Avis du Contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

(2011/C 101/04)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu 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 ([1]),

vu la demande d'un avis conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ([2]),

A ADOPTÉ LE PRÉSENT AVIS:

I. INTRODUCTION

Description de la proposition

1. Le 30 septembre 2010, la Commission a adopté une proposition de règlement du Parlement européen et du Conseil concernant l'ENISA, l'Agence européenne chargée de la sécurité des réseaux et de l'information ([3]).

2. L'ENISA a été instituée en mars 2004 par le règlement (CE) n° 460/2004 ([4]) pour une durée initiale de cinq ans. En 2008, son mandat a été prolongé jusqu'en mars 2012 par le règlement (CE) n° 1007/2008 ([5]).

3. Comme il ressort de l'article premier, paragraphe 1, du règlement (CE) n° 460/2004, l'Agence a été instituée pour assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et pour contribuer au bon fonctionnement du marché intérieur.

4. La proposition de la Commission a pour objet de moderniser l'Agence, d'élargir ses compétences et de lui accorder un nouveau mandat de cinq ans garantissant la continuité de ses activités au-delà de mars 2012 ([6]).

5. Le règlement proposé trouve son fondement juridique dans l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE) ([7]), qui accorde à l'Union la compétence d'adopter des mesures destinées à établir ou assurer le fonctionnement du marché intérieur. L'article 114 du TFUE remplace l'article 95 de l'ancien traité CE sur lequel se fondaient les précédents règlements concernant l'ENISA ([8]).

6. La note explicative qui accompagne la proposition précise que l'obligation de prévenir et de combattre la criminalité est devenue une compétence commune depuis l'entrée en vigueur du traité de Lisbonne. Cela a donné à l'ENISA la possibilité de jouer un rôle de plateforme concernant les aspects de sécurité des réseaux et de l'information (*Network Information Security* — NIS) en matière de lutte contre la cybercriminalité et d'échanger des points de vue et des bonnes pratiques avec les autorités chargées de la cyberdéfense, du respect de la loi et de la protection des données.

7. Parmi les différentes options qui se présentaient à elle, la Commission a choisi de proposer une extension des responsabilités de l'ENISA et de faire des autorités chargées du respect de la loi et de la protection des données des membres à part entière de son groupe permanent des parties prenantes. La nouvelle liste des fonctions n'inclut pas les tâches opérationnelles, mais actualise et reformule les tâches actuelles.

Consultation du CEPD

8. Le 1er octobre 2010, la proposition a été adressée au CEPD pour consultation, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Le CEPD se félicite d'avoir été consulté sur cette question et recommande que référence soit faite à cette consultation dans les considérants de la proposition, comme cela se fait généralement dans les textes législatifs sur lesquels il est consulté conformément au règlement (CE) n° 45/2001.

9. Avant l'adoption de la proposition, le CEPD a été consulté de manière officieuse et a formulé plusieurs commentaires informels. Toutefois, il n'a été tenu compte d'aucune de ces remarques dans la version finale de la proposition.

Évaluation générale

10. Le CEPD souligne le fait que la sécurité du traitement des données est un élément primordial de la protection des données ([9]). À cet égard, il se dit favorable à l'objectif de

([1]) JO L 281 du 23.11.1995, p. 31.
([2]) JO L 8 du 12.1.2001, p. 1.
([3]) COM(2010) 521 final
([4]) JO L 77 du 13.3.2004, p. 1.
([5]) JO L 293 du 31.10.2008, p. 1.
([6]) Pour éviter tout vide juridique au cas où la procédure législative au Parlement européen et au Conseil se prolongerait au-delà de la date d'expiration du mandat actuel, la Commission a adopté, le 30 septembre 2010, une deuxième proposition de modification du règlement (CE) n° 460/2004 visant uniquement à repousser de 18 mois la date limite du mandat actuel. Voir COM(2010) 520 final.
([7]) Cf. supra.
([8]) Le 2 mai 2006, la Cour de Justice a rejeté un recours en annulation du précédent règlement (CE) n° 460/2004 qui contestait sa base juridique (Affaire C-217/04).
([9]) Les exigences en matière de sécurité sont précisées dans les articles 22 et 35 du règlement (CE) n° 45/2001, les articles 16 et 17 de la directive 95/46/CE et les articles 4 et 5 de la directive 2002/58/CE.

la proposition visant à renforcer les compétences de l'Agence de manière à permettre à cette dernière d'assumer plus efficacement ses tâches et responsabilités actuelles, et d'étendre le champ de ses activités. Le CEPD se félicite en outre de l'implication des autorités chargées de la protection des données et des organes répressifs en tant que membres de plein droit du groupe des parties prenantes. Il considère que l'extension du mandat de l'ENISA est un moyen d'encourager, à l'échelon européen, la gestion professionnelle et harmonisée relative aux mesures de sécurité des systèmes d'information.

