EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 6/2015

Une nouvelle étape vers une protection européenne complète des données

Recommandations du CEPD sur la directive pour la protection des données dans les secteurs police et justice

28 octobre 2015

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE. Le contrôleur est chargé, en vertu de l'article 41, paragraphe 2, du règlement 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel […] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», *et* «[…] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Le contrôleur européen et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'être plus constructifs et proactifs, et ils ont publié en mars 2015 une stratégie quinquennale exposant la manière dont ils entendaient mettre en œuvre ce mandat et en rendre compte.[1]

Le présent avis est une autre étape importante de la stratégie du CEPD qui souligne que la réforme des règles européennes en matière de protection des données est plus urgente que jamais. Comme le souligne le récent avis nº 3/2015, le CEPD est, conjointement avec d'autres autorités nationales de protection des données, un partenaire actif dans les discussions entre la Commission européenne, le Parlement et le Conseil concernant la réforme de la protection des données, bien qu'il ne fasse pas partie du trilogue final même en ce qui concerne la directive pour la protection des données dans les secteurs police et justice. Nous continuons notre quête de solutions fiables, efficaces, pratiques et réalisables. Le présent avis reflète à nouveau notre engagement. Il sera suivi dans les prochaines semaines de recommandations spécifiques relatives au texte pertinent du projet de directive, qui seront également intégrées dans l'application de la protection des données du CEPD destinée aux appareils mobiles.

Le présent avis sur la directive pour la protection des données dans les secteurs police et justice s'aligne sur l'avis exhaustif du CEPD concernant la proposition de paquet de mesures de la Commission adoptée en mars 2012. Les opinions exprimées dans cet avis restent valides. Après plus de trois ans et demi, nous nous devions toutefois de mettre à jour notre avis pour soutenir plus directement les positions des colégislateurs et proposer des recommandations spécifiques[2]*. Comme l'avis de 2012, le présent avis s'aligne sur les avis et déclarations du groupe de travail «Article 29».*

Table des matières

I. Cette directive est un pas important vers une protection des données au sein de l'UE moderne.

Grâce à l'adoption d'un accord général sur la directive pour la protection des données dans les secteurs police et justice[3], le Conseil a franchi une étape vers l'établissement d'un nouveau cadre pour la protection des données au sein de l'Union européenne.

L'une des principales lacunes des législations actuelles en matière de protection des données au niveau de l'Union européenne dans ces secteurs est qu'il s'agit d'un assemblage de diverses règles relatives à des secteurs spécifiques et d'un instrument destiné à être applicable d'une manière générale, mais qui ne remplit pas cet objectif. En effet, la décision-cadre du Conseil relative à la protection des données de 2008[4] s'applique uniquement lorsque les données sont échangées entre des États membres, et non lorsque les données restent au niveau national. À la suite de la présente directive, les citoyens européens peuvent enfin bénéficier d'un instrument législatif actualisé de l'Union qui s'appliquera à l'ensemble des secteurs de la police et de la justice.

La présente proposition est également appréciée, car elle confirme la nécessité d'une protection complète des données. Le règlement général sur la protection des données visant à moderniser le régime législatif du secteur privé et une grande partie du secteur public, il ne serait pas acceptable que les secteurs de la police et de la justice, où tant de données à caractère personnel sensibles sont traitées, n'aient pas connaissance des modifications législatives actuelles. Un régime complet de protection est également nécessaire, ne fût-ce qu'en raison des grandes quantités de données à caractère personnel qui sont échangées entre les différents secteurs dans nos sociétés modernes.

Ce besoin d'approche globale est également une raison pour laquelle le CEPD recommande vivement l'entrée en vigueur simultanée des différents instruments de la réforme de la protection des données. À cet égard,

1. le délai de transposition de la directive devrait demeurer de deux ans, comme le propose la Commission, et ne devrait pas être étendu à trois ans;
2. il conviendrait que la Commission présente dès que possible sa proposition relative à un nouvel instrument pour la protection des données au niveau des institutions et organes de l'UE, remplaçant le règlement nº 45/2001.

