Avis du Contrôleur européen de la protection des données

sur la proposition de décision du Conseil relative à la conclusion de l'accord commercial anti-contrefaçon entre l'Union européenne et ses États membres, l'Australie, le Canada, la République de Corée, les États-Unis d'Amérique, le Japon, le Royaume du Maroc, les États-Unis mexicains, la Nouvelle-Zélande, la République de Singapour et la Confédération suisse

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 le règlement (CE) n° 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], et notamment son article 41, paragraphe 2,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

I.1. Le processus législatif de l'UE sur l'ACAC

1. Le 24 juin 2011, la Commission a présenté une proposition pour une décision du Conseil relative à la conclusion de l'accord commercial anti-contrefaçon («ACAC» ou «l'accord») entre l'Union européenne et ses États membres, l'Australie, le Canada, la République de Corée, les États-Unis d'Amérique, le Japon, le Royaume du Maroc, les États-Unis mexicains, la Nouvelle-Zélande, la République de Singapour et la Confédération suisse[3].

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] Proposition de la Commission pour une décision du Conseil relative à la conclusion de l'accord commercial anti-contrefaçon entre l'Union européenne et ses États membres, l'Australie, le Canada, la République de Corée,

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
Courrier électronique: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

2. L'accord entend faire appliquer les droits de propriété intellectuelle («DPI») en développant une approche commune à la mise en application et en facilitant la coopération au niveau international. Le Chapitre II contient des mesures dans plusieurs domaines du droit, notamment dans le domaine des mesures civiles (section 2), des mesures à la frontière (section 3), des mesures pénales (section 4), et des moyens de faire respecter les droits de propriété intellectuelle dans l'environnement numérique (section 5). Le Chapitre III contient des mesures pour améliorer les pratiques en matière de respect des droits, et le Chapitre IV traite de la coopération internationale.

3. L'ACAC a été adopté à l'unanimité par le Conseil en décembre 2011[4] et a été signé par la Commission européenne et 22 États membres[5] le 26 janvier 2012. Conformément à l'article 40 de l'accord, l'ACAC entrera en vigueur après la ratification par six États signataires. Toutefois, pour entrer en vigueur en tant que législation européenne, l'accord doit être ratifié par l'UE, ce qui signifie après approbation par le Parlement européen en vertu de la procédure de consentement pour les accords commerciaux internationaux[6] et la ratification par les États membres conformément à leurs procédures constitutionnelles. Le vote du Parlement européen sur l'ACAC devrait intervenir dans le courant de 2012 en séance plénière.

I.2. État d'avancement de l'ACAC dans l'UE

4. Ces derniers mois, l'ACAC a fait l'objet de préoccupations croissantes[7]. C'est pourquoi la Commission européenne a annoncé le 22 février 2012 son intention de saisir la Cour de justice de l'Union européenne pour obtenir un avis sur l'accord[8]. Cette procédure est prévue à l'article 218, paragraphe 11, du traité sur le fonctionnement de l'Union européenne («TFUE»)[9].

5. Le 4 avril 2012, la Commission a décidé de poser à la Cour la question suivante: *«L'accord commercial anti-contrefaçon (ACAC) est-il compatible avec les traités européens, en particulier avec la Charte des droits fondamentaux de l'Union européenne?»*.[10] En cas d'avis négatif, l'article 218, paragraphe 11, du TFUE stipule clairement que *«l'accord envisagé ne peut entrer en vigueur, sauf modification de celui-ci ou révision des traités»*.

---

les États-Unis d'Amérique, le Japon, le Royaume du Maroc, les États-Unis mexicains, la Nouvelle-Zélande, la République de Singapour et la Confédération suisse, COM(2011)380 final.

[4] La dernière version du texte de l'accord du Conseil du 23 août 2011 est disponible à l'adresse suivante: register.consilium.europa.eu/pdf/fr/11/st12/st12196.fr11.pdf.

[5] L'Allemagne, Chypre, l'Estonie, les Pays-Bas et la Slovaquie ne l'ont pas encore signé.

[6] Conformément à l'article 218, paragraphe 6, du TFUE.

[7] Voir entre autres: http://euobserver.com/9/115043; http://euobserver.com/871/115128; https://www.bfdi.bund.de/bfdi_forum/showthread.php?3062-ACTA-und-der-Datenschutz, http://www.bbc.co.uk/news/technology-17012832.

[8] Déclaration par le commissaire Karel De Gucht sur l'ACAC (Accord commercial anti-contrefaçon), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/128.

[9] L'article 218, paragraphe 11, du TFUE stipule qu'«[un] État membre, le Parlement européen, le Conseil ou la Commission peut recueillir l'avis de la Cour de justice sur la compatibilité d'un accord envisagé avec les traités. En cas d'avis négatif de la Cour, l'accord envisagé ne peut entrer en vigueur, sauf modification de celui-ci ou révision des traités». En vertu de l'article 107, paragraphe 2, du règlement de procédure de la Cour de justice, «l'avis peut porter tant sur la compatibilité de l'accord envisagé avec les dispositions des traités que sur la compétence de l'Union ou de l'une de ses institutions pour conclure cet accord».

[10] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/354&format=HTML&aged=0&language=FR&guiLanguage=en.

6. Toutefois, la saisine de la Cour de justice par la Commission ne suspendrait pas automatiquement la procédure de consentement en cours au Parlement européen. Après discussion au sein de la commission du commerce international du Parlement européen, il a été décidé de procéder au vote sur l'accord conformément au calendrier envisagé[11].

I.3. Les raisons justifiant un second avis du CEPD sur l'ACAC

7. En février 2010, le CEPD a émis un avis de sa propre initiative afin d'attirer l'attention de la Commission sur les aspects de la protection de la vie privée et des données à prendre en compte dans les négociations de l'ACAC[12]. Bien que les négociations aient été menées de manière confidentielle, certains éléments ont laissé supposer que l'ACAC contenait des mesures d'application en ligne ayant un impact sur la protection des données, notamment le mécanisme de déconnexion d'Internet en trois temps[13].

8. À l'époque, le CEPD avait axé son analyse sur la licéité et la proportionnalité de ce type de mesure et avait conclu que l'introduction dans l'ACAC d'une mesure impliquant la surveillance massive des utilisateurs d'Internet serait contraire aux droits fondamentaux de l'UE et plus particulièrement aux droits au respect de la vie privée et à la protection des données, qui sont protégés par l'article 8 de la Convention européenne des droits de l'homme et les articles 7 et 8 de la Charte des droits fondamentaux de l'UE[14]. Le CEPD a en outre souligné les garanties nécessaires pour les échanges internationaux de données à caractère personnel dans le contexte de l'application des droits de propriété intellectuelle.

9. Maintenant que le texte de l'accord proposé sur l'ACAC a été rendu public[15], le CEPD considère utile d'émettre un second avis sur l'ACAC pour évaluer certaines des dispositions contenues dans l'accord d'un point de vue de la protection des données, et ce faisant, de fournir des recommandations spécifiques qui pourraient être prises en considération dans le processus de ratification. Agissant de sa propre initiative, le CEPD a, par conséquent, adopté le présent avis sur la base de l'article 41, paragraphe 2, du règlement (CE) n° 45/2001, en vue de fournir une orientation sur les questions relatives au respect de la vie privée et à la protection des données soulevées par l'ACAC.

