

	<b>SYSTÈMES EMBARQUÉS ET GRANDES INFRASTRUCTURES</b>	Réservé à l'organisme gestionnaire du programme N° de dossier : ANR-08-XXXX-00 Date de révision :
	Document de soumission <b>B</b>	<b>Edition 2008</b>

<b>Acronyme/Acronym</b>	<b>DEMOTIS</b>
<b>Titre du projet/Proposal title</b> <i>(en français/ inFrench)</i>	<b>Définir, Evaluer et MOdéliser les Technologies de l'Information de Santé</b>
<b>Titre du projet/Proposal title</b> <i>(en anglais/ in English)</i>	<b>Collaborative Analysis, Evaluation and Modelling of Health Information Technology</b>

*Les pages seront numérotées et l'acronyme du projet devra figurer sur toutes les pages du document en pied de page.  
Un sommaire du document est bienvenu*

# Sommaire

<b>1. Programme scientifique et technique</b> .....	2
1.1 Problème posé .....	2
1.2 Contexte et enjeux du projet .....	3
1.3 Objectifs et caractère ambitieux/novateur du projet .....	6
1.4 Positionnement du projets .....	8
1.5 Description des travaux : programme scientifique et technique .....	8
1.6 Résultats escomptés et Retombées attendues .....	22
1.7 Organisation du projet .....	23
1.8 Organisation du partenariat .....	24
1.9 Stratégie de valorisation et de protection des résultats .....	29
<b>2. Justification scientifique des moyens demandés</b> .....	30
2.1 Partenaire 1. <i>Sopinspace</i> .....	30
2.2 Partenaire 2. <i>INRIA</i> .....	31
2.3 Partenaire 3. <i>CECOJI</i> .....	31
<b>Annexes</b> .....	33

# 1. Programme scientifique et technique/Description du projet. *Technical and scientific description of the activities*

## 1.1 Problème posé. *Rationale.* (1/2 page maximum)

*Présentation générale du problème qu'il est proposé de traiter dans le projet et du cadre de travail (recherche fondamentale, industrielle ou développement expérimental).*

[français]

La conception et la mise en oeuvre de grandes infrastructures techniques en charge de la gestion de données d'importance essentielle se heurte à des problèmes nouveaux difficilement abordables par une simple approche basée sur l'analyse des besoins et la traduction en fonctionnalités techniques. Ces systèmes sont dès leur conception pris dans un enchevêtrement de dispositifs juridiques, de normes techniques, de craintes et d'attentes positives de la société. En particulier lorsque des architectures centralisées et interconnectées manipulent des données sensibles comme les données de santé, des problèmes de sécurité sans précédent se posent.

Le projet DEMOTIS a pour champ d'investigation deux types de systèmes : l'infrastructure en charge du dossier médical personnalisé (DMP) et celles des dossiers des réseaux de soins liés à certaines affections (SIDA, cancer). Ces choix s'expliquent par leurs enjeux économiques et sociaux majeurs, la complexité du contexte juridique (y compris concernant la sécurité des données) et la mobilisation possible de parties prenantes dans des processus de consultation.

Eclairer les limitations et compromis réciproques que l'intrication des domaines juridiques et informatiques impose à la conception de telles infrastructures est au coeur du projet DEMOTIS. Il comporte deux volets interdépendants, juridique (droit de la santé, des données personnelles ou de la propriété intellectuelle, par exemple) et informatique (sécurité des bases de données et techniques cryptographiques utilisées pour les protéger) qui seront abordés de manière conjointe par les partenaires. Un corpus des textes juridiques et normatifs pertinents fera l'objet de lectures croisées de juristes et informaticiens. Ces lectures croisées utiliseront un service Web 2.0 d'annotation de textes développé par le partenaire industriel du projet et publié sous licence libre. Elles auront pour objectif de confronter les différentes exigences juridiques encadrant les dossiers médicaux informatisés et fichiers « maladies » et l'état de l'art en informatique. Elles déboucheront sur l'identification des fonctionnalités attendues pour ce type d'infrastructures et des barrières technologiques rencontrées, puis sur une évaluation de l'adéquation des réponses existantes et l'exploration des solutions offertes par de nouvelles techniques émergeant dans les domaines de la cryptographie et des bases de données.

Enfin, une consultation des parties prenantes sera organisée pour expérimenter et évaluer les bénéfices d'une mobilisation d'un public plus large dans la conception et spécification de systèmes techniques de ce type.

DEMOTIS est un projet de recherche partenariale entre organismes de recherche et entreprise. Son débouché sera un ensemble de publications et recommandations, de techniques (implémentées sous forme de services Web en logiciel libre) et de méthodes de concertation. L'ensemble sera largement réutilisable dans d'autres champs que celui des données de santé.

[English]

The design and implementation of large-scale infrastructure for sensitive and critical data faces new problems that can no longer be tackled using classical methods such as requirement analysis followed by functional design. From their design stage, these infrastructural projects are positioned in a tangle of legal provisions, technical standards, and societal concerns and expectations. When sensitive data such as health records are processed within centralised and interconnected architectures, unprecedented safety issues arise.

Two types of systems have been chosen for the investigation conducted in the DEMOTIS project: The infrastructure for the French personal medical file system (DMP) and the data infrastructure for the

research and public health networks associated with specific diseases (AIDS, cancer). This choice is motivated by the major social and economic stakes, the complexity of the legal context and the possible involvement of stakeholders in consultation processes.

At the heart of the DEMOTIS project is the aim to understand how the interconnection between the legal and technical domains constrains the design of such data infrastructures. DEMOTIS consists of two interdependent facets: legal (health law, privacy or intellectual property law, for instance) and computer science (database security, cryptographic techniques for data protection). These two facets will be investigated in conjunction by the partners. A corpus of relevant legal and normative texts will be annotated jointly by lawyers and computer scientists. These interacting readings will use a Web 2.0 text annotation service developed by the industry partner in the project and published under a free / open source software license. Their aim will be to collate the various legal prescriptions that frame the digital personal medical files and epidemiological files and to analyse them in view of the state of the art of possible software implementations. They will result in an identification of the expected functionality for this type of infrastructures and of the corresponding technological challenges. Then, an evaluation of the adequacy of existing technological answers and an exploration of solutions based on new emerging techniques in the database and cryptography fields will be performed. Finally, a consultation of stakeholders will be organized to experiment and evaluate the benefits of involving a wider public in the design and specification of this type of information systems.

DEMOTIS is an academic research-industry partnership project. Its outcome will be a set of publications and recommendations, specifications, technology (implemented as free software Web services) and stakeholder concertation methods. A large part of these results will be potentially reusable in fields other than health data.

## 1.2 Contexte et enjeux du projet. *Background, state of the art, issues and hypothesis.* (1 à 5 pages maximum)

*Décrire le **contexte économique, social, réglementaire**...dans lequel se situe le projet en présentant une analyse des enjeux sociaux, économiques, environnementaux, industriels...Donner si possible des arguments chiffrés, par exemple, pertinence et portée du projet par rapport à la demande économique (analyse du marché, analyse des tendances), analyse de la concurrence, indicateurs de réduction de coûts, perspectives de marchés (champs d'application, ...). Indicateurs des gains environnementaux, cycle de vie...*

*Décrire le **contexte et les enjeux scientifiques** dans lequel se situe le projet en présentant un **état de l'art national et international** en incluant les références nécessaires.*

DEMOTIS est l'acronyme de Définir, Evaluer et MODéliser les Technologies d'Information de Santé. En grec ancien, « dêmotês » désigne quelqu'un du peuple, un concitoyen et « dêmotis » est son féminin. Le choix de ce nom évoque l'impact sur tout un chacun de la généralisation de l'usage des grandes infrastructures de données pour gérer des questions d'envergure nationale comme la santé. C'est précisément le changement d'échelle dans le nombre des utilisateurs de ce type de système (y compris les personnes à propos de qui des données sont collectées) qui impose la prise en compte des contextes juridiques et sociétaux et motive les innovations à apporter à leur processus de conception.

Le projet émane d'une communauté pluridisciplinaire dont la structuration a débuté dans le projet Asphales<sup>1</sup>, qui a montré qu'une collaboration suivie entre des chercheurs en droit et en informatique constituait une démarche particulièrement pertinente dans le domaine de la sécurité et des technologies dans un contexte juridique complexe. Asphales était consacré à l'analyse des interactions entre sécurité juridique et sécurité informatique sur des sujets aussi variés que le droit d'auteur, la conservation des documents électroniques ou la protection des données personnelles. Le projet DEMOTIS entend poursuivre et étendre dans un sens plus opérationnel ces travaux interdisciplinaires dans le champ plus spécifique de la sécurité des grands systèmes informatiques gérant des données de santé.

