Réponse du CEPD à la consultation de la Commission sur son rapport concernant l'application de la directive relative au respect des droits de propriété intellectuelle

1. Introduction

1. Le présent document fournit une réponse à la consultation de la Commission sur son rapport concernant l'application de la directive relative au respect des droits de propriété intellectuelle («IPRED»[1]), publié le 22 décembre 2010 (ci-après «le rapport de la Commission» ou «le rapport»)[2]. Un document de travail interne[3] accompagne ce rapport.

2. Le rapport est essentiellement consacré aux défis que l'internet semble avoir créés en relation avec le respect des droits de propriété intellectuelle, ainsi qu'aux moyens de les relever. Différents instruments ou mécanismes sont utilisés pour partager du contenu sur l'internet et peuvent donner lieu à des échanges illicites de matériel soumis à des droits d'auteur. Il s'agit entre autres de partage de fichiers P2P. Le rapport souligne qu'il n'est pas facile de collecter des preuves de violations présumées des droits d'auteur commises à l'aide de ce type d'instruments ou de mécanismes. Plus spécifiquement, il épingle les législations relatives à la protection des données et au droit de la vie privée comme étant susceptibles de faire obstacle à l'article 8 IPRED, qui autorise la collecte d'informations sur l'identité du contrevenant[4].

3. Le rapport ne formule aucune proposition concrète pour résoudre ce problème si ce n'est suggérer une évaluation approfondie et, *«(l)e cas échéant, […] des moyens de remédier à la situation»* relative à la relation entre le droit d'information (ex-article 8 IPRED) et la protection de la vie privée et des données, faisant probablement allusion à la nécessité d'assouplir la protection des données et de la vie privée.

4. En l'absence de propositions concrètes de la Commission, le CEPD a décidé de contribuer à l'exercice de consultation à l'aide de réflexions sur le cadre actuel garantissant le respect des droits de propriété intellectuelle en ligne («DPI») ainsi que sur de possibles modifications de ce cadre[5]. Ces réflexions sont structurées comme suit.

5. La section 2 décrit les actions traditionnellement mises en œuvre (aspects techniques et faits) pour garantir le respect des droits d'auteur sur les réseaux P2P. Le cadre juridique qui s'applique au respect des DPI lors de l'utilisation de plateformes P2P est expliqué à la section 3. Le respect de ces droits sur les réseaux P2P a été choisi

---

[1] Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, JO L195 du 2.6.2004, pp.16 – 25.

[2] Rapport sur le respect des droits de propriété intellectuelle (COM(2010) 779).

[3] *Analysis of the application of Directive 2004/48/EC on the enforcement of intellectual property rights in the Member States* (Analyse de l'application de la directive 2004/48/CE relative au respect des droits de propriété intellectuelle dans les États membres) (SEC(2010) 1589), ci-après «le document de travail interne».

[4] L'article 8 autorise également que des informations soient recueillies sur, par exemple, une personne qui a été trouvée en train de fournir, à l'échelle commerciale, des services utilisés dans des activités contrefaisantes.

[5] Ces commentaires ne concernent naturellement que les aspects du cadre juridique qui ont une incidence sur la protection des données et de la vie privée des personnes.

comme exemple, non seulement parce qu'il est souvent considéré comme la principale plateforme pour l'échange de contenu soumis à des droits d'auteur, mais également parce qu'il illustre bien la façon dont les exigences de protection des données et de la vie privée s'appliquent dans le cadre des différentes mesures prises en vue du respect des DPI[6].

6. La section 4 contient des remarques sur le rapport de la Commission et met en doute certaines de ses conclusions explicites et implicites. Dans ce contexte, le CEPD soumet des propositions tendant à clarifier le cadre juridique et à remédier aux problèmes perçus.

2. Réseaux P2P: faits et mesures visant à garantir le respect des DPI

7. La technologie P2P est une architecture logicielle distribuée qui permet la connexion et la communication entre ordinateurs. Elle permet ainsi aux internautes de partager des informations, dont du matériel soumis à des droits d'auteur stocké sur leur propre ordinateur, avec d'autres internautes[7].

8. La **première phase**, pour ce qui est de garantir le respect des DPI sur les réseaux P2P, consiste à collecter des preuves de violations présumées. Les titulaires de droits doivent collecter des preuves prima facie sur des infractions éventuelles. À cette fin, ils peuvent adhérer à des réseaux P2P, surveiller toute utilisation suspecte et ensuite télécharger du matériel soumis à des droits d'auteur afin d'obtenir les éléments suivants: i) la preuve que ledit matériel soumis à des droits d'auteur est effectivement disponible, ii) les adresses IP des sources à partir desquelles ils ont téléchargé le contenu en question, iii) la date et l'heure de l'infraction présumée, et iv) un rapport d'activité prouvant qu'une personne (utilisant une adresse IP spécifique) est en infraction[8].

9. La **deuxième phase** consiste à lier concrètement les éléments de preuve à un contrevenant présumé. Les preuves d'infractions en ligne présumées ne révèlent pas directement l'identité d'une personne. Elles portent sur une adresse IP qui peut être liée à une personne avec la collaboration du fournisseur d'accès internet («FAI»).