II. Les règles devraient garantir un niveau élevé de protection.

Notre demande d'approche globale vise également à garantir que les règles applicables à l'ensemble des secteurs de la société sont uniformes et assurent un niveau élevé de protection. Ce besoin d'un niveau élevé de protection est la conséquence de l'intégration du droit à la protection des données dans le droit primaire de l'UE, notamment à l'article 16 TFUE et à l'article 8 de la charte des droits fondamentaux de l'Union. La protection des données est étroitement liée au droit au respect de la vie privée, une valeur fondamentale dans nos sociétés démocratiques qui était déjà reconnue dans la législation en 1950 dans la Convention européenne des droits de l'homme, et qui est à présent également reprise à l'article 7 de la charte.

Les arrêts de la Cour de justice dans les affaires *Digital Rights Ireland*[5] et, récemment, *Schrems*[6], confirment en outre l'importance que revêt un niveau élevé de protection, en particulier en ce qui concerne l'application de la loi et la sécurité nationale. Dans l'arrêt *Digital Rights Ireland*, la Cour signale que l'instrument de conservation des données était «*susceptible de générer dans l'esprit des personnes concernées […] le sentiment que leur vie privée fait l'objet d'une*

surveillance constante»[7]. Dans l'arrêt *Schrems,* la Cour estime que l'accès des autorités publiques au contenu de communications électroniques de manière généralisée porte atteinte au contenu essentiel du droit au respect de la vie privée[8].

Ce ne sont que quelques exemples d'une approche adoptée dans le traité et confirmée par la plus haute Cour de l'UE, qui souligne la nécessité d'une protection forte des personnes, dans le cadre des valeurs de l'Union européenne. Cette même approche devrait se refléter dans la directive, qui non seulement doit respecter les obligations légales prévues dans le droit international et le droit européen, mais doit également traduire le fait que le respect de la vie privée et la protection des données sont des valeurs essentielles pour les personnes et la société en tant que telle.

L'avis du CEPD concernant la proposition sur le paquet de mesures de mars 2012 a particulièrement critiqué le niveau de protection prévu dans la proposition de directive. Nous avons souligné le niveau très insuffisant de protection.

La principale justification d'un régime spécifique de protection des données dans les secteurs de la police et de la justice réside dans la nature spécifique de ces secteurs[9]. En d'autres termes, ce sont des règles spécifiques qui sont nécessaires et non pas des règles qui contiennent principalement des exceptions aux principes de protection des données prévus dans la proposition de règlement général sur la protection des données. La protection des données dans les secteurs de la police et de la justice doit être parfaitement cohérente avec les règles générales et ne prévoir des spécifications qu'en cas de nécessité.

L'accord général du Conseil vise de plus à transformer la nature de la directive en un instrument assurant une harmonisation minimale, permettant aux États membres de prévoir des garanties plus élevées en matière de protection des données aux termes de la législation nationale[10]. Bien que nous ne soyons pas opposés à un pouvoir discrétionnaire des États membres pour renforcer les garanties en matière de protection des données au niveau national, nous soulignons qu'il appartient au législateur européen, en vertu de l'article 16 TFUE, de garantir des normes élevées de protection des données et de ne pas laisser cette gestion à chaque État membre. De plus, la différenciation des normes entre les États membres entraverait la libre circulation des informations entre les autorités compétentes et aurait ainsi une incidence négative sur l'efficacité de la coopération judiciaire et policière. S'il existait des différences trop marquées au niveau des normes entre les États membres, cela compliquerait également l'échange d'informations avec Europol, qui dispose, par rapport à la directive, d'un régime de protection des données propre et relativement strict: les États membres peuvent choisir de coopérer bilatéralement, sur la base du plus petit dénominateur commun.

