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

819/14/FR
WP 215

Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale

Adopté le 10 avril 2014

Synthèse

Depuis l'été 2013, plusieurs médias internationaux ont consacré de nombreux articles aux activités de surveillance menées par les services de renseignement, tant aux États-Unis que dans l'Union européenne, en se fondant sur des documents transmis essentiellement par Edward Snowden. Ces révélations ont suscité un débat international relatif aux conséquences d'une surveillance à aussi grande échelle pour la vie privée des citoyens. Le traitement réservé par les services de renseignement aux données ayant trait à nos communications quotidiennes de même qu'à leur contenu met en lumière la nécessité de limiter l'envergure de cette surveillance.

Le droit au respect de la vie privée et à la protection des données à caractère personnel est un droit fondamental consacré dans le pacte international relatif aux droits civils et politiques, dans la convention européenne des droits de l'homme (CEDH) et dans la Charte des droits fondamentaux de l'Union européenne. Par conséquent, le respect de l'état de droit suppose nécessairement d'accorder à ce droit le degré de protection le plus élevé possible.

Il ressort de l'analyse réalisée par le groupe de travail que les programmes de surveillance secrets, massifs et non ciblés sont incompatibles avec nos lois fondamentales et ne peuvent être justifiés par la lutte contre le terrorisme ou contre d'autres menaces importantes pour la sécurité nationale. Toute mesure prévoyant de restreindre les droits fondamentaux de l'ensemble des citoyens n'est acceptable que si elle est strictement nécessaire et proportionnée au sein d'une société démocratique.

C'est la raison pour laquelle le groupe de travail recommande plusieurs mesures dans l'optique de garantir et de respecter l'état de droit.

Le groupe de travail appelle tout d'abord à une transparence accrue quant au mode de fonctionnement des programmes de surveillance. La transparence contribue à renforcer et à rétablir la confiance des citoyens vis-à-vis des gouvernements et des entités privées. Il convient notamment de mieux informer les personnes du fait qu'un accès à des données les concernant a été donné à des services de renseignement. Pour que les individus soient mieux informés des conséquences potentielles de l'utilisation de services de communications électroniques en ligne et hors ligne ainsi que des moyens de protection disponibles, le groupe de travail prévoit d'organiser, au second semestre 2014, une conférence sur la surveillance qui réunira toutes les parties prenantes concernées.

En outre, le groupe de travail préconise vivement un contrôle plus strict des activités de surveillance. Une supervision efficace et indépendante des services de renseignement, y compris du traitement des données à caractère personnel, est fondamentale pour garantir que la mise en œuvre de ces programmes ne donnera lieu à aucun abus. Par conséquent, le groupe de travail estime qu'une supervision efficace et indépendante des services de renseignement doit reposer sur une véritable participation des autorités chargées de la protection des données.

Le groupe de travail recommande par ailleurs de veiller à l'application des obligations existantes qui incombent aux États membres de l'Union et aux parties à la CEDH en matière de protection du droit au respect de la vie privée et des données à caractère personnel. Qui

plus est, le groupe de travail rappelle que les responsables du traitement des données soumis à la juridiction de l'Union européenne sont tenus de se conformer à la législation européenne applicable en matière de protection des données. Le groupe de travail rappelle en outre que les autorités chargées de la protection des données peuvent suspendre les flux de données et qu'elles devraient décider en vertu de leur compétence nationale si des sanctions s'imposent dans une situation donnée.

Ni les principes de la sphère de sécurité, ni les clauses contractuelles types, ni les règles d'entreprise contraignantes ne peuvent servir de base juridique pour justifier le transfert de données à caractère personnel vers les autorités d'un pays tiers en vue d'une surveillance massive et non ciblée. En fait, les exceptions incluses dans ces instruments ont une portée limitée et devraient être interprétées de manière restrictive. Elles ne devraient jamais être mises en œuvre au détriment du degré de protection garanti par la réglementation et les instruments européens qui régissent les transferts de données.

Le groupe de travail demande instamment aux institutions européennes d'achever les négociations sur le paquet de réformes relatif à la protection des données. Il se félicite en particulier de la proposition du Parlement européen de créer un nouvel article 43 *bis*, prévoyant d'informer obligatoirement les personnes lorsqu'un accès aux données les concernant a été donné à une autorité publique au cours des douze derniers mois. La confiance sera grandement renforcée par une transparence accrue à l'égard de ces pratiques.

Qui plus est, le groupe de travail estime que la portée de la dérogation au titre de la sécurité nationale devrait être clarifiée, dans un souci de sécurité juridique en ce qui concerne le champ d'application de la législation européenne. À ce jour, le législateur européen n'a pas adopté de définition claire de la notion de sécurité nationale, et la jurisprudence des juridictions européennes ne permet pas non plus de tirer des conclusions à ce sujet.

Enfin, le groupe de travail recommande d'entamer rapidement les négociations sur un accord international visant à accorder aux personnes des garanties adéquates en matière de protection des données dans le cadre des activités de renseignement. Le groupe de travail soutient en outre la mise au point d'un instrument d'envergure mondiale prévoyant des principes de haut niveau ayant force exécutoire en matière de respect de la vie privée et de protection des données.

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES

À l'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu l'article 29, l'article 30, paragraphe 1, point c), et l'article 30, paragraphe 3, de ladite directive,

vu son règlement intérieur, et en particulier ses articles 12 et 14,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

Depuis l'été 2013, plusieurs médias internationaux ont consacré de nombreux articles aux activités de surveillance électronique menées par les services de renseignement, tant aux États-Unis que dans l'Union européenne, ainsi que dans d'autres régions du monde, en se fondant essentiellement sur des documents transmis par Edward Snowden. Ces révélations ont suscité un débat international relatif aux conséquences d'une surveillance électronique à aussi grande échelle pour la vie privée des citoyens. La question de la liberté qu'il convient d'accorder légalement aux services de renseignement, au niveau tant de la collecte que de l'utilisation des informations relatives à notre vie quotidienne, a également été posée. Le présent avis expose les conclusions des analyses juridiques réalisées par les autorités chargées de la protection des données dans l'Union, réunies au sein du groupe de travail «article 29» (ci-après le «groupe de travail»), au sujet des implications des programmes de surveillance électronique pour la protection du droit fondamental à la protection des données et au respect de la vie privée.

