MONDIALISTION ET INTERNET - PORTUGAL[1]

A/ Comment sont protégées dans votre droit les données personnelles ?[2]

Quelle est la définition des données à caractère personnel dans votre droit ? Existe-t-il une définition formelle ?

Les données à caractère personnel sont definis par la loi n. 67/98 du 26 octobre comme «toute information de tout type, quel que soit le support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable (personne concernée) », i.e., une qui peut être identifiée directement ou indirectement, notamment en se référant à un certain nombre d' identification ou à un ou plusieurs facteurs spécifiques comme physique, physiologique, mentale, économique, culturelle ou identité sociale» (Article 3, al. a). Cette définition correspond à celle prévue par l'article 2, al. a), de la Diretive 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, transposée au Portugal par la loi n. 67/98.

Pour l'interpretation de cette définition la Cour de justice de l'Union européenne a un rôle importante: voire par exemple les arrêts *Lindqvist* du 6 novembre 2003[3] e *Worten c ACT* du 30 mai 2013[4] ; voire aussi les documents de travail de l' «Article 29 Working Party»[5].

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 loi n. 67/98 ne consacre pas un droit de propriété sur les données. Il s'agit plutôt d'un droit à la protection de la vie privée concernant l'information des individus. Le code civil prévoit le droit à la protection de la personnalité (article 70) et des droits spéciaux de personnalité, comme le droit à l'image et le droit au respect the l'intimité de la vie privée

---

[1] Rapport national sur le thème « Mondialisation et Internet », rédigé par Mr Alexandre Dias Pereira, professeur auxiliaire de la Faculté de droit de l'université de Coimbra, après le rapport général de Madame le Professeur Martine BEHAR-TOUCHAIS, pour les Journées allemandes de l'Association Henri Capitant sur la « Mondialisation », qui se réalisent du 23 au 27 mai 2016 à Berlin.

[2] À partir du 25 mai 2018 Il s'applique le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[3] Affaire C-101/01, Bodil Lindqvist, ECLI:EU:C:2003:596: « L'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé »

[4] Affaire C-342/12, Worten c. Autoridade para as Condições de Trabalho (ACT), ECLI:EU:C:2013:355: « un registre du temps de travail, tel que celui en cause au principal, qui comporte l'indication pour chaque travailleur des heures de début et de fin du travail, ainsi que des interruptions ou des pauses correspondantes, relève de la notion de 'données à caractère personnel'»

[5] Le réglement n. 2016/679 porte une définition de données à caractère personnel, comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

(articles 70 e 80)[6], la protection des données à caractère personnel en étant assimilé.[7] La Cour suprême a utilisé la désignation, provenant de la doctrine allemande, de « droit fondammental à l'autodétermination informationelle »[8].
Nonobstant, la Constitution de la république portugaise autonomise la protection des données à caractère personnelle du droit à la vie privée, en prévoyant dans un article sur l'utilisation de l'informatique (article 35). Dans le même sens la Charte des droits fondamentaux de l'Union Européenne prévoit un article propre (l'article 8) pour garantir la protection juridique des données à caractère personnelle.
D'ailleurs, il est intéressant de remarquer que la loi n. 12/2005 du 26 janvier sur l'information génétique et personnelle de santé établi que cette information est propriété de la personne en concernant, y compris les données cliniques registrées, les résultats des analyses et des autres examens subsidiaires (article 3, para. 1).
En prévoyant l'information de santé comme objet d'une propriété la loi a ouvert une nouvelle branche des droits exclusifs sur des biens incorporels, en plus du droit d'auteur et des droits voisins et de la propriété industrielle. Mas on ne saurait pas dire s'il s'agit d'un nouveau droit de propriété intellectuelle.

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 ?
Non. Le traitement des données à caractère personnel peut être licite sans un accord de l'internaute dans les cas prévus par la loi n. 67/98 (article 6, en transposant article 7 de la directive 95/46), i.e., s'il est necessaire :
1 - à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mésures précontractuelles prises à la demande de celle-ci;
2 –au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
3- à la sauvegarde de l'intérêt vital de la personne concernée;
4 - 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 ou le tiers auquel les données sont communiquées, ou
5 - à la réalisation de l'intérêt legitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Y a-t-il des données plus sensibles que d'autres, qui sont soumises à un régime spécial (données de santé, religion, opinions politiques, …) ?
Oui, les « données sensibles », c'est à dire, des catégories particulières de données. Selon la Constitution, «l'ordinateur ne peut pas être utilisé pour le traitement des données concernant les croyances philosophiques ou politiques, le parti ou l'appartenance syndicale, les croyances religieuses, la vie privée ou l'origine ethnique, à moins que par

[6] CAMPOS, Diogo Leite de (1991). Lições de Direitos da Personalidade. Boletim da Faculdade de Direito da Universidade de Coimbra, vol. 57.
[7] PINTO, Paulo Mota (1993). O direito à reserva sobre a intimidade da vida privada. Boletim da Faculdade de Direito (Universidade de Coimbra), Vol. LXIX, 479-585.
[8] Arrêt du 16 octobre 2014, affaire 679/05.7TAEVR.E2.S1, Helena MONIZ – www.dgsi.pt

consentement exprès de titulaire, prévue par l'autorisation de la loi avec des garanties de non -discrimination ou de traitement données statistiques non identifiables individuellement» (article 35, para. 2).

En outre, la loi 67/98 interdit le traitement des données personnelles relatives aux croyances philosophiques ou politiques, parti ou à un syndicat, les croyances religieuses, la vie privée et l'origine raciale ou ethnique et le traitement des données relatives à la santé ou la vie sexuelle, y compris les données génétiques (article 7, para. 1; voire article 8 de la directive 95/46).

Toutefois, le traitement des «données sensibles» est licite si, en étant assurées les mésures adéquates:
1 - la personne concernée a donné son consentement explicite à un tel traitement (article 7, para. 2), ou

2 - le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée n'a pas la capacité physique ou juridique pour donner son consentement (article 7, para. 3, al. a);

3 - le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées (article 7, para. 3, al. b)

4 - le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d' un droit en justice (article 7, para. 3, al. c)

5 – le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, et est effectué par un praticien de la santé soumis au secret professionnel, ou par une autre personne également soumise à une obligation de secret equivalente; en plus, ce traitement doit être notifié à la Comission nationale de protection des données (article 7, para. 4).

En conformité avec l'article 7, para. 4, de la directive 95/46, la loi 67/98 prévoit en article 7, para. 2, que le traitement des données sensibles peut être autorisé par disposition légale ou par la Commission nationale de protection des données (CNPD) quand il est indispensable par des raisons d'intérêt public important pour l'exercice des compétences légales ou statutaires du responsable par le traitement.