En substance, le législateur européen devrait s'assurer que:

1. Aucune des dispositions de la directive ne diminue le niveau de protection qui est actuellement offert par la législation européenne, notamment la décision-cadre du Conseil de 2008, et par les instruments du Conseil de l'Europe[11].
2. Les éléments essentiels de la protection des données, prévus à l'article 8 de la charte des droits fondamentaux de l'Union, sont respectés et ces exceptions satisfont au critère rigoureux de la proportionnalité, comme le précise l'arrêt *Digital Rights Ireland*[12]. Dans le présent avis, nous attirons principalement l'attention sur le principe de limitation de la finalité, sur le droit d'accès des personnes à leurs données à caractère personnel et sur le contrôle par des autorités indépendantes de protection des données[13].
3. Les éléments essentiels de la protection des données font partie de la directive et ne sont pas laissés à l'appréciation des États membres[14].

III. Le champ d'application de la directive devrait se limiter aux domaines pour lesquels des règles spécifiques sont réellement nécessaires.

Nous constatons que dans l'accord général du Conseil portant sur la directive, le champ d'application est étendu à la protection contre les menaces à la sécurité publique ainsi qu'à la prévention de telles menaces[15], un domaine ne relevant pas du droit pénal qui, en vertu de la loi en vigueur, n'est pas couvert par la décision-cadre actuelle du Conseil relative à la protection des données. Le considérant 11 *bis* donne des exemples de ce qui pourrait être couvert: des activités policières lors de manifestations, de grands événements sportifs majeurs et d'émeutes, ou, de façon plus générale, des activités policières destinées au maintien de l'ordre public.

Toutefois, la définition de la «*protection contre les menaces pour la sécurité publique et de la prévention de telles menaces*» demeure obscure. Ce terme peut recevoir différentes interprétations et ne permet pas une délimitation claire des tâches de la police relevant du champ d'application de la directive[16]. Nous recommandons par conséquent de restreindre le champ d'application de la directive aux activités d'application du droit pénal par les autorités judiciaires et policières, comme cela était prévu dans la proposition initiale de la Commission.

Le CEPD estime que la notion d'«autorité compétente», telle que définie à l'article 3, paragraphe 13, doit également rester aussi limitée que possible: l'exercice de l'application de la loi par des organisations et des entités non publiques devrait être assujetti au règlement et non à la directive. Ces organisations et entités privées ne nécessitent pas de régime spécifique. Par exemple, des compagnies aériennes ou des opérateurs de télécommunications, qui sont légalement tenus de recueillir et de communiquer leurs données, ne devraient pas être assujettis à la directive étant donné que l'objectif principal et initial de la collecte de ces données est totalement différent de la prévention et de la détection d'infractions pénales ainsi que des enquêtes et des poursuites en la matière. Le considérant 11 de l'accord général du Conseil fait également référence à la conservation des données par des établissements financiers et, dans ce cas particulier, à l'obligation pour ces entités privées d'être liées par un contrat conformément à l'article 21 de la directive.

Par ailleurs[17], l'article 2, paragraphe 3, de la proposition exclut de son champ d'application le traitement des données à caractère personnel dans le cadre d'une activité n'entrant pas dans le champ d'application du droit de l'Union. La référence à la sécurité nationale a été supprimée de l'article 2, paragraphe 3, mais a été réintroduite dans le considérant 11 *bis*. Comme le CEPD l'a déjà mentionné, ce que cette notion couvre n'est pas toujours clair, car elle dépend de la politique nationale des États membres. Nous prenons acte de l'exception, mais estimons qu'elle ne devrait pas être invoquée pour légitimer le traitement de données à caractère personnel en dehors du champ d'application du règlement et de la directive, par exemple dans le cadre de la lutte contre le terrorisme. Par conséquent:

1. Le règlement devrait rester applicable à l'ensemble des activités qui ne sont pas directement liées à la prévention et à la détection d'infractions pénales, ainsi qu'aux enquêtes et aux poursuites en la matière ou à l'exécution des sanctions pénales et dans le cas où des règles spécifiques se révéleraient nécessaires.
2. L'exercice de l'application de la loi par des organisations et entités non publiques devrait être assujetti au règlement.

