisé dans son acception naturelle, à savoir que les données "circulent" ou sont autorisées à "circuler" entre différents utilisateurs»[110]. Concernant le règlement (CE) n° 45/2001, il ajoute ensuite que «les responsables du traitement doivent considérer que ce terme implique normalement les éléments suivants: la communication, la diffusion ou toute forme de mise à disposition de données à caractère personnel, étant entendu que l'expéditeur soumis au règlement sait ou prévoit que le ou les destinataires accéderont à

[110] Document d'orientation du CEPD (en anglais), «Le transfert de données à caractère personnel vers des pays tiers et des organisations internationales au départ d'institutions, organes et organismes de l'UE», 14 juillet 2014, p.6.

ces données. Ce terme engloberait dès lors tant les "transferts délibérés" que l'"accès autorisé" aux données par le ou les destinataires»[111].

5.1. Niveau de protection adéquat

À l'instar de toute forme de traitement, un transfert doit, en premier lieu, être conforme aux principes suscités établis par la législation relative à la protection des données. Ensuite, aux termes de l'article 25 de la directive, le destinataire est également tenu d'assurer un niveau de protection adéquat.

Article 25, paragraphe 2: Adéquation des pays tiers et sphère de sécurité: l'article 25 de la directive 95/46/CE interdit tout transfert au départ de l'Union européenne à moins qu'un pays tiers n'assure un niveau de protection adéquat. Si la Commission européenne prend une décision reconnaissant que le pays tiers en cause offre effectivement un tel niveau de protection des données, les transferts peuvent avoir lieu sans autres formes de restrictions. Cela signifie en réalité que les transferts vers le pays tiers en question seront traités de la même manière que les exportations de données à destination d'un autre État membre de l'UE.

Ainsi, la Commission a déjà constaté que, dans le cas des États-Unis, l'accord sur la sphère de sécurité assurait un niveau de protection adéquat pour les transferts de données à caractère commercial de l'Union européenne vers les entreprises américaines ayant adhéré à cet accord. Cependant, cet instrument n'a pas été conçu pour offrir un niveau de protection adéquat à des fins répressives, contrairement à d'autres accords tels que celui sur l'utilisation et le transfert des données des dossiers passagers (accord PNR) entre l'UE et les États-Unis, lequel fournit un cadre pour l'échange de données à caractère personnel entre l'UE et les États-Unis à des fins répressives, dont la prévention du terrorisme et des formes graves de criminalité ainsi que la lutte contre ces phénomènes[112].

Article 26, paragraphe 2: clauses contractuelles types et règles d'entreprise contraignantes: parallèlement à la sphère de sécurité et conformément à l'article 26, paragraphe 2, de la directive, les transferts de l'UE vers un pays tiers peuvent également être autorisés lorsque le responsable du traitement offre «*des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants*». Ces garanties peuvent résulter de *«clauses contractuelles appropriées»* (par exemple, les décisions de la Commission européenne relatives aux clauses contractuelles types pour le transfert de données d'un responsable de traitement à un autre responsable de traitement ou d'un responsable de traitement à un sous-traitant). En outre, depuis 2003, le groupe de travail élabore des règles d'entreprise contraignantes autorisant des transferts au sein d'un groupe d'entreprises.

---

[111] Idem, page 7.

[112] Ces accords ont été négociés après l'annulation de la décision d'adéquation adoptée par la Commission en 2004 de manière à permettre le transfert de ces données.

Article 26, paragraphe 1: dérogations aux règles afférentes aux transferts de données: l'article 26, paragraphe 1, de la directive prévoit qu'un transfert vers un pays tiers n'assurant pas un niveau de protection adéquat ne peut être effectué que s'il est justifié par une des conditions énoncées dans l'article, y compris lorsque «*le transfert [est] nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice*».

Le groupe de travail a déjà élaboré des orientations sur l'application des articles 25 et 26 de la directive 95/46/CE dans son document de travail «Transferts de données à caractère personnel vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données»[113]. Dans le document WP114 publié ultérieurement par le groupe de travail, les orientations indiquaient que les dérogations au principe général devaient être interprétées de manière restrictive, même lorsqu'il était question de l'intérêt public[114]. Il en va de même lorsque des autorités publiques étrangères sont concernées. Le document de travail WP114 précise: *«il est évident que les rédacteurs de la directive ont envisagé que seuls des intérêts publics importants, définis comme tels par la loi nationale applicable aux responsables du traitement établis dans l'UE, puissent être valablement pris en compte dans ce contexte.»*[115]

Le recours à ces dérogations implique qu'une fois transférées, les données ne bénéficient plus de la protection offerte par la directive. C'est la raison pour laquelle, conformément à la jurisprudence de la Cour, ces dérogations doivent être interprétées de manière restrictive (voir le point 3.2.1.3) et pour laquelle le groupe de travail recommande que «*les transferts de données personnelles qui pourraient être qualifiés de répétés, massifs ou structurels soient, dans toute la mesure du possible et justement en raison de ces caractéristiques, effectués dans un cadre juridique spécifique (c'est-à-dire des contrats ou des règles d'entreprise contraignantes)*»[116]. En tout état de cause, le groupe de travail est d'avis que le recours à la dérogation visée à l'article 26, paragraphe 1, ne doit - il va de soi - jamais créer une situation dans laquelle les droits fondamentaux pourraient être violés.