Par exemple, le traitement des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté doit être autorisée par la CNPD, et doit être nécessaire à l'éxécution des finalités légitimes de son responsable (article 8, para. 2).
Le traitement nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, prévue par la directive (article 7, para. 2, al. b), est disciplinée dans Code du travail portugais (article 17), et se conforme avec la jurisprudence de la Cour de justice de l'Union européenne[9].

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 ?
Portugal fair partie de l' Union européenne. Le Conseil et le Parlement européen ont chargé la Commission de déterminer, sur la base de l'article 25, para. 6, de la directive 95/46/CE, quels sont les pays tiers qui assurent un niveau de protection adéquat en raison de sa législation interne ou des engagements internationaux qu'il a conclus.[10]
Le 6 octobre 2015[11], la Cour de justice de l'Union Européenne a jugé l'invalidité de la décision 2000/520/CE de la Commission du 26 juillet 2000 «EU-US Safe-Harbour».
Le 2 février 2016, la Commission européenne et les États-Unis ont convenu d'un nouveau cadre pour les transferts de données transatlantiques: l'UE-U.S. «Privacy Shield».[12]

Comment protège-t-on les personnes dans le cloud-computing (l'informatique en nuage) ?
Le «Cloud-computing» or l'informatique en nuage a été caracterisée comme « le stockage, le traitement et l'utilisation de données sur des ordinateurs situés à distance accessibles sur Internet. Cela signifie que les utilisateurs peuvent commander une puissance de calcul quasi illimité à la demande, sans faire d'importants investissements de capitaux pour répondre à leurs besoins, et qu' ils peuvent se rendre à leur données partout avec une connexion Internet ».[13]
La question de la protection des données personnelles dans le cloud computing a été abordée dans plusieurs documents officiels, notamment Article 29 Working Group sur le Cloud Computing (2012), et le Groupe international de Berlin de travail sur la protection des données dans les télécommunications, Document de travail sur le Cloud Computing

[9] Voire par exemple l'arrêt du 30 mai 2013 (affaire C-342/12, Worten c. Autoridade para as Condições de Trabalho (ACT), ECLI:EU:C:2013:355), dans lequel la Cour a décidé que la directive 95/46 n'interdit pas une réglementation nationale « qui impose à l'employeur l'obligation de mettre à la disposition de l'autorité nationale compétente en matière de surveillance des conditions de travail le registre du temps de travail afin d'en permettre la consultation immédiate, pour autant que cette obligation est nécessaire aux fins de l'exercice par cette autorité de ses missions de surveillance de l'application de la réglementation en matière de conditions de travail, notamment, en ce qui concerne le temps de travail. »
[10] Voire ici la liste des pays y compris (seulement en anglais) :
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[11] Affaire C-362/14, Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650.
[12] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[13] Unleashing the Potential of Cloud Computing in Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 529 final, Brussels, 27.9.2012.

- les questions de confidentialité et de protection des données - "Sopot Mémorandum" (2014).
Aucune exception is prévue pour le cloud computing, donc la legislation en vigueur, notamment la loi 67/98, doit être respectée.
Le règlement général sur la protection des données remplacera la directive 95/46 en modernisant la protection des données à caractère personnel pour l'environnement de la nuage et du «Big Data». Selon l'information du *Consilium*[14], le règlement prévoit comme droits de la personne concernée
«- la nécessité d'obtenir de la personne qu'elle indique clairement qu'elle consent au traitement des données à caractère personnel
- un accès plus facile de la personne concernée aux données à caractère personnel qui la concernent
- les droits à la rectification, à l'effacement des données et à l'oubli
- le droit de s'opposer notamment à l'utilisation des données à caractère personnel à des fins de profilage
- le droit à la portabilité des données d'un prestataire de services à un autre »
Le règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, y « compris l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques. » (considérant 18).

Comment protège-t-on les personnes dans le big data ?
Voire la réponse à la question anterieure.

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 ?
Un droit à l'oubli a été proposé comme manifestation du droit général de personnalité[15], mas il n'est pas prévu par la loi et aucun décision des tribunaux a été trouvée en affirmant.
La loi 67/98 établi le droit d'accès selon le quel toute personne concernée a le droit d'obtenir du responsable du traitement, notamment, selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à cette loi, notamment en raison du caractère incomplet ou inexact des données (article 11, para., al. d; correspond à l'article 12, al. b de la directive 95/46).
La jurisprudence de la Cour de justice de l'UE dans l'arrêt Google Spain[16] a consacré le droit à l'oubli en jugeant que

[14] http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/
[15] CARVALHO, Orlando de (1973). Les droits de l'Homme dans le Droit Civil Portugais. Boletim da Faculdade de Direito, vol. 49, 1-24.
[16] Arrêt du 13 mai 2014, affaire C-131/12, Google Spain SL e Google Inc c. Associação Espanhola de Dados Pessoais (AEPD) c. Mário Costeja Gonzalez. ECLI:EU:C:2014:317.

« l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite. » La Cour a ajouté en plus que « ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. »

Aucune forme de matérialisation de la mise en œuvre du droit à l'oubli a été trouvée dans la législation ni dans la jurisprudence ni dans la pratique de la Commission nationale de protection des données[17]. Toutefois, il y avait en mai 2015 plus de 2000 applications d'élimination de presque 9000 URLs, mais seulement peu plus que 25% avait été supprimés.[18]

Est-ce que votre législation prévoit un cadre spécifique pour le transfert des données à caractère personnel ?

Le transfert des données à caractère personnel est discipliné par la loi 67/98, en transposant la directive 95/46 (articles 25 e 26).

La circulation des donnés à caractère personnel est libre entre les États-membres de l'UE, sans préjudice des dispositions communautaires de nature fiscale ou des douanes (article 18).

Le transfert des données pour des pays tiers démande que ces pays assurent un niveau de protection adéquat, en considerant toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données, en particulier, la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées (article 19, paras. 1 et 2). La CNPD decide si un pays tiers assure un niveau de protection adéquat et, en cas de réponse negative, comunique celà à la Commission européenne (article 19, paras. 3 et 4). En tout cas le transfert des données pour un pays tiers dont la protection n'est pas adéquate selon la Commission européene est strictement interdit (article 19, para. 5)

Malgré le pays tiers n'a pas un niveau de protection adequat le transfert des données peut être authorisé par la CNPD si, selon l'article 20, para. 1, si:

1 - la personne concernée ait indubitablement donné son consentement au transfert envisagé, ou

2 - le transfert soit necessaire:

[17] Vide : www.cnpd.pt

[18] http://www.computerworld.com.pt/2015/05/13/um-ano-apos-o-direito-ao-esquecimento-no-google/ (4/5/16)

- à l'exécution d' un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concerne, ou
- à la conclusion ou à l'exécution d' un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers
- ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou
- à la sauvegarde de l'intérêt vital de la personne concernée, ou
- intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l' information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

D'ailleurs, le transfert pour pays tiers sans niveau de protection adéquat peut aussi être autorisé par la CNPD lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvant notamment résulter de clauses contractuelles appropriées (article 19, para. 3). La CNPD informe la Commission européenne et les autres États membres de ces autorisations (article 19/4). En outre, Na CNPD autorise le transfert des données qui respect les clauses contractuelles types ayant les garanties suffisantes selon la Commission européenne (article 19, para. 5).