Les autorités chargées de la protection des données ont pour mission principale de protéger le droit fondamental de tout individu à la protection des données et de veiller au respect des dispositions législatives pertinentes par les responsables du traitement des données. Cependant, de nombreuses autorités chargées de la protection des données ne disposent que de compétences de supervision limitées, voire nulles, vis-à-vis des services de renseignement. Les États membres ont pris d'autres dispositions pour le contrôle de ces services, y compris pour ce qui est du traitement des données à caractère personnel. Le groupe de travail a dès lors dressé un inventaire des différentes modalités mises en œuvre dans l'Union pour la supervision des services de renseignement, lequel est présenté dans cet avis.

Le présent avis ne traite pas des scénarios relatifs à l'interception de données à caractère personnel transmises par le câble. À ce stade, le groupe de travail ne dispose pas d'informations suffisantes à propos des allégations dans ce domaine pour apprécier le régime juridique applicable, même de manière hypothétique.

2. Métadonnées

Pour évaluer l'ampleur d'éventuelles infractions aux règles de protection des données, il convient tout d'abord de préciser clairement ce dont il s'agit. Les représentants des gouvernements se réfèrent souvent à la collecte de métadonnées, en sous-entendant que ce processus a une portée moindre que la collecte de contenus. Or, ce n'est pas exact. Les métadonnées sont toutes les données relatives à une communication, à l'exception du contenu même de la conversation. Il peut s'agir du numéro de téléphone ou de l'adresse IP de la personne qui passe un appel ou qui envoie un courriel, du moment et de l'endroit, de l'objet, du destinataire, etc. Leur analyse peut révéler des données sensibles à propos des personnes concernées, par exemple parce que certains numéros d'information liés à des centres médicaux ou religieux sont composés. Comme la Cour européenne des droits de l'homme l'a déjà indiqué dans l'affaire Malone [1], le traitement des métadonnées, en l'occurrence le «comptage», comporte des informations qui «font partie intégrante des communications téléphoniques. […] Les révéler à la police sans l'accord de l'abonné porte donc aussi atteinte à un droit consacré par l'article 8». La Cour a maintenu cette position au fil des ans.

Il est également particulièrement important de souligner que les métadonnées donnent fréquemment des informations plus facilement que ne le font les contenus réels de nos communications[2]. Du fait de leur nature structurée, elles sont faciles à regrouper et à analyser. Des outils informatiques sophistiqués permettent d'analyser de grands ensembles de données en vue de déterminer des relations et des caractéristiques intégrées, y compris des informations personnelles, des habitudes et des comportements. Ce n'est pas le cas pour les conversations, qui peuvent avoir lieu sous n'importe quelle forme ou dans n'importe quelle langue.

D'après l'article 2, point a), de la directive 95/46/CE, on entend par «données à caractère personnel» «toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement». Une définition similaire est donnée à l'article 2, point a), de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Par conséquent, en Europe, contrairement à dans d'autres pays, les métadonnées sont considérées comme des données à caractère personnel, qu'il convient de protéger[3].

Dans le récent arrêt rendu dans les affaires de conservation des données, la Cour de justice de l'Union européenne a confirmé que «ces données [relatives aux télécommunications], prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises

[1] Cour européenne des droits de l'homme, Malone c. Royaume-Uni, 2 août 1984.
[2] ACLU c. Clapper, affaire n° 13-3994 (WHP) – déclaration écrite du professeur Edward W. Felten devant le tribunal de district des États-Unis pour le district sud de New York.
[3] Il s'agit d'une interprétation de longue date de la législation sur la protection des données. Dans son avis 4/2007 sur le concept des données à caractère personnel, le groupe de travail déclarait déjà que «pour les cas où, de prime abord, les identifiants sont insuffisants pour permettre à quiconque de distinguer une personne particulière, cette personne peut néanmoins être "identifiable", car ces informations combinées à d'autres éléments d'information (que ces derniers soient conservés par le responsable du traitement ou non) permettent de la distinguer parmi d'autres personnes».

concernant la vie privée des personnes dont les données ont été conservées»[4]. Enfin, la Cour a statué dans cet arrêt 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. […] La circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées […] le sentiment que leur vie privée fait l'objet d'une surveillance constante»[5].

3. Points essentiels

Les révélations d'Edward Snowden ont, pour beaucoup, constitué un rappel brutal à la réalité. L'existence d'un aussi grand nombre de programmes de surveillance différents mis en œuvre par des services de renseignement et capables de collecter des données sur la quasi-totalité de la population n'avait encore jamais été divulguée. Certaines affaires avaient bien été révélées auparavant, mais c'est la première fois que des preuves détaillées attestant du caractère systématique de ces pratiques sont rendues publiques. La manière dont les services de renseignement utilisent les données relatives à nos communications quotidiennes de même que leur contenu met en évidence la nécessité de limiter l'envergure de cette surveillance.

Même ceux qui gèrent avec prudence leur vie en ligne ne peuvent à l'heure actuelle pas se protéger contre les programmes de surveillance massive. Compte tenu des nombreuses difficultés d'ordre juridique, technique et pratique, les autorités chargées de la protection des données dans le monde ne parviennent pas non plus à assurer une protection satisfaisante. Un changement s'impose donc.

