BULLETIN
Droit européen de la e-santé

N°1- Janvier/Mai 2015

- Edito -

Le Centre d'études et de recherches internationales et communautaires (CERIC-CNRS UMR 7318 – Aix-Marseille Université) développe, depuis plusieurs années, une recherche en droit européen de la santé. Cet axe de recherche est notamment porté par Estelle Brosset, Maître de conférences en droit public et habilitée à diriger les recherches. Elle est lauréate, depuis 2012 d'une Chaire Jean Monnet de la Commission européenne (2012-2015) intitulé « Droit européen et santé ». A travers cette Chaire, Estelle Brosset a entrepris de promouvoir le développement de cette spécialité tant au niveau de la formation que de la recherche au sein d'Aix-Marseille Université[1].

Dans ce cadre, le Centre d'études et de recherches internationales et communautaires s'est, depuis la rentrée 2014, associé à un projet de recherche « APPRISE HIT e-santé » coordonné par Rachid Bouchakour et Ahmed Charaï (IM2NP-UMR 7334) financée par Amidex. A travers cette recherche, l'ambition est de réfléchir aux différentes questions juridiques suscitées par le développement des pratiques de E santé et d'analyser les réponses apportées, pour ce qui concerne notre contribution au projet, par le droit européen.

Le bulletin d'information sur le droit européen de la e-santé est l'une des activités prévues dans le cadre de ce projet de recherche. Ce bulletin a vocation à être un document d'informations permettant de faire le point sur l'actualité législative et jurisprudentielle dans ce domaine. Chaque actualité sera résumée en quelques lignes afin de cibler rapidement les apports de celle-ci. Ce bulletin servira aussi de support pour faire part des publications et des manifestations passées et à venir portées par le Centre d'études et de recherches internationales et communautaires dans le domaine du droit européen de la santé. Nous espérons ainsi développer un outil utile et pratique pour étudiants, chercheurs et praticiens confrontés aux problématiques juridiques que pose la e-santé.

Le premier numéro du bulletin bimensuel de droit européen de la e-santé est consacré à la « protection des données personnelles ». Cette thématique fera certainement l'objet de plusieurs bulletins tant elle est au cœur même des défis posés par la e-santé au droit européen. L'objet de ce premier bulletin n'est alors pas de traiter de manière exhaustive toutes les questions que soulève la protection des données personnelles dans le domaine de la e-santé mais simplement de poser les jalons de la réflexion et de fournir au lecteur les références des textes européens et actualités jurisprudentielles à ce propos.

« E-santé et données personnelles : quelle relation ? »

E-santé, cybersanté, télémédecine, autant de termes qui ont fait leur entrée dans le vocabulaire des juristes alors même que leurs définitions d'un côté se multiplient mais de l'autre restent floues et leur périmètre incertain[2]. La notion de e-santé fait référence de manière générale à l'application au domaine de la santé des TIC c'est-à-dire des technologies de l'information et de la communication[3]. Envisagée de la sorte, le domaine de la e-santé est très large englobant tout

[1] Pour de plus amples information sur la Chaire « Hygie » voir : http://droiteuropeen.wix.com/ceric-sante

[2] Des chercheurs ont réalisé une étude sur la ou les définitions de la « ehealth ». Selon leurs résultats, il existerait au moins 51 définitions différentes de la notion. Hans OH, Carlos RIZO, Murray ENKIN, and Alejandro JADAD, « What Is eHealth (3): A Systematic Review of Published Definitions », Journal of Medical Internet Research, Published online Feb 24, 2005. Available at : http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550636/

[3] L'OMS rejoint cette definition de la e-santé. WHO, Resolution WHA58.28 eHealth, 58th World Health Assembly, 2005; Geneva, Switzerland.

