I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

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)

(2010/C 147/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 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 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 télécommunications électroniques [2],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, notamment son article 41 [3],

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. L'Union européenne prend part aux négociations sur l'ébauche d'un accord commercial anti-contrefaçon (ACAC). Ces négociations ont été lancées en 2007 par un groupe initial de différentes parties intéressées. Elles se sont ensuite élargies à d'autres participants et incluent, aujourd'hui l'Australie, le Canada, l'Union européenne, le Japon, la Corée, le Mexique, le Maroc, la Nouvelle-Zélande, Singapour, la Suisse et les États-Unis. La Commission européenne a reçu pour mandat, de la part du Conseil, d'intégrer ces négociations en 2008.

2. Le CEPD reconnaît que le commerce transfrontalier de biens contrefaits ou piratés est de plus en plus préoccupant et implique souvent des réseaux criminels organisés. Ce phénomène exige donc l'adoption de mécanismes de coopération adéquats à l'échelle internationale, afin de lutter contre cette forme de criminalité.

3. Le CEPD insiste sur le fait que la négociation, par l'Union européenne, d'un accord multilatéral ayant pour objet principal le respect des droits relatifs à la propriété intellectuelle soulève de nombreuses questions quant à l'impact des mesures prises pour lutter contre la contrefaçon et le piratage sur les droits fondamentaux des individus, et en particulier leur droit à la vie privée et la protection des données.

4. À cet égard, le CEPD regrette particulièrement de ne pas avoir été consulté par la Commission européenne en ce qui concerne le contenu d'un tel accord. Le CEPD a donc adopté le présent avis de sa propre initiative, en se basant sur l'article 41, paragraphe 2, du Règlement (CE) nº 45/2001. Cet avis a pour but de présenter à la Commission une orientation en matière de respect de la vie privée et de protection des données, à prendre en compte dans le cadre des négociations sur l'ACAC.

II. ÉTAT DES LIEUX ET CONTENU ESCOMPTÉ DE L'ACAC

5. Le 7ème cycle de négociations qui s'est déroulé à Mexico, du 26 au 29 janvier 2010, avait pour but de parvenir à un accord courant 2010. Cependant, à ce jour, aucune version officielle d'un tel accord n'a encore été rendue publique.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 201 du 31.7.2002, p. 37.
[3] JO L 8 du 12.1.2001, p. 1.

6. Ces négociations ont pour but d'adopter un nouvel accord multilatéral visant à renforcer le respect des droits de propriété intellectuelle (DPI) et à combattre la contrefaçon et le piratage. S'il est adopté, ce nouvel accord déboucherait sur l'amélioration des normes internationales en matière de lutte contre les infractions à grande échelle des droits de propriété intellectuelle. La direction générale du commerce de la Commission européenne a particulièrement souligné le fait que «l'accent est mis sur les actes de contrefaçon et de piratage qui affectent sensiblement les intérêts commerciaux, plutôt que sur les actes émanant de citoyens ordinaires» ([4]).

7. En ce qui concerne le contenu de l'accord, le document *Summary of key elements under discussion* (*Résumé des éléments clés en cours d'examen*), publié par la direction générale du commerce de la Commission européenne en novembre 2009, précise que l'objectif de l'ACAC, à savoir la lutte contre le piratage et la contrefaçon, sera poursuivi par le biais de trois processus majeurs: i) coopération internationale, ii) pratiques de mise en application et iii) définition d'un cadre légal pour l'application des droits de propriété intellectuelle dans différents domaines identifiés et, en particulier, dans l'environnement numérique ([5]). Les mesures prévues traiteront notamment des procédures légales (telles que les injonctions ou les mesures temporaires), le rôle et les responsabilités des fournisseurs d'accès à Internet pour contrecarrer les atteintes aux droits d'auteur sur Internet, et la coopération internationale afin de prévenir le trafic de marchandises d'un pays à l'autre. Toutefois, les informations rendues publiques ne présentent l'accord que dans ses grandes lignes, sans entrer dans le détail des mesures spécifiques et concrètes.

8. Le CEPD observe que, même si l'intention de l'ACAC est de s'attaquer exclusivement aux infractions à grande échelle des droits de propriété intellectuelle, il n'est pas exclu que les actes commis par les citoyens ordinaires soient concernés, dès lors surtout que des mesures seront mises en œuvre dans l'environnement numérique. Le CEPD insiste sur le fait que des garanties appropriées devront être présentées pour la protection des droits fondamentaux des individus. Par ailleurs, les législations relatives à la protection des données concernent tous les individus, y compris les personnes potentiellement impliquées dans des actes de piratage et de contrefaçon. La lutte contre les infractions à grande échelle impliquera certainement aussi le traitement de données à caractère personnel.

9. À cet égard, le CEPD encourage vivement la Commission européenne à amorcer un dialogue public et transparent sur l'ACAC, par exemple sous la forme d'une consultation publique. Cette démarche contribuerait également à s'assurer que les mesures adoptées seront conformes aux législations européennes sur le respect de la vie privée et la protection des données.

III. **PORTÉE DES COMMENTAIRES DU CEPD**

10. Le CEPD en appelle vivement à l'Union européenne, et en particulier à la Commission européenne qui a reçu pour mandat de conclure cet accord, afin de trouver un juste équilibre entre les exigences de protection des droits de propriété intellectuelle, d'une part, et les droits des personnes physiques en matière de respect de la vie privée et de protection des données d'autre part.

11. Le CEPD insiste sur le fait que le respect de la vie privée et la protection des données représentent des valeurs fondamentales de l'Union européenne, reconnues dans 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'Union européenne ([6]). Ces valeurs doivent être respectées dans toutes les politiques et réglementations adoptées par l'Union européenne, conformément à l'article 16 du Traité relatif au fonctionnement de l'Union européenne (TFUE).

12. De plus, le CEPD met en avant le fait que tout accord conclu par l'Union européenne sur l'ACAC doit respecter les obligations légales imposées à l'UE en ce qui concerne le respect de la vie privée et la protection des données, comme le prévoient notamment la directive 95/46/CE, la directive 2002/58/CE ([7]), la jurisprudence de la Cour européenne des droits de l'homme ([8]) et de la Cour de Justice ([9]).

13. Le respect de la vie privée et la protection des données doivent être pris en compte dès le début des négociations, et non une fois que le projet et les procédures ont été définis et finalisés. Il serait alors trop tard pour trouver des solutions alternatives respectant la vie privée.

14. Vu le peu d'informations rendues publiques, le CEPD remarque qu'il n'est pas en position de présenter une analyse des dispositions spécifiques de l'ACAC. Dès lors, le CEPD mettra l'accent sur la description des menaces potentielles (en matière de respect de la vie privée et de protection des données) que les mesures concrètes possibles de l'accord, tel qu'il a été annoncé, pourraient poser dans les deux domaines suivants: respect des droits de propriété intellectuelle dans l'environnement numérique (chapitre IV) et mécanismes de coopération internationale (chapitre V).

([4]) Voir http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, p. 2.

([5]) Voir note 2 ci-dessus.

([6]) Charte des droits fondamentaux de l'Union européenne, JO C 303 du 14.12.2007, p. 1.

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

([8]) Après interprétation des principaux éléments et conditions stipulés dans l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), adoptée à Rome le 4 novembre 1950, applicables à différents domaines. Voir plus particulièrement la jurisprudence à laquelle il est fait référence ailleurs dans ce document.

([9]) Voir en particulier: affaire C-275/06, *Productores de Música de España* (Promusicae), REC [2008], p. I-271 et affaire C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, nyr.

