Questionnaire pour le 4ème thème du Congrès Capitant

« Mondialisation et communications »

Je comprends ce thème comme un synonyme de Mondialisation et Internet

Je fais ci –dessous un questionnaire sous forme de tableau. Vous pouvez répondre, si vous le souhaitez, dans les cases du tableau. Mais c'est à votre gré.

Abréviations :
RGPD : Règlement général à la protection des données
LIL : Loi informatique et libertés
TTIP : Transatlantic Trade and Investment Partnership

I/ **MONDIALISATION, INTERNET ET LES DROITS DES INDIVIDUS**	
A/ Comment sont protégées dans votre droit les données personnelles ?	
Quelle est la définition des données à caractère personnel dans votre droit ? Existe-t-il une définition formelle ?	Il existe une définition formelle, contenue dans l'article 2 de la LIL, qui sera modifiée à compter de 2018 par le RGPD. « *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.* » A compter de l'entrée en vigueur du RGPD, les données à caractère personnel seront définies de la façon suivante : art. 4, 1. RGPD « *toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, par exemple un nom, un numéro*

	d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » → La liste énumérative prévue dans le RGPD est intéressante en ce qu'elle laisse ouverte la possibilité de considérer comme des données à caractère personnel des éléments qui ne sont pas purement des éléments d'identification, mais qui peuvent permettre de singulariser la personne concernée à l'instar des données de géolocalisation ou d'un identifiant en ligne.
Du côté de l'internaute, y a-t-il un droit de propriété sur les données ? S'agit-il plutôt d'un droit à la protection de la vie privée ? (du côté de l'opérateur : valorisation des données : ce sera vu dans le II)	La nature des droits sur les données n'est pas déterminée expressément par le législateur. C'est la jurisprudence européenne qui, semble-t-il, a montré la voie à suivre, sans pour autant que les choses soient définitives en la matière. La CJUE dans son arrêt du 8 avril 2014 (C-293/12 et C-594/12) souligne, en effet, dans son point 53 que « *la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci* ». Le débat reste entier à la lumière du RGPD qui ne prend pas formellement position sur la nature des droits en cause. Il rappelle, certes, dans son premier considérant que « *La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du traité disposent que toute personne a droit à la protection des données à caractère*

	personnel la concernant ». Il est néanmoins prévu dans le texte du RGPD, à l'instar de ce qui existe dans la LIL, un régime relatif à la circulation des données. Ainsi le droit à la portabilité des données atteste de ce droit de nature quasi-réelle dont dispose la personne concernée sur ses données à caractère personnel. Cf. Rédaction de l'article 18 du RGPD. « *Les personnes concernées ont le droit de recevoir les données les concernant qu'elles ont communiquées à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle (…)* *Lorsque la personne concernée exerce son droit à la portabilité des données conformément au paragraphe 1, elle a le droit d'obtenir que les données soient transmises directement d'un responsable du traitement à un autre, lorsque c'est techniquement possible* ».
Faut-il toujours un accord de l'internaute pour recueillir et pour utiliser ses données personnelles ou y a-t-il des cas où on peut le faire sans cet accord ?	Le consentement n'est qu'un des fondements sur lequel la licéité des traitements peut reposer. Dans la **LIL** le consentement semble être le fondement le plus important pour assurer la licéité des traitements. Quoique prédominant, il n'en n'est pas pour autant exclusif. La loi prévoit 5 expédients au consentement : *« 1°- Le respect d'une obligation légale incombant au responsable du traitement ;* *2°- La sauvegarde de la vie de la personne concernée ;* *3°- L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;* *4°- L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de*

	mesures précontractuelles prises à la demande de celle-ci ; *5°- La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée*. » Dans **le RGPD**, le consentement est un mode alternatif aux 5 autres existants, sans préséance *a priori* de l'un sur l'autre : « *- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;* *- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;* *- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;* *- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;* *- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. Ces considérations ne s'appliquent pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.* ».
Y a-t-il des données plus sensibles que d'autres, qui sont soumises à un régime spécial (données de santé, religion, opinions politiques,…) ?	Certaines données sont en effet soumises à un régime spécifique prévu à l'article 8 de la LIL : « *Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou*

	religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ». Il est, certes, prévu, des exceptions à ce régime spécifique, mais le traitement des données sensible reste largement dérogatoire. Le RGPD reproduit largement ce régime d'exception. Il faut toutefois noter que le considérant 8 souligne que les Etats membres disposent d'une certaine marge d'appréciation quant à la protection qu'ils souhaitent reconnaître à cette catégorie singulière des données sensibles. « *Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, notamment en ce qui concerne le traitement des données sensibles. À cet égard, le présent règlement n'exclut pas les législations des États membres qui définissent les situations particulières de traitement, notamment en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite* ».
Votre pays a-t-il conclu (ou fait-il partie d'une Union qui a conclu) un Traité sur le sort des données (comme le traité transatlantique entre l'Europe et les USA par exemple) ? Dans ce cas, comment sont traitées les données ? Ce traité favorise-t-il la protection des personnes ou l'économie ?	Le TTIP en cours de discussion entre dans une nouvelle phase de négociations (25-29 avril NY) mais il est difficile de déterminer dans quelle mesure le droit des données à caractère personnel sera concerné. Formellement les données à caractère personnel sont exclues du champ de la négociation. Néanmoins, parce que cet accord à vocation à faciliter la libre circulation des biens et des services, notamment ceux relatifs aux nouvelles technologies et aux services de l'information, les données à caractère personnel sont susceptibles d'être indirectement concernées par l'accord. En outre, les transferts de données hors UE à destination des Etats-Unis ont été fortement atteints du fait de l'invalidation du *Safe Harbor* par la décision *Max Schrems* (CJUE 6 oct. 2015, C-362/14).

	Bien que la question ne soit pas abordée dans le cadre du TTIP, des discussions sont actuellement en cours afin de faire adopter le *Privacy Shield* qui aura vocation à garantir le niveau de sécurité équivalent nécessaire au transfert des données à caractère personnel vers les Etats-Unis, notamment. A cet égard, le G29 a rendu son avis le 13 avril 2016 sur ce *Privacy Shield* qui a vocation à se substituer au *Safe Harbor* invalidé. Il considère qu'en dépit des améliorations effectives, ils demeurent de sérieuses préoccupations. Le G29 demande notamment que la Commission veille à ce que soit apportées des précisions nécessaires pour améliorer le projet de décision d'adéquation, ce pour garantir un niveau de protection des données personnelles « essentiellement équivalent » au niveau exigé par l'Union européenne.
Comment protège-t-on les personnes dans le cloud-computing (l'informatique en nuage) ?	Il n'existe pas, à l'heure actuelle, de disposition propre à la protection des personnes dans le cloud computing. D'une part, cette absence de protection spécifique tient au fait que le concept de cloud computing revêt différentes réalités. On retiendra ici une approche générale du Cloud computing, consistant dans un système de stockage externalisé de données. Ce qui caractérise la première difficulté à l'égard du Cloud computing dans la perspective de la protection des droits des personnes concernées, c'est de parvenir à qualifier les rapports afin d'appliquer à la relation idoine le régime juridique qui convient. Ainsi, la personne concernée dont les données, notamment à caractère personnel, seront stockées dans le Cloud n'est pas en lien contractuel avec le prestataire de service de Cloud, qui n'est donc pas à proprement parler le responsable de traitement au sens de la loi française. En revanche, le cocontractant du