Il faut rémarquer que la notion de transfert de données a été interpretée para la Cour de justice au sens de que « Il n'existe pas de «transfert vers un pays tiers de données» (…) lorsqu'une personne qui se trouve dans un État membre inscrit sur une page Internet, stockée auprès d'une personne physique ou morale qui héberge le site Internet sur lequel la page peut être consultée et qui est établie dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à Internet, y compris des personnes se trouvant dans des pays tiers. »[19]

Qui est compétent pour faire respecter ces règles ? Existe-t-il une autorité de régulation et de contrôle indépendante, et de quel pouvoir de sanction dispose-t-elle ?

Au niveau de l'Union européenne c'est compétent la Commission européenne. Au niveau national c'est compétent la CNPD (Commission nationale de protection des données), une autorité administrative indépendante qui fonctionne auprès du Parlement (article 20 de la loi 67/98). Cette Commission a le pouvoir notamment d'appliquer des amendes établies pour les infractions à la loi des données (article 41).

[19] Arrêt du 6 novembre 2003, dans l'affaire C-101/01, Bodil Lindqvist, ECLI:EU:C:2003:596

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

La Constitution consacre la liberté d'expression et d'information, selon laquelle « toute personne a le droit d'exprimer et de diffuser librement ses pensées par des mots, des images ou par tout autre moyen, ainsi que le droit d'informer, d'informer et d'être informé, sans entrave ni discrimination»; l'exercice de ces droits ne peut être empêchée ou restreinte par tout forme de censure (article 37, para. 1 et 2).
L'entité regulatrice des media (ERC) a rendu décisions contre sites de racism et xenophobie (le 27 june 2001), canibalism et d'autres violences gothiques (le 25 aout 2004) hebergé par un serviteur web établi au Portugal.[20]

Y a t-il à l'inverse des abus de la liberté d'expression qui ont été sanctionnés par vos juridictions ? Propos diffamatoires par exemple. Injures sur Internet.

Il y a plusières arrêts des tribunaux sur l'abus de la liberté e'expression. La jurisprudence de la Cour d'appel du Porto est particulièrement expressive. Dans l'arrêt du 5 juin 2015, affaire 101/13.5TAMCN.P1, la Cour a decidé que la publication en *Facebook* d'une photographie avec l'image du personne contra sa volonté est un acte incriminé par le Code pénal (article 199, para. 2). Dans un autre cas il s'agissait d'un texte ironique et critique publiée dans une la page personnelle au Facebook d'un homme politique qui exprimait des jugements. La Cour a estimé que l'agent n'attentait personnellement contre son adversaire politique et donc il n'y avait pas de diffamation. Selon la cour, il y a plus tolérance versée aux jugements de valeur que celui accordée à des imputations personnelles et ses limites sont plus larges quand il s'agit d'un homme politique agissant en sa qualité de personnage public, que lorsqu'on se réfère à un seul particulier[21].
En autre, la Cour a estimé que la colocation de messages dans la page du Facebook est une publication si elles sont à la disposition du public, et alors ne peuvent pas être considerées comme des communications privées (arrêt du 13 avril 2016, l'affaire 471/15.0T9AGD-A.P1). Toutefois, les messages avec « Messenger » sont estimées privées et donc des convictions basées sur telles preuves ont été annulées para la Cour (arrêts du 25 novembre 2015, affaire 848/13.6TAVRF.P1, et du 16 décembre 2015, affaire 886/14.1PBAVR.P1).
Parfois le licenciement de travailleurs est justifié à cause de messages qu'ils ont publiée dans ses page du Facebook et qui portent atteinte contre l'image et la réputation de

[20] http://www.erc.pt/pt/deliberacoes
[21] Arrêt de la Cour suprême du 16 novembre 2012, affaire 54/11.4TASVC.L1 – 3.

l'employer. Les travailleurs contestent en disant que les pages sont privées et donc ne peuvent pas être utilisées comme preuve. Toutefois, en général, les tribunaux ne sont pas d'accord, parce que les pages du Facebook ne sont pas normalement strictes aux amis intimes, mais par contre sont assez ouvertes aux amis des amis ou même publiques.
Dans l'arrêt du 29 septembre 2014, affaire 431/13.6TTFUN.L1-4, la Cour d'appel de Lisbonne a décidé que les publications en Facebook peuvent être utilisées comme preuve des actes illicites, en particulier quand l'agent appelle à partager la publication par ses amis

Quels moyens peuvent être mis en œuvre pour faire cesser ces atteintes ? Sont-ils efficaces ?
Ceux qui estiment d'être victimes d'un atteint peuvent démander l'ordinnance par la Cour d'une injonction selon le Códe de procédure civil (article 362). Il s'agit d'unne injonction non spécifiée dans le Code, comme par exemple, ordonner l'éffacement de la page ou le blocage d'accès à la publication. D'ailleurs, la victime peut demander les remèdes prévus dans le Code civil, comme le payment des dommages-intérêsts causés et bien aussi que l'agent ne poste plus le contenu diffamatoire ou injurieux sous peine d'une astreinte (articles 483, 829 e 829-A du Code civil).

C/ Autres droits

Comment est protégé le droit au respect de la vie privée sur Internet (en dehors de la question des données personnelles) ? Notamment sur les sites de journaux en ligne ?
La liberté de presse et des media est protégée par la Constitution (article 38), et la compétence pour régulation de la communication sociale est attribuée à une autorité administratif indépendante (article 39), en espèce la ERC.
Le balance entre la liberté de presse et le droit au respect de la vie privée fait objet d'abondante jurisprudence national[22] et international, en particulier la jurisprudence de la Cour européenne des droits de l'homme. Toutefois, contrairement à la CEDH[23], la jurisprudence interne concernant les atteintes contre la vie privé par les media n'est pas abondant.
Dans l'arrêt du 8 mai 2013, affaire 1755/08.0TVLSB.L1.S1, la Cour suprême a décidé que la révélation du domicile d'une personne avec projection publique dans un reportage publiée par un journal en ligne n'était pas justifié par le fin d'information et alors constituait un abuse de liberté de presse.
Le Code civile prévoit le droit au respect de la vie privée selon la nature du cas et la condition des personnes (article 80). Par analogie avec le droit à l'image, il est accepté de publier des informations sur la vie privée des personnes en fonction de leur notoriété ou

[22] Voire par exemple l'arrêt de la Suprême Cour de justice du 29 janvier 2015, affaire 24412/02.6TVLLSB.L1.S1
[23] Vide : http://echr.coe.int/Documents/Research_report_internet_FRA.pdf

profession, ou par des exigences de justice, finalités scientifiques, didactiques ou culturelles, ou quand l'image est dans places publiques ou des faits d'intérêt public ou des évènements publiques (article 79, para. 2). L'exercice de la liberté de presse par moyen des journaux en ligne doit respecter la vie privée en les mêmes conditions.

