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

00379/13/FR
WP 201

Avis 01/2013 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

Adopté le 26 février 2013

1. Introduction

Le 25 janvier 2012, la Commission européenne a adopté une 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* (ci-après, la «directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale» ou la «directive»). Cette proposition a été présentée parallèlement au règlement général sur la protection des données. Tant le Conseil que le Parlement européen ont ensuite lancé leurs procédures législatives respectives pour les deux instruments, en vue d'obtenir un accord sur l'intégralité du paquet avant les élections européennes de 2014. Cependant, le débat législatif sur la directive progresse lentement.

Le groupe de travail «Article 29» a transmis sa première réaction générale à la proposition de la Commission dans son avis du 23 mars 2012, dans lequel il soulignait les points qu'il estimait préoccupants et faisait des suggestions d'améliorations.

Le groupe se félicite de l'approche globale («paquet») adoptée par les rapporteurs du Parlement européen dans leurs projets de rapports destinés à la commission LIBE. Il est convaincu que tous les groupes politiques continueront à tenir dûment compte de tous les éléments du paquet et à veiller à la cohérence absolument nécessaire entre les deux propositions afin de les améliorer encore. Le groupe se félicite également de l'intensification du débat législatif au Conseil, à l'instigation des présidences chypriote et irlandaise.

Après avoir adopté le 5 octobre 2012 son premier avis apportant une nouvelle contribution aux discussions sur le règlement, le groupe formule dans le présent avis d'autres orientations relatives à plusieurs éléments particuliers de la directive proposée sur la protection des données traitées dans les domaines de la police et de la justice pénale. Bien que d'autres questions puissent encore être examinées, le groupe a décidé, vu l'état d'avancement des négociations, de se concentrer sur quatre éléments actuellement considérés comme les plus importants. Il s'agit de l'utilisation des données concernant des personnes non suspectes, des droits des personnes concernées, de l'utilisation des analyses d'impact sur la vie privée et des pouvoirs des autorités chargées de la protection des données, notamment en ce qui concerne les informations confidentielles ou classifiées.

2. L'utilisation des données concernant des personnes non suspectes

L'article 5 de la proposition de directive fait obligation au responsable du traitement d'établir une distinction claire entre les données à caractère personnel concernant différentes catégories de personnes et définit cinq catégories de personnes concernées. Le considérant 23 indique que cette distinction découle nécessairement du traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Le groupe souligne que cette distinction est également indispensable pour garantir la bonne application des principes relatifs au traitement des données à caractère personnel définis à l'article 4.

L'article 5 établit une distinction entre plusieurs catégories de personnes ayant un lien direct ou un lien indirect (éventuel) avec une infraction pénale particulière ou des suspects [catégories a) à d), les autres personnes constituant la catégorie e)]. Compte tenu de la

description donnée du lien qu'ont les personnes visées aux points a) à d) avec une infraction pénale ou une enquête, il est manifeste que les personnes relevant de la catégorie e) peuvent être qualifiées de personnes n'ayant aucun lien connu avec une infraction ou des suspects, lien mentionné pour les autres catégories.

C'est précisément à l'égard de ce groupe de personnes que les autorités européennes chargées de la protection des données ont souligné, en 2005[1] déjà, qu'il y avait lieu de faire une distinction entre le traitement de données à caractère personnel concernant des personnes non suspectes et le traitement des données relatives à des personnes liées à une infraction particulière. Le traitement de données concernant des personnes non soupçonnées d'avoir commis une infraction pénale (autres que les victimes, témoins, informateurs, contacts et complices) «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». Parallèlement, la directive devrait préciser que des restrictions et des garanties supplémentaires s'appliquent aux victimes et autres tiers, visés à l'article 5, paragraphe 1, point c), de la proposition actuelle. La législation doit reconnaître qu'il y a lieu de distinguer entre le traitement de données à caractère personnel concernant des personnes déclarées coupables d'infractions pénales et celui de données relatives à des victimes de telles infractions, en particulier dans les bases de données créées à des fins préventives ou pour faciliter les poursuites à l'encontre des auteurs de futures infractions.