IV. Limitation de la finalité et catégories particulières de données

Nous constatons que dans l'accord général du Conseil relatif à la directive, un deuxième paragraphe a été ajouté à l'article 4 qui permet le traitement par le même ou un autre responsable du traitement pour des finalités autres que celles pour lesquelles les données ont été collectées ,à condition que le responsable du traitement soit autorisé à traiter ces données pour ces finalités en vertu des dispositions juridiques applicables et que le traitement soit nécessaire et proportionné à ces autres finalités. Nous souhaiterions souligner l'importance du respect du principe de la limitation de la finalité, qui est une pierre angulaire du régime de la protection des données[18]. Il convient de veiller à ce que les données traitées par des autorités compétentes agissant dans le champ d'application de la directive ne fassent pas l'objet d'un traitement ultérieur pour une finalité totalement différente, qui serait par conséquent facilement considérée comme incompatible (par exemple, une utilisation ultérieure des données collectées par la police à des fins d'immigration). Nous recommandons d'ajouter des éléments supplémentaires au texte afin de délimiter la notion de limitation de la finalité dans le domaine de la police et de la justice et de préciser la notion de traitement ultérieur incompatible. Des considérations semblables sont actuellement avancées dans le cadre du règlement d'Europol[19] et ont été mentionnées dans l'avis récemment adopté par le CEPD sur le règlement général sur la protection des données (article 6, paragraphe 2).

Nous souhaiterions en outre attirer l'attention sur la formulation de la limitation relative au traitement portant sur des catégories particulières de données à caractère personnel prévue à l'article 8, qui devrait être formulée comme une interdiction de traiter ces catégories de données, sauf dans le cas où une dérogation expresse et particulière s'applique (comme le propose le texte du Parlement). La formulation ne devrait pas descendre au-dessous du niveau actuel de protection offert sur le fondement du principe 2.4 de la recommandation du Conseil de l'Europe nº R(87)15. En substance,

1. Il convient de préciser davantage ce que signifie la limitation de la finalité dans les domaines de la police et de la justice, et ce qu'est un traitement ultérieur incompatible.
2. Le traitement portant sur des catégories particulières de données à caractère personnel dans les domaines de la police et de la justice doit rester interdit, sauf dans le cas où une dérogation particulière prévue à l'article 8 de la directive s'applique.

V. Droits des personnes concernées

Nous rappelons que les droits des personnes en ce qui concerne le traitement de leurs données à caractère personnel sont un élément essentiel du droit à la protection des données à caractère personnel garanti à l'article 8 de la charte. Ces droits comprennent la communication d'informations à des personnes concernant le traitement de leurs données à caractère personnel et l'existence de leurs droits, de manière à garantir un traitement loyal, ainsi que la possibilité d'accéder aux données les concernant et de demander la rectification, l'effacement et/ou la limitation du traitement de ces données. Nous constatons que les dispositions convenues dans l'orientation générale du Conseil ne garantissent pas pleinement le respect des droits des personnes, notamment dans les cas où une limitation aux droits des individus n'est pas, ou n'est plus, applicable.

Nous exhortons par conséquent les colégislateurs à veiller à ce que les termes des articles 10 et 16 respectent les exigences minimales de ces droits et ne descendent pas en dessous du niveau

actuel de protection des données garanti dans la charte, les traités de l'UE et les traités internationaux (notamment la Convention 108).

Il convient de préciser clairement dans le texte que les limitations aux droits des personnes, qui sont des exceptions à un droit fondamental, doivent être interprétées de manière restrictive, comme le demande la jurisprudence de la Cour. La conséquence de ces limitations peut être que, au cas par cas et dans la mesure et pour aussi longtemps que cela est nécessaire, la communication d'informations à la personne peut être refusée. Toutefois, lorsque la limitation cesse de s'appliquer, la personne devrait être en mesure d'exercer pleinement ses droits. En outre, la personne concernée devrait toujours être informée par écrit de tout refus ou de toute limitation; la communication du raisonnement ne peut être limitée que lorsque cela s'avère nécessaire dans l'intérêt de l'un des motifs légitimes de refus. En substance,