II. PORTÉE DES COMMENTAIRES DU CEPD

10. Le CEPD reconnaît la préoccupation légitime d'assurer l'application des DPI dans un contexte international. Toutefois, bien qu'une coopération internationale soit nécessaire pour l'application des DPI, les moyens envisagés pour le renforcement de leur application ne doivent pas se faire au détriment des droits fondamentaux des individus, et, en particulier, de leurs droits au respect de la vie privée et à la protection des données. Le CEPD a, par conséquent, appelé la Commission européenne, au moment de la négociation de l'accord, à trouver un juste équilibre entre les exigences de protection des droits de propriété intellectuelle, d'une part, et les droits des personnes physiques en

[11] Voir http://www.neurope.eu/article/parliament-halts-sending-acta-court-justice.
[12] Avis du Contrôleur européen de la protection des données sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC), JO C 147 du 5.6.2010, p.1.
[13] Les «politiques de déconnexion d'Internet en trois temps» ou les systèmes de «riposte graduée» permettent aux titulaires des droits d'auteur ou des tiers habilités à surveiller les utilisateurs Internet et les contrefacteurs présumés. Après avoir contacté le fournisseur d'accès à Internet (FAI) du contrefacteur présumé, les FAI doivent avertir l'utilisateur identifié comme contrefacteur, et le déconnecter d'Internet après trois avertissements.
[14] Charte des droits fondamentaux de l'Union européenne, JO C 303 du 14.12.2007, p. 1.
[15] Voir note de bas de page 3.

matière de respect de la vie privée et de protection des données, d'autre part[16]. La nécessité de trouver un juste équilibre entre les droits dans le contexte de l'application des DPI a été récemment réaffirmée par la Cour de justice de l'Union européenne, le 19 avril 2012, dans l'affaire *Bonnier Audio AB*[17].

11. Comme il sera développé plus avant, le CEPD note que les dispositions visant à faire respecter les DPI sur l'Internet soulèvent des craintes du point de vue de la protection des données. Comme susmentionné, il a été demandé à la Cour de justice de clarifier si les dispositions de l'ACAC sont conformes aux traités européens, en particulier la Charte des droits fondamentaux. L'analyse dans le présent avis adopte une perspective plus ciblée puisqu'elle évalue la compatibilité de l'accord uniquement avec la législation de l'UE en matière de respect de la vie privée et de protection des données, et elle vérifie également si les dispositions de l'accord peuvent entraîner des effets secondaires indésirables et inacceptables sur la vie privée et la protection des données d'un individu si elles ne sont pas mises en œuvre correctement. En d'autres termes, l'accord fournit-il les bons incitants pour que les législateurs de l'UE et des États membres prennent en considération les besoins en matière de protection des données ? Le présent avis ne doit en aucun cas être considéré comme préjugeant de l'avis de la Cour de justice.

12. Bien que cet avis soit axé sur les mesures d'application présentées au chapitre numérique de l'ACAC, il évalue également d'autres dispositions de l'accord lorsque cela s'avère pertinent. Il se fonde sur l'analyse effectuée dans le cadre de l'avis précédent du CEPD sur l'ACAC, qui reste totalement valide en ce qui concerne les menaces à la vie privée et à la protection des données causées par la surveillance généralisée des activités des internautes et les garanties nécessaires pour les échanges internationaux de données à caractère personnel dans le cadre de l'application de droits de propriété intellectuelle. Il n'entend donc pas répéter l'analyse précédente dans son intégralité mais y fera référence lorsque nécessaire. Après l'évaluation des menaces à la protection des données et à la vie privée posées par les mécanismes d'application envisagés dans l'environnement numérique (section III), une analyse plus spécifique de certaines des dispositions de l'accord sera réalisée d'un point de vue de la protection des données (section IV).

III. MENACES À LA PROTECTION DES DONNÉES ET À LA VIE PRIVÉE POSÉES PAR LES MÉCANISMES D'APPLICATION ENVISAGÉS DANS L'ENVIRONNEMENT NUMÉRIQUE

III.1. Mesures prévues dans le chapitre numérique de l'ACAC (Chapitre II, section 5)

13. Le Chapitre II, section 5, de l'ACAC contient certaines mesures visant à faciliter le respect des DPI dans l'environnement numérique. Bien que ces mesures soient conçues pour aider à lutter contre toute violation des DPI, y compris les marques de fabrique, la protection du droit d'auteur est au cœur de ce chapitre.

14. Le chapitre numérique de l'ACAC contient deux mesures spécifiquement conçues pour faire respecter les DPI dans un environnement en ligne, que les parties contractantes ont la possibilité, mais pas l'obligation explicite, d'introduire dans leur système juridique: (i) un mécanisme par lequel un fournisseur de services en ligne peut se voir ordonner par les «autorités compétentes» de divulguer rapidement au détenteur du droit des

[16] Voir paragraphe 10 de l'avis du CEPD du 22 février 2010 sur l'ACAC.
[17] Voir arrêt du 19 avril 2012, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB.*

renseignements suffisants pour lui permettre d'identifier un abonné[18], et (ii) la promotion *«au sein des milieux d'affaires, des efforts de coopération destinés à contrer les atteintes portées aux marques de fabrique ou de commerce et au droit d'auteur ou à des droits connexes»*[19].

15. Le premier type de mesure vise à assurer la divulgation aux détenteurs du droit de l'identité des individus dont le comportement laisse suspecter une atteinte aux DPI en ligne. En vertu de ce mécanisme, les fournisseurs de services en ligne seraient dans l'obligation de divulguer des données à caractère personnel de certains de leurs abonnés aux détenteurs du droit si certains critères sont remplis, sous réserve de l'intervention et du contrôle d'une autorité.

16. Le second type de mesure n'est pas aussi explicite que le premier et nul ne sait à quels types de mesures la promotion *«au sein des milieux d'affaires, des efforts de coopération»* fait référence. Un considérant dans le préambule de l'ACAC est plus spécifique en indiquant que cette coopération est souhaitable *«entre fournisseurs de services et détenteurs de droits afin de s'attaquer aux atteintes relatives aux droits dans l'environnement numérique»*. Plusieurs parties contractantes ayant déjà mis en œuvre certains types de mécanismes de coopération volontaire en matière d'application sur leur territoire entre les fournisseurs d'accès à Internet et les détenteurs du droit sont susceptibles de faire valoir que ces mécanismes relèvent de l'article 27, paragraphe 3, de l'accord. Plusieurs formes de mécanismes de coopération volontaire en matière d'application des droits sont mis en œuvre, tels que le mécanisme de déconnexion d'Internet en trois temps, le blocage et le filtrage du trafic «peer to peer» (services de partage de fichiers), ou le blocage de sites Web dont on présume une violation des droits d'auteur.

III.2. Pourquoi ces mécanismes sont-ils problématiques d'un point de vue de la protection des données de l'UE?

17. L'Internet facilite les échanges, de diverses manières[20], de contenus couverts par un droit d'auteur. Certains de ces échanges sont des échanges licites d'œuvres protégées, tandis que d'autres ont trait à la création illicite et à des échanges de contenus couverts par un droit d'auteur. Parmi tous les DPI, le droit d'auteur est sans doute le droit dont le respect sur Internet pose le plus de problèmes et de préoccupations en matière de protection de la vie privée, en particulier vu le nombre d'individus qui peuvent être affectés par les mesures visant à faire respecter les droits d'auteur applicables aux activités en ligne.