Quels sont les moyens pour faire cesser les atteintes ?

La loi du commerce électronique – décret-loi n. 7/2004 du 7 janvier prévoit un méchanisme de « *notice and take down* » (article 18). La personne qui s'estime lesée peut démander au fournisseur d'hébèrgement (ou des moteurs de recherche) le blocage d'accès aux contenus illicites. Si l'illicéité n'est pas manifeste, le fournisseur d'Internet n'a pas le devoir de bloquer l'accès. En ce cas, l'interessée peut demander à l'entité de supervision – en espèce, l'entité réglemantaire de la communication (ERC) -, laquelle doit produire une décision provisoire dans 48 heures et la communiquer par moyen électronique aux parties. Quand-même, si le fournisseur d'Internet décide le blocage d'accès, l'interessé en mantenir de contenu disponible peut appeller pour l'entité de supervision. Cette entitié peut à tout le temps modifier ses décisions sans y avoir aucune responsabilité. Le fournisseur d'Internet n'a pas aussi aucune responsabilité si l'illiceité n'est pas manifeste. La décision de entité de supervision fait objet d'appell judiciare et ce méchanisme de « *notice and take down* » ne préjudice pas l'utilisation au même temps des voies judiciaires communes. Parfois le contenu illicit se trouve dans les commentaires des lecteurs, voire par exemple la déliberation n. 19/CONT-I/2012 du 26 septembre 2012 de l'entité réglementaire de la communication.[24]

Les droits de propriété intellectuelle sont-ils fragilisés par Internet ?

Oui, les droits de propriété intellectuelle, y compris le droit d'auteur et les droits voisins et la propriété industrielle, en particulier les marques et d'autres signes distinctifs, sont fragilisés par Internet. Par exemple, la mise en circulation dans le web des œuvres protégées, l'utilisation des marques et des autres signes distinctifs comme noms de domaine ou mots clé.

Selon la directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle « Le développement de l'usage de l'Internet permet une distribution instantanée de produits pirates dans le monde entier » (considérant 9). La directive 2004/48 (*enforcement*) a été transposée par la loi n. 16/2008 du 1 avril, qui a modifié le code du droit d'auteur et le code de la propriété industrielle.

En autre, la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, considère que « Les services d'intermédiaires peuvent, en particulier dans un environnement numérique, être de plus en plus utilisés par des tiers pour porter atteinte à des droits. Dans de nombreux cas, ces intermédiaires sont les mieux à même de mettre fin à ces atteintes. Par conséquent, sans préjudice de toute autre sanction ou voie de recours dont ils peuvent se prévaloir, les titulaires de droits doivent avoir la possibilité de demander qu'une ordonnance sur requête soit rendue à l'encontre d'un

[24] Source : http://www.erc.pt/

intermédiaire qui transmet dans un réseau une contrefaçon commise par un tiers d'une œuvre protégée ou d'un autre objet protégé. »
En conformité, l'article 8, para. 3, de la directive 2001/29 dispose que « Les États membres veillent à ce que les titulaires de droits puissent demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin. »
La directive 2001/29 a été transposée par la loi n. 50/2004 du 24 aout qui modifie le Code du droit d'auteur et des droits voisins. En particulier, l'ordonnance est prévue dans l'article 227, para. 2, du Code.
La configuration de cette ordonnance (injonction) dans le droit interne des États membres a suscité des arrêts de la Cour de justice, notamment l'arrêt *Scarlet* du 24 novembre 2011[25] au quel la Cour n'a pas accepté des filtres préventifs par temps indéterminé et aux frais exclusif du fournisseur d'Internet. Plus récemment, dans l'arrêt *Telekabel* du 27 mars 2014[26], la Cour a décidé que « Les droits fondamentaux reconnus par le droit de l'Union doivent être interprétés en ce sens qu'ils ne s'opposent pas à ce qu'il soit fait interdiction, au moyen d'une injonction prononcée par un juge, à un fournisseur d'accès à Internet d'accorder à ses clients l'accès à un site Internet mettant en ligne des objets protégés sans l'accord des titulaires de droits, lorsque cette injonction ne précise pas quelles mesures ce fournisseur d'accès doit prendre et que ce dernier peut échapper aux astreintes visant à réprimer la violation de ladite injonction en prouvant qu'il a pris toutes les mesures raisonnables, à condition cependant que, d'une part, les mesures prises ne privent pas inutilement les utilisateurs d'Internet de la possibilité d'accéder de façon licite aux informations disponibles et, d'autre part, que ces mesures aient pour effet d'empêcher ou, au moins, de rendre difficilement réalisables les consultations non autorisées des objets protégés et de décourager sérieusement les utilisateurs d'Internet ayant recours aux services du destinataire de cette même injonction de consulter ces objets mis à leur disposition en violation du droit de propriété intellectuelle, ce qu'il appartient aux autorités et aux juridictions nationales de vérifier. »
D'abords, le rôle des fournisseurs d'Internet touche des autres droits de propriété intellectuelle, comme le droit des marques. L'interprétation de la loi interne en transposant des instruments de l'Union de fait normalement en conformité avec la jurisprudence de la Cour de justice. En particulier, l'arrêt *Google c Louis Vuitton* du 23 mars 2010[27] clarifie la responsabilité du prestataire d'un service de référencement sur

[25] Affaire C-70/10, Scarlet Extended c SABAM et al. ECLI:EU:C:2011:771: les dispositions concernées des directives 2000/31, 2001/29, 2004/48, 95/46 et 2002/58 «lues ensemble et interprétées au regard des exigences résultant de la protection des droits fondamentaux applicables, doivent être interprétées en ce sens qu'elles s'opposent à une injonction faite à un fournisseur d'accès à Internet de mettre en place un système de filtrage de toutes les communications électroniques transitant par ses services, notamment par l'emploi de logiciels «peer-to-peer» (a), qui s'applique indistinctement à l'égard de toute sa clientèle (b), à titre préventif (c), à ses frais exclusifs (d), et sans limitation dans le temps (e), capable d'identifier sur le réseau de ce fournisseur la circulation de fichiers électroniques contenant une œuvre (…), en vue de bloquer le transfert de fichiers dont l'échange porte atteinte au droit d'auteur. » La Cour a confirmé cette jurisprudence dans l'arrêt du 16 februar 2012, Affaire C-360/10, SABAM c. Netlog NV. ECLI:EU:C:2012:85.
[26] Affaire C-314/12, UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft GmbH. ECLI:EU:C:2014:192.
[27] Affaires jointes C-236/08 à C-238/08, Google c. Louis Vuitton et al., ECLI:EU:C:2010:159.