<sup>1</sup>Action Concertée Incitative Sécurité et Informatique (<http://www.asphales.cnrs.fr>)

Le projet DEMOTIS est naturellement motivé par la volonté actuelle de mise en place de diverses infrastructures informatiques de grande envergure destinées à gérer des données de santé. Le dossier médical personnel, créé par la loi 2004-810 du 13 août 2004, est le plus célèbre d'entre eux, mais on peut aussi mentionner par exemple les registres du cancer [CNI03], les différents fichiers épidémiologiques comme ceux créés pour la surveillance épidémiologique du SIDA [CNI99]. La création par les pouvoirs publics de ces dossiers médicaux informatisés suscite de nombreuses interrogations sur le plan technique, mais aussi juridique et social. Les craintes liées à la protection des données personnelles de santé, au droit à l'oubli mais aussi aux modifications des relations patients-médecins inhérentes à l'apparition de ces nouveaux outils sont à l'origine de réactions, parfois virulentes, des professionnels de santé et des associations d'usagers et de malades (cf. par exemple le rapport IPSOS Santé/CNAM intitulé « Opinions et attitudes des médecins et des patients à l'égard du Dossier médical partagé » [IC03], les travaux du groupe « informatisation du système de santé » de l'association DELIS - Droits Et Libertés face à l'Informatisation de la Société [Del], le rapport du Conseil national de l'ordre des médecins [CNO05] ou le dossier de la revue « Pratiques » sur ce sujet, notamment [Mar00]). La mise en oeuvre du dossier médical personnel est d'une actualité brûlante sur le plan juridique et cela depuis la création en 2005 du groupement chargé de sa mise en oeuvre. En effet, le gouvernement a approuvé la constitution de ce GIP - arrêtés des 11 avril et 28 décembre 2005 - qui s'intitule depuis l'arrêté du 6 juillet 2006 « groupement d'intérêt public du dossier médical personnel » (GIP DMP). C'est cet organisme qui fait état des besoins d'évolution des normes pour répondre aux nécessités techniques de l'outil DMP. Pour y satisfaire, le gouvernement a successivement pris le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et le décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique. Est préparé la publication pour mi-2008 du décret identifiant (relatif aux conditions dans lesquelles un identifiant peut être utilisé pour l'ouverture et pour la tenue du DMP) et du décret relatif aux conditions d'accès aux différentes catégories d'informations qui figurent au DMP. De plus, certaines mesures étant de nature législative, ce sont respectivement la loi n° 2007-127 du 30 janvier 2007 « ratifiant l'ordonnance no 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions » et la loi n° 2007-1786 du 19 décembre 2007 « de financement de la sécurité sociale pour 2008 » qui ont servi de véhicule législatif. Ainsi, la loi du 30 janvier 2007 dispose de la prise en charge des patients en cas d'urgence, de la convergence entre le DMP et le dossier pharmaceutique, de l'adoption d'un identifiant de santé et donne une base légale pour la tarification des hébergeurs de données. Quant à la Loi de financement de la sécurité sociale 2008, elle dispose notamment de la création d'un service unique d'accueil dématérialisé, dénommé « portail du dossier médical personnel ».

Ces questionnements débordent largement le seul droit des données personnelles et concernent tout à la fois le droit de la santé, au travers, notamment de la régulation des organismes de sécurité sociale et de la relation particulière liant le patient à son médecin, mais également le droit des marchés publics, qui est amené, au moins indirectement, à prendre en considération des aspects techniques. Ils concernent également l'informatique, qui se trouve entraînée, par les contraintes juridiques, dans certains de ses retranchements les plus actuels à la fois dans le domaine des bases de données et dans celui de la cryptographie.

Les informations de santé font clairement partie des données qualifiées de sensibles par notre droit et appellent, de ce fait, des précautions particulières dans les divers traitements dont elles sont susceptibles de faire l'objet. En plus de problèmes bien identifiés (mais parfois encore mal résolus voire complètement ouverts) comme celui de la protection de la confidentialité d'une base de données ou de celui de l'identification des différents acteurs du système, la mise en place de dossiers de santé informatiques nécessite notamment la définition d'une politique complexe de contrôle d'accès, par exemple un contrôle d'accès d'ordre « sémantique » qui permette au patient de masquer toutes les informations relevant d'une pathologie donnée. La protection du journal enregistrant l'ensemble des informations sur les requêtes effectuées sur la base de données, journal indispensable tant sur le plan technique que juridique, pose également des problèmes cruciaux puisqu'il s'agit du seul moyen dont dispose le patient pour savoir quel professionnel a accédé à son dossier et quelles données il a

consultées. La mise en place d'un tel journal nécessiterait des politiques de confidentialité et de contrôle d'accès très strictes. Il pourrait être la source de problèmes de performances, étant l'objet d'un grand nombre de requêtes. Son existence même modifie peut-être radicalement les possibilités d'engagement de la responsabilité des médecins dans la mesure où il devient possible de déterminer exactement quelles informations celui-ci a consulté pour établir son diagnostic.

Les données de santé, plus que bien d'autres, touchent l'intimité de la vie privée des personnes, mais elles sont également précieuses pour la collectivité. Elles permettent notamment de mettre en place des systèmes de prévention, d'améliorer les connaissances épidémiologiques, mais aussi de gérer plus rationnellement les dépenses publiques de santé, même si ce dernier objectif est souvent présenté comme accessoire. Tout ceci implique, aussi bien du point de vue juridique qu'informatique, de ménager au mieux la coexistence de valeurs parfois contradictoires.

La mise en évidence des exigences juridiques portant sur les données de santé et leur confrontation aux spécificités techniques de leur gestion informatique est donc l'enjeu principal de ce projet de recherche. En effet, dire qu'un système est sûr signifie que son comportement est conforme aux spécifications, même en présence d'un utilisateur ou d'un tiers malintentionné. Ainsi, avant d'étudier et d'analyser la sécurité d'un système, il est indispensable d'avoir une compréhension claire des fonctionnalités que ce système est censé apporter (et également d'identifier les différents types de menaces qui peuvent mettre à mal sa sécurité). Sécuriser un dossier de santé n'a donc de sens que si les contraintes juridiques qui lui sont appliquées sont clairement définies et analysées. Dans ce sens, le premier objectif de ce projet est, à travers des lectures croisées entre juristes et informaticiens, de confronter les textes juridiques régissant les différents aspects du droit liés aux dossiers médicaux à l'état de l'art dans le domaine de la sécurité informatique. Cette mise à plat des contraintes d'un point de vue informatique et juridique devrait ensuite permettre d'évaluer l'adéquation des solutions existantes et d'identifier un certain nombre de barrières technologiques. A travers l'exploration de solutions émergentes, cette étude pourra ensuite donner lieu à certaines pistes de solutions techniques.

Ces travaux sont à nos yeux essentiels pour les informaticiens chargés de mettre en œuvre des systèmes de ce type, pour le législateur qui doit déterminer si les textes en vigueur peuvent être appliqués concrètement et s'ils garantissent une protection suffisante, mais aussi pour le citoyen désireux de connaître le niveau de sécurité offert tant juridiquement que techniquement par son dossier médical informatisé. L'information du public sur la sécurité réelle des dossiers de santé ainsi que l'amélioration de cette dernière, tant au plan technique que juridique, dans le cadre d'un chantier juridique encore en construction, le dossier médical personnel, sont donc des objectifs concrets affichés par notre recherche. Le projet inclut une opération de concertation structurée, ouverte au public, mobilisant les acteurs de la société civile (associations de médecins, de patients et d'usagers du système de santé) et experts dans un dialogue constructif. Cette opération permettra de surmonter les difficultés de compréhension et de recueillir un paysage des positions qui s'expriment sur les grands problèmes et pistes de solutions esquissées dans le projet.

A la complexité des systèmes techniques envisagés répond l'importance des enjeux économiques liés au développement du DMP (coût, gains espérés, etc.). Ainsi l'investissement consacré au seul DMP s'élève à 1 milliard d'euros sur la période 2006-2010. Cet investissement sera accompagné d'une politique de mise en cohérence des financements des projets de santé visant à la compatibilité avec le DMP. Il s'inscrit dans un budget global de systèmes d'information de santé de 2,3 milliards d'euros par an.

L'informatisation des dossiers médicaux est par ailleurs un sujet d'actualité dans de nombreux pays, qui a donné lieu à divers développements dans le domaine de la sécurité informatique. On peut notamment citer les travaux menés à la demande de la British Medical Association par Ross Anderson sur la définition d'une politique de sécurité dédiée aux applications médicales [And96] ou encore le lancement prochain par le géant américain Google de « Google Health », plateforme destinée à recueillir les données de santé de ses usagers. La comparaison avec des études et projets menés dans

d'autres pays sera d'ailleurs abordée au cours de nos recherches. Toutefois, le fait que les pays concernés aient des législations très différentes nécessite clairement des travaux spécifiques à la France intégrant l'ensemble des textes juridiques qui encadrent l'informatisation des dossiers médicaux.

Différents projets liés à la sécurité dans le domaine de la santé ont également vu le jour récemment. Par exemple, le projet « PlugDB – dossier personnel nomade et sécurisé » labellisé en 2006 par le Réseau national en technologies logicielles regroupe des spécialistes de sécurité des bases de données (en particulier l'équipe-projet SMIS de l'INRIA, également partenaire de DEMOTIS), une entreprise experte en informatisation des réseaux de soins et une association de médecins. Toutefois, le projet PlugDB est consacré à la gestion de dossiers médicaux « portables », c'est-à-dire embarqués dans un composant sécurisé, alors que les dossiers médicaux comme le DMP suivent a priori une architecture centralisée de type client-serveur (même si cette option a été récemment remise en cause dans le rapport d'information du député Jean-Pierre Door [Doo08]). Par ailleurs, PlugDB ne traite pas des aspects juridiques, qui sont une des spécificités de notre projet.