	prestataire de service de Cloud est le responsable de traitement à l'égard de la personne concernée. Il ne dispose toutefois pas, en premier lieu, dans la plupart des cas, de la faculté de négocier le contrat (ce sont généralement des offres standards contenues dans des contrats d'adhésion) et en second lieu, de la faculté d'assurer la protection effective des données stockées puisque précisément il en externalise le stockage. Cette situation tripartite implique d'adapter les règles pensées dans un rapport bilatéral entre le responsable de traitement et la personne concernée afin d'impliquer le prestataire de service de Cloud, tiers à la relation initiale. S'il peut être considéré comme un sous-traitant, ses obligations devraient toutefois être renforcées afin de tenir compte du pouvoir effectif dont il dispose (obligations, notamment d'information, renforcées et responsabilité renforcée).
Comment protège-t-on les personnes dans le big data ?	Le *Big data*, en tant que technique de traitement massif des données ne permet pas et ne suppose pas à proprement parler l'application de la LIL. Le postulat réside dans le fait, que les données traitées par le Big data ne seraient pas ou plus nécessairement des données à caractère personnel du fait du traitement massif de celles-ci. Pour autant, le *big data* par les perspectives, notamment de profilage, qu'il autorise impose de s'interroger sur un moyen d'assurer la protection des individus dont les données en sont à l'origine. Cette protection peut passer par plusieurs moyens : - il peut tout d'abord être exigé que soit respectée la finalité du traitement initial pour fonder la licéité des traitements ultérieurs massifs. - Il peut ensuite être exigé que le traitement ne concerne pas des

	données à caractère personnel, mais exclusivement des données anonymisées (ou pseudonymisées). - Plus sûrement la protection passera par une responsabilisation des acteurs (plateformes) à l'origine de ces traitements massifs de données, en leur imposant davantage d'obligations de transparence, de vigilance, d'information et de sécurité source de responsabilité accrue. C'est également cette voie qui est suivie en imposant des normes de *privacy by design* ou de *privacy by defaut*, par lesquelles le responsable de traitement doit mettre en place des mesures techniques permettant d'assurer la protection des individus (art ; 23 RGPD) - Enfin, il est prévu de mettre en place des mesures dites d'*empowerment* par lesquelles les personnes concernées reprennent le pouvoir sur leurs données grâce, par exemple, aux mesures de portabilité des données.
Existe-t-il dans votre droit un droit à l'oubli ? Comment se matérialise-t-il ? Pour les pays de l'UE, comment se matérialise dans votre pays la mise en œuvre du droit à l'oubli consacré par les arrêts Google Spain de la Cour de Justice?	La proposition de Règlement en matière de protection des données à caractère personnel dans sa version initiale du 25 janvier 2012 proposait formellement la reconnaissance d'un droit à l'oubli numérique. Pourtant, les mesures admises ne constituaient qu'une application dans l'environnement numérique du droit d'opposition et de retrait déjà connu dans le cadre de la directive de 95 et partant de la LIL. En effet, les dispositions ne prévoyaient l'effacement que de données traitées illicitement. Il convient dès lors de s'entendre sur ce qui constitue un véritable « droit à l'oubli ». Il semble que pour constituer un droit subjectif autonome, il faille admettre que le droit à l'oubli est celui qui permet la remise en cause de données traitées licitement pour lesquelles la personne concernée souhaite que ce traitement

	cesse et que soit déréfencée l'information considérée la concernant. Un tel droit à l'oubli numérique a dans un premier temps était formellement consacré par la CJUE dans un arrêt Costeja contre Google Spain du 13 mai 2014. La cour a en effet admis que « ***le droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom*** (…) ». Il s'agit donc là d'admettre le déréférencement d'une donnée traitée licitement. A la suite de cette consécration prétorienne, les moteurs de recherche ont mis en place un outil pour permettre la mise en œuvre de ce droit à l'oubli. La CNIL a toutefois mis en demeure le géant Google d'appliquer la décision de manière stricte et partant que le déréférencement soit effectif sur toutes les extensions géographiques du moteur de recherche. Faute de se plier à cette injonction, la CNIL française a condamné Google le 25 mars 2016 à une sanction de 100.000 euros d'amende (bien dérisoire pour le géant concerné). Les juridictions françaises ont, en outre, depuis condamné Google (en référé et sous astreinte) au déréférencement dans de multiples décisions notamment celles rendues le 16 septembre 2014 par le TGI de Paris. Depuis cette décision, l'évolution à l'égard du droit à l'oubli se fait également d'un point de vue législatif. **<u>En droit interne</u>**, la loi pour une République numérique, actuellement en discussion devant le Sénat, a consacré expressément un droit à l'oubli mais uniquement à l'adresse des mineurs dont les données sont collectées dans les services de la société de l'information. Il est en effet prévu un complément à l'article 40 de la LIL rédigé comme suit :

	« *Sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte* ». Suivent ensuite les conditions et limites dans lesquelles s'exercerait un tel droit. Il convient de noter que rien n'est précisé quant à la licéité originelle de la collecte, si bien qu'il semble possible d'admettre que soit ici consacré un véritable droit à l'oubli, autorisant la remise en cause de données traitées licitement. De même dans le **RGPD** dans la version issue du trilogue adopté le 14 avril 2016 par le Parlement et le Conseil, il est expressément reconnu un droit au retrait *lato sensu* qui équivaut à un droit au retrait de données traitées licitement, autrement dit un droit à l'oubli, consacré à l'article 7 §3. La personne concernée peut en effet retirer, à tout moment et sans condition, le consentement qui fonde le traitement. De fait, le responsable de traitement, n'est plus autorisé à réaliser les traitements pour l'avenir, ce qui ne porte toutefois pas atteinte aux traitements passés. Un droit à l'oubli est par ailleurs formellement consacré à l'article 17 qui appelle plusieurs observations : - le concept de droit à l'oubli numérique a, d'une part, été formellement réintroduit, entre parenthèse, certes, mais néanmoins explicitement présent dans l'intitulé de l'article 17 ; - aux classiques hypothèses d'effacement de traitements illicites (originellement ou devenus tels) s'ajoutent, d'autre part, deux dispositions qui consacre un véritable droit à

	l'oubli : • *Art 17 c) la personne s'oppose au traitement des données à caractère personnel en vertu de l'article 19 §1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'art. 19, §2* » → une telle disposition autorise un effacement beaucoup plus important et **<u>indépendamment des fondements (licites ou illicites) du traitement,</u>** dès lors qu'il appartient au responsable de traitement de rapporter la preuve de motifs légitimes justifiant son refus lorsque le traitement est justifié par *l'exécution d'une mission d'intérêt public* ou par *une autorité public*, ou ***fondé sur l'intérêt légitime***. • obligation d'effacer art. 17 f) *les données qui ont été collectées dans l'offre de services de la société de l'information visée à l'art. 8, §1.* Le renvoi qui est opéré peut faire l'objet de deux interprétations : - la moins probable, sont visées toutes les données collectées dans le cadre d'un service de la société de l'information (autrement dit le renvoi ne vaut que pour la définition du mode de collecte) ; - la plus probable, le renvoi s'opère pour tout le texte et ne