---

[113] Groupe de travail «article 29», WP12, document de travail «Transferts de données à caractère personnel vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données», 24 juillet 1998.

[114] Groupe de travail «article 29», WP114, document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, p. 7.

[115] Groupe de travail «article 29», WP114, document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, p. 15.

[116] Groupe de travail «article 29», WP114, document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, p. 9.

5.2. Instruments spécifiques utilisés pour démontrer l'adéquation de la protection ou apporter des garanties adéquates conformément à la directive 95/46/CE

5.2.1. L'accord sur la sphère de sécurité

Sur la base de la décision de la Commission relative à l'accord sur la sphère de sécurité[117], les principes de cet accord sont jugés adéquats au sens de l'article 25, paragraphe 2, de la directive 95/46/CE. En conséquence, le respect des principes de la sphère de sécurité ainsi que l'adhésion à ces derniers peuvent être invoqués pour justifier les transferts. Ces principes sont respectés par un large éventail d'organisations américaines[118] qui ont autocertifié leur adhésion à ces derniers pour légitimer des transferts au départ de l'UE.

Concernant les transferts ultérieurs, la sphère de sécurité prévoit que «*pour divulguer des informations à un tiers, les organisations sont tenues d'appliquer les principes de notification et de choix*». En d'autres termes, lors de la communication de données à un tiers agissant en qualité de responsable du traitement[119], l'entreprise établie aux États-Unis et agissant en tant que responsable du traitement[120] informe la personne concernée du transfert ultérieur au tiers, offrant ainsi la possibilité à la personne concernée de consentir (ou de s'opposer) au transfert ultérieur en question lorsque les données sont destinées à être utilisées dans «*un but incompatible avec le ou les objectifs pour lesquels les données ont été initialement collectées*».

La sphère de sécurité permet que l'adhésion aux principes puisse être limitée par «*les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis; les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; les exceptions ou les dérogations prévues par*

---

[117] Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique [notifiée sous le numéro C(2000) 2441].

[118] Le champ d'application de la sphère de sécurité est limité de sorte que toutes les organisations ne peuvent y adhérer.

[119] Si l'organisation souhaite procéder à des transferts ultérieurs vers une entité agissant en tant que sous-traitant, elle n'est pas tenue d'appliquer les principes de notification et de choix. L'organisation doit néanmoins, soit s'assurer que le tiers agissant en tant que sous-traitant souscrit aux principes de la sphère de sécurité ou est soumis aux dispositions de la directive ou d'un autre mécanisme attestant du niveau adéquat de la protection, soit passer un accord écrit avec ce tiers assurant au minimum le même niveau de protection de la vie privée que celui exigé dans l'accord sur la sphère de sécurité. Il convient toutefois de tenir à l'esprit qu'en matière de surveillance, l'autorité de renseignement d'un pays tiers ne peut être considérée que comme responsable du traitement.

[120]

la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables»[121].

Le niveau de protection garanti par la sphère de sécurité a été remis en question dès son processus de création. La mise en œuvre des principes de la sphère de sécurité a fait notamment l'objet de critiques virulentes. Dans sa récente communication relative au fonctionnement de la sphère de sécurité, la Commission européenne a soulevé la question de la surveillance de masse au regard du régime de la sphère de sécurité et signalé que *«Ces programmes [programmes de surveillance des États-Unis] étant à grande échelle, il est possible que les données transférées dans le cadre de la sphère de sécurité soient accessibles aux autorités américaines et traitées par celles-ci au-delà de ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale, comme le prévoit l'exception énoncée dans la décision relative à la sphère de sécurité»*[122].

La Commission a ajouté en outre que les entreprises ne mentionnent pas systématiquement, dans leurs dispositions de protection de la vie privée, à quel moment elles dérogent aux principes. Les particuliers et les entreprises n'ont donc pas connaissance de l'usage qui est fait des données les concernant.

La Commission européenne a conclu en déclarant que *«Les lacunes qui affectent la transparence et l'exécution de l'accord contribuent à perpétuer des problèmes spécifiques qui doivent être résolus:*

a) transparence des dispositions de protection de la vie privée adoptées par les adhérents à la sphère de sécurité;

b) mise en œuvre effective des principes relatifs à la protection de la vie privée par les entreprises établies aux États-Unis; et

c) caractère effectif du contrôle de l'application desdits principes.

Par ailleurs, l'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis»[123].

La Commission européenne a formulé treize recommandations, dont les deux suivantes concernent l'accès des données par les autorités des États-Unis:

---

[121] De plus amples explications sur cette disposition sont fournies à l'annexe IV de la décision relative à la sphère de sécurité: «Autorisations légales explicites».

[122] COM(2013) 847 final, communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, 27 novembre 2013, p. 17.

[123] idem, pp. 17-18.