1. Il conviendrait de rétablir le texte original de l'article 10 de la proposition de la Commission concernant la communication et les modalités d'exercice des droits de la personne concernée, étant donné que des éléments essentiels ont été supprimés dans l'orientation générale du Conseil.
2. La notification aux personnes devrait également comprendre des informations concernant i) le délai de conservation des données, ii) l'existence du droit de demander l'accès, la rectification, l'effacement ou la limitation, et iii) le type de destinataires, y compris des tiers ou des organisations internationales, conformément à l'article 11 de la proposition de la Commission.
3. Le droit d'accès devrait être clairement établi à l'article 12 et son exercice ne devrait pas être soumis aux dérogations prévues par la législation nationale (comme le prévoit l'article 12, paragraphe 1, de l'orientation générale du Conseil). C'est l'inverse: le droit d'accès devrait être garanti par principe, et on ne devrait pouvoir y déroger que dans des circonstances précisément prévues dans la législation et tant que ces limitations sont valables.

VI. Garantir le contrôle par des autorités indépendantes de protection des données

Pour notre part, il n'est pas nécessaire de différencier les pouvoirs conférés aux autorités chargées de la protection des données (DPA) au titre du règlement et de la directive. Le contrôle est un élément essentiel du droit fondamental à la protection des données[20], et le niveau et l'intensité de contrôle ne devraient pas dépendre du secteur dans lequel les données à caractère personnel sont traitées.

Nous constatons que les pouvoirs des autorités de contrôle conférés par la directive ne coïncident pas avec ceux énumérés à l'article 53 de la proposition de règlement[21]. Par exemple, le pouvoir d'infliger des sanctions est proposé uniquement par le Parlement européen, alors que le règlement prévoit cette possibilité. Un autre exemple est l'absence de description des pouvoirs d'enquête des autorités de contrôle, qui ne devraient pas être restreints par rapport aux pouvoirs d'enquête prévus dans la proposition de règlement.

La possibilité d'exclure les tribunaux, dans le cadre de leurs fonctions juridictionnelles, du contrôle soulève des questions importantes d'interprétation et de champ d'application[22]. Faisant référence au considérant 55 de la proposition de la Commission, nous recommandons par conséquent de conserver l'expression «activités "**purement**" judiciaires» que le Conseil a supprimée. La raison d'être de l'exemption prévue à l'article 44, paragraphe 2 semble être, comme le souligne le considérant, de «*préserver l'indépendance des juges dans l'exercice de*

leurs fonctions judiciaires»[23]. Dans ce contexte, nous constatons également que, notamment au regard des différences importantes entre les systèmes judiciaires des États membres, il n'est pas toujours évident de savoir quand et si les procureurs sont des «des autorités judiciaires indépendantes», ni quand et dans quelle mesure leurs activités constituent des «activités judiciaires». Des éclaircissements appropriés s'avèrent par conséquent nécessaires.

Le comité européen de la protection des données sera composé, aux termes de la proposition de règlement, d'une autorité de contrôle de chaque État membre et du CEPD. Toutefois, conformément à l'article 39, paragraphe 2, de la proposition de directive, l'autorité de contrôle n'est pas obligatoirement l'autorité de contrôle désignée conformément au règlement proposé. Par conséquent, un membre du comité européen de la protection des données n'est pas nécessairement chargé du contrôle dans le cadre de la directive. Nous recommandons de clarifier ce point, en précisant par exemple à l'article 39, paragraphe 3, que lorsque différentes autorités sont désignées aux termes du règlement et de la directive, elles devraient coordonner leur action afin de représenter la voix des deux autorités au sein du comité européen de la protection des données. En substance,

1. Il n'est pas nécessaire de différencier les pouvoirs conférés aux autorités chargées de la protection des données en vertu du règlement et de la directive.
2. L'exception des pouvoirs de contrôle des autorités chargées de la protection des données dans le secteur judiciaire devrait se limiter aux activités «purement» judiciaires, en clarifiant également la position du ministère public.

