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

3211/15/FR
WP 233

Avis 3/2015 sur la proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

adopté le 1er décembre 2015

Observations générales

Applicabilité de la Charte des droits fondamentaux de l'Union européenne au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales

L'article 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après «la Charte») dispose que les données à caractère personnel «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. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification». L'article 8, paragraphe 3, de la Charte déclare que le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Conformément à l'article 52, paragraphe 1, de la Charte, «[t]oute limitation de l'exercice des droits et libertés reconnus par la Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui». Ainsi que la Cour de justice de l'Union européenne (ci-après «la CJUE») l'a récemment rappelé dans ses arrêts dans l'affaire Schrems et dans l'affaire Digital Rights Ireland et autres[1], les ingérences dans la vie privée des personnes physiques et dans le droit à la protection des données à caractère personnel sont limitées au strict nécessaire et sont proportionnelles aux objectifs d'intérêt général prévus, à savoir la prévention et la détection d'infractions pénales, les enquêtes et poursuites en la matière, ou l'exécution de sanctions pénales[2].

Le groupe de travail «Article 29» rappelle que ces droits et la jurisprudence correspondante de la CJUE s'appliquent au traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales et insiste sur le fait qu'ils sont dûment transposés dans les principes énoncés dans la directive.

À cet égard, le texte actuel du Conseil concernant la proposition de directive soulève des inquiétudes dans la mesure où il ne garantit pas que les ingérences dans la vie privée des personnes physiques et dans le droit à la protection des données à caractère personnel sont limitées au strict nécessaire.
Plus précisément, ainsi que cela sera exposé plus en détail ci-dessous, le groupe de travail «Article 29» observe que les données à caractère personnel traitées à des fins répressives pourraient faire l'objet d'un traitement ultérieur ayant des finalités incompatibles.

De plus, le responsable du traitement n'est pas tenu d'opérer une distinction entre différentes catégories de personnes concernées et les données à caractère personnel des enfants ne sont pas soumises à des mesures de protection particulières. Le texte ne contient pas d'obligation de procéder à une analyse d'impact relative à la protection des données (AIPD) avant de lancer un nouveau traitement; les règles relatives au transfert de données vers des organismes privés et des pays tiers et à leur utilisation ne sont pas définies de façon adéquate et les

[1] Arrêt dans l'affaire Digital Rights Ireland et autres, C-293/12 et C-594/12, point 52.
[2] Arrêt du 6 octobre 2015 dans l'affaire C-362/14, point 92.

données pourraient être utilisées pour créer des profils ou distinguer une personne ou une catégorie de personnes sur le seul fondement de données sensibles. De plus, s'agissant de la sécurité du traitement de données, les risques posés par les violations des données sont laissés à l'appréciation des responsables du traitement et la tenue de journaux connaît des exceptions. Enfin, les pouvoirs des autorités de contrôle compétentes ne sont pas suffisamment détaillés.
Si ces lacunes devaient se retrouver dans le texte définitif de la directive, elles pourraient avoir des conséquences extrêmement préjudiciables pour les personnes physiques et le texte pourrait être incompatible à la fois avec l'article 8 de la convention européenne des droits de l'homme[3], les articles 7 et 8 de la Charte et la convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Le groupe de travail «Article 29» insiste sur le fait que l'établissement de règles qui respectent les principes consacrés par la Charte et, plus généralement, par le cadre applicable à la protection des données sera non seulement bénéfique pour les personnes concernées, mais également pour les responsables du traitement dans leur travail quotidien.

Principes énoncés dans la recommandation n° R(87)15 en tant que minimum requis pour l'établissement d'un cadre juridique équivalent au niveau de l'UE.

Au niveau européen, la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales est déjà abordée dans plusieurs documents spécifiques: la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 (ci-après la «décision-cadre 2008/977/JAI») au niveau de l'UE et la recommandation n° R(87)15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[4] au niveau du Conseil de l'Europe (ci-après la «recommandation n° R(87)15»)[5].
Les principes de la protection des données énoncés dans la décision-cadre 2008/977/JAI ne concernent que la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale, tandis que la recommandation n° R(87)15 présente un ensemble de règles spécifique et plus complet.

Le groupe de travail «Article 29» recommande donc que la recommandation n° R(87)15 soit considérée comme le minimum requis pour l'établissement d'un cadre juridique équivalent au niveau de l'UE.

Risques inhérents aux activités des autorités répressives et mesures de sauvegarde nécessaires en découlant

Le groupe de travail «Article 29» s'est servi de son expérience et de la jurisprudence pertinente de la CJUE et de la CEDH[6] pour élaborer son avis selon lequel un traitement de

[3] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4 novembre 1950.
[4] Recommandation n° R(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police adoptée par le Comité des ministres du Conseil de l'Europe le 17 septembre 1987, lors de la 410e réunion des délégués des ministres.
[5] La recommandation n° R(87)15 a servi de point de référence pour déterminer le niveau de protection des données dans les textes réglementant le système d'information Schengen et EUROPOL.
[6] Voir, notamment, l'arrêt de la CJUE sur la directive relative à la conservation des données dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e. a.
Voir aussi la CEDH: La collecte, la mémorisation, l'utilisation et la divulgation d'informations personnelles par l'État, par exemple dans un registre de police, portent atteinte au droit au respect de la vie privée, garanti par l'article 8, paragraphe 1, de la convention (Leander c. Suède, 26 mars 1987, point 48, série A n° 116). L'utilisation ultérieure des informations mémorisées importe peu (Amann c. Suisse [GC], n° 27798/95, point 69,

données à caractère personnel qui, dans un contexte général ou ordinaire, peut ne pas être perçu comme une menace pour les droits fondamentaux, peut néanmoins requérir une attention particulière lorsqu'il est effectué dans un contexte répressif ou judiciaire, dans la mesure où les risques pour les droits fondamentaux augmentent. Loin de justifier des exigences moins strictes ou de déroger à l'obligation générale, un traitement impliquant une limitation des droits fondamentaux des personnes concernées, telle que visée à l'article 52, paragraphe 1, de la Charte[7], doit donc être effectué dans le plein respect des principes fondamentaux de la protection des données. Le recours à des dérogations ou à des limitations doit être exceptionnel et interprété de manière étroite, en particulier lorsqu'elles concernent le plein exercice des droits des personnes. Les données à caractère personnel doivent être traitées avec des garanties et des sauvegardes suffisantes prévoyant une responsabilité et une transparence complètes à l'égard des personnes physiques[8].