Dans les chapitres qui suivent, le groupe de travail «article 29» analyse la collecte massive de données par les services de renseignement à la lumière de leurs programmes de surveillance. D'un point de vue juridique, il convient d'opérer une distinction entre, d'une part, les programmes de surveillance menés par les services de renseignement des États membres et, d'autre part, ceux qui sont appliqués par les services de renseignement de pays tiers qui utilisent les données des citoyens de l'Union européenne.

Les programmes de surveillance menés par les États membres de l'Union ne seront en général pas soumis à la législation de l'Union, en vertu de la dérogation au titre de la sécurité nationale prévue dans les traités européens, de même que dans plusieurs règlements et directives de l'Union, dont la directive 95/46/CE sur la protection des données, conformément à la décision prise en ce sens par les États membres contractants. Cela ne signifie pas pour autant que ces programmes ne soient couverts que par la législation nationale. L'analyse réalisée par le groupe de travail «article 29» révèle que, même si la législation européenne en général et la directive sur la protection des données en particulier ne s'appliquent pas, les

[4] Voir l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, point 27.

[5] Voir l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, points 34, 35 et 37

principes de protection des données[6] découlant de la convention européenne des droits de l'homme et de la convention n° 108 du Conseil de l'Europe sur la protection des données à caractère personnel devront, en grande partie, toujours être respectés par les services de renseignement s'ils souhaitent accomplir leurs missions en toute légalité. Ces principes sont souvent également inscrits dans les constitutions nationales des États membres. Les programmes de surveillance fondés sur la collecte généralisée et non ciblée de données à caractère personnel ne peuvent en aucun cas satisfaire aux exigences de nécessité et de proportionnalité fixées dans ces principes de protection des données. Les limites imposées aux droits fondamentaux doivent être interprétées de manière restrictive, conformément à la jurisprudence de la Cour européenne des droits de l'homme[7] et de la Cour de justice de l'Union européenne[8]. En conséquence, toute ingérence doit être nécessaire et proportionnée par rapport au but à atteindre. En outre, il convient de garder à l'esprit que l'existence et la validité de l'argument de la sécurité nationale invoqué par une autorité nationale ne sont pas automatiquement présupposées. Elles doivent être démontrées.

Le groupe de travail souligne qu'il relève de la responsabilité des gouvernements des États membres de satisfaire à toutes leurs obligations nationales et internationales, y compris à celles qui découlent du pacte international relatif aux droits civils et politiques. Le non-respect de ces exigences porte non seulement atteinte aux droits fondamentaux de leurs citoyens mais amoindrit également la confiance placée par la société dans l'état de droit.

Pour les programmes de surveillance mis en œuvre par des pays tiers, la situation est plus complexe. Lorsque des données sont recueillies, soit directement à partir d'une source au sein de l'Union ou à la suite d'un transfert vers le pays tiers en question (ou, du reste, vers un autre pays tiers), la législation européenne peut toujours être applicable aux informations divulguées dans le cadre des programmes de surveillance. En fait, la dérogation au titre de la sécurité nationale susmentionnée ne s'applique qu'à la sécurité nationale d'un État membre de l'Union, et non à la sécurité nationale d'un pays tiers. Bien entendu, il peut arriver que l'intérêt d'un pays tiers en matière de sécurité nationale coïncide avec celui d'un État membre, et que des opérations de surveillance conjointes soient dès lors justifiées. Là encore, les autorités publiques qui interviennent dans la surveillance doivent être en mesure de démontrer pourquoi et comment les intérêts de sécurité nationale coïncident et excluent dès lors l'application de la législation européenne.

Toutes les conditions relatives aux transferts internationaux de données à caractère personnel prévues dans la directive 95/46/CE doivent être respectées. Cela signifie surtout que le destinataire doit garantir un degré suffisant de protection et que les transferts doivent être conformes à l'objectif initial pour lequel les données ont été collectées. Les transferts doivent

[6] Les grands principes de la protection des données sont les suivants: un traitement juste et licite, la limitation de la finalité, la nécessité et la proportionnalité, l'exactitude, la transparence, le respect des droits des personnes et une sécurité adéquate des données.

[7] Voir les arrêts de la Cour européenne des droits de l'homme du 17 janvier 1970 dans l'affaire Delcourt et du 6 septembre 1978 dans l'affaire Klass.

[8] Voir l'arrêt de la Cour de justice du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, 8 avril 2014, dans lequel la Cour a déclaré que la conservation des données relatives au trafic «sans qu'aucune différenciation, limitation ni exception soient opérées» constitue «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» (points 57 et 65).

aussi impérativement reposer sur la base juridique appropriée pour un traitement juste et licite.

Aucun des instruments disponibles pouvant être utilisés comme autre base pour transférer des données à caractère personnel vers des pays considérés comme n'assurant pas un niveau de protection (principes de la sphère de sécurité, clauses contractuelles types et règles d'entreprise contraignantes) ne permet aux autorités publiques d'un pays tiers, aux fins d'une surveillance non ciblée et massive, d'accéder aux données à caractère personnel transférées sur la base de ces instruments. En fait, les exceptions prévues dans ces instruments ont une portée limitée et doivent être interprétées de manière restrictive (autrement dit, elles doivent être utilisées dans des cas spécifiques et pour des enquêtes spécifiques). Sachant que les instruments visant à assurer un niveau de protection adéquat visent avant tout à protéger les données à caractère personnel émanant de l'Union, ils ne devraient jamais être mis en œuvre au détriment du degré de protection garanti par la réglementation et les instruments européens qui régissent les transferts. Le groupe de travail souligne en outre qu'au titre de la directive sur la protection des données, l'actuelle évaluation du degré de protection des données dans les pays tiers en général ne couvre pas le traitement des données à des fins de répression ou de surveillance.