	sont alors visées que les données collectées relatives à un enfant de moins de 16 ans ou à tout le moins pas au-dessous le 13 ans. En revanche, quel que soit le fondement du traitement, autrement dit y compris quand le traitement est fondé sur le consentement. Cette rédaction des textes atteste d'un élargissement du droit à l'oubli, à l'égard duquel le législateur européen se montrait, à l'origine, très réticent. Toutefois, en dépit de cet élargissement, le droit à l'oubli reste largement encadré. Seules certaines hypothèses sont formellement envisagées. Par ailleurs, les textes (RGPD et Rép. Num) prévoient spécifiquement, de manière assez semblable, que le droit à l'oubli n'est pas absolu, **des limites sont en effet prévues** au rang desquelles figurent notamment: - l'exercice de la liberté d'expression et d'information. Reste posée la question de la personne qui sera à même de réaliser cet arbitrage, souhaitons que ce soit le juge, quoiqu'il faille nécessairement constater que, de fait, ce sera le responsable de traitement qui en sera le premier arbitre en cas de refus d'effacement malgré la demande de la personne concernée.
Qui est compétent pour faire respecter ces règles, existe-t-il une autorité de régulation et de contrôle indépendante, et e quel pouvoir de sanction dispose-t-elle ?	Le juge est, naturellement, l'autorité compétente pour assurer le respect des règles relatives à la protection des libertés individuelles. Toutefois, en France, la Commission Nationale de l'informatique et des libertés, autorité administrative indépendante est compétente pour veiller au respect des droits des personnes concernées. Cette autorité de régulation nationale collabore au sein du Groupe de travail de

	l'article 29 (G29) afin de remplir les missions qui lui sont dévolues. Le Groupe Article 29 est composé de représentants des autorités nationales chargées de la protection des données, du CEPD (contrôleur européen de la protection des données) et de la Commission européenne. Il constitue une plate-forme très importante pour la coopération, et ses principales missions consistent à: . donner à la Commission **des avis d'experts** des Etats membres sur des questions relatives à la protection des données**;** . **promouvoir l'application uniforme** de la directive 95/46 dans tous les États membres de l'UE ainsi qu'en Norvège, au Liechtenstein et en Islande; . **donner à la Commission un avis sur** tout acte communautaire (premier pilier) ayant une incidence sur le droit à la protection des données à caractère personnel. Dans le RGPD il est institué à l'article 64 un comité européen de la protection des données qui assurera la fonction de régulateur européen et aura notamment pour mission d'assurer la coopération renforcée entre les autorités de régulation nationales.
B/ La liberté d'expression sur Internet	
Y a-t-il des atteintes à la liberté d'expression sur Internet qui ont été sanctionnées dans votre droit ou par des juridictions de votre pays ? -sur les réseaux sociaux (ex : cache pudique par Facebook sur le tableau de Courbet « l'origine du monde » révélant un nu féminin un peu osé, qui avait été reproduit par un internaute) -par des moteurs de recherche	Les atteintes à la liberté d'expression peuvent avoir deux types de sources distinctes : - de la part des états, - de la part des opérateurs (acteurs, moteurs de recherche, réseaux sociaux). **1) <u>atteinte à la liberté d'expression de la part des Etats</u>**. Le contexte de lutte antiterroriste depuis les attentats de janvier 2015 a, sans aucun

	doute, accentué les atteintes à la liberté d'expression réalisées par les gouvernements en accroissant, notamment par le recours à la loi sur le renseignement adoptée le 24 juillet 2015 (n°2015-912), la faculté de procéder à des recherches algorithmiques et une surveillance massive sur les réseaux. L'ONG Freedom house, à l'origine du rapport *freedom on the net*, note dans son rapport annuel de 2015 que, notamment en France, les gouvernements ont « *de plus plus tendance à pratiquer la censure sur des informations d'intérêt public* » et « *exercent une pression accrue sur les acteurs du secteur privé pour retirer certains contenus* ». **2) Atteinte à la liberté d'expression de la part des acteurs privés opérant sur le réseau**. Les CGU des opérateurs tels que les grands réseaux sociaux (Facebook) ou moteur de recherche (Google) font référence au droit qu'ils s'octroient de limiter les contenus jugés contraire à leur « moralité », à la politique du réseau ou encore aux règles de la communauté. Ces clauses ont été jugées comme présumées irréfragablement abusives par la Commission des clauses abusives dans sa recommandation 2014-02 du 7 novembre 2014, point 30. En outre, les juridictions françaises ont été saisies d'une telle question. Si pour l'heure les juridictions françaises (TGI 5 mars 2015, et CA Paris 12 février 2016) ne se sont prononcées que sur la faculté à appliquer le droit français à la société Facebook en dépit d'une clause de choix de loi désignant la loi californienne, elles devront à terme déterminer si de telles atteintes à la liberté d'expression des internautes sont tolérables et légales.
Y a t-il à l'inverse des abus de la liberté d'expression qui ont été sanctionnés par vos juridictions ?	Dans une affaire Facebook jugé par le Tribunal correctionnel de Cayenne du 15 juillet 2014, une peine de prison ferme a

Propos diffamatoires par exemple Injures sur Internet	été prononcée à l'encontre d'une élue Front national qui avait tenu sur sa page Facebook des propos racistes (photo d'un singe et de la ministre de l'Intérieur de l'époque, avec l'indication respectivement « à 18 mois » et « maintenant »). Plus récemment, le TGI de Béthune a condamné, le 16 septembre 2015, à une amende un internaute pour avoir diffamé une boîte de nuit sur son mur Facebook. Ces affaires, recensées de manière non exhaustives, attestent que les réseaux ne sauraient être le lieu de la liberté d'expression absolue et que la balance des intérêts qui doit être opérée pour, proportionnellement, établir l'application des droits et libertés fondamentales dans le monde réel doit également s'appliquer dans le monde digital. Il convient toutefois de noter que dans ces affaires, les opérateurs ne sont que des intermédiaires, les médias, le support du contenu illicite ou diffamatoire. L'action, et la condamnation, pèsent sur l'internaute.
Quels moyens peuvent être mis en œuvre pour faire cesser ces atteintes ? Sont-ils efficaces ?	Afin de faire cesser le trouble, la personne qui souffre d'un préjudice en raison d'un contenu illicite peut agir auprès de l'hébergeur en lui notifiant les contenus illicites sur le fondement de l'article 6 de la LCEN. L'hébergeur engage sa responsabilité si, en dépit du caractère manifestement illicite et de la notification faite, il ne retire pas promptement le contenu. Le caractère illicite du contenu pourra être invoqué sur des fondements juridiques classiques : diffamation, propos injurieux, racistes ou homophobes, vie privée, atteinte aux droits de propriété intellectuelle.
C/ Autres droits	
Comment est protégé le droit au respect de la vie privée sur Internet (en dehors de la question des données personnelles) ?	La protection de la vie privée est assurée par les mêmes moyens dans l'univers digital que dans le monde réel.