#### Références :

- [And96] R. Anderson. "A Security Policy Model for Clinical Information Systems". Proceedings of the 1996 IEEE Symposium on Security and Privacy, pages 30-43, mai 1996.
- [CNI03] CNIL, Délibération n° 03-053 du 27 novembre 2003 portant adoption d'une recommandation relative aux traitements de données à caractère personnel mis en œuvre par les registres du cancer.
- [CNI99] CNIL, « Rapport relatif aux modalités d'informatisation de la surveillance épidémiologique du SIDA – à propos de la déclaration obligatoire de la séropositivité au virus de l'immunodéficience humaine ». Rapport adopté le 9 septembre 1999.
- [CNO05] Conseil National de l'Ordre des médecins, « Questions sur l'informatisation des dossiers médicaux, le partage et l'hébergement des données, rapport adopté le 18 juin 2005.
- [Del] DELIS – association « Droits Et Libertés face à l'Informatisation de la Société », <http://www.delis.sgdg.org/>.
- [Doo08] Rapport d'information N°659, Enregistré à la Présidence de l'Assemblée nationale le 29 janvier 2008, déposé par la Commission des Affaires Culturelles, Familiales et Sociales, sur le dossier médical personnel, et présenté par M. Jean-Pierre DOOR, Député.
- [IC03] IPSOS Santé / CNAM, « Opinions et attitudes des médecins et des patients à l'égard du Dossier médical partagé », octobre 2003.
- [Mar00] A. Marcheix. « Comment préserver la confidentialité du dossier de santé », Pratiques n°12, pages 30-33, décembre 2000-janvier 2001

### 1.3 Objectifs et caractère ambitieux/novateur du projet. *Specific aims of the proposal, highlighting the originality and the novelty (1 à 2 pages maximum)*

*Décrire les objectifs scientifiques/techniques du projet.*

*Présenter l'avancée scientifique attendue. Préciser l'originalité et le caractère ambitieux du projet.*

*Détailler les verrous scientifiques et techniques à lever par la réalisation le projet.*

*Décrire éventuellement le ou les produits finaux développés à l'issue du projet montrant le caractère innovant du projet.*

L'ambition du projet DEMOTIS est de développer et de mettre en oeuvre une démarche novatrice par son caractère pluridisciplinaire pour la conception des grandes infrastructures de données opérant dans des cadres juridiques et sociétaux complexes. Ce type d'approche des méthodes de conception technique est rendu nécessaire par l'émergence dans des domaines très divers (santé, multimédia, militaire etc.) d'infrastructures de grande ampleur où se traitent et s'échangent des données numériques sensibles (par exemple les données dites « personnelles »).

L'originalité du projet DEMOTIS est sa démarche qui consiste à aborder conjointement les aspects juridiques et informatiques des problèmes de sécurité des dossiers médicaux informatisés. Ceci est essentiel d'abord parce que seule une mise à plat des contraintes juridiques émanant des différents domaines du droit peut permettre de définir des spécifications techniques précises et de formuler des recommandations pertinentes du point de vue de la sécurité. Ensuite, le fait d'aborder de

concert les aspects juridiques et informatiques peut apporter des réponses à des questions que l'on ne peut résoudre si on ne tient compte que d'un de ces deux domaines. Pour donner un exemple, le modèle de sécurité classique utilisé en cryptographie impose des contraintes extrêmement lourdes (et souvent irréalistes) car il suppose a priori que chaque intervenant du système est potentiellement malveillant. Au contraire, le droit permet de définir des responsabilités (par exemple, le fait qu'un horodatage comme le cachet de la Poste soit présumé fiable) qui permettent d'envisager d'autres procédés que les protocoles cryptographiques classiques.

Nous pouvons dès à présent identifier quelques barrières technologiques ou juridiques rencontrées dans la mise en oeuvre des textes juridiques protégeant l'accès aux données personnelles de santé et leur usage. Nous serons en effet naturellement confrontés aux questions ouvertes suivantes:

- Peut-on mettre en oeuvre de façon sécurisée un contrôle d'usage des données plutôt qu'un contrôle d'accès classique, ce qui permettrait d'exprimer un consentement pour certains objectifs sans détailler quelles données interviennent ni les acteurs censés les utiliser ?
- Comment réaliser une fonctionnalité de masquage de certaines données de santé répondant simultanément aux contraintes de protection des droits du patient et aux situations d'urgence médicale ? Quel serait l'impact d'une telle fonctionnalité sur l'engagement de la responsabilité du médecin ?
- Par quel procédé est-il souhaitable d'identifier les patients afin d'éviter les inconvénients du NIR ?
- Comment peut-on « anonymiser » les données de façon qu'il ne soit pas possible d'identifier un individu par un recoupement de données qui ne contient pas son identifiant ?
- Comment protéger la confidentialité des données tout en conservant la possibilité d'effectuer aisément des requêtes dans la base ?
- Comment assurer la traçabilité des accès aux données pour le patient et quelles conséquences aura cette fonctionnalité sur l'engagement de la responsabilité des professionnels de santé d'une part et sur les rapports entre le patient et son médecin ?
- Comment parvenir à assurer à la fois la robustesse d'une base de données et à garantir le droit à l'oubli ? Quelles pourraient être les options juridiques envisagées pour aboutir à un compromis entre ces deux notions ?

Répondre à chacune de ces questions va nécessiter de lever un verrou scientifique dans les domaines de la sécurité ou des bases de données.

Au niveau de la méthodologie, l'interdisciplinarité ne doit pas être considérée, dans le montage de ce projet, comme un verrou. Les équipes participantes dans DEMOTIS ont, pour certaines d'entre elles (CECOJI – INRIA) déjà travaillé ensemble lors du projet Asphales ([www.asphales.net](http://www.asphales.net)). Tous les acteurs de cette recherche ont, en outre, développé une culture des rapports interdisciplinaires leur permettant de franchir rapidement les obstacles qui jalonnent généralement les débuts de ce type d'expérience (notamment mise en commun d'un vocabulaire). En outre, le choix effectué de fonder le travail commun sur les textes de droit applicables aux dossiers de santé permet d'avoir comme socle des documents qui, de par leur généralité, ont vocation à s'appliquer à chacun d'entre nous, et dont les lectures croisées permettront de mettre en lumière les avantages et les incohérences. Au plan juridique, la coopération envisagée entre une équipe de spécialistes des questions de protection des données personnelles et de la propriété intellectuelle (le CECOJI) et une maître de conférence dont les travaux en matière de droit de la santé et de la sécurité sociale font référence (Anne-Sophie Ginon), est le gage d'une prise en considération globale des problématiques suscitées par les dossiers de santé. Par ailleurs, le fait que le CECOJI soit adossé, dans son fonctionnement quotidien, aux travaux et aux expertises du GDR « Réseau Droit, Sciences et Techniques » permet aux chercheurs juristes prenant part à ce projet de bénéficier, au-delà de leurs recherches propres, des résultats et de la coopération des membres de ce réseau, dont les compétences sont très étendues.

Enfin, le projet permettra la réalisation d'une plateforme web de commentaires de texte web 2.0 spécifiquement adaptée au travail collaboratif pluridisciplinaire sur les enjeux techniques et juridiques. Le point de départ de cette réalisation est un logiciel existant et opérationnel (cf. <http://www.co-ment.net>) qui est lui-même le produit des efforts de R&D interne du partenaire industriel (Sopinspace) de DEMOTIS. En faire un outil pertinent pour l'annotation de textes

techniques et juridiques est un travail significatif mais réaliste. Comme pour l'existant, la base logicielle du nouvel outil sera publiée sous une licence libre spécifiquement adaptée aux services Web (Affero GPL3) permettant sa réutilisation dans d'autres contextes mais aussi la poursuite de son développement.

#### **1.4 Positionnement du projet. *Progress beyond the state of the art and relevance to the call for proposals* (1 page maximum)**

*Préciser :*

- *positionnement du projet par rapport au contexte développé précédemment : vis-à-vis des projets concurrents, de l'état de l'art national et international, des brevets et standards...*
- *positionnement du projet par rapport aux axes thématiques de l'appel à projets*

Le présent projet s'inscrit dans l'axe thématique 5 : « sûreté, sécurité et outils associés ». Plus particulièrement, les problématiques techniques et juridiques liées à la sécurité des bases de données d'informations sensibles au coeur de vastes architectures techniques sont l'objet de la recherche du projet. DEMOTIS apporte également une contribution significative à l'axe thématique 6 (systèmes d'information et technologies Web) notamment à travers le développement d'une technologie Web 2.0 fournissant un nouveau type de support à l'intelligence collective appliquée à des documents structurés. Enfin, il présente une pertinence pour l'axe thématique 4 (méthodes et outils logiciels de spécification, modélisation, validation et optimisation) à travers la mise en point d'une méthode de mobilisation de compétences multidisciplinaires dans le cycle de développement de grandes infrastructures de traitement d'information.

Les spécificités du projet DEMOTIS vis-à-vis des divers projets évoqués précédemment concernent la portée de ses objets d'étude, la nature de ses productions ainsi que les méthodes de travail.

Le projet se focalise sur les architectures centralisées et interconnectées et particulièrement sur les problématiques spécifiques que ce type d'architecture pose à la question de la sécurité : vulnérabilité due à la centralisation des données, besoin de performance en ce qui concerne la sécurité (composant technique coûteux sur ce plan) etc..