10. Pour établir le lien entre l'adresse IP et la personne qui l'utilise, le titulaire de droits peut demander à un tribunal d'ordonner au FAI de divulguer l'identité du

[6] Il existe d'autres mécanismes pour l'échange d'informations, dont du contenu protégé par des droits d'auteur, tels que le téléchargement en ligne, le streaming, etc. Par ailleurs, d'autres plateformes telles que les sites de commerce en ligne, qui peuvent être utilisés pour échanger des produits contrefaits, constituent aussi un défi s'agissant du respect des DPI. Certains des problèmes identifiés en rapport avec les plateformes P2P peuvent également se présenter lors de l'utilisation de ces autres mécanismes, mais pas nécessairement tous.

[7] Chaque ordinateur représente un «pair» et est à la fois fournisseur et consommateur d'informations.

[8] Cette description résume les principales mesures prises par des sociétés spécialisées privées pour le traçage en ligne des violations présumées pour le compte de titulaires de droits. Il existe de nombreuses variantes de cette technique générale. Il semble toutefois que le principal élément récurrent dans tous les cas consiste en la surveillance, sous couvert d'anonymat, de sites et de serveurs d'échanges en ligne de contenus pendant un certain temps, suivie d'une analyse des données collectées.

propriétaire des adresses IP à partir desquelles le partage de matériel protégé par des droits d'auteur a eu lieu.

11. Aux fins de l'IPRED, un tribunal doit mettre en balance plusieurs considérations, dont le degré de gravité de l'infraction présumée et les droits à la protection des données et de la vie privée du contrevenant présumé. Au terme de cette évaluation, il peut ordonner au FAI de divulguer des informations concernant l'abonné auquel l'adresse IP a été attribuée.

12. Si elles sont mises en œuvre dans le respect de certains paramètres, les actions susmentionnées, indispensables pour garantir aux titulaires de droits le respect de ces derniers sur l'internet, ne sont pas incompatibles avec le cadre juridique existant en matière de protection des données, ce que démontrent les paragraphes suivants.

3. Le cadre juridique actuel

3.1. Surveillance et relevé des adresses IP suspectes par les titulaires de droits

13. Comme illustré ci-dessus, de manière générale, garantir le respect des DPI sur l'internet peut impliquer la surveillance de l'utilisation des plateformes P2P, y compris la collecte, par les titulaires de droits, d'adresses IP de personnes soupçonnées d'infraction. Cette collecte concerne des données à caractère personnel telles que définies à l'article 2 de la directive relative à la protection des données[9].

14. En vertu de l'article 8, paragraphe 5, de la directive sur la protection des données[10], le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté (généralement appelées «données judiciaires») ne peut être effectué que sous certaines conditions strictes appliquées par les États membres. Les adresses IP, collectées comme indiqué supra, sont considérées comme des données judiciaires par le groupe de travail «Article 29». Bien que certaines variations puissent exister entre les divers États membres, de manière générale, ce type de données ne peut être traité que pour la constatation, l'exercice ou la défense d'un droit dans le cadre d'une action en justice.

15. Cependant, l'article 8 lu en conjonction avec l'article 6, point c), de la directive, disposant que le traitement est limité aux données «adéquates, pertinentes et non excessives», limite la portée de la surveillance en termes d'étendue et de quantité de données collectées et ultérieurement traitées. La directive doit être interprétée à la lumière de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme («CEDH») et de l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Cela met également en lumière les exigences à remplir pour que le traitement soit jugé nécessaire et proportionné au regard des finalités légitimes pour lesquelles les données sont collectées. En d'autres termes, le traitement doit être effectué dans le contexte d'actions en justice, pendantes ou futures, *spécifiques* visant à

[9] Voir aussi le point 27 de l'avis du CEPD du 22 février 2010 sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC).
[10] 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 (ci-après «la directive sur la protection des données»). JO L 281 du 23.11.1995, pp.31 – 50.

la constatation, à l'exercice ou à la défense d'un droit. Une surveillance généralisée, suivie du stockage à grande échelle aux fins de l'exercice de droits, par exemple le balayage de l'internet de manière générale ou de toutes les activités sur des réseaux P2P, irait au-delà de ce qui est légitime[11].

16. En outre, la directive sur la protection des données établit des conditions supplémentaires visant à garantir un traitement légitime des données. Ces conditions s'appliquent au traitement d'adresses IP décrit plus haut. Il s'agit par exemple de celles incluses à l'article 6 de la directive concernant la qualité des données (article 6, paragraphe 1, point d))[12], le principe de conservation (article 6, paragraphe 1, point e))[13] et le principe de spécification de la finalité (article 6, paragraphe 1, point b))[14].

17. De plus, certains États membres invoquent l'article 20 de la directive[15] pour exiger la réalisation d'un contrôle préalable ou la délivrance d'une autorisation avant toute collecte de données[16]. Étant donné le caractère sensible de la collecte de telles informations, une telle approche devrait être obligatoire.

18. Après avoir collecté les adresses IP (et les informations décrites à la section 2), les titulaires de droits doivent établir l'identité des propriétaires de ces adresses IP via les FAI dans le respect des conditions citées ci-dessous.

3.2. Stockage et traitement ultérieur d'adresses IP par les FAI

19. Pour assurer le respect des DPI, la coopération des FAI est indispensable, étant donné qu'ils peuvent avoir stocké des informations sur les personnes utilisant une adresse IP relevée par le titulaire de droits. Elle est nécessaire pour identifier ladite personne.

