AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur la décision 2011/141/UE de la Commission modifiant la décision 2007/76/CE de la Commission concernant le système de coopération en matière de protection des consommateurs («SCPC») et sur la recommandation 2011/136/UE de la Commission concernant les lignes directrices régissant l'application de règles relatives à la protection des données au SCPC

(2011/C 217/06)

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'avis formulée 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 L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 1er mars 2011, la Commission européenne a adopté une décision modifiant sa décision 2007/76/CE concernant le SCPC (ci-après la «deuxième modification de la CPC») [3]. Le même jour, la Commission a également adopté une recommandation concernant les lignes directrices régissant l'application de règles relatives à la protection des données au SCPC (ci-après «les lignes directrices en matière de protection des données dans le cadre de la CPC») [4]. Ces deux documents ont été transmis au CEPD pour consultation conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001.

2. Le SCPC est un système informatique conçu et exploité par la Commission conformément au règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs (ci-après le «règlement CPC»). Le SCPC facilite la coopération entre les «autorités compétentes» des États membres de l'UE et la Commission dans le domaine de la protection des consommateurs, pour ce qui est des infractions à une série préétablie de directives et de règlements de l'UE. Pour relever du champ d'application du règlement CPC, les infractions doivent être de nature transfrontalière et porter préjudice aux «intérêts collectifs des consommateurs».

3. Dans le cadre de leur coopération, les utilisateurs du SCPC échangent des informations, y compris des données à caractère personnel. Celles-ci peuvent se rapporter aux directeurs ou aux salariés d'un vendeur ou d'un fournisseur soupçonné d'infraction, au vendeur ou au fournisseur lui-même (s'il s'agit d'une personne physique) ainsi qu'à des tiers tels que des consommateurs ou des plaignants.

4. Le système est conçu comme un outil de communication sécurisé entre autorités compétentes ainsi que comme une base de données. Le SCPC est utilisé par les autorités compétentes pour demander des informations susceptibles de les aider à instruire une affaire [5] ou pour demander de l'aide en matière d'exécution [6] («demandes d'assistance mutuelle»). Les autorités compétentes peuvent en outre envoyer un message d'avertissement («alerte») pour informer d'autres autorités compétentes et la Commission d'une infraction avérée ou présumée [7]. Le SCPC comprend d'autres fonctions, notamment un système de

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] Décision de la Commission du 1er mars 2011 modifiant la décision 2007/76/CE portant application du règlement (CE) n° 2006/2004 du Parlement européen et du Conseil relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs en ce qui concerne l'assistance mutuelle (2011/141/UE) (JO L 59 du 4.3.2011, p. 63).
[4] Recommandation de la Commission du 1er mars 2011 concernant les lignes directrices régissant l'application de règles relatives à la protection des données au système de coopération en matière de protection des consommateurs (SCPC) (2011/136/UE) (JO L 57 du 2.3.2011, p. 44).
[5] Voir l'article 6 du règlement CPC relatif à l'«échange d'informations sur demande».
[6] Voir l'article 8 du règlement CPC relatif aux «demandes de mesures d'exécution».
[7] Voir l'article 7 du règlement CPC relatif à l'«échange d'informations sans demande préalable» (ou «alerte» en abrégé).

notification ([8]) et un forum d'échanges de données qui ne sont pas liées à des affaires.

5. Dans le présent avis, le CEPD aborde un certain nombre de questions liées à la protection des données qui concernent le cadre juridique du SCPC, en se concentrant essentiellement sur la deuxième modification de la CPC récemment adoptée. Le CEPD fait également le point sur les progrès réalisés à ce jour et met en exergue certaines autres préoccupations et considérations pour l'avenir. Il commente aussi certaines dispositions des lignes directrices en matière de protection des données dans le cadre de la CPC.

6. Parallèlement au présent avis [adopté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001], le CEPD publie également un avis sur la notification d'un contrôle préalable dans le cadre de sa mission de supervision (conformément à l'article 27 dudit règlement) (ci-après l'«avis sur la notification d'un contrôle préalable»). L'avis sur la notification d'un contrôle préalable comporte une description plus détaillée du SCPC ainsi que du traitement de données à caractère personnel qu'il implique. Dans cet avis, le CEPD recommande principalement d'adopter des mesures spécifiques sur le plan pratique, technique et organisationnel afin de renforcer le respect de la protection des données dans le SCPC. Étant donné que les lignes directrices en matière de protection des données dans le cadre de la CPC sont aussi étroitement liées à ces mesures spécifiques, l'avis sur la notification d'un contrôle préalable commentera également certaines dispositions des lignes directrices.