• les politiques de protection de la vie privée adoptées par les entreprises autocertifiées doivent comporter des informations sur la mesure dans laquelle la législation des États-Unis permet aux autorités publiques de collecter et de traiter des données transférées conformément aux principes de la sphère de sécurité. En particulier, les entreprises devraient être encouragées à indiquer, dans leurs politiques de protection de la vie privée, si elles dérogent auxdits principes pour répondre à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois;

• il importe que la dérogation pour raison de sécurité nationale prévue par la décision relative à la sphère de sécurité ne soit utilisée que dans une mesure strictement nécessaire et proportionnée.

Dans une lettre datée du 10 avril 2014[124], le groupe de travail a publiquement soutenu les recommandations de la Commission européenne, y compris celles concernant l'accès des données par les autorités des États-Unis, et a relevé un certain nombre d'éléments supplémentaires pour lesquels des améliorations devraient être apportées dans la décision relative à la sphère de sécurité. Les améliorations que les États-Unis apporteront dans les prochains mois à la sphère de sécurité doivent être suffisantes pour que soit rétablie la confiance. Le groupe de travail reconnaît que, si le processus de révision actuellement entrepris par la Commission européenne ne débouche pas sur un résultat satisfaisant, il conviendrait alors de suspendre l'accord sur la sphère de sécurité. En tout état de cause, le groupe de travail rappelle que les autorités responsables de la protection des données peuvent suspendre les flux de données en vertu de leur compétence nationale et conformément au droit de l'UE. Le groupe de travail attend également l'issue de l'affaire Max Schrems, récemment renvoyée devant la CJUE par la Irish High Court et concernant le rôle des autorités responsables de la protection des données dans le cadre des suspensions prévues dans l'accord sur la sphère de sécurité[125].

5.2.2. Clauses contractuelles types

Les clauses contractuelles types de 2001 et 2004 contiennent une liste de principes en matière de protection des données qu'il convient de respecter lors de tout traitement de données, y compris lors du transfert de celles-ci. Ces principes comprennent notamment le principe de limitation de la finalité, le principe de transparence, le principe de sécurité et de confidentialité, les règles régissant les transferts ultérieurs, ainsi que les droits d'accès, d'effacement et d'opposition.

---

[124] Lettre adressée par le groupe de travail «article 29» à la vice-présidente Reding sur les mesures prises par la Commission européenne pour rétablir la confiance dans les flux de données entre l'UE et les États-Unis.

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf (consulté en dernier lieu le 20 novembre 2014).

[125] Schrems contre le commissaire à la protection des données, affaire C-362/14 [numéro d'enregistrement de la High Court of Ireland: 2013 765JR, (2014) IEHC 351].

Conformément aux clauses contractuelles types de 2010, l'importateur de données non établi dans l'UE traitera les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier. Attendu que l'exportateur de données établi dans l'UE est soumis aux obligations de la directive, ses instructions respecteront nécessairement les principes en matière de protection des données contenus dans la directive. En outre, l'importateur de données non établi dans l'UE n'est pas autorisé au transfert de données à moins que l'exportateur de données établi dans l'UE ne le lui demande.

Les clauses contractuelles types contiennent également des règles applicables en cas de conflit de juridictions. Ainsi, dans les clauses contractuelles types de 2001 et de 2004, l'importateur de données accepte et garantit ce qui suit: «*il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties fournies par les clauses, il communiquera la modification à l'exportateur de données et à l'autorité de supervision dont relève l'exportateur de données, auquel cas l'exportateur de données a le droit de suspendre le transfert de données et/ou de résilier le contrat*».

Les clauses contractuelles types de 2010 stipulent que l'importateur accepte ce qui suit: «*il traitera les données à caractère personnel pour le compte de l'exportateur de données et conformément aux instructions de ce dernier et aux présentes clauses; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat*». En outre, les clauses précisent que l'importateur de données communiquera sans retard à l'exportateur de données «*toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre*». Cependant, cette notification ne s'applique pas lorsqu'elle fait l'objet d'une interdiction, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière.

Comme il a déjà été établi, l'accès massif, non ciblé et secret à des données à caractère personnel est jugé disproportionné par rapport à la finalité ou au but poursuivis. Il s'agit du facteur déterminant dans l'appréciation du caractère licite du traitement. Dans ce contexte, et au vu des récentes révélations sur les programmes de surveillance menés par les États-Unis, il y aurait lieu de penser que la législation américaine empêche l'importateur de s'acquitter de ses obligations au titre du contrat et que l'exportateur est autorisé à suspendre le transfert de données et/ou à résilier le contrat. Il appartient au responsable du traitement d'évaluer le statut ultérieur du transfert. Ce même raisonnement s'appliquerait à toute situation analogue rencontrée dans un autre pays tiers.

Enfin, toutes les séries de clauses contractuelles types contiennent des dérogations sur la base desquelles les clauses seront applicables sous réserve des exigences impératives de la législation nationale de l'État membre de l'UE concernant l'importateur de données, qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique pour l'un des

intérêts énoncés à l'article 13, paragraphe 1, de la directive 95/46/CE[126], c'est-à-dire si elles constituent une mesure nécessaire pour sauvegarder la sûreté de l'État; la défense; la sécurité publique; la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées; un intérêt économique ou financier important d'un État ou la protection de la personne concernée ou des droits et libertés d'autrui[127].