IV. APPLICATION DES DROITS DE PROPRIÉTÉ INTELLECTUELLE DANS L'ENVIRONNEMENT NUMÉRIQUE

IV.1. Besoin d'analyser les implications des «politiques de déconnexion d'Internet en trois temps» sur le respect de la vie privée/la protection des données

15. Selon la Commission européenne, l'ACAC établira un cadre légal permettant de lutter contre le piratage dans l'environnement numérique ([10]). Ce cadre de travail définira les conditions dans lesquelles les fournisseurs d'accès à Internet et d'autres intermédiaires en ligne ([11]) pourront être tenus responsables des infractions aux droits d'auteur commises par le biais des supports transitant par leurs équipements. Il est également susceptible de suggérer des mesures et des solutions à imposer aux internautes qui chargeraient ou téléchargeraient des contenus en infraction avec les droits d'auteur. Bien que ce cadre de travail n'ait pas encore été officiellement présenté dans le détail, au vu des informations recueillies auprès des différentes sources, celui-ci prévoirait vraisemblablement des obligations à l'encontre des fournisseurs d'accès à Internet. Ceux-ci devront adopter des «politiques de déconnexion d'Internet en trois temps», que l'on appelle également une «riposte graduée». Un tel schéma permettra aux détenteurs de droits d'auteur de surveiller les internautes et d'identifier les utilisateurs qui commettent potentiellement des infractions. Une fois contacté, le fournisseur d'accès de l'internaute incriminé avertirait celui-ci. Après trois avertissements, sa connexion à Internet serait coupée.

16. Parallèlement aux négociations sur l'ACAC, ces politiques de déconnexion d'Internet en trois temps sont mises en œuvre dans certains États membres, dont la France. Elles font également l'objet de discussions sur différents forums de l'UE, dont les dialogues entre les parties intéressées sur le chargement illégal, animés par DG MARKT, conjointement à l'adoption de la communication de la Commission, renforçant le respect des droits de propriété intellectuelle sur le marché intérieur ([12]). Des discussions sur ce même sujet ont également lieu au sein du Parlement européen, dans l'attente d'un projet de résolution du Parlement européen sur le renforcement du respect des droits de propriété intellectuelle sur le marché intérieur («rapport Gallo»).

17. De telles pratiques portent clairement atteinte à la sphère privée des personnes physiques. Elles favorisent la surveillance généralisée des activités des internautes, y compris les activités parfaitement légales. Elles affectent ainsi des millions d'internautes respectueux des lois, dont de nombreux enfants et adolescents. Elles sont mises en œuvre par des sociétés privées et non par des autorités de contrôle. De plus, Internet joue aujourd'hui un rôle central dans pratiquement tous les aspects de la vie moderne. Par conséquent, une suspension de l'accès à Internet peut avoir des effets désastreux, isolant les personnes de leur travail, de la culture, des sites institutionnels, etc.

18. Dans ce contexte, il paraît indispensable de mesurer l'adéquation de telles règles avec la législation européenne en matière de protection des données et de respect de la vie privée, et plus particulièrement de vérifier si ces politiques de déconnexion en trois temps constituent une mesure nécessaire pour faire appliquer les droits de propriété intellectuelle. D'autres méthodes, moins intrusives, devraient également être envisagées.

19. L'intégration ou de ces politiques de déconnexion d'Internet en trois temps à l'ACAC n'a pas encore été clairement établie. Cependant, ces règles sont également envisagées dans d'autres domaines et ont un impact potentiel énorme sur la protection des données à caractère personnel et le respect de la vie privée. Pour ces raisons, le CEPD estime qu'il est nécessaire d'examiner ces différents aspects dans le cadre du présent avis. Mais avant de procéder à cette analyse, le CEPD souhaite décrire brièvement le cadre légal applicable en matière de protection des données et de respect de la vie privée.

20. Il est à noter qu'en plus de la protection des données et du respect de la vie privée, les politiques de déconnexion en trois temps suscitent des craintes sur d'autres valeurs, comme les droits de la défense et la liberté de parole. Toutefois, les présentes recommandations traiteront uniquement des aspects liés à la protection des données à caractère personnel et au respect de la vie privée.

IV.2. Politiques de déconnexion d'Internet en trois temps et application du cadre légal européen sur le respect de la vie privée/la protection des données

Mise en œuvre des politiques de déconnexion d'Internet en trois temps

21. En un mot, si les politiques de déconnexion d'Internet en trois temps étaient appliquées, les détenteurs de droits d'auteur utiliseraient des outils techniques automatiques, potentiellement mis à leur disposition par des tiers, afin d'identifier d'éventuelles infractions aux droits d'auteur. Pour cela, ils surveilleraient les activités des internautes,

([10]) Voir note 2 plus haut.

([11]) Les différents intermédiaires en ligne peuvent être définis selon leur rôle fonctionnel. Cependant, dans la réalité, les intermédiaires associent généralement plusieurs de ces fonctions. Les intermédiaires en ligne incluent, entre autres: a) *fournisseurs d'accès:* les utilisateurs se connectent au réseau via le serveur d'un fournisseur d'accès; b) *fournisseurs de réseaux:* ils fournissent les routeurs, autrement dit les équipements techniques nécessaires pour la transmission des données; c) *hébergeurs:* ils louent de l'espace sur leur serveur, afin que les utilisateurs ou les fournisseurs de contenus puissent y charger leurs contenus. Les utilisateurs peuvent télécharger des supports depuis/vers un service en ligne, tel qu'un bulletin ou un réseau P2P.

([12]) Communication de la Commission au Conseil, au Parlement européen et au Comité économique et social européen, renforçant le respect des droits de propriété intellectuelle sur le marché intérieur, Bruxelles, le 11 septembre 2009, COM(2009) 467 final.

par exemple en épiant les forums et les blogs ou en se faisant passer pour des utilisateurs dans les réseaux peer-to-peer afin de repérer les internautes qui échangent des supports soumis à des droits d'auteur ([13]).

22. Après avoir identifié les internautes prétendument impliqués dans une violation des droits d'auteur en recueillant leur adresse IP (Internet Protocol), les détenteurs des droits d'auteur transmettraient ces adresses IP aux fournisseurs d'accès concernés. Ceux-ci avertiraient ensuite les abonnés en question sur leur infraction potentielle aux droits d'auteur. Plusieurs avertissements de la part du fournisseur d'accès déboucheraient sur une résiliation ou une suspension de l'abonnement à Internet ([14]).

Cadre légal européen applicable en matière de protection des données/respect de la vie privée

23. Les politiques de déconnexion d'Internet en trois temps doivent être conformes aux dispositions en matière de respect de la vie privée, telles qu'énoncées à l'article 8 de la Convention européenne des droits de l'homme et à l'article 7 de la Charte de droits fondamentaux, ainsi qu'aux dispositions en matière de droit à la protection des données, telles qu'énoncées à l'article 8 de la Charte des droits fondamentaux et à l'article 16 du TFUE, et définies dans la directive 95/46/CE et dans la directive 2002/58/CE.

24. Selon le CEPD, la surveillance des comportements des internautes et la collecte de leur adresse IP équivalent à une interférence dans leur droit au respect de la vie privée et de leurs correspondances. En d'autres mots, il y a là une interférence dans la vie privée. Ce point de vue est en adéquation avec la jurisprudence de la Cour européenne des droits de l'homme ([15]).

25. La directive 95/46/CE est applicable ([16]) étant donné que les politiques de déconnexion d'Internet en trois temps impliquent la manipulation des adresses IP, lesquelles doivent être considérées, en tout cas dans les circonstances appropriées, comme des données personnelles. Les adresses IP sont des identifiants semblables à une chaîne de chiffres séparés par des points, par exemple 122.41.123.45. Tout abonnement chez un fournisseur d'accès permet à l'abonné de se connecter à Internet. Chaque fois que l'abonné souhaite se connecter à Internet, il se voit attribuer une adresse IP par le biais du matériel utilisé pour accéder au Web (un ordinateur par exemple) ([17]).

26. Si un internaute s'engage dans une activité donnée, par exemple s'il publie un document sur Internet, il peut être identifié par un tiers via l'adresse IP qu'il utilise. Par exemple, il est présumé que l'internaute dont l'adresse IP est 122.41.123.45 a publié un document violant les droits d'auteur sur un service P2P, le 1er janvier 2010 à 15h. Le fournisseur d'accès à Internet pourra alors relier cette adresse IP au nom de l'abonné à qui il l'a attribuée et donc établir son identité.