11. L'évaluation globale de la proposition est positive. Toutefois, sur plusieurs points, le règlement proposé manque de clarté ou est incomplet, ce qui suscite quelques inquiétudes du point de vue de la protection des données. Ces aspects sont examinés et évalués dans le chapitre suivant du présent avis.

II. **COMMENTAIRES ET RECOMMANDATIONS**

Les attributions élargies de l'ENISA ne sont pas suffisamment claires

12. Les attributions élargies de l'Agence relativement à la participation des organes répressifs et des autorités chargées de la protection des données sont formulées de manière très générale dans l'article 3 de la proposition. La note explicative est plus explicite à cet égard. Elle fait allusion à l'interaction de l'ENISA avec les organes de répression de la cybercriminalité et la réalisation de tâches non opérationnelles dans la lutte contre la cybercriminalité. Toutefois, ces tâches ne figurent pas dans l'article 3 ou n'y sont mentionnées qu'en termes très généraux.

13. Pour éviter toute incertitude juridique, le règlement proposé doit exposer clairement et sans ambiguïté les tâches de l'ENISA. Comme cela a déjà été souligné, la sécurité du traitement des données est un élément primordial de la protection des données. L'ENISA jouera un rôle de plus en plus important dans ce domaine. Les citoyens, institutions et organes doivent savoir clairement quels types d'activités peuvent être assurés par l'ENISA. Cet aspect serait même encore plus important au cas où les attributions élargies de l'ENISA incluraient le traitement de données à caractère personnel (voir les points 17 à 20 ci-dessous).

14. L'article 3, paragraphe 1, point k), de la proposition précise que l'Agence doit assurer toute autre tâche qui lui est confiée par les actes législatifs de l'Union. Le CEPD exprime des craintes quant à cette clause non limitative qui constitue une faille susceptible d'altérer la cohérence des instruments juridiques et d'entraîner un détournement de la vocation de l'Agence.

15. Une des tâches mentionnées à l'article 3, paragraphe 1, point k), de la proposition figure dans la directive 2002/58/CE ([1]). Elle prévoit que la Commission est tenue de consulter l'Agence sur toutes mesures techniques de mise en œuvre applicables aux notifications dans le contexte des violations de données. Le CEPD recommande que cette activité de l'Agence soit décrite de façon plus détaillée et se limite au domaine de la sécurité. Compte tenu de l'impact potentiel de l'ENISA sur l'élaboration des stratégies dans ce domaine, cette activité doit être précisée et occuper une place plus importante dans le règlement proposé.

16. Le CEPD recommande en outre l'inclusion d'une référence à la directive 1999/5/CE ([2]) dans le considérant 21 compte tenu de la tâche particulière mentionnée à l'article 3, paragraphe 1, point c), de la proposition, selon lequel l'ENISA doit assister les États membres et les institutions et organismes européens dans leurs efforts pour recueillir, analyser et diffuser des données sur la sécurité des réseaux et de l'information. Cela devrait alimenter les exercices promotionnels de l'ENISA en faveur des bonnes pratiques et techniques en matière de sécurité des réseaux et de l'information (*Network Information Security* — NIS) en illustrant mieux les éventuelles interactions constructives entre l'Agence et les organismes de normalisation.

Il convient de préciser si des données à caractère personnel seront traitées par l'Agence

17. La proposition ne précise pas si les tâches attribuées à l'Agence peuvent inclure le traitement de données à caractère personnel. Elle ne comporte par conséquent pas de base juridique pour le traitement de données à caractère personnel au sens de l'article 5 du règlement (CE) n° 45/2001.

18. Toutefois, certaines des tâches attribuées à l'Agence peuvent comporter (au moins dans une certaine mesure) le traitement de données à caractère personnel. Par exemple, il n'est pas exclu que l'analyse d'incidents de sécurité et d'atteintes à la protection des données ou l'exécution de tâches non opérationnelles dans le cadre de la lutte contre la cybercriminalité entraînent la collecte et l'analyse de données à caractère personnel.