Notamment sur les sites de journaux en ligne ?	L'article 9 du Code civil peut ainsi être invoqué par toute personne qui souffre d'une atteinte à sa vie privée. Le juge devra donc opérer une balance des intérêts entre la protection de la vie privée demandée et la liberté d'expression. L'action peut être exercée directement contre l'éditeur, si le site internet dispose de ce statut c'est directement contre lui que le recours sera exercé, à défaut s'il n'est qu'hébergeur, l'action sera dirigée contre l'éditeur de contenu.
Quels sont les moyens pour faire cesser les atteintes ?	L'action peut être exercée en référé pour faire cesser au plus vite les atteintes. Il peut également, lorsque le contenu est manifestement illicite, être notifié auprès de l'hébergeur afin qu'il le retire promptement, sauf à engager sa responsabilité (Art. 6.5 LCEN).
Les droits de propriété intellectuelle sont-ils fragilisés par Internet ? Votre droit prévoit-il un cadre spécifique de responsabilité pour les hébergeurs ou les plateformes pour le contenu qu'ils hébergent ou diffusent ?	Les droits de propriété intellectuelle sont nécessairement fragilisés par Internet en raison de l'importance du réseau et du caractère extraterritorial qu'il autorise. Il y a, en effet, une double antinomie de principe entre internet et les droits de propriété intellectuelle : - logique de liberté (Internet) Vs. Logique de privatisation et de réservation (Droit de propriété intellectuelle) - logique de mondialisation et d'universalisme (Internet) Vs. Logique territoriale (Droit de propriété intellectuelle). Les atteintes au droit de propriété intellectuelle qui peuvent être réalisées sur internet ou par le biais d'internet sont multiples et variées. Il peut s'agir d'atteintes au droit de l'auteur, du fait de l'existence de plateformes de téléchargement en ligne de type *Peer-to-Peer*, de plateformes vidéos qui donnent accès à des œuvres protégées sans l'autorisation de l'auteur, de plateformes de commerce en ligne proposant à la vente des biens contrefaisants, de l'usage de marque à titre de mots-clés dans des systèmes de référencement de moteur de

	recherche ou encore de l'absence de respect des droits de PI par les prestataires de services de réseaux sociaux. Si une importante variété caractérise les atteintes susceptibles d'intervenir, une difficulté commune existe qui consiste dans l'effectivité des recours destinés à assurer la protection des titulaires de droits. Outre que la plupart des opérateurs revendiquent l'application de dispositions étrangères qui ne sont pas toutes aussi protectrices des droits de PI que l'est le droit français, certaines limitations ou exceptions peuvent être parfois opposées aux droits de PI avec un certain succès. Le droit français prévoit un cadre particulier pour la ***responsabilité des intermédiaires techniques***. La LCEN distingue trois catégories d'acteurs : les FAI (Fournisseurs d'accès à internet) qui ne sont pas responsables du contenu en qualité de simples intermédiaires techniques, les éditeurs qui sont pleinement responsables du contenu qu'ils éditent et une sorte de catégorie intermédiaire, les hébergeurs, qui en raison de l'absence de rôle actif pris dans la diffusion du contenu, ne sont pas responsables à l'égard du contenu, sauf si étant notifiés du caractère manifestement illicite de celui-ci ils ne le retirent pas promptement. Ce statut très bienveillant est notamment reconnu à la plupart des géants du Net (Google, Ebay, Youtube, Dailymotion) qui le revendiquent largement pour l'immunité qu'il leur confère.
D/ Aspects de droit international privé	
Quel est dans votre droit le tribunal compétent en matière de cyber-délits ?	La détermination de la juridiction compétente dépend de la détermination du lieu du fait dommageable. Cette notion ouvre une alternative à la victime entre le lieu du fait générateur et le lieu du

	dommage. L'interprétation de ces deux notions à la lumière des cyber-délits a été réalisée en considérant, sans que cela suscite de polémique, que le lieu du fait générateur, qui permet l'indemnisation de l'entier dommage, est celui du lieu où la décision de mise en ligne à été prise ; en revanche la détermination du lieu du dommage est sujette à davantage de controverses. La détermination du lieu du dommage dépend en effet du critère retenu. Le droit européen comme le droit commun se fondent sur deux critères possibles pour déterminer le lieu du dommage : - Le critère de l'accessibilité qui permet à la juridiction d'être compétente dès lors que le site est accessible dans le ressort de la juridiction. - Le critère de la focalisation, qui suppose un critère de rattachement plus précis et que le public du pays soit ciblé (par l'usage par exemple de la langue). Le choix entre ces deux critères dépend de la nature du cyber-délit et, parfois, de la juridiction saisie. - en matière d'atteinte à **des droits de la personnalité**, la CJUE a consacré, au titre du lieu du dommage, le critère de l'accessibilité (arrêt eDate CJUE 25 oct. 2011, C-509/09 et C-161/10). Il en résulte que la victime peut saisir la juridiction de n'importe quel lieu où le site litigieux est simplement accessible, mais, c'est essentiel, uniquement pour les dommages subis dans le ressort de cette juridiction. Il faut toutefois souligner que cet arrêt important a ajouté un chef de compétence non prévu par les textes qui permet à la victime d'agir devant le tribunal de son domicile pour l'intégralité du dommage, ce qui diminue l'intérêt du critère du lieu du fait générateur. - en matière d'atteinte aux droits de

	propriété intellectuelle, il semble qu'il faille distinguer, puisqu'en matière de **droit d'auteur**, la CJUE a semble-t-il retenu le critère de l'accessibilité (CJUE Pinckney, 3 octobre 2013, C-170/12, et Hejduk 22 janvier 2015, C-441/13). La Cour de cassation a suivi la position des juges luxembourgeois dans un arrêt rendu le même jour que celui ayant donné lieu au recours préjudiciel dans l'affaire Pinckney, Civ. 1e 22 janvier 2014, en retenant le critère de l'accessibilité. - en matière d'atteinte au **droit de marques**, notamment en cas d'usage de la marque à titre de mot clé, la CJUE (Wintersteiger,19 avril 2012, C-523/10) a dit pour droit que, selon l'article 5§3 du Règlement Bruxelles I, le litige peut être porté soit devant les juridictions de l'État membre dans lequel la marque est enregistrée, soit devant celles de l'État membre du lieu d'établissement de l'annonceur, ne retenant donc pas le critère de l'accessibilité, mais semblant également s'écarter de celui de la focalisation. Cette solution devrait être, selon certains auteurs (V. Not. T. Azzi), étendue à toutes les hypothèses de contrefaçon de droits de propriété industrielle. La Cour de cassation n'adopte toutefois pas la même position en matière de contrefaçon de marque puisque dans deux affaires postérieures elle a retenu le critère de la focalisation (Com. 3 mai 2012 et Com. 12 février 2013). - en matière **de concurrence déloyale**, la Cour de cassation a saisie la CJUE d'une question préjudicielle (Com. 10 novembre 2015) afin de déterminer quel est le critère applicable en cas violation alléguée d'interdictions de revente hors d'un réseau de distribution sélective et via une place de marché, au moyen d'offres de vente mises en ligne sur plusieurs sites exploités dans différents Etats membres. La réponse n'est toujours pas connue.

Est-ce le même pour tous les cyber-délits ?	Non, Cf. Supra
Quelle est dans votre droit la loi applicable à l'indemnisation de la victime d'un cyber-délit ?	Les sources diffèrent selon les types de cyber-délits. Le règlement Rome II est compétent pour les **atteintes à la concurrence** et aux droits **de propriété intellectuelle**, à l'exclusion des droits d'auteur pour lesquels la compétence de la convention de Berne prime. Enfin, relativement aux atteintes aux **droits de la personnalité**, faute d'entrer dans le champ de compétence du Règlement Rome II, elles relèvent des règles de conflits jurisprudentielles françaises. De manière synthétique, l'ensemble de ces textes, par des qualifications différentes (*lex loci delicti*, loi du marché affecté, loi du pays pour lequel la protection est demandée), exige que soit déterminé pour résoudre le conflit de loi, le lieu du dommage. Or à cet égard, la jurisprudence, française comme européenne, semble se fonder sur le critère de la focalisation (Cass. Civ. 1e 1er juillet 2012, aufeminin.com, CJUE, 12 juillet 2011, L'Oréal, aff. C 324/09, CJUE, 8 octobre 2012, Football Dataco, C 173/11).
Est-ce la même pour tous les cyber-délits ?	Cf. Supra
II/ MONDIALISATION, INTERNET ET LA PUISSANCE DES ACTEURS (les géants de l'Internet : GAFA : Google Apple Facebook Amazon, et d'autres encore : booking, expedia, twitter, etc…)	
Le modèle économique des géants de l'Internet repose sur une prétendue gratuité : -gratuité apparente parce que l'internaute transfère ses données à caractère personnel -gratuité apparente parce que le géant se paye sur une autre face du marché par de la publicité Votre droit a-t-il déjà fait une analyse de cette fausse gratuité ? Y a t-il déjà eu des textes, des recommandations ou des	La commission des clauses abusives à l'occasion de la recommandation (n°2014-02) rendue sur les conditions générales des contrats de fourniture de service de réseaux sociaux s'est prononcée sur la prétendue gratuité utilisée par les géants de l'internet. Afin de déclarer abusive les clauses revendiquant cette prétendue gratuité, la commission des clauses abusives a considéré que « *de nombreux contrats de fourniture de service de réseautage social*

