Rapport relatif au thème n. 4

Mondialisation et Internet

1/Mondialisation, Internet et les droits des individus

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

1. *Quelle est la définition de donnée à caractère personnelle dans votre droit ? Existe-t-il une définition formelle ?*

Oui, il existe une définition formelle donnée par la loi italienne (D.lgs. n. 196/2003 *Code en matière de protection des données personnelles*). Il y, d'ailleurs, plusieurs définitions juridiques de données relatives à chaque type de typologie de donnée ainsi qu'au dégrée de protection que la loi veut leur assurer. La loi fait une distinction entre les suivantes catégories de données : données personnelles ; données identificatrices ; données judiciaires ; données sensibles (voir plus bas pour la définition des données sensibles). Les données personnelles sont définies de la façon suivante à l'article 4, alinéa 1, lettre b, D.lgs. n. 196/2003) : « Donnée personnelle : toute information concernant une personne physique identifiée ou identifiable, même indirectement, par référence à toute autre information, y compris un numéro d'identification personnel ».

2. *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 ?*

Il n'y a pas un véritable droit de propriété sur les données. Il s'agit plutôt d'un complexe régime juridique qui assure la protection de la vie privée ainsi que la protection des données personnelles. Nous pouvons distinguer deux formes de protection (Pagallo 2014), selon cette répartition : d'une part, la protection de la vie privée qui veut protéger « l'opacité » des données personnelles, à savoir le droit de l'individu d'empêcher l'accès à la connaissance et au partage de certaines données. D'autre part, la protection des données personnelles vise à protéger la « transparence » des données personnelles, à savoir le droit de l'individu à connaitre « les quelles, comment, pendant quel temps et par quel sujet » ses données sont utilisés, conformément au principe d'autodétermination de l'identité informationnelle (tel qu'il a été élaborée par la Cour constitutionnelle allemande).

En général, il y a aujourd'hui une tendance répandue, notamment au niveau européen, de création de formes de contrôle toujours plus intenses sur les données personnelles. Si, traditionnellement, le droit de propriété était le moyen pour assurer aux individus un pouvoir de contrôle sur les choses, maintenant, dans le cadre actuel du régime de la protection des données, les normes juridiques, qui garantissent le pouvoir de contrôle sur les données personnelles, peuvent être interprétées soit comme visant à renforcer les droits personnels (en dehors de la logique commerciale du « data market »), soit comme une sorte de « ersatz » du droit de propriété sur les données personnelles (suivant la logique commerciale du « data market »).

3. *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 ?*

En règle générale, il faut l'accord de la partie intéressée pour recueillir et pour utiliser ses données personnelles. L'art. 23, D.lgs. n. 196/2003, prévoit que le traitement des données personnelles par des parties privées ou publiques est admis uniquement avec le consentement exprès de la partie intéressée ; que le consentement peut porter sur l'ensemble du traitement des données ou sur une ou plusieurs opérations du traitement même ; et, enfin, que le consentement est valable que si il est donné librement et en référence spécifique à un traitement de données clairement identifié, si il est prouvé par écrit, et si la

partie intéressée a reçu les informations visées à l'article 13 du D.lgs. n. 196/2003. Toutefois, il y a des cas où le consentement de la partie intéressée n'est pas nécessaire pour le traitement de ses données personnelles : il s'agit des hypothèses expressément prévues et réglées par l'art. 24, D.lgs. n. 196/2003 (parmi les quelles, si le traitement est nécessaire pour obtempérer à une obligation juridique ou dérivante d'un contrat ; s'il concerne des données personnelles déjà publiques ou accessibles publiquement ; s'il est nécessaire pour la protection de la vie ou de l'intégrité physique des tiers ; s'il concerne des données personnelles qui sont relatives à l'activité économique ; etc.).