à la fois les systèmes d'information sur la santé (dossier médical personnel, interopérabilité..), la télémédecine (usage du numérique par les professionnels de la santé) ou encore la télésanté (services du numérique à la personne pour son bien être). Le développement important, ces dernières années, de la e-santé interroge alors sur les enjeux qui la sous-tendent. Pourquoi développer la e-santé ? Permet-elle de renforcer la qualité de la santé, la qualité des soins, de l'accès aux soins ? Selon le rapport de Pierre Simon et Dominique Acker, la e-santé promet des avancées de tous ces points de vue et permet dans le même temps de réduire les dépenses de santé[4]. La e-santé serait alors l'Eldorado de demain pour la santé offrant tout à la fois des perspectives pour le renforcement de la qualité de la santé et pour l'assainissement des finances des systèmes de santé. Pourtant la diversité des données générées et traitées par le biais de la e-santé invite à porter un regard prudent quant à la protection de ces données. La e-santé permet sans doute quelques avancées en matière de qualité des soins mais comment garantir la protection de nos droits et libertés ?

« Les données à caractère personnel : quelle définition ? »

L'échange et le partage de données dans le cadre de la e-santé pose, en effet, plusieurs questions au juriste : de quelles types de données s'agit-il ? Quelle est leur nature ? Doivent-elles être protégées ? Si oui, comment et par qui sont-elles protégées ? Il n'y a bien évidemment pas lieu dans ces quelques propos de développer toutes ces questions qui font au contraire l'objet d'une réflexion précisément en cours. Nous aimerions simplement poser ici les repères de la réflexion qu'engendre la nébuleuse qui entoure la définition de la nature des données. L'identification et la classification des données concernées par la e-santé est une entreprise audacieuse mais nécessaire pour pouvoir protéger les individus des dérives auxquelles pourrait conduire le traitement de leurs données. La première distinction à opérer parmi les données, sans qu'elle soit pour autant la plus aisée, consiste à opposer les données à caractère personnel des autres données. En effet, la collecte et le traitement des données à caractère personnel nécessitent un régime juridique particulier permettant d'assurer le respect de la vie privée du titulaire de ces données. La catégorie juridique des données à caractère personnel qui apparaît dans les années 80 – auparavant certaines de ces données étaient classées dans la catégorie des données nominatives[5] – englobe, selon les termes de la directive 95/46/CE, « toute information concernant une personne physique identifiée ou identifiable (personne concernée) » de manière directe ou indirecte[6]. Les données qui répondent à cette définition bénéficient alors d'une protection juridique renforcée en ce qui concerne leur collecte, leur traitement et leur échange. Par ailleurs, au sein de la catégorie des données à caractère personnel, l'article 8 de la directive 95/46/CE invite à identifier une sous-catégorie de données donc la protection est renforcée : les données dites particulières ou sensibles. L'article 8 fait entrer dans la catégorie des données sensibles celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Or, la e-santé va bien évidemment être génératrice de données de santé et traiter ainsi des données dites sensibles. Cependant, que recouvre la catégorie des données de santé ?

« Les données de santé : quelle définition ? »

Si les données de santé sont considérées comme des données personnelles sensibles, aucun texte juridique ne définit la notion jusqu'à présent. La donnée de santé s'appréhende alors généralement comme toute donnée susceptible de révéler l'état pathologique ou non de la personne. Cette définition pourrait être élargie dans le cadre du futur projet de règlement européen de 2012 sur la protection des données personnelles puisqu'est considérée comme donnée de santé « toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne ». Cette définition ferait ainsi entrer dans la catégorie des

[4] Pierre SIMON et Dominique ACKER, « La place de la télémédecine dans l'organisation des soins », Rapport Mission thématique n° 7/PS/DA, Ministère de la Santé et des Sports, Direction de l'Hospitalisation et de l'Organisation des Soins, 2008. Disponible à l'adresse suivante : http://www.sante.gouv.fr/IMG/pdf/Rapport_final_Telemedecine.pdf

[5] Sur la différence entre « données à caractère personnel » et « données nominatives » voir : Jessica EYNARD, Les données personnelles : quelle définition pour un régime de protection efficace ?, Paris, Michalon, 2013.