décisions sur ce point ?	*prévoient des clauses affirmant que les services proposés sont gratuits ; que ces clauses laissent croire à l'utilisateur consommateur ou non-professionnel que le service est dépourvu de toute contrepartie de sa part, alors que, si toute contrepartie monétaire à sa charge est exclue, les données, informations et contenus qu'il dépose, consciemment ou non, à l'occasion de l'utilisation du réseau social, constituent une contrepartie qui s'analyse en une rémunération ou un prix, potentiellement valorisable par le professionnel ; que cette ambiguïté de la clause de rémunération autorise son examen par une interprétation a contrario de l'article L. 132-1, alinéa 7, du code de la consommation, selon lequel l'appréciation du caractère abusif des clauses ne porte pas sur l'adéquation de la rémunération au service offert « pour autant que les clauses soient rédigées de façon claire et compréhensible » ; que ces clauses sont de nature à créer un déséquilibre significatif entre les droits et obligations des parties au contrat au détriment du consommateur ou du non-professionnel en ce qu'elles lui laissent croire qu'il ne fournit aucune contrepartie, alors que celle-ci réside dans l'ensemble des traitements de ses données à caractère personnel, des informations et des contenus déposés sur le réseau* ». Il convient également de relever dans la proposition de Directive du 9 décembre 2015 concernant certains aspects des contrats de fourniture de contenu numérique (COM (2015) 634 Final), une définition de l'objet du contrat qui atteste d'une prise en compte de cette prétendue gratuité. L'article 3 relatif au champ d'application de la directive dispose en effet que « *La présente directive s'applique à tout contrat par lequel un fournisseur fournit un contenu numérique au consommateur ou s'engage à le faire, en* ***échange duquel un prix doit être acquitté ou une contrepartie non pécuniaire, sous la forme de données*****

	personnelles ou de toutes autres données*, doit être apportée de façon active par le consommateur* ».
Les géants jouent avec les différents systèmes juridiques pour optimiser au mieux leur situation : -d'abord leur **situation juridique** : clause attributive de juridiction, clause de loi applicable -ensuite leur **situation fiscale**, notamment en faisant de la marge, là où l'impôt est le plus faible (Google et le double Irlandais ou le sandwich néerlandais ex : certains réseaux sociaux payent moins de 6000 euros d'impôts en France pour plusieurs milliards engrangés) Quelle est la position de votre droit face à une telle optimisation permise par la mondialisation, dans ces deux domaines?	**1) Face à l'optimisation juridique**, les juridictions françaises, suivant en cela la position notamment de la commission des clauses abusives dans la recommandation précitée (n°2014-02), considèrent que les clauses attributives de juridiction et de choix de loi présentes dans des ***contrats passés avec des consommateurs*** sont des clauses abusives qui doivent en conséquence être réputées non écrites (Cf. CA Pau 23 mars 2012, Arrêt confirmatif Facebook CA Paris 12 février 2016). Le raisonnement de ces juridictions repose essentiellement, pour les clauses attributives de juridiction, sur le Règlement Bruxelles I (applicable désormais même lorsque le défendeur a son domicile hors UE) ; pour les clauses de choix de loi, le raisonnement repose sur le double fondement de l'article 6 du Règlement Rome I qui prévoit que la loi applicable au consommateur ne peut le priver de la protection que lui assurent les dispositions impératives de la loi de sa résidence habituelle et de l'article 14 du règlement Rome II qui n'admet, en matière d'obligations non contractuelles, le choix de la loi applicable à l'obligation non-contractuelle qu'après la survenance du fait dommageable. A l'inverse, lorsqu'il ne s'agit pas de contrats BTC ***mais de contrats entre professionnels***, la jurisprudence française se montre bienveillante avec les clauses attributives de juridiction (Com. 24 novembre 2015). Il n'en va pas de même pour les clauses de choix de loi, si elles sont admises à l'égard des obligations contractuelles dans le Règlement Rome I, le Règlement Rome II se montre plus hostile à leur égard dans les obligations non contractuelles. Elles sont interdites pour les obligations résultant d'une

	atteinte aux droits de propriété intellectuelle ou de concurrence déloyale. S'agissant des atteintes aux droits de la personnalité, exclues du domaine du règlement, l'autonomie n'est pas non plus permise, si ce n'est un accord procédural en faveur de la loi du for. Ces dispositions pourront être, de fait, aisément contournées grâce à la validité de principe des clauses attributives de juridiction. 2) **<u>Face à l'optimisation fiscale</u>**, la ***jurisprudence*** tente d'apporter des réponses mesurées avec les outils dont elle dispose. Ainsi, la CJUE a décidé dans un arrêt du 17 décembre 2015, saisie d'une question préjudicielle par les juridictions hongroise, « *qu'en l'absence d'autres éléments, ne constitue pas une pratique abusive le transfert du savoir-faire permettant l'exploitation d'un site érotique de la Hongrie vers Madère où un taux de TVA moins élevé s'applique. En revanche, ce transfert constitue une pratique abusive si son objectif est de dissimuler le fait que le site est en réalité exploité depuis la Hongrie* ». Dès lors, l'optimisation fiscale peut être appréhendée comme une pratique abusive s'il existe d'autres éléments que la simple conclusion de licence avec des opérateurs dans un état pratiquant des taux fiscaux plus attractifs. A l'aune de cette jurisprudence il apparaît nécessaire de modifier les outils permettant d'appréhender ces pratiques d'optimisation fiscale. ***Au plan national***, le 18 janvier 2013 un rapport a été rendu sur la fiscalité du secteur numérique (Rapport Colin – Collin). Ce rapport invite le gouvernement à poursuivre ses efforts pour détecter et lutter contre les comportements frauduleux prenant appui sur les technologies du numérique. Certaines propositions innovantes sont formulées dans le rapport, au sujet d'une fiscalité nationale assise sur la détention des données personnelles.