Cohérence entre les deux textes

Le groupe de travail «Article 29» insiste sur l'importance de considérer à la fois le projet de règlement et la proposition de directive comme faisant partie d'un paquet afin de garantir la nécessaire cohérence entre les deux textes.

À titre d'exemple, un degré moindre d'obligations imposées au responsable du traitement concernant les analyses d'impact relatives à la protection des données, les violations des données et les droits des personnes concernées dans la proposition de directive pourrait poser

---

CEDH 2000-II). Pareille ingérence méconnaît l'article 8 sauf si, «prévue par la loi», elle poursuit un ou des buts légitimes au regard du paragraphe 2 et, de surcroît, est «nécessaire dans une société démocratique» pour atteindre ces derniers.
Dans l'affaire **M.K. c. France** (requête n° 19522/09) du 18 avril 2013, la Cour européenne des droits de l'homme a conclu, à l'unanimité, que la conservation des empreintes digitales d'un ressortissant français ayant fait l'objet de deux enquêtes pour vol de livres, qui se sont terminées l'une par un acquittement et l'autre par une décision de classement sans suite, **viole l'article 8** (droit au respect de la vie privée et familiale) de la convention européenne des droits de l'homme. Eu égard aux circonstances de l'espèce, la Cour a considéré que les données en cause constituaient une ingérence disproportionnée dans le droit du requérant au respect de sa vie privée.
Dans l'affaire **S. et Marper c. Royaume-Uni** (requêtes n^{os} 30562/04 et 30566/04) du 4 décembre 2008, la Cour a conclu 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 traduisait 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'analysait en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne pouvait passer pour nécessaire dans une société démocratique. La Cour a conclu, à l'unanimité, à une violation de l'article 8.
Plus récemment, dans l'affaire **M.M. c. Royaume-Uni** (24029/07) du 13 novembre 2012, la Cour n'était pas convaincue que le système de conservation et de divulgation des données relatives aux antécédents judiciaires présentât des garanties suffisantes permettant d'éviter que les données relatives à la vie privée de la requérante fussent divulguées, en violation de ses droits au respect de sa vie privée. Dès lors, on ne saurait considérer que la conservation et la divulgation des données relatives à l'avertissement infligé à la requérante étaient prévues par la loi.
Voir aussi B.B. c. France (requête n° 5335/06), Gardel c. France (requête n° 16428/05), M.B. c. France (n° 22115/06), où la CEDH a conclu que l'inclusion dans le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ne portait pas atteinte au droit au respect de la vie privée et qu'il n'y avait pas violation de l'article 8 (droit au respect de la vie privée et familiale) de la convention européenne des droits de l'homme.

[7] L'article 52, paragraphe 1, de la Charte des droits fondamentaux dispose que: «Toute limitation de l'exercice des droits et libertés reconnus par la Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés». Voir plus haut l'analyse relative à la Charte.

[8] Voir l'arrêt de la CJUE sur la directive relative à la conservation des données: «S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire».

problème aux responsables du traitement qui traitent des données relevant du champ d'application du règlement et de la directive[9].

Le groupe de travail «Article 29» rappelle donc sa recommandation visant à s'assurer que «les aspects "essentiels" des deux textes sont cohérents et compris de manière uniforme, quel que soit l'instrument juridique choisi, afin d'éviter toute confusion et tout chevauchement ayant une incidence sur le niveau de protection garanti aux particuliers» [10]. Les définitions, les principes, les obligations, les droits des particuliers et les pouvoirs de l'autorité de contrôle doivent être cohérents et les exceptions prévues dans la proposition de directive doivent être limitées au strict nécessaire.
Cette cohérence est d'autant plus importante lorsque l'on considère le nombre croissant de cas où les activités du secteur privé et des services répressifs interagissent les unes avec les autres[11].

Observations spécifiques

1/ Objet et objectifs

Ainsi qu'il l'a déjà fait valoir dans son avis[12] sur les points fondamentaux du règlement, afin d'assurer la cohérence et un niveau élevé de protection, le groupe de travail «Article 29» estime que les traitements effectués par les autorités compétentes à des fins qui ne sont pas liées à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales, devraient clairement continuer de relever du champ d'application du règlement.

À cet égard, le groupe de travail «Article 29» rappelle qu'une extension du champ d'application de la directive, telle qu'elle est proposée par le Conseil de l'UE, à tous les traitements destinés à «préserver la sécurité publique et à prévenir les menaces à son encontre» - outre les traitements effectués à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions

[9] Les transferts de données PNR et de données sur les transactions financières aux autorités répressives en sont des exemples. À l'annexe III de l'analyse d'impact des deux instruments proposés, la décision-cadre 2008/977/JAI est fortement critiquée au motif qu'elle ne lève pas l'insécurité juridique dans les cas où des données collectées à des fins commerciales sont utilisées à des fins répressives.
Cela vaut également dans d'autres cas, par exemple lorsque l'information est transférée entre une autorité répressive et une entité privée ou lorsqu'une autorité répressive transfère les données à une autre autorité publique qui n'est pas chargée de l'application de la loi.

[10] Avis du groupe de travail «Article 29» sur les points fondamentaux dans la perspective du trilogue, 17 juin 2015, voir notamment le haut de la page 3 (disponible sur: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_fr.pdf).

[11] Les transferts de données PNR et de données sur les transactions financières aux autorités répressives en sont des exemples. À l'annexe III de l'analyse d'impact des deux instruments proposés, la décision-cadre 2008/977/JAI est fortement critiquée au motif qu'elle ne lève pas l'insécurité juridique dans les cas où des données collectées à des fins commerciales sont utilisées à des fins répressives.
Cela vaut également dans d'autres cas, par exemple lorsque l'information est transférée entre une autorité répressive et une entité privée ou lorsqu'une autorité répressive transfère les données à une autre autorité publique qui n'est pas chargée de l'application de la loi.[12] Avis du groupe de travail «Article 29» sur les points fondamentaux dans la perspective du trilogue, 17 juin 2015 (disponible sur: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_fr.pdf).