4. *Y a-t-il des données plus sensibles que d'autres qui sont donc soumises à un régime spécial (données de santé, religion, opinions politiques, …) ?*

La loi italienne prévoit l'existence de données sensibles, qui sont soumis à un régime renforcé de protection. Ces données sont ainsi définies par l'art. 4, comma 1, lettre d, D.lgs. n. 196/2003 : «Les données sensibles : les données personnelles qui révèlent l'origine raciale ou ethnique, les convictions religieuses, philosophiques ou autres, les opinions politiques, l'appartenance à des partis, syndicats, associations ou organisations à caractère religieux, philosophique, politique ou d'un syndicat, ainsi que les données personnelles qui concernent la santé et le sexe ». Cette liste doit être considérée comme une liste close, dans le sens qu'il est interdit de procéder par analogie, même si d' autres catégories des données (relatives, par exemple, à l'éducation scolaire, à la formation et à l'expérience de travail, à la solvabilité du débiteur, aux revenus perçus etc.) sont reconnues et protégées par le *Code de la privacy*. En ce qui concerne le traitement des données sensibles par des parties privées, le *Code de la privacy* prévoit qu'elles peuvent être traitées « seulement avec le consentement écrit de la partie intéressée et avec l'approbation du Garant » (art. 26, comma 1, D.lgs. n. 196/2003). La loi exige donc la forme écrite du consentement pour la validité de l'accord lui-même (art. 23, comma 4, D.lgs. n. 196/2003). En ce qui concerne le traitement des données sensibles par des entités publiques, le *Code* prévoit que le traitement des données sensibles est consenti « seulement si expressément autorisé par une disposition de la loi où sont spécifiés les types de données qui peuvent être traitées, les opérations exécutables ainsi que les finalités d'intérêt public poursuivies » (art. 20, comma 1, D.lgs. n. 196/2003).

5. *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 ?*

L'Italie est partie de l'Union européen : ses règlements, ses directives ainsi que les traités entre l'Europe et les autres pays sont progressivement appliqués et transposés dans le système juridique italien. Je ne suis pas sur (comme observé auparavant) que la protection des données personnelles et la constitution d'un « digital data market » peuvent toujours être interprétées uniquement par la dichotomie protection des personnes ou protection de l'économie. Le droit à l'initiative économique, l'établissement d'un marché digital unitaire ainsi que le développement de l'économie de l'information peuvent aussi assurer une certaine protection des personnes. Actuellement la protection de la privacy et des données personnelles est mise en danger plutôt par la récolte et rétention, parfois systématique et indiscriminée, des données personnelles et notamment des « meta-data » (dont on peut commodément tirer beaucoup d'informations), justifiée par d'exigences de sureté publique.

6. *Comment protège-t-on les personnes dans le cloud-computing (l'informatique en nuage) ?*

La « Cloud Computing Strategy » de l'Union Européen (Communication COM(2012) 529 final) vise à harmoniser les disciplines juridiques nationales en Europe (notamment en ce qui concerne la protection des données personnelles ainsi que les droits des consommateurs) mais elle ne soutient pas la création d'un cloud-computing européen, qui pourrait bien aider à dépasser la fragmentation actuelle du marché digitale européen. Au niveau national, il faut remarquer qu'il n'existe pas en Italie une discipline juridique spécifique et unitaire concernant le cloud-computing. Les rapports existants entre les acteurs qui opèrent

dans le cloud-computing (à savoir, notamment, le *cloud service provider* et le *cloud service consumer*, auxquels on pourrait ajouter le *cloud auditor*, le *cloud broker* et le *cloud carrier*) sont réglés contractuellement. Il s'agit surtout des contrats par adhésion – prédéterminés par les fournisseurs de services de cloud-computing – dont la généralité des clauses contractuelles a été déjà fixée (n'étaient pas celles-ci négociables) et qui disciplinent des aspects importants du rapport contractuel (tels que le niveau des services prêtés, la discipline juridique applicable ou le régime de responsabilité des parties contractuelles) de telle façon que les consommateurs des services ne sont pas toujours à même de s'apercevoir explicitement des effets juridiques de ce règlement contractuel (Mensi – Falletta 2015, 238).