Internet vis-à-vis l'utilisation des marques comme mot clé – question laissée ouverte par la directive du commerce électronique - en décidant que « Le prestataire d'un service de référencement sur Internet qui stocke en tant que mot clé un signe identique à une marque et organise l'affichage d'annonces à partir de celui-ci, ne fait pas un usage de ce signe ». Le prestataire d'un service de référencement sur Internet en est comme le fournisseur d'hébergement parce que s'il «n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées (…), ledit prestataire ne peut être tenu responsable pour les données qu'il a stockées à la demande d'un annonceur à moins que, ayant pris connaissance du caractère illicite de ces données ou d'activités de cet annonceur, il n'ait pas promptement retiré ou rendu inaccessibles lesdites données. »
À propôs de la protection des marques vis-à-vis les enregistrements spéculatifs et abusifs, de 'mauvaise foi', des domaines .eu, disciplinés par le Règlement (CE) n° 874/2004, la Cour a decidé dans l'arrêt du 3 juin 2010[28] que la « juridiction nationale est tenue de prendre en considération tous les facteurs pertinents propres au cas d'espèce, et notamment les conditions dans lesquelles l'enregistrement de la marque a été obtenu et celles dans lesquelles le nom de domaine de premier niveau .eu a été enregistré » et, en s'agissant des conditions d'enregistrement du nom de domaine, notamment, « le fait d'avoir introduit un grand nombre de demandes d'enregistrement de noms de domaine correspondant à des dénominations génériques. »
Au Portugal le règlement des noms de domaine .pt incorpore les recommandations de l'OMPI contre l'enregistrement abusif des marques comme noms domaine. En particulier, le règlement prévoit que la mauvaise-foi peut être prouvée par le fait que le nom de domaine a été enregistré ou acquis en vue de leur cession ultérieure à la requérante ou dans le but principal de perturber les activités professionnelles du demandeur ou l'utilisation intentionnelle du nom de domaine pour attirer les utilisateurs d'Internet (nom de domaine parking). En outre, la Cour suprême a décidé que l'enregistrement peut porter atteinte aux droit des marques même s'il est en conformité avec le règlement de noms de domaine .pt.[29]

D/ Aspects de droit international privé

Quel est dans votre droit le tribunal compétent en matière de cyber-délits ?

Les règles de compétence judiciaire en matière de cyber-délits privés sont établies dans le Code de procédure civile[30] (articles 59 et suivants) e dans certains instruments internationaux et européens, notamment le règlement (UE) n. 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Brussels refonte).

[28] Affaire C-569/08, Internetportal c. Richard Schlicht, ECLI:EU:C:2010:311.
[29] Arrêt du 29 janvier 2015, affaire 1222/06.6TYLSB.L1.S1, Silva GONÇALVES.
[30] Loi n. 41/2013 du 26 juin.

Dans les matières couvertes par le règlement, la règle générale c'est le *forum domicilii*, c'a veut dire, « les personnes domiciliées sur le territoire d'un État membre sont attraites, quelle que soit leur nationalité, devant les juridictions de cet État membre » (article 4, para. 1).
Toutefois, pour les matières contractuelles, délictuelles et d'autres, le règlement Brussels prévoit des compétences spéciales. Les cyber-délits ne sont pas une catégorie autonome. Les cyber-délits concernent les violations par l'internet des droits absolus, comme les droits de personnalité ou les droits de propriété intellectuelle, et bien aussi les infractions par l'internet aux intérêts protégés par la loi. Donc, selon l'article 7, para. 2 du règlement Brussels, le tribunal compétent en matière délictuelle ou quasi délictuelle, est celui du lieu où le fait dommageable s'est produit ou risque de se produire (*forum delicti commissi*).

Est-ce le même pour tous les cyber-délits ?
Non. La jurisprudence de la Cour de justice de l'Union européenne en fait la distinction entre action en responsabilité au tire de l'intégralité du dommage causé (1) et action devant les juridictions de chaque État membre sur le territoire duquel un contenu mis en ligne est accessible ou l'a été (2). [31]
Dans le premier cas, la personne qui s'estime lésée peut choisir le tribunal de l'État membre du lieu d'établissement de l'émetteur de ces contenus ou le tribunal de l'État membre dans lequel se trouve le centre de ses intérêts. Dans la deuxième situation, le tribunal compétent c'est celui de chaque État membre sur le territoire duquel un contenu mis en ligne est accessible ou l'a été, mais seulement pour connaître du seul dommage causé sur le territoire de l'État membre de la juridiction saisie.
Cette jurisprudence concerne des atteintes aux droits de personnalité, mais elle serait aussi valide pour des atteintes à d'autres droits absolus, comme le droit d'auteur et les droits voisions ou le droit des marques. Toutefois, la jurisprudence de la Cour de justice de l'Union européenne semple assez restrictive à admettre un super-forum en matière des droits patrimoniaux à cause du principe de territorialité de ces droits. Selon l'arrêt de la Cour 3 octobre 2013[32], « en cas d'atteinte alléguée aux droits patrimoniaux d'auteur garantis par l'État membre de la juridiction saisie, celle-ci est compétente pour connaître d'une action en responsabilité introduite par l'auteur d'une œuvre à l'encontre d'une société établie dans un autre État membre et ayant, dans celui-ci, reproduit ladite œuvre sur un support matériel qui est ensuite vendu par des sociétés établies dans un troisième État membre, par l'intermédiaire d'un site Internet accessible également dans le ressort

[31] Arrêt du 25 octobre 2011, affaires jointes C-509/09 et C-161/10, eDate Advertising, ECLI:EU:C:2011:685: «en cas d'atteinte alléguée aux droits de la personnalité au moyen de contenus mis en ligne sur un site Internet, la personne qui s'estime lésée a la faculté de saisir d'une action en responsabilité, au titre de l'intégralité du dommage causé, soit les juridictions de l'État membre du lieu d'établissement de l'émetteur de ces contenus, soit les juridictions de l'État membre dans lequel se trouve le centre de ses intérêts. Cette personne peut également, en lieu et place d'une action en responsabilité au titre de l'intégralité du dommage causé, introduire son action devant les juridictions de chaque État membre sur le territoire duquel un contenu mis en ligne est accessible ou l'a été. Celles-ci sont compétentes pour connaître du seul dommage causé sur le territoire de l'État membre de la juridiction saisie. »
[32] Affaire C-170/12, Peter Pinckney c. KDG Mediatech AG. ECLI:EU:C:2013:635.