[6] Selon la directive « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »

données dites « sensibles », toutes les données relatives aux interactions entre un patient et le système de santé. Si progressivement, la catégorie des données de santé semble s'étendre, les frontières de celles-ci restent approximatives voire poreuses. Ainsi comment distingue-t-on une donnée de santé, d'une donnée de bien être ? Plusieurs données de bien-être peuvent-elles constituer une donnée de santé ? À quelles conditions ?

Autant de questions qui plongent davantage la question de la protection des données dans l'incertitude terminologique et donc juridique car au final comment fixer un cadre juridique efficace sans connaître avec certitude la nature de ce que ce cadre juridique doit protéger ?

Législation européenne sur les données à caractère personnel

Article 8 de la Convention européenne des droits de l'Homme

Le droit à la protection des données à caractère personnel fait partie des droits protégés par l'article 8 de la CEDH, qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance, et énonce les conditions dans lesquelles des restrictions à ce droit sont admises. La Cour européenne des droits de l'Homme a développé une jurisprudence abondante sur ce point[7].

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

Cette Convention a été adoptée dans la cadre du Conseil de l'Europe en 1981. Elle a pour but de protéger les individus du traitement abusif de leurs données à caractère personnel collectées aussi bien par des entités publiques que privées. Les Etats membres du Conseil de l'Europe prenant acte de l'intensification des échanges de données transfrontières ont adopté, en 2001, un Protocole additionnel à la Convention concernant les autorités de contrôle et les flux transfrontières de données.

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

L'application territoriale de la directive relative à la protection des données s'étend au-delà des 28 États membres de l'UE et inclut aussi les États non membres de l'UE qui font partie de l'Espace économique européen – à savoir l'Islande, le Liechtenstein et la Norvège. Cette directive est la clé de voûte du droit de l'Union européenne en la matière toutefois d'autres actes de l'Union sont venus la compléter comme par exemple le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ; la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ; ou encore la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE mais qui a été invalidée par la CJUE le 8 avril 2014 dans l'affaire *Digital Rights Ireland Ltd & Michael Seitlinger e.a*. Un projet de règlement relatif aux données personnelles modernisant la directive 95/46/CE a, par ailleurs, été adopté en mars 2014 en première lecture par le Parlement européen mais les négociations sur ce texte semblent aujourd'hui bloquées. Le 13 mars 2015, le Conseil a arrêté une orientation générale partielle sur certains points : mécanisme de guichet unique (chapitre VI et VII du projet); principe du traitement des données personnelles (chapitre II du projet). L'objectif est de clore le dossier en juin 2015 « sous réserve du principe selon lequel il n'y a d'accord sur rien tant qu'il n'y a pas d'accord sur tout »[8].

[7] Pour un panorama de cette jurisprudence voir la fiche thématique « données personnelles » à l'adresse suivante : http://www.echr.coe.int/Pages/home.aspx?p=press/factsheets&c=fra).

[8] Pour plus de détail voir le communiqué de presse du Conseil de l'Union européenne à l'adresse suivante : http://www.consilium.europa.eu/fr/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism-background-note-fac_doc/

Article 8 de la Charte des droits fondamentaux.

La Charte consacre un article distinct de celui relatif à la protection de la vie privée et familiale à la protection des données à caractère personnel

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Jurisprudence européenne 2014 sur les données à caractère personnel

Cour de justice de l'Union européenne

Cour de justice de l'Union européenne : affaires jointes C-141/12 et C-372/12 - YS et autres c/ Minister voor Immigratie, Integratie en Asiel, Arrêt (troisième chambre) du 17 juillet 2014.

Dans ces deux affaires, les requérants ont introduit une demande de permis de séjour temporaire au titre du droit d'asile. Ces demandes ont été rejetées et les requérants ont demandé la communication des minutes relatives aux décisions de rejet ce qui leur a été refusé. Les deux requérants ont alors fait un recours afin d'obtenir les minutes. Le Conseil d'Etat et le tribunal néerlandais ont alors décidé de surseoir à statuer et de poser à la Cour plusieurs questions préjudicielles sur la définition de la notion de données à caractère personnel. En premier lieu, la Cour s'est livrée à une appréciation concrète du contenu de la minute afin de déterminer si elle entre dans le champ d'application de la directive 95/46 CE et de l'article 8 de la Charte des droits fondamentaux. Elle distingue entre les données relatives au demandeur du titre de séjour qui figurent dans la minute d'une part, et l'analyse juridique figurant dans la minute et fondée sur ces données, d'autre part. S'agissant des premières, elles constituent indéniablement des données à caractère personnel. Au contraire, s'agissant de l'analyse juridique, elle ne constitue pas une information concernant le demandeur. La Cour confirme ensuite la portée du droit d'accès aux données personnelles et les conditions de sa mise en œuvre comme notamment le caractère intelligible des données.