II. CADRE JURIDIQUE DU SCPC

7. Le CEPD note avec satisfaction que le SCPC repose sur une base juridique solide, notamment un règlement adopté par le Conseil et le Parlement. Le CEPD se félicite en outre que la base juridique ait été complétée au fil du temps afin de fournir de plus amples précisions et de régler certains problèmes liés à la protection des données. Plus particulièrement, le CEPD se réjouit de constater que la décision 2007/76/CE de la Commission du 22 décembre 2006 mettant en œuvre la CPC (ci-après la «décision mettant en œuvre la CPC») a été adoptée et modifiée ultérieurement le 17 mars 2008, et plus récemment encore, le 1er mars 2011 par la deuxième modification de la CPC. Il est heureux d'apprendre que la Commission a adopté les lignes directrices en matière de protection des données dans le cadre de la CPC, qui traitent spécifiquement de problèmes liés à la protection des données.

8. Bien qu'il regrette de ne pas avoir été consulté au moment où le règlement CPC et la décision mettant en œuvre la CPC ont été initialement adoptés, il se félicite que la Commission l'ait consulté à l'occasion de l'adoption de chacune des deux modifications de la décision mettant en œuvre la CPC ainsi qu'au sujet des lignes directrices en matière de protection des données dans le cadre de la CPC. Le CEPD se réjouit de même que la Commission ait également consulté au préalable le groupe de travail sur la protection des données institué par l'article 29 (ci-après «GT 29»), qui a publié le 21 septembre 2007 son avis nº 6/2007 (GT 139). Enfin, le CEPD se félicite que les considérants des lignes directrices en matière de protection des données dans le cadre de la CPC fassent référence à ces consultations.

9. Le CEPD note que: i) la Commission a soigneusement examiné les recommandations formulées par le CEPD dans une correspondance informelle antérieure ainsi que celles émises par le GT 29 dans son avis nº 6/2007; et que ii) bon nombre de ces recommandations ont été observées lors de l'amélioration du cadre législatif du SCPC et/ou sur le plan pratique, technique et organisationnel. Les observations qu'il formule dans le présent avis ainsi que dans son avis sur la notification d'un contrôle préalable doivent être considérées dans ce contexte positif.

III. QUESTIONS LIÉES À LA PROTECTION DES DONNÉES EN CE QUI CONCERNE LA DEUXIÈME MODIFICATION DE LA CPC

3.1. Conservation de données à caractère personnel dans le SCPC

3.1.1. *Introduction*

10. À titre préliminaire, le CEPD fait remarquer que les questions des classements d'affaires et des périodes de conservation n'ont pas été abordées de manière adéquate et complète dans le règlement CPC ([9]).

11. En effet, le règlement CPC n'établit que deux règles spécifiques concernant la suppression de données et n'en prévoit aucune pour ce qui est des classements d'affaires ([10]). Premièrement, il dispose que si une alerte «s'avère infondée», l'autorité compétente doit la retirer et la Commission supprimer sans délai l'information de la base de données. Deuxièmement, il dispose que lorsqu'une autorité requise notifie, en vertu de l'article 8, paragraphe 6, du règlement CPC, qu'une infraction a cessé, les données stockées doivent être supprimées cinq ans après la notification.

12. Le règlement CPC n'établit pas la finalité de la période de conservation de cinq ans. Il ne fournit pas davantage de précisions quant à la manière dont il convient d'apprécier si une alerte est «infondée», ni à quel moment cette appréciation doit avoir lieu. En outre, le règlement CPC ne dit mot sur la durée pendant laquelle les informations doivent rester dans la base de données dans les cas qui ne sont pas couverts par les deux règles spécifiques précitées (par exemple, le règlement ne précise pas pendant combien de temps les demandes d'assistance mutuelle sont conservées

([8]) Voir l'article 7, paragraphe 2, et l'article 8, paragraphe 6, du règlement CPC.

([9]) Voir aussi l'avis nº 6/2007 du groupe de travail sur la protection des données institué par l'article 29 (cité au chapitre II ci-dessus).

([10]) Voir l'article 10, paragraphe 2, du règlement CPC.

dans la base de données si elles n'ont pas donné lieu à une mesure d'exécution menée à bien qui aurait entraîné la cessation de l'infraction).

13. Le CEPD se réjouit de constater que la décision mettant en œuvre la CPC, telle que modifiée, et les lignes directrices en matière de protection des données dans le cadre de la CPC tentent de fournir de plus amples précisions. Cela dit, le CEPD reste préoccupé par plusieurs aspects des règles concernant les classements d'affaires et la conservation de données dans le SCPC, qui seront évoqués plus loin aux sections 3.1.2 à 3.1.4.

14. Le CEPD recommande de tenir compte de ces préoccupations lors de la prochaine révision du cadre juridique du SCPC, par une nouvelle modification de la décision mettant en œuvre la CPC ou, de préférence, par une modification du règlement CPC lui-même.

15. En attendant que ces mesures législatives soient possibles, le CEPD recommande que les problèmes concernant les périodes de conservation soient réglés sur le plan pratique, technique et organisationnel et qu'ils soient aussi clairement énoncés dans le document «Consumer Protection Cooperation Network: Operating Guidelines» («Le réseau de coopération pour la protection des consommateurs: lignes directrices») évoqué à la section 3.1.2 ci-dessous.