Il y a toutefois une série des règles qui peuvent être appliquées aux rapports de cloud-computing : le D.lgs. n. 206/2005 (*Code des consommateurs*) établit des garanties en faveur des consommateurs, qui ne peuvent pas être dérogées contractuellement (notamment l'intégrité des données commerciales des consommateurs des services peut constituer un patrimoine sociétaire protégé en termes absolu comme droit de propriété industrielle; le D.lgs. n. 70/2003 (qui a transposé la directive 2003/31/CE sur le commerce électronique) exclut la responsabilité du fournisseur de services qui n'intervient pas dans les activités des utilisateurs, ainsi qu'une obligation générale de surveillance sur les données transmises. Le fournisseur n'a qu'une obligation générale d'informer l'autorité judiciaire ou administrative de vigilance, et non pas celui d'interrompre le service fourni dans le cas où il prenne connaissance des violations commises par le biais de l'Internet (*e.g.* des actes illicites de mise à disposition de contenu violant le droit d'auteur).

En ce qui concerne la protection des données personnelles, on essaye d'appliquer, au moins en partie, les principes et les normes du *Code de la privacy* (D.lgs. n. 196/2003) aux rapports de cloud-computing, qu'il faut parfois adapter à la spécificité de ces services, car il peut y avoir des différences entre la protection des données personnelles et celle des données qui ont une relevance commerciale en tant qu'informations industrielles et commerciales réservées(par exemple, en ce qui concerne la destruction des données personnelles par le fournisseur de services lorsque le rapport contractuel de cloud-computing est terminé). Les parties peuvent négocier des *Privacy Level Agreements* (PLA), qui définissent les termes et les garanties contenues dans le contrat de cloud-computing.

En ce qui concerne le transfert des données personnelles à l'étranger, l'art. 25 de la directive 95/46/CE interdit le transfert des données personnelles vers des pays qui ne garantissent pas un niveau de protection adéquat. « Cependant, quand il y a des transferts de données personnelles dans des contextes non-européens, dans lesquels il n'y a pas une garantie d'un niveau de protection adéquat aux normes européennes, certains outils spécifiques viennent au secours, tels que : a) le consentement de la personne concernée ; b) les *Model Clause* approuvées par la Commission européenne ; d) le soi-dit *Safe Harbor* dans le cas d'un *data importer* des Etats-Unis » (Mensi – Falletta 2015, 246).

7. Comment protège-t-on les personnes dans le big data ?

En ce qui concerne la protection des personnes (voire des données personnelles) dans le big data, il faut tout d'abord rappeler qu'il n'y a pas une normative spécifique au niveau national italien. Il faut donc appliquer à ce sujet les normes générales en matière de protection des données personnelles (D.lgs. n. 196/2003), tout en tenant compte de la spécificité des big data, qui sont notamment utilisés pour créer des corrélations statistiques et pour profiler les individus sur la base des inférences tirées de la récolte, analyse et traitement des big data. Pour cette raison, le consentement du sujet intéressé (qui est nécessaire afin d'effectuer des activités de profilage, car cette activité peut affecter les droits des individus puisqu'il est possible de retracer les données personnelles à partir des données agrégées des personnes profilées) doit respecter trois exigences fondamentales : la plénitude, la liberté et la spécificité. Un consentement est plein lorsque le sujet intéressé est conscient qu'il y aura une activité de profilage. En d'autres termes, la personne concernée doit être pleinement conscient que les informations fournies feront l'objet d'un traitement automatique, afin de créer un profil qui lui serait attribué. Le consentement doit également

être libre : il ne doit pas être structuré de manière à qu'il puisse constituer une condition préalable nécessaire pour l'accès à des services ou des avantages. Enfin, le consentement doit être spécifique : le document concernant le consentement à des fins de profilage doit être clairement diversifié de ceux utilisés pour l'acceptation des conditions générales du contrat (ou plus en général du traitement des données personnelles). Les big data posent aussi des problèmes dans le cadre de leur transfert aux tiers, en ce qui concerne le principe de la finalité du traitement, compte tenu de leur intrinsèque utilisation à d'autres fins que celles pour lesquelles elles ont été recueillies.