	Au plan international, afin de lutter contre les pratiques d'érosion de la base d'imposition et de transferts des bénéfices permettant en toute légalité l'optimisation fiscale décriée, le G20 et l'OCDE ont mis en place le projet BEPS qui doit permettre de lutter contre ces pratiques et permettre une meilleure coopération fiscale entre les Etats à l'horizon 2020. Dans le cadre du projet BEPS différentes mesures sont actuellement discutées et négociées au rang desquelles il est prévu: - un réexamen des standards fiscaux visant à supprimer la double imposition, pour mettre un terme à l'utilisation abusive des règles existantes et éliminer les possibilités d'érosion de la base d'imposition et de transfert des bénéfices. - Une révision des principes applicables en matière de prix de transferts concernant les actifs incorporels. - Une révision de la définition de l'établissement stable pour mettre en échec les stratégies visant à éviter artificiellement un lien fiscal, notamment au moyen de la conclusion d'accords de commissionnaires et d'une fragmentation des activités commerciales. - Négociation en vue de l'adoption d'un instrument multilatéral pour appliquer les mesures du BEPS afin de renforcer la coopération fiscale internationale.
Les géants de l'Internet se rendent parfois coupables d'abus de position dominante ? Y a-t-il eu dans votre pays des affaires concernant de tels abus ?	La société Google, acteur essentiel sur le marché des moteurs de recherche, propose également toute une gamme de services à l'égard desquels l'abus de position dominante a pu être recherché. Ainsi, par un arrêt du 16 avril 2013, la Chambre commerciale de la Cour de cassation a refusé de reconnaître un tel abus dans le fait pour Google de suspendre

	l'accès à la société eKanopi aux services Adwords et Adsense pour non-respect des CGU, faute de caractériser l'impact négatif de cette pratique sur le jeu de la concurrence. Solution confirmée après saisine de l'Autorité de la concurrence par Com. 19 janvier 2016. La société Google a également était assignée à l'égard de son service Google Maps pour abus de position dominante par la société Bottin cartographe. Le Tribunal de Commerce de Paris dans une décision du 31 janvier 2012 avait admis cet abus. Par un arrêt du 20 novembre 2013, la CA de Paris a renvoyé dans cette affaire, la question à l'Autorité de la concurrence afin qu'elle donne son « *avis sur le caractère de pratique anticoncurrentielle, au regard des articles 102 du TFUE et L 420-2 du code de commerce, de la pratique alléguée (…), et par conséquent, sur le marché pertinent, le marché affecté, la position de la société Google sur ce marché, et la constitution de l'abus de prédation à partir du test de coûts pertinents* ». Après l'avis rendu en ce sens le 16 décembre 2014 par l'Autorité de la concurrence, la CA de Paris, dans un arrêt du 25 novembre 2015 a refusé d'admettre l'abus de position dominante de la part de Google sur ce service Google Maps. Au niveau Européen, certaines actions ont également été menées à l'encontre de la société Google. Après avoir emprunté, en vain, la voie de la procédure négociée (procédure dite d'engagement), la Commission a notifié le 15 mai 2015 des griefs à la société Google, marquant ainsi le début de la procédure contentieuse. Une seule pratique est pour l'heure stigmatisée par la Commission, celle du référencement prioritaire du comparateur de prix Google Shopping. L'abus de position dominante pourrait bien être retenu à son encontre pour ne pas avoir fait application des critères neutres de son algorithme.

Les géants de l'Internet construisent souvent des systèmes fermés ou semi-fermés: exemple : Apple : vous avez un Iphone, il faut aller sur apple store, etc.. Votre droit a-t-il appréhendé ces exclusivités et ces écosystèmes fermés ou semi-fermés ?	L'autorité de la concurrence, ainsi que de nombreuses études, ont démontré que le caractère fermé d'un écosystème n'est pas nécessairement néfaste à la concurrence et peut même s'avérer vertueux pour le consommateur, à la condition notamment que soit préservée sa liberté d'accès à d'autres écosystèmes en lui assurant la faculté de récupérer l'objet de ce dont il dispose dans le premier environnement. Ainsi à cette fin, la reconnaissance de système de portabilité des données ou du contenus numérique ou en ligne, à l'instar de ce qui est proposé tant au plan interne par la loi pour la république numérique ou les diverses propositions de règlement et de directive qui s'inscrivent dans le cadre de l'agenda numérique de la Commission (9 décembre 2015), sont autant de solutions que le droit peut apporter pour appréhender ces systèmes et les rendre plus vertueux en diminuant les coûts de commutation ou *switching cost,* ce qui contribue à préserver la liberté de choix du consommateur qui n'est alors pas un consommateur captif.
Les contrats que proposent les géants de l'Internet aux internautes sont des contrats d'adhésion. Votre droit protège-t-il les internautes dans ce cadre et si oui, comment ? (clauses abusives, pratiques commerciales déloyales, mais est-ce commercial si c'est gratuit ? etc…)	Le droit français assure la protection des internautes face à ces contrats d'adhésion que le consommateur ne peut qu'accepter "en bloc" sans disposer d'un quelconque pouvoir de négociation ou de discussion relativement à son contenu – ce d'autant plus, lorsqu'il n'aura même pas eu conscience de contracter... – par le recours aux clauses abusives dans les **contrats de BTC**. Dans les multiples domaines de l'Internet, la Commission des clauses abusives à stigmatisé les clauses (forts nombreuses) de ces contrats qui sont susceptibles d'être réputées non écrites en raison de leur caractère abusif. L'examen de l'ensemble de ces contrats, pourtant fort différents, amène à un constat commun qui tient dans l'absence d'équilibre entre les prestations de chacune des parties. Ainsi, depuis la

	recommandation relative aux contrats de fourniture d'Internet (Recommandation n°03-01), celle relative aux contrats proposant aux consommateurs les services groupés de l'Internet, du téléphone et de la télévision (dite *triple play*) (Recommandation n°07-01), celle relative aux contrats de vente conclus par Internet (n°07-02) jusqu'à celle qui a été rendue en matière de contrats de fourniture de services de réseaux sociaux , toutes les étapes de l'Internet se sont vues analysées et à, chaque fois, les géants de l'Internet ont été sanctionnés. La **question de la reconnaissance de pratiques commerciales déloyales** peut se poser face à la revendication de la gratuité qui est faite par de nombreux opérateurs de l'internet. Cette prétendue gratuité ne doit toutefois pas tromper, et ne doit pas, selon nous, exclure l'application de la directive PCD, directive n°2001/83. La directive a, en effet, vocation à s'appliquer, conformément à l'article 3, « *à tout contrat conclu entre un professionnel et un consommateur* » entendu largement, et non aux seuls contrat de vente ou de service conclus entre un professionnel et un consommateur comme pourrait le laisser penser une lecture croisée, mais néanmoins erronée, de l'article 3 et de l'article 2 qui définit ces conventions. Le champ d'application de la directive doit en effet s'entendre largement. Le législateur européen n'a nullement entendu circonscrire le champ d'application du texte de manière exhaustive et semble avoir privilégié une définition ouverte limitée uniquement par les exclusions prévues à l'article 3. 3. Ainsi, il n'existe pas de liste exhaustive des types de contrats inclus dans le champ d'application de la directive, la seule exigence formelle étant qu'il s'agisse d'un contrat entre un professionnel et un consommateur.