[12] Avis du groupe de travail «Article 29» sur les points fondamentaux dans la perspective du trilogue, 17 juin 2015 (disponible sur: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_fr.pdf).

pénales - aboutirait à un niveau de protection différent, en fonction de sa mise en œuvre par les États membres[13].

En outre, la notion de «prévention des menaces à la sécurité publique» qui n'est pas liée au concept d'infractions pénales est assez vague et peut inclure certains types de traitement simplement parce qu'ils sont effectués par des responsables du traitement agissant dans le contexte plus large de l'application de la loi, voire de la sécurité publique. Le groupe de travail «Article 29» rappelle, par exemple, que dans certains États membres, la santé publique relève de la sécurité publique dans son acception administrative.

De plus, une telle extension inclurait dans le champ d'application de la directive un nombre indéfini d'autorités dont la mission peut n'être qu'occasionnellement liée à cette finalité, ce qui aboutirait à un niveau de protection des données dans le secteur public inférieur à celui proposé par le règlement. Aucune raison impérieuse n'oblige à introduire une telle flexibilité et à exclure l'activité de sécurité publique du règlement.

Le groupe de travail «Article 29» soutient donc les versions de l'article premier proposées par la Commission et le Parlement européen, qui limitent l'objet et les objectifs au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

2/ Loyauté du traitement

La loyauté du traitement est un principe standard garanti dans la plupart des textes traitant de la protection des données. Dans le contexte particulier et très sensible où des États membres font usage de leur pouvoir coercitif, il est encore plus important que la loyauté du traitement ne suscite aucun doute.

Le groupe de travail «Article 29» se réjouit donc que le texte de la proposition de directive fasse de la loyauté du traitement un principe préalable et essentiel et le groupe de travail est favorable à ce texte.

Dans le cadre de cette exigence de loyauté et en vue de se conformer au principe 2.3[14] de la recommandation n° R(87)15 du Conseil de l'Europe, le groupe de travail «Article 29» recommande que des dispositions juridiques spécifiques déterminent les pouvoirs de collecter des données par le biais de moyens techniques de surveillance ou d'autres moyens automatisés afin d'assurer la loyauté du traitement effectué dans ce contexte.

3/ Limitation de la finalité

Le groupe de travail «Article 29» observe que la limitation de la finalité est un principe essentiel de la protection des données, dont le but est de fixer les limites à l'intérieur desquelles des données à caractère personnel collectées pour une finalité particulière peuvent être traitées et faire l'objet d'une utilisation ultérieure différente. Le responsable du traitement ne doit collecter des données qu'à des fins légitimes, explicites et spécifiques et, une fois les

[13] Le groupe de travail «Article 29» a déjà exprimé cette position dans sa lettre relative aux points fondamentaux dans la perspective du trilogue, publiée le 17 juin 2015 (voir http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf).

[14] Recommandation n° R(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, principe 2 «Collecte des données»: La collecte de données par le biais de moyens techniques de surveillance ou d'autres moyens automatisés devrait être prévue dans des dispositions spécifiques.

données collectées, elles ne doivent pas faire l'objet d'un traitement ultérieur incompatible avec ces finalités. Le principe 4 de la recommandation n° R(87)15 susvisée a formulé cela comme suit: «[...] les données à caractère personnel collectées et enregistrées par la police à des fins de police devraient servir exclusivement à de telles fins».

De ce fait, les données collectées pour un crime spécifique peuvent également être utilisées par les autorités compétentes pour résoudre un autre crime, pour autant que la compatibilité soit évaluée au cas par cas et sous réserve d'une base juridique prévoyant des mesures de protection claires et explicites.

Le groupe de travail «Article 29» insiste néanmoins sur le fait que la répression proprement dite ne doit pas être considérée comme une finalité légitime, explicite et spécifique.

En outre, la limitation de la finalité et la distinction entre différentes catégories de données à caractère personnel[15] sont fondamentalement liées. Des données spécifiques ou des données sur des catégories spécifiques de personnes concernées peuvent être nécessaires dans certaines enquêtes criminelles. Cependant, leur utilisation ultérieure devrait être limitée et soumise à des conditions strictes, notamment lorsque le lien entre une personne et un crime n'est pas établi (la collecte de données sur cette personne est liée à un crime, mais la personne n'est ni un suspect, ni une victime, ni un témoin). Plus précisément, contrairement aux données relatives aux suspects ou aux personnes condamnées, l'utilisation ultérieure de données relatives à des «personnes non suspectes» devrait être prohibée.

Cette limitation devrait également s'appliquer au traitement de données sensibles. Bien que leur nécessité ait été établie pour l'infraction pour laquelle elles ont été collectées, leur nécessité en vue d'une utilisation ultérieure devrait être démontrée.

Le groupe de travail insiste sur le fait que tout traitement pour une finalité différente de la finalité spécifique pour laquelle les données ont été traitées au départ devrait toujours avoir sa propre base juridique, incluant des mesures de protection claires et spécifiques.

4/ Réduction au minimum des données

Le groupe de travail «Article 29» rappelle que seule une quantité minimale de données à caractère personnel devrait être traitée pour atteindre la finalité fixée; elles ne sont traitées que si, et pour autant que, les finalités du traitement ne peuvent pas être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel. Le groupe de travail renvoie à la recommandation n° R(87)15, qui précise, en son principe 2.1, que la collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Le groupe de travail insiste sur le fait que les principes de nécessité et de proportionnalité doivent être pris en compte lors du traitement de données à caractère personnel à des fins répressives et que ce traitement ne doit pas conduire à la collecte massive et indiscriminée et au traitement ultérieur de données à caractère personnel, même si les nouvelles technologies le permettent.

À cet égard, le groupe de travail «Article 29» est favorable à la version de l'article 4, point c), proposée par le Parlement européen, qui mentionne, parmi les principes se rapportant au traitement de données à caractère personnel, que les données traitées devraient être adéquates, pertinentes et «*limitées au minimum nécessaire pour les finalités pour lesquelles elles sont*

[15] Voir l'analyse de la distinction entre les différentes catégories de personnes concernées.

traités» et qu'«*elles ne sont traitées que si, et pour autant que, les finalités ne peuvent pas être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel*».

5/ Distinction entre les différentes catégories de personnes concernées.