19. Le considérant 9 de la proposition renvoie aux dispositions de la directive 2002/21/CE ([3]) établissant que, le cas échéant, notification est faite à l'Agence par les autorités réglementaires nationales en cas d'atteintes à la sécurité. Le CEPD recommande que la proposition fournisse davantage de détails sur les notifications qui doivent être adressées à l'ENISA et sur la façon dont l'ENISA doit y répondre. De même, la proposition doit tenir compte des implications que l'analyse de ces notifications (le cas échéant) peut avoir sur le traitement de données à caractère personnel.

([1]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) JO L 201 du 31.7.2002, p. 37.

([2]) Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, JO L 91 du 7.4.1999, p. 10, et notamment son article 3, paragraphe 3, alinéa c).

([3]) Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre», JO L 108 du 24.4.2002, p. 33).

20. Le CEPD invite le législateur à préciser si les activités de l'ENISA énumérées dans l'article 3 incluront le traitement de données à caractère personnel et, dans l'affirmative, lesquelles.

Nécessité de préciser les règles internes de sécurité de l'ENISA

21. Bien que l'ENISA joue un rôle important dans la discussion sur la sécurité des réseaux et de l'information en Europe, la proposition ne fait pratiquement pas état de la mise en place de mesures de sécurité pour l'Agence proprement dite (qu'elles soient ou non liées au traitement de données à caractère personnel).

22. Le CEPD estime que l'Agence sera encore mieux placée pour promouvoir les bonnes pratiques relatives à la sécurité du traitement des données si de telles mesures de sécurité sont strictement appliquées en interne par l'Agence elle-même. Cela favorisera la reconnaissance de l'Agence non seulement comme centre d'expertise mais également comme point de référence pour la mise en œuvre pratique des meilleures techniques disponibles dans le domaine de la sécurité. La recherche de l'excellence dans la mise en œuvre des pratiques de sécurité doit par conséquent être inscrite dans le règlement régissant les procédures de travail de l'Agence. Le CEPD suggère donc d'ajouter à la proposition une disposition allant dans ce sens, par exemple en exigeant que l'Agence applique les meilleures techniques disponibles, c'est-à-dire les procédures de sécurité les plus modernes et les plus efficaces, ainsi que leurs modes d'opération.

23. Cette approche permettra à l'Agence de donner des conseils sur l'adéquation pratique de techniques particulières visant à offrir les garanties de sécurité nécessaires. De plus, la mise en œuvre de ces meilleures pratiques doit donner la priorité à celles qui garantissent la sécurité tout en minimisant, autant que possible, leur impact sur la vie privée. Il faudra choisir les techniques correspondant le mieux au concept de *privacy by design* (respect de la vie privée dès la conception).

24. Même avec une approche moins ambitieuse, le CEPD recommande, au minimum, que le règlement contienne les exigences suivantes: i) la création d'une politique de sécurité interne faisant suite à une évaluation approfondie des risques et tenant compte des normes internationales et des meilleures pratiques appliquées dans les États membres; ii) la nomination d'un délégué à la sécurité chargé de mettre en œuvre cette politique et disposant des ressources et de l'autorité nécessaires; iii) l'approbation de cette politique après un examen approfondi du risque résiduel et des contrôles proposés par le conseil d'administration; et iv) un examen périodique de la politique avec spécification de la périodicité choisie et des objectifs de l'examen.

Nécessité de mieux définir les mécanismes de coopération avec les autorités de protection des données (y compris le CEPD) et le groupe de travail «Article 29»

25. Comme cela a été souligné ci-dessus, le CEPD se félicite de l'élargissement du mandat de l'Agence et est persuadé que les autorités de protection des données pourront tirer grand profit de son existence (tout comme l'Agence bénéficie de l'expertise de ces autorités). Compte tenu de la convergence naturelle et logique entre sécurité et protection des données, l'Agence et les autorités de protection des données sont appelées à agir en étroite collaboration.

26. Les considérants 24 et 25 font référence à la proposition de directive de l'UE sur la cybercriminalité et mentionnent qu'il conviendrait que l'Agence se concerte avec les autorités répressives et celles chargées de la protection de la vie privée pour dégager les aspects «sécurité des réseaux et de l'information» de la lutte contre la cybercriminalité ([1]).