	En outre, la lecture du considérant n°20, atteste de la volonté d'ouverture du législateur européen vers les contrats de la société de l'information. Il y est en effet précisé ce qu'il convient d'entendre par la notion de contrat à distance. Le texte dispose en effet : « (20) *La définition du contrat à distance devrait couvrir tous les cas dans lesquels un contrat est conclu entre le professionnel et le consommateur dans le cadre d'un système organisé de vente ou de prestation de service à distance par le recours exclusif à une ou plusieurs techniques de communication à distance (vente par correspondance, internet, téléphone ou fax), jusqu'au moment, et y compris au moment, où le contrat est conclu. (…)* ***La notion de système organisé de vente ou de prestation de service à distance devrait inclure les systèmes proposés par un tiers autre que le professionnel mais utilisés par ce dernier, par exemple une plateforme en ligne.*** *Elle ne devrait pas couvrir, cependant, les cas où des sites internet offrent uniquement des informations sur le professionnel, ses biens et/ou ses services ainsi que ses coordonnées.* » . L'esprit de la loi vient donc confirmer sa lettre et atteste de la volonté du législateur de couvrir le plus large spectre concernant le champ d'application de la directive sans le restreindre à des contrats prédéfinis. Une telle démarche est louable dans une perspective d'évolution des techniques contractuelles qui ne permet que difficilement d'anticiper les évolutions de la pratique et évite ainsi l'obsolescence trop rapide du dispositif législatif. Un contrat de services au sens de l'article 2.6 de la directive PCD peut-il être un contrat gratuit ? L'objection, fondée sur la définition du contrat de prestation de service contenue à l'article 2. 6, selon laquelle les contrats proposés par les géants de l'internet étant des contrats gratuits ne saurait être des contrats de

	services au sens de la directive, excluant ainsi son application, ne devrait pas être dirimante. D'une part, car ainsi qu'il vient d'être dit cette définition ne nous paraît pas devoir circonscrire le champ d'application de la directive dès lors que la lettre de l'article 3, non démentie par l'esprit du texte, invite à retenir une conception large des contrats auxquels s'applique la directive. Le texte prévoit que les dispositions s'appliquent « *à tout contrat conclu entre un professionnel et un consommateur* », nullement à tout contrat de vente ou de prestation de services. Il n'est donc par principe nullement nécessaire de se référer à la définition du contrat de prestation de services pour déterminer le champ d'application de la directive. D'autre part, l'objection n'est pas dirimante dès lors que les contrats de la société de l'information peuvent néanmoins répondre à la définition posée à l'article 2.6. Le texte dispose en effet que constitue un contrat de services : « *tout contrat autre qu'un contrat de vente en vertu duquel le professionnel fournit ou s'engage à fournir un service au consommateur et le consommateur paie ou s'engage à payer le prix de celui-ci* ». La référence au paiement d'un prix par le consommateur ne devrait nullement exclure du champ de la définition les contrats proposés par les géants de l'internet et ce à plusieurs titres : • Tout d'abord, car le prix doit s'entendre également d'une contrepartie non-monétaire. Or le contrat n'étant pas gratuit, ainsi qu'il a été démontré, la contrepartie du consommateur existe bien et réside dans les données, contenus et autres informations laissés volontairement ou non, par le consommateur et utilisés par le géant de l'internet en cause, fournisseur de service de réseau

	social, de moteur de recherche ou autres application de service à l'instar d'un service de cartes en ligne. • Ensuite, car la notion de paiement ne suppose par nécessairement la remise d'une somme d'argent. Ainsi, un auteur souligne (J. François), à raison, que « *dans la langue juridique, le terme « paiement » est plus largement entendu que dans la langue courante. Pour le non juriste, ce terme évoque la remise d'une somme d'argent au créancier d'une obligation pécuniaire. Pour le juriste, le paiement désigne plus généralement l'exécution volontaire de l'obligation, quel qu'en soit l'objet (…). Il convient donc de définir abstraitement le paiement comme l'extinction de l'obligation par son exécution volontaire* ». Il peut donc y avoir un contrat de service quoiqu'il n'y ait pas de versement d'argent. L'évaluation monétaire du service fourni n'est pas un critère pour justifier de l'application de la directive, ce même s'il est loisible aux Etats d'en décider autrement. Il est en effet prévu à l'article 3.4 que « *Les États membres peuvent décider de ne pas appliquer la présente directive ou de ne pas maintenir ou introduire des dispositions nationales correspondantes, pour les contrats hors établissement pour lesquels le paiement à charge du consommateur n'excède pas 50 EUR. Les États membres peuvent prévoir une valeur inférieure dans leur législation nationale.* ». A contrario, dès lors qu'aucun seuil n'est prévu expressément, à l'instar du droit français, tous les contrats de prestation de service pour lesquels un paiement, quelque soit son

	objet, de la part du consommateur est réalisé sont susceptibles d'entrer dans le champ de la directive. • Enfin, car les opérateurs de l'internet proposent un ensemble de service tel que des services de mise en relation des utilisateurs, ou de moteur de recherche, mais également des services qui suppose un versement monétaire de la part de l'utilisateur. Qu'il s'agisse d'achats de bien (ou de contenus numériques) proposés par des annonceurs hébergés sur la plateforme en cause (Facebook ou Google) et accessible dans le « fil » ou sur le mur des utilisateurs ou des achats d'applications ou de services directement proposés par la plateforme. Les services proposés ne sont donc pas nécessairement et intégralement dénués de contrepartie monétaire. Il ne fait donc aucun doute, pour l'ensemble de ces raisons, que la directive n°2001/83 s'applique à la plupart des contrats des géants de l'internet.
III/ MONDIALISATION, INTERNET ET LES DIFFICULTES DE LA REPRESSION DES PRATIQUES ILLICITES	
Comment votre droit lutte-t-il contre la pédopornographie sur Internet ?	La pédopornographie constitue une infraction pénale incriminée par l'article L. 227-23 du Code pénal qui dispose que *« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende*. *Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou*

	représentation. *Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.* *Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.* *Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende.* *Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.* *La tentative des délits prévus au présent article est punie des mêmes peines.* *Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette per-* *sonne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image.* ». Lorsque de tels faits sont constatés sur les réseaux une notification doit être faite à l'hébergeur qui doit promptement retirer le contenu pédopornographique à défaut sa responsabilité serait engagée conformément aux dispositions de l'article 6. 5 de la LCEN. Afin d'assurer une plus grande efficience du dispositif répressif, il a été mis en place à partir de 2006 une plateforme de signalement, PHAROS (plate-forme

	d'harmonisation, d'analyse, de recoupement et d'orientation des signalements). Un site internet unique, www.internetsignalement.gouv.fr, a également été mis en place en 2009 afin de centraliser les plaintes et les adresser au service idoine.
Comment votre droit lutte-t-il contre les propos racistes, haineux sur Internet ?	Les propos injurieux, diffamatoires ou qui incitent à la haine raciale ou religieuse constituent des infractions incriminées par les articles 29 et suivants de la loi du 29 juillet 1881. L'auteur des propos, ainsi que l'éditeur, sont les seuls à pouvoir être poursuivis directement du chef de ces infractions. L'action publique est enfermée dans un court délai de prescription prévu à l'article 65 de la loi du 29 juillet 1881 qui s'applique, contrairement à ce qui avait été souhaité par le législateur en raison de la censure opérée par le Conseil Constitutionnel (Ccel 10 juin 2004), de manière identique que les propos soient tenus par voie de presse écrite ou par voie numérique. Le point de départ court à compter de la date à laquelle le message à été mis pour la première fois à disposition des utilisateurs du réseau. En revanche, l'hébergeur informé des propos racistes ou injurieux qu'il héberge engage sa responsabilité en vertu de l'article 6.5 de la LCEN s'il ne retire pas promptement ce contenu manifestement illicite. En outre, la LCEN prévoit que les fournisseurs d'accès à internet et les hébergeurs sont tenus par une obligation de mise en place d'un dispositif facilement accessible et visible, qui permet à tous de porter à leur connaissance tout abus de l'expression sur leur réseau ou site Web. Ils sont de même soumis à deux obligations générales, dont le manquement est sanctionné par un an de prison et 75 000 euros d'amende. Il leur