8. *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 ?*

Le droit à l'oubli dans le système juridique italien

Il n'y a pas encore, à présent, une explicite prévision normative du droit à l'oubli dans le système juridique italien, dans l'attente de l'approbation du nouveau Règlement européen en matière de protection des données personnelles. Toutefois, ce droit a été reconnu et développé à travers une interprétation jurisprudentielle. Il a été reconnu pour la première fois par l'arrêt de la Cour de Cassation n. 3679/1998, qui affirme : « il faut entendre le droit à l'oubli comme l'intérêt bien-fondé de chaque personne à ne pas rester indéterminément exposé aux dommages ultérieurs que la publication réitérée d'une information, légitimement divulguée dans la passé, cause à son honneur et à sa réputation ». Cet arrêt a été, pour ainsi dire, intégré dans le temps par les articles 11 et 7, alinéa 3, lettre b, du D.lgs. n. 196/2003 (« Code en matière de protection des données personnelles »), qui disposent, respectivement, que : les données, qui permettent d'identifier un sujet intéressé, ne peuvent pas être conservés pour une période excédante celle nécessaire à accomplir les finalités pour lesquelles les données avaient été récoltes et traités (la *finalité* a été toujours réaffirmée par la jurisprudence comme un réquisit obligé de licéité du traitement : Cour de Cassation n. 5525/2012) ; le sujet intéressé peut demander au sujet titulaire du traitement l'élimination ou la transformation des données qui le concernent dans tous les cas prévus par le Code susmentionné.

Suite au développement d'Internet et des journaux en ligne, la Cour de Cassation a ultérieurement précisé le sens et la portée du droit à l'oubli dans le système juridique italien, en particulier en relation au droit d'information. L'arrêt de la Cour de Cassation n. 5525/2012 établit que : l'éditeur du journal en ligne (dans ce cas le *Corriere della Sera*) doit intégrer et updater les informations archivées, car une information, qui n'est pas updatée, résulte partielle et incorrecte et, par conséquence, fausse. La solution envisagée par la Cour de Cassation n'a donc pas été celle de l'élimination de l'information, à savoir de l'oubli de celle-ci, mais plutôt celle de la nécessaire « remise en contexte » de l'information (Frosini 2013, 93). La Cour a voulu de cette façon équilibrer le droit à l'oubli (la donnée permettant l'identification du sujet intéressé peut être éliminée, lorsqu'il n y a plus un intérêt publique actuel à l'information) et le droit d'information (l'information partielle et incorrecte doit être updatée et ainsi remise en contexte : ce qui assure aussi le droit à l'identité personnelle du sujet intéresse, à savoir son intérêt à ne pas sombrer dans un *false light*).

Dans ce cadre, on peut dire avec Franco Pizzetti, déjà Garant italien pour la protection des données personnelles, que : « en Europe et en Italie le droit à l'oubli, dans sa forme jurisprudentielle qui s'est formée notamment dans les années '90 et au début des années deux-milles, a été développé, non pas seulement, en actuation des principes propres de la protection des données personnelles, mais plutôt en tant que (…) point d'équilibre entre le respect des droits de la personnalité, d'un côté, et la liberté d'information et de manifestation de la pensée, de l'autre côté » (Pizzetti, 2013, 34). Cela signifie aussi que, dans le système juridique italien, le droit à l'oubli est (encore) principalement lié à la tutelle de la vie privée,

de la dignité et de l'identité personnelle, à savoir au respect de la personnalité en tant que droit fondamental de l'être humain.