de la juridiction saisie. Cette juridiction n'est compétente que pour connaître du seul dommage causé sur le territoire de l'État membre dont elle relève. » D'ailleurs, la Cour a décidé dans l'arrêt du 22 janvier 2015[33] que « en cas d'atteinte alléguée aux droits d'auteur et aux droits voisins du droit d'auteur garantis par l'État membre de la juridiction saisie, celle-ci est compétente, au titre du lieu de la matérialisation du dommage, pour connaître d'une action en responsabilité pour l'atteinte à ces droits du fait de la mise en ligne de photographies protégées sur un site Internet accessible dans son ressort. Cette juridiction n'est compétente que pour connaître du seul dommage causé sur le territoire de l'État membre dont elle relève. »

Quel est dans votre droit la loi applicable à l'indemnisation de la victime d'un cyber-délit ?

Le Code civile contient des dispositions sur la loi applicable (articles 25 et suivants), y compris un article sur la responsabilité extracontractuelle. D'ailleurs, cette matière est disciplinée par le règlement (CE) n. 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (« Rome II »), qui a précédence sur les règles du code civile.

Le principe générale du règlement Rome II c'est la *lex loci damni*: «la loi applicable à une obligation non contractuelle résultant d'un fait dommageable est celle du pays où le dommage survient, quel que soit le pays où le fait générateur du dommage se produit et quels que soient le ou les pays dans lesquels des conséquences indirectes de ce fait surviennent » (article 4, para. 2). Le considérant 18 du règlement explique que cette règle générale s'applique « indépendamment du ou des pays où pourraient survenir des conséquences indirectes. Ainsi, en cas de blessures physiques causées à une personne ou de dommages aux biens, le pays où les blessures ont été subies ou les biens endommagés devrait être entendu comme celui où le dommage survient. »

Ce principe générale connait une exception : si les parties ont leur résidence habituelle dans le même pays au moment de la survenance du dommage, la loi de ce pays s'applique (article 4, para. 2). En chaque cas, toutefois, s'il résulte de l'ensemble des circonstances que le fait dommageable présente des liens manifestement plus étroits avec un autre pays, la loi de cet autre pays s'applique (article 4, para. 3) en dérogation de la *lex loci damni* ou de la *lex* du pays de résidence commun des parties.

Est-ce la même pour tous les cyber-délits ?

Non.

Premier, le règlement Rome II exclu de son champ d'application « les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité, y compris la diffamation » (article 1, para. 2, al. g). Donc ces cas sont disciplinés par la respective disposition du Code civil (article 45): il s'applique la loi où l'activité principale a eu lieu causant des blessures (*lex loci delicti commissi*) ; si cette loi ne rend pas responsable l'agent mais la loi de l'Etat où elle a produit les blessures le fait, cette loi

[33] Affaire C-441/13, Pez Hejduk c. EnergieAgentur.NRW GmbH. ECLI:EU:C:2015:28.

s'applique à condition que l'agent doit prévoir la production de dommages dans ce pays en raison de son acte ou son omission.[34]

D'ailleurs, le règlement contient des dispositions spéciales pour la loi applicable aux délits en matière de responsabilité du fait des produits (article 5), concurrence déloyale et actes restreignant la libre concurrence (article 6), et bien aussi aux atteintes à l'environnement (article 7) et aux droits de propriété intellectuelle (article 8).

Concernant les cyber-délits en matière des droits de propriété intellectuelle, le règlement 'préserve' impérativement (article 8, para. 3) le principe *lex loci protectionis*, importé de la Convention de Berne sur la protection de la propriété littéraire et artistique.[35] Le considérant 28 affirme que ce principe est « universellement reconnu » et que « l'expression 'droits de propriété intellectuelle' est utilisée en sens très large », en « visant notamment le droit d'auteur, les droits voisins, le droit sui generis pour la protection des bases de données ainsi que les droits de propriété industrielle.»

Alors, selon l'article 8, para. 1 e 2 : la loi applicable est celle du pays pour lequel la protection est revendiquée (article 8, para. 1) ou, en s'agissant d'un droit de propriété intellectuelle communautaire à caractère unitaire, la loi applicable à toute question qui n'est pas régie par l'instrument communautaire pertinent est la loi du pays dans lequel il a été porté atteinte à ce droit.

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 décisions sur ce point ?

Pas encore. Si la proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique[36] est adoptée les contrats d'utilisation des services et applications d'Internet, comme ceux de Google ou Facebook, ne seront plus des contrats gratuits puisque l'utilisation de ces services ou applications é autorisée en exchange de données. Ça veut dire, les données sont considérées comme équivalent à l'argent. Selon l'exposé des motifs de la proposition « elle ne couvre pas

[34] Paragraphe 3 de l'article 45 du Code civile prévoit encore une troisième situation : si l'agent et la victime sont de la même nationalité ou, en son absence, la même résidence d'habitude, et se rencontrent dans un pays étranger, la loi applicable est celle de la nationalité ou de la résidence commune, sous réserve des dispositions de l'Etat local applicables indistinctement à toutes les personnes.

[35] Article 5, para. 2, 2ème per.: "l'étendue de la protection ainsi que les moyens de recours garantis à l'auteur pour sauvegarder ses droits se règlent exclusivement d'après la législation du pays où la protection est réclamée ».

[36] COM(2015) 634 final, Bruxelles, le 9.12.2015.

uniquement le contenu numérique fourni contre paiement, mais aussi le contenu fourni en échange de données (à caractère personnel et autre) transmises par le consommateur » (p. 13).

Les géants jouent avec les différents systèmes juridiques pour optimiser au mieux leur situation :
-d'abord leur <u>situation juridique</u> : clause attributive de juridiction, clause de loi applicable
-ensuite leur <u>situation fiscale</u>, 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 ?
En ce qu'il concerne la situation juridique (clause attributive de juridiction, clause de loi applicable), le Code civile prévoit la prohibition de fraude de la loi au sens de que l'application les règles de conflit ne doit pas éviter l'applicabilité de la loi qui, dans d'autres circonstances, aurait compétence (article 20). Le Code civile prévoit aussi la clause générale d'ordre public, selon laquelle « les dispositions de la loi étrangère indiquée par la règle de conflit ne sont pas applicables lorsque leur application viole les principes fondamentaux de la politique publique internationale de l'État portugais » (article 21).
En outre, les règlements ont des dispositions qui limitent la liberté contractuelle concernant des clauses attribution de juridiction (Brussels, articles 15, 19, 23, 25) et clauses de loi applicable (Rome II, articles 6, para. 4, 8, para 3, 14, para 2). Le règlement Rome II sauvegarde que ses dispositions « ne portent pas atteinte à l'application des dispositions de la loi du for qui régissent impérativement la situation, quelle que soit la loi applicable à l'obligation non contractuelle » (article 16).