27. La proposition doit également prévoir des mécanismes de collaboration concrets i) garantissant la cohérence des activités de l'Agence avec celles des autorités chargées de la protection des données; et ii) permettant une coopération étroite entre l'Agence et les autorités de protection des données.

28. En ce qui concerne la cohérence, le considérant 27 fait explicitement référence au fait que les activités de l'Agence ne doivent pas entrer en conflit avec les autorités chargées de la protection des données des États membres. Le CEPD se félicite de cette référence mais constate qu'aucune référence n'est faite au CEPD et au groupe de travail «Article 29». Le CEPD recommande au législateur d'inclure également, dans la proposition, une disposition similaire de non-interférence concernant ces deux entités. Cela créera un environnement de travail plus clair pour toutes les parties et structurera les voies et mécanismes de collaboration qui permettront à l'Agence d'aider les différentes autorités de protection des données et le groupe de travail «Article 29».

29. De même, en ce qui concerne la coopération étroite, le CEPD se félicite de l'inclusion d'une représentation des autorités chargées de la protection des données dans le groupe permanent des parties prenantes qui conseillera l'Agence dans ses activités. Il recommande qu'il soit explicitement mentionné que les représentants des autorités nationales de protection des données soient nommés par l'Agence sur la base d'une proposition du groupe de travail «Article 29». Il serait également souhaitable d'inclure une référence prévoyant la présence du CEPD, à ce titre, aux réunions au cours desquelles les questions concernant la coopération avec le CEPD doivent être examinées. En outre, le CEPD recommande que l'Agence (conseillée par le groupe permanent de parties prenantes et avec l'approbation du conseil d'administration) mette en place des groupes de travail ad hoc pour les différents sujets sur lesquels la protection des données et la sécurité se chevauchent, afin de mieux cadrer cet effort de coopération étroite.

([1]) Proposition de diretive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil, COM(2010) 517 final.

30. Enfin, pour éviter tout malentendu, le CEPD recommande d'utiliser l'expression «autorités de protection des données» plutôt que l'expression «autorité de protection de la vie privée» et de préciser ce que sont ces autorités en faisant référence à l'article 28 de la directive 95/46/CE, ainsi qu'au CEPD conformément aux dispositions du chapitre V du règlement (CE) nº 45/2001.

Il n'est pas établi clairement quels bénéficiaires peuvent demander l'aide de l'ENISA

31. Le CEPD constate une incohérence dans le règlement proposé relativement à ceux qui peuvent demander l'aide de l'ENISA. Il ressort des considérants 7, 15, 16, 18 et 36 de la proposition, que l'ENISA peut assister les organes des États membres et l'Union dans son ensemble. Toutefois, l'article 2, paragraphe 1, ne fait référence qu'à la Commission et aux États membres, alors que l'article 14 restreint les demandes d'assistance: i) au Parlement européen; ii) au Conseil; iii) à la Commission; et iv) à tout organisme compétent désigné par un État membre et ignore certains organes, institutions, agences et bureaux de l'Union.

32. L'article 3 de la proposition est plus spécifique et envisage différents types d'assistance en fonction des types de bénéficiaires: i) collecte et analyse de données sur la sécurité de l'information (dans le cas des États membres et des institutions et organismes européens); ii) analyse ponctuelle de la sécurité des réseaux et de l'information en Europe (dans le cas des États membres et des institutions européennes); iii) promotion du recours à la gestion des risques et aux bonnes pratiques de sécurité (dans toute l'Union et tous les États membres); iv) développement de la détection de sécurité des réseaux et de l'information (dans les institutions et organes européens); et v) collaboration au dialogue et coopération avec les pays tiers (dans le cas de l'Union).

33. Le CEPD invite le législateur à remédier à cette incohérence et à harmoniser les dispositions susmentionnées. À cet égard, il recommande que l'article 14 soit modifié de manière à inclure tous les organes, institutions, bureaux et agences de l'Union et à indiquer clairement le type d'assistance pouvant être demandé par les différentes entités de l'Union (au cas où cette différenciation serait envisagée par le législateur). De même, il est recommandé que certaines entités publiques et privées puissent demander l'assistance de l'Agence à condition que le soutien demandé présente clairement un intérêt du point de vue européen et qu'il soit conforme aux objectifs de l'Agence.