3.1.2. *Classements d'affaires en temps opportun*

16. La deuxième modification de la CPC omet de fixer la date ultime à laquelle une affaire impliquant une demande d'assistance mutuelle (demande d'information ou demande de mesures d'exécution) doit être classée.

17. Dans l'avis sur la notification d'un contrôle préalable, le CEPD prend note d'un certain nombre de mesures pragmatiques que la Commission prend actuellement pour contribuer à ce que les affaires en suspens soient classées en temps utile.

18. Dans le présent avis, le CEPD recommande de fixer des délais maximaux pour les demandes d'information et les demandes de mesures d'exécution. Ceux-ci doivent être précisés dans le cadre législatif lors de sa prochaine révision. Les délais doivent être liés au type d'affaire ainsi qu'à l'activité effective. Dans le même temps, les règles doivent donner aux autorités compétentes la latitude de prolonger l'affaire pour un motif valable, afin de garantir que certaines affaires ne soient pas classées prématurément même si le classement d'une affaire complexe prend plus de temps qu'en moyenne.

19. À cet effet, le CEPD recommande de prendre comme point de départ le document intitulé «Consumer Protection Cooperation Network: Operating Guidelines», approuvé par le comité CPC le 6 décembre 2010. Ces directives traitent, au point 2.7 intitulé «phases and time-limes in a CPC case» («phases et délais d'une affaire de CPC»), des flux d'affaires typiques et prévoient que les demandes d'informations doivent être traitées dans un délai moyen de un à trois mois. D'après ces directives, le traitement des demandes de mesures d'exécution doit être possible dans un délai moyen de six à neuf mois (à l'exception des cas d'injonctions ou de recours contre une décision administrative, dans lesquels un délai de un an ou plus est davantage réaliste).

3.1.3. *Alertes*

20. La deuxième modification de la CPC a introduit un nouveau paragraphe au point 2.2.2 de l'annexe à la décision mettant en œuvre la CPC, qui exige que les alertes «fondées» soient retirées de la base de données cinq ans après avoir été émises (quant aux alertes «non fondées», les dispositions existantes imposent déjà qu'elles soient supprimées dès qu'elles se sont «avérées infondées»).

21. Pour replacer cette nouvelle disposition dans son contexte, le CEPD insiste sur le fait qu'une de ses principales préoccupations est de veiller à ce que des données à caractère personnel ne restent pas dans la base de données du SCPC plus longtemps que nécessaire. Cette question est sensible, en particulier en ce qui concerne les alertes (dont les destinataires sont plus nombreux que les échanges bilatéraux) et, parmi ces dernières, en particulier celles qui concernent des infractions présumées. Dans la pratique, l'absence d'un délai clair pendant lequel l'alerte reste ouverte impliquerait que certaines alertes pourraient rester pendantes durant une période de temps excessivement longue (tant qu'elles ne se sont pas clairement avérées infondées). Ces mesures, basées sur des soupçons non confirmés, feraient peser des risques significatifs sur le droit fondamental à la protection des données ainsi que sur d'autres droits fondamentaux tels que la présomption d'innocence.

22. À cet égard, le CEPD constate avec plaisir qu'une période de conservation a été instaurée pour les alertes. Il considère néanmoins que la Commission n'a pas fourni de justification adéquate démontrant qu'une période de conservation de cinq ans serait proportionnée. Le CEPD recommande à la Commission de procéder à une évaluation de la proportionnalité et de réévaluer la durée de la période de conservation pour les alertes. En principe, toutes les alertes signalées devraient être supprimées de la base de données beaucoup plus tôt, sauf si une alerte relative à une infraction avérée ou présumée a donné lieu à une demande d'assistance mutuelle et si l'enquête transfrontalière ou la mesure d'exécution est encore en cours. La période de conservation doit être assez longue pour permettre à chaque autorité qui reçoit le message de déterminer si elle souhaite prendre des mesures d'enquête ou d'exécution supplémentaires, et si elle souhaite soumettre une demande d'assistance mutuelle par l'intermédiaire du SCPC. Elle doit cependant être suffisamment courte pour réduire le plus possible le risque d'utilisation abusive des alertes à des fins de chantage ou d'exploration des données.

23. Dans cette perspective, le CEPD recommande à la Commission de revoir le cadre juridique de manière à garantir que les alertes soient supprimées au plus tard six mois après avoir été téléchargées, sauf si une autre période de conservation plus appropriée peut être justifiée.

24. Cette limitation devrait contribuer à garantir notamment que, dans les affaires où la suspicion n'a pas été confirmée (ni même fait l'objet d'une enquête ultérieure), des personnes innocentes liées au soupçon ne continuent à figurer sur une «liste noire» ou ne restent «suspectes» pendant un délai excessivement long, ce qui serait contraire à l'article 6, point e), de la directive 95/46/CE.

25. Cette limitation est également nécessaire pour garantir le principe de qualité des données [voir l'article 6, point d), de la directive 95/46/CE] ainsi que d'autres principes juridiques importants. Elle ne peut que se traduire par un niveau de protection plus adéquat pour les personnes, tout en permettant aux agents des services répressifs de se concentrer plus efficacement sur les affaires intéressantes.