VII. Transferts internationaux et transferts vers des parties privées.

L'arrêt *Schrems*[24] confirme les conditions strictes régissant le transfert de données à caractère personnel vers des pays tiers. Nous recommandons de revoir le chapitre V de la directive en tenant compte comme il se doit de l'arrêt Schrems. Cela signifie, par exemple, qu'une décision constatant le caractère adéquat du niveau de protection devra être fondée sur une évaluation complète du secteur de l'application de la loi. Une décision constatant le caractère adéquat du niveau de protection ne doit pas priver l'autorité de contrôle du pouvoir d'examiner un transfert spécifique et de prendre des mesures coercitives lorsque le transfert ne satisfait pas aux exigences requises.

De plus, nous recommandons de veiller à ce que le transfert de données à caractère personnel sans une décision constatant le caractère adéquat de la protection se limite aux situations où il existe un instrument juridiquement contraignant, ou lorsqu'il est nécessaire de protéger les intérêts vitaux de la personne concernée ou dans le cas d'une menace grave et immédiate à la sécurité publique[25]. Nous recommandons d'adapter l'article 34, paragraphe 6, et l'article 36 en conséquence.

Enfin, nous pensons qu'un transfert vers une partie privée ne peut avoir lieu que si les conditions actuellement exposées dans la recommandation nº R(87)15 du Conseil de l'Europe sont remplies. Ce transfert ne doit intervenir que lorsque la communication est sans aucun doute dans l'intérêt de la personne concernée et si celle-ci y a consenti ou si les circonstances permettent de présumer sans équivoque un tel consentement, ou si la communication est nécessaire pour éviter un danger grave et imminent. Nous recommandons d'adapter en conséquence l'article 36 *bis bis*, comme suggéré par le Conseil. En substance,

1. Nous recommandons de revoir le chapitre V de la directive, en tenant également compte comme il se doit de l'arrêt Schrems.
2. Les transferts vers une partie privée ne pourront avoir lieu que si les conditions actuellement exposées dans la recommandation nº R(87)15 du Conseil de l'Europe sont remplies.

VIII. Dispositions finales

Le présent avis a déjà mentionné que, afin de s'assurer qu'un système complet de protection des données soit requis au sein de l'Union, il faudrait que la directive puisse entrer en vigueur en même temps que le règlement général sur la protection des données. Le même argument s'applique à la nécessité de veiller à ce que les instruments actuels comportant des dispositions sur la protection des données soient conformes à la directive.

Nous constatons qu'aux termes de la proposition de la Commission, la directive n'affecte en rien les instruments internes de l'Union européenne existants, mais oblige la Commission à apprécier la nécessité de les mettre en conformité avec la présente directive, dans un délai de deux ans à compter de son adoption (article 61, paragraphe 2). Le Conseil propose de porter ce délai à cinq ans après l'adoption, ce qui prolonge indûment la période d'incertitude juridique.

En outre, le Conseil supprime l'obligation de modifier, au besoin, les accords existants portant sur le transfert de données à caractère personnel conclus par les États membres. En revanche, l'accord général du Conseil stipule que tous les accords conclus avant l'entrée en vigueur de la directive ne sont pas affectés. Cela signifierait non seulement que les dispositions de ces accords qui ne sont pas conformes à la directive restent en vigueur pour une période indéterminée, mais également que les États membres sont habilités à conclure des accords avec des pays tiers durant la période de transposition de la directive, sans prendre en considération son contenu substantiel[26]. En substance,

1. Il conviendra de s'assurer que la nécessité de mettre les instruments internes de l'UE existants en conformité avec la directive est examinée aussi tôt que possible et, en tout état de cause, au plus tard dans les deux ans qui suivent son entrée en vigueur.
2. Si nécessaire, il conviendra de modifier dans un délai donné les accords existants portant sur le transfert de données à caractère personnel conclus par les États membres. Il devrait être interdit aux États membres de conclure des accords avec des pays tiers durant la période de transposition de la directive.

Fait à Bruxelles, le 28 octobre 2015.

(signé)

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

Notes

[1] Avis de vacance du poste de contrôleur européen de la protection des données COM/2014/10354 (2014/C 163 A/02), JO C 163 A/6 du 28.5.2014. La stratégie du CEPD 2015-2019 promettait de «*rechercher des solutions réalisables qui requièrent moins d'administration, restent ouvertes aux innovations technologiques et aux flux de données transfrontaliers et garantissent que les personnes puissent faire valoir leurs droits plus efficacement tant en ligne qu'hors ligne*»; Montrer l'exemple: La stratégie du CEPD 2015-2019, mars 2015.