L'évolution des techniques et méthodes répressives au cours de la dernière décennie indique clairement que tous les groupes de personnes relevant de la catégorie générale des «personnes non suspectes» doivent bénéficier d'une protection particulière. Cela est d'autant plus vrai lorsque le traitement n'est pas effectué dans le cadre d'une enquête ou de poursuites pénales particulières. La question qui se pose est celle de la distinction entre les informations que les services répressifs «doivent connaître» et les informations «souhaitables».

Pour protéger les personnes non suspectes, le groupe recommande vivement qu'un nouvel article 7 *bis* soit inséré, en complément de l'article 5. Ce nouvel article 7 *bis*, dont le libellé est proposé ci-dessous, garantirait que la différenciation des catégories de données ne représente pas une charge administrative et ne constitue pas une fin en soi, comme la proposition actuelle semble le laisser entendre. Il y a lieu de faire en sorte que les États membres ne puissent procéder au traitement de données relatives à des personnes non suspectes que si certaines conditions sont remplies et qu'une protection supplémentaire est exigée lorsque de telles données sont soumises à un traitement. Par conséquent, il est plus pertinent d'insérer une nouvelle disposition dans le contexte de l'article 7 qui régit la licéité des traitements.

Le groupe est conscient de la nature particulière des traitements de données effectués dans un contexte répressif et comprend que le traitement de données concernant des personnes non suspectes peut se révéler nécessaire dans certains cas. La proposition tient également compte des divers motifs pour lesquels les services répressifs peuvent traiter les données de personnes non suspectes et propose notamment des règles strictes applicables aux cas dans lesquels le traitement ne sert pas à une enquête ou à des poursuites particulières. Il s'agit des cas dans lesquels des données concernant des personnes non suspectes ne peuvent être traitées que si

[1] Document de synthèse sur les services répressifs et l'échange d'informations dans l'UE, adopté par la Conférence de printemps des autorités européennes de protection des données, Cracovie (Pologne), 25-26 avril 2005.

leur traitement est indispensable dans un but légitime, clairement défini et spécifique, se borne à apprécier la pertinence des données pour l'une des catégories indiquées à l'article 7 *bis*, paragraphe 1, points a) à d), et est limité à une période déterminée, l'utilisation ultérieure de ces données étant interdite.

Afin d'éviter les discussions sémantiques sur la distinction entre «nécessaire» (employé dans la proposition de directive et «absolument nécessaire» (employé dans le document de synthèse établi à Cracovie), le groupe a utilisé l'adjectif «indispensable» dans sa proposition d'amendement. Le libellé de la disposition vise à prendre en compte la nécessité de subordonner à une condition plus stricte le traitement des données concernant une personne non suspecte en raison de l'absence de lien, direct ou indirect, entre cette personne et une enquête ou une infraction pénale spécifiques.

Amendement proposé relatif à un nouvel article

Article 7 *bis* - Différentes catégories de personnes concernées

1. Les États membres prescrivent que les autorités compétentes ne peuvent traiter des données à caractère personnel, aux fins visées à l'article 1er, paragraphe 1, qu'en ce qui concerne les différentes catégories de personnes concernées suivantes:

a) les personnes dont il y a raisonnablement lieu de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale;

b) les personnes reconnues coupables d'une infraction pénale;

c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale;

d) les tiers à l'infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, ou une personne pouvant fournir des informations sur des infractions pénales, ou un contact ou un associé de l'une des personnes mentionnées aux points a) et b);

2. Les données à caractère personnel concernant d'autres personnes que celles visées au paragraphe 1 ne peuvent faire l'objet d'un traitement

a) que dans la mesure où ce dernier est nécessaire à l'enquête relative à une infraction pénale spécifique ou aux poursuites y afférentes, afin d'apprécier la pertinence des données pour l'une des catégories indiquées au paragraphe 1, ou

b) que si ce dernier est indispensable à des fins préventives ciblées ou à des fins d'analyse criminelle, si et aussi longtemps que ces fins sont légitimes, clairement définies et spécifiques et que le traitement se limite strictement à apprécier la pertinence des données pour l'une des catégories indiquées au paragraphe 1. Cette condition fait l'objet de réexamens réguliers, au moins tous les six mois. Toute utilisation ultérieure des données est interdite.

3. Les États membres prescrivent que des restrictions et des garanties supplémentaires s'appliquent, dans le respect de leur droit national, aux traitements ultérieurs des données à caractère personnel concernant des personnes visées au paragraphe 1, points c) et d).