3.1.4. *Période de conservation pour les demandes d'assistance mutuelle classées*

26. La deuxième modification de la CPC a ajouté un nouveau paragraphe au point 2.15 de l'annexe de la décision mettant en œuvre la CPC, qui dispose que «[t]oute autre information concernant des demandes d'assistance mutuelle formulées au titre de l'article 6 du règlement (CPC) est retirée de la base de données cinq ans après le classement de l'affaire».

27. Lu en combinaison avec le texte existant, le point 2.15 révisé impose une conservation de cinq ans après le classement de l'affaire de toutes les informations échangées au titre de l'article 6 sauf:

— lorsque des données erronées ont été supprimées,

— lorsque l'échange d'informations n'a pas donné lieu à une alerte ou à une demande de mesures d'exécution, ou

— lorsqu'il a été établi qu'aucune infraction n'a eu lieu au sens du règlement CPC.

28. Comme exposé dans l'avis sur la notification d'un contrôle préalable, il semble en effet que le délai de conservation «standard» appliqué dans le SCPC, à la suite du classement d'une affaire est (sauf exceptions particulières) de cinq ans, tant pour les demandes d'information que pour les demandes de mesures d'exécution.

29. Le texte de la décision mettant en œuvre la CPC telle que modifiée par la deuxième modification de la CPC ne semble pas concorder totalement avec le règlement CPC. Ainsi, l'article 10, paragraphe 2, du règlement CPC opère une distinction entre les informations échangées qui donnent lieu à des mesures d'exécution menées à bien (c'est-à-dire les affaires pour lesquelles l'infraction a cessé à la suite des mesures d'exécution prises), d'une part, et les informations qui n'ont pas donné lieu à des mesures d'exécution menées à bien, d'autre part. Dans le premier cas, une période de conservation de cinq ans est prévue dès que l'affaire est classée. Dans le second cas, aucune disposition spécifique n'est formulée (si ce n'est que les alertes infondées doivent être retirées et supprimées).

30. En d'autres termes, le règlement CPC ne prévoit une période de conservation de cinq ans après le classement de l'affaire qu'à condition que des mesures d'exécution aient été prises et qu'elles soient parvenues à faire cesser l'infraction.

31. Bien que le CEPD ait des doutes quant à la finalité et à la proportionnalité de la conservation de n'importe quel type de données pour une période de cinq ans après le classement de l'affaire (voir ses observations formulées à la section 3.1.4 ci-dessous), la distinction entre les affaires qui se sont conclues par une exécution effective et les autres affaires présente une certaine logique du point de vue de la protection des données. Ainsi, les données concernant de simples soupçons, qui sont conservées pendant une longue période de temps, sont davantage susceptibles d'être inexactes et cette conservation risque également de violer d'autres principes juridiques importants. On peut donc dire que, de manière générale, la conservation de ce genre de données pour une longue période est davantage susceptible de soulever des questions liées à la protection des données que la conservation de données concernant des infractions réelles, qui ont été établies de manière adéquate et ont donné lieu à des mesures d'exécution.

32. Contrairement au règlement CPC, la décision mettant en œuvre la CPC telle que modifiée semble permettre, du moins dans certains cas, que la période de conservation de cinq ans s'applique également aux informations n'ayant pas donné lieu à des mesures d'exécution menées à bien.

33. Par exemple, d'après la décision mettant en œuvre la CPC, une demande d'information ayant donné lieu à une alerte mais pas à une mesure d'exécution semble rester dans le système pendant cinq ans à compter du «classement de l'affaire».

34. Le règlement CPC et la décision mettant en œuvre la CPC semblent donc suivre l'un et l'autre une approche légèrement différente. La décision mettant en œuvre la CPC, tout en reproduisant, dans une certaine mesure, les dispositions du règlement CPC, introduit aussi d'importantes règles supplémentaires en matière de conservation. Si une clarification des règles serait en soit la bienvenue, le CEPD s'interroge sur la légalité de l'établissement de périodes de conservation plus longues, alors que le règlement CPC ne le prévoit pas. Cela imposerait de nouvelles restrictions au droit fondamental à la protection des données, en mettant en œuvre une législation contraire au règlement CPC et aux lois applicables en matière de protection des données.

35. Eu égard à ce qui précède, le CEPD recommande à la Commission de revoir le cadre juridique et de réexaminer la possibilité d'appliquer la période de conservation de cinq ans aux affaires autres que celles pour lesquelles des mesures d'exécution ont été menées à bien, comme le règlement CPC le prévoit.

36. Par ailleurs, le CEPD se réjouit que les lignes directrices en matière de protection des données dans le cadre de la CPC visent à préciser la finalité de la conservation après le classement de l'affaire, une question importante qui n'avait pas été abordée par le règlement CPC et la deuxième modification de la CPC. Ainsi, ces lignes directrices prévoient que «pendant la période de conservation, les agents de l'autorité compétente qui sont chargés de veiller au respect de la législation et à qui une affaire donnée avait été initialement confiée peuvent consulter le dossier en question afin d'établir des liens avec des infractions éventuellement répétées. Une telle démarche contribue à améliorer le contrôle de l'application de la réglementation, notamment du point de vue de son efficacité» ([11]).