27. Si l'on prend en compte la définition des données à caractère personnel, telle qu'énoncée à l'article 2 de la directive 95/46/CE, «toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification» ([18]), la seule conclusion possible est que les adresses IP et les informations relatives aux activités de ces adresses constituent des données personnelles dans tous les cas pertinents ici. En effet, une adresse IP sert de numéro d'identification qui permet de déterminer le nom de l'abonné à qui cette adresse a été attribuée. De plus, les informations collectées sur l'abonné qui possède cette adresse IP («il a publié certains documents sur le site Web ZS, le 1er janvier 2010 à 15h») *portent sur*, autrement dit concernent clairement les activités d'une personne identifiable (le propriétaire de l'adresse IP). Elles doivent donc également être considérées comme des données personnelles.

([13]) La technologie P2P est une architecture logicielle distribuée qui permet à différents ordinateurs de se connecter et de communiquer directement avec d'autres ordinateurs.

([14]) Des sanctions alternatives pourraient inclure, par exemple, la limitation des fonctionnalités de la connexion Internet, par exemple le débit ou le volume de données, etc.

([15]) Voir notamment la CEDH 26 juin 2006, *Weber and Saravia* v. *Germany* (déc.), nº 54934/00, point 77 et CEDH 1er juillet 2008, *Liberty and others* v *the UK*, nº 58243/00.

([16]) La Cour de Justice adopte un point de vue général sur l'applicabilité de la directive 95/46/CE, dont les dispositions doivent être interprétées à la lumière de l'article 8 de la CEDH. La Cour de Justice a précisé, dans son arrêt du 20 mai 2003, *Rundfunk*, affaires jointes C-465/00, C-138/01 et C-139/01, REC [2003], p. I-4989, point 68, que «les dispositions de la directive 95/46/CE, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect».

([17]) L'adresse IP que le fournisseur d'accès à Internet alloue à un utilisateur peut rester la même chaque fois que celui-ci navigue sur Internet (il s'agit alors d'une adresse IP statique). D'autres adresses IP sont dynamiques, ce qui signifie que le fournisseur d'accès alloue à l'utilisateur une adresse IP différente chaque fois qu'il se connecte à Internet. Évidemment, le fournisseur peut relier l'adresse IP au compte de l'abonné à qui il a attribué l'adresse IP, qu'elle soit statique ou dynamique.

([18]) Le considérant 26 complète cette définition: «Il y a lieu d'appliquer les principes de la protection à toute information concernant une personne identifiée ou identifiable. Afin de déterminer si une personne est identifiable, il convient de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement utilisés par le responsable du traitement ou par toute autre personne pour identifier ladite personne. Il n'y a pas lieu d'appliquer les principes de la protection aux données qui auront été rendues suffisamment anonymes pour que la personne concernée ne soit plus identifiable».

28. Ces points de vue sont entièrement partagés par le groupe de travail Article 29 qui, dans un document relatif aux aspects de protection des données à l'égard des droits de propriété intellectuelle, stipule que les adresses IP collectées pour faire appliquer les droits de propriété intellectuelle, *autrement dit* pour identifier les internautes incriminés dans des violations des droits de propriété intellectuels, sont des données à caractère personnel en ce sens qu'elles sont utilisées pour contraindre une personne données à respecter ces droits ([19]).

29. La directive 2002/58/CE est également applicable, étant donné que les politiques de déconnexion d'Internet en trois temps impliquent la collecte de données relatives au trafic et aux communications. La directive 2002/58/CE réglemente l'utilisation de ces données et définit le principe de confidentialité des communications réalisées sur des réseaux de communications publics, ainsi que des données inhérentes à ces communications.

IV.3. **Politiques de déconnexion d'Internet en trois temps: mesure nécessaire ou non?**

30. L'article 8 de la Convention européenne des droits de l'homme met en avant le principe de nécessité, en ce qu'une mesure, quelle qu'elle soit, violant le droit à la vie privée des individus est autorisée uniquement si elle constitue une mesure nécessaire, au sein d'une société démocratique, pour atteindre le but légitime poursuivi ([20]). Ce principe de nécessité apparaît également dans les articles 7 et 13 de la directive 95/46/CE et dans l'article 15 de la directive 2002/58/CE ([21]). Le principe exige une analyse de la proportionnalité de la mesure, laquelle doit être mesurée et fondée sur un équilibre des intérêts en jeu, dans une société démocratique dans son ensemble ([22]). Ceci implique également de déterminer s'il existe des mesures alternatives moins intrusives.

31. Le CEPD reconnaît l'importance de faire respecter les droits de propriété intellectuelle. Cependant, il estime que la règle de déconnexion d'Internet en trois temps telle qu'elle se présente, impliquant certains éléments d'application générale, constitue une mesure disproportionnée et ne peut donc être considérée comme une mesure nécessaire. De plus, le CEPD est convaincu que des solutions alternatives, moins intrusives, existent ou que les règles envisagées peuvent être mises en œuvre de façon moins intrusive ou plus limitée. Enfin, si l'on examine plus en détail les aspects juridiques, cette approche des trois avertissements pose certains problèmes. Ces conclusions sont décrites ci-dessous.

L'approche à trois avertissements est disproportionnée

32. Le CEPD souhaite souligner la grande portée des mesures imposées. À cet égard, il faut mentionner les éléments suivants:

i) la surveillance (invisible) affecterait des millions d'individus et *tous* les utilisateurs, qu'ils soient ou non suspects;

ii) la surveillance impliquerait l'enregistrement systématique des données, ce qui peut, dans certains cas, déboucher sur des procédures civiles, voire criminelles; de plus, certaines des informations collectées seraient considérées comme sensibles, conformément à l'article 8 de la directive 95/46/CE qui exige des garanties plus importantes;

iii) la surveillance est susceptible de générer de nombreux cas de faux positifs. Une violation des droits d'auteur n'est pas une simple question de «oui» ou de «non». Les tribunaux doivent souvent examiner une quantité très significative de détails techniques et juridiques, sur des dizaines de pages, avant de déterminer une éventuelle violation ([23]);

([19]) Groupe de travail Article 29, document de travail sur les aspects relatifs à la protection des données dans le cadre des droits de propriété intellectuelle (WP 104), adopté le 18 janvier 2005. Ce groupe de travail a été créé par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant dédié à la protection des données et au respect de la vie privée. Ses missions sont décrites à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. Voir également l'opinion 4/2007 du groupe de travail sur le concept des données à caractère personnel (WP 136), adoptée le 20 juin 2007, notamment p. 16.

([20]) L'article 8 de la Convention européenne des droits de l'homme dispose explicitement que toute interférence ou restriction est acceptable si elle se révèle «nécessaire à l'aune d'une société démocratique».

([21]) L'article 13 de la directive 95/64/CE autorise une limitation uniquement si celle-ci constitue «une mesure nécessaire pour sauvegarder: a) la sûreté de l'État; b) la défense; c) la sécurité publique; d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées; e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal; f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e); g) la protection de la personne concernée ou des droits et libertés d'autrui». L'article 15 de la directive 2002/58/CE exige qu'«une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, c'est-à-dire la sûreté de l'État, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE».

([22]) Voir aussi CEDH, 2 août 1984, *Malone v. the United Kingdom*, série A n° 82, p. 32, points 81 et suivants, et CEDH, 4 décembre 2008, *Marper v. the United Kingdom* [GC], n° 30562/04 et 30566/04, points 101 et suivants.