Le groupe de travail «Article 29» est favorable à une disposition substantielle de la directive qui distingue différentes catégories de personnes concernées (suspect, auteur, victimes, témoins, informateurs, contacts et complices). Comme il l'a déjà souligné dans son avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive [16], une telle distinction est également indispensable pour garantir la bonne application des principes relatifs au traitement des données. Il insiste également sur l'importance capitale d'actualiser ces données à la fin de l'enquête ou de la procédure judiciaire. Les politiques et législations de l'UE qui visent à lutter contre la traite des êtres humains et suivent une approche centrée sur la victime font obligation aux responsables du traitement d'établir une distinction adéquate. En l'absence d'une obligation d'introduire de telles distinctions, l'efficacité de ces politiques sera limitée ou inexistante.

Dans son avis 01/2013 susvisé[17], le groupe de travail «Article 29» insistait notamment sur la catégorie de personnes n'ayant pas de lien connu avec une infraction pénale, à savoir les personnes dites «non suspectes». Le traitement des données de personnes qui ne sont pas suspectées d'avoir commis une infraction pénale (autres que les victimes, témoins, informateurs, contacts et complices) doit être strictement distingué de celui des données de personnes en lien avec une infraction pénale spécifique et il «ne devrait être autorisé que dans certaines conditions spécifiques et pour autant qu'il soit absolument nécessaire à une finalité **légitime, clairement définie et particulière**». Par ailleurs, ce traitement devrait (de l'avis des autorités de protection des données) «être limité à une période déterminée et l'utilisation ultérieure de ces données à d'autres fins devrait être interdite». Une protection spécifique des «personnes non suspectes» est tout particulièrement requise lorsque le traitement n'est pas effectué dans le cadre d'une enquête criminelle ou d'une procédure pénale spécifique.

Le groupe de travail a déjà suggéré d'introduire un article sur ce point[18] et est donc favorable à l'article 5 proposé dans la version du Parlement européen, qui oblige les responsables du traitement à établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées (suspect, auteur, victimes, témoins, informateurs, contacts et complices). Cela garantirait que les données introduites dans les fichiers de la police sont exactes et régulièrement mises à jour en ce qui concerne la catégorie de personnes concernées et soumettrait le traitement des données de ces différentes catégories à des conditions spécifiques.

6/ Catégories spéciales de données

[16] Avis 01/2013, 00379/13/FR, WP201 de février 2013, apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_fr.pdf

[17] Avis 01/2013, 00379/13/FR, WP201 de février 2013, apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_fr.pdf

[18] Voir avis 01/2013 précité, 00379/13/FR, WP201 de février 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_fr.pdf

Le groupe de travail considère que le traitement de données sensibles devrait être en principe interdit et que des exceptions devraient être accordées sous réserve de conditions strictes. À cet égard, le groupe de travail rappelle le principe 2.4 de la recommandation R(87)15, en vertu duquel «la collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée. La collecte de données concernant ces facteurs ne peut être effectuée que si elle est absolument nécessaire pour les besoins d'une enquête déterminée».
Le traitement de catégories spéciales de données pourrait donc être autorisé lorsque:

- (a) le traitement est autorisé par une loi offrant des garanties adéquates ***strictement nécessaires et proportionnelles à l'exécution d'une tâche par les autorités compétentes aux fins énoncées à l'article premier, paragraphe 1, conformément au droit de l'Union ou de l'État membre, qui prévoira des mesures spécifiques et adéquates pour préserver les intérêts légitimes de la personne concernée, notamment une autorisation spécifique d'une autorité judiciaire, si le droit national l'exige****;* ou

- (b) le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne; ou

- (c) le traitement concerne des données qui ont manifestement été divulguées par la personne concernée, ***pour autant qu'elles soient pertinentes et strictement nécessaires à la finalité poursuivie dans le cas spécifique.***

Le groupe de travail considère que le traitement de données sensibles devrait être en principe interdit et que des exceptions devraient être accordées sous réserve de conditions strictes. Le groupe de travail «Article 29» est donc favorable à l'article 8 tel que présenté dans la version du Parlement européen.

Données génétiques et biométriques

Le groupe de travail «Article 29» se félicite que les données génétiques soient définies à l'article 3 et considérées comme une catégorie spéciale de données. Il souligne que la création de profils génétiques généraux en dehors du cadre d'une enquête spécifique devrait être strictement interdite.
Étant donné que les données biométriques peuvent identifier une personne de manière automatique et unique en utilisant une ou plusieurs de ses caractéristiques physiques, physiologiques ou comportementales, elles sont différentes des autres données à caractère personnel et devraient bénéficier de davantage de précautions [19] dans la mesure où elles

[19] Dans l'affaire S. et Marper c. Royaume-Uni (requêtes n[os] 30562/04 et 30566/04), la Cour a donné son avis sur le traitement de données génétiques et biométriques. Elle a d'abord noté que, vu la nature et la quantité des informations personnelles contenues dans les échantillons cellulaires, leur conservation doit passer pour constituer en soi une atteinte au droit au respect de la vie privée des individus concernés. Selon la Cour, le fait que les profils ADN fournissent un moyen de découvrir les relations génétiques pouvant exister entre des individus suffit en soi pour conclure que leur conservation constitue une atteinte au droit à la vie privée de ces individus. La possibilité qu'offrent les profils ADN de tirer des déductions quant à l'origine ethnique rend leur conservation d'autant plus sensible et susceptible de porter atteinte au droit à la vie privée. La Cour a également estimé que les empreintes digitales contiennent des informations uniques sur l'individu concerné et que leur conservation, avec ou sans le consentement de celui-ci, ne saurait passer pour une mesure neutre ou banale. La conservation des empreintes digitales peut en soi donner lieu à des préoccupations importantes concernant le respect de la vie privé et constituer une atteinte au droit au respect de la vie privée.

permettent une identification sur la base d'une réalité biologique qui ne peut être modifiée, effacée ou annulée. En outre, un traitement de données biométriques entraîne souvent des problèmes de collecte (cas où les empreintes digitales ne sont pas lisibles, par exemple) et de qualité aboutissant à de faux positifs (contrôle automatisé des frontières, par exemple).