En matière fiscale, le régime général des infractions tributaires – loi n. 15/2001 du 5 juin – incrimine la fraude fiscale (articles 103 et 104). Il semble toutefois qu'il faut une action de l'Union européenne pour combattre la piraterie fiscale au cœur de l'Union elle-même.

Les géants de l'Internet se rendent parfois coupables d'abus de position dominante ?
Dans l'arrêt Microsoft[37] le géant nord-américain a été rendu coupable d'abus de position dominante en se refusant de licencier le code-source de son système Windows à des concurrents dans le marché des systèmes opératifs pour serveurs qui voulaient développer des programmes compatibles avec le Windows.
Récemment, selon le communiqué de presse de la Commission européenne, du 20 avril 2016, « La Commission européenne a informé Google de sa conclusion préliminaire selon

[37] Arrêt du Tribunal de première instance du 17 septembre 2007, Microsoft Corp. contre Commission des Communautés européennes, affaire T-201/04. ECLI:EU:T:2007:289.

laquelle la société a, en violation des règles de concurrence de l'UE, abusé de sa position dominante en imposant des restrictions aux fabricants d'appareils Android et aux opérateurs de réseaux mobiles. »[38]

Y a-t-il eu dans votre pays des affaires concernant de tels abus ?
Il y a une conviction par abus de position dominante concernant la refuse par une grande entreprise de télécommunications de fournir accès à ses pipelines pour les concurrents dans le secteur de tv par câble et services associés. Toutefois, l'entreprise a été acquittée par la Cour d'appel.[39]

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 ?
La loi de la concurrence – loi n. 19/2012 du 8 mai – interdit les accords et les pratiques concertées entre entreprises, et bien aussi les décisions d'associations d'entreprises, qui sont susceptibles d'affecter la concurrence dans le marché national, et notamment ceux qui consistent à subordonner la conclusion de contrats à l'acceptation, par les partenaires, de prestations supplémentaires qui, par leur nature ou selon les usages commerciaux, n'ont pas de lien avec l'objet de ces contrats (article 9, para 1, al. e). Toutefois, les accords sont acceptés si les entreprises font preuve qu'ils remplissent les conditions du bilan économique et, en particulier, si les accords s'encadrent dans un règlement d'exemption adopté par la Commission européenne (article 10). Le *tying* ou *bundling* est aussi prévu comme un exemple de possible abus de position dominante, interdite par la loi de la concurrence (article 11, para 1 et 2, al. e). Cettes dispositions sont basées sur les dispositions du droit de l'Union européenne (maintenant articles 101 et 102 du TFUE).

En outre, le règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établisse des mesures relatives à l'accès à un internet ouvert et modifie la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union. En particulier le règlement 2015/2120 établie pour les utilisateurs finals « le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet. » Alors, le fournisseur d'accès ne peut pas fermer les utilisateurs dans son écosystème. Ils doivent en plus traiter « tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés », sans préjudice

[38] http://europa.eu/rapid/press-release_IP-16-1492_fr.htm
[39] http://www.concorrencia.pt/vPT/Praticas_Proibidas/Decisoes_da_AdC/Paginas/lista.aspx

de mettre en œuvre des mesures raisonnables de gestion du trafic dans les conditions prévues par le règlement (article 3, para 3).

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…)

Pour utiliser les services des géants de l'Internet il faut toujours accepter des conditions d'utilisation par moyen de cliquer : « Oui, je comprends et j'accepte ». Ces licences clique-wrap ne sont pas toutefois libres de vices.

Pour commencer, elles sont des conditions générales, écrites sans négociation individuelle préalable et proposées a des bénéficiaires indéterminées. En tant que tel, font objet du décret-loi n. 446/85 du 25 octobre. Inspiré sur la loi allemande (AGB), le régime a été modifié pour transposer la Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.

En essence, il consiste à contrôler la formation e le contenu des conditions générale. En premier, les conditions doivent être communiquées préalablement à son destinataire, qui a aussi le droit à recevoir réponse complète à tous ses questions raisonnables. Autrefois les clauses sont exclues du contrat autant que « clauses – surprise » (articles 5, 6 et 8). D'autre part, le contenu des clauses doit être conforme aux listes noires et grises de clauses absolument ou relativement interdites dans les contrats entre entrepreneurs ou entités similaires (B2B) ou dans les contrats avec les consommateurs (B2C). Par exemple, les clauses qui limitent ou excluent, directement ou indirectement, la responsabilité pour les dommages causés à la vie, physique ou l'intégrité morale ou la santé sont absolument interdites (art. 18, al a). D'ailleurs, les clauses qui font des fictions d'acceptation sont relativement interdites, et on peut se demander s'il n'est pas le cas des licences clique-wrap. En autre, la loi du commerce électronique – décret-loi n. 7/2004 du 7 janvier - interdit les conditions générales du contrat qui imposent la conclusion par voie électronique des contrats avec des consommateurs (article 25 para. 4).

La directive 2005/29/ce du Parlement européen et du Conseil du 11 mai 2005, relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur, a été transposée par le décret-loi n. 57/2008 du 26 march, dont l'article 12, al. c) prévoit comme absolument agressive se livrer à des sollicitations répétées et non souhaitées notamment par courrier électronique ou tout autre outil de communication à distance, sauf si et dans la mesure où la législation nationale l'autorise pour assurer l'exécution d'une obligation contractuelle. La gratuité des sollicitations n'empêche pas la nature commerciale des pratiques.

III/ MONDIALISATION, INTERNET ET LES DIFFICULTES DE LA REPRESSION DES PRATIQUES ILLICITES

Comment votre droit lutte-t-il contre la pédopornographie sur Internet ?

Le Code pénal incrimine l'abus sexuel, la prostitution et la pornographie des mineurs (articles 171-176). L'acte de séduire mineurs par moyen des technologies d'information et de communication pour des rendez-vous sexuelles ou pour la pornographie est aussi incriminé (article 176-A). D'ailleurs, la consommation intentionnelle de pédopornographie est incriminée et la pénalisation de l'exploitation de la pédopornographie avec des fins lucratives est aggravée (article 178, paras. 5-7).
Le Code pénal a été modifié par la loi n. 103/2015 du 24 aout a fin de transposer la Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil.