Cour de justice de l'Union européenne, huitième chambre : affaire C-683/13 - Pharmacontinente - Saúde e Higiene et autres, Ordonnance du 19 juin 2014.

Le Tribunal du travail portugais de Covilha saisit la CJUE d'une question préjudicielle relative à l'interprétation des articles 2 et 17 de la directive 95/46 CE. Le litige oppose l'entreprise Pharmacontinente – Saúde e Higiene SA et certains de ses employés à l'autorité administrative de surveillance des conditions de travail. Cette dernière voulait accéder au registre de temps de travail d'un des établissements de la société, ce qui lui a été refusé. Le Tribunal portugais demande alors à la Cour, en premier lieu, si les données contenues dans un registre de temps de travail sont des données à caractère personnel. La Cour considère que ces données sont des données à caractère personnel au sens de l'article 2 a) de la directive mais les articles 6, paragraphe 1, sous b) et c), ainsi que 7, sous c) et e), de la directive 95/46 doivent être interprétés en ce sens qu'ils ne s'opposent pas à 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.

Cour de justice de l'Union européenne, grande chambre : affaire C-131/12 – Google v Costeja González, arrêt du 13 mai 2014.

En 2010, M. Costeja González a introduit auprès de l'Agence espagnole de protection des données, une réclamation à l'encontre de La Vanguardia Ediciones SL ainsi qu'à l'encontre de Google Spain et de Google Inc au motif que, lorsqu'un internaute introduisait son nom dans le moteur de recherche du groupe Google, la liste de résultats affichait des liens vers deux pages du quotidien de La Vanguardia, datées de janvier et mars 1998 qui annonçaient notamment une vente aux enchères

immobilière organisée à la suite d'une saisie destinée à recouvrer les dettes de sécurité sociale dues par M. Costeja González. M. Costeja González voulait qu'il soit demandé à La Vanguardia de supprimer ou de modifier les pages en cause ou de recourir à certains outils fournis par les moteurs de recherche pour protéger ses données. D'autre part, M. Costeja González demandait qu'il soit ordonné à Google Spain ou à Google Inc. de supprimer ou d'occulter ses données personnelles afin qu'elles disparaissent des résultats de recherche et des liens de La Vanguardia. L'Agence espagnole de protection des données accepte la requête dirigée contre Google spain et écarte celle dirigée contre la Vanguardia. Google décide alors d'intenter une action et la juridiction saisie de l'affaire défère une série de questions à la Cour de justice.
Dans son arrêt, la Cour considère qu'en recherchant de manière automatisée, constante et systématique des informations publiées sur Internet, l'exploitant d'un moteur de recherche procède à une « collecte » des données au sens de la directive 95/46 CE et à un traitement de ces données et qu'à ce titre, il est responsable de ce traitement puisqu'il en détermine les finalités et les moyens. Enfin, la Cour considère, que si une personne en fait la demande, les données d'une personne peuvent être effacées après une appréciation de cette demande, eu égard au contexte. La cour reconnaît ainsi une forme de « droit à l'oubli » très encadré.

Cour de justice de l'Union européenne, grande chambre : affaires jointes C-293/12 et C-594/12 - Digital Rights Ireland, Seitlinger et autres, arrêt du 8 avril 2014.