	incombe, d'une part, une obligation d'information à l'égard des autorités publiques compétentes de toutes activités illicites, prévues aux articles 23 et suivants de la loi de 1881, qu'exerceraient les destinataires de leurs sites. Ils sont, d'autre part, tenus de mettre à la disposition du public les moyens qu'ils consacrent à la lutte contre ces activités illicites. De telles obligations liant les fournisseurs d'accès et hébergeurs sont justifiées du fait de l'existence d'un impératif de garantie du droit de réponse. En effet, outre le droit de réponse prévu par la loi du 29 juillet 1881 sur la liberté de la presse, la LCEN a instauré un droit de réponse propre à internet à l'article 6.4.
Le droit pénal de votre pays est-il efficace pour lutter contre de telles infractions ?	La question de la détermination du point du départ de la courte prescription (la plus courte d'Europe) est très débattue et contribue largement à l'efficacité du dispositif. En effet, pour de nombreux auteurs, une lutte efficace ne peut être assurée que grâce à une prise en compte différenciée de la prescription selon que les propos ont été tenus en ligne ou par voie de papier. Pour ces auteurs, il serait souhaitable, conformément à ce qu'avait proposé le législateur en 2004, à ce que le point de départ du délai de prescription soit reporté à la date à laquelle cesse la mise à disposition du public. La balance des intérêts avec la liberté d'expression justifie toutefois une appréciation stricte de l'infraction considérée.
Votre pays met-il en avant la soft law, l'autorégulation pour lutter contre de telles infractions ?	Pas à ma connaissance. (Il existe bien une autorégulation en matière de lutte contre les infractions de contrefaçon avec la mise en place de chartes (Cf. Charte Ebay), mais je ne connais pas de système semblable à l'égard des infractions précitées).
Existe-t-il des lois d'exception permettant de requérir le transfert des données par les acteurs d'internet aux autorités	La directive permettant la conservation des données générées ou traitées par les fournisseurs de services de

nationales ?	communications électroniques accessibles au public ou de réseaux publics de communication, visant ainsi à garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite des infractions graves, comme notamment les infractions liées à la criminalité organisée et au terrorisme a été invalidée par une décision de la CJUE du 8 avril 2014. Dans le cadre du paquet « données » est actuellement discutée la réforme du 3e pilier, et notamment de la décision-cadre 2008/977/JAI du Conseil 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. Dans ce contexte, une proposition de directive a été faite le 25 janvier 2012 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière ou d'exécution de sanctions pénales et à la libre circulation de ces données. Elle a été adoptée par le Parlement et le Conseil le 14 avril 2016.
IV/ MONDIALISATION, INTERNET ET LES NOUVELLES OPPORTUNITES	
Votre droit a-t-il une réglementation spéciale des jeux en ligne ?	La loi relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne n° 2010-476 du 12 mai 2010 constitue une telle réglementation spéciale. Ce texte a créé l'ARJEL qui est une autorité administrative indépendante chargée de veiller à la protection des consommateurs et des populations vulnérables ; à la sécurité et la sincérité des opérations de jeux grâce à l'encadrement des paris et par la reconnaissance d'un droit d'exploitation profitant aux organisateurs d'événements

	sportifs ; aux équilibres économiques en luttant contre la fraude (les sites illégaux notamment) et le blanchiment d'argent ; et enfin à la fiscalité : prélèvement sur les mises redistribué, en partie, aux filières hippiques et sportives.
Votre droit a-t-il une réglementation spéciale du crowdfunding ? = financement participatif	Le droit français a été précurseur en ce domaine. L'ordonnance du 30 mai 2014 a permis de mettre en place un cadre règlementaire pour le Crowdfunding. Elle fixe le cadre juridique du financement participatif, entrée en vigueur pour l'essentiel le 1er octobre 2014, en distinguant les trois formes de crowdfunding, le financement par titre (l'équity crowdfunding), le financement par prêt (le crowdlending), et le financement par don (le crowdgiving). Ce texte a également créé des statuts pour les plateformes de crowdfunding, elles peuvent en effet revendiquer le statut d'intermédiaires en financement participatif (Crowdlending et sans dout quoique cela ne soit pas explicite crowdgiving) ou de conseillers en investissement participatif (Equity crowdfunding), statuts auxquels sont associés un certain nombre d'obligations notamment professionnelles, d'assurance, d'information.... De même, les textes prévoient un aménagement des règles classiques notamment à l'égard du monopole bancaire. Ce cadre, quoique largement perfectible en raison des nombreuses incertitudes persistantes, a le mérite de poser le premier cadre nécessaire au développement vertueux de cette nouvelle forme de financement.
Votre droit a-t-il plus généralement une réglementation de l'économie de partage que permet Internet ? Exemple Blablacar (covoiturage facilité par Internet)	Le Rapport P. Terrasse remis au Premier Ministre en février 2016 dresse un premier panorama de l'économie collaborative. Il élabore une série de 19 propositions qui ont vocation à permettre le développement de l'économie

	collaborative dans un cadre régulé. Parmi ces propositions, il est fait référence à la nécessité d'imposer aux plateformes une obligation de loyauté renforcée, obligation par ailleurs déjà présente dans le projet de loi pour une république numérique actuellement en cours d'adoption. La création d'un cadre juridique pour l'économie collaborative fait également partie des préoccupations de la Commission dans le cadre de sa stratégie numérique.
Votre droit a-t-il réagi à l'uberisation de l'économie permise par Internet? exemple du monopole des taxis mis à mal par une application permettant de partager un véhicule contre un prix entre particuliers (uberpop), ou de réserver les services d'un professionnel en passant par Internet, l'opérateur (uber) prenant des commissions sur chaque opération. Exemple des hôteliers qui supportent les charges des établissements ouverts au public et qui se voient concurrencés par des sites comme AirBnB qui permettent de louer un appartement ou une maison , sans que le loueur soit soumis aux mêmes exigences qu'un hôtel, etc…	Le Conseil constitutionnel a été saisi le 23 juin 2015 par la Cour de cassation d'une QPC, posée par les sociétés Uber France SAS et UberBV, relative à la conformité aux droits et libertés que la Constitution garantit des dispositions du premier alinéa de l'article L. 3124-13 du code des transports. Ce texte réprime de deux ans d'emprisonnement et de 300 000 € d'amende le fait d'organiser un système de mise en relation de clients avec des personnes qui, sans pouvoir légalement s'y livrer en application du code des transports, faute d'être, par exemple, taxis ou VTC, effectuent pourtant des prestations de transport routier de personnes à titre onéreux. Le Conseil constitutionnel a écarté l'ensemble des griefs soulevés par les sociétés requérantes et déclaré les dispositions contestées conformes à la Constitution. Il a en particulier jugé que les dispositions contestées n'ont ni pour objet ni pour effet d'interdire les systèmes de mise en relation des personnes souhaitant pratiquer le covoiturage tel qu'il est défini par le code des transports. Le Conseil constitutionnel a en conséquence écarté le grief tiré de l'atteinte au principe de légalité des délits et des peines. Cette décision a pour conséquence

	d'interdire le service Uberpop. Parallèlement, le projet de loi pour une république numérique, actuellement en discussion au Sénat prévoit un article 23 *ter* qui limite le recours à Airbnb de la part des locataires, en imposant à la plateforme de s'assurer du statut de propriétaire du loueur ou du fait qu'il dispose de l'autorisation de ce dernier.