18. Bon nombre des mesures qui pourraient être mises en œuvre dans le cadre de l'article 27, paragraphes 3 et 4 de l'ACAC, impliqueraient une certaine forme de surveillance de l'activité d'un individu sur Internet, que ce soit en détectant des violations réelles des DPI ou en essayant de prévenir toute violation future. Dans de nombreux cas, la surveillance serait entreprise par les détenteurs du droit ou les associations de détenteurs du droit et des tiers agissant en leur nom, même s'ils ont généralement tendance à déléguer cette tâche aux fournisseurs d'accès à Internet[21].

[18] Article 27, paragraphe 4, de l'ACAC.
[19] Article 27, paragraphe 3, de l'ACAC.
[20] Par exemple, via les réseaux de partage de fichiers, le téléchargement web, le streaming, etc.
[21] Ceci est particulièrement vrai dans le contexte de la prévention des violations, où les détenteurs des droits ont par exemple demandé aux fournisseurs d'accès à Internet de mettre en œuvre des outils de filtrage qui impliquent une surveillance des comportements des internautes par les fournisseurs d'accès à Internet.

19. Les mesures impliquant la surveillance généralisée des activités des internautes sont extrêmement intrusives dans la vie privée des individus. Elles sont généralement appliquées de manière invisible et peuvent affecter des millions d'individus, voire tous les utilisateurs, qu'ils soient ou non suspects. Elles peuvent impliquer la surveillance des communications électroniques échangées sur Internet et l'examen du contenu des communications des individus sur Internet, notamment les courriers électroniques envoyés et reçus, les sites web visités, les fichiers téléchargés ou chargés, etc. En outre, une telle surveillance implique généralement l'enregistrement systématique des données, notamment l'adresse IP des utilisateurs suspectés. Toutes ces informations peuvent être reliées à un individu particulier par le fournisseur d'accès à Internet, qui peut identifier l'abonné auquel l'adresse IP suspecte a été attribuée. Elles constituent par conséquent des données à caractère personnel au sens de l'article 2 de la directive 95/46/CE sur la protection des données à caractère personnel[22].

20. En conséquence, ces mesures constituent souvent une interférence avec les libertés et droits fondamentaux des individus, tels que le droit au respect de la vie privée, à la protection des données et à la confidentialité des communications, protégés à l'article 8 de la Convention européenne des droits de l'homme et aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[23].

21. La licéité des mesures d'application spécifiques qui interfèrent avec les libertés et droits fondamentaux doit être évaluée à la lumière des critères établis à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme[24] et de l'article 52 de la Charte des droits fondamentaux de l'Union européenne[25]. Ils exigent que toute limitation soit prévue par la loi et nécessaire et proportionnée à l'objectif légitime poursuivi. En outre, les mesures impliquant le traitement des données à caractère personnel doivent être conformes à la législation sur la protection des données qui, entre autres, requiert qu'elles soient fondées sur une base juridique valide.

22. S'agissant de la nécessité d'une mesure d'application spécifique interférant avec un ou plusieurs droits fondamentaux, il doit d'abord être démontré comment cette mesure répond à un besoin pressant de la société. Il convient en outre de considérer si des alternatives moins intrusives sont disponibles ou pourraient être envisagées[26].

23. L'évaluation de la proportionnalité d'une mesure d'application spécifique doit se faire au cas par cas et à la lumière des droits fondamentaux avec lesquels elle pourrait interférer. Afin de réaliser une telle évaluation, il est nécessaire que la mesure soit suffisamment précise et bien définie pour évaluer son impact concret sur le partage de

[22] Voir également paragraphe 27 de l'avis du CEPD du 22 février 2010 sur l'ACAC.
[23] Voir l'avis du CEPD du 7 octobre 2011 sur la neutralité du net, la gestion du trafic et la protection de la vie privée et des données personnelles, JO C 34 du 8.2.2012, p. 1.
[24] L'article 8, paragraphe 2, dispose que *«[i]l ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui»*.
[25] L'article 52, paragraphe 1, dispose que *«[t]oute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui»*.
[26] Voir paragraphe 42 et suivants de l'avis du CEPD du 22 février 2010 sur l'ACAC.

données ainsi que sur d'autres droits fondamentaux[27]. De plus, dans le contexte de l'application des DPI, la mesure doit être proportionnée en réponse à une violation individualisée des DPI; une mesure qui viserait à prévenir les violations des DPI en général ne serait pas proportionnée.

24. Deux aspects sont particulièrement importants pour évaluer la proportionnalité d'une mesure visant à faire respecter les DPI: (i) l'échelle et la profondeur de toute surveillance de l'utilisation d'Internet et des internautes, et (ii) l'échelle des violations des DPI contre lesquelles cette mesure s'adresse.

25. Une forme ciblée de surveillance par les détenteurs du droit serait légitime si le traitement est effectué dans le cadre de procédures judiciaires spécifiques, qu'elles soient actuelles ou futures, visant à établir, déposer ou défendre des actions en justice. Toutefois, la surveillance généralisée suivie par le stockage de données à grande échelle dans le but de faire valoir ses droits, tels que le balayage d'Internet, ou de toute l'activité sur les réseaux P2P, irait au-delà de ce qui est légitime. Une telle surveillance est particulièrement intrusive envers les droits et libertés des individus lorsqu'elle n'est pas bien définie et qu'elle n'est pas assortie d'une limitation spatiale, temporelle et personnelle[28]. En conséquence, la surveillance aveugle ou généralisée du comportement d'un internaute en rapport avec une violation mineure, à petite échelle et sans but lucratif serait disproportionnée et serait contraire à l'article 8 de la CEDH, aux articles 7 et 8 de la Charte des droits fondamentaux, et à la directive relative à la protection des données[29].

III.3. Le cadre juridique actuel de l'UE

26. Du point de vue de l'UE, les dispositions de l'ACAC doivent être lues à la lumière de l'ordre juridique actuel de l'UE en matière de protection des droits fondamentaux et de son cadre juridique concernant l'application des DPI, la protection des données, ainsi que le régime de responsabilité des intermédiaires d'Internet. Les mesures d'application contenues dans le chapitre numérique de l'ACAC doivent par conséquent être sujettes aux limitations de l'ordre juridique de l'UE.

27. Dans l'UE, les droits fondamentaux au respect de la vie privée et à la protection des données ont été davantage développés dans le droit primaire de l'UE, à l'article 16 du TFUE, et dans le droit dérivé de l'UE, dans la directive 95/46/CE et dans la directive «vie privée et communications électroniques» 2002/58/CE[30]. Les droits au respect de la vie privée et à la protection des données doivent en outre être interprétés à la lumière de la jurisprudence de la Cour européenne des droits de l'homme[31] et de la Cour de justice.