20. Il convient de se demander si les FAI ont réellement besoin et sont légalement autorisés à conserver les informations destinées aux fins susmentionnées qui établissent un lien entre des personnes et des adresses IP données utilisées pour une communication spécifique. En vertu de la directive «Vie privée et communications électroniques», les FAI peuvent être autorisés à stocker et traiter ultérieurement des adresses IP utilisées par des personnes après la fin de la communication. Toutefois, la directive limite cette possibilité en raison du caractère sensible des informations impliquées dans les activités de communication. Concrètement, les FAI peuvent conserver des données sur les adresses IP à des fins de facturation (article 6 de la

[11] Voir la note de bas de page 9. Pareille surveillance généralisée par des entités privées a été déclarée illicite par l'Autorité italienne chargée de la protection des données.
[12] Il requiert que les données à caractère personnel soient exactes et mises à jour.
[13] Il prévoit que les données doivent être rendues anonymes ou effacées lorsqu'elles ne sont plus nécessaires à la réalisation des finalités pour lesquelles elles ont été collectées.
[14] Il requiert que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes.
[15] L'article 20 dispose que les États membres précisent 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.
[16] Ces contrôles préalables, suivis de la délivrance d'autorisations, sont (ou ont été) obligatoires dans des pays tels que la France, la Norvège et la Suède. Dans ces pays, des autorisations étaient demandées (et octroyées ou non) en vue de la réalisation de certains traitements de données destinés à lutter contre le phénomène des copies illégales. En Suède, l'obligation d'obtenir une autorisation a été abolie avec la transposition de l'IPRED.

directive) pendant la période établie pour toute contestation éventuelle de la facture, bien que dans de nombreux cas, cela ne s'avère pas nécessaire en raison de l'utilisation prédominante de forfaits[1], qui limite les cas dans lesquels les FAI peuvent légitimement conserver des données sur les adresses IP à des fins de facturation.

21. En outre, les États membres peuvent, sous certaines conditions définies à l'article 15, paragraphe 1, de la directive «Vie privée et communications électroniques», adopter des mesures législatives obligeant les fournisseurs à conserver certaines données. Une telle obligation est inscrite dans la directive sur la conservation des données[17], qui impose aux FAI de conserver les adresses IP pendant une période limitée[18]. La divulgation de ces informations est toutefois limitée aux autorités nationales compétentes *«aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne»*[19]. Les violations des droits d'auteur ne constituent pas nécessairement des infractions graves[20].

22. Il résulte des éléments susmentionnés que les FAI peuvent, au moment de la réception d'une demande de divulgation des informations, être ou non en possession des données nécessaires pour lier un abonné spécifique à une adresse IP donnée. Toutefois, le simple fait que les FAI aient à leur disposition des données destinées à des fins spécifiques (à des fins de facturation ou en vertu d'une obligation de prolongation de la période de conservation dans le contexte de la lutte contre des infractions graves) ne signifie pas que ces données puissent être transférées aux titulaires de droits d'auteur à d'autres fins. La section suivante analyse dans quelles conditions la divulgation de données pourrait être autorisée.

3.3. Traitement des demandes et transfert d'informations personnelles dans le contexte d'une procédure civile ou pénale

23. En vertu de l'article 15, paragraphe 1, de la directive «Vie privée et communications électroniques», les États membres peuvent adopter des mesures législatives obligeant les fournisseurs de communications électroniques à coopérer avec les autorités aux fins de la recherche, de la détection et de la poursuite d'infractions pénales. Ces mesures doivent être en conformité avec le droit de l'UE. Au titre de l'article 8, paragraphe 2, de la CEDH, elles devraient être nécessaires, appropriées et proportionnées. Dans le cas présent, cela signifie que les FAI peuvent recevoir l'ordre de divulguer l'identité de propriétaires d'adresses IP à des autorités judiciaires dans le contexte de procédures pénales, dans les conditions prévues par la législation nationale.

---

[17] 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, JO L105 du 13.4.2006, pp. 54-63.

[18] Ces commentaires n'abordent pas la question de savoir si la conservation des données relatives au trafic et des données de localisation concernant toutes les personnes dans l'UE est nécessaire et justifiée. Le CEPD a traité ces points dans d'autres contextes. Voir, par exemple, le communiqué de presse du CEPD du 3 décembre 2010 intitulé *«The moment of truth for the Data Retention Directive: EDPS demands clear evidence of necessity»* (le moment de vérité pour la directive sur la conservation des données: le CEPD exige des preuves manifestes de nécessité).

[19] Voir l'article 4 de la directive sur la conservation des données. Cette disposition n'entrave en rien la possibilité pour les États membres de déroger au principe de confidentialité des communications à d'autres fins en application de l'article 15, paragraphe 1.

[20] Il n'existe à l'heure actuelle aucune définition harmonisée du terme «infraction grave» au sein de l'UE.

24. En outre, en application de l'arrêt *Promusicae* de la CJE[21], les États membres ont également la possibilité de prévoir l'obligation légale de divulguer, dans le cadre d'une procédure civile, des données à caractère personnel. Cette disposition doit être lue en conjonction avec l'article 8 IPRED, qui oblige les États membres à permettre aux tribunaux d'ordonner à des tierces parties, dont des FAI, de fournir des informations sur des contrevenants présumés lorsque l'infraction présumée a été commise à l'échelle commerciale[22].