Attributions du conseil d'administration

34. La note explicative prévoit un élargissement des compétences du conseil d'administration dans son rôle de surveillance. Le CEPD se félicite de ce rôle accru et recommande que plusieurs aspects concernant la protection des données soient inclus dans les attributions du conseil d'administration. Par ailleurs, le CEPD recommande que le règlement précise, sans la moindre ambiguïté, qui est habilité à: i) définir les dispositions d'application du règlement (CE) nº 45/2001 par l'Agence, y compris celles concernant la nomination d'un délégué à la protection des données; ii) approuver la politique de sécurité et ses révisions périodiques ultérieures; et iii) déterminer le protocole de coopération avec les autorités de protection des données et les organes chargés du respect de la loi.

Applicabilité du règlement (CE) nº 45/2001

35. Bien que le règlement (CE) nº 45/2001 l'exige déjà, le CEPD suggère d'inclure dans l'article 27 la nomination du délégué à la protection des données, dans la mesure où cela revêt une importance particulière, et de l'accompagner par la mise en place rapide de dispositions d'application concernant la portée des compétences et tâches à confier au délégué à la protection des données conformément à l'article 24, paragraphe 8, du règlement (CE) nº 45/2001. Plus concrètement, l'article 27 pourrait être formulé comme suit:

1) les informations traitées par l'Agence conformément au présent règlement sont soumises aux dispositions du règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données;

2) le conseil d'administration définit les dispositions d'application du règlement (CE) nº 45/2001 par l'Agence, y compris celles qui concernent le délégué à la protection des données à l'Agence.

36. Au cas où une base juridique spécifique serait nécessaire pour le traitement de données à caractère personnel, comme nous l'avons vu aux points 17-20 ci-dessus, elle devrait également préciser les garanties, restrictions et conditions appropriées en vertu desquelles un traitement aurait lieu.

III. **CONCLUSIONS**

37. L'évaluation globale de la proposition est positive et le CEPD se félicite de l'élargissement du mandat et des attributions de l'Agence grâce à l'implication des autorités de protection des données et des organismes chargés du respect de la loi en tant que parties prenantes de plein droit. Le CEPD estime que la continuité de l'Agence encouragera, au niveau européen, la gestion professionnelle et harmonisée des mesures de sécurité appliquées aux systèmes d'information.

38. Pour éviter toute incertitude juridique, le CEPD recommande que la proposition soit clarifiée quant à l'élargissement des tâches de l'Agence et en particulier de celles qui concernent la participation des organes répressifs et des autorités de protection des données. Par ailleurs, le CEPD attire l'attention sur la faille potentielle créée par l'inclusion, dans la proposition, d'une disposition permettant, par tout autre acte législatif de l'Union, d'ajouter de nouvelles attributions à l'Agence sans restrictions supplémentaires.

39. Le CEPD invite le législateur à préciser si les activités de l'ENISA incluront le traitement de données à caractère personnel et, si oui, lesquelles.

40. Le CEPD recommande d'inclure des dispositions concernant la mise en place d'une politique de sécurité pour l'Agence elle-même, afin de renforcer le rôle de cette dernière comme catalyseur de l'excellence en matière de pratiques de sécurité et comme promoteur du concept de *privacy by design* (respect de la vie privée dès la conception) en intégrant l'application des meilleures techniques disponibles dans le domaine de la sécurité, avec le respect des droits à la protection des données à caractère personnel.

41. Les mécanismes de coopération avec les autorités de protection des données, y compris avec le CEPD et le groupe de travail «Article 29», doivent être mieux définis en vue d'assurer la cohérence et la coopération étroite.

42. Le CEPD invite le législateur à remédier à certaines incohérences quant aux restrictions exprimées à l'article 14 en ce qui concerne la capacité de demander l'assistance de l'Agence. En particulier, le CEPD recommande que ces restrictions soient abandonnées et que tous les organes, institutions, bureaux et agences de l'Union puissent demander l'assistance de l'Agence.

43. Enfin, le CEPD recommande que les compétences élargies du conseil d'administration incluent certains aspects concrets pouvant accroître la garantie que l'Agence appliquera de bonnes pratiques de protection de la sécurité et des données. Entre autres, il est proposé d'inclure la nomination d'un délégué à la protection des données et l'approbation de mesures visant à assurer la bonne application du règlement (CE) n° 45/2001.

Fait à Bruxelles, le 20 décembre 2010.

Giovanni BUTTARELLI

Contrôleur européen adjoint de la protection des données