3. Les droits des personnes concernées

Les divers éléments de la législation relative à la protection des données s'articulent autour de trois grands acteurs: les responsables du traitement (et leurs sous-traitants), les autorités de contrôle et les personnes concernées. Tant le règlement que la directive accordent à cette dernière catégorie de personnes une série de droits qui peuvent être exercés sur demande, notamment le droit à l'information, le droit d'accès aux données et le droit de rectifier ou de supprimer des données erronées ou traitées illégalement. Dans le règlement, ces droits font l'objet d'une mise en œuvre relativement libérale, le nombre d'exceptions possibles étant limité. Dans la directive, la situation est différente, également en raison de la nature du secteur répressif concerné. On comprend aisément que les autorités policières et judiciaires ne puissent pas toujours afficher une parfaite transparence quant à leurs modes de traitement des données et quant aux types de données à caractère personnel figurant dans leurs fichiers, car les enquêtes en cours pourraient être compromises.

Le groupe estime parallèlement que les exemptions et restrictions actuellement applicables aux droits des personnes concernées sont trop larges. Il n'est en particulier pas défendable que, sans autre explication, les États membres soient autorisés à soustraire au droit d'accès des catégories entières de données à caractère personnel. En conséquence, il conviendrait de supprimer l'article 11, paragraphe 5, et l'article 13, paragraphe 2. Le groupe insiste sur le fait que toute restriction des droits de la personne concernée devrait toujours être décidée au cas par cas, en tenant compte des circonstances particulières dans lesquelles s'inscrit la demande. La décision prise pourrait, par exemple, ne consister qu'en un refus partiel de la demande. Par ailleurs, le groupe reste d'avis que les dérogations à un droit fondamental devraient toujours faire l'objet d'une interprétation restrictive.

4. L'utilisation des analyses d'impact sur la vie privée dans le secteur répressif

Dans sa première réaction à la proposition de directive, le groupe a déjà vivement recommandé au législateur européen d'insérer dans la directive des dispositions exigeant la réalisation d'analyses d'impact sur la protection des données, y compris pendant la procédure législative. La réalisation de ce type d'analyses est d'autant plus importante à l'égard des traitements de données à caractère personnel effectués à des fins répressives, notamment au vu des risques accrus que comportent ces traitements pour les personnes. Le groupe ne comprend pas en quoi le secteur répressif se distinguerait fondamentalement des autres secteurs visés dans le règlement, dans lesquels des analyses d'impact sur la protection des données sont exigées pour apprécier les risques de nouvelles opérations de traitement envisagées. Dans ce domaine, il est extrêmement important de prévoir des garanties globales applicables au traitement des données à caractère personnel et ces garanties devraient donc être envisagées et mises en œuvre avant le début du traitement.

Le groupe est par conséquent satisfait des amendements 27, 28, 110 et 113 proposés par le rapporteur du Parlement européen, qui imposent au secteur répressif des obligations en matière d'analyse d'impact sur la protection des données, largement comparables aux obligations déjà instaurées dans le règlement. Cette mesure importante pour assurer aux personnes une meilleure protection de leurs droits fondamentaux, même dans un environnement bien informé comme le secteur répressif, devrait également être incluse dans l'approche générale du Conseil à l'égard de la proposition de directive.

Il y a toutefois un point sur lequel l'avis du groupe diverge de celui du rapporteur. Dans ses amendements du considérant 41 et de l'article 25, paragraphe 2, le rapporteur introduit une obligation, imposée aux autorités de protection des données, d'évaluer toutes les analyses d'impact sur la protection des données et de formuler «des propositions appropriées afin de remédier à [toute] non-conformité». Le groupe considère que les autorités de contrôle ne devraient procéder que s'il y a lieu à une évaluation des analyses d'impact sur la protection des données.