5.2.3 Règles d'entreprise contraignantes

À l'instar des clauses contractuelles types, les règles d'entreprise contraignantes à l'intention des responsables du traitement et des sous-traitants contiennent tous les principes en matière de protection des données qu'il convient de respecter lors du traitement des données, même lorsqu'un transfert est effectué vers un autre membre du groupe[128].

- **Règles d'entreprise contraignantes à l'intention des responsables du traitement**: selon les WP74 et WP153, les règles d'entreprise contraignantes doivent contenir un engagement clair stipulant que, lorsqu'une filiale du groupe a une ou des raisons de penser que la législation qui lui est applicable empêche l'ensemble du groupe de remplir ses obligations en vertu des règles d'entreprise contraignantes et a un impact négatif considérable sur les garanties fournies par les règles, ladite filiale en informera immédiatement le siège européen du groupe ou la filiale européenne responsable par délégation de la protection des données, ou tout autre délégué/instance chargé(e) de la confidentialité des données (à moins que cela ne soit interdit par une autorité chargée d'assurer le respect de la loi, comme par exemple une interdiction prévue par le code pénal pour préserver le secret de l'instruction).

En outre, les règles d'entreprise contraignantes contiennent également un engagement spécifique stipulant que, lorsque la législation nationale du destinataire des données comporte

---

[126] En d'autres termes, si elles constituent une mesure nécessaire pour sauvegarder la sûreté de l'État; la défense; la sécurité publique; la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées; un intérêt économique ou financier important d'un État ou la protection de la personne concernée ou des droits et libertés d'autrui.

[127] Décision de la Commission 2010/87/UE du 5 février 2010, article 4.

[128] Voir le document de travail: Transferts de données à caractère personnel vers des pays tiers: application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données (WP74), adopté par le groupe de travail «article 29» le 3 juin 20013, ci-après le «WP74»; le document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes (WP108), adopté par le groupe de travail «article 29» le 14 avril 2005, ci-après le «WP108»; la recommandation 1/2007 sur la liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes en vue du transfert de données à caractère personnel (WP133), adoptée par le groupe de travail «article 29» le 10 janvier 2007, ci-après le «WP133»; le document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes (WP153), adopté par le groupe de travail «article 29» le 24 juin 2008, ci-après le «WP153»; le document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes (WP154), adopté par le groupe de travail «article 29» le 24 juin 2008, ci-après le «WP154»; le document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes (WP155), adopté par le groupe de travail «article 29» le 24 juin 2008, tel que révisé et adopté le 8 avril 2009, ci-après le «WP155»; la recommandation 1/2012 sur la liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes en vue du transfert de données à caractère personnel à des fins de traitement (WP195) - tous les documents sont disponibles sur le site internet du groupe de travail.

une exigence impérative applicable aux membres du groupe et présentant une différence entre une législation nationale et les engagements au titre des règles d'entreprise contraignantes, le siège européen, la filiale européenne responsable par délégation de la protection des données, ou tout autre délégué/instance chargé(e) de la confidentialité des données, prendra une décision responsable sur l'action à entreprendre et consultera les autorités compétentes en matière de protection des données. En outre, toute incidence découlant de ces exigences doit être détaillée et examinée lors de contrôles réguliers, tel que prévu dans les règles d'entreprise contraignantes.

Règles d'entreprise contraignantes à l'intention des sous-traitants: l'avis WP 195 mentionne que toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre doit être communiquée **sans délai** au responsable du traitement des données, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière. Dans tous les cas, la demande de divulgation sera suspendue et l'autorité de protection des données dont relève le responsable du traitement ainsi que l'autorité chef de file pour les règles d'entreprise contraignantes en seront expressément informées. Toute autorité responsable de la protection des données prendra des mesures conformément à la législation nationale applicable et aux pratiques établies.

En outre, le WP195 prévoit que les différents membres d'un groupe adoptant les règles d'entreprise contraignantes prendront un engagement clair stipulant que, lorsqu'un membre du groupe soumis aux règles d'entreprise contraignantes a des raisons de penser que la législation actuelle ou future qui lui est applicable risque de l'empêcher de se conformer aux instructions reçues du responsable du traitement des données ou de remplir les obligations qui lui incombent aux termes des règles d'entreprise contraignantes ou du contrat de service, les mesures suivantes seront appliquées: il en informe sans délai:

- le responsable du traitement des données autorisé à suspendre le transfert des données et/ou à résilier le contrat;
- le siège européen du sous-traitant ou la filiale européenne responsable par délégation de la protection des données;
- ou tout autre délégué/instance chargé(e) de la confidentialité des données; de même que
- l'autorité de protection des données dont relève le responsable du traitement..