Les travaux du projet DEMOTIS se positionnent comme relevant de la recherche amont (recherche fondamentale dans la nomenclature des projets ANR). Toutefois, le résultat de cet effort de recherche sera pour partie résolument tourné vers les applications de par la production de documents destinés à être intégrés au cycle de conception de systèmes concrets et du fait de l'exploitation dérivée par le partenaire industriel du service Web 2.0 d'annotation de textes juridiques et techniques

Du fait de l'effort international autour de ce type de problématiques, les études détaillées des systèmes techniques (en place ou en projet) qui seront menées lors de la première phase du projet DEMOTIS devront être étendues au delà du champ national. Toutefois, la prise en compte des textes normatifs encadrant la gestion automatisées de données de santé, originalité de DEMOTIS implique un ancrage du projet dans le contexte de la loi française.

#### **1.5 Description des travaux : programme scientifique et technique. *Detailed description of the work. For each specific aim: a proposed workplan should be described (including preliminary data, work packages and deliverables).* (10 pages maximum)**

*Décrire le programme de travail décomposé en tâches en cohérence avec les objectifs poursuivis. Les tâches représentent les grandes phases du projet. Elles sont en nombre limité. La décomposition en tâche doit être cohérente avec les tâches mentionnées dans le document de soumission A.*

*Pour chaque tâche, décrire :*

- *les objectifs de la tâche*
- *le programme détaillé des travaux par tâche*
- *la description des méthodes et des choix techniques et de la manière dont les solutions seront apportées*
- *les risques de la tâche et les solutions de repli envisagées*

WP#	Description
WP0	Coordination
WP1	Constitution et annotation du corpus juridique et développement des outils logiciels associés
WP2	Sécurité des données dans le cadre des grandes infrastructures
WP3	Analyse juridique et normative du domaine des données de santé
WP4	Concertation publique avec les associations de médecins et de patients autour des résultats de la recherche sur le DMP
WP5	Diffusion et exploitation des résultats

Tableau 1: Work-Packages du projet

## WP0 : Coordination

La coordination du projet est assurée par le partenaire industriel. Le responsable du projet (Project Manager) sera Philippe Aigrain, directeur et fondateur de la société. Comme responsable d'équipe de recherche (IRIT, 1986-1996) puis comme chef de secteur « technologies du logiciel » des programmes de recherche de la Commission européenne (ESPRIT puis IST, 1996-2003), il a acquis une expérience poussée de gestion de la recherche collaborative.

Le schéma de coordination du projet sera simple : un responsable pour chaque partenaire, agissant comme point de contact pour le chef de projet et participant au comité de pilotage. La coordination effective des activités sera largement facilitée par la localisation géographique proche des différents partenaires et par une répartition des rôles dans les différentes tâches qui limite les besoins de coordination et qui évite des dépendances excessives (tout en assurant la synergie quand elle est à la base du projet).

Les tâches essentielles de la coordination seront les suivantes :

- servir de point de contact unique avec l'ANR ;
- produire et transmettre à l'ANR tous les rapports (CR intermédiaires et CR scientifique final, information sur les publications et autres actions de diffusion des résultats) ;
- mettre en place les dispositifs de travail collaboratif interne au projet (extranet collaboratif, listes de diffusion) ;
- organiser la tenue des réunions du projet : lancement, réunions périodiques de comité de pilotage, réunions de revue du projet, etc. ;
- veiller à la bonne exécution du plan de travail et prendre les mesures nécessaires dès qu'apparaissent des retards ou risques ;
- produire et assurer la signature de l'accord de consortium ;
- mettre en oeuvre la politique de résolution de conflits si le besoin en survient ;
- veiller à l'exécution correcte du budget par les différents partenaires ;
- effectuer l'interface entre le projet et le pôle de compétitivité System@TIC ;
- produire et animer le site Web du projet (voir WP5).

Le choix résolu du projet en faveur d'une politique de diffusion ouverte de ses résultats limite les risques de conflits. Ce choix est fait y compris pour les résultats du partenaire industriel, avec des dispositifs adaptés de protection par les marques et licences qui ne bloquent pas la diffusion.

Néanmoins des conflits peuvent toujours surgir sur l'exécution du plan de travail. Le mécanisme de résolution sera le suivant :

- réunion du ou des partenaires concernés avec le responsable de projet pour parvenir à une solution ;

- s'il s'avère impossible de trouver une solution ou que celle-ci nécessite une réorganisation du plan de travail, réunion du comité de pilotage, tranchant à la majorité qualifiée de trois partenaires ou un partenaire et le coordinateur ;
- au cas où les décisions prises entraînent une modification significative de la géométrie du projet, l'ANR sera notifiée.

Tâche	Description	Livrables	Partenaire leader
T0	Reporting	L0, L1	Sopinspace
T1	Communication interne	L2	Sopinspace

Tableau 2: Tâches du WP0

Livrable	Description	Date
L0	Rapports périodiques (5)	M7 – M12 – M18 – M24 – M30
L1	Rapport final	M36
L2	Intranet du projet	M3 – M36 (interne)

Tableau 3: Livrables du WP0

## **WP1 : Constitution et annotation du corpus juridique et développement des outils logiciels associés**

Les équipes du projet seront, durant les 3 années de celui-ci, divisées en deux pôles : juristes du CECOJI et informaticiens de l'INRIA.

Une première phase menée par l'équipe du CECOJI sera consacrée à la constitution du corpus juridique. Puis les deux pôles entameront un travail collaboratif de lecture croisée, chacun apportant son expertise sur ses thématiques propres pour éclairer le socle commun de textes juridiques.

Sur la base d'une lecture autonome selon un calendrier propre, les travaux de ces deux pôles seront régulièrement confrontés, par l'intermédiaire de réunions de travail communes permettant de faire le point sur les avancées de chacun. Nous souhaitons également mettre en place des séminaires d'études réservés aux doctorants et post-doctorants de nos équipes de recherches respectives dans le but de diffuser dans nos communautés respectives les éléments méthodologiques et les résultats de nos travaux interdisciplinaires.

Ces réunions internes consistent en une mise à plat de ces textes juridiques, effectuée en procédant à une lecture commune des juristes et des informaticiens pour faire ressortir :

- les points touchant à une demande de sécurité sur lesquels il y a besoin de s'expliquer de part et d'autre ;
- les divergences de compréhension et/ou le double sens des termes et concepts utilisés.

En termes plus concrets, il s'agit de commenter les textes lus ensemble et d'utiliser les matériaux que nous fournissent nos incompréhensions mutuelles et nos explications pour tenter de faire évoluer nos domaines d'expertise respectifs.

Le support technique de cette étude sera un système Web d'annotation de texte basé sur le logiciel co-ment (<http://www.co-ment.net>) issu d'un effort de R&D du partenaire industriel (Sopinspace) du projet.

Les développements d'adaptation à l'annotation de textes techniques et juridiques prévus seront réalisés par le partenaire industriel du projet en collaboration avec les équipes de recherche. Ils portent notamment sur les fonctionnalités :

- de typage et traitement des commentaires adaptés à la nature juridique (ex : jurisprudence) ou technique des textes commentés ;
- de présentation (des textes commentés comme des commentaires)
- de présentation et d'exploration du corpus ;
- d'export sous une version statique de la totalité du travail.

Ce travail s'effectuera en deux phases :

- une phase de spécification et développement des nouvelles fonctionnalités qui se déroulera en parallèle avec la constitution du corpus (M3-M12) ;
- une phase de suivi, support et adaptation pendant le cours de l'annotation (M13-M30).

La diffusion en logiciel libre (sous la licence déjà utilisée pour la base logicielle du service existant aura lieu à plusieurs étapes à partir de la mise en service opérationnel (M13). Cette diffusion précoce est nécessaire à la stratégie de diffusion et d'exploitation industrielle future du projet (cf. WP5).

Les commentaires de concepts, mots-clefs, phrases, etc. serviront de base à la communication externe des résultats de nos recherches. Ils serviront également de base aux travaux de chacun, en nous fournissant les moyens de faire avancer les connaissances dans nos domaines de compétence respectifs. Il va de soi que les résultats de ces travaux personnels, qu'il s'agisse de nouvelles fonctionnalités techniques ou de propositions doctrinales d'amélioration des textes, devront également faire l'objet de lectures croisées.

Au cours de nos travaux, nous confronterons les résultats de nos recherches avec les points de vue des praticiens (médecins, patients, etc.) des dossiers de santé, mais également avec le regard de chercheurs en droit et en informatique ayant abordé ces mêmes questions dans le cadre d'autres systèmes juridiques (notamment au Royaume-Uni et en Belgique, qui ont déjà mené des expériences d'informatisation des dossiers de santé similaires).

Tâche	Description	Livrables	Partenaire leader
T2	Constitution et commentaire du corpus juridique par les équipes de recherche de juristes et d'informaticiens	L3	CECOJI
T3	Développement et adaptation du logiciel du système d'annotation	L4	Sopinspace

Tableau 4: Tâches du WP1

Livrable	Description	Date
L3	Corpus juridique commenté conjointement par les équipes de recherche de juristes et d'informaticiens	M3 – M30
L4	Logiciel (cf. L12 pour la diffusion en logiciel libre) de commentaire de texte juridique et technique Web 2.0	M3- M24

Tableau 5: Livrables du WP1

## WP2 : Sécurité des données dans le cadre des grandes infrastructures

Les exigences introduites par la législation en matière de protection des données à caractère personnel en général (ex : consentement éclairé du porteur des données, droit à l'oubli, information du porteur relatives aux accès et à l'usage de ses données), et des données de santé en particulier, ne

rencontrent pas toujours de moyens effectifs de mise en œuvre dans l'état actuel de la technologie informatique. Devant ce constat, l'objectif du Work-package WP2 est double. Le premier objectif consiste à confronter les textes juridiques régissant l'utilisation des données à caractère personnel (et principalement données de santé) à l'état de l'art dans le domaine de la sécurité informatique. La mise à plat des contraintes d'un point de vue informatique et juridique est essentielle pour la définition des spécifications techniques d'un système et peut s'avérer particulièrement fructueuse. Ainsi la sécurité juridique (à travers la définition de la responsabilité de certains acteurs, par exemple) peut pallier une impossibilité technique. Inversement, la sécurité technique peut, dans certains cas, remédier aux lacunes des textes applicables, comme l'ont déjà démontré, par le passé, les travaux interdisciplinaires effectués dans le cadre du programme Asphales précité. Le deuxième objectif consiste à s'appuyer sur les compétences des partenaires informatiques du projet DEMOTIS pour évaluer l'impact de technologies émergentes (ex : nouveaux algorithmes cryptographiques, nouveaux composants matériels sécurisés, bases de données embarquées, SGBD Hippocratique) sur la satisfaction des exigences attendues par les textes juridiques. Ces deux objectifs sont poursuivis respectivement dans les tâches T4 et T5 décrites ci-dessous.