28. Le cadre juridique actuel de l'UE sur la protection de la PI a été soigneusement conçu en vue de respecter d'autres droits fondamentaux tels que les droits au respect de la vie

[27] Voir conclusions de l'avocat général M. Pedro Cruz Villalón, affaire C-70/10, *Scarlet Extended SA contre SABAM*, 14 avril 2011, paragraphes 66 et 68.
[28] Voir en particulier l'arrêt du 24 novembre 2011, C-70/10, *Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, et l'arrêt du 16 février 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) / Netlog NV*.
[29] Voir paragraphes 31 à 34 de l'avis du CEPD du 22 février 2010 sur l'ACAC.
[30] 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.
[31] Interprétant les principaux éléments et conditions définis à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales adoptée à Rome le 4 novembre 1950.

privée et à la protection des données. La directive IPRE (respect des droits de propriété intellectuelle)[32], et dans une certaine mesure la directive 2001/29/CE[33], énoncent les conditions pour le respect des DPI dans les procédures civiles. En outre, les mesures d'application prévues dans l'ACAC devraient également respecter le régime de responsabilité spécial des fournisseurs d'accès à Internet, établi par la directive sur le commerce électronique 2000/31/CE[34] et les obligations et limitations imposées aux fournisseurs d'accès à Internet dans la directive sur la conservation des données 2006/24/CE[35].

29. Il n'y a, cependant, aucune harmonisation au niveau de l'UE concernant les sanctions et procédures pénales en matière de respect des DPI, puisque aucun consensus n'a pu être rallié au niveau de l'UE. L'aspect pénal relève donc de la compétence nationale[36].

30. La nécessité d'assurer un juste équilibre entre le droit de propriété et les droits fondamentaux, tels que le droit à la protection des données, n'a cessé d'être souligné et peaufiné par la Cour de justice depuis l'arrêt *Promusicae*[37].

31. Il est donc primordial que les mesures d'application prévues dans l'ACAC soient conformes au cadre juridique actuel de l'UE en matière de respect des DPI, qui respecte cet équilibre des droits.

III.4. Impact de l'ACAC sur les cadres juridiques futurs de l'UE et des États membres

32. Bien que la formulation de l'article 27, paragraphe 3, et de l'article 27, paragraphe 4, laisse entendre que l'introduction de ces types de mesures n'est pas obligatoire pour les parties[38], ils énoncent néanmoins clairement la possibilité pour les parties, notamment l'UE ainsi que ses États membres, de le faire. Si l'utilisation d'une formulation permissive en lieu et place d'une formulation contraignante semble moins problématique, elle n'apaise toutefois pas les craintes suscitées par l'introduction de ces mécanismes, pour diverses raisons.

33. L'accord résultant des négociations manque de précision et laisse trop de place à l'interprétation par les parties. Ce manque de précision est regrettable car l'accord n'établit pas avec une certitude juridique suffisante les types de mécanismes qui

[32] Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, JO L 195 du 2.6.2004, p. 16.
[33] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, JO L 167 du 22.6.2001, p. 10–19.
[34] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000, p. 1.
[35] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54.
[36] C'est la raison pour laquelle la section sur les mesures pénales de l'ACAC a été négociée directement par les États membres de l'UE et non par la Commission.
[37] Voir plus particulièrement l'arrêt du 24 novembre 2011, C-275/06 *Promusicae*, Rec. 2008 I-271, points 62 à 68, affaire C-70/10, *Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, paragraphe 44, l'arrêt du 16 février 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) / Netlog NV*, points 42 à 44, et l'arrêt du 19 avril 2012, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB.*
[38] L'article 27, paragraphe 3, stipule que chaque partie «s'efforce de promouvoir» et l'article 27, paragraphe 4, dispose que chaque partie «peut» prévoir (…).

pourraient être mis en place suite à la conclusion de l'ACAC et les garanties contre l'usage abusif des données à caractère personnel ou pour protéger le droit à la défense.

34. En principe, les mesures devant être adoptées dans l'UE pour renforcer le respect des droits dans l'environnement numérique après la conclusion de l'ACAC ne devraient pas dépasser le cadre du droit de l'UE et du respect des droits fondamentaux tels qu'ils sont garantis dans l'UE. Toutefois, il y a un risque que l'ACAC ait un impact sur le cadre futur de l'UE puisque de nouvelles lois et modifications au droit actuel de l'UE pourraient être motivées par la ratification de l'ACAC, allant dans le sens de ce qui a été convenu. Ajoutons que la mise en œuvre générale de mesures au titre de ces dispositions dans des pays tiers relevant de l'ACAC pourrait avoir une influence sur la discussion législative au sein de l'UE. Bien que la Commission envisage actuellement de réviser la directive IPRE, la ratification de l'ACAC pourrait encourager l'introduction de mécanismes de coopération volontaire en matière d'application, bien qu'aucun consensus n'ait été rallié jusqu'à présent au niveau de l'UE. Il semble par conséquent prématuré pour l'UE de s'engager déjà sur certains principes de base, en particulier en ce qui concerne les mécanismes de coopération entre les parties prenantes et les fournisseurs d'accès à Internet, compte tenu du désaccord actuel sur le principe même de ces systèmes.

35. Par ailleurs, les États membres peuvent, entretemps, poursuivre la mise en œuvre de leurs propres mesures. Les lacunes actuelles dans la formulation du texte, ainsi que les incitants fournis aux parties pour la mise en œuvre et la conception de mécanismes d'application dans l'environnement numérique sur leur propre territoire, sont une porte ouverte à des approches fragmentées au sein de l'UE, générant à leur tour un risque élevé de respect inapproprié ou insuffisant des exigences en matière de protection des données au sein de l'UE.

36. Compte tenu des considérations qui précèdent, le CEPD aurait préféré un accord contenant des termes plus précis et des garanties spécifiques, ce qui aurait contribué à prévenir des approches indésirables.

IV. ANALYSE DÉTAILLÉE DES DISPOSITIONS SPÉCIFIQUES DE L'ACAC

IV.1. La portée du chapitre numérique et la notion d'«échelle commerciale» doivent être clarifiées

37. Dans le chapitre numérique de l'accord, il est prévu que les moyens de faire respecter les DPI doivent avant tout être conformes aux procédures d'application en matière civile et pénale définies dans la législation des parties. D'autres moyens de faire respecter les DPI, spécifiques à l'environnement numérique, sont fournis à l'article 27, aux paragraphes 3 et 4, mais sans préciser dans quelle mesure ces autres moyens s'intégreraient dans les procédures d'application en matière civile et pénale des parties ou s'ils constitueraient des moyens d'application ad hoc.

38. Le chapitre numérique ne définit pas avec suffisamment de clarté le type d'actes qui seraient soumis à des procédures d'application dans l'environnement numérique et si ceux-ci incluraient, ou au contraire excluraient, les activités réalisées sur Internet à des fins purement privées, telles que le partage privé de fichiers.

39. À cet égard, il est particulièrement difficile de déterminer si seules les activités menées à une «échelle commerciale» seraient soumises aux mesures énoncées dans le chapitre

numérique. Le critère d'«échelle commerciale» est mentionné dans l'accord uniquement en ce qui concerne les procédures pénales (article 23)[39] mais pas en ce qui concerne les procédures civiles ou autres procédures d'application envisagées dans le chapitre numérique. Cela semble être contraire à l'approche de l'UE dans la directive 2004/48/CE, qui applique la notion d'«échelle commerciale» également aux mesures d'application civiles et administratives[40]. Par conséquent, l'ACAC n'offre aucune garantie suffisante que seules les activités ayant une «échelle commerciale» seraient soumises aux mesures envisagées dans le chapitre numérique.