Comment votre droit lutte-t-il contre les propos racistes, haineux sur Internet ?
Le Code pénal prévoit comme un délit criminel l'organisation ou le financement de participation en des activités de propagande avec des propos racistes, religieux, haineux ou sexuelles (article 240, para 1). En dehors des activités organisées il est aussi incriminé la divulgation par les media ou système informatique des messages avec propos discriminatoires qui causent actes violence, menacent ou atteinte contre des autres à cause de leur race, religion, nationalité, ethnie ou orientation sexuelle (article 240, para 2).

Le droit pénal de votre pays est-il efficace pour lutter contre de telles infractions ?
Les réseaux de pédopornographie en Internet ne sont pas confinés aux frontières nationaux et donc la lutte contre de telles infractions n'est toujours la plus efficace. Toutefois il y a plusieurs arrêts des tribunaux portugais.[40]
Récemment, le 29 mars 2016, un homme a été arrêté en flagrant délit, à sa résidence à Lisbonne, à cause de la forte suspicion de la pratique sur 1262 crimes de pédopornographie. Selon les éléments de preuve recueillis, l'accusé avait gardé et téléchargé des images illégales contenant l'abus sexuel des enfants de moins de quatorze ans, et ces fichiers étaient partagés contenant des images d'enfants à des actes sexuels avec des adultes.[41]

Votre pays met-il en avant la soft law, l'autorégulation pour lutter contre de telles infractions ?
La soft law ou l'autorégulation est faite par les agents de l'Internet avec ses conditions d'utilisation et règles (par exemple, la netiquette de Youtube). Elle existe et est respectée, autant qu'elle ne porte pas atteinte contre la « hard law » (par exemple, des conditions d'utilisation excessivement restrictives en matière de liberté d'expression).

---

[40] Plus récemment voire les arrêts de la Cour suprême de justice du 12 juin 2013, affaire 1291/10.4JDLSB.S1, du 12 novembre 2014, affaire 1287/08.6JDLSB.L1.S1, du 22 avril 2015, affaire 45/13.0JASTB.L1.S1, et du 23 septembre 2015, affaire 524/13.0JDLSB.E1.S1 – source: www.dgsi.pt
Voire aussi par exemple l'arrêt de la Cour d'appel de Coimbra du 11 novembre 2015, affaire 372/12, dans lequel la Cour a estimé que ne fait pas partie du concept normatif de détention, aux fins du paragraphe 4 de l'article 176 du Code pénal (version avant la loi n ° 103/2015, de 24-08), l' accès de l'agent à un site de pédopornographie, avec une expansion ultérieure et l'affichage des photographies des mineurs en actes sexuelles.
[41] Source : http://www.pgdlisboa.pt/novidades/nov_main.php?comarcas=S

Existe-t-il des lois d'exception permettant de requérir le transfert des données par les acteurs d'internet aux autorités nationales ?

La loi du cyber-crime - loi n. 109/2009 du 15 septembre[42] - prévoit des dispositions processuels qui s'appliquent aux cyber-crimes mais aussi à des crimes commis par moyen d'un système informatique ou pour lesquels il faut obtenir des preuves en support électronique.

Ces dispositions processuelles comprennent la conservation rapide de données, notamment par le fournisseur des services de l'Internet (article 12) et la divulgation rapide de données de trafic (article 13). Pendant le procès, les cours peuvent aussi ordonner une injonction pour la présentation ou l'accès aux données (article 14), la recherche (article 15) et la saisie de données informatiques (article 16) ou, selon les dispositions du code de procédure pénale, la saisie de l'e -mail et des dossiers de communication similaires (article 17). L'interception des communications (article 18) et les « actions secrètes » (article 19) sont aussi prévues dans la loi du cyber-crime pour certains types de crimes.

La loi n. 41/2004 du 18 aout[43] protège la vie privée dans les communications électroniques, en particulier les données relatives au trafic et les données de localisation. Elle sauvegarde que le régime des données relatives au trafic ne préjudice pas les dispositions processuelles de prévention et combattre la criminalité.

IV/ MONDIALISATION, INTERNET ET LES NOUVELLES OPPORTUNITÉS

Votre droit a-t-il une réglementation spéciale des jeux en ligne ?

Oui, c'est le décret-loi n. 66/2015 du 29 avril.

L'État se réserve de droit de l'exploitation des jeux en ligne (article 8) et le concède par licence administrative à des personnes morales privées, sous la forme de société anonyme ou équivalente, établie dans un État-membre de l'Union européenne ou d'un État signataire de l'accord sur l'espace économique européen qui est lié à la coopération administrative dans le domaine la fraude fiscale et la lutte contre le blanchiment d'argent le capital, à condition d'avoir succursale au Portugal (article 9, para. 1). Le fonctionnement des jeux et paris en ligne ne peut être attribués qu'à des personnes morales dont l'objet est, pendant toute la durée de l'exploration de licence, des jeux et des paris (article 9, para. 2).

Le principe du pays d'origine de la directive sur le commerce électronique ne s'applique pas en ce secteur[44]. L'exploitation des jeux en ligne pour les opérateurs reconnus par les

---

[42] Cette loi transpose la décision-cadre du Conseil 2005/222 / JAI du Conseil du 24 février, sur les attaques contre les systèmes d'information, et adapte le droit national à la Convention sur la cybercriminalité du Conseil de l'Europe.

[43] Transpose en droit national la directive 2002/58 / CE du Parlement européen et du Conseil du 12 Juillet, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[44] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), article 1, para. 5.

autres États-membres de l'Union dépend de l'octroi d'une licence par l'entité le contrôle, l'inspection et la réglementation et ne sont pas valides au Portugal les licences ou d'autres titres habilitants octroyées par d'autres Etats (article 9, para. 3).

Votre droit a-t-il une réglementation spéciale du crowdfunding ?
= financement participatif
Oui, c'est la loi n. 102/2015 du 24 aout (régime juridique du financement du crowdfunding). L'ordonnance n. 344/2015 du 12 octobre établit des règles pour le préavis de mise en activité des plates-formes de crowdfunding dans les modalités de don et / ou de récompense dédiée prévus dans la loi 102/2015.

Votre droit a-t-il plus généralement une réglementation de l'économie de partage que permet Internet ? Exemple Blablacar (covoiturage facilité par Internet)
Non, l'économie de partage permise par l'Internet est connue et discutée mais il n'y a pas de loi spécifique pour la réguler.

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…
Non, la « ubérisation » de l'économie est discutée, en particulier concernant les taxis. Récemment il y a eu une grande manifestation des taxis contre l'Uber, mais aucune loi ou décret-loi a été passé pour accommoder cette nouvelle économie.