25. L'article 8 IPRED établit des exigences minimales qui limitent les circonstances dans lesquelles la divulgation d'informations est obligatoire, à savoir en cas d'infraction «à l'échelle commerciale», «dans le cadre d'une action» et en réponse à une demande «justifiée et proportionnée». Il incombe ensuite aux tribunaux d'évaluer, au cas par cas, les faits, la gravité de l'infraction présumée, à savoir son étendue et les risques d'atteinte à la vie privée des personnes, afin de statuer sur la nécessité d'ordonner la divulgation d'informations.

26. Il ressort des éléments susmentionnés que les exigences à remplir pour que la surveillance initiale des adresses IP soit nécessaire et proportionnelle (article 6, paragraphe 1, point c), et article 8, de la directive sur la protection des données) sont en parfaite adéquation avec les critères de proportionnalité, de justification et d'échelle commerciale qui régissent la divulgation d'informations prévus à l'article 8 IPRED.

4. Le rapport de la Commission à la lumière du cadre juridique existant

4.1. Un cadre juridique équitable et raisonnable à préserver

27. De manière générale, le système juridique décrit ci-dessus – correctement transposé – contient des garanties visant à permettre des actions, tant au civil qu'au pénal, sans porter inutilement atteinte aux droits individuels à la protection des données et de la vie privée. Il fournit aux titulaires de droits les moyens d'établir l'existence d'infractions, tant pénales que civiles. L'article 15 de la directive «Vie privée et communications électroniques» – tel qu'expliqué par la CJE dans l'affaire *Promusicae* – autorise les États membres à prévoir la possibilité d'ordonner aux FAI de divulguer l'identité de propriétaires d'adresses IP également dans le cadre de procédures civiles. Une transposition adéquate de l'article 8 IPRED exigerait des États membres qu'ils accordent effectivement cette possibilité.

28. Parallèlement, les moyens à la disposition des titulaires de droits ne sont pas illimités. Les limitations sont le résultat logique de l'application des droits fondamentaux et de l'État de droit dans les sociétés démocratiques[23]. Par conséquent, les identités de personnes ne seront divulguées que lorsque l'infraction présumée sera commise à l'échelle commerciale et que le demandeur aura produit suffisamment de preuves de

---

[21] *Promusicae/Telefonica*, C-275/06; voir le point 54.

[22] Le critère relatif à «l'échelle commerciale» provient de l'article 61 de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord TRIPS), conclu le 15 avril 1994 et signé par tous les membres de l'Organisation mondiale du commerce. Il couvre les cas qui portent gravement atteinte aux intérêts du titulaire de droits.

[23] *Promusicae/Telefonica* C-275/06, voir les points 68 et 69.

cette infraction présumée. La gravité de la violation et le tort considérable causé au titulaire de droits parlent en faveur, dans pareil cas, de la divulgation d'informations sur l'identité du contrevenant. Les droits à la protection des données et de la vie privée devraient prévaloir lorsque l'infraction n'atteint pas ce seuil.

29. Le CEPD estime que, globalement, le système prévoit les garanties voulues. Plus spécifiquement, le critère de l'«échelle commerciale» visé dans l'IPRED, en vertu duquel le droit d'information prévaut en principe, est bienvenu. Ceci ainsi que la nécessité de demandes justifiées et proportionnées et formulées dans le cadre d'une action en justice sont des critères appropriés pour la détermination des limites au-delà desquelles le droit d'établir l'identité de personnes doit prévaloir sur le droit à la protection des données à caractère personnel.

30. Le rapport de la Commission recommande d'accorder une attention particulière à la relation entre le droit d'information et la protection de la vie privée. Il semble suggérer que des modifications de la législation sur ce point pourraient être envisagées.

31. En principe, le CEPD n'est pas favorable à une modification de l'article 8 IPRED pour les raisons expliquées ci-dessus et ci-dessous. Toutefois, si des modifications étaient proposées, il insisterait auprès de la Commission pour qu'elle évite toute perturbation de l'équilibre qui existe dans le cadre juridique actuel. Il l'invite en particulier à considérer ce qui suit:

a) Garantir le principe du jugement en bonne et due forme et l'implication des tribunaux

32. Le rapport semble indiquer que les FAI devraient divulguer les données à caractère personnel avant le lancement de la procédure judiciaire, et par conséquent sans ordonnance du tribunal[24]. Cela irait à l'encontre de l'article 8 IPRED, qui établit le mécanisme exclusif par lequel les titulaires de droits peuvent obtenir des informations. En vertu de cet article, seules les «autorités judiciaires compétentes» peuvent ordonner la divulgation des informations, à l'issue d'une opération de mise en balance des divers intérêts. L'implication des autorités judiciaires est un élément essentiel du système actuel; elle est primordiale pour faire en sorte que le respect des DPI soit assuré dans le respect du principe du jugement en bonne et due forme et des droits fondamentaux ainsi que de garanties spécifiques pour préserver la liberté et la confidentialité des communications prévues par les chartes constitutionnelles dans certains États membres.