Le traitement de données biométriques requiert donc des exigences plus strictes en matière de protection des données, notamment en ce qui concerne la qualité, l'exactitude et la sécurité des données.

Le groupe de travail souligne que, à l'instar d'autres données «sensibles» (comme les données génétiques), les données biométriques devraient être définies à l'article 3 et couvertes par l'article 8.

7/ Traitement des données relatives aux enfants

Le traitement de données à caractère personnel à des fins répressives pourrait poser des risques supplémentaires pour les enfants, un groupe particulièrement vulnérable. Leur intérêt supérieur devrait être la préoccupation première des États membres lorsqu'ils appliquent cette directive, conformément à l'article 24, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne[20]. Le groupe de travail «Article 29» estime que le traitement de données relatives à des enfants impose l'adoption de mesures de protection renforcées, y compris des délais de conservation plus stricts et des évaluations régulières de l'efficacité d'un tel traitement. La possibilité de garantir le rétablissement éducatif et moral des auteurs mineurs d'infractions pénales en leur offrant, dans certains cas, la possibilité de demander l'effacement ou de bloquer l'utilisation de ces données devrait exister. Les États membres devraient disposer d'une certaine flexibilité afin que ces mesures de protection soient conformes à la législation nationale tout en garantissant le degré de protection le plus élevé. Le groupe de travail «Article 29» recommande donc l'introduction de dispositions spécifiques en la matière.

Le groupe de travail «Article 29» est favorable à un texte introduisant des garanties supplémentaires lors du traitement de données à caractère personnel relatives à des enfants, par exemple: «Les mesures prises par le responsable du traitement incluent, notamment l'élaboration et la mise en œuvre de garanties spécifiques concernant le traitement de données à caractère personnel relatives à des enfants, le cas échéant.» [21] Cette attention particulière accordée aux données à caractère personnel des enfants doit également être une préoccupation majeure lors de l'analyse d'impact relative à la protection des données.

8/ Profilage

Au minimum, aucun profilage ne sera réalisé et aucune décision automatisée ne sera prise sur la seule base de données sensibles. À ce propos, le groupe de travail «Article 29» regrette que cette garantie ait été omise dans le texte approuvé par le Conseil.

La personne concernée devrait toujours avoir le droit de contester une décision automatisée et de faire valoir son point de vue.

[20] L'article 24, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne sur les droits de l'enfant se lit comme suit: «Dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale». [21] Voir l'article 18, point da), de la version du texte proposée par le Parlement européen.

[21] Voir l'article 18, point da), de la version du texte proposée par le Parlement européen.

Le groupe de travail «Article 29» est favorable à l'article 9, paragraphe 2, proposé dans les versions de la Commission et du Parlement européen, qui interdit le profilage reposant uniquement sur des données sensibles.

9/ Droits de la personne concernée

Le groupe de travail «Article 29» recommande que les droits des particuliers soient, par principe, clairement définis et énoncés dans des articles et que les limitations imposées à ces droits soient justifiées au cas par cas, en fonction de la sensibilité des données traitées ou des conséquences potentielles de l'exercice de ces droits sur une enquête ou une procédure en cours. Le législateur et/ou l'autorité de contrôle, lorsqu'il est chargé de la notification préalable, devrait avoir l'occasion de déterminer si cette limitation est justifiée et s'il serait pertinent de prévoir un droit d'accès indirect. En tout état de cause, l'autorité de contrôle devrait avoir l'occasion de contrôler a posteriori les modalités de l'exercice de ces droits, qu'ils soient directs ou indirects.

Informations à la personne concernée

Afin de permettre à la personne concernée de contester la légalité du traitement de données à caractère personnel la concernant et sans préjudice des exceptions légitimes, le groupe de travail «Article 29» soutient fermement le droit de la personne concernée d'être informée par principe, en particulier lorsque les données sont collectées à son insu. Ce principe ne devrait faire l'objet d'une dérogation que lorsque les informations mettraient en danger une enquête en cours, exposeraient une personne à un danger ou porteraient atteinte aux droits et libertés d'autrui. Ce droit est particulièrement important pour les témoins et les personnes non suspectes.

Dans ces cas, les informations devraient être communiquées à la personne concernée en tant que norme harmonisée et comprendre à tout le moins les éléments couverts par la proposition de la Commission[22].

Droit d'accès de la personne concernée et limitations du droit d'accès: établissement d'un droit d'accès indirect

Lorsqu'un accès direct mettrait en danger une enquête en cours, exposerait une personne à un danger ou porterait atteinte aux droits et libertés d'autrui, les États membres devraient avoir la possibilité de fournir un accès indirect.

Le droit d'accès devrait inclure, en tant que partie intégrante des informations minimales à fournir, sous réserve d'exceptions dûment justifiées, le droit de la personne concernée d'obtenir auprès du responsable du traitement une copie des données à caractère personnel faisant l'objet d'un traitement ainsi que des informations intelligibles sur la logique suivie par le traitement automatisé, à tout le moins dans le cas des mesures liées à l'article 9 sur les décisions automatisées individuelles.

[22] L'identité et les coordonnées du responsable du traitement et du délégué à la protection des données, le cas échéant; les finalités du traitement auquel les données à caractère personnel sont destinées; la durée pendant laquelle les données sont conservées; l'existence du droit de demander au responsable du traitement l'accès aux données, leur rectification, leur effacement ou la limitation de leur traitement; le droit d'introduire une réclamation auprès de l'autorité de contrôle et les destinataires ou les catégories de destinataires des données à caractère personnel.

Le groupe de travail «Article 29» est favorable à l'article 12 proposé dans la version du Parlement européen, qui détaille les informations à fournir en cas de demande d'accès et à l'article 13 de la même version, dans la mesure où il garantit que les limitations du droit d'accès ne peuvent être utilisées qu'après un examen du cas particulier.

Droit d'opposition

Le groupe de travail «Article 29» comprend que, dans la plupart des traitements effectués par la police ou des autorités judiciaires, le droit d'opposition au traitement ne devrait pas être autorisé afin que la fonction publique puisse s'exercer. Cependant, dans certaines situations, les personnes (des victimes ou des témoins, par exemple) devraient être autorisées à s'opposer au traitement de leurs données à caractère personnel (par exemple, après la fin de la procédure judiciaire). Cette possibilité existe en Europe et le groupe de travail demande que le texte de la directive reconnaisse ce droit individuel important.