Toutefois, la protection du droit à l'oubli est bien destinée à se lier, de façon de plus en plus étroite, à la protection des données personnelles en tant que telle, c'est-à-dire en tant que droit autonome, qui vise à assurer soit la « liberté informatique passive » (le droit de protéger la vie privée et de connaitre *qui* connait *quelles* données personnelles, *pendant quel* temps et *par quels* moyens) soit la « liberté informatique active » (le pouvoir d'avoir un contrôle sur ses propres données, en participant de façon active à l'ensemble du circuit des informations) (Frosini 2013, 88). L'évolution du droit à l'oubli envisagé par le nouveau Règlement européen (art. 17) va précisément dans cette direction : le droit à l'oubli ne s'exerce plus en tant que conséquence de la violation de quelques aspects des droits de la personnalité (vie privé, dignité, identité personnelle), mais en tant qu'expression d'un pouvoir de contrôle sur la circulation des propres données personnelles, dont on peut demander la de-indexation *tout simplement* à la suite à la retrait implicite de l'accord de l'internaute pour recueillir et pour utiliser ses données personnelles (art 17, comma 1, lettre b, et sauf dans les cas prévus par l'art. 17, comma 3).

La mise en œuvre du droit à l'oubli suite à l'arrêt Google Spain de la Cour de Justice

Les mesures prises par Google, suite à l'arrêt de la Cour de Justice dans le cas *Google Spain*, ont été classifié comme un comportement d'autoprotection, qui a été assimilé à certains égards à la procédure dénommée de « notice and take down », qui appartient au système juridique des Etats-Unis et est réglé en particulier par la section 512 du Digital Millennium Copyright Act (DMCA) de 1998. Cette mesure vise à assurer la protection du droit d'auteur dans le monde en ligne. En réalité, les différences entre la procédure américaine et les mesures prises par Google sont considérables, même si parfois on a parlé d'une réception de ce modèle dans le système juridique européen de protection des données personnelles.

Afin de mieux saisir le sens et la portée des mesures prises par Google, il est nécessaire d'apprécier les particularités de la procédure américaine et les différences qu'elle entretient avec celle européenne. La procédure de « notification et retrait » est divisée en plusieurs phases au cours desquelles plusieurs acteurs sont concernés. La principale caractéristique de cette procédure est la volonté d'instaurer, tout au long de son déroulement, un débat entre les parties opposées qui s'inspire au principe du contradictoire. La procédure peut avoir lieu avec facilité ; d'autant plus que, tous les fournisseurs des services Internet (*Internet service providers*) doivent être fournis d'une figure professionnelle spécifique, à savoir un sujet préparé ad hoc pour la réception de toute réclamation, nommé l'« agent désigné ». La procédure commence à la suite d'une demande spécifique déposée par la partie lésée au fournisseur des services Internet : dans le cas prévu par le DMCA cette réclamation est effectuée par ceux qui croient que leur droit d'auteur a été compromis à cause d'un produit présent en ligne. Ces derniers, dans ce cas d'espèce, déposerons une plainte, la soi-disant « notification ».

Il s'agit d'une demande écrite qui vise à mettre fin à la violation du droit dénoncée, dont certaines parties sont en effet très similaires à celles requises par le formulaire Google pour demander la suppression (voire la désindexation) des données personnelles. En fait, apparaissaient comme nécessaires : le nom, l'indication spécifique du sujet de la plainte, une indication claire de l'URL, les coordonnées du demandeur de contact, une déclaration de bonne foi de la part de l'instant, une affirmation de l'exactitude des informations publiés et la signature de l'instant. La notification est envoyée à l'agent désigné, qui appelle le fournisseur de services pour désactiver l'accès à les informations contentieux ; en respectant cette indication le fournisseur profite d'une présomption générale d'irresponsabilité pour le contenu litigieux. Ce *favor legis* est exclu dans le cas où le fournisseur ne garantit pas un minimum de contradictoire entre le propriétaire du droit d'auteur, qui apparait comme prétendument violé, et l'auteur des activités

contentieuse. Une fois reçue la notification et la mise en œuvre de la mesure restrictive (à savoir la désactivation du contenu litigieux), il est nécessaire que : l'agent désigné communique sans délai le début de la procédure au sujet auteur du contenu supprimé (à savoir le « subscriber »).