Les entreprises doivent en outre être conscientes du fait qu'elles peuvent contrevenir à la législation européenne si les services de renseignement de pays tiers parviennent à accéder aux données de citoyens européens stockées sur leurs serveurs ou si elles donnent suite à une injonction de transmettre des données à caractère personnel à grande échelle. À cet égard, les entreprises peuvent se retrouver dans une situation difficile lorsqu'il s'agit de décider de donner suite ou non à l'injonction de transmettre des données à caractère personnel à grande échelle: dans un cas comme dans l'autre, elles risquent d'enfreindre la législation européenne ou d'un pays tiers. Des mesures répressives à l'encontre de ces entreprises ne sont pas à exclure, en particulier lorsque les responsables du traitement ont coopéré de leur plein gré et en connaissance de cause avec les services de renseignement en vue de leur donner accès aux données en leur possession. Les entreprises doivent être aussi transparentes que possible et veiller à ce que les personnes concernées soient conscientes du fait qu'une fois que les données à caractère personnel les concernant sont transférées vers des pays tiers n'assurant pas un niveau de protection adéquat sur la base des instruments disponibles pour ces transferts, les autorités de pays tiers peuvent les soumettre à une surveillance ou se prévaloir de droits d'accès les concernant, pour autant que ces exceptions soient prévues par les instruments mentionnés ci-dessus. Il s'agit toutefois de trouver une solution efficace au niveau politique avant tout. Un accord international prévoyant des garanties pourrait permettre d'assurer le respect des droits fondamentaux par les services de renseignement.

Dans l'optique de garantir que les services de renseignement respectent bel et bien les limites imposées aux programmes de surveillance, des mécanismes de contrôle judicieux doivent être intégrés dans la législation de tous les États membres. Ces mécanismes devraient inclure des contrôles des opérations de traitement des données effectués de manière totalement impartiale par un organisme indépendant, de même que des compétences répressives effectives. Outre un contrôle parlementaire solide et efficace, cette tâche pourrait être confiée à une autorité chargée de la protection des données ou à un autre organisme indépendant approprié, en fonction des modalités de supervision adoptées par l'État membre en question. Si la

supervision devait être prise en charge par un autre organisme, le groupe de travail préconise des contacts réguliers entre ce dernier et l'autorité nationale chargée de la protection des données, en vue de garantir une application cohérente et homogène des principes de protection des données.

Il convient de souligner que les mécanismes de supervision ne doivent pas seulement exister sur papier mais doivent également être appliqués systématiquement. Les révélations de Snowden ont montré que, même si, en théorie, de nombreux contrôles et contrepoids sont prévus, y compris le contrôle de la légalité des mécanismes envisagés en matière de collecte de données, l'efficacité du mode de mise en œuvre des garanties laisse à désirer. Si les garanties en place contre l'accès non justifié aux données ne sont pas applicables à tous les programmes de surveillance ni à toutes les personnes, elles ne répondent pas aux critères d'une supervision satisfaisante d'après le groupe de travail.

4. Supervision des services de renseignement

Si, au cours de l'année dernière, d'autres organismes ont analysé de manière approfondie les modalités de supervision en ce qui concerne les services de sécurité et de renseignement de pays tiers, les analyses portant sur les services de renseignement en place dans chaque État membre de l'Union ont été plus rares. Soucieux de dresser un tableau plus complet des différentes modalités adoptées en Europe pour la supervision des services nationaux de renseignement, le groupe de travail a envoyé un questionnaire à toutes les autorités chargées de la protection des données (y compris à celles de deux pays tiers observateurs non membres de l'UE) afin de mieux cerner leurs pratiques nationales en matière de supervision à cet égard[9].

Deux points en particulier méritent d'être analysés:

1. l'existence d'une supervision globale dans le cadre juridique applicable aux services nationaux de sécurité et de renseignement;

2. le rôle joué (ou non) par l'autorité nationale chargée de la supervision de la protection des données dans ce cadre.

Par le présent avis, le groupe de travail répond également à la demande de Viviane Reding, vice-présidente de la Commission européenne, d'analyser le rôle qui pourrait être celui des autorités chargées de la protection des données[10].

4.1. Aperçu des mécanismes de supervision nationaux applicables

Les activités de surveillance abordées dans le présent avis et dans le document de travail ci-joint sont principalement menées par les services de renseignement dans le cadre de leur mission de protection de la sécurité nationale. Un large éventail de modèles de supervision existe, le modèle retenu dépendant des traditions juridiques nationales et des structures

[9] Les réponses à ce questionnaire ont été fournies par 27 autorités nationales de l'Union chargées de la protection des données, par l'autorité infranationale chargée de la protection des données de Saxe (Allemagne) et par les autorités chargées de la protection des données de Suisse et de Serbie, qui ne sont pas membres de l'Union.
[10] Lettre de la vice-présidente Reding au président du groupe de travail «article 29», 30 août 2013.

consacrées aux modalités nationales en matière de sécurité. Dans 26 des 27 États membres qui ont fourni des informations en réponse au questionnaire[11], des services de renseignement existent et mènent leurs activités sur la base de lois précisant leurs compétences, leur structure et leurs responsabilités. Un seul État membre ne dispose pas de service de renseignement, la mission de sécurité de l'État étant dévolue à une force de police nationale[12].

La plupart des pays interrogés font état de l'existence de une à trois autorités chargées de la sécurité et du renseignement à l'échelon national. En règle générale, les tâches sont réparties selon que les menaces posées à la sécurité nationale sont internes ou externes (étrangères), ce qui entraîne des responsabilités différentes, pouvant être civiles (ministère de l'intérieur ou de la justice) ou militaires (ministère de la défense). Dans trois États, les différentes structures sont intégrées de manière à former un système de protection directement responsable devant le chef du gouvernement (le Premier ministre, par exemple).