- Digital Rights a introduit le 11 août 2006 un recours devant la High Court dans le cadre duquel elle soutient qu'elle est propriétaire d'un téléphone portable qui a été enregistré le 3 juin 2006 et qu'elle utilise celui-ci depuis cette date. Elle met en cause la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques et demande, notamment, à la juridiction de renvoi de constater l'invalidité de la directive 2006/24 prévoyant que les fournisseurs de services de communications téléphoniques doivent conserver les données afférentes à ces dernières relatives au trafic et à la localisation pour une période déterminée par la loi, afin de prévenir et de détecter les infractions, d'enquêter sur celles-ci et de les poursuivre ainsi que de garantir la sécurité de l'État. La Cour considère que la directive 2006/24 prévoit une ingérence au droit à la vie privée et au droit à la protection des données personnelles tels qu'ils résultent des articles 7 et 8 de la Charte sur les droits fondamentaux. L'intérêt général ne fait pas de doute : l'objectif matériel de cette directive est en effet de contribuer à la lutte contre la criminalité grave et en fin de compte à la sécurité publique. Toutefois encore faut-il que cette ingérence soit proportionnée au but recherché. Or, selon la Cour, l'ingérence de cette directive dans les droits fondamentaux n'est pas suffisamment encadrée et limitée. D'abord, elle impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. En outre, elle couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En plus, s'agissant de la durée de conservation des données, la directive impose une durée d'au moins six mois sans opérer une quelconque distinction entre les catégories de données en fonction des personnes concernées ou de l'utilité éventuelle des données par rapport à l'objectif poursuivi. La Cour constate également que la directive ne prévoit pas des garanties suffisantes permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. Elle en conclut que la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, est invalide.

Cour de justice de l'Union européenne, grande chambre: affaire C-288/12 - Commission v Hongrie, Arrêt du 8 avril 2014.

En vertu de la directive 95/46 CE sur la protection des données à caractère personnel, les États membres doivent désigner une ou plusieurs autorités chargées de veiller au respect des règles de la directive sur leur territoire. Ces autorités doivent exercer leurs fonctions en toute indépendance. La Cour considère qu'en mettant fin de manière anticipée au mandat du commissaire chargé de la protection des données, la Hongrie a porté atteinte à l'indépendance des autorités chargées de la protection des données à caractère personnel.

Cour européenne des droits de l'Homme

CourEDH cinquième section, *Brunet c. France*, Requête n°21010/10, arrêt du 18 septembre 2014.
Le requérant considérait que son inscription dans le fichier du système de traitement des infractions constatées malgré le classement sans suite de la procédure pénale engagée contre lui constituait une atteinte à sa vie privée. La Cour a conclu à la violation de l'article 8 de la Convention, au motif que l'État français avait outrepassé sa marge d'appréciation en la matière, puisque la conservation des données devait s'analyser comme une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne pouvait être considérée comme nécessaire dans une société démocratique. La Cour relève notamment que « le requérant n'avait pas disposé d'une possibilité réelle de demander l'effacement du STIC des informations le concernant et que la durée de conservation de ces données, qui était de vingt ans, était en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum » (§43).

CourEDH, *Radu c. République de Moldova*, Requête n°50073/07, arrêt du 15 avril 2014.
La requérante, formatrice dans une école de police, a été en arrêt de travail en raison d'un risque de fausse couche. L'école de police a demandé à l'hôpital de lui fournir les raisons de l'arrêt de travail de la requérante, ce que l'hôpital a fait. Suite à sa fausse couche, la requérante a intenté une action à l'encontre de l'hôpital et de l'école de police au motif que ses informations médicales avaient été diffusées sur son lieu de travail et qu'il en avait résulté un stress qui avait pu provoquer sa fausse couche. L'action de la requérante n'ayant pas abouti, l'affaire fut portée devant la Cour. La Cour a considéré que l'ingérence dans l'exercice du droit au respect de la vie privée dont se plaignait la requérante n'était pas prévue par la loi au sens de l'article 8 de la Convention.

Publications

A paraître

E. Brosset (Dir.), *Droit européen et protection de la santé - Bilan et perspectives*, Bruxelles, Bruylant, coll. Travaux de droit international et européen, 2015, à paraître prochainement.