40. En outre, l'article 23 implique la pénalisation de certains actes commis sur l'Internet, qui seront soumis à des peines *«qui comprennent l'emprisonnement, ainsi que des amendes suffisamment lourdes pour être dissuasives en vue d'empêcher de futures atteintes»* (article 24). Il suggère la pénalisation de certains types d'actes, tels que des actes délibérés de «piratage portant atteinte à un droit d'auteur» ou «à des droits connexes», commis «à une échelle commerciale», sans toutefois définir clairement les types d'actes qui constitueraient une infraction pénale. En outre, il ne relie pas l'application de sanctions pénales à ces actes qui sont reconnus comme des infractions pénales dans la législation des parties. L'article 23 semble donc créer de nouvelles catégories d'infractions qui seraient soumises à des procédures pénales, sans toutefois fournir une quelconque définition qui satisferait aux normes de certitude juridique requise en ce qui concerne les sanctions pénales.

41. Cela est d'autant plus inquiétant que la notion d'«échelle commerciale» en elle-même n'a pas été définie avec suffisamment de précision pour fournir la certitude juridique sur la portée des mesures d'application dans l'environnement numérique en ce qui concerne les actes commis par des individus dans le cadre d'un usage privé. S'agissant des mesures pénales, l'article 23 précise que *«les actes commis à une échelle commerciale comprennent au moins ceux qui sont commis à titre d'activités commerciales en vue d'un avantage économique ou commercial direct ou indirect»*. Toutefois, la notion d'avantage économique ou commercial «indirect» est très large et pourrait être interprétée très largement pour couvrir un éventail d'activités réalisées par les individus sur l'Internet à des fins purement privées et dont ils ne retirent aucun gain ou bénéfice économique. En outre, l'article 23 n'est pas une liste exhaustive d'actes qui seraient jugés comme relevant de la notion d'échelle commerciale (utilisation du terme *«au moins»*). Cela pourrait être en contradiction avec l'interprétation donnée à la notion d'«échelle commerciale» dans l'UE, où l'on considère que cela *«exclut normalement les actes qui sont perpétrés par des consommateurs finaux agissant de bonne foi»*[41] et les actes *«accomplis par les usagers privés à des fins personnelles et non lucratives»*[42].

---

[39] L'article 23 dispose que *«[c]haque Partie prévoit des procédures pénales et des peines applicables au moins pour les actes délibérés de contrefaçon de marque de fabrique ou de commerce ou de piratage portant atteinte à un droit d'auteur ou à des droits connexes, commis à une échelle commerciale»*.

[40] Le considérant 14 stipule que «[l]es mesures prévues à l'article 6, paragraphe 2, à l'article 8, paragraphe 1, et à l'article 9, paragraphe 2, ne doivent s'appliquer qu'à des actes perpétrés à l'échelle commerciale, sans préjudice de la possibilité qu'ont les États membres d'appliquer également ces mesures à d'autres actes (...)».

[41] Voir considérant 14 de la directive 2004/48/CE.

[42] Résolution législative du Parlement européen du 25 avril 2007 sur la proposition modifiée de directive du Parlement européen et du Conseil relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle (COM(2006)0168 - C6-0233/2005 - 2005/0127(COD)), JO C 74 E du 20.3.2008, p. 526. Voir également l'avis du Comité économique et social européen sur la proposition de directive du Parlement européen et du Conseil relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle COM(2005) 276 final — 2005/0127 (COD), JO C 256 du 27.10.2007, p. 0003-0007. Plus particulièrement que *«les échanges privés de fichiers sur internet ou la reproduction (ou le "remix" musical), ou la représentation d'œuvres, matérielles ou intellectuelles, dans un cadre familial ou privé ou aux fins d'étude et*

42. En conséquence, le CEPD souligne que l'accord n'est pas clair concernant la portée des mesures d'application dans l'environnement numérique, et ne permet pas de déterminer si elles ne visent que les violations à grande échelle des DPI. Il regrette que la notion d'«échelle commerciale» ne soit pas définie avec suffisamment de précision et que les actes commis par des utilisateurs privés à des fins personnelles et non lucratives ne soient pas expressément exclus de la portée de l'accord.

IV.2. Les injonctions et la surveillance des internautes par les détenteurs du droit

43. Afin de renforcer le respect des DPI dans l'environnement numérique, l'article 27, paragraphe 4, de l'accord prévoit la possibilité pour les parties d'introduire une injonction spécifique à l'intention des fournisseurs d'accès à Internet[43]. Cette procédure d'injonction permettrait aux *«autorités compétentes»* d'imposer aux fournisseurs d'accès à Internet d'identifier la personne derrière l'adresse IP, dont le comportement laisse suspecter une atteinte aux DPI, et de divulguer ces informations *«rapidement»* au détenteur du droit.

44. Le recours à ce mécanisme d'injonction implique que le détenteur du droit s'engagerait dans une certaine forme de surveillance de l'utilisation de l'Internet pour identifier les comptes dont *«il est allégué»* qu'ils auraient été utilisés *«en vue de porter atteinte à des droits»*. Ceci implique le traitement de données sensibles relatives à des infractions présumées ou des condamnations pénales qui, conformément à l'article 8, paragraphe 5, de la directive 95/46/CE *«ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national»*. Bien que le traitement des données relatives à des violations présumées des DPI soit accordé au détenteur du droit pour défendre ses intérêts dans des conditions spécifiques, il ne doit pas être accordé au-delà de ce qui est nécessaire et proportionné à cette finalité.

45. À cet égard, comme expliqué à la section III.2 ci-dessus, d'un point de vue de la protection des données, les détenteurs du droit ne seraient autorisés à entreprendre qu'une surveillance ciblée dans le cadre de situations ad hoc spécifiques et limitées, basées sur des soupçons fondés de violations de droit d'auteur à l'échelle commerciale.[44] En outre, compte tenu des risques spécifiques posés aux droits et libertés des individus, cette surveillance devrait être soumise à des garanties supplémentaires en matière de protection des données, telles que le contrôle préalable ou l'autorisation par les autorités nationales pertinentes en matière de protection des données[45].

---

d'expérience sont implicitement exclus du champ d'application de la législation proposée; il serait utile que cette exclusion soit explicite».

[43] D'après l'article 27, paragraphe 4, une partie *«peut prévoir que ses autorités compétentes seront habilitées, en conformité avec ses lois et réglementations, à ordonner à un fournisseur de services en ligne de divulguer rapidement au détenteur du droit des renseignements suffisants pour lui permettre d'identifier un abonné dont il est allégué que le compte aurait été utilisé en vue de porter atteinte à des droits, lorsque le détenteur du droit a présenté des allégations suffisantes sur le plan juridique, relativement à une atteinte à une marque de fabrique ou de commerce ou au droit d'auteur ou à des droits connexes, et lorsque ces renseignements sont demandés aux fins de la protection ou du respect de ces droits»*

[44] Voir paragraphe 45 et suivants de l'avis du CEPD du 22 février 2010 sur l'ACAC.

[45] L'article 20 de la directive 95/46/CE permet aux États membres de déterminer les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre.