Le traitement des données à caractère personnel repose sur une loi promulguée à l'échelon national et la supervision repose soit sur la loi générale en matière de protection des données (ci-après la «LGPD»), soit sur une ou plusieurs lois spécifiques régissant le traitement des données à caractère personnel par un ou plusieurs services de renseignement.

4.2. Le rôle de l'autorité nationale chargée de la supervision de la protection des données

Il ressort clairement de l'évaluation des législations nationales pertinentes que, dans de nombreux pays, la LGPD ne s'applique pas aux activités des services de renseignement et que l'autorité chargée de la protection des données joue un rôle de supervision limité, voire inexistant dans certains cas. La loi prévoit fréquemment un régime spécifique de protection des données, mais sans inclure nécessairement une supervision ciblée par l'autorité chargée de la protection des données.

Dans les deux pays non européens qui ont eu l'amabilité de répondre au questionnaire[13], le traitement des données à caractère personnel par les services de renseignement est régi par la LGPD. Ces services sont soumis à la supervision de l'autorité nationale chargée de la protection des données, en vertu des dispositions de la LGPD.

Lorsqu'elle est applicable, la LGPD prévoit généralement plusieurs exceptions (dérogations à un ou plusieurs principes) pour le traitement des données à caractère personnel par les services de renseignement. Ces exceptions renvoient habituellement aux devoirs fondamentaux des responsables du traitement et aux droits des personnes concernées[14]. Il peut s'agir de la restriction du droit d'être informé et du droit d'accès des personnes concernées, ces droits devant en général être exercés par l'intermédiaire de l'autorité chargée de la protection des données.

[11] Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède.
[12] L'Irlande.
[13] La Serbie (un service civil, deux services militaires) et la Suisse (un service civil, un service militaire).
[14] Par exemple, en Allemagne, en Belgique, en Bulgarie, à Chypre, en Grèce et en Hongrie. Il a été impossible d'établir des informations sur les exceptions pour certains États membres.

Pour ce qui est de la supervision du traitement des données, il semble que les lois nationales générales relatives à la protection des données (ou la loi instituant des organes chargés de la supervision générale de la protection des données) de quatre États membres seulement prévoient en principe, en ce qui concerne les services de renseignement, les mêmes pouvoirs de supervision que pour n'importe quel autre responsable du traitement[15]. Dans treize États membres, la compétence de supervision de l'autorité chargée de la protection des données couvre les services nationaux de sécurité et de renseignement, mais, dans certains cas, des règles ou procédures spécifiques s'appliquent à la supervision des services de renseignement, y compris la possibilité d'imposer des sanctions[16]. Dans neuf États membres, l'autorité chargée de la protection des données n'a aucun pouvoir de supervision sur les services de renseignement agissant en qualité de responsables du traitement[17].

Seules la Suède et la Slovénie ont mis en place une supervision totale, par l'autorité chargée de la protection des données, du respect des obligations applicables en matière de protection des données. Lorsque d'autres autorités nationales chargées de la protection des données ont des pouvoirs sur les services de renseignement, elles vérifient la conformité à la LGPD applicable et traitent les plaintes et l'exercice du droit d'accès par la personne concernée. Elles ont également la compétence d'enquêter sur des affaires, de leur propre initiative ou à la demande d'un tiers, ainsi que de procéder à des inspections sur place. Certains États membres ont fixé des limites à ces pouvoirs, par exemple en imposant le respect de règles spéciales en matière de sécurité dans certaines enquêtes en vue de prendre en considération les exigences relatives au secret d'État.

4.3. Le rôle d'autres mécanismes de supervision indépendants

Vingt États membres ont déclaré que leur législation prévoit une surveillance et/ou un contrôle parlementaire des activités menées par les services de renseignement, en plus des compétences des autorités chargées de la protection des données pour le traitement des données[18], ainsi que des systèmes internes spécifiques en matière de contrôle[19]. Cependant, les États membres semblent avoir des interprétations différentes du terme «contrôle parlementaire». Rares sont celles qui peuvent être considérées comme supposant l'existence d'un véritable organe chargé de superviser la protection des données (y compris l'appréciation des droits de la personne concernée et du respect des dispositions de la LGPD et de la législation spécifique)[20].

Les régimes de supervision existants sont très diversifiés, comme nous pouvons le voir ci-dessous:

[15] La Bulgarie, la Hongrie, la Slovénie et la Suède.
[16] L'Allemagne, l'Autriche, la Belgique, Chypre, l'Estonie, la Finlande, la France, l'Irlande, l'Italie, la Lettonie, le Luxembourg, la Pologne et la Suède.
[17] Le Danemark, l'Espagne, Malte, les Pays-Bas, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni et la Slovaquie.
[18] Par exemple, en Finlande, le médiateur parlementaire est responsable aux côtés de l'autorité chargée de la protection des données, mais ses compétences sont fondées sur la loi spécifique relative aux services de sécurité et de renseignement.
[19] Les vingt États membres visés sont les suivants: l'Allemagne, l'Autriche, la Bulgarie, Chypre, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Italie, la Lettonie, le Luxembourg, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Slovaquie et la Slovénie.
[20] Le présent avis n'analyse pas les informations relatives au contrôle politique de gestion (ministériel) et général fournies par plusieurs États contributeurs.