37. Toutefois, bien que cette clarification soit opportune, en l'absence d'une justification supplémentaire de la nécessité de cet accès, le CEPD n'est pas convaincu de la proportionnalité et de la suffisance de cette finalité pour justifier la période de conservation de cinq ans. Par conséquent, il recommande à la Commission:

— de préciser davantage la finalité de la conservation des données pendant cinq ans;

— d'évaluer si une période de conservation plus courte permettrait d'atteindre les mêmes objectifs; et

— d'évaluer si toutes les informations prévues actuellement doivent être conservées ou si une partie d'entre elles suffirait (par exemple, il convient d'examiner si la conservation des seules notifications introduites au titre de l'article 8, paragraphe 6, serait suffisante; il y a lieu également d'évaluer spécifiquement si la conservation des noms des directeurs ou des pièces jointes pouvant contenir des données supplémentaires à caractère personnel est nécessaire; une distinction doit en outre être établie entre les données liées à des infractions présumées et celles liées à des infractions «avérées»).

3.2. **L'accès de la Commission aux données du SCPC**

38. Le CEPD note avec satisfaction que la deuxième modification de la CPC (en introduisant un nouveau point 4.3 à l'annexe à la décision mettant en œuvre la CPC) précise l'accès de la Commission aux données du SCPC et que cet accès est clairement et spécifiquement limité à ce qui est nécessaire dans le cadre du règlement CPC. Le CEPD se félicite en particulier que la Commission ne se soit pas vu octroyer un accès aux communications confidentielles entre les autorités compétentes des États membres, telles que les demandes d'assistance mutuelle.

39. Cette précision et cette limitation sont particulièrement importantes, étant donné qu'un manque de clarté aurait pu donner lieu à une situation dans laquelle la Commission aurait été en mesure d'accéder à certaines informations, y compris des données à caractère personnel, qui ne sont destinées qu'aux autorités compétentes des États membres.

40. Ainsi qu'on peut le lire à la section 5 des lignes directrices en matière de protection des données dans le cadre de la CPC, «1'accès de la Commission a pour objectif la surveillance de l'application du règlement CPC et la législation visée à son annexe concernant la protection des consommateurs, ainsi que la compilation de données statistiques relatives à l'exécution de ces tâches».

41. Cela ne signifie pas que la Commission devrait avoir accès à n'importe quelles informations échangées entre les États membres dans le cadre du SCPC.

42. En effet, le CEPD insiste sur le fait que l'accès à des bases de données telles que le SCPC relève de la définition du traitement de données à caractère personnel. Aux termes de l'article 5, point a), du règlement (CE) n° 45/2001, qui s'applique aux droits d'accès de la Commission au SCPC, les institutions ne peuvent traiter des données à caractère personnel que si cela est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public, et à condition que le traitement soit basé sur les traités ou le droit dérivé.

([11]) Voir la section 8 des lignes directrices, «Conseils supplémentaires; Pourquoi la période de conservation est-elle fixée à cinq ans?». Les lignes directrices en matière de protection des données dans le cadre de la CPC ajoutent également que «La période de conservation vise à faciliter la coopération entre les autorités publiques responsables de l'application des lois protégeant les intérêts des consommateurs, lorsqu'elles traitent de cas d'infractions intracommunautaires et à contribuer au fonctionnement harmonieux du marché intérieur, à favoriser la qualité et la cohérence dans l'application des lois qui protègent les intérêts des consommateurs, à contrôler la protection des intérêts économiques des consommateurs et à permettre d'améliorer la qualité et la cohérence de l'application».

43. D'après le CEPD, ces exigences — qui découlent directement du droit à la protection des données consacré par l'article 8 de la Convention européenne des droits de l'homme et par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne — impliquent que la Commission ne peut être habilitée à accéder aux systèmes d'information des États membres que si cela est prévu par des dispositions législatives spécifiques reposant sur une base juridique tout à fait adéquate (normalement, la procédure législative normale). La certitude juridique et la transparence sont les deux valeurs fondamentales qui expliquent pourquoi il est particulièrement important que l'accès de la Commission repose sur une base juridique spécifique et sûre qui garantisse les droits fondamentaux des personnes en ce qui concerne la protection des données.

44. Ni le pouvoir général de contrôle de la Commission en tant que «gardienne du traité», ni l'obligation qu'ont les États membres de veiller à une coopération loyale ne sont suffisamment précis pour donner à la Commission l'accès à des bases de données contenant des données à caractère personnel. La coopération loyale suppose que les États membres fournissent — à certaines conditions — des informations à la Commission lorsqu'ils sont saisis d'une demande à cet effet ou lorsqu'ils sont invités à fournir des informations en vertu d'une règle particulière. En revanche, elle n'implique pas que la Commission doive avoir accès à leurs bases de données.