([23]) Les tribunaux devront, dans certains cas, vérifier si les supports sont effectivement protégés par des droits d'auteur, si ces droits ont été violés, si l'utilisation peut être considérée comme un cas d'usage loyal, la législation applicable, les dommages occasionnés, etc.

iv) les *effets* potentiels de la surveillance, qui peuvent se traduire par une interruption de l'accès à Internet. Ceci risque d'interférer avec le droit de chacun à la liberté d'expression, la liberté d'information et l'accès à la culture, aux sites institutionnels, aux places de marché, à la messagerie électronique et, dans certains cas, à des activités professionnelles. Dans ce contexte, il est particulièrement important de comprendre que ces effets seront ressentis non seulement au niveau de l'internaute incriminé, mais aussi de tous les membres de la famille qui utilisent la même connexion à Internet, y compris les enfants qui en ont besoin pour leurs activités scolaires;

v) l'entité qui évaluera la situation et prendra la décision sera généralement une entité privée (*autrement dit* les détenteurs des droits d'auteur ou le fournisseur d'accès à Internet). Le CEPD a déjà exprimé, lors de précédentes recommandations, ses inquiétudes concernant la surveillance des personnes physiques par le secteur privé (*par exemple* les fournisseurs d'accès ou les détenteurs de droits d'auteur), dans des domaines qui relèvent, en principe, de la compétence des autorités chargées de l'aplication de la loi ([24]).

33. Le CEPD n'est pas convaincu que les avantages des mesures contrebalancent l'impact sur les droits fondamentaux des individus. La protection des droits d'auteur est primordiale à la fois pour les détenteurs de droits et pour la société. Cependant, les restrictions imposées aux droits fondamentaux ne semblent pas justifiées si la gravité de l'interférence, *autrement dit* l'ampleur de l'intrusion dans la vie privée comme soulignée plus haut, est mise en balance avec les avantages attendus, dissuadant la violation des droits de propriété intellectuelle impliquant, pour la majeure partie, des infractions mineures aux droits de propriété intellectuelle. Comme indiqué dans l'avis de l'avocat général Kokott dans *Promusicae*: «Il n'est … pas certain que le partage privé de fichiers, en particulier lorsqu'il est réalisé sans aucune intention de réaliser des profits, menace la protection des droits d'auteur suffisamment sérieusement pour justifier le recours à cette exception. L'ampleur réelle des dommages causés par le partage privé de fichiers fait l'objet de nombreuses contestations» ([25]).

34. Dans ce contexte, il est également utile de rappeler la réaction du Parlement européen aux «politiques des trois avertissements» dans le cadre du Paquet Télécom, en particulier l'amendement 138 de la directive «cadre» ([26]). Cet amendement prévoit que toute restriction des libertés et droits fondamentaux ne peut être instituée que si elle est appropriée, proportionnée et nécessaire dans le cadre d'une société démocratique, et si sa mise en œuvre est subordonnée à des garanties procédurales adéquates, conformément à la Convention européenne 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 ([27]).

35. À cet égard, le CEPD souligne également que toute restriction des droits fondamentaux fera l'objet d'une investigation approfondie, à l'échelle nationale comme à l'échelle européenne. Dans ce cadre, un parallèle peut être fait avec la directive sur la rétention des données 2006/24/CE ([28]), qui déroge au principe général de protection des données qui exige leur effacement lorsqu'elles ne servent plus les finalités pour lesquelles elles ont été collectées. Cette directive exige que les données de trafic soient conservées à des fins de lutte contre les infractions pénales graves. Il est à noter que cette rétention est autorisée uniquement pour les cas d'infractions pénales graves, qu'elle doit se limiter aux «données relatives au trafic», ce qui exclut en principe toute information relative au contenu des communications. De plus, des garanties strictes doivent être appliquées. Néanmoins, des doutes ont été émis quant à sa compatibilité avec les règles en matière de droits fondamentaux; la Cour constitutionnelle roumaine a décidé qu'une rétention globale était incompatible avec les droits fondamentaux ([29]). Une affaire est également pendante devant la Cour constitutionnelle allemande ([30]).

Existence d'autres méthodes moins intrusives

36. Les conclusions ci-dessus sont renforcées par le fait que des méthodes moins intrusives permettent d'atteindre le même objectif. Le CEPD insiste pour que de tels modèles moins intrusifs soient examinés et testés.

([24]) Avis du CEPD du 23 juin 2008 sur la proposition de décision établissant un programme communautaire pluriannuel pour la protection des enfants utilisant Internet et d'autres technologies de communication, JO C 2 du 7.1.2009, p. 2.

([25]) Voir le cas mentionné à la note 8, pt. 106.

([26]) Voir la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009, JO L 337 du 18.12.2009, p. 37.

([27]) La formulation finale du fameux amendement 138 est la suivante: «Article 1.3a. Les mesures prises par les États membres concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de 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 œuvre 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.»

([28]) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006, JO L 105 du 13.4.2006, p. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. Dans ce contexte, le CEPD rappelle que la directive 2002/22/CE telle que modifiée concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive «service universel»), qui fait partie du Paquet Télécom récemment réformé, contient certaines règles et procédures limitant les petites infractions des droits d'auteur parmi les consommateurs ([31]). Ces procédures incluent, entre autres, l'obligation, pour les États membres, de communiquer des informations normalisées d'intérêt public sur différents sujets, en mentionnant spécifiquement les violations des droits d'auteur et autres droits associés, ainsi que leurs conséquences légales ([32]). Les États membres peuvent ensuite demander aux fournisseurs d'accès à Internet de diffuser ces informations à tous leurs clients et de les intégrer dans leurs contrats.

38. Ce système a pour but d'informer et de dissuader les internautes de diffuser des informations protégées par des droits d'auteur et de s'adonner à des activités illicites, tout en évitant toute surveillance des accès à Internet et autres risques liés à la protection des données et au respect de la vie privée. La directive «service universel» doit entrer en vigueur en mai 2011. Ces procédures ne sont donc pas encore applicables. Par conséquent, leurs avantages n'ont pas encore pu être vérifiés. Il semble donc prématuré de négliger les avantages potentiels de ces nouvelles procédures et d'adopter à la place les «politiques de déconnexion en trois temps», lesquelles sont bien plus restrictives en matière de droits fondamentaux.

39. En outre, il faut rappeler que la directive 2004/48/CE du 28 avril 2004 relative au respect des droits de propriété intellectuelle présente différents outils permettant de faire appliquer ces droits devant les tribunaux (voir ci-dessous, paragraphes 43 et suivants) ([33]).

40. La directive IPRE (respect des droits de propriété intellectuelle) n'a été que récemment transposée dans les législations respectives des États membres. Trop peu de temps s'est écoulé, jusqu'à présent, pour permettre de mesurer l'efficacité de ses dispositions dans le respect des droits de propriété intellectuelle. Par conséquent, toute nécessité de remplacer le système actuel, basée sur des procédures juridictionnelles, est au minimum contestable, faute d'expérimentation. Les considérations ci-dessus posent inévitablement la question suivante: pourquoi les violations ne peuvent-elles pas être punies par les pénalités civiles et criminelles déjà existantes pour les infractions aux droits de propriété intellectuelle? Par conséquent, avant de proposer de telles mesures, la Commission doit présenter des informations fiables démontrant que le cadre juridique actuel ne parvient pas à produire les effets escomptés.

41. De plus, il n'a pas été clairement établi si des modèles économiques alternatifs, qui n'impliqueraient pas la surveillance systématique des utilisateurs, ont été, ou non, sérieusement envisagés. Par exemple, si des détenteurs de droits d'auteur démontrent les pertes subies suite à l'utilisation d'un réseau PEP, ils pourraient, ainsi que les fournisseurs d'accès à Internet, par exemple, expérimenter différents types d'abonnements à Internet, dans lesquels une partie du prix d'un abonnement à accès illimité serait redistribuée aux détenteurs de droits d'auteur.

Possibilité d'une surveillance ciblée et moins intrusive

42. Outre l'utilisation de modèles complètement différents, qui devraient, comme indiqué, être examinés et testés, une surveillance ciblée pourrait également être mise en place de façon moins intrusive.