46. D'un point de vue procédural, le traitement de données judiciaires par des parties privées, en particulier la divulgation par les fournisseurs d'accès à Internet aux détenteurs du droit de données à caractère personnel permettant l'identification d'un abonné soupçonné de violation des DPI, en vue de faire respecter ces droits, doit se faire sous le contrôle d'une autorité judiciaire.[46] Cela est actuellement le cas en ce qui concerne la divulgation de données à caractère personnel dans le contexte des procédures civiles au titre de la directive IPRE, dont l'article 8 dispose que les autorités judiciaires peuvent imposer aux fournisseurs d'accès à Internet de fournir les informations personnelles dont ils disposent sur les contrevenants présumés (par ex. des informations sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle) en réponse à une demande justifiée et proportionnée du requérant dans des cas de violations à l'«échelle commerciale». L'implication des autorités judiciaires est un élément essentiel du système actuel de l'UE, et capital pour assurer que l'application se fait dans le respect de la procédure et des droits fondamentaux.

47. Toutefois, aucune précision n'est donnée quant aux *«autorités compétentes»* investies de ce pouvoir d'injonction conformément à l'article 27, paragraphe 4, de l'accord. L'utilisation d'une notion vague d'*«autorités compétentes»* n'offre pas la certitude juridique selon laquelle la divulgation de données à caractère personnel au titre de cette disposition ne se fera que sous le contrôle d'organes judiciaires. Bien au contraire, cette notion peut également inclure les organes administratifs qui se sont vus confier des tâches quasi-judiciaires spécifiques, sans toutefois être soumis à toutes les garanties d'indépendance, d'impartialité et de respect des droits à la présomption d'innocence et à un jugement équitable qui s'appliquent aux organes judiciaires.

48. De plus, les conditions devant être remplies par les détenteurs du droit pour se voir accorder un tel pouvoir d'injonction ne sont également pas particulièrement satisfaisantes. Le détenteur du droit doit avoir présenté «*des allégations suffisantes sur le plan juridique, relativement à une atteinte à une marque de fabrique ou de commerce ou au droit d'auteur ou à des droits connexes»* et doit demander ces renseignements *«aux fins de la protection ou du respect de ces droits»*. Cette formulation est sensiblement plus faible que celle de la directive IPRE, en vertu de laquelle l'injonction ne serait accordée que si la requête est posée *«dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle»*, et si la demande est *«justifiée et proportionnée»*. Dans le cadre de la directive IPRE, il appartient aux cours et tribunaux d'évaluer, au cas par cas, les faits et la gravité du méfait présumé, comme son échelle et les risques d'atteinte à la vie privée des individus, afin de décider si oui ou non ces informations doivent être divulguées.

49. Les incertitudes relevées à l'article 27, paragraphe 4, pourraient avoir un impact significatif dans le contexte des ordonnances extraterritoriales émises par des autorités compétentes étrangères aux fournisseurs d'accès Internet basés en Europe. La formulation actuelle de l'accord pourrait légitimer les ordonnances des organes non

[46] Document du Groupe de travail «Article 29», WP104, page 7: «Comme indiqué à l'article 8 de la directive sur la protection des données, le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que dans des conditions strictes, telles que prévues par les États membres. Même si tout individu a naturellement le droit d'exploiter des données judiciaires dans le cadre de litiges le concernant, le principe ne va pas jusqu'à permettre l'examen approfondi, la collecte et la centralisation de données à caractère personnel par des tiers, y compris, notamment, la recherche systématique à grande échelle, comme le balayage d'Internet ou la demande de communication de données personnelles détenues par d'autres acteurs, tels que les fournisseurs d'accès (…). De telles enquêtes sont de la compétence des autorités judiciaires».

judiciaires étrangers faites aux fournisseurs d'accès à Internet basés dans l'UE, pour qu'ils divulguent aux détenteurs du droit des informations permettant l'identification de leurs abonnés basés dans l'UE, même lorsque ces ordonnances dépassent le champ d'application d'une procédure juridique en cours. Ceci signifie que la protection des droits des individus à laquelle les abonnés à l'Internet basés dans l'UE auraient droit conformément à la législation de l'UE ne serait plus correctement garantie dans ce contexte.

IV.3. Les mécanismes de coopération en matière d'application et la surveillance d'Internet par les fournisseurs d'accès à Internet

50. Comme expliqué dans la section III.1 ci-dessus, l'article 27, paragraphe 3, prévoit l'introduction de mécanismes volontaires «privés» d'application, fondés sur une coopération volontaire entre les détenteurs de droits et les fournisseurs d'accès à Internet.

51. Leur coopération peut varier en termes de champ d'action et de forme: (i) dans le cadre des politiques de déconnexion d'Internet en trois temps, les fournisseurs d'accès à Internet sont généralement tenus d'identifier leurs abonnés afin de pouvoir leur transmettre des avertissements qui pourraient mener à la résiliation du contrat conclu avec eux, (ii) les fournisseurs d'accès à Internet sont également chargés par les détenteurs de droits de surveiller les comportements suspects sur Internet pour leur compte, par exemple dans le cas des déconnexions d'Internet en trois temps ou la surveillance des sites Web soupçonnés de présenter du contenu illicite, et (iii) les fournisseurs d'accès à Internet peuvent éventuellement être chargés par les détenteurs de droits de mettre en place des outils techniques qui permettent de filtrer le trafic «peer-to-peer» et de bloquer tout contenu présumé illicite, ce qui équivaudrait à surveiller, à grande échelle, les utilisateurs et leurs communications électroniques.

52. Ces formes de mécanismes de coopération en matière d'application impliquant le traitement de données à caractère personnel par des fournisseurs d'accès à Internet dans le but de faire respecter les DPI et/ou de surveiller le comportement des utilisateurs, y compris les communications électroniques, à grande échelle, suscitent de sérieuses inquiétudes d'un point de vue de la protection de la vie privée et des données. En outre, ces mécanismes pourraient mener à une interruption de l'accès à Internet ou au blocage de sites Web, ce qui pourrait entraver certaines libertés fondamentales, comme la liberté d'expression, la liberté de recevoir ou de communiquer des informations et l'accès à la culture[47].

53. Il y a lieu d'assurer que le rôle que devraient endosser les fournisseurs d'accès à Internet dans le cadre des mécanismes de coopération en matière d'application, qu'ils soient introduits dans la nouvelle législation ou à la demande des détenteurs de droits sous la forme d'accords privés, est conforme à leurs droits et obligations prévus par la législation européenne ainsi qu'à la protection des données à caractère personnel et de la vie privée des personnes physiques dans l'UE. La récente jurisprudence de la Cour de justice en ce qui concerne les mesures imposées aux fournisseurs d'accès à Internet pour faire respecter les DPI permet véritablement de clarifier les limites qui régissent les activités des fournisseurs d'accès à Internet dans le contexte du respect des DPI sur Internet conformément à la législation européenne.

[47] Ces points sont mentionnés à titre de référence mais ne feront pas l'objet d'une discussion plus approfondie étant donné que cet avis ne traite que des questions liées à la protection des données et de la vie privée des personnes physiques.