33. Par ailleurs, toute divulgation volontaire d'informations personnelles par les FAI sans le consentement des utilisateurs serait contraire aux dispositions de la directive «Vie privée et communications électroniques».

b) Maintenir le juste équilibre entre les divers intérêts

34. Le rapport de la Commission affirme que le droit à la protection des données et de la vie privée entrave le droit d'information au titre de l'IPRED, en dépit du fait que, comme le reconnaît le rapport, l'expérience relative à l'application de la directive est

[24] Voir la page 12 du document de travail interne.

limitée et seuls quelques procès ont été rapportés. La Commission semble prôner la recherche d'un équilibre différent entre les DPI et les droits à la vie privée et à la protection des données.

35. Cependant, le rapport ne fournit aucune suggestion concrète sur la façon d'atteindre ce nouvel équilibre. Quoique non formulée explicitement, la solution proposée par la Commission tant dans le rapport que dans le document de travail interne semble ambigüe et paraît tendre vers l'autorisation ou la facilitation des transferts illimités des identités des personnes par les FAI aux titulaires de droits[25].

36. Tel que décrit plus haut, l'article 8 IPRED contient des exigences autorisant la divulgation lorsqu'il est question d'une allégation d'infraction commise à une échelle commerciale, que la divulgation est demandée dans le cadre d'une action en justice et que la demande d'informations est «justifiée et proportionnée». Toutefois, il semblerait que la Commission souhaite abandonner une partie de ces critères. Elle semble au contraire favoriser la divulgation d'informations personnelles – les identités de personnes et/ou les adresses IP qu'elles utilisent – également dans des affaires mineures. Cela va à l'encontre de l'intention des législateurs lors de l'élaboration de la directive, telle qu'interprétée dans les questions fréquemment posées à la Commission, selon laquelle la directive «ne vise pas à autoriser la poursuite des nombreuses personnes qui utilisent les réseaux pair à pair (P2P) pour échanger occasionnellement des fichiers»[26]. Cela est également en contradiction avec le considérant 14 de l'IPRED, qui évoque le critère de «l'échelle commerciale» et établit plus particulièrement que cela «exclut normalement les actes qui sont perpétrés par des consommateurs finaux agissant de bonne foi».

37. Ces critères ont été adoptés en 2004. Le rapport semble insinuer qu'ils pourraient être obsolètes. Il déclare dans ses conclusions qu'«il s'est avéré que le défi posé par l'internet par rapport à l'application des droits de propriété intellectuelle n'était pas entré en ligne de compte lors de l'élaboration de la directive». Cependant, en 2004, le phénomène internet existait déjà, quelque 43 % des ménages étant connectés à l'internet et 15 % disposant de l'accès à la large bande[27]. L'échange d'informations, y compris l'échange présumé illicite de contenu protégé par des droits d'auteur via des réseaux P2P, existe depuis quelque temps déjà, et est en réalité à l'origine de l'élaboration de la directive IPRED, ainsi que le souligne la proposition initiale de la

---

[25] Voir, à cet égard, diverses déclarations extraites du document de travail interne, qui semblent toutes aller dans le sens de l'autorisation du transfert systématique d'informations à caractère personnel aux titulaires de droits. Par exemple, «La possibilité d'intermédiaires pour partager les données avec les titulaires de droits constituerait un élément important dans ce contexte». «La situation est plus complexe si la demande d'informations est soumise avant le lancement de la procédure judiciaire», ce qui indique clairement un transfert sans l'implication des tribunaux. L'extrait suivant suggère également la nécessité de transférer des données avant toute ordonnance du tribunal (afin de faciliter la production de preuves quant à l'échelle à laquelle a lieu l'infraction): «Dans le même temps, il apparaît que certains titulaires de droits parviennent difficilement à établir que le contrevenant a agi à l'échelle commerciale sans avoir obtenu au préalable des informations du fournisseur d'accès internet, en particulier sur différentes adresses IP utilisées par le même contrevenant». Par ailleurs, «dans les États membres où les lois relatives à la vie privée prévalent actuellement sur le droit de propriété (intellectuelle), il peut être difficile pour les titulaires de droits d'exercer effectivement leur droit d'information». Voir aussi la note sur le partage de fichiers du Parlement européen, direction générale des politiques internes, département Droits des citoyens et affaires constitutionnelles, 2011, pages 13 et 14, qui partage le même point de vue.

[26] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/03/20&format=HTML&aged=1&language=FR&guiLanguage=en

[27] http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables

Commission[28]. Cela confirme que les législateurs ont pris ce paramètre en considération et ont malgré tout établi le seuil actuellement en vigueur. Le considérant 14 et l'article 8 IPRED ainsi que les questions fréquemment posées à la Commission renforcent cette interprétation.

38. Les critères prévus à l'article 8 IPRED sont, dans une certaine mesure, équivalents aux critères qui s'appliqueraient autrement au titre des directives sur la protection des données et «Vie privée et communications électroniques». En effet, cet article rassemble les critères de nécessité et de proportionnalité présents à la fois dans les directives et dans la CEDH – un argument de plus en faveur de sa non-modification.

39. En outre, il existe un risque accru qu'en dépit du fait qu'à court terme, de nouvelles règles et de nouveaux critères autorisant les transferts illimités d'adresses IP aux titulaires de droits puissent être considérés comme des instruments répressifs efficaces, ils puissent perdre de leur efficacité à moyen terme. Il faut s'attendre à ce que des contre-mesures techniques soient prises pour rendre l'identification des adresses IP très difficile, voire impossible[29]. En pratique, cela signifierait qu'une mesure portant gravement atteinte à la vie privée serait adoptée sans garantie d'un retour durable.