43. L'objectif qui consiste à faire respecter les droits de propriété intellectuelle peut également être atteint par une surveillance limitée aux seuls internautes soupçonnés de violations majeures des droits d'auteur. La directive IPRE fournit quelques orientations en ce sens. Elle met en avant les conditions dans lesquelles les autorités peuvent ordonner la divulgation des données à caractère personnel détenues par les fournisseurs d'accès à Internet, afin de faire respecter les droits de propriété intellectuelle. L'article 8 dispose que les fournisseurs d'accès à Internet peuvent se voir ordonner, par les autorités juridiques compétentes, de fournir les informations personnelles en leur possession à propos d'internautes soupçonnés d'infractions (par exemple, des informations relatives à l'origine et aux réseaux de diffusion des biens ou services en infraction avec des droits de propriété intellectuelle), en réponse à une requête, justifiée et proportionnée, dans des affaires de violations à *échelle commerciale* ([34]).

44. En conséquence, le critère d'échelle commerciale est décisif. Selon ce critère, la surveillance peut être proportionnée dans le contexte de situations *ad hoc* spécifiques et limitées, basées sur des soupçons fondés de violations de droits d'auteur à l'échelle commerciale. Ce critère peut concerner

([31]) Voir la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, JO L 337 du 18.12.2009, p. 11.

([32]) En particulier, l'article 21, paragraphe 4, de la directive 2009/136/CE dispose que «les États membres peuvent exiger que les entreprises visées au paragraphe 3 communiquent gratuitement aux abonnés existants et nouveaux des informations d'intérêt public, si besoin est, en recourant aux mêmes moyens que ceux qu'elles utilisent normalement pour communiquer avec leurs abonnés. Dans ce cas, ces informations sont fournies par les autorités publiques compétentes sous une forme normalisée et couvrent, entre autres, les sujets suivants: a) les modes les plus communs d'utilisation des services de communications électroniques pour se livrer à des activités illicites ou diffuser des contenus préjudiciables, en particulier lorsqu'ils peuvent porter atteinte au respect des droits et des libertés d'autrui, y compris les atteintes aux droits d'auteur et aux droits voisins, et les conséquences juridiques de ces utilisations (…).» De plus, comme précisé à l'article 20, paragraphe 2, «les États membres peuvent également exiger que le contrat comporte toutes les informations pouvant être fournies par les autorités publiques compétentes à cette fin sur l'utilisation des réseaux et des services de communications électroniques pour se livrer à des activités illicites ou diffuser des contenus préjudiciables, ainsi que sur les moyens de protection contre les risques d'atteinte à la sécurité individuelle, à la vie privée et aux données à caractère personnel, qui sont visées à l'article 21, paragraphe 4, et concernent le service fourni.»

([33]) JO L 157 du 30.4.2004, p. 45 (voir aussi: directive IPRE).

([34]) Ceci est également confirmé dans le considérant 14 de la directive IPRE.

des situations de violations claires des droits d'auteur par des particuliers, dans le but de générer des profits commerciaux directs ou indirects.

45. En pratique, pour que la procédure ci-dessus soit efficace, les détenteurs de droits d'auteur pourraient effectuer une surveillance ciblée de certaines adresses IP, afin de mesurer l'ampleur de la violation de leurs droits. Ceci signifie que les détenteurs de droits d'auteur seraient également, à ces fins, autorisés à conserver des rapports faisant état de ces violations. De telles informations ne pourraient être utilisées qu'après avoir évalué l'importance de la violation: par exemple, les cas avérés de violations majeures, ainsi que les violations non significatives mais répétées sur une période définie, à des fins d'avantages commerciaux ou de gains financiers. La nécessité d'une continuité sur une certaine période est soulignée et décrite plus en détail ci-dessous, dans la discussion relative au principe de conservation.

46. Autrement dit, en pareils cas, la collecte d'informations dans le but de démontrer une infraction présumée sur Internet peut être considérée comme proportionnée et nécessaire à la préparation des procédures légales, notamment des litiges.

47. À titre de garantie supplémentaire, le CEPD considère que les opérations de traitement des données dans le but de collecter ce type de preuves doivent être préalablement contrôlées et autorisées par les autorités nationales de protection des données. Ces propositions sont basées sur le fait que les opérations de traitement des données présenteraient des risques spécifiques pour les droits et les libertés des individus compte tenu de leur objectif, *à savoir* mener à bien des actions d'application de la loi éventuellement au niveau pénal, et sur la nature sensible des données collectées. Le fait que ce traitement implique la surveillance des communications électroniques est un facteur supplémentaire exigeant une supervision accrue.

48. Le CEPD considère que «l'échelle commerciale» dont il est question dans la directive IPRE est un élément tout à fait approprié pour définir les limites de la surveillance, si l'on veut respecter le principe de proportionnalité. Par ailleurs, il ne semble pas y avoir de preuve fiable démontrant, selon les critères établis par la directive IPRE, qu'une action légale effective en cas de violation des droits d'auteur se révèle impossible ou inefficace. Par exemple, des situations telles que celle de l'Allemagne qui a connu, suite à la transposition de la directive IPRE en 2008, près de 3 000 ordonnances judiciaires suite à la divulgation, par des fournisseurs d'accès à Internet, des informations concernant 300 000 abonnés, semblent suggérer le contraire.

49. En conclusion, étant donné que la directive IPRE est entrée en vigueur il y a seulement deux ans, il est difficile de comprendre pourquoi les législateurs délaisseraient les critères établis dans cette directive pour adopter des méthodes plus intrusives, alors que l'UE commence seulement à tester les méthodes récemment adoptées. Pour la même raison, il est également difficile de comprendre la nécessité de remplacer le système actuel, basé sur les décisions des tribunaux, par d'autres types de mesures (en plus de soulever des questions de droit commun, non traitées ici).

IV.4. **Conformité des «politiques de déconnexion d'Internet en trois temps» avec les dispositions plus détaillées de protection des données**

50. En matière de protection des données, la riposte en trois temps pose d'autres problèmes juridiques spécifiques. Le CEPD souhaite exprimer des doutes sur le fondement juridique du traitement, requis par la directive 95/46/CE, ainsi que sur le respect de l'obligation stipulée dans la directive 2002/58/CE pour la suppression des fichiers journaux.

Fondement légal du traitement

51. Les méthodes de riposte en trois temps impliquent le traitement de données personnelles, dont certaines seront utilisées dans le cadre de procédures légales ou administratives débouchant sur une suspension de l'accès à Internet en cas de violations répétées. De ce point de vue, ces données sont qualifiées de données sensibles, conformément à l'article 8 de la directive 95/46/CE. L'article 8, paragraphe 5, dispose que «le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté 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 …»

52. Dans ce contexte, il est pertinent de citer le document du groupe de travail Article 29, mentionné précédemment, qui aborde le traitement des données judiciaires ([35]). Le document précise que «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 (…). De telles enquêtes sont de la compétence des autorités judiciaires» ([36]). Bien que la collecte de preuves spécifiques et ciblées, en particulier dans les cas de violations graves, puissent s'avérer nécessaires pour établir et exercer une requête légale, le CEPD partage complètement les conclusions du groupe de travail Article 29 sur le manque de légitimité des investigations à grande échelle, impliquant l'exploitation de grandes quantités de données concernant les internautes.

53. La discussion décrite ci-dessus, autour du principe de proportionnalité, et le critère d'«échelle commerciale» sont pertinents pour déterminer les conditions dans lesquelles la collecte des adresses IP et autres informations connexes seront légitimes.

([35]) Voir le paragraphe 28 des présentes recommandations.
([36]) Soulignement ajouté.

54. Les fournisseurs d'accès à Internet pourraient essayer de légitimer cette procédure effectuée par les détenteurs de droits d'auteur, en insérant dans le contrat de leurs clients des clauses autorisant la surveillance de leurs données et la suspension de leur abonnement. En s'engageant dans ce type de contrat, le client serait considéré comme «ayant donné son aval à la surveillance». Cependant, cette pratique soulève d'abord la question fondamentale suivante: un individu peut-il donner à un fournisseur d'accès à Internet son accord pour l'exploitation de ses données par un tiers qui n'est pas sous «l'autorité» de ce fournisseur?