45. À cet égard, le CEPD souligne également que le règlement CPC exclut la possibilité que la Commission ait accès aux informations contenues dans les demandes d'assistance mutuelle et de mesures d'exécution. Les articles 6 et 8 du règlement CPC ne désignent que l'autorité requise, et non la Commission, comme les destinataires de ces données.

3.3. **Catégories particulières de données dans le SCPC**

46. Le CEPD se félicite que la deuxième modification de la CPC ait introduit, au point 4.4 de l'annexe à la décision mettant en œuvre la CPC, une disposition portant sur le traitement de catégories particulières de données dans le SCPC. Le CEPD est particulièrement heureux de constater que la disposition limite ce traitement aux cas où l'exécution des obligations conformément au règlement CPC serait «impossible autrement» et que le traitement de ces données soit soumis à la condition supplémentaire qu'il soit «autorisé en vertu de la directive 95/46/CE».

IV. **VIE PRIVÉE DÈS LA CONCEPTION ET RESPONSABILITÉ**

47. Après avoir examiné, au chapitre III, les questions spécifiques soulevées par la deuxième modification de la CPC, le CEPD souhaite, aux chapitres IV à VI, attirer l'attention de la Commission sur quelques autres points qui méritent d'être abordés en vue de l'amélioration du cadre juridique du SCPC.

4.1. **Vie privée dès la conception**

48. Le CEPD encourage depuis un certain temps la Commission et d'autres institutions de l'UE à adopter des mesures sur le plan technologique et organisationnel pour intégrer la protection et la sécurité des données comme un élément fondamental de la conception et de la mise en œuvre de leurs systèmes d'information («vie privée dès la conception») ([12]).

49. Bien qu'il reconnaisse que certaines mesures ont été prises en ce sens, ce dont il se félicite, le CEPD recommande à la Commission de procéder à une évaluation globale des garanties supplémentaires en matière de vie privée dès la conception qui pourraient être incorporées à l'architecture du SCPC. Les garanties suivantes devraient notamment être envisagées et, au besoin, mises en œuvre:

— des solutions de vie privée dès la conception aidant les utilisateurs d'un système à prendre des décisions «adéquates» en matière de protection des données (voir la section 3.2 de l'avis sur la notification d'un contrôle préalable);

— des mesures pour faciliter le classement et la suppression d'affaires en temps utile (idem, section 3.3);

— des procédures pour faciliter les droits d'information et d'accès des personnes concernées (idem, section 3.5);

— des procédures claires applicables à toute modification effectuée directement au niveau de la base de données, à l'accès par connexion, au motif de l'action et à l'approbation au niveau adéquat (idem, section 3.6); et

— le stockage «crypté» des informations dans la base de données de manière à ce que les informaticiens ne puissent y accéder (du moins pour certaines des données, telles que les pièces jointes confidentielles) (idem, section 3.6).

4.2. **Responsabilité**

50. Par ailleurs, conformément au principe de «responsabilité» ([13]), le CEPD recommande également l'adoption d'un cadre clair de responsabilité qui garantisse le respect des règles relatives à la protection des données et en apporte la preuve, comme:

([12]) Voir la section 7 de l'avis du CEPD sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», publié le 14 janvier 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

([13]) Idem.

— l'adoption et la mise à jour, si nécessaire, d'une politique de protection des données qui devra être approuvée par la DG SANCO au plus au niveau hiérarchique. Cette politique de protection des données doit également comprendre un plan de sécurité (voir la section 3.6 de l'avis sur la notification d'un contrôle préalable) ([14]);

— la réalisation d'audits périodiques afin d'évaluer l'adéquation et le respect constants de la politique de protection des données (y compris l'audit du plan de sécurité, idem, section 3.6);

— la publication (au moins partielle) des résultats de ces audits afin de rassurer les parties prenantes au sujet du respect de la protection des données; et

— la notification des violations de données et d'autres incidents de sécurité au DPD de la Commission et aux personnes concernées (ainsi que, le cas échéant, à d'autres parties prenantes et autorités) ([15]).

V. TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL EN DEHORS DE L'UNION EUROPÉENNE

5.1. Accords bilatéraux

51. L'article 14, paragraphe 2, du règlement CPC prévoit que les informations transmises en application dudit règlement peuvent également être transmises à l'autorité d'un pays tiers par une autorité compétente, dans le cadre d'un accord bilatéral d'assistance conclu avec ledit pays, i) dès que l'autorité compétente qui a initialement fourni l'information y consent; et ii) conformément à la législation communautaire relative à la protection des données.

52. Les articles 25 et 26 de la directive 95/46/CE soumettent les transferts à des pays tiers à certaines conditions supplémentaires, qui visent à garantir que les données seront protégées de manière adéquate à l'étranger. Ces conditions prévoient en outre un certain nombre d'exceptions. L'application et l'interprétation de ces dispositions de la directive 95/46/CE peuvent différer d'un État membre à l'autre.