Le groupe de travail «Article 29» se déclare donc favorable à un texte accordant ce droit à des catégories de personnes concernées telles que les victimes et les témoins.

10/ Obligations des responsables du traitement et des sous-traitants

Analyse de l'impact sur la protection des données (AIPD)

Le groupe de travail «Article 29» soutient fermement l'établissement d'une approche AIPD systématique dans le domaine du traitement de données à caractère personnel à des fins répressives[23]. Cette obligation est d'autant plus importante que le responsable du traitement est, selon le texte actuel, censé évaluer lui-même, éventuellement avec l'aide du DPD, le risque que pose le traitement, afin de déterminer s'il consulte ou non l'autorité de contrôle.

L'AIPD devrait faire partie de l'analyse d'impact réalisée avant le lancement d'un traitement de données, laquelle devrait non seulement inclure la protection des données, mais aussi des considérations sur l'impact plus large du traitement des données envisagé sur les droits et libertés des personnes concernées.

Le groupe de travail «Article 29» se réjouit de l'amendement proposé par le Parlement européen pour l'article 25, point a), qui prévoit un cadre imposant aux responsables du traitement d'effectuer une AIPD[24].

Tenue de journaux

Le groupe de travail «Article 29» rappelle que la tenue de journaux est un élément clé de la responsabilité et de la transparence, lié au contrôle interne et à l'audit ainsi qu'au contrôle de la licéité du traitement par les autorités de contrôle. Elle permet également l'exercice effectif de leurs droits par les personnes concernées. De ce fait, l'absence de journaux détaillés et compréhensibles, également protégés par des mesures destinées à assurer leur intégrité, réduirait l'efficacité de tout type de contrôle.

Le groupe de travail «Article 29» rappelle la nécessité de tenir des journaux des traitements automatisés et non automatisés effectués afin de s'assurer de la traçabilité des traitements et, sur ce point, il soutient la version de l'article 24 proposée par le Parlement européen.

[23] À cet égard, voir la motivation détaillée du groupe de travail «Article 29» dans l'avis 01/2013 précité.
[24] Voir l'article 25, point a), de la version de la proposition de directive présentée par le Parlement européen.

Consultation préalable de l'autorité de contrôle

Comme indiqué dans son avis sur le projet de règlement, le groupe de travail «Article 29» note que l'obligation de procéder à une consultation préalable de l'autorité de contrôle est un pouvoir qui n'existe que dans certains États membres.

Compte tenu de la sensibilité particulière des dossiers de la police et des autorités judiciaires, dans de nombreux cas, une consultation préalable de l'autorité de contrôle est particulièrement nécessaire pour protéger les droits et libertés des personnes concernées. Le groupe de travail «Article 29» est donc d'avis que lorsque les autorités de contrôle conservent la possibilité d'insister pour qu'une consultation préalable ait lieu, en tant que principe général, l'absence de notification est l'exception. Ce pouvoir devrait être maintenu pour les autorités de contrôle qui ont été ou sont en mesure de procéder à un contrôle préalable complet du traitement envisagé.

La possibilité de donner une autorisation préalable, lorsqu'elle existe, ne devrait pas soustraire les autorités de contrôle à l'exigence de fournir des conseils pour garantir le respect des droits fondamentaux à la protection de la vie privée et des données à caractère personnel de la personne concernée. Elle ne devrait pas davantage priver les autorités de contrôle du pouvoir d'examiner le traitement des données en cours afin de vérifier sa conformité avec la législation relative à la protection des données.

Le groupe de travail «Article 29» recommande donc le maintien d'un pouvoir de contrôle préalable complet pour les autorités de contrôle qui ont été ou sont en mesure de l'exercer en vertu de la législation applicable.

Sécurité des traitements

Le groupe de travail «Article 29» est favorable à des obligations strictes en ce qui concerne la sécurité des données à caractère personnel qui sont traitées. À cet égard, il se réjouit des obligations imposées au responsable du traitement en matière de conservation des documents et de mise en œuvre de mesures spécifiques. Cependant, le groupe de travail insiste sur la nécessité d'une disposition permettant d'adopter des normes minimales pour la mise en œuvre de ces mesures de sécurité, notamment des normes de cryptage.

Le groupe de travail «Article 29» penche donc en faveur d'un texte faisant référence à l'établissement par la Commission, par le biais d'actes d'exécution, de normes minimales pour la mise en œuvre des mesures de sécurité, notamment des normes de cryptage, comme le prévoient les versions de l'article 27, paragraphe 3, proposées par la Commission et le Parlement européen.

Notification des violations de données

À la personne concernée

Le groupe de travail «Article 29» est favorable à la fixation de différents seuils basés sur les risques pour la notification aux personnes des violations de données à caractère personnel et souhaiterait un alignement sur le libellé de la directive «vie privée et communications électroniques», à savoir une notification aux personnes concernées lorsque la «violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'une personne concernée...». À cet égard, le groupe de travail insiste sur le fait que les dérogations aux obligations de notification aux personnes concernées tiennent compte des différentes catégories de personnes concernées par le traitement. En

particulier, les personnes non suspectes devraient être informées lorsque la violation des données leur fait courir un risque.

À l'autorité de contrôle

Les risques inhérents au traitement des données effectué par des autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, sont généralement élevés. Il est donc probable qu'une violation de ces données soit extrêmement préjudiciable pour les personnes concernées. De telles violations peuvent également porter préjudice à la sécurité des États membres, comme des affaires récentes l'ont montré.

Ces raisons expliquent que le groupe de travail «Article 29» considère que, contrairement à l'article 28, paragraphe 1, actuel et à l'article 28, paragraphe 1, point a), de la version présentée par le Conseil pour la proposition de directive[25], les violations de données devraient être notifiées à l'autorité de contrôle. Cette notification sera indépendante de la notification à la personne concernée.

Le groupe de travail est donc favorable à un texte énonçant une obligation générale de notification à l'autorité de contrôle. Conscient des risques liés à la divulgation de l'existence d'une violation des données, le groupe de travail «Article 29» insiste sur le fait que les autorités de contrôle sont soumises à une obligation de confidentialité, qui s'applique naturellement dans de tels cas.