54. Premièrement, conformément au régime de responsabilité actuel des fournisseurs d'accès à Internet détaillé dans la directive sur le commerce électronique, et notamment son article 15, paragraphe 1[48], aucune mesure impliquant la mise en place d'une surveillance générale des informations passant par leur réseau ne peut être imposée aux fournisseurs d'accès à Internet. Dans l'affaire *Scarlet / Sabam*[49], la Cour a analysé le traitement des données effectué par un fournisseur d'accès qui avait été chargé de mettre en place un système de filtrage dans le but de prévenir la violation des DPI. La Cour a fait remarquer que ce type de système de filtrage contraindrait le fournisseur d'accès à Internet à surveiller activement toutes les données liées à ses clients et à surveiller toutes les communications électroniques effectuées sur son réseau, qu'ils pratiquent ou non des activités de téléchargement illégal. La Cour a conclu que ce genre de système de filtrage donnerait lieu à une obligation générale de surveillance, ce qui serait contraire à l'article 15, paragraphe 1, de la directive sur le commerce électronique 2000/31/CE.

55. Deuxièmement, ces types de mesures dépasseraient le cadre légal du traitement que les fournisseurs d'accès à Internet sont autorisés à effectuer en vertu de la loi sur la protection des données, et en particulier de la directive «vie privée et communications électroniques». Il n'existe aucune base juridique au titre de la directive «vie privée et communications électroniques» et de la directive 2006/24/CE sur la conservation des données qui autoriserait les fournisseurs d'accès à Internet à conserver légalement les liens entre les adresses IP individuelles et l'utilisation d'Internet aux fins de surveillance ou d'analyse à long terme pour l'identification d'«éventuelles» violations de DPI[50]**.** En outre, le fait que les fournisseurs d'accès à Internet puissent détenir certaines données ne signifie pas que ces données puissent être transférées aux détenteurs de droits d'auteur à d'autres fins. À cet égard, la divulgation des informations qu'ils détiennent conformément à la directive sur la conservation des données est limitée aux autorités nationales compétentes *«à des fins d'enquête, de détection et de poursuite judiciaire d'une infraction pénale grave, telle que définie par chaque État membre dans son droit interne»*[51]. En outre, la surveillance des communications électroniques échangées sur leurs réseaux constituerait une violation de la confidentialité des communications développée à l'article 5 de la directive «vie privée et communications électroniques», sans pour autant être justifiée par l'une des exceptions prévues à l'article 15 de la même directive. Enfin, la divulgation par des fournisseurs d'accès à Internet de données relatives aux communications électroniques à des tiers sans l'accord des utilisateurs constituerait une violation de l'article 5 de la directive «vie privée et communications électroniques».

56. Troisièmement, comme expliqué dans la section III.2 ci-dessus, ce type de mesures pourrait impliquer une surveillance des activités des internautes disproportionnée par rapport à l'objectif du respect des DPI. À cet égard, la Cour a défendu, dans le cadre de l'affaire *Scarlet / Sabam*[52], le principe suivant: si une mesure implique la surveillance de

[48] L'article 15, paragraphe 1, de la directive 2000/31/CE prévoit que *«[l]es États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites»*.

[49] Voir note de bas de page 37.

[50] Voir para. 54 à 60 de l'avis du CEPD du 22 février 2010 sur l'ACAC.

[51] Voir article 4 de la directive sur la conservation des données, ainsi que l'arrêt du 19 avril 2012, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB*, paragraphe 41.

[52] Voir note de bas de page 37.

toutes les communications électroniques et que cette mesure n'est pas bien définie et spécifique au niveau spatial, temporel et personnel, elle ne respecterait pas l'exigence selon laquelle un juste équilibre doit être établi entre les DPI et les autres libertés et droits fondamentaux[53].

57. Enfin, les mécanismes de coopération volontaire en matière d'application ne peuvent être utilisés comme moyen de contourner la loi. Le CEPD considère qu'il n'y a pas suffisamment de garanties que les mesures volontaires prises par des acteurs privés en plus de celles de l'ACAC n'aillent pas au-delà du juste équilibre à assurer entre les DPI et la protection des données.

IV.4. Coopération et échanges de données transfrontaliers

58. Plusieurs dispositions de l'ACAC prévoient l'échange international d'informations, par exemple, entre les autorités frontalières (article 29) et entre les autorités publiques (article 34). Toutefois, les dispositions de l'ACAC sur le partage des informations et la coopération sont formulées de manière très large, si bien que la question du type de données pouvant être échangées et des destinataires n'est pas très claire. Ces échanges pourraient couvrir tout type d'informations, y compris des données à caractère personnel liées à des suspicions de violation de DPI. De plus, d'autres dispositions de l'ACAC pourraient impliquer le transfert international d'informations entre des parties privées et/ou entre des parties publiques et privées (par exemple, dans le contexte de procédures d'application envisagées à l'article 11 et à l'article 27, paragraphe 4).

59. Premièrement, le CEPD insiste sur le fait que l'ensemble des procédures envisagées dans l'accord impliquant le traitement de données à caractère personnel d'individus relevant de la législation européenne doit respecter les lois relatives à la protection des données; cette protection couvre toutes les catégories d'individus, quel que soit leur nationalité ou leur lieu de résidence, y compris ceux soupçonnés ou susceptibles d'être impliqués dans des actes de contrefaçon et de piratage à grande échelle.

60. À l'instar de toutes les mesures ayant un impact sur les droits des individus au respect de la vie privée et à la protection des données, les transferts de données à caractère personnel, dans ce contexte, doivent satisfaire aux critères de nécessité et de proportionnalité. Le CEPD a déjà déclaré dans son précédent avis que les principes de nécessité et de proportionnalité des transferts de données seraient plus facilement appliqués si l'accord se limitait expressément à la lutte contre les infractions les plus graves en matière de droits de propriété intellectuelle, plutôt que d'autoriser des transferts de données en masse au moindre soupçon de violation[54]. Cette position n'a pas été suivie puisque la formulation de l'accord est particulièrement floue quant à la portée des procédures d'application (comme expliqué à la section IV.1 ci-dessus).

61. En outre, les transferts de données à caractère personnel à des destinataires situés en dehors de l'UE doivent être effectués conformément aux exigences en matière de protection des données. Les articles 25 et 26 de la directive 95/46/CE détaillent les conditions en vertu desquelles les transferts internationaux de données à caractère personnel peuvent être effectués. Des règles spécifiques s'appliquent aux transferts de données dans le cadre de l'application des lois pénales. Elles ont été détaillées dans la

[53] Voir points 45 et suivants de l'arrêt.
[54] Voir paragraphe 67 de l'avis du CEPD du 22 février 2010 sur l'ACAC.

convention n° 108 du Conseil de l'Europe et dans son protocole additionnel[55], ainsi que dans la décision cadre 2008/877/JAI du Conseil[56]. Toutes ces règles sont fondées sur des principes communs, en particulier du fait que les transferts à des destinataires situés dans des pays qui ne sont pas réputés pour fournir un niveau de protection approprié doivent respecter des garanties additionnelles clairement définies dans un instrument juridiquement contraignant (comme par exemple, la quantité et les types de données transférées, les restrictions au niveau des transferts suivants, le délai de conservation des données, les mécanismes de supervision et de recours efficaces).

62. Par conséquent, le CEPD souligne que l'UE devra conclure des accords spécifiques avec ses partenaires commerciaux afin d'assurer des garanties de protection des données adéquates dans le cadre des échanges de données à caractère personnel avec des destinataires dans ces pays.