40. De l'avis du CEPD, une approche équilibrée devrait permettre la coexistence des deux droits (propriété intellectuelle et respect de la vie privée). Pareille approche doit également respecter l'État de droit, le principe du jugement en bonne et due forme et les autres droits fondamentaux. Le CEPD est d'avis que le cadre actuel, correctement mis en œuvre, offre ces garanties et permet d'atteindre un juste équilibre. Il paraît donc inutile de le modifier.

41. Néanmoins, le CEPD reconnaît qu'un cadre juridique équilibré n'est pas nécessairement synonyme de cadre clair. Dans le cas présent, comme l'indique le rapport de la Commission, le cadre est en effet ambigu. Ainsi qu'il est détaillé plus bas, les interconnexions entre diverses directives et la façon dont les critères devraient être appliqués dans la pratique pourraient être précisées. Cela serait particulièrement utile pour les tribunaux et contribuerait à la mise en place d'une approche européenne harmonisée.

---

[28] Voir la proposition de la Commission, http://www.europarl.europa.eu/oeil/file.jsp?id=230622&noticeType=null&language=fr. Par exemple, il est indiqué en page 3 que «(l)e développement de l'usage de l'Internet permet une distribution instantanée et globale de produits piratés. Enfin, ce phénomène apparaît de plus en plus lié à la criminalité organisée». La page 11 dispose ce qui suit: «Pour l'industrie des produits multimédias, la contrefaçon et la piraterie par l'Internet ne cessent de croître et représentent d'ores et déjà, et ce malgré le développement relativement récent de ce réseau, des pertes considérables». À la page 12, il est mentionné que «(l)a contrefaçon et la piraterie, autrefois artisanales, sont devenues des activités quasi industrielles. Celles-ci offrent, en effet, pour les contrevenants des perspectives de profit économique important sans risque excessif. Dans le contexte de l'Internet, la rapidité d'exécution des opérations illicites et la difficulté liée à la traçabilité de ces opérations réduisent encore les risques pour les contrevenants. La contrefaçon et la piraterie seraient même devenues aujourd'hui des activités plus attractives que le trafic illicite de drogue parce que des profits potentiels élevés pourraient être obtenus sans risque de sanctions légales importantes.»

[29] Par exemple, la technologie permet de modifier les applications P2P traditionnelles de manière à garantir l'anonymat. Les applications P2P peuvent être perfectionnées de façon à permettre l'échange anonyme de données par divers moyens, par exemple en n'utilisant pas les identifiants de l'application ou en autorisant des hops doublement sécurisés pour chaque portion d'octets échangée. Il est également possible d'utiliser les services de camouflage offerts par des réseaux privés virtuels (RPV) afin que les FAI ne puissent pas lier une adresse IP à un abonné.

4.2. Clarification du cadre juridique existant

42. Le rapport de la Commission a correctement identifié la relation entre le droit d'information (article 8 IPRED) et la protection des données à caractère personnel et de la vie privée comme un domaine comportant des incertitudes et par conséquent susceptible de nécessiter des clarifications.

43. Comme il a été montré précédemment, le cadre juridique existant permet d'établir l'existence d'infractions, tant pénales que civiles, sans porter indûment atteinte aux droits individuels à la protection de la vie privée et des données. Le CEPD reconnaît toutefois, à l'instar de la Commission, que le cadre n'est pas limpide. Plusieurs facteurs sont à l'origine de cette situation. Le cadre est relativement fragmenté, car il est composé de plusieurs directives, qui traitent de différents sujets, rendant les interactions entre celles-ci pas nécessairement évidentes. Par exemple, la relation entre l'article 8 IPRED et la directive «Vie privée et communications électroniques» n'est pas évidente pour tout un chacun; le fait que cet article définisse les conditions à remplir pour la divulgation de données à caractère personnel sur ordonnance judiciaire ne fait pas l'unanimité. Le nombre de questions préjudicielles soumises à la CJE concernant le cadre applicable explique que de nombreuses questions restent sans réponse. Les disparités au niveau de la transposition par les États membres peuvent ajouter à la confusion (voir section 4.3). Ce point doit être éclairci. Outre la clarification des interactions entre l'article 8 IPRED et la directive «Vie privée et communications électroniques», des éclaircissements sont nécessaires dans les deux domaines ci-après.

a) Établir des limites claires à la surveillance légale des internautes

44. Comme décrit supra, l'application des DPI sur l'internet implique dans un premier temps la surveillance et la collecte de données à caractère personnel, à savoir les adresses IP de particuliers. En vertu de l'article 8 de la directive sur la protection des données, une telle surveillance peut être mise en œuvre dans le contexte d'actions en justice, pendantes ou futures, spécifiques. La surveillance de personnes réalisée sous couvert d'anonymat, en particulier par des entités privées, irait à l'encontre des exigences légales. Il serait utile, à cet égard, de disposer d'orientations claires sur la portée de la surveillance légale.