5.3. Conclusion sur les transferts de données

L'accès massif, non ciblé et secret à des données à caractère personnel dont le traitement initial relève de la juridiction de l'UE et transférées de l'UE vers un pays tiers dans lequel elles sont ensuite accessibles aux programmes de surveillance dudit pays tiers n'est pas conforme aux exigences imposées par les dispositions de la directive 95/46/CE relatives au transfert des données. Les transferts structurels (en masse) effectués par des responsables du traitement relevant de la juridiction de l'UE sont soumis à la législation européenne – une obligation

concernant également les transferts ultérieurs vers d'autres parties dans le pays destinataire, lesquels ne peuvent être effectués que si les dispositions de la directive et des divers instruments de transfert disponibles sont respectées. Cependant, aucune de ces conditions ne prévoit le transfert, à des fins de surveillance, de données à caractère personnel détenues par des responsables du traitement du secteur privé vers des autorités du secteur public de pays tiers. De manière plus générale, il n'a jamais été envisagé d'utiliser dans le secteur public ces mêmes instruments, notamment dans l'optique de transférer des informations dans le cadre des activités des services de répression. [129]

En conséquence, les autorités publiques de pays tiers – dont les services de répression et les agences de renseignement – souhaitant accéder aux données stockées dans un État membre de l'UE ou relevant sous une autre forme de la juridiction de l'UE, doivent introduire auprès des autorités nationales compétentes une demande d'entraide judiciaire en empruntant les canaux officiels existants tels que, le cas échéant, les traités d'entraide judiciaire. Ces instruments doivent tenir compte des principes applicables en matière de protection des données.

Dans des cas exceptionnels, des transferts ponctuels peuvent être effectués au titre des dérogations contenues dans la directive relative à la protection des données (article 13 et article 26, paragraphe 1) ou dans la législation nationale du pays tiers, dans le cas de pays considérés comme garantissant un niveau de protection adéquat dans le secteur privé. Les instruments examinés ci-dessus (règles d'entreprise contraignantes, sphère de sécurité, clauses contractuelles types) renferment également des exceptions. Cependant, ces exceptions constituent des restrictions à un droit fondamental et doivent, à ce titre, être interprétées de manière restrictive. Elles ne sauraient justifier des transferts massifs, structurels ou répétés.

En tout état de cause, l'accès de la part d'autorités de pays tiers à des données à caractère personnel transférées à des fins répressives – a fortiori à des fins de surveillance – ne peut avoir qu'une portée limitée. Ces exceptions ne peuvent donc s'appliquer à un nombre illimité de cas ou de personnes, dans la mesure où une telle pratique serait contraire au principe de proportionnalité qui est au cœur de la règlementation de l'UE et qui est consacré à l'article 8 de la CEDH.

Il convient également de rappeler que le groupe de travail ad hoc UE-USA sur la protection des données a confirmé dans son rapport que, bien qu'il existe dans la législation des États-Unis de nombreuses bases juridiques autorisant la collecte massive de données à caractère personnel recueillies et traitées par les entreprises américaines, celles-ci ne respectent pas les critères de nécessité et de proportionnalité établis par la Convention européenne des droits de l'homme. Cela confirme en outre que le caractère général de ces programmes est susceptible

[129] Étant donné que les évaluations de l'adéquation de la protection exigent que soit analysée l'application de l'État de droit dans un pays tiers, il est à tout le moins tenu compte de manière limitée des spécificités du secteur public (bien qu'il ne puisse être affirmé qu'une évaluation complète de l'adéquation puisse être effectuée, de manière réaliste, pour l'ensemble du secteur public d'un pays tiers). C'est en partie la raison pour laquelle une attention moindre a été accordée au secteur public lors de la conception des instruments de transfert.

de donner lieu à des accès et à des traitements qui vont au-delà de ce qui est jugé comme proportionné et strictement nécessaire.

5.4. Exemples

Le chapitre suivant illustrera, sur la base de divers scénarios, un certain nombre de transferts différents susceptibles de se produire, en principe indépendamment du pays tiers vers lequel les données sont transférées.

Il va sans dire que tous les scénarios envisageables ne peuvent être examinés dans le présent document de travail. En outre, le cadre juridique entourant la multitude de scénarios est extrêmement complexe. Afin d'évaluer le caractère licite des demandes d'aide juridique introduites par les autorités de pays tiers, et compte tenu de la nécessité de garantir que le destinataire fournit les garanties appropriées en matière de protection des données, il est particulièrement important de savoir si le responsable du traitement est soumis ou non au droit de l'UE en matière de protection des données[130]. En ce qui concerne l'applicabilité du droit de l'UE en matière de protection des données, ce n'est cependant pas la localisation des données qui importe mais le fait de savoir si le responsable du traitement dispose d'un établissement dans l'UE ou recourt à des moyens dans l'UE, et si les données sont traitées dans le cadre d'activités exercées par cet établissement. En ce qui concerne l'applicabilité du droit des pays tiers autorisant la collecte de données, plusieurs scénarios sont susceptibles d'entraîner des conflits de juridictions (entre le droit de l'UE et le droit du pays tiers en cause), en fonction de la portée de la juridiction dudit pays tiers.

Les réponses à ces questions sont souvent complexes et peuvent encore nécessiter la constatation de nouveaux faits ainsi que des clarifications d'ordre législatif, notamment en ce qui concerne la notion de «transfert». C'est pourquoi le groupe de travail a réduit le niveau de complexité aux fins du présent document.