### **Tâche T4 : Confrontation des exigences techniques et juridiques**

Cette section donne une première illustration des barrières technologiques pouvant être rencontrées dans la mise en œuvre des textes juridiques protégeant l'accès aux données personnelles de santé et leur usage. Cette liste ne prétend pas à l'exhaustivité. C'est justement l'objectif de la tâche T4 de la compléter et d'identifier un certain nombre de carences génératrices de futurs travaux pour la communauté des juristes comme pour celle des informaticiens.

#### *Contrôle d'accès et contrôle d'usage*

Un aspect central de la sécurité d'un système d'information est la définition d'une politique de contrôle d'accès, régissant *qui* est autorisé à faire *quoi* sur *quelles données* et dans *quel contexte*. Établir cette politique dans un système d'information de santé est d'autant plus complexe que le nombre d'acteurs est grand (patients, médecins, infirmiers, pharmaciens, personnels administratifs, organismes de sécurité sociale, hébergeurs etc.), que les données de santé sont souvent obscures pour le patient qu'elles concernent, qu'il est reconnu à ce même patient le pouvoir d'autoriser ou d'interdire l'accès à certaines de ces données et que ces règles peuvent être contextuelles (exemple du bris de glace en situation d'urgence).

La législation applicable impose un certain nombre de règles d'accès aux données. Les acteurs de sa mise en œuvre (typiquement, dans le cadre du DMP, le Groupement d'Intérêt Public mis en place en 2005) prévoient par ailleurs l'adoption de nomenclatures techniques sur la base d'un découpage du dossier médical en thèmes et d'une répartition des rôles pour les acteurs. Un patient peut légitimement exiger une granularité plus fine, par exemple pour distinguer des droits particuliers en fonction de la confiance apportée à chaque acteur ou de la sensibilité de certaines information (par exemple, viol, avortement, pathologie telle que le SIDA), voire pour masquer totalement certaines parties de son dossier [Fag07]. Hélas, les règles de contrôle d'accès sont aujourd'hui très « syntaxiques », obligeant à connaître la structure des données à protéger [DDP+02], et l'on est loin d'un contrôle « sémantique » (ex : masquer toute donnée révélant la pathologie X). On peut donc estimer que les solutions mises en œuvre actuellement ne sont pas aptes à permettre un consentement éclairé du patient sur la façon dont ses données sont partagées.

#### *Identification des acteurs*

La mise en place d'une politique de contrôle d'accès sous-entend la capacité d'identifier et d'authentifier tous les utilisateurs du système d'information. L'identification/authentification des professionnels de santé est aujourd'hui résolue par l'usage des cartes professionnel de santé (CPS). Par contre, l'identification des patients reste une question cruciale. La loi 2007-127 du 30 janvier 2007 [Loi07] définit dans son article 25, un « identifiant de santé » utilisé « pour la conservation, l'hébergement et la transmission des informations de santé ». Cet identifiant doit être défini par décret, mais le communiqué de la CNIL en date du 20 février 2007 [CNI07], souligne que le NIR (Numéro

d'Inscription au Répertoire national d'identification des personnes physiques, communément appelé numéro de sécurité sociale) « compte tenu de son usage répandu, du fait qu'il est signifiant et facile à reconstituer [...], ne constitue pas, aujourd'hui un numéro adapté pour identifier le dossier médical de chacun ». La CNIL recommande alors l'utilisation d'un « identifiant de santé spécifique, généré à partir du NIR [...] mais transcodé selon des techniques reconnues d'anonymisation ». La question de l'irréversibilité et du coût de la transformation du NIR en identifiant de santé reste aujourd'hui une question ouverte adressée aux cryptographes.

### *Protection contre les attaques externes et internes*

Les données doivent être protégées contre (1) des fuites par négligence (ex : perte récentes de données financières concernant 25 millions de citoyens Britanniques [BBC]), (2) des attaques externes (tentatives de piratage depuis l'extérieur) et (3) des attaques internes (actions malveillantes provenant de personnes ayant un accès autorisé à tout ou partie du système) [CuPu06]. Les attaques internes ne doivent pas être négligées car, comme l'atteste le rapport « Computer crime and security survey » établi par le FBI et le Computer Security Institute [CSI05], elles représentent plus de la moitié des attaques menées contre les serveurs de base de données et sont particulièrement difficiles à contrer. Le risque est encore accru lorsque les données sont hébergées par des tiers. La protection des données passe par leur chiffrement lors des communications et du stockage sur le serveur [IBM03, Ora02b, Mat04]. Ce dernier point introduit un problème crucial de performance du fait du volume de données impliqué et du besoin impérieux de performance dans le traitement des requêtes bases de données. Par ailleurs, si le chiffrement des données stockées permet de résister à des attaques menées contre l'empreinte disque de la base de données, il reste inopérant contre des attaques internes espionnant le fonctionnement du serveur pendant l'exécution des requêtes. En effet, les mécanismes usuels déchiffrent les données sur le serveur au moment de leur interrogation. Résister à de telles attaques impose de déporter le chiffrement/déchiffrement sur les postes clients [HIL+02], introduisant de nouvelles contraintes en terme de performance et de partage sélectif des données. Se pose également le problème fondamental de la protection des données dès lors qu'elles ont quitté la zone sécurisée du serveur. Par exemple, quelle garantie de sécurité peut être fournie pour des fragments de dossiers extraits du serveur et stockés sur le terminal du professionnel de santé a priori vulnérable et cible potentielle de nombreuses attaques ? Autant de questions ouvertes à destination des cryptographes et des spécialistes de bases de données.

### *Traçabilité des accès*

Un individu qui fait l'objet d'une collecte de données personnelles se voit offrir un droit d'audit lui permettant d'identifier quels acteurs ont eu accès à ses données et pour y voir quoi. Aujourd'hui, les systèmes d'audit mis à disposition des patients semblent se limiter à indiquer qui s'est connecté sur leur dossier, sans indication sur les données qui ont été consultées. Tout Système de Gestion de Bases de Données (SGBD) dispose pourtant d'un outil appelé journal mémorisant l'activité précise de la base de données et permettant de retrouver cette information. Se posent alors plusieurs problèmes encore peu abordés dans l'état de l'art. Le premier concerne la gestion des droits d'accès sur ce journal, aujourd'hui accessible uniquement par l'administrateur de la base de données ou par un organisme d'audit mandaté. Par ailleurs, l'interprétation du contenu d'un journal est une opération complexe, nécessitant un langage d'interrogation particulier [ABF+04], probablement hors de portée d'un individu non informaticien. Le pendant d'une telle fonctionnalité est également la possibilité d'engagement de la responsabilité d'un médecin en cas d'actions erronées sur le dossier d'un patient (par exemple, non consultation d'une information majeure pour l'établissement du diagnostic).

### *Durée de rétention des données*

Fixer une limite maximale à la période de rétention des données est un principe fondateur de la législation protégeant les données à caractère personnel. Ce principe doit garantir qu'une donnée sera physiquement détruite une fois passée sa « date de péremption ». Il s'agit en fait de garantir le droit à l'oubli, dont le principe même fait débat dans le cadre des dossiers de santé. Il a été montré que les

SGBD actuels gardent de multiples traces des données après une opération de destruction [MLS07] et que ces traces sont particulièrement difficiles à effacer et souvent indélébiles. Par exemple, les données sont généralement marquées comme détruites plutôt que d'être physiquement effacées pour des raisons de performance. Même lorsqu'elles sont effacées, il est fréquent que les index permettant de retrouver ces données efficacement ne soient pas mis à jour, à nouveau pour des raisons de performance. Enfin, une trace des données est gardée dans des journaux ou logs afin d'assurer la propriété de durabilité des données, c'est-à-dire la capacité du système à restaurer une base de données cohérente et complète après une panne. Il est donc raisonnable de penser qu'aujourd'hui, aucun SGBD n'est réellement capable de supporter techniquement le droit à l'oubli.

D'autres barrières technologiques apparaîtront naturellement à partir de nos lectures croisées entre juristes et informaticiens, et en fonction de l'évolution du cadre législatif. Le résultat de cette tâche sera la production du livrable L5 détaillant l'ensemble des barrières technologiques identifiées.