Le groupe de travail «Article 29» est donc favorable aux versions de l'article 28 présentées par la Commission et le Parlement européen, qui énoncent une obligation générale de notification à l'autorité de contrôle et établissent une distinction entre les catégories de personnes concernées pour ce qui concerne la notification à la personne concernée.

11/ Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Les transferts vers des pays tiers ne peuvent avoir lieu que si le transfert est nécessaire à des fins de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales dans le cadre d'une enquête/procédure spécifique.

Interdiction stricte de transferts massifs, répétés et structurés de données à caractère personnel vers des pays tiers, interprétation restrictive des dérogations et documentation systématique des transferts

Sur ce point, le groupe de travail «Article 29» est favorable à l'introduction d'une interdiction stricte des transferts massifs, répétés et structurés de données à caractère personnel vers les autorités de pays tiers et répète que les dérogations à l'interdiction des transferts vers des pays où le niveau de protection n'est pas adéquat devraient être interprétées de manière restrictive.

[25] *Article 28 Notification à l'autorité de contrôle d'une violation de données à caractère personnel*
1. Les États membres prévoient qu'en cas de violation de données à caractère personnel susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées, (...) le responsable du traitement en adresse notification à l'autorité de contrôle sans retard injustifié et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 72 heures, la notification comporte une justification à cet égard.
1a. La notification visée au paragraphe 1 n'est pas nécessaire si l'article 19, paragraphe 3, points a) et b), n'exige pas une communication de la personne concernée. (…)

Il soutient l'article 36, paragraphe 2, point b), dans la version présentée par le Parlement européen, qui se lit comme suit: «*Tous les transferts de données à caractère personnel décidés sur la base de dérogations doivent être dûment justifiés et limités au strict nécessaire et les transferts massifs et fréquents de données ne sont pas autorisés*».

Documentation relative aux transferts

Afin de s'assurer que les autorités chargées de la protection des données sont en mesure de vérifier correctement si les transferts sont conformes aux exigences de la directive et du droit national, la directive devrait aussi prévoir expressément que les transferts soient adéquatement documentés.

Le groupe de travail «Article 29» est donc favorable à l'article 23, qui prévoit que chaque responsable du traitement conserve une trace documentaire des transferts de données vers un pays tiers ou à une organisation internationale, y compris leur identification respective. À cet égard, la version de la Commission européenne et du Parlement européen faisant référence aux transferts internationaux et pas uniquement à des catégories de transferts internationaux devrait être privilégiée.

Conséquences du récent arrêt Schrems/Data Protection Commissioner

Le groupe de travail «Article 29» souligne que l'arrêt récent de la CJUE dans l'affaire Schrems/Data Protection Commissioner[26] énonce les critères applicables à un niveau de protection adéquat, lorsque des données à caractère personnel sont transférées vers des pays tiers, qui doivent être pris en compte en cas de transferts de données à caractère personnel vers des pays tiers au titre du régime mis en place par la directive. Conformément aux critères énoncés par la Cour, les exceptions au principe d'adéquation doivent être interprétées de manière restrictive. Selon la Cour, l'article 26, paragraphe 6, de la directive 95/46/CE qui impose ce niveau de protection adéquat met en œuvre l'obligation explicite énoncée à l'article 8, paragraphe 1, de la Charte[27].

Considérant que celle-ci est applicable dans un contexte répressif[28], l'exigence d'une protection équivalente des données à caractère personnel s'applique vraisemblablement aussi aux transferts de données à caractère personnel effectués dans un tel contexte.

En tout état de cause, la décision prise par la Commission ou un État membre constatant le caractère adéquat du niveau de protection est complétée par une appréciation complète du secteur de la police et de la justice et pourrait également être appréciée par l'autorité de contrôle nationale indépendante dans le cadre de l'examen d'une réclamation.

Le groupe de travail «Article 29» recommande donc aux institutions de modifier les dispositions pertinentes en conséquence.

En particulier, il recommande le maintien à l'article 41, paragraphe 2, point a), du règlement proposé, une référence spécifique à la sécurité publique et au droit pénal, entre autres éléments que la Commission devrait prendre en considération lors de l'appréciation du

[26] Arrêt du 6 octobre 2015 dans l'affaire C-362/14.
[27] Toute personne a droit à la protection des données à caractère personnel la concernant.
[28] À cet égard, l'expression «niveau de protection adéquat» doit être comprise comme imposant au pays tiers d'assurer, par son droit interne ou ses engagements internationaux et par sa pratique/efficacement, un niveau de protection des libertés et droits fondamentaux quasiment équivalent à celui garanti au sein de l'Union européenne.

caractère adéquat du niveau de protection[29]. Le groupe de travail suggère également d'ajouter la phrase suivante au début de l'article 34, paragraphe 2: «(...) ou que la décision n'a pas pris en considération la législation relative à la protection des données applicable aux autorités compétentes du pays tiers pour les finalités visées à l'article premier, paragraphe 1, (...)».

Il suggère également que le libellé de l'article 59 tienne compte des arrêts récents de la Cour de justice de l'Union européenne.

Transferts vers des entités publiques/privées d'un pays tiers

Le transfert de données à caractère personnel vers des entités privées de pays tiers en dehors de tout accord bilatéral ou mutuel en matière d'entraide judiciaire devrait, en principe, être interdit. Conformément à l'article 5.3.i de la recommandation n° R(87)15[30], la communication de données à des personnes privées **établies dans le même pays** ne devrait être permise que si, dans un cas déterminé, il y a obligation ou autorisation légales claires ou autorisation de l'autorité de contrôle. Toutefois, l'article 5.3.ii de ladite recommandation **autorise exceptionnellement** le transfert de données à caractère personnel vers des personnes privées établies dans le même pays si le transfert est, sans aucun doute, dans l'intérêt de la personne concernée et si, soit celle-ci y a consenti, soit les circonstances permettent de présumer sans équivoque un tel consentement, ou si le transfert est nécessaire pour éviter un danger grave et imminent. Ceci est particulièrement important lorsque le transfert est prévu vers des personnes privées établies dans des pays tiers.