Exemple 1: transfert direct de données d'une entité privée de l'UE vers une autorité publique hors UE / accès direct d'une autorité publique hors UE à ces données

Le groupe de travail rappelle tout d'abord que le droit public international ainsi que le droit national s'appliquent pleinement à ces scénarios[131]. Les transferts directs de données à caractère personnel d'une entité privée de l'UE vers une autorité publique d'un pays tiers de même que l'accès direct à ces données par une autorité publique d'un pays tiers doivent respecter ces ordres juridiques.

Dans sa lettre du 5 décembre 2013 adressée au comité de la convention de la cybercriminalité du Conseil de l'Europe[132], le groupe de travail avait déjà souligné que la procédure visée à

[130] Voir l'article 4 de la directive 95/46/CE.

[131] Voir en particulier l'article 2, paragraphes 1 et 4, de la Charte des Nations unies.

[132] Réf. Ares(2013)3645289 - 05/12/2013, Lettre du groupe de travail «article 29» à la division de la protection des données et cybercriminalité du Conseil de l'Europe.

l'article 32, point b), de la convention de Budapest sur la cybercriminalité[133] impliquait que l'accès à des données informatiques stockées dans un autre État, de même que la réception de ces données, étaient soumis au consentement légal et volontaire de la personne légalement autorisée à divulguer ces données à la Partie requérante au moyen du système informatique situé sur le territoire de cette dernière**,** en l'occurrence des services de répression ou des autorités judiciaires devant échanger des données pour les besoins d'une affaire spécifique.

Le groupe de travail a également spécifié dans sa lettre que «*des entreprises agissant en qualité de responsables du traitement ne sont généralement pas "légalement autorisées à divulguer les données" qu'elles traitent, par exemple, à des fins commerciales, conformément à l'acquis de l'UE en matière de protection des données*[134]*. Elles ne peuvent normalement divulguer des données que sur présentation préalable d'une autorisation ou mandat judiciaire ou de tout autre document justifiant la nécessité d'accéder aux données et renvoyant à la base juridique applicable à cet accès, présenté par une autorité chargée de l'application du droit national conformément au droit national interne de cette dernière, qui spécifiera la finalité pour laquelle les données sont requises. Les responsables du traitement ne sont pas légalement autorisés à fournir l'accès ou à divulguer des données aux autorités de répression étrangères qui opèrent dans un cadre juridique et procédural différent tant au niveau de la protection des données que de la procédure pénale»*[135].

Le groupe de travail «article 29» souligne en outre que, s'ils devaient se produire, ces scénarios remettraient en question des considérations plus générales en matière de droits fondamentaux, ayant trait notamment aux garanties pénales et procédurales qui sont dues. Ces scénarios pourraient même, dans certains États membres de l'UE, être considérés comme des

---

Objet: Observations du groupe de travail «article 29» sur la question de l'accès direct par les services de répression de pays tiers à des données stockées dans une autre juridiction, comme proposé dans les projets d'éléments d'un protocole supplémentaire à la convention de Budapest sur la cybercriminalité http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

[133] Article 32 – Accès transfrontière à des données informatiques stockées, avec consentement ou lorsqu'elles sont accessibles au public

«Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.»

[134] Voir en particulier les articles 25 et 26 de la directive 95/46/CE concernant les transferts vers des pays tiers.

[135] Voir la lettre susmentionnée, page 3.

infractions pénales. Ainsi, en France et en Allemagne, de telles pratiques seraient de nature à violer le secret des télécommunications consacré dans le droit national de ces pays[136].

[136] Par exemple, le paragraphe 206 du code pénal allemand, ayant trait à la «Violation du secret des postes et des télécommunications», dispose que:
(1) Quiconque dévoile de manière illicite à un tiers des faits qui relèvent du secret des postes ou des télécommunications et dont il est venu à connaissance en sa qualité de propriétaire ou d'employé d'une organisation fournissant des services postaux ou de télécommunications, est passible d'une peine d'emprisonnement n'excédant pas cinq ans ou d'une amende.

(2) Quiconque, en sa qualité de propriétaire ou d'employé d'une organisation telle que définie à la sous-section 1) supra

1. ouvre de manière illicite un envoi postal scellé confié à l'entreprise aux fins de sa livraison ou vient à connaissance de son contenu à l'aide de moyens techniques sans que le cachet ne soit brisé;

2. fait disparaître un envoi postal confié à l'entreprise aux fins de sa livraison; ou

3. autorise ou favorise l'une des infractions visées à la sous-section (1) ou aux numéros 1 ou 2 ci-dessus, encourt une peine identique.

(3) les sous-sections (1) et (2) ci-dessus s'appliquent aux personnes qui

1. exercent des fonctions de supervision sur une organisation telle que mentionnée à la sous-section (1) ci-dessus;

2. sont chargées par une telle organisation ou avec son autorisation de fournir des services postaux ou de télécommunications; ou

3. sont chargées de la mise en place des installations servant aux activités d'une telle organisation ou d'y effectuer des travaux.

(4) Quiconque dévoile de manière illicite à un tiers des faits dont il est venu à connaissance en sa qualité de fonctionnaire public en dehors de la prestation des services postaux ou de télécommunications sur la base d'une violation autorisée ou non autorisée du secret des postes ou des télécommunications est passible d'une peine d'emprisonnement n'excédant pas deux ans ou d'une amende.