55. Ensuite, il y a la question de la validité de ce consentement. L'article 2, point h, de la directive 95/46/CE définit ce consentement comme «toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement». Un point important réside dans le fait que, pour être valable, le consentement doit, quelles que soient les circonstances dans lesquelles il est donné, être une manifestation de volonté libre, spécifique et informée, comme décrit à l'article 2, point h, de la directive. Le CEPD émet de sérieux doutes quant au fait que les individus invités à autoriser la surveillance de leurs activités sur Internet auront réellement le choix, en particulier lorsque l'alternative est l'absence de connexion à Internet, ce qui peut mettre en péril de nombreux autres aspects de leur vie.

56. Troisièmement, la *nécessité* même d'une telle surveillance pour la mise en œuvre d'un contrat dans lequel le sujet des données est un tiers, telle que requise à l'article 7, point b, de la directive 95/46/CE, est elle-même très discutable, étant donné que cette surveillance n'est visiblement pas l'un des objets du contrat conclu par le sujet, mais seulement un moyen, pour le fournisseur d'accès à Internet, de servir d'autres intérêts.

Suppression des fichiers journaux

57. Selon la directive 2002/58/CE, et plus particulièrement son article 6, les données de trafic, telles que les adresses IP, peuvent uniquement être collectées et stockées à des fins directement liées à la communication elle-même, notamment la facturation, la gestion du trafic et la prévention des fraudes. Ensuite, ces données doivent être effacées. Ceci ne porte pas préjudice aux obligations prévues dans la directive sur la rétention des données. Comme il a été mentionné celle-ci rend obligatoire la conservation des données de trafic, ainsi que leur transmission aux services de police ou aux magistrats, dans le cadre d'investigations, **uniquement pour des infractions pénales graves** ([37]).

([37]) Voir le paragraphe 35 du présent avis.

58. Conformément à ce qui précède, les fournisseurs de services Internet doivent supprimer tous les fichiers journaux faisant apparaître les activités des internautes, si ces données ne sont plus nécessaires aux fins décrites plus haut. En considérant que les fichiers journaux ne sont pas nécessaires à la facturation, trois ou quatre semaines devraient suffire pour la gestion du trafic par les fournisseurs d'accès à Internet ([38]).

59. Cela signifie que, lorsqu'ils sont contactés par des détenteurs de droits d'auteur et à moins que ce contact n'ait lieu pendant la période limitée décrite ci-dessus, les fournisseurs d'accès à Internet ne devraient plus avoir en leur possession les fichiers reliant les adresses IP à leurs abonnés. Au-delà de cette période, les fichiers journaux doivent être conservés uniquement pour des motifs justifiés, dans les limites et objectifs autorisés par la loi.

60. Pratiquement, ceci revient à dire que, à moins d'être traitées très rapidement, les requêtes effectuées par les détenteurs de droits d'auteur auprès des fournisseurs d'accès ne pourront pas être satisfaites, simplement parce que le fournisseur d'accès n'aura plus ces informations en sa possession. Ceci permet, en soi, de définir les limites de ce que l'on appelle une surveillance acceptable, comme il est décrit dans la section ci-dessus.

Risques de réaction en chaîne

61. Le CEPD est également inquiet des implications des politiques de déconnexion d'Internet en trois temps, non seulement en matière de respect de la vie privée et de protection des données, mais aussi des effets d'entraînement potentiels. Si l'on autorise la déconnexion d'Internet en trois temps, celle-ci peut devenir une pente glissante vers la légitimation d'une surveillance encore plus massive des activités des internautes, dans différents domaines et à différentes fins.

62. Le CEPD invite instamment la Commission à s'assurer que l'ACAC ne dépasse, ni ne va à l'encontre du régime actuel de l'UE pour le respect des droits de propriété intellectuelle. Ce régime respecte les libertés et droits fondamentaux et les libertés civiles, comme la protection des données à caractère personnel.

V. **INQUIÉTUDES CONCERNANT LA PROTECTION DES DONNÉES DANS LE CADRE DES MÉCANISMES DE COOPÉRATION INTERNATIONALE**

63. L'un des moyens mis en avant par les participants à l'ACAC pour résoudre le problème du respect des droits de propriété intellectuelle consiste à renforcer la coopération

([38]) La gestion du trafic inclut l'analyse du trafic réseau à des fins d'optimisation ou de garantie des performances, de réduction de la latence et/ou d'augmentation de la bande passante disponible.

internationale, avec un certain nombre de mesures qui permettraient de faire respecter efficacement ces droits dans les juridictions des signataires de l'ACAC.

64. Au vu des informations disponibles, certaines des mesures prévues pour le respect des droits de propriété intellectuelle incluront vraisemblablement l'échange, à l'échelle internationale, d'informations sur les violations présumées de ces droits, entre les autorités publiques (par exemple, les douanes, la police et la justice), mais également entre des acteurs publics et des acteurs privés (comme les fournisseurs d'accès à Internet et les organismes de défense des droits de propriété intellectuelle). De tels transferts de données soulèvent un certain nombre de questions quant à la protection des données.

V.1. **Les échanges de données envisagés dans le contexte de l'ACAC sont-ils légitimes, nécessaires et proportionnés?**

65. En l'état actuel des négociations, alors qu'un certain nombre d'éléments demeurent indéfinis ou inconnus en ce qui concerne l'exploitation proprement dite des données, il est impossible de vérifier si le cadre de mesures proposé est conforme aux principes fondamentaux et législations européennes en matière de protection des données.

66. Il est tout d'abord loisible de se demander si les transferts de données vers des pays tiers, dans le cadre de l'ACAC, sont ou non légitimes. En l'absence d'un accord des États membres de l'UE sur l'harmonisation des mesures de contrôle dans l'environnement numérique et les types de sanctions à appliquer en cas d'infractions, la pertinence de mesures à l'échelle internationale dans ce domaine demeure discutable ([39]).

67. Au vu de ce qui précède, il apparaît que les principes de nécessité et de proportionnalité des transferts de données dans le cadre de l'ACAC 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. Ceci nécessite une définition précise des «violations graves des droits de propriété intellectuelle» qui entraîneraient des transferts de données.

68. De plus, une attention particulière doit être portée aux personnes impliquées dans les échanges de données. Il faut également se demander si les données seront uniquement échangées entre des autorités publiques ou entre des acteurs privés et des autorités publiques. Comme décrit précédemment dans ces recommandations, l'intervention d'acteurs privés dans un domaine qui relève, en principe, de la compétence des autorités publiques suscite un certain nombre de préoccupations ([40]). Les conditions dans lesquelles ces acteurs privés seront impliqués dans la collecte et l'échange de données à caractère personnel en rapport avec les violations de droits d'auteur doivent strictement se limiter à certaines circonstances spécifiques, avec des garanties appropriées.

V.2. **Loi applicable en matière de protection des données dans le cadre des transferts de données de l'ACAC**

Régime général pour les transferts de données

69. Le cadre général de protection des données applicable au sein de l'UE est établi dans la directive 95/46/CE. Les articles 25 et 26 de la directive 95/46/CE définissent le régime applicable pour les transferts de données vers des pays tiers. L'article 25 dispose que les transferts doivent se limiter à des pays garantissant un niveau de protection adéquat. Dans le cas contraire, de tels transferts sont en principe interdits.

70. Le niveau de protection garanti par les pays tiers est évalué au cas par cas par la Commission européenne. Celle-ci a édicté plusieurs décisions reconnaissant une protection adéquate dans un certain nombre de pays, suite à une analyse approfondie du groupe de travail Article 29 ([41]).