45. Des clarifications sur les modalités d'application du cadre et la mise en équilibre effective des intérêts qu'il prévoit seraient non seulement utiles, mais également nécessaires. Plus concrètement, il serait utile pour les titulaires de droits, mais aussi pour les autorités chargées de la protection des données et les tribunaux, de s'entendre sur le type de surveillance qui satisferait aux critères de spécificité et de ciblage. Les questions pratiques telles que la mesure dans laquelle la localisation de certains pisteurs ou liens associés à du contenu protégé par des droits d'auteur et, ensuite, la surveillance de l'adresse IP qui le partage sont légales devraient être examinées et clarifiées. Les questions liées à l'établissement de l'existence d'infractions récurrentes sont également utiles, par exemple, pour démontrer que l'infraction a lieu à une échelle commerciale (voir infra).

b) Garantir une approche équilibrée du transfert des renseignements sur l'abonné dans le contexte de procédures judiciaires

46. En sus des éléments susmentionnés, des critères concrets, pratiques, pourraient également s'avérer particulièrement utiles lorsque des demandes d'informations sont présentées à des juridictions nationales. Ils contribueraient aussi à l'élaboration d'une approche européenne harmonisée.

47. Des discussions et des orientations sur la nature de l'infraction et les facteurs visant à établir l'existence d'une «échelle commerciale» dans les échanges P2P (et dans d'autres mécanismes) seraient particulièrement utiles pour la mise en balance des intérêts des parties. Il pourrait s'avérer judicieux de fournir des orientations sur les conditions dans lesquelles des infractions mineures mais persistantes, au cours d'une période donnée, aux fins d'un avantage commercial ou d'un gain financier, représenteraient une «échelle commerciale» et sur les moyens de mettre au jour pareilles situations. Par exemple, les applications P2P ont généralement leurs propres identifiants, qui peuvent servir à détecter des infractions mineures mais persistantes. Ces violations pourraient aussi être éventuellement détectées si les adresses IP ne changent pas pendant un certain temps (ce qui n'est pas rare)[30].

48. Ainsi, le CEPD encourage la Commission à continuer de travailler sur ce point et accepterait volontiers de contribuer à cet exercice.

4.3. Nécessité de garantir une mise en œuvre appropriée du cadre juridique applicable

49. Le rapport de la Commission soutient que la mise en œuvre de l'IPRED dans les États membres, mais également de la législation relative à la protection des données et de la vie privée, pourrait entraver l'exercice effectif du droit d'information (article 8). Le document de travail interne déclare ce qui suit: *«Dans certains États membres (…) il semblerait que la divulgation des informations pertinentes soit impossible d'un point de vue pratique dans les procédures tant civiles que pénales»*. À cet égard, s'agissant de déterminer si ces pratiques enfreignent l'acquis communautaire, le rapport mentionne explicitement que *«des évaluations approfondies pourraient s'avérer nécessaires en ce qui concerne la mesure dans laquelle les législations des États membres et leur application sont en accord avec ces exigences»*. Cela semble indiquer que la Commission envisage d'analyser la compatibilité des législations existantes des États membres avec l'acquis communautaire.

50. La Commission est tenue de s'assurer que les États membres respectent le Traité et les actes juridiques qui en découlent, dans le cas présent les directives concernées. Elle peut recourir à cette fin aux procédures d'infraction en vertu de l'article 263 TFUE. Le CEPD approuve totalement l'intention de la Commission d'aligner la transposition des États membres sur lesdites directives et suggère à la Commission d'en faire une priorité.

[30] Des méthodes plus élaborées existent:
http://hal.inria.fr/docs/00/47/03/24/PDF/bt_privacy_LEET10.pdf

51. Le CEPD a conscience que, dans le cas présent, la situation est relativement complexe. L'évaluation par la Commission de la mise en œuvre du cadre juridique doit englober non seulement l'IPRED mais aussi les autres directives et décisions de la CJE applicables ainsi que leur mise en œuvre concrète. Toutefois, cette complexité ne devrait pas dissuader la Commission d'agir.

4.4. Nécessité d'explorer des modèles commerciaux alternatifs

52. Le rapport souligne que l'internet et les technologies numériques représentent un défi pour le respect des DPI. Il mentionne également que la pratique répandue consistant à partager des fichiers au contenu protégé par des droits d'auteur est due à l'insuffisance de l'offre légale de contenu numérique par rapport à la demande existante. Cette offre légale pourrait en réalité être pratiquement inexistante dans certains États membres.

53. Il s'ensuit que l'élargissement de l'offre légale à travers l'UE pourrait avoir une incidence significative sur le niveau de violation et de respect global – monétisation – des DPI. En dépit de cela, ni le rapport ni le document de travail interne n'évoquent les moyens d'encourager l'accroissement de l'offre légale ou la façon dont cette augmentation pourrait contribuer à résoudre les problèmes perçus. Une disponibilité massive de la bande passante et une connectivité universelle devraient permettre le développement, entre autres, de services de streaming, tant dans le domaine de la musique que dans celui du cinéma, à des prix très attractifs. L'apparition de ces nouvelles possibilités sur le marché pourrait rendre le partage illicite de matériel soumis à des droits d'auteur moins attractif (sur le plan économique et du point de vue de la disponibilité et de la qualité).

54. Le CEPD déplore également que le rapport n'accorde aucune attention particulière aux modèles commerciaux alternatifs, qui permettraient de réduire considérablement les aspects liés à la protection de la vie privée. Par exemple, si les titulaires de droits prouvaient les pertes occasionnées par l'utilisation du P2P, les FAI pourraient proposer des abonnements internet différenciés, certains comprenant un accès aux plateformes P2P, les autres pas. La fraction du prix payée pour un abonnement avec accès illimité pourrait être redistribuée aux titulaires de droits.