(5) Les circonstances immédiates entourant les opérations postales effectuées par des particuliers ainsi que le contenu de la correspondance sont soumis au secret postal. Le contenu de télécommunications de même que les circonstances immédiates entourant ces dernières, notamment le fait qu'une personne ait pris, ou prend part, à une télécommunication, sont soumis au secret des télécommunications. Le secret des télécommunications s'étend également aux circonstances immédiates entourant des tentatives de connexion échouées.

La législation française condamne également la violation de la correspondance émise, transmise ou reçue au moyen des télécommunications à l'**article 226-15 du code pénal** et réglemente la communication de données d'ordre commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères dans la loi n° **68-678 du 26 juillet 1968.**

Pour de plus amples détails, voir en particulier l'article 226-15 du code pénal français qui s'énonce comme suit:

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni

Exemple 2: transfert d'une entité privée de l'UE vers une entité privée hors UE ne relevant pas de la juridiction de l'UE

Dans ce scénario, les demandes émanant d'une autorité publique d'un pays tiers concernent des données provenant de l'UE et stockées dans ce pays tiers. Un transfert de données a dû nécessairement avoir été effectué au préalable par un exportateur de données de l'UE vers un importateur de données hors UE à des fins commerciales.

a) Transferts vers des pays assurant une protection adéquate ou transferts bénéficiant de garanties adéquates

Le transfert initial effectué à des fins commerciales doit s'effectuer conformément à l'article 25 ou à l'article 26, paragraphe 2, de la directive 95/46/CE. Les personnes concernées doivent en outre être informées du transfert et de ses spécificités, telles que la destination (les destinataires) et la finalité, ainsi que de leurs droits, comme prescrit à l'article 10 de la directive. Tous les autres principes relatifs à la protection des données de même que les droits et obligations des personnes concernées doivent également être respectés. Le respect de ces dispositions est exigé indépendamment du fait que l'exportateur de données établi dans l'UE soit une entité entièrement distincte de l'importateur de données hors UE ou l'une de ses filiales.

En outre, tout accès à ces données à caractère personnel par les autorités de pays tiers ainsi que la communication de ces données à caractère personnel auxdites autorités doivent respecter les principes de l'UE en matière de protection des données, les règles régissant les transferts ultérieurs fixées dans la directive 95/46/CE de même que les dispositions des instruments de transfert utilisés comme référence pour l'apport de garanties adéquates (tels que les clauses contractuelles, la sphère de sécurité ou les règles d'entreprise contraignantes).

La portée des dérogations prévues dans les instruments de transfert examinés ci-dessus n'est pas suffisamment étendue pour justifier une surveillance massive, non ciblée et secrète qui irait au-delà du champ d'application des restrictions visées à l'article 13 et à l'article 26, paragraphe 1, de la directive. Au contraire:

a. l'accès doit être limité au strict nécessaire; et

b. la finalité doit être confinée à la sûreté de l'État, à la défense, à la sécurité publique, à la prévention, à la recherche, à la détection et à la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées, à un intérêt économique ou financier important de l'État ou à la protection de la personne concernée ou aux droits et libertés d'autrui; et

---

d'un an d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions. - voir également la loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, telle que modifiée par la loi française n° 80-538 du 16 juillet 1980.

c. conformément au cadre juridique européen et à la jurisprudence de la Cour et de la CJUE, les restrictions doivent être interprétées de manière restrictive et satisfaire aux critères de nécessité et de proportionnalité.

Dernier point mais non des moindres, quand bien même les critères applicables aux dérogations au titre de la sécurité nationale seraient respectés, ces outils de transfert ne se sont pas révélés appropriés dès lors qu'il s'agit de garantir qu'une agence de renseignement ou de sécurité nationale d'un pays tiers offre aux personnes concernées un niveau de protection adéquat.

b) Transferts fondés sur les dérogations visées à l'article 26, paragraphe 1, de la directive

Dans des situations exceptionnelles, les dérogations visées à l'article 26, paragraphe 1, de la directive peuvent justifier le transfert de données d'une entité privée établie dans l'UE vers une entité privée hors UE. Cependant, ces exceptions ne sauraient justifier des transferts massifs, structurels ou répétés ni être à l'origine de violations des droits fondamentaux.

La surveillance massive, non ciblée et secrète de données à caractère personnel ne respecte pas les exigences de protection adéquate tant au regard des principes énoncés dans la directive 95/46/CE qu'au regard des conditions prévues dans l'outil de transfert utilisé. L'évaluation de la conformité du transfert ultérieur avec les principes ci-avant ne saurait être positive lorsqu'il est question de surveillance massive, non ciblée, secrète et structurelle de données à caractère personnel. En fait, de telles activités ne peuvent en aucun cas être considérées conformes à certains des principes régissant la protection des données (finalités incompatibles, accès disproportionné, manque de transparence, impossibilité d'accès pour la personne concernée, impossibilité d'opposition au traitement de la part de la personne concernée et absence de moyens de recours adéquats).