53. Au vu de ce qui précède, le CEPD peut accepter les garanties incluses dans le règlement CPC, à savoir que tout transfert vers un pays tiers est subordonné: i) au consentement de l'autorité compétente qui a initialement transmis l'information; et ii) au respect de la législation de l'Union applicable en matière de protection des données.

54. Le CEPD se réjouit également que les lignes directrices en matière de protection des données dans le cadre de la CPC recommandent que tout accord bilatéral d'assistance prévoie des garanties adéquates en matière de protection des données — sauf si le pays tiers garantit un niveau adéquat de protection — et, si nécessaire, que l'accord soit également notifié aux autorités de contrôle compétentes chargées de la protection des données.

55. Cela dit, les modalités définies dans le règlement CPC ne sont pas idéales. Leur application est complexe: une autorité compétente qui envisagerait de transférer des informations à un pays tiers devrait tenir compte non seulement de l'accord bilatéral qu'il a conclu avec ce pays, de sa législation nationale en matière de protection des données et de sa propre appréciation de la possibilité du transfert des données au pays tiers en question sur la base de sa législation nationale en matière de protection des données, mais elle devrait également se demander si les autres autorités compétentes concernées qui ont contribué au dossier (et elles peuvent être plusieurs) ont donné ou non leur consentement sur la base de leur propre législation en matière de protection des données.

56. Du point de vue de la protection des données, cette complexité génère des incertitudes quant aux droits de la personne concernée, notamment quant à la question de savoir si ses données sont transférées à l'étranger et à quelles conditions. En outre, les personnes concernées ne bénéficient pas pleinement d'une législation européenne solide et harmonisée en matière de protection des données. De plus, du point de vue des autorités compétentes, cette complexité est également susceptible d'entraver la coopération entre elles et elle leur occasionne une surcharge administrative.

57. À la lumière de ce qui précède, le CEPD encourage la conclusion d'accords à l'échelle de l'UE prévoyant des garanties adéquates en matière de protection des données, tout en contribuant également à éviter l'application de critères hétérogènes et l'augmentation de la charge administrative qui en résulte pour les autorités compétentes.

5.2. Accords à l'échelle de l'UE

58. En plus de la possibilité de coopération bilatérale prévue à l'article 14, l'article 18 du règlement CPC relatif aux accords internationaux prévoit également que «1a Communauté coopère avec les pays tiers et les organisations internationales compétentes» et que «1es modalités de la coopération, y compris la mise en place de dispositifs d'assistance mutuelle, peuvent faire l'objet d'accords entre la Communauté et les pays tiers concernés».

([14]) La Commission devrait également envisager, si nécessaire, de procéder à tout le moins à une évaluation d'impact partielle sur la protection des données et de la vie privée en se focalisant sur la finalité, la durée et les modalités de la période de conservation et discuter éventuellement d'autres questions en suspens qui n'ont pas encore été totalement résolues.

([15]) Voir la section 6.3 de l'avis du CEPD du 14 janvier 2011 cité ci-dessus.

59. Pour les raisons exposées à la section 5.1 ci-dessus, le CEPD soutient l'initiative de la Commission tendant à négocier et à conclure des accords à l'échelle de l'UE contenant des garanties adéquates en matière de protection des données, harmonisées au niveau de l'UE, afin de remplacer les accords bilatéraux existants.

60. Son soutien à de tels accords européens est toutefois subordonné à l'engagement de la Commission et des législateurs de l'UE de garantir le niveau de protection le plus élevé pour les échanges de données à caractère personnel avec les pays tiers. Les implications des accords de coopération internationale conclus avec les pays tiers doivent être examinées minutieusement du point de vue de la protection des données, des règles claires régissant ces échanges doivent être établies, et des garanties adéquates en matière de protection des données doivent être prévues après consultation du CEPD et, le cas échéant, des autorités nationales chargées de la protection des données.

61. Bien que l'article 18 du règlement CPC ne règle pas spécifiquement la question de l'accès direct des autorités des pays tiers au SCPC, cet accès peut être possible sur le plan technique. Le CEPD ne souhaite pas décourager l'intégration de nouvelles fonctions dans le SCPC qui accorderaient aux autorités compétentes des pays tiers un accès strictement limité et sélectif par un mécanisme spécialement conçu à cet effet (canal de transmission et interface). Ces nouvelles fonctions pourraient en effet améliorer l'efficacité de la coopération.

62. Cela dit, ce genre d'accès direct présente des risques inhérents. Il convient dès lors d'aborder spécifiquement la question de ses implications pour la protection des données et d'examiner les dispositions techniques et organisationnelles et les garanties nécessaires. Toute fonction technique de ce genre doit être conçue sur la base des principes de la «vie privée dès la conception». La sécurité doit également être une priorité claire. Enfin, le CEPD doit être consulté, de même que, le cas échéant, les autorités nationales chargées de la protection des données.