### **Tâche T5 : Exploration de nouvelles solutions technologiques**

Le projet DEMOTIS n'a pas la prétention de lever définitivement les barrières technologiques identifiées dans la tâche T4, chacune représentant des efforts de recherche considérables, souvent à la frontière de plusieurs thématiques scientifiques. Par contre, les partenaires informaticiens du projet ont des compétences en cryptographie et en bases de données qui leur permettent d'identifier des technologies émergentes dans ces deux domaines, d'en proposer également qui leur sont propres, et d'évaluer la pertinence de ces technologies pour répondre à certains problèmes identifiés, en concertation avec les partenaires juristes. Nous indiquons ci-dessous certaines pistes qui méritent d'être explorées dans cette tâche.

#### *Nouveaux composants matériels sécurisés*

Le domaine des composants sécurisés portables a connu récemment une profonde évolution avec l'apparition des Secure Portable Token, associant dans un même facteur de forme la sécurité intrinsèque d'une carte à puce (microcontrôleur sécurisé), la capacité de stockage d'une clé USB (à terme plusieurs Giga-octets) et l'universalité et le débit du protocole USB. De tels composants peuvent servir des objectifs allant bien au-delà d'un mécanisme d'authentification forte, en permettant notamment de réaliser de véritables dossiers portables sécurisés, avec des applications évidentes dans le domaine médical mais plus généralement dans la gestion de tout type de données personnelles. De telles technologies peuvent avoir un impact significatif (1) sur la façon d'échanger des informations sensibles entre acteurs en apportant un meilleur contrôle du porteur des données, (2) sur la façon d'assurer le droit au masquage (et au masquage du masquage) évoquée dans le rapport du député Pierre-Louis Fagniez [Fag07], et (3) sur la façon d'auditer les accès réalisés sur un dossier, répondant ainsi à certains problèmes soulevés dans la section précédente.

Une telle réflexion prospective s'inscrit bien dans le cadre du rapport d'information du député Jean-Pierre Door [Doo08] sur la relance du programme DMP, préconisant « l'expérimentation d'un dossier médical personnel crypté et sécurisé sur un support de type mémoire flash USB ». Cette réflexion peut également se nourrir d'une expérimentation terrain [DMSP-web] conduite dans le département des Yvelines en relation avec un des partenaires du projet DEMOTIS. Cette expérimentation vise l'implantation d'un dossier médico-social nomade et sécurisé facilitant la coordination des soins au domicile des personnes dépendantes. Dans ces deux exemples, le composant de type Secure Portable Token constitue la clé de voûte d'une architecture offrant de nouveaux usages qu'il convient de confronter aux exigences techniques et juridiques évoquées précédemment.

#### *Nouvelles solutions cryptographiques*

Les différentes études que nous avons menées montrent qu'il est particulièrement difficile de concevoir des SGBD conciliant performance et haute résistance aux attaques. Les techniques développées dans la communauté base de données permettent de réaliser des SGBD performants mais malheureusement peu résistants aux attaques. Les algorithmes et protocoles cryptographiques

classiques exhibent, eux, de fortes propriétés sécuritaires mais génèrent parallèlement d'importants problèmes de performance lorsqu'ils sont utilisés dans un contexte de bases de données. La définition de techniques cryptographiques (chiffrement, intégrité, authenticité, complétude, version) applicables au contexte des bases de données (volume de données considérable mais accès à un grain fin, interrogation assertionnelle, règles de partage complexes et évolutives, haut débit transactionnel) constitue aujourd'hui un véritable challenge. La quantité et la granularité des données manipulées conditionne le choix des algorithmes de chiffrement, hachage, signature utilisés et/ou pousse au développement de nouveaux algorithmes. Par exemple, des avancées récentes ont été effectuées dans le domaine du chiffrement symétrique, telles que les nouvelles propositions de chiffrement à flot faites dans le cadre du projet européen eSTREAM [ECR05] ou les travaux sur les chiffrements par blocs opérant sur des blocs de petite taille [GP07].

De nouvelles solutions cryptographiques peuvent également apporter des solutions au problème de l'identification des patients posé par la CNIL. On peut par exemple imaginer une transformation du NIR en identifiant de santé soit irréversible, soit réversible mais avec une complexité d'inversion élevée, ce qui pourrait suffire à rendre le croisement de fichiers indexés par le NIR et par l'identifiant de santé infaisable en pratique car trop coûteux en temps de calcul. Ainsi, la définition précise des fonctionnalités attendues en fonction de l'état du droit conditionne clairement le choix de la solution cryptographique (fonction de hachage, chiffrement symétrique, chiffrement asymétrique...).

### *Nouvelles générations de SGBD*

Le concept de SGBD Hippocratique [AKS+02], à savoir donnant l'assurance du respect d'un serment de confidentialité, a été introduit, se basant sur les directives de l'ONU concernant la gestion de données personnelles. Un tel SGBD est notamment tenu de respecter 10 principes fondateurs parmi lesquels : préciser l'objectif d'utilisation de chaque donnée collectée sur un utilisateur, recueillir l'assentiment de ce dernier sur cet objectif, ne stocker que l'information strictement nécessaire à l'atteinte de cet objectif et pendant le laps de temps adéquat, ne pas divulguer cette information à des tiers sans autorisation préalable de l'utilisateur, donner à l'utilisateur la possibilité de consulter les informations qui le concernent et enfin offrir des outils permettant à un tiers de contrôler que ces principes sont bien respectés. Ces travaux vont donc dans le sens d'une meilleure prise en compte des principes législatifs dès la conception des noyaux de SGBD. Cependant, un long chemin reste à parcourir. Par exemple, comme discuté dans la section précédente, les SGBD commerciaux actuels n'ont pas été conçus pour détruire de façon irréversible une information précédemment stockée, rendant inapplicable le principe de droit à l'oubli. Se pose alors la question de savoir si le problème peut être contourné par une modification mineure des noyaux de SGBD ou si une réflexion plus fondamentale doit être menée. Des travaux en bases de données, en cryptographie (une façon de détruire l'information pouvant être de la chiffrer puis d'oublier la clé), mais aussi en droit doivent être menées pour combler la carence technologique actuelle. Rétention des données et traçabilité étant étroitement liées, on imagine également qu'une réflexion tant juridique que technologique doit être conduite pour réguler l'accès à des historiques d'information.

<b>Tâche</b>	<b>Description</b>	<b>Livrables</b>	<b>Partenaire leader</b>
T4	Confrontation des exigences techniques et juridiques	L5	INRIA
T5	Exploration de nouvelles solutions technologiques	L6	INRIA

*Tableau 6: Tâches du WP2*

Livrable	Description	Date
L5	Identification des carences technologiques à la mise en œuvre des textes juridiques sur les données à caractère personnel	M12
L6	Identification et impact des technologies émergentes en base de données et cryptographie sur la sécurité des données personnelles	Mois 36 (brouillon M30)

Tableau 7: Livrables du WP2

## Bibliographie pour le WP2 :

- [ABF+04] R. Agrawal, R. J. Bayardo Jr., C. Faloutsos, J. Kiernan, R. Rantzau, R. Srikant, "Auditing Compliance with a Hippocratic Database". *VLDB 2004*: 516-527, 2004.
- [AKS+02] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, "Hippocratic Databases", *28th International Conference on Very Large Data Bases (VLDB)*, 2002.
- [BBC] UK government loses personal data on 25 million citizens. <http://www.edri.org/edriagram/number5.22/personal-data-lost-uk>, 2
- [CNI07] CNIL, Communiqué du 20 février 2007 sur l'utilisation du NIR comme identifiant de santé.
- [CSI05] Computer Security Institute, "CSI/FBI Computer Crime and Security Survey", 2005.
- [CuPu06] F. Cuppens, P. Pucheral, "Sécurité des bases de données", chapitre de *l'encyclopédie informatique Vuibert*, éditions Vuibert, ISBN : 2-7117-4846-4, 2006.
- [DDP+02] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, "A Fine-Grained Access Control System for XML Documents", *ACM Transactions on Information and System Security (ACM TISSEC)*, (5)2, 2002.
- [DMSP-web] site web des projets DMSP/PlugDB, <http://www-smis.inria.fr/~DMSP>
- [Doo08] Rapport d'information N°659, Enregistré à la Présidence de l'Assemblée nationale le 29 janvier 2008, déposé par la Commission des Affaires Culturelles, Familiales et Sociales, sur le dossier médical personnel, et présenté par M. Jean-Pierre DOOR, Député.
- [ECR05] ECRYPT – European network of excellence in cryptology, « The eSTREAM Stream Cipher project », <http://www.ecrypt.eu.org/stream>, 2005.
- [Fag07] P.-L. Fagniez, "Le masquage d'informations par le patient dans son DMP", *Rapport au ministre de la santé et des solidarités*, [http://www.sante.gouv.fr/hm/actu/fagniez\\_dmp/rapport.pdf](http://www.sante.gouv.fr/hm/actu/fagniez_dmp/rapport.pdf), 30 janvier 2007.
- [GP07] L. Granboulan, T. Pornin, "Perfect Block Ciphers With Small Blocks", *Fast Software Encryption – FSE 2007*, Lecture Notes in Computer Science, à paraître.
- [HIL+02] H. Hacigumus H., B. Iyer, C. Li, S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model", *ACM International Conference on Management of Data (SIGMOD)*, 2002.
- [IBM03] IBM corporation. (2003), "IBM Data Encryption for IMS and DB2 Databases v. 1.1", 2003.
- [Loi07] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance no 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique.
- [Mat04] U. Mattsson, "Transparent Encryption and Separation of Duties for Enterprise Databases -A Solution for Field Level Privacy in Databases", *Protegrity Technical Paper*, 2004.
- [MLS07] G. Miklau, B. Levine, P. Stahlberg, "Securing history: Privacy and Accountability in Database Systems", *Conference on Innovative Data Systems Research (CIDR)*, 2007.
- [Ora02b] Oracle Corporation, "Oracle Advanced Security - Administrator's Guide", *Release 2 (9.2)*, Part No. A96573-01, 2002.