Exemple 3: transfert d'un établissement situé dans l'UE vers un établissement hors UE relevant de la juridiction de l'UE (établissement ou moyens de traitement situés dans l'UE)

Ce scénario suit la même structure de transfert que le scénario précédent si ce n'est que l'entité privée hors UE relève de la juridiction de l'UE, soit parce que l'entité située dans l'UE est un établissement au sens de l'article 4, paragraphe 1, point a), de la directive, soit parce que l'entité privée hors UE recourt à des moyens de traitement situés dans l'UE conformément à l'article 4, paragraphe 1, point c).

En conséquence, l'entité privée hors UE est tenue de se conformer au droit de l'UE et le conflit de juridictions est encore plus flagrant que dans le scénario précédent.

Le même raisonnement juridique peut être suivi dans le scénario présent:

- la portée des dérogations autorisées au titre de l'article 13 de la directive n'est pas suffisamment étendue pour justifier une surveillance à grande échelle, systématique et disproportionnée;

- à ce jour, aucun outil de transfert n'a démontré qu'il pouvait être utilisé pour garantir aux personnes concernées un niveau de protection adéquat de la part des services de sécurité nationale ou des agences de renseignement d'un pays tiers.

6. Observations concernant des pistes envisageables pour la suite

As stated in the introduction, this Working Document is intended as a contribution to a much needed debate on the scope and boundries of the fundamental right to data protection when dealing with surveillance. As is shown in the previous chapters, the Working Party considers several parts of the data protection legislation will continue to apply to data controllers and processors, even when dealing with intelligence services. And rightfully so: the rule of law and the courts require restrictions to fundamental rights to be limited to what is strictly necessary and proportionate, specific and codified in law.

6.1. La réforme de la réglementation en matière de protection des données

Seuls deux acteurs peuvent réellement garantir une sécurité juridique lorsque la protection des données est envisagée dans le contexte de la surveillance et de la sécurité nationale: les tribunaux et le législateur. La réforme de la réglementation en matière de protection des données actuellement en cours au sein de l'UE offre une opportunité unique de pouvoir encadrer les situations auxquelles le mécanisme de protection des données s'applique, y compris dans le cas de transmissions de données vers des services de renseignement et de répression.

6.1.1. Proposition d'un nouvel article 43 *bis*

La commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a introduit un nouvel article 43 *bis* dans la proposition de la Commission relative à un règlement général en matière de protection des données. L'article 43 *bis* se fonde sur l'article 42 du projet de proposition initial de la Commission[137] qui a été retiré de la proposition finale adoptée par le collège des commissaires, laquelle ne conserve que le seul considérant 90 correspondant.

Cet article concerne les transferts ou divulgations non autorisés par le droit de l'Union. Il rappelle que la divulgation de données à caractère personnel à une autorité d'un pays tiers (cour, tribunal, autorité administrative) ne peut avoir lieu qu'après notification de la demande et moyennant l'autorisation préalable de l'autorité de contrôle, sans préjudice d'un traité d'assistance juridique mutuelle ou d'un accord international en vigueur entre le pays tiers demandeur et l'Union ou un État membre.

L'article précise ensuite que l'autorisation accordée par l'autorité de contrôle doit se fonder sur une évaluation de la conformité de la demande avec le règlement général sur la protection des données et que la demande doit être portée à la connaissance de l'autorité nationale

[137] Divulgué sur statewatch.org.

compétente chargée de l'application de la loi. Dans une certaine mesure, les personnes concernées doivent également être informées de la demande de divulgation.

À cet égard, le groupe de travail renvoie à sa déclaration sur le vote du 21 octobre 2013 de la commission LIBE du Parlement européen. Dans les observations concernant l'accès par des autorités publiques et les transferts de données vers des pays tiers, le groupe de travail se félicite en particulier de l'obligation d'informer les personnes lorsque l'accès aux données a été accordé à une autorité publique. Il a également insisté sur la nécessité d'instaurer un cadre de protection stable et solide et salue le recours à des traités d'entraide juridique ou à des accords internationaux en cas de divulgations non autorisées par le droit de l'Union ou des États membres. Enfin, il a déclaré qu'«en cas de demandes d'accès de la part d'autorités publiques d'un pays tiers, l'autorité de contrôle compétente devrait être l'autorité nationale de l'UE saisie de la demande et non l'autorité responsable de la protection des données».

6.2 Questions d'ordre juridique en suspens

Même si certains éléments du nouvel article 43 *bis* proposé constituent un pas dans la bonne direction, cet article ne représente pas le *deus ex machina* apportant une réponse à toutes les autres questions. L'analyse réalisée dans le présent document de travail révèle clairement que certaines questions d'ordre juridique fondamentales demeurent en suspens, telles que la définition des notions essentielles que sont la «sécurité nationale» et les «transferts de données». Un débat difficile devra être instauré afin d'envisager des solutions viables à ces problèmes fondamentaux, tant au niveau européen que mondial, associant l'ensemble des parties prenantes. Le groupe de travail est d'avis qu'à l'ère de la mondialisation, caractérisée par des flux illimités de données entre les pays et vers le nuage informatique, de nouvelles solutions devront voir le jour. Celles-ci devront faire en sorte que nous puissions, en tant que société, continuer à protéger les droits fondamentaux des citoyens tout en garantissant un environnement de vie sûr et sécurisé.