71. Le CEPD constate que la plupart des participants à l'ACAC ne figurent pas dans la liste des pays offrant une protection adéquate des données, dressée par la Commission: à l'exception de la Suisse et, dans certaines circonstances spécifiques, du Canada et des États-Unis, les autres participants à l'ACAC ne sont pas reconnus comme offrant un niveau de protection adéquat. En d'autres termes, pour transférer des données depuis l'UE vers l'un de ces pays, l'une des conditions de l'article 26, paragraphe 1, de la directive 95/46/CE doit être remplie ou des garanties appropriées doivent être apportées par les parties concernées au moment du transfert de données, conformément à l'article 26, paragraphe 2, de la directive.

Régime spécifique pour les transferts de données dans le cadre de la répression des infractions

72. Bien que la directive 95/46/CE constitue le principal instrument en vigueur au sein de l'UE pour la protection des données, sa portée est actuellement limitée. En effet, elle exclut expressément les opérations concernant, *inter alia*, les activités de l'État dans le domaine pénal (article 3). Par conséquent, les échanges de données dans le cadre de procédures pénales ne tombent pas sous le coup de la directive 95/46/CE et sont soumis aux principes généraux

([39]) Une proposition de sanctions pénales est en cours d'examen au sein du Conseil, COM(2006) 168 du 26 avril 2006.

([40]) Voir les paragraphes 32 et 52 du présent avis. Voir également l'avis du CEPD en date du 11 novembre 2008 sur le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel, JO C 128 du 6.6.2009, p. 1.

([41]) Voir les décisions d'adéquation accordées par la Commission européenne à l'Argentine, au Canada, à la Suisse, au Bureau des douanes et de la protection des frontières des États-Unis (données PNR), à Guernesey, à l'Île de Man et de Jersey; disponibles sur le site http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

de protection des données, établis dans la Convention nº 108 du Conseil de l'Europe et son protocole supplémentaire, qui concernent tous les États membres de l'UE ([42]). En outre, les règles adoptées par l'UE concernant la coopération de la police et de la justice dans le cadre d'affaires pénales, établies dans la décision 2008/877/JAI du Conseil sont applicables ([43]).

73. Ces instruments posent également, comme principe, que le pays vers lequel les données seront transférées doit présenter un niveau adéquat de protection des données. Différentes dérogations sont prévues, en particulier lorsque le pays tiers fournit des protections adéquates. Comme pour les échanges de données prévus par la directive 95/46/CE, les échanges de données dans le cadre de procédures pénales nécessiteront donc des garanties appropriées entre les parties concernées par le transfert de données, avant que celui-ci ne soit effectué.

Vers un nouveau régime pour les transferts de données

74. Dans un futur proche, de nouvelles règles communes de protection des données, applicables à tous les champs d'activités de l'UE, devraient être adoptées par l'UE, sur la base de l'article 16 du TFUE. Cela signifie que, d'ici quelques années, un cadre complet de protection des données pourrait voir le jour au sein de l'UE, avec des règles cohérentes pour la protection des données dans tous les champs d'activités de l'UE. Ce cadre imposera le même niveau de protections et de garanties pour toutes les opérations de traitement des données. Comme souligné par Viviane Reding ([44]), Commissaire à la Justice, aux Droits fondamentaux et à la Citoyenneté, ce nouveau cadre de travail servirait d'«instrument juridique unique, moderne et complet» pour la protection des données dans l'UE. Un tel cadre de travail est particulièrement bienvenu, étant donné qu'il renforcerait la clarté et la cohérence des règles applicables dans l'UE en matière de protection des données.

75. Dans un contexte international, le CEPD attire également l'attention sur la Résolution sur les normes internationales pour la protection des données à caractère personnel et la vie privée, adoptée récemment par les autorités de contrôle de la protection des données. Ceci constitue une première étape vers l'établissement de normes globales en la matière ([45]). Les normes internationales incluent, en termes de protection des données, un certain nombre de garanties similaires à celles figurant dans la directive 95/46/CE et la Convention nº 108. Bien que les normes internationales ne soient pas encore en vigueur, elles apportent une orientation utile en termes de principes de protection des données, que les pays tiers peuvent appliquer volontairement afin de rendre leur cadre juridique compatible avec les normes européennes. Le CEPD estime que les signataires de l'ACAC doivent également tenir compte des principes établis dans les normes internationales lors du traitement de données à caractère personnel en provenance de l'UE.

V.3. **Nécessité de mettre en œuvre des garanties appropriées pour la protection des transferts de données entre l'UE et des pays tiers**

Quelle forme les garanties doivent-elles adopter afin de protéger efficacement les transferts de données vers les pays tiers?

76. Si la nécessité du transfert de données à caractère personnel vers des pays tiers est démontrée, le CEPD insiste sur le fait que l'Union européenne doit négocier avec les pays tiers, en plus de l'ACAC lui-même, des instruments spécifiques contenant des garanties appropriées pour la protection de données dans le cadre des échanges de données à caractère personnel.

77. Des garanties appropriées en matière de protection des données doivent généralement être établies dans le cadre d'un accord contraignant entre l'UE et le pays tiers destinataire, selon lesquelles le destinataire s'engage à respecter la législation européenne sur la protection des données et à garantir aux individus les mêmes droits et recours que ceux octroyés par la législation européenne. Cette nécessité d'un accord contraignant découle de l'article 26, paragraphe 2, de la directive 95/46/CE, et de l'article 13, paragraphe 3, point b, de la décision cadre. Elle est également étayée par la pratique actuelle de l'UE qui consiste à conclure des accords spécifiques afin d'autoriser des transferts de données spécifiques vers des pays tiers ([46]).

78. De même, selon les normes internationales envisagées, le destinataire devra, dans certains cas, présenter des garanties du niveau de protection requis afin que le transfert puisse avoir lieu. Ces garanties peuvent également revêtir la forme d'un engagement contractuel.

Contenu des garanties à apporter par les signataires de l'ACAC dans le cadre des transferts de données à caractère personnel

79. Le CEPD insiste particulièrement sur le fait que les échanges internationaux d'informations dans le cadre de l'application des lois sont particulièrement sensibles du point de vue de la protection des données. En effet, un tel cadre de travail

([42]) 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 transfrontaliers de données, Strasbourg, 8 novembre 2001.

([43]) Décision cadre du Conseil 2008/877/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60.

([44]) Voir les réponses au questionnaire du Parlement européen pour le Commissaire désigné Viviane Reding, p.5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Résolution adoptée à Madrid en novembre 2009.

([46]) Par exemple, les accords Europol et Eurojust avec les États-Unis, l'accord sur les données PNR, accord Swift, l'accord entre l'UE et l'Australie sur le traitement et le transfert des données PNR (dossiers passagers) en provenance de l'Union européenne, par les compagnies aériennes, vers les douanes australiennes.

pourrait légitimer les transferts de données en masse dans un domaine où l'impact sur les individus est particulièrement sérieux et où des protections strictes et fiables sont d'autant plus nécessaires.