Cette communication assure la correcte mise en place du contradictoire entre toutes les parties, donnant au sujet résistant la possibilité de présenter une justification d'appui de sa position. Le défi de la notification se fait par la rédaction d'une déclaration écrite, qui est la « contre-notification ». Dans cette déclaration, en outre, le sujet résistant accepte que la controverse soit remise à la Cour fédérale de district appropriée dans le cas où sa déclaration soit acceptée. En fait, « l'acceptation éventuelle de la contre-notification par l'intermédiaire a deux conséquences principales: d'une part l'intermédiaire peut continuer à profiter du régime de responsabilité limitée – bien que le contenu dont la légalité fait l'objet de débat soit ensuite remis en ligne – et, d'autre part, suite à la notification du titulaire du droit d'auteur, une procédure spécifique peut s'instaurer devant le tribunal compétent. Il ne sera, en effet, qu'à la fin de cette procédure que le contenu litigieux pourra être définitivement désactivé, si son caractère illicite est enfin établi par le tribunal » (Bertoni – Montagnani, 2013, 547). Dans le cas où les raisons du sujet résistant soient reconnues, l'agent désigné doit aviser l'instant de la remise en l'état des choses dans la même manière qu'elles l'étaient antécédemment à la notification. Le système de « notification et retrait » est renforcé par une disposition particulière (section 512 (f) DMCA) qui vise à sanctionner ceux qui agissent avec une notification sans fondement et prétentieux. Après avoir examiné brièvement la procédure de « notification et retrait », il est bien possible saisir les différences substantielles avec la procédure adoptée par Google suite à l'arrêt C-131/2012.

La différence la plus évidente est, bien sûr, l'omission de la mise en place d'un débat entre les parties, qui soit réellement inspiré au principe du contradictoire. Cette omission soulève bien des doutes sur la légitimité et le bienfondé de la procédure européenne. En fait, cette procédure ne contemple pas la figure de l'auteur du contenu qu'on veut désindexer : les intérêts du sujet résistant ne sont aucunement pris en compte lors qu'il s'agit de prendre une décision sur la demande de désindexation des contenus (au moment même où il faudrait équilibrer les intérêts opposés). Google et les autres fournisseurs de services Internet ne sont pas légalement tenus (même pas à la suite à l'arrêt C-131/2012) à informer le sujet titulaire des informations contentieuses. En fait, sa participation à la procédure de désindexation des résultats de recherche est purement potentielle, de sorte que ce sujet pourrait bien arriver à connaître uniquement après une longue période (ou même jamais) la désindexation de sa page.

Actuellement, par conséquent, la position du sujet auteur des informations contentieuse est complètement négligée bien qu'il soit titulaire d'un intérêt bien-fondé. Faudrait-il garantir à cette partie, dont la position n'est pas moins digne de protection, la capacité d'agir en réponse à la notification ou bien à la désindexation auprès des Autorités nationales garantes ou des organes juridictionnels compétents. Nous sommes donc confrontés à une situation juridiquement inadéquate et déséquilibrée : le processus utilisé par Google n'a pas de véritable mécanisme de coordination entre le secteur privé, auquel a été confié un excessif pouvoir de médiation entre des intérêts en conflit, et une éventuelle phase publique confiée à des organismes institutionnels compétents. Il semble donc nécessaire une réglementation appropriée de cette médiation, désormais entièrement laissée aux fournisseurs de services Internet. Une attitude correcte pourrait ainsi consister dans la mise en place d'une procédure de «notification et retrait » comparable aux États-Unis, en ce qui concerne les garanties du principe du contradictoire, afin d'assurer un bon équilibre des droits concernés, de sorte que les fournisseurs de service Internet ne soient pas toujours tentés de désindexer et ainsi censurer tous les ressource informatives contentieux qui font l'objet de notification.