- une commission parlementaire peut avoir la vaste tâche de superviser les autorités de renseignement et de sécurité en général, ou un service de renseignement en particulier;

- la supervision et/ou le contrôle parlementaire est mis en œuvre parallèlement aux tâches d'autres organes de supervision indépendants (autres que l'autorité chargée de la protection des données). Les modes de contrôle parlementaire existants revêtent la forme d'un médiateur parlementaire, d'une délégation parlementaire ou d'une commission parlementaire;

- une commission parlementaire est la seule autorité de supervision en dehors de la structure du pouvoir exécutif. Les tâches du Parlement sont alors formulées de manière assez générale ou sans prévoir l'accès à des affaires ouvertes;

- la supervision est confiée à une autorité spéciale exclusivement. La compétence peut toutefois être créée par la législation relative à la protection des données mais il a également été signalé dans un cas que cette autorité était jusqu'à récemment régie par des dispositions non contraignantes;

- un contrôle juridictionnel spécialisé est couplé à la supervision parlementaire générale;

- un contrôle exécutif et parlementaire mixte est couplé à l'autorité chargée de la protection générale des données: la commission spéciale est présidée par un juge et réunit des membres provenant de différents partis politiques qui sont ou ont été représentés au Parlement. Des procédures de consultation avec l'autorité chargée de la protection des données sont en place;

- des idées pour améliorer certaines composantes e la supervision peuvent également être tirées des systèmes dans lesquels un organe spécial a été spécifiquement créé pour s'acquitter de la supervision des services de renseignement en matière de protection des données: la commission de supervision des données, composée de trois procureurs, nommés par le procureur général qui supervise les services de renseignement aux côtés du conseil de supervision parlementaire;

- si l'autorité chargée de la protection des données peut être saisie de certaines affaires pour déterminer si la sécurité nationale est en jeu, une fois que cet enjeu est établi, elle doit renvoyer l'affaire devant deux commissaires indépendants, chargés de la supervision judiciaire indépendante des services de renseignement nationaux et du rôle de secrétaire d'État dans l'octroi de mandats pour réaliser des opérations de surveillance secrètes. Ces commissaires sont soutenus par un tribunal spécial qui traite les recours introduits par les personnes concernées;

- la législation spécialisée prévoit une coopération entre l'organe de supervision spécial et l'autorité générale chargée de la protection des données: un commissaire indépendant chargé de la protection juridique doit donner son autorisation si les services de renseignement veulent réaliser certaines opérations (infiltrations ou surveillance vidéo de certaines personnes, par exemple). Le commissaire à la protection juridique est en outre tenu de déposer une plainte auprès de l'autorité chargée de la protection des données s'il estime que des droits au titre de la LGPD ont été enfreints.

L'autorité chargée de la protection des données est compétente pour superviser les services de renseignement sous réserve de certaines limites, mais un organe parlementaire spécial est chargé de la supervision en matière d'interception de communications ainsi que du traitement des plaintes. Les membres de la commission concernée sont nommés par la commission de contrôle parlementaire. Le président doit être habilité à exercer une fonction judiciaire.

5. Recommandations

A. Une transparence accrue

1. Il convient de renforcer la transparence en ce qui concerne le mode de fonctionnement des programmes et les actions et décisions des superviseurs

Le groupe de travail estime qu'il est important que les États membres fassent preuve de la plus grande transparence possible en ce qui concerne leur participation aux programmes de collecte et de partage de renseignements, de préférence en public, mais si nécessaire à tout le moins devant leur parlement national et les autorités de supervision compétentes. Il est recommandé aux autorités chargées de la protection des données de partager leur expertise au niveau national en vue de rétablir l'équilibre entre les intérêts de sécurité nationale et le droit fondamental des citoyens au respect de leur vie privée.

Il convient également de prévoir, sous une forme à déterminer, la présentation de rapports sur les activités de surveillance, notamment conformément à l'obligation de transparence qui incombe aux États membres d'après la Cour européenne des droits de l'homme[21]. Toute ingérence dans les droits fondamentaux devant être prévisible, ces programmes doivent reposer sur une législation claire, spécifique et accessible. Les autorités nationales chargées de la protection des données sont invitées à attirer l'attention de leur gouvernement respectif sur ce point.

[21] Voir également l'arrêt de la Cour européenne des droits de l'homme du 25 juin 2013 dans l'affaire n° 48135/06 – Youth Initiative for Human Rights c. Serbie, p. 6.

2. Une transparence accrue de la part des responsables du traitement

Les entreprises doivent être aussi transparentes que possible et veiller à ce que les personnes concernées soient conscientes du fait qu'une fois que les données à caractère personnel les concernant sont transférées vers des pays tiers n'assurant pas un niveau de protection adéquat sur la base des instruments disponibles pour ces transferts, les autorités de pays tiers peuvent les soumettre à une surveillance ou se prévaloir de droits d'accès les concernant, pour autant que ces exceptions soient prévues par ces instruments. Le groupe de travail sait que les responsables du traitement peuvent recevoir l'ordre de ne pas informer la personne concernée de l'injonction émanant d'une autorité publique. Il salue les efforts déployés récemment en vue de fournir aux personnes concernées des informations plus étoffées et de meilleure qualité au sujet des demandes reçues et encourage les entreprises à continuer d'améliorer les politiques en matière d'information.

3. Accroître la sensibilisation de la population

Les personnes concernées doivent être conscientes des conséquences de l'utilisation de services de communications électroniques en ligne et hors ligne, de même que de la manière dont elles peuvent se protéger. Il s'agit d'une responsabilité partagée par les autorités chargées de la protection des données, par d'autres autorités publiques, par les entreprises et par la société civile. Le groupe de travail prévoit d'organiser à cette fin au second semestre 2014 une conférence réunissant toutes les parties prenantes en vue de discuter d'une approche possible.

B. Une supervision plus stricte

1. Maintenir un système juridique cohérent pour les services de renseignement, y compris des règles sur la protection des données

Les révélations de Snowden ont clairement montré que les services de renseignement des États membres de l'Union européenne traitent quotidiennement de grandes quantités de données à caractère personnel. Ces données sont également partagées avec d'autres services à l'intérieur et à l'extérieur de l'Union. Le groupe de travail estime qu'il est important que les États membres disposent d'un cadre juridique cohérent pour les services de renseignement, y compris des règles sur le traitement des données conformes aux principes de protection des données établis dans le droit européen et international. Les droits de la personne concernée doivent être garantis dans toute la mesure du possible, tout en préservant l'intérêt public en jeu.