**WP3 : Analyse juridique et normative du domaine des données de santé**

Un système de gestion partagée des données de santé n'est pas un système de traitement de données personnelles comme les autres. Il traite des données qui sont communément qualifiées de données sensibles, car, comme le rappelait la CNIL le 10 juin 2004 [CNI04] au sujet du projet de loi relatif à la réforme de l'assurance maladie, « elles relèvent de l'intimité de la vie privée et doivent donc faire l'objet d'une protection particulière ». Ces données n'ont pourtant pas toujours été traitées de manière spécifique par la Loi Informatique et Libertés [Loi78]. Il importe donc de repérer les évolutions juridiques qu'a subi, depuis 1978, le concept même de données de santé. L'analyse de cette évolution pourra en effet permettre de mieux cibler les fonctionnalités techniques qui sont attendues

d'un système informatisé de gestion de ces données et d'en évaluer la pertinence à la fois technique et juridique.

Par ailleurs, la fonction sociale qui est dévolue au dossier médical depuis ses origines est celle d'une amélioration des rapports existants entre le soignant et ses patients. Cette fonction, qui est nettement perceptible dans les dossiers médicaux partagés des établissements de santé et les dossiers des réseaux de soins qui existent d'ores et déjà, est d'ailleurs mise en avant dans le cadre du futur dossier médical personnel. La loi du 13 août 2004, qui crée le DMP [Loi04], introduit celui-ci dans les dispositions du Code de la sécurité sociale par un article L. 161-36-1 débutant par la phrase suivante : « Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du code de la santé publique et dans le respect du secret médical, d'un dossier médical personnel ». De même, le Groupement d'intérêt public dont la création a été approuvée par arrêté du 11 avril 2005 [Arr05] afin d'assurer le suivi et la coordination de ses expérimentations, puis sa mise en place, annonce clairement que « Le DMP va enrichir le dialogue singulier entre le professionnel de santé et son patient grâce à cette approche plus globale et plus éclairée de la prise en charge médicale ».

Il semble néanmoins, à l'analyse préliminaire des textes normatifs qui encadrent ce dossier médical, que cet objectif ne soit plus l'unique fonction du dossier médical tel qu'il est envisagé par la loi française. Cette loi crée en effet le dossier médical personnel dans le cadre d'une meilleure gestion de l'assurance maladie, et instaure, pour cela, un système de modification du niveau de prise en charge des actes et prestations de soins, lié à l'autorisation d'accès au dossier donnée par le patient. Une telle évolution des fonctions du dossier médical mérite d'être identifiée et également d'être interrogée dans ses croisements avec des fonctionnalités techniques et administratives (problèmes d'égalité de traitement des citoyens pour la santé, d'administration à deux vitesses) qui ont parfois pu déjà être expérimentées dans les dossiers mis en place dans le cadre des réseaux de soins ou des établissements de santé et dans d'autres systèmes juridiques.

Depuis 2002, les données de santé ont une place de choix dans le Code de la santé publique. Intégrées dans le Titre premier de ce Code relatif aux « droits des personnes malades et des usagers du système de santé », les données de santé constituent le support d'un certain nombre de droits créés au bénéfice de l'utilisateur du système de santé. Elles sont le support du droit à l'information de la personne malade, du pouvoir de décision dont elle dispose sur sa santé également du droit d'accès au dossier médical qui a été consacré par l'article L. 1111-7 du Code de la santé publique. Mais l'évolution juridique ne s'arrête pas là. La loi du 13 août 2004 portant réforme de l'assurance maladie a en effet sensiblement modifié le rôle attribué aux données de santé. En créant une section V sur le dossier médical personnel (DMP), le législateur de 2004 attribue une nouvelle fonction aux données de santé. Il est désormais prévu que chaque bénéficiaire de l'assurance maladie dispose d'un dossier médical personnel, constitué de l'ensemble des données mentionnées à l'article L. 1111-1 du Code de la santé publique, afin « de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé ». Et l'article L. 161-32-2 du Code de la sécurité sociale d'ajouter dans son alinéa 2 que « le niveau de prise en charge des actes et prestations de soins par l'assurance maladie est subordonnée à l'autorisation que donne le patient, à chaque consultation ou hospitalisation, aux professionnels de santé auxquels il a recours, d'accéder à son dossier médical personnel et de le compléter ».

La nouveauté ne réside ni dans la création du dossier ni dans les motifs affichés pour sa constitution mais dans le choix qui est laissé à l'assuré d'en autoriser ou pas la consultation par les professionnels de santé. En majorant le montant de la participation de l'assuré lorsque celui-ci n'autorise pas la consultation de son dossier médical personnel, la loi du 13 août 2004 modifie le libre choix de l'assuré [Vac05] et met en cause, de ce fait, le principe d'égalité des citoyens devant le service public.

Aussi s'agit-il de constater qu'aujourd'hui les législations relatives aux données de santé se donnent pour objet de garantir la conciliation de trois principes à valeur constitutionnelle : la protection de la vie privée, la protection de la santé de la personne et l'équilibre financier de la sécurité sociale, exigences qui n'ont pas toutes pour objet d'offrir de nouveaux droits aux personnes ni

l'égalité des usagers devant le service public. Cette évolution juridique dans les finalités et donc dans le rôle conféré aux données de santé modifie également les relations qui se nouent dans le colloque singulier entre le médecin et le patient dès lors que si le patient acquiert des droits, professionnels de santé comme patients sont désormais largement incités voire obligés de produire un certain comportement.

Si le colloque singulier a pu être défini comme un pacte de confiance entre le médecin et le patient [Ric96] au sein duquel personne ni même le juge ne pouvait s'immiscer, le changement est aujourd'hui profond. Cette évolution qui a d'abord été repérée dans la jurisprudence a fait une entrée remarquée dans le Code de la santé publique avec la loi du 4 mars 2002 [Loi02]. Le libre choix de la personne, le respect de sa vie privée comme sa participation à la décision médicale sont autant de droits reconnus désormais non seulement à la personne malade mais également à tous les usagers du système de santé, qu'il faut envisager également sous l'angle du respect du secret médical et, dans certains cas, de la contre expertise.

Il faut néanmoins noter que ce changement profond dans la représentation juridique du patient s'accompagne d'une autre évolution moins perceptible. L'article L. 1111-1 du CSP indique en effet que « les droits reconnus aux usagers s'accompagnent des responsabilités de nature à garantir la pérennité du système de santé et des principes sur lesquels il repose ». Aux droits des usagers s'ajoutent ainsi les responsabilités des assurés sociaux dans la préservation du système de protection de leur santé, en particulier de son système de financement. L'exemple du dossier médical personnel et de la modification du niveau de remboursement des prestations de soins témoigne de la mise en œuvre de ces nouvelles responsabilités de l'assuré.

Il reste également à observer que le texte fait parfois obstacle à la consultation du DMP sous peine de sanctions pénales même si cette consultation se fait avec le consentement de la personne qui en est titulaire. Ainsi, l'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus à l'article L. 161-36-2, même avec l'accord de la personne concernée. L'article L. 161-36-3 du CSS prévoit que « l'accès au DMP est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties ». Est également exclue de cet accès la médecine du travail. Aussi est-il nécessaire dans le cadre de ce projet d'évaluer le degré d'autonomie de décision dont dispose le patient titulaire de droits qui est également un assuré social et parfois un salarié. L'informatique fait une entrée retentissante dans les obligations du médecin, là où elle n'était, jusqu'alors, dans la plupart des cas, qu'un outil supplémentaire de gestion, elle devient un élément sensible de la relation médicale et de sa prise en charge par les organismes de sécurité sociale, ce qui implique d'en connaître à la fois les avantages et les inconvénients, afin de l'adapter au mieux à cette relation particulière.

La mise en place de dossiers contenant des données de santé est intimement liée à l'outil informatique, qui en est le support incontournable, comme c'est le cas dans le cadre du DMP. Elle invite ainsi à s'interroger sur l'existence de droits spécifiquement liés à l'utilisation de cette technologie. Une analyse comparée entre les normes juridiques encadrant le dossier médical personnel et les règles classiques de protection des données de santé (Loi CNIL, Code de la santé publique, etc.) devra être menée. Une attention particulière sera prêtée à la question de la cohérence des dispositifs techniques prévus par la loi, non seulement vis-à-vis de l'état de l'art en matière informatique (cryptologie, bases de données, sécurité, etc.), mais également en termes de légistique, ces textes venant s'insérer dans une législation d'ores et déjà complexe et empruntant ses principes et logiques dans de nombreuses disciplines juridiques (droit de la santé, droit de la sécurité sociale, droit d'auteur, droit des données personnelles, droit des marchés publics, etc.)

Une fois mis en évidence ces nouveaux droits, le projet aura donc pour ambition d'en évaluer la faisabilité technique et juridique. Une phase plus prospective de recommandations quant aux évolutions souhaitables dans les textes applicables, en droit français, aux dossiers et aux données de santé, sera rendue possible lors que cette première analyse aura été menée, confrontée aux travaux et aux pistes des partenaires informaticiens du programme et que ces résultats auront été validés par le travail commun.