E. Brosset, « Regard sur le principe de précaution en droit de l'Union européenne », *Revue de droit de l'Université de Sherbrooke*, été 2015, à paraître

E. Gennet, R. Andorno & B. Elger, "Does the new EU Regulation on clinical trials adequately protect vulnerable research participants?", Health Policy, à paraître.

Le volume 38 (2015-1) de *L'Observateur des Nations Unies* revue de l'AFNU Aix sera dédié au thème suivant : Droits de l'homme 2.0 : quelle protection à l'ère numérique ? L'appel à contribution est en cours : http://afnuaix.free.fr/

Parus

E. Brosset, « Le droit à la sécurité des soins est-il un droit du patient européen ? », *in* Laude (A.) (Dir), *Les droits du patient européen au lendemain de la transposition de la directive mobilité des patients*, Société de législation comparée, 1/2015.

E. Brosset, « Tourisme médical et sécurité des soins », *Note sous l'arrêt CJUE*, 9 octobre 2014, Petru, fa. C-268/13, *RDSS* n° 1 /2015.

Manifestations

Passées

Conférence de Xavier Tracol, vendredi 14 novembre 2014 dans l'amphithéâtre Louis Favoreu, FDSP, Aix-Marseille Université.
Dans le cadre du Master 2 « Droit de l'Union européenne » du CERIC (CNRS-UMR DICE 7318), Xavier Tracol, Senior Legal Officer à Eurojust, a livré une conférence sur l'arrêt rendu par la Cour de justice de l'Union européenne le 8 avril 2014 dans l'affaire *Digital Rights Ireland, Seitlinger et autres*.

Séminaire du 12 décembre 2014, « La protection des données de santé - Enjeux théoriques et mise en œuvre européenne », organisé dans le cadre du programme de recherche ATARAXIE PEPS CNRS Risque et Communication : innovation, expertise, controverse. FDSP, Aix-Marseille Université
Nous avons eu le plaisir d'accueillir dans le cadre de ce séminaire sur la protection des données de santé : Stéphanie Lacour, directrice de recherche CNRS à l'Institut de Sciences Sociales du Politique de l'Ecole normale supérieure de Cachan ; Nathalie Devillier, enseignant-chercheur à l'Ecole de Management de Grenoble et Jean Cattan, docteur en droit. Si la question de la protection des données personnelles est brûlante d'actualité à l'heure de l'adoption du règlement européen et du développement continu de la e-santé, les juristes se sont déjà à bien des égards saisis de ces questions. Le projet DEMOTIS financé par l'ANR, qui s'est déroulé de 2008 à 2012, et auquel Stéphanie Lacour a pris part a permis d'investir juridiquement le champ du dossier médical personnalisé et des dossiers des réseaux de soins liés à certaines maladies. Stéphanie Lacour nous a ainsi permis de nous plonger au cœur de ces questions à travers son intervention sur les enjeux juridiques relatifs à la protection des données de santé : le droit français et le dossier médical personnel. Par la suite, Nathalie Devillier qui a consacré ses recherches, depuis plusieurs années, à la protection des données de santé nous a transportés à l'échelle européenne pour nous entretenir des données de santé et de leur protection dans la proposition de règlement européen sur les données personnelles. Enfin, Jean Cattan nous a offert des pistes de réflexion stimulantes pour une meilleure protection des données de santé en nous invitant à réfléchir à une gestion collective des données personnelles de santé.

A venir

VIII^{ème} Journée de l'UMR DICE 7318
« Protection des données personnelles et Sécurité nationale Quelles garanties juridiques dans l'utilisation du numérique ? », Université de Toulon, Faculté de droit, Vendredi 27 novembre 2015.

Colloque organisé par le Réseau Droit, Sciences et Techniques (GDR 3178) et l'UMR de Droit comparé de Paris I.
« Sciences et droits de l'homme », Paris-Sorbonne (octobre/novembre 2015, date en cours de détermination)

Journées franco-québécoises de droit de l'environnement et de la santé : lundi 2 novembre 2015
« L'obligation de vigilance en droit international, européen et comparé de l'environnement et de la santé ».