55. Il s'agit là de domaines qui, de l'avis du CEPD, devraient faire l'objet d'études approfondies et être davantage promus.

5. Conclusions et recommandations

56. Selon le CEPD, le cadre existant, appliqué de manière adéquate, offre une approche efficace pour garantir le respect des DPI tout en respectant le droit à la protection des données à caractère personnel et de la vie privée. Le CEPD estime également que l'actuel article 8 prévoit un juste équilibre entre les différents droits et ne devrait pas être modifié. Plus particulièrement, il considère que:

    - le critère de l'«échelle commerciale» devrait être maintenu – quoiqu'éventuellement clarifié – de même que l'exigence de divulgation «dans

le cadre d'une action» et la nécessité d'une demande d'informations «justifiée et proportionnée»;

- la nécessité d'impliquer les tribunaux dans les décisions relatives au transfert de données à caractère personnel aux titulaires de droits devrait être maintenue. Au terme de l'évaluation des preuves prima facie produites par les titulaires de droits ou les organes chargés de l'application de la loi, les autorités judiciaires peuvent ordonner le transfert de données à caractère personnel dans le cadre d'une procédure en vertu du droit applicable. Ces données ne devraient être transférées dans le cadre de procédures civiles que sur demande ou moyennant autorisation d'un juge qui a évalué les circonstances particulières de l'affaire. Autrement, l'équilibre entre les deux types de droits (DPI et droits à la protection des données) serait perdu.

57. En dépit de ce qui précède, le CEPD convient avec la Commission que la situation peut encore être améliorée. Il se réjouit, à cet égard, que le rapport de la Commission renferme des suggestions potentielles de clarifications. Plus spécifiquement, il admet la nécessité de clarifier la relation entre le droit d'information (article 8 IPRED) et les directives relatives à la protection de la vie privée et des données. Ce besoin de précision existe également dans d'autres domaines, mentionnés ci-dessous.

•Publier des orientations sur les limites à la surveillance légale de l'utilisation d'internet

58. L'application des DPI sur l'internet implique dans un premier temps la surveillance et la collecte de données à caractère personnel, à savoir les adresses IP de particuliers. En vertu de l'article 8 de la directive sur la protection des données, une telle surveillance peut être mise en œuvre dans le contexte d'actions en justice, pendantes ou futures, spécifiques. La surveillance de personnes réalisée sous couvert d'anonymat irait à l'encontre des exigences légales.

59. Il serait utile, à cet égard, de disposer d'orientations claires sur l'étendue de la surveillance légale. Par exemple, les titulaires de droits pourraient mener des activités de surveillance ciblée de certaines adresses IP suspectes afin de préparer la procédure et de vérifier l'étendue de la violation présumée. Actuellement, ce type de surveillance semble courant, mais il a en réalité lieu en dehors du cadre juridique en matière de protection des données, y compris de la supervision adéquate des autorités chargées de la protection des données.

60. Cette situation n'est clairement pas satisfaisante. Le CEPD propose par conséquent deux séries de mesures. ***Premièrement***, des orientations sur la surveillance légale devraient être publiées. La Commission, en concertation avec le groupe de travail «Article 29», serait probablement la mieux placée pour mener à bien cette tâche. Ces orientations contribueraient à la mise en place de l'approche harmonisée qui fait actuellement défaut. ***Deuxièmement***, étant donné la nature spécifique de cette surveillance, il serait approprié de soumettre ce traitement de données à un contrôle préalable / la supervision des autorités chargées de la protection des données. Ces autorités devraient analyser les méthodes et procédures employées et accorder ou refuser l'autorisation.

•Publier des orientations sur la façon de garantir une approche équilibrée du transfert d'informations (renseignements sur l'abonné) dans le contexte de procédures judiciaires

61. L'article 8 IPRED définit des critères adéquats sur la base desquels les tribunaux peuvent ordonner la divulgation de l'identité de contrevenants présumés dans le cadre de procédures civiles ou pénales. Comme mentionné précédemment, le CEPD considère que la législation actuelle contribue à la mise en place d'une approche prudente et équilibrée qui permet de garantir le respect des DPI sans entraver excessivement les droits individuels à la protection des données et de la vie privée.

62. Toutefois, la relation entre l'article 8 IPRED, la directive sur la protection des données, la directive «Vie privée et communications électroniques» et l'arrêt *Promusicae* devrait être clarifiée, par exemple dans une communication interprétative de la Commission. Cette communication pourrait également servir de base à la mise en œuvre de procédures d'infraction à l'encontre des États membres qui n'ont pas transposé correctement la législation européenne. Plus spécifiquement, des orientations pratiques sont nécessaires afin d'appliquer l'article 8 IPRED de manière à équilibrer les intérêts des différentes parties et à garantir que les critères qu'il renferme et l'équilibre entre les divers intérêts sont bien compris et respectés.

•Si des modifications sont proposées, elles doivent garantir la protection de la vie privée et des données à caractère personnel

63. Si en dépit des éléments susmentionnés, la Commission soumettait des propositions modifiant le cadre actuel, il est impératif de s'assurer qu'aucune modification du droit existant ne met en péril un système approprié de garanties, de telle sorte que non seulement la protection des droits des titulaires de droits mais aussi la protection des données et de la vie privée soient garanties au sein du système juridique.

Bruxelles, le 8 avril 2011