Le groupe de travail recommande en outre de veiller à ce que le cadre juridique national comporte des règles claires en matière de coopération et d'échange de données à caractère personnel avec les autorités répressives en vue de prévenir, de combattre et de poursuivre les infractions, y compris au niveau du transfert de ces données aux autorités d'autres États membres de l'Union et de pays tiers.

2. Garantir une supervision efficace des services de renseignement

Dans le cadre juridique national applicable aux services de renseignement, une attention particulière devrait être accordée aux mécanismes de supervision en place. Un contrôle approprié, indépendant et efficace est de la plus haute importance au sein d'une société démocratique. Le groupe de travail estime dès lors que les bonnes pratiques suivantes observées dans les différents mécanismes de supervision actuellement en vigueur dans les États membres devraient être intégrées dans les mécanismes de supervision de tous les États membres. Les autorités nationales chargées de la protection des données sont priées d'aborder les éléments suivants dans le débat national relatif au contrôle des services de renseignement:

- des contrôles internes stricts de la conformité avec le cadre juridique national en vue de garantir la responsabilité et la transparence;

- un contrôle parlementaire efficace conforme aux traditions parlementaires nationales. Les autorités nationales chargées de la protection des données devraient encourager les parlements disposant déjà de pouvoirs de contrôle sur les services de renseignement à effectuer ces tâches de manière active;

- 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, ayant le pouvoir d'accéder aux données et à d'autres documents pertinents de manière régulière et de sa propre initiative (ex officio), de même que l'obligation d'instruire les plaintes y afférentes. Les services de renseignement qui feront l'objet de cette supervision ne doivent pas donner leur approbation préalable.

C. Application effective de la législation actuelle

1. Veiller à l'application des obligations incombant aux États membres de l'Union et aux parties contractantes à la CEDH en matière de droits au respect de la vie privée et à la protection des données

Tous les États membres sont parties à la convention européenne des droits de l'homme. Ils doivent dès lors satisfaire aux conditions établies par les articles 7 et 8 de la CEDH concernant leurs propres programmes de surveillance. Leurs obligations ne s'arrêtent pas là. L'article premier de la CEDH dispose également que les parties doivent reconnaître à toute personne relevant de leur juridiction les droits et libertés définis dans la convention. Dans les deux cas, les États membres de l'Union, à l'instar de toutes les parties à la CEDH, peuvent être traduits devant la Cour européenne des droits de l'homme s'ils enfreignent le droit au respect de la vie privée dont jouit tout sujet de droit européen.

2. Les responsables du traitement relevant de la juridiction de l'Union doivent respecter la législation européenne applicable en matière de protection des données

Les responsables du traitement des données établis dans l'Union ou utilisant les installations d'un État membre doivent respecter les obligations imposées par la législation européenne,

même lorsque la législation d'autres pays dans lesquels ils agissent est en contradiction avec la législation européenne. À cet égard, les autorités chargées de la protection des données ne peuvent ignorer le fait que des transferts de données peuvent être effectués en violation de la législation européenne. Le groupe de travail rappelle par conséquent que les autorités chargées de la protection des données peuvent suspendre, au titre des conditions fixées par les dispositions européennes et nationales en matière de protection des données, les flux de données prévus dans les instruments de transfert lorsqu'il existe une forte probabilité que les principes de protection des données soient violés et que la poursuite des transferts entraînerait un risque imminent de préjudice grave pour la personne concernée. Les autorités nationales chargées de la protection des données devraient décider en fonction de leur compétence nationale s'il convient ou non d'appliquer des sanctions dans une situation donnée.

D. Amélioration de la protection au niveau européen

1. Adoption du paquet de réformes relatif à la protection des données

Dans l'optique d'assurer une solide protection des données en Europe, la conclusion des négociations sur le paquet de réformes relatif à la protection des données revêt la plus haute importance. D'une part, le nouveau règlement général relatif à la protection des données et la directive sur la protection des données policières et judiciaires visent à mieux protéger les données des personnes. D'autre part, ils doivent permettre de clarifier leur champ d'application et de confier davantage de compétences répressives aux autorités chargées de la protection des données. La possibilité d'imposer, en dernier ressort, des sanctions (financières) devrait en particulier leur donner davantage de poids vis-à-vis des responsables du traitement. Le groupe de travail se félicite de la proposition du Parlement européen prévoyant d'informer obligatoirement les personnes lorsqu'un accès aux données les concernant a été donné à une autorité publique au cours des douze derniers mois. La confiance sera grandement renforcée par une transparence accrue à l'égard de ces pratiques. Le groupe de travail invite dès lors le Conseil et le Parlement européen à s'en tenir au calendrier dont ils ont convenu[22] et à faire en sorte que les deux instruments puissent être adoptés au cours de l'année 2014.

2. Clarifier la portée de la dérogation au titre de la sécurité nationale

Il n'existe actuellement pas de définition commune du terme «sécurité nationale». Le législateur européen n'a pas adopté de définition claire, et la jurisprudence des juridictions européennes ne permet pas non plus de tirer des conclusions. La dérogation ne doit toutefois pas être étendue au traitement des données à caractère personnel à des fins pour lesquelles elles ne peuvent pas légalement être utilisées.