Le groupe de travail «Article 29» s'inquiète donc de l'introduction de l'article 36, point aa), par le Conseil dans la mesure où il autoriserait un vaste transfert de données vers des pays tiers sur la seule base de l'exécution des tâches par l'autorité compétente et non par rapport à l'intérêt public prévu par la loi. Les dérogations au régime général applicable aux transferts ne devraient pas reposer uniquement sur l'exécution de tâches, qui peuvent être définies largement, mais sur l'existence de raisons importantes d'intérêt public.

De plus, l'utilisation du terme "destinataire" implique que les données peuvent être transférées à toute entité publique ou privée dans le pays tiers. Ces deux éléments contribuent à fixer un seuil très bas pour l'application d'une dérogation susceptible d'impliquer le transfert de données vers des pays où le niveau de protection n'est pas adéquat et où il n'existe aucune garantie adéquate. À cet égard, le groupe de travail renvoie à ses travaux récents sur l'accès transfrontière aux données, menés en coopération avec le comité de la convention sur la cybercriminalité du Conseil de l'Europe[31].

Le groupe de travail recommande donc de modifier l'article 36, point aa), pour clarifier les cas où cette disposition peut être utilisée, de réfléchir au fait que le principe devrait être une interdiction et de dresser une liste exhaustive des dérogations autorisées.

Assurer la cohérence avec l'article 43 bis du projet de règlement

Le groupe de travail «Article 29» insiste sur le fait que le texte de la directive doit être cohérent avec le projet de règlement en ce qui concerne les demandes émanant des autorités

[29] Voir, en ce sens, les versions du texte proposées par la Commission et le Parlement européen.
[30] Recommandation n° R(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police adoptée par le Comité des ministres du Conseil de l'Europe le 17 septembre 1987, lors de la 410e réunion des délégués des ministres.

publiques de pays tiers. La transparence devrait être assurée en ce qui concerne les demandes reçues.

12/ Rôles et pouvoirs des autorités de contrôle

Le groupe de travail «Article 29» insiste sur le fait qu'une disposition énonçant la possibilité que les États membres prévoient une obligation de consulter l'autorité de contrôle devrait être introduite dans le texte de la directive. Cela permettrait de respecter les pratiques nationales en matière de notifications.

Pour produire des effets, la directive devrait doter les autorités chargées de la protection des données d'outils efficaces. Le pouvoir de suspendre un traitement, y compris, le cas échéant, la suspension des transferts de données vers des pays tiers, et de rendre les traitements conformes d'une façon spécifique devrait être introduit afin de donner à l'autorité de contrôle des pouvoirs suffisamment dissuasifs, forts et efficaces. Ces derniers sont essentiels pour garantir la conformité.

En ce qui concerne le contrôle au quotidien, notamment lors de la conduite d'inspections et de l'imposition de sanctions, les autorités chargées de la protection des données ont besoin de pouvoirs harmonisés et effectifs d'investigation et de sanction. Dans la mesure où la directive est censée établir des garanties minimales, le groupe de travail «Article 29» serait favorable à une description plus détaillée de ces pouvoirs afin d'assurer une cohérence entre les autorités de contrôle et de veiller à ce que les responsables du traitement les respectent.

Compte tenu des différences entre les systèmes juridiques nationaux et étant donné qu'un simple accès à l'information n'est pas suffisant, le groupe de travail recommande d'imposer à tous les États membres l'obligation d'investir leur autorité de contrôle de pouvoirs d'enquête couvrant l'accès à toute donnée et document nécessaire à l'exécution de ses tâches, et de lui donner des moyens et des locaux pour effectuer le traitement des données. Cela devrait se faire dans le respect du droit de l'Union et/ou du droit procédural des États membres.

Le groupe de travail «Article 29» est donc favorable à une disposition portant sur les pouvoirs des autorités chargées de la protection des données, y compris des pouvoirs effectifs d'enquête et de correction.

13/ Droit d'introduire une réclamation

Le groupe de travail «Article 29» estime que les personnes concernées devraient avoir le droit d'introduire une réclamation, à tout le moins auprès de l'autorité chargée de la protection des données, dans l'État membre où elles ont leur résidence habituelle (article 50). Le comité européen de la protection des données devrait être chargé de veiller à la coopération nécessaire entre les autorités chargées de la protection des données des États membres.

À cet égard, le groupe de travail «Article 29» suggère de veiller à la cohérence entre le libellé de l'article 50 et celui proposé par le Conseil pour l'article 73, paragraphe 1, du projet de règlement, à savoir: «Sans préjudice de tout autre recours administratif ou judiciaire, toute personne concernée A le droit d'introduire une réclamation auprès d'une seule autorité de contrôle, **notamment dans l'État membre de sa résidence habituelle**, de son lieu de travail ou du lieu de l'infraction alléguée, si elle considère que le traitement de données à caractère personnel la concernant n'est pas conforme au présent règlement».

14/ Accords internationaux conclus antérieurement dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière

La question de l'articulation de la directive avec les décisions constatant le caractère adéquat de la protection et les accords bilatéraux conclus avec des pays tiers n'est toujours pas réglée.

Le groupe de travail «Article 29» est d'avis qu'un réexamen des accords existants s'impose pour s'assurer que ces instruments ne sont pas utilisés de manière à contourner les règles énoncées dans la directive et que le nouveau régime en matière de protection des données s'applique à tous les traitements de données à caractère personnel relevant de son champ d'application[32].

Sur ce point, alors que le projet de proposition de 2012 confiait aux autorités compétentes l'obligation de modifier, si nécessaire, des accords internationaux conclus antérieurement dans les cinq ans suivant l'adoption de la directive, le libellé retenu par le Conseil semble éviter ce réexamen en déclarant que les accords qui sont conformes au droit de l'Union applicable avant l'entrée en vigueur de la directive resteront en vigueur jusqu'à ce qu'ils soient modifiés, remplacés ou abrogés.

Le groupe de travail «Article 29» est donc favorable à la proposition de la Commission, soutenue par le Parlement européen, à savoir l'introduction à l'article 60 d'une obligation de modifier, si nécessaire, dans les cinq ans suivant l'adoption de la directive, les accords internationaux conclus antérieurement. Au minimum, le groupe de travail souhaiterait que l'on veille à ce que les instruments existants soient appliqués d'une manière compatible avec la directive.

[32] Voir également, en ce sens, l'observation relative à l'article 59 ci-dessus.