Tâche	Description	Livrables	Partenaire leader
T6	Analyse des problèmes et piste de résolution	L7	CECOJI
T7	Analyse du corpus juridique relatif au traitement automatisé des données de santé	L8	CECOJI

Tableau 8: Tâches du WP3

Livrable	Description	Date
L7	Etat des problèmes et pistes de résolution	M12
L8	Analyse et recommandations sur le corpus juridique relatif au traitement automatisé des données de santé	Mois 36 (brouillon M30)

Tableau 9: Livrables du WP3

## Bibliographie pour le WP3 :

- [Gin02] A.-S. Ginon, « *Organisation mondiale de la santé – La norme internationale comme ressource pour le droit communautaire* », Chronique de droit européen n°11, Questionnement sur la place des normes internationales dans l'ordre juridique, Les Petites Affiches, 2002, n° 149, p. 15-17.
- [Gin05] A.-S. Ginon, « Le médecin traitant, révélateur des nouvelles fonctions de la protection sociale complémentaire », *Revue du droit de la sécurité sociale*, nov.-déc. 2005 p. 907 et s.
- [GL04] B. Gleize et S. Lacour, Note sous Paris, 6 mars 1931 et Civ 1<sup>ère</sup>, 20 décembre, De l'indépendance des propriétés incorporelle et corporelle, in *Les grands arrêts de la propriété intellectuelle*, Dalloz, 2004, p. 101.
- [GL04b] B. Gleize et S. Lacour, Note sous OEB, Grande Chambre des Recours, 5 décembre 1984 ; Com. 26 octobre 1993, Brevetabilité des secondes applications thérapeutiques in *Les grands arrêts de la propriété intellectuelle*, Dalloz, 2004, p. 251.
- [GT05] A.-S. Ginon, T. de Roehogonde, « *L'encadrement méconnu de la recherche biomédicale en France* », *Revue Esprit*, 2005, p. 130-144.
- [Lac04] S. Lacour, Le temps dans les propriétés intellectuelles. Contribution à l'étude du droit des créations, Editions Litec, Bibliothèque du droit de l'entreprise, n° 65, 2004.
- [Arr05] Arrêté du 11 avril 2005 portant approbation de la convention constitutive d'un groupement d'intérêt public.
- [CNI99] CNIL, « Rapport relatif aux modalités d'informatisation de la surveillance épidémiologique du SIDA – à propos de la déclaration obligatoire de la séroposivité au virus de l'immunodéficience humaine ». Rapport adopté le 9 septembre 1999.
- [CNI03] CNIL, Délibération n° 03-053 du 27 novembre 2003 portant adoption d'une recommandation relative aux traitements de données à caractère personnel mis en œuvre par les registres du cancer.
- [CNI04] CNIL, Délibération n° 04-054 du 10 juin 2004 portant avis sur le projet de loi relative à la réforme de l'assurance maladie.
- [CNI07] CNIL, Communiqué du 20 février 2007 sur l'utilisation du NIR comme identifiant de santé.
- [CNO05] Conseil National de l'Ordre des médecins, « Questions sur l'informatisation des dossiers médicaux, le partage et l'hébergement des données, rapport adopté le 18 juin 2005.
- [Con04] Conseil Constitutionnel n° 2004-504 DC du 12 août 2004, *Loi relative à l'assurance maladie*
- [DMP06] GIP DMP, « Expérimentation du DMP : une faille dans le dispositif de protection des données est détectée chez Santénergie, un des hébergeurs du DMP », Communiqué de presse, [http://www.d-m-p.org/docs/communiqu%C3%A9GIP\\_DMPdu211106.pdf](http://www.d-m-p.org/docs/communiqu%C3%A9GIP_DMPdu211106.pdf), 21 novembre 2006.
- [Fag07] P.-L. Fagniez, « Le masquage d'informations par le patient dans son DMP », rapport au ministre de la santé et des solidarités, [http://www.sante.gouv.fr/htm/actu/fagniez\\_dmp/rapport.pdf](http://www.sante.gouv.fr/htm/actu/fagniez_dmp/rapport.pdf), 30 janvier 2007.
- [IC03] IPSOS Santé / CNAM, « Opinions et attitudes des médecins et des patients à l'égard du Dossier médical partagé », octobre 2003.
- [Lam04] I. de Lamberterie, Qu'est ce qu'une donnée de santé ? *Revue générale de droit médical*, n° special « *Le droit des données de santé* », 2004, p. 11 et s.
- [Loi78] Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- [Loi94] Loi n°94-548 du 1er Juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la Santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- [Loi02] Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé

- [Loi04] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.
- [Loi07] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance no 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique.
- [Ric96] P. Ricoeur, Les trois niveaux du jugement medical, *Revue Esprit*, 29(2), 1996.
- [Vac88] I. Vacarie, Le traitement informatique des données de santé – questions juridiques et éthiques, *Convention de recherche avec le commissariat général du plan*, 1988
- [Vac05] I. Vacarie. Les tensions entre le droit de la santé et le droit de la sécurité sociale. *Revue du droit de la sécurité sociale*, nov.-déc. 2005 p. 899 et s.

#### **WP4 : Concertation publique avec les associations de médecins et de patients autour des résultats de la recherche sur le DMP**

Notre objectif est de disséminer les résultats de la recherche réalisée lors du projet et de nourrir la réflexion des acteurs sociaux en lien avec le sujet [Aig06]. La mise en place des systèmes techniques opérationnels de gestion des données de santé aura un impact important sur les pratiques et parfois les droits ou responsabilités de ces acteurs. Pour ce faire, nous prévoyons d'organiser un débat en ligne ouvert au grand public mais plus spécifiquement organisé en partenariat avec des associations de médecins, de patients et d'usagers du système de santé pendant une durée de 4 mois. Ce débat en ligne sera clôturé par un colloque réunissant les parties prenantes aux échanges assurant une visibilité médiatique à l'événement.

Les résultats de la recherche, sous une forme hiérarchisée et « problématisée » seront le point de départ de l'information disponible sur le site Web support du débat. Les échanges seront co-animés par l'équipe de Sopinspace et les associations partenaires [Aig05].

Une mobilisation insuffisante est le principal risque lors de la concertation. Il existe en effet un seuil critique en dessous duquel la légitimité du débat ne s'installe pas chez les acteurs cibles (associations de médecins et de patients) et par conséquent ne capte par l'attention du grand public [ABB+06]. Ce risque n'est pas propre à ce débat particulier et Sopinspace a une expérience poussée des mesures destinées à le prévenir. Dans le cas particulier (consultation dans le cadre d'un projet de recherche), la mobilisation visible d'acteurs politiques et institutionnels de santé et d'une ou deux associations très porteuses est seule à même de crédibiliser la consultation, d'installer une perception d'enjeux réels à y participer. La nature exacte de ces « porteurs du débat » ne peut être définie aujourd'hui (3 ans avant le débat), mais fera l'objet de choix dans la phase de préparation.

Une vulgarisation des résultats de la recherche destinée à alimenter le débat doit par ailleurs permettre un bon démarrage de la participation par une structuration adéquate des problématiques soumises au débat. Le partenaire industriel du projet, Sopinspace, mettra son expérience et ses compétences en matière de débat participatif au service du bon déroulement du débat pour l'avoir mis en oeuvre dans différents débats notamment sur des sujets liés aux questions de santé :

- modération et synthèse du forum de mise en débat des conclusions de la Commission Alzheimer, [http://www.forum.gouv.fr/article\\_archive.php3?id\\_article=278](http://www.forum.gouv.fr/article_archive.php3?id_article=278)
- animation du débat internet associé aux Etats généraux de l'alcool, <http://www.etatsgenerauxalcohol.fr/forum/>
- débat sur la santé environnementale, <http://www.ledebatmde.org> [Moi07]

Tâche	Description	Livrables	Partenaire leader
T8	Préparation, organisation et animation de la concertation en ligne et de le colloque de clôture du débat	L9, L10	Sopinspace

Tableau 10: Tâches du WP4

Livrable	Description	Date
L9	Site support du débat, documentation grand public, site plateforme des échanges	M28 - M34
L10	Synthèse et conclusions du débat, analyse de la participation	M34

Tableau 11: Livrables du WP4

### Bibliographie pour le WP4 :

- [ABB+06] Ph. Aigrain, R. Badin, R. Bernard, Ph. Bourlito, K. Chevalet, Livre blanc sur la démocratie participative et le débat public utilisant internet, [http://www.co-ment.net/docs/livre\\_blanc\\_sopinspace.pdf](http://www.co-ment.net/docs/livre_blanc_sopinspace.pdf)
- [Aig06] Ph. Aigrain, ICT for the public debate by citizens of policy issues, hearing by the Industry, Research and Energy Committee of the European Parliament on the i2010 initiative, 26 January 2006, <http://www.sopinspace.com/press/presentations/pha-ITRE-260106-fr-notesen.pdf>
- [Aig05] Ph. Aigrain, Usages citoyens des technologies de l'information : des outils qui ne doivent pas faire écran, Territoires 2006(5).
- [Moi07] F. Moisan, Consultation publique – Maîtrise de l'énergie, un bon début pour le débat, ADEME et vous, 8, sept. 2007, <http://www.ademe.fr/htdocs/publications/lettre/08/conjoncture.htm>

### WP5 : Diffusion et exploitation des résultats

A la pluridisciplinarité des partenaires du