Un autre point auquel il convient de répondre est de déterminer dans quelle mesure une dérogation fondée sur la sécurité nationale demeure le reflet de la réalité, maintenant qu'il apparaît que le travail des services de renseignement est plus que jamais interconnecté avec celui des autorités répressives et qu'il poursuit plusieurs objectifs différents. Les données sont partagées en continu et à l'échelle mondiale, en laissant de côté la question de savoir quelle

[22] http://euobserver.com/justice/122853

nation devrait voir sa sécurité renforcée par l'analyse des données en question. Le groupe de travail invite par conséquent le Conseil, la Commission et le Parlement à s'accorder sur une définition du principe de sécurité nationale et à délimiter clairement ce qui devrait être considéré comme relevant du domaine exclusif des États membres. À l'heure de définir le principe de sécurité nationale, il convient de prendre dûment en considération les réflexions du groupe de travail, y compris celles présentées dans cet avis. Les institutions européennes sont également invitées à préciser, dans le paquet de réformes relatif à la protection des données, que la protection de la sécurité nationale des pays tiers ne peut à elle seule exclure l'applicabilité de la législation européenne.

E. Protection internationale des résidents de l'Union

1. Insister sur des garanties adéquates pour le partage des données en matière de renseignement

Les autorités des pays tiers en général, et les services de renseignement en particulier, ne doivent pas avoir un accès direct aux données du secteur privé traitées dans l'Union. Si elles ont besoin d'accéder à ces données dans une situation particulière, sur la base de soupçons raisonnables, elles doivent le cas échéant en introduire la demande au titre d'accords internationaux, en fournissant des garanties adéquates en matière de protection des données. Pour ce qui est du partage des informations en matière de renseignement, les États membres doivent veiller à ce que la législation nationale prévoie une base juridique spécifique pour ces transferts, de même que des garanties adéquates en matière de protection des données à caractère personnel. Selon le groupe de travail, les accords de coopération secrets conclus entre les États membres et/ou des pays tiers ne satisfont pas aux critères de la Cour européenne des droits de l'homme définissant une base juridique claire et accessible.

2. Négocier des accords internationaux en vue d'accorder des garanties adéquates en matière de protection des données

L'idée d'un «accord global», actuellement négocié entre les États-Unis et l'Union européenne, constitue un pas dans la bonne direction. Malgré tout, cet accord présentera probablement deux défauts. D'une part, il exemptera les cas liés à la sécurité nationale, du moins d'une perspective européenne, puisqu'il est négocié à titre d'accord fondé sur la législation européenne uniquement. D'autre part, sa structure suggère qu'il serait uniquement applicable aux données transférées entre les pouvoirs publics des États-Unis et de l'Union, et non aux données collectées par des entités privées. Le même constat peut être fait à partir du rapport du groupe de contact de haut niveau Union européenne – États-Unis (HLCG) sur le partage des informations et la protection de la vie privée et des données à caractère personnel[23], lequel sous-tend les négociations de l'accord global. Le groupe de travail souligne qu'au titre de l'accord global, la finalité du traitement des données transférées devrait être la même dans l'Union et aux États-Unis. Il ne serait pas acceptable que des données émanant des services répressifs de l'Union soient ultérieurement utilisées par les renseignements américains à des fins de sécurité nationale, si cette possibilité n'existe pas dans l'Union également.

[23] Document n° 15851/09 du Conseil, 23 novembre 2009.

Puisque l'accord global n'offrira pas une protection complète à tous les citoyens, il s'agit de conclure un accord international offrant une protection adéquate contre la surveillance non ciblée. Par ailleurs, l'actuel conflit de juridictions qui touche une partie des activités de surveillance divulguées pourrait être atténué si un accord de ce type fixait des limites précises à la surveillance. Cet accord serait toutefois directement lié à la dérogation au titre de la sécurité nationale et tomberait dès lors en dehors du champ d'application de la législation européenne. Il appartient par conséquent aux États membres d'entamer les négociations de manière coordonnée. Il convient de bien distinguer les activités de surveillance qui seraient couvertes par la sécurité nationale de celles qui seraient davantage liées aux finalités de répression et de politique étrangère, domaines relevant de la législation de l'Union. Cette démarche permettrait une participation plus étroite des institutions européennes si des mesures sont prises en ce sens.

Ce nouvel accord ne doit pas être secret. Il doit être rendu public et inclure des obligations pour les parties contractantes quant à la supervision nécessaire des programmes de surveillance, à la transparence, à l'égalité de traitement des citoyens de toutes les parties à l'accord (à tout le moins), aux mécanismes de recours et à d'autres droits liés à la protection des données. Qui plus est, les parties concernées devraient être encouragées à veiller à ce que leurs parlements soient régulièrement informés de l'utilisation et de l'importance de l'accord conclu.

3. Développer un instrument d'envergure mondiale protégeant la vie privée et les données à caractère personnel

Le groupe de travail soutient l'élaboration d'un instrument d'envergure mondiale prévoyant des principes de haut niveau ayant force exécutoire en matière de respect de la vie privée et de protection des données, comme convenu par la Conférence internationale des commissaires à la protection des données et de la vie privée, dans sa déclaration de Madrid[24]. À cet égard, l'adoption d'un protocole additionnel à l'article 17 du pacte international des Nations unies relatif aux droits civils et politiques pourrait être envisagée. Dans un accord international de ce type, il convient de veiller à ce que les garanties proposées soient applicables à toutes les personnes concernées. Il s'agit également de parvenir à une interprétation commune du terme «traitement des données», étant donné qu'il est compris de manières très différentes de par le monde.

Le groupe de travail soutient l'initiative prise par le gouvernement allemand et l'appel lancé par la Conférence internationale des commissaires à la protection des données et de la vie privée[25,26]. Par ailleurs, le groupe de travail continue de soutenir l'adhésion de pays tiers à la convention 108 du Conseil de l'Europe.

[24] Normes internationales sur la protection des données à caractère personnel et de la vie privée, adoptées par la 31e Conférence internationale des commissaires à la protection des données et de la vie privée, organisée à Madrid.
[25] http://www.bundesregierung.de/Content/EN/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html
[26] Résolution sur l'inscription de la protection des données et de la protection de la vie privée dans le droit international, adoptée lors de la 35e Conférence internationale des commissaires à la protection des données et de la vie privée, organisée à Varsovie.