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

Comme observé auparavant, en ce qui concerne le transfert des données personnelles à l'étranger, l'art. 25 de la directive 95/46/CE interdit le transfert des données personnelles vers des pays qui ne garantit pas un niveau de protection adéquat de celles-ci. Le transfert des données à caractère personnel vers les tiers est réglé par les normes générales en matière de protection des données personnelles. Il est vrai, toutefois, qu'il est bien difficile d'assurer le respect des principes de nécessité, proportionnalité et consentement dans le traitement des données à caractère personnel une fois qu'elles ont été transférées (soit à l'étranger soit aux tiers).

10. *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 ?*

Il y a en Italie une Autorité Garante pour la protection des données personnelles instituée par la loi n. 675/1996, transposant la directive 95/46/CE, et aujourd'hui réglé par le D.lgs. n. 196/2003. Il s'agit d'une autorité administrative indépendante, qui est notamment compétent pour faire respecter les règles en matière de protection des données personnelles et pour sanctionner les violations des données personnelles (« data breaches »). Plus spécifiquement, l'Autorité Garante a les fonctions et les pouvoirs suivants : vérifier que les traitements des données personnelles soient conformes aux dispositions normatives et réglementaires et, le cas échéant, suggérer les mesures qu'il faut adopter pour se conformer à la discipline en matière ; examiner les réclamations signalant les violations des données personnelles ; décider de requêtes présentées conformément à l'art. 145, D.lgs. n. 196/2003 ; interdire, totalement ou en partie, ou ordonner l'arrêt du traitement des données personnelles, qui peut mettre en danger les droits du sujet intéressé en raison de la nature, de la modalité ou de la finalité du traitement en cours ; adopter les mesures nécessaires prévues par la normative en matière de protection des données personnelles et notamment les autorisations générales pour le traitement des données sensibles.

B/ La liberté d'expression sur Internet

1. *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 ?*

En Italie, bien que dans le passé certaines conduites ou choix de *policy* des réseaux sociaux et des principaux moteurs de recherche aient été dénoncées (par exemple, le filtrage automatique des contenus jugés « inappropriés » par le réseau même), nous n'avons pas encore une jurisprudence sanctionnant ces pratiques.

2. *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 ?*

Oui, les juridictions italiennes sont très actives contre les crimes conduits sur Internet, surtout en matière d'injure et diffamation sur les réseaux sociaux. Par exemple, la diffamation sur Facebook est considérée comme une hypothèse de diffamation aggravée selon le droit pénal italien (Cassation n. 8328/2016).

3. *Quels moyens peuvent être mis en œuvre pour faire cesser ces atteintes ? Sont-ils efficaces ?*

Les juridictions ordinaires sont assez efficaces dans leur lutte contre les crimes commis sur Internet : toutefois, les exigences de sécurité souvent l'importent sur le respect des droits d'expression des internautes. Par exemple, suite à des arrêts assez contradictoires, les Sections Unies de la Cour de Cassation italienne sont intervenues (arrêt 31022/2015) pour clarifier et discipliner le séquestre judiciaire préventif d'une page Internet, afin de prévenir une utilisation incorrecte de cette mesure judiciaire. En suivant l'exemple donné par HADOPI en France, le législateur italien a doué l'Autorité des Télécommunications (AGCOM) du pouvoir de sanctionner, par voie administrative, les infractions aux droits d'auteurs sur Internet. Ce pouvoir de sanction a été contesté devant la Cour Constitutionnelle, qui a toutefois déclaré

(fin 2015) la question inadmissible. En l'attente d'un nouvel arrêt de la cour administrative régionale du Lazio (TAR Lazio) sur ce sujet, l'efficacité de ces mesures n'est pas encore prouvée.