IV.5. L'absence de garanties appropriées dans l'ACAC

63. En vertu de l'article 27, paragraphes 2, 3 et 4, de l'accord, les moyens de faire respecter les droits de propriété intellectuelle dans l'environnement numérique doivent respecter les «principes fondamentaux comme la liberté d'expression, les procédures équitables et le respect de la vie privée». Le CEPD précise qu'une simple référence à ces principes n'est pas suffisante. De plus, les «principes fondamentaux» et les «procédures équitables» sont des notions vagues.

64. Au niveau international, la liberté d'expression et le respect de la vie privée sont considérés comme des droits fondamentaux dans la déclaration universelle des droits de l'homme, et non comme de simples «principes». De plus, la notion de «procédure équitable» ne correspond à aucun droit de l'homme généralement reconnu. Elle semble reprendre deux concepts juridiques: d'une part, le droit à un procès équitable (reconnu à l'article 10 de la déclaration universelle des droits de l'homme et à l'article 47 de la Chartre des droits fondamentaux de l'UE) et, d'autre part, la notion de «respect du droit» (utilisé par exemple dans la constitution des États-Unis comme moyen de protection contre la privation de la vie, de la liberté ou des biens sans le respect du droit).

65. Il est important de souligner que l'Union européenne a énoncé, précisément dans le contexte de la révision de la directive 2002/21/CE susmentionnée, les garanties nécessaires pour l'exécution des mesures concernant l'accès des utilisateurs finals aux services et aux applications, et leur utilisation, via les réseaux de communications électroniques. Elles comprennent notamment des garanties procédurales appropriées et conformes à la Convention européenne des droits de l'homme et aux principes généraux du droit communautaire, y compris le droit à une protection juridictionnelle effective, le respect du droit, le principe de présomption d'innocence et le droit au respect de la vie privée.[57]

---

[55] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée à Strasbourg le 28 janvier 1981, et Conseil de l'Europe, protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières des données, Strasbourg, le 8 novembre 2001.

[56] Décision cadre 2008/877/JAI du Conseil du 27 novembre 2008 sur la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60.

[57] L'article 1er, paragraphe 1, point b), de la directive 2009/140/CE, insérant un nouveau paragraphe 3 *bis*, à l'article 1er de la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communication électroniques (appelé l'«amendement 138»): «Les mesures prises par les États membres concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de

66. Le CEPD insiste sur les avantages d'une telle approche, qui établit clairement les limites et les garanties dans le cadre desquelles les mesures relatives à l'utilisation et à la surveillance des réseaux de communication électronique peuvent s'appliquer. Il aurait par conséquent été utile que l'ACAC établisse clairement ce genre de garantie.

V. CONCLUSION

67. Bien que le CEPD reconnaisse la préoccupation légitime d'assurer le respect des DPI dans un contexte international, il convient de trouver un juste équilibre entre les demandes de protection des DPI et des droits au respect de la vie privée et à la protection des données.

68. Le CEPD souligne que les moyens envisagés pour renforcer le respect des DPI ne doivent pas se faire aux dépens des libertés et droits fondamentaux des individus au respect de la vie privée, à la protection des données, à la liberté d'expression, et d'autres droits tels que la présomption d'innocence et une protection judiciaire efficace.

69. Bon nombre des mesures envisagées dans l'accord en vue de faire respecter les DPI dans l'environnement numérique impliqueraient la surveillance du comportement des utilisateurs et de leurs communications électroniques sur Internet. Ces mesures sont extrêmement intrusives dans la vie privée des individus et, si elles ne sont pas mises en œuvre correctement, elles pourraient interférer avec leurs droits et libertés, notamment le droit au respect de la vie privée, à la protection des données et à la confidentialité de leurs communications.

70. Il convient d'assurer que toute mesure d'application en ligne mise en œuvre au sein de l'UE suite à la conclusion de l'ACAC est nécessaire et proportionnée eu égard à la finalité du respect des DPI. Le CEPD souligne que les mesures qui permettent la surveillance indifférenciée ou généralisée du comportement des utilisateurs d'Internet et/ou de leurs communications électroniques, dans la lutte contre des infractions minimes, à petite échelle et sans but lucratif, seraient disproportionnées et contraires à l'article 8 de la CEDH, aux articles 7 et 8 de la Charte des droits fondamentaux et à la directive sur la protection des données.

71. Plusieurs dispositions de l'accord suscitent des craintes spécifiques chez le CEPD, plus particulièrement:

---

communications électroniques respectent les libertés et droits fondamentaux des personnes physiques, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les principes généraux du droit communautaire. Toute mesure susvisée concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques qui serait susceptible de limiter les libertés et droits fondamentaux précités ne peut être instituée que si elle est appropriée, proportionnée et nécessaire dans le cadre d'une société démocratique, et sa mise en oeuvre est subordonnée à des garanties procédurales adéquates conformément à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et aux principes généraux du droit communautaire, y compris le droit à une protection juridictionnelle effective et à une procédure régulière. Par voie de conséquence, les mesures en question ne peuvent être prises que dans le respect du principe de la présomption d'innocence et du droit au respect de la vie privée. Une procédure préalable, équitable et impartiale est garantie, y compris le droit de la ou des personnes concernées d'être entendues, sous réserve de la nécessité de conditions et de modalités procédurales appropriées dans des cas d'urgence dûment établis conformément à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Le droit à un contrôle juridictionnel effectif en temps utile est garanti».

- l’accord ne donne aucune précision concernant la portée des mesures d’application dans l’environnement numérique envisagées à l’article 27, et permettant de déterminer si elles ne visent que les violations à grande échelle des DPI. La notion d’«échelle commerciale» contenue à l’article 23 de l’accord n’est pas définie avec suffisamment de précision, et les actes commis par les utilisateurs privés à des fins personnelles et non lucratives ne sont pas expressément exclus du champ d’application de l’accord;

- la notion d’«autorités compétentes» investies d’un pouvoir d’injonction conformément à l’article 27, paragraphe 4, de l’accord est trop vague et n’offre pas de certitude suffisante que la divulgation des données à caractère personnel des contrevenants présumés ne se ferait que sous le contrôle d’autorités judiciaires. En outre, les conditions à remplir par les détenteurs du droit pour se voir accorder une telle injonction ne sont également pas satisfaisantes. Ces incertitudes ont un impact particulier dans le cadre des requêtes d’«autorités compétentes» étrangères faites aux fournisseurs d’accès à Internet basées dans l’UE;

- bon nombre des mesures de coopération volontaire en matière d’application qui pourraient être mises en œuvre au titre de l’article 27, paragraphe 3, de l’accord impliqueraient un traitement des données à caractère personnel par les fournisseurs d’accès à Internet allant au-delà de ce qui est autorisé par la législation de l’UE;

- l’accord ne contient pas de limitations et garanties suffisantes en ce qui concerne la mise en œuvre des mesures qui impliquent la surveillance des réseaux de communications électroniques à grande échelle. Plus particulièrement, il ne prévoit pas de garanties telles que le droit au respect de la vie privée et à la protection des données, une protection juridictionnelle effective, une procédure régulière, et le respect du principe de la présomption d’innocence.

Fait à Bruxelles, le 24 avril 2012

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données