[2] Avis du CEPD sur le paquet de mesures pour une réforme de la protection des données du 7.3.2015.

[3] 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, COM(2012)10 final; résolution législative du Parlement européen du 12 mars 2014 sur la proposition de directive du Parlement européen et du Conseil 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, P7_TA(2014)0219.

[4] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350/60.

[5] Affaires jointes C-293/12 et C-594/12, Digital Rights Ireland (C-293/12) et Seitlinger (C-594/12), ECLI:EU:C:2014:238.

[6] Affaire C-362/14, Schrems, ECLI:EU:C:2015:650.

[7] Affaires jointes C-293/12 et C-594/12, Digital Rights Ireland (C-293/12) et Seitlinger (C-594/12), ECLI:EU:C:2014:238, point 37.

[8] Affaire C-362/14, Schrems, ECLI:EU:C:2015:650, point 94.

[9] Voir, par exemple, déclaration 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée au traité de Lisbonne: «*La Conférence reconnaît que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 du traité sur le fonctionnement de l'Union européenne pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines*».

[10] Article 1 *bis* de l'accord général.

[11] Le rapporteur ne cesse également de le souligner à l'égard du règlement général sur la protection des données. Voir, par exemple, Jan Philipp Albrecht, No EU Data Protection Standard Below the Level of 1995 (Aucune norme européenne de protection des données inférieure au niveau de 1995), EDPL 2015, volume 1, pages 3 et 4.

[12] Affaires jointes C-293/12 et C-594/12, Digital Rights Ireland (C-293/12) et Seitlinger (C-594/12), ECLI:EU:C:2014:238.

[13] Le contrôle est un élément essentiel de la protection de la personne: considérant 62 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281/31, et jurisprudence de la Cour de justice, plus récemment, affaire C-362/14, Schrems, EU:C:2015:650, point 42.

[14] Cela ne serait pas conforme à la jurisprudence de la Cour de justice, notamment des affaires jointes C-293/12 et C-594/12, Digital Rights Ireland (C-293/12) et Seitlinger (C-594/12), ECLI:EU:C:2014:238, points 54 à 62.

[15] Article 1, paragraphe 1, de l'accord général.

[16] Par exemple, le suivi d'une tentative de suicide ou d'une arrestation administrative relèverait-il du champ d'application?

[17] Comme le CEPD l'a souligné dans son avis sur le paquet de mesures pour une réforme de la protection des données du 7.3.2015, au point 323.

[18] Voir avis nº 03/2013 du groupe de travail «Article 29» sur la protection des données relatif à la limitation de la finalité, adopté le 2 avril 2013.
[19] Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI.
[20] Ainsi que cela a été récemment confirmé dans l'affaire C-362/14, Schrems, ECLI:EU:C:2015:650.
[21] Voir également avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, du 7.3.2015, partie III.8.
[22] Voir également avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, du 7.3.2015, partie III.8.
[23] (Le CEPD considère que le critère permettant d'exclure l'activité de traitement des données du contrôle des autorités chargées de la protection des données (ou de l'y inclure) devrait être, respectivement, le fait que le traitement des données à caractère personnel a lieu dans le cadre de l'activité judiciaire («procès», acte judiciaire, activités judiciaires intervenant dans le cadre d'affaires portées devant les tribunaux) ou dans celui d'autres activités auxquelles les juges pourraient être associés en vertu du droit national, plutôt que de se baser sur la distinction tout court entre des catégories de responsables du traitement, à savoir le tribunal, d'un côté, et le procureur, comme exemple d'une «autre autorité judiciaire», de l'autre.
[24]Affaire C-362/14, Schrems, ECLI:EU:C:2015:650.
[25] Voir également avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, du 7.3.2015, partie III.7.
[26] Le pouvoir peut, dans certaines conditions, être limité par le principe de coopération loyale (article 4, paragraphe 3, du TUE).