RAPPORT SOMMAIRE SUR LA PROTECTION DES DONNEES PERSONNELLES

Les enjeux :

- ✓ Limitations inhérentes au paradigme de l'informative et du consensus : ces limites sont perçues notamment par rapport à la capacité de l'individu à être vraiment informé, à percevoir les conséquences de leurs choix ainsi qu'à percevoir la valeur, aussi économique, de leurs données personnelles, une fois que ceux-ci ont été regroupées ;
- ✓ Limitations inhérentes aux principes de nécessité, proportionnalité et finalité du traitement : ces limites sont perçues notamment en ce qui concerne la protection des données personnelles dans le cloud-computing, dans les big data et en général en cas de transfert des données personnelles aux tiers ;
- ✓ Limitations inhérentes la dimension territoriale de la compétence juridique et la fragmentation des normatives nationales par rapport à des phénomènes qui ont de plus en plus une dimension internationale et supranationale (concernant les relations entre les Etats ou au-dessus des Etats) et notamment transnationale (concernant les relations avec les acteurs non étatiques qui opèrent globalement) ;
- ✓ Limitations inhérentes à la dimension individuelle des utilisateurs du réseau : ces limites sont perçus, en particulier, dans la relation contractuelle entre l'utilisateur individuel du réseau et les grands acteurs du marché, qui souvent abusent de leur position dominante ; et par rapport à des phénomènes tels que le « group privacy » (la privacy d'un group), où l'individu fait partie d'une communauté, qui n'a pas une position juridique subjective autonome ou par rapport à laquelle l'individu n'a pas de pouvoir réel d'interlocution.

Orientations pour assurer une meilleure protection des données personnelles :

- ✓ Renforcer la protection juridique des personnes concernées par le biais d'un rééquilibre entre la position des utilisateurs individuels et les principaux acteurs du marché ; de formes de protection collective de la privacy (d'un group ou à l'intérieur d'un group) ; une définition plus précise d'intérêts juridiques protégés ;
- ✓ Augmenter les devoirs des responsable du traitement des données à travers : la révision des devoirs d'informative (qui va vers une clarification plus ponctuelle des conséquences possibles du traitement des données) ; la prévision d'une évaluation de l'impact des techniques automatisées avec lesquelles les données sont collectées, traitées et analysées (en particulier dans le cas de Big data) ;
- ✓ La création d'un cloud-computing européen ;
- ✓ L'incorporation de certaines normes sur la protection des données personnelles par le biais de : mécanismes ou dispositifs technologiques *by design* ou *par défaut*, de sorte que certaines questions sont déjà soulevées lorsqu'il s'agit de programmer les techniques automatisés avec lesquelles les données sont collectées, traitées et analysées.

RÉFÉRENCES BIBLIOGRAPHIQUES

Bertoni A. – Montagnani M. L. (2013), "Il ruolo degli intermediari internet tra tutela del diritto all'autore e valorizzazione della creatività in rete", in *Giur. Comm.*, fasc. 3, pp. 537-573.

Frosini T. E. (2013), "Il diritto all'oblio e la libertà informatica", in Pizzetti F. (a cura di) (2013), *Il caso del diritto all'oblio*, Giappichelli, Torino.

Mensi M. – Falletta P. (2015), *Il diritto del web. Casi e materiali*, Wolters Kluwer, Torino.

Pagallo U. (2014), *Il diritto nell'età dell'informazione*, Giappichelli, Torino.

Pizzetti F. (a cura di) (2013), *Il caso del diritto all'oblio*, Giappichelli, Torino.

Prof. Massimo Durante

Associato in Filosofia del diritto e Informatica giuridica

Dipartimento di Giurisprudenza, Università di Torino

massimo.durante@unito.it – tel. + 39.011.6706904