5. Les pouvoirs des autorités de protection des données

La décision-cadre en vigueur, qui relève du troisième pilier, contient peu de dispositions consacrées aux missions et aux pouvoirs des autorités de protection des données, ainsi qu'aux possibilités et/ou obligations de coopération dans l'exercice des missions de contrôle et de répression. La proposition de directive représente à cet égard une grande avancée. Elle contient non seulement des dispositions soulignant la nécessité de disposer d'une autorité indépendante pour contrôler toutes les opérations de traitement des données qui se déroulent dans le cadre de la directive, mais aussi un chapitre spécifique sur la coopération entre ces autorités. Le groupe est favorable à l'esprit général de ces dispositions.
Malheureusement, les dispositions de la directive sont bien moins précises que celles de la proposition de règlement. Dans son avis général sur le paquet législatif, le groupe de travail «Article 29» a donc déjà indiqué la nécessité de permettre aux autorités de contrôle d'avoir accès à tous les locaux. Il a également souligné la nécessité de rapprocher les dispositions des deux instruments pour assurer la cohérence du cadre juridique de la protection des données. Cet aspect est particulièrement important à l'égard de la nécessaire coopération entre les autorités chargées de la protection des données. Si ces autorités ne possèdent pas des pouvoirs similaires dans toute l'Union européenne, il pourrait être très difficile de préserver les droits des citoyens. Il pourrait arriver qu'une autorité soit habilitée, en vertu de sa législation d'exécution nationale, à entrer dans les locaux d'un service répressif pour y effectuer une inspection sans avoir préalablement obtenu le consentement de ce service, tandis qu'une autre autorité d'un pays voisin pourrait ne pas avoir ce pouvoir et donc se voir refuser l'accès à ces locaux.

En ce qui concerne la situation des autorités de protection des données en matière d'information, la coopération pourrait se révéler d'autant plus compliquée si les pouvoirs de ces autorités restent non harmonisés, comme c'est le cas actuellement. Une étude menée par le groupe de travail «Article29» indique que certaines autorités chargées de la protection des données ont accès, en application d'une disposition particulière de droit national, à l'ensemble des informations et documents qu'elles demandent, qu'ils soient publics, confidentiels ou classifiés, afin d'accomplir leurs missions de contrôle des traitements de données effectués à des fins répressives. Dans le cas d'autres autorités, un tel accès n'est accordé à leur personnel que s'il a obtenu une habilitation de sécurité délivrée par les services de renseignement

compétents. D'autres autorités encore ne disposent d'absolument aucun accès aux informations confidentielles et/ou classifiées.

Par conséquent, si la directive impose aux autorités chargées de la protection des données de coopérer, il importe que toutes aient accès aux mêmes informations. Dans le cas contraire, elles pourraient ne pas avoir une vue d'ensemble des circonstances d'une affaire particulière et ne pas tirer la même conclusion, peut-être au détriment des intérêts de la personne concernée. Le groupe de travail «Article 29» propose donc que la directive mentionne les types d'informations dont l'accès doit être accordé aux autorités chargées de la protection des données pour l'exercice de leurs missions de contrôle. Cette proposition n'a pas pour but d'abaisser les seuils d'accès aux informations classifiées dont bénéficient actuellement les autorités de protection des données.

Plus généralement, le groupe accueille favorablement les propositions faites par le rapporteur du Parlement européen sur les pouvoirs des autorités chargées de la protection des données et approuve la description plus détaillée de ces pouvoirs qu'il propose. L'amendement ci-après doit être envisagé comme un complément à ces propositions.

Amendement proposé

Article 46 – Pouvoirs (paragraphes à ajouter)

1. Les États membres veillent à ce que chaque autorité de contrôle possède un pouvoir d'enquête lui permettant d'obtenir du responsable du traitement ou du sous-traitant l'accès à tous ses locaux, y compris à tous les équipements et moyens de traitement des données.
2. Les États membres veillent à ce que chaque autorité de contrôle se voit communiquer l'ensemble des informations et des documents nécessaires à l'exercice de ses pouvoirs d'enquête. Aucune obligation de confidentialité ne peut être opposée aux demandes des autorités de contrôle, à l'exception de l'obligation de secret professionnel visée à l'article 43.
3. Les États membres peuvent, conformément à leur droit national, subordonner à une enquête de sécurité supplémentaire l'accès aux informations classifiées à un niveau correspondant à «CONFIDENTIEL UE» ou à un niveau supérieur. Si aucun autre contrôle de sécurité n'est requis au titre de la législation de l'État membre de l'autorité de contrôle, ce fait doit être reconnu par tous les autres État membres.

Fait à Bruxelles, le 26 février 2013.

Pour le groupe de travail
Le président
Jacob KOHNSTAMM