VI. «DROITS DES CONSOMMATEURS À LA PROTECTION DES DONNÉES» ET COOPÉRATION RENFORCÉE ENTRE LES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES À TRAVERS LE SCPC

63. Pour autant que ses recommandations soient suivies (y compris celles formulées dans son avis sur la notification d'un contrôle préalable), le CEPD est convaincu que le SCPC peut être un outil efficace et respectueux de la protection des données pour la lutte transfrontalière contre les violations des droits des consommateurs dans le marché intérieur.

64. À la suite du développement du commerce électronique et de l'utilisation croissante des réseaux de communications électroniques par les consommateurs de divers produits et services, de plus en plus de données de personnes seront traitées lorsque celles-ci agissent en tant que consommateurs. Les consommateurs peuvent donc être de plus en plus confrontés à des violations de leurs droits pour ce qui est du respect de la protection des données. Par conséquent, il est également nécessaire que les autorités chargées de la protection des données coopèrent efficacement pour mettre fin à ces violations.

65. Parmi les cas les plus courants de violation des «droits des consommateurs à la protection des données», on peut citer les messages commerciaux non sollicités (spams), l'usurpation d'identité, le profilage illégal, la publicité comportementale illicite et les violations de données (violations de la sécurité).

66. Étant donné qu'il est probable que le nombre d'affaires de nature transfrontalière augmentera dans la société de l'information, le CEPD encourage la Commission à envisager d'éventuelles mesures législatives pour protéger les «droits des consommateurs à la protection des données» et renforcer la coopération transfrontalière entre les autorités compétentes, tant celles chargées de la protection des données que celles chargées de la protection des consommateurs.

67. Tout en envisageant d'autres options possibles, il convient en particulier d'examiner avec soin la possibilité d'accorder aux autorités chargées de la protection des données un accès adapté au SCPC afin de leur permettre de coopérer entre elles ainsi qu'avec d'autres autorités compétentes qui ont déjà accès au SCPC.

68. L'accès des autorités chargées de la protection des données doit être clairement limité à ce qui est nécessaire pour leur permettre d'accomplir leur mission dans leurs domaines de compétence, conformément aux synergies définies. Il convient bien sûr de garantir également que le cadre de participation des autorités chargées de la protection des données soit conçu de telle manière à tenir compte de leur indépendance.

VII. CONCLUSIONS

69. Le CEPD se réjouit de constater que le SCPC repose sur une base juridique qui prévoit également des garanties spécifiques en matière de protection des données. Pour répondre à toute autre préoccupation subsistant dans ce domaine, le CEPD fait observer que les recommandations formulées ci-dessous devront être prises en compte lors de la prochaine révision du cadre juridique du SCPC.

70. Dans l'intervalle, des mesures supplémentaires prises sur le plan pratique, technique et organisationnel (comme recommandé dans l'avis sur la notification d'un contrôle préalable) peuvent apporter une solution intermédiaire partielle à ces préoccupations. Dans l'attente des modifications législatives, certains changements peuvent également être introduits par le biais des lignes directrices du SCPC.

71. En ce qui concerne la période de conservation, le CEPD recommande: i) de classer les demandes d'assistance mutuelle dans des délais bien précis; ii) sauf si une enquête ou une mesure d'exécution est en cours, de retirer et de supprimer les alertes dans un délai de six mois suivant leur publication (à moins qu'une autre période de conservation, plus appropriée, puisse être justifiée); et iii) que la Commission précise et réexamine la finalité et la proportionnalité de la conservation de toutes les données liées à des affaires closes pendant une période supplémentaire de cinq ans.

72. Par ailleurs, le CEPD se réjouit que la deuxième modification de la CPC précise l'accès de la Commission aux données du SCPC. Le CEPD se félicite en particulier du fait que la Commission n'ait pas accès aux communications confidentielles entre les autorités compétentes des États membres, comme les demandes d'assistance mutuelle.

73. Le CEPD note également avec satisfaction que la deuxième modification de la CPC a introduit une disposition concernant le traitement de catégories particulières de données dans le SCPC.

74. Le CEPD recommande en outre à la Commission de réévaluer les mesures techniques et organisationnelles supplémentaires à prendre pour garantir que la protection de la vie privée et des données soit «conçue» dans l'architecture du SCPC («vie privée dès la conception») et que des contrôles adéquats soient mis en place pour veiller au respect de la protection des données et pour en apporter la preuve («responsabilité»).

75. D'autre part, si un accord à l'échelle de l'UE doit être conclu entre l'Union européenne et tout pays tiers pour régir la coopération en matière de protection des consommateurs, les implications de ces dispositions doivent être examinées avec soin, des règles claires doivent être établies pour régir ces échanges et des garanties adéquates en matière de protection des données doivent être fournies.

76. Enfin, le CEPD recommande à la Commission d'examiner les synergies éventuelles qui pourraient s'instaurer si les autorités chargées de la protection des données avaient la possibilité de se joindre à la communauté des utilisateurs du SCPC afin de coopérer pour contribuer à faire respecter les «droits des consommateurs à la protection des données».

Fait à Bruxelles, le 5 mai 2011.

Giovanni BUTTARELLI

Contrôleur européen adjoint de la protection des données