80. Le CEPD souligne que des conditions et protections spécifiques peuvent être définies seulement au cas par cas, à la lumière de tous les paramètres des échanges de données. À titre d'orientation, le CEPD met toutefois en évidence, ci-dessous, certains des principes et protections qui doivent être apportés par les destinataires tiers afin que les transferts de données puissent avoir lieu:

— il faut vérifier la justification légale entourant le traitement des données (à savoir, le traitement s'appuie-t-il sur une obligation légale, sur le consentement des personnes concernées ou sur toute autre justification valable?) et s'assurer que les transferts de données respectent l'objectif initial de la collecte des données. Aucun transfert ne doit être réalisé hors du périmètre de l'objectif spécifié;

— la quantité et le type des données personnelles échangées doivent être clairement précisés et réduits au strict minimum nécessaire pour atteindre l'objectif du transfert. Les données personnelles collectées et transférées peuvent notamment inclure l'adresse IP des internautes, la date et l'heure de l'activité suspecte et le type d'infraction commise. Le CEPD conseille de ne pas associer les données à un individu spécifique pendant la phase des investigations. Il rappelle également que l'identification d'une personne suspecte doit s'effectuer conformément à la loi et sous le contrôle d'un juge. À cet égard, le CEPD souligne le fait que les données relatives aux violations des droits de propriété intellectuelle et aux soupçons d'infractions forment une catégorie de données spéciale, dont le traitement est généralement limité aux autorités compétentes et nécessite des protections supplémentaires. Les personnes autorisées à traiter les données relatives aux violations des droits de propriété intellectuelle et aux soupçons d'infractions, ainsi que les conditions de traitement de ces données, doivent donc être spécifiquement précisées, conformément à la législation actuelle en matière de protection des données;

— les personnes qui pourront accéder à ces informations doivent être clairement identifiées. De plus, les transferts ultérieurs vers d'autres destinataires doivent en principe être interdits, sauf s'ils sont nécessaires pour une enquête déterminée. Cette limitation est particulièrement cruciale, étant donné que les destinataires désignés ne doivent pas inutilement partager ces informations avec des destinataires non autorisés;

— le CEPD présume que l'ACAC ne prévoira pas seulement une coopération entre les autorités publiques, mais qu'il confiera également des tâches de contrôle à des entités privées (telles que des fournisseurs d'accès à Internet, des organismes de défense des droits de propriété intellectuelle, etc.). Dans ce dernier cas, les conditions et le niveau d'implication des entités privées dans l'application des droits de propriété intellectuelle doivent être soigneusement évalués. En effet, les mesures de l'ACAC ne doivent pas accorder aux fournisseurs d'accès et aux détenteurs de droits le droit *de facto* de surveiller le comportement des utilisateurs en ligne. De plus, le traitement des données à caractère personnel par des organismes privés dans le contexte de l'application de la loi doit s'effectuer uniquement sur une base légale appropriée. Il est également important de clarifier si ces organismes privés seront tenus de coopérer avec la police et de préciser l'étendue d'une telle coopération. Cette procédure doit, dans tous les cas, se limiter exclusivement aux «infractions pénales graves», dont la définition devra également être précisée, étant donné que toutes les violations de droits de propriété intellectuelle ne seront pas considérées comme des infractions pénales graves;

— la méthode utilisée pour l'échange de données à caractère personnel doit être clairement choisie. Surtout, il faut préciser s'il sera effectué au moyen d'un système «push» (par exemple, les fournisseurs d'accès à Internet et les organismes de défense des droits de propriété intellectuelle transféreraient, sous leur contrôle, une certaine quantité de données à des tiers, comme la police ou les autorités compétentes, situées à l'étranger) ou d'un système «pull» (par exemple, la police et les autorités compétentes auraient un accès direct aux bases de données des parties privées ou aux bases de données centralisant les informations). Comme décrit précédemment dans le contexte des PNR, un système push est la seule option conforme aux principes européens de protection des données. En effet, il permet à l'expéditeur (dans l'Union européenne), qui correspond généralement au responsable de traitement, d'exercer un contrôle sur le transfert des données ([47]);

— la durée de conservation des données à caractère personnel par les destinataires doit être précisée, ainsi que le but pour lequel une telle conservation est nécessaire. Cette période de rétention doit être proportionnée au regard de l'objectif à atteindre. En d'autres mots, une fois qu'elles ne sont plus nécessaires pour réaliser cet objectif, les données doivent être supprimées ou éliminées;

— les obligations imposées aux responsables de traitement dans les pays tiers doivent être clairement établies. Les mécanismes de contrôle et/ou d'imputabilité doivent être garantis, avec la possibilité de recours et sanctions efficaces à l'encontre desdits responsables en cas de traitement injustifié ou d'autres incidents pertinents. De plus, des mécanismes de recours doivent être mis

([47]) Voir les recommandations du groupe de travail Article 29 (4/2003) sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers, WP78, 13 juin 2003;

en place, afin que les individus puissent déposer une plainte devant une autorité indépendante de protection des données et qu'ils puissent trouver un recours efficace devant un tribunal indépendant et impartial ([48]);

— l'instrument convenu entre les parties doit clairement spécifier les droits des personnes concernées en ce qui concerne leurs données à caractère personnel, lorsque ces données sont traitées par un destinataire tiers, afin de leur garantir un moyen efficace d'application de leurs droits en cas de traitement effectué à l'étranger;

— par ailleurs, la transparence est cruciale et les parties concernées par l'instrument de protection des données doivent convenir de la façon dont elles informeront les sujets à propos du traitement des données, ainsi que sur leurs droits et la façon de les exercer.

VI. **CONCLUSIONS**

81. Le CEPD encourage vivement la Commission européenne à amorcer un dialogue public et transparent sur l'ACAC, par exemple sous la forme d'une consultation publique. Cette démarche contribuerait également à s'assurer que les mesures adoptées seront conformes aux législations européennes sur le respect de la vie privée et la protection des données.

82. Les négociations autour de l'ACAC étant en cours, le CEPD en appelle vivement à la Commission européenne, afin de trouver un juste équilibre entre les exigences de protection des droits de propriété intellectuelle, d'une part, et les droits en matière de respect de la vie privée et de protection des données d'autre part. Selon le CEPD, il est particulièrement crucial que le respect de la vie privée et la protection des données soient pris en compte dès le début des négociations, avant même que des mesures soient convenues. Ceci évitera de devoir, ultérieurement, trouver des solutions alternatives respectant la vie privée.

83. La propriété intellectuelle est importante pour la société. Elle doit donc être protégée. Toutefois, elle ne doit pas prévaloir sur les droits fondamentaux des individus en matière de respect de la vie privée, de protection des données et d'autres droits, comme la présomption d'innocence, une protection judiciaire efficace et la liberté d'expression.

84. Dans la mesure où le projet actuel de l'ACAC inclut, ou tout au moins encourage indirectement les politiques de déconnexion d'Internet en trois temps, l'ACAC limiterait profondément les droits fondamentaux et les libertés des citoyens européens, surtout en ce qui concerne la protection des données à caractère personnel et le respect de la vie privée.

85. Le CEPD considère que les politiques de déconnexion d'Internet en trois temps ne sont pas nécessaires pour atteindre l'objectif d'application des droits de propriété intellectuelle. Le CEPD est convaincu que des solutions alternatives, moins intrusives, existent ou, à tout le moins, que les règles envisagées peuvent être mises en œuvre de façon moins intrusive ou plus limitée, notamment sous la forme d'une surveillance *ad hoc* ciblée.

86. Les politiques de déconnexion d'Internet en trois temps sont également problématiques d'un point de vue juridique plus détaillé. En effet, le traitement des données judiciaires, notamment par des organismes privés, doit s'appuyer sur une base légale appropriée. Le système de riposte en trois temps peut également impliquer le stockage des fichiers journaux à plus long terme, ce qui serait contraire à la législation actuelle.

87. De plus, étant donné que l'ACAC implique les échanges de données à caractère personnel entre les autorités et/ou des organismes privés situés dans les pays signataires, le CEPD en appelle à l'Union européenne pour mettre en œuvre les protections appropriées. Ces protections doivent s'appliquer à tous les transferts de données réalisés dans le cadre de l'ACAC, que ce soit dans le domaine civil, pénal ou numérique. Elles doivent être conformes aux principes de protection des données établis dans la convention n° 108 et la directive 95/46/CE. Le CEPD recommande que ces protections revêtent la forme d'accords contraignants entre les expéditeurs (UE) et les pays destinataires tiers.

88. Le CEPD souhaite enfin être consulté sur les mesures à mettre en œuvre pour les transferts de données dans le cadre de l'ACAC, afin de vérifier leur proportionnalité et de s'assurer qu'elles garantissent un niveau adéquat de protection des données.

Fait à Bruxelles, le 22 février 2010.

Peter HUSTINX

Contrôleur européen de la protection des données

([48]) Voir l'avis du CEPD en date du 11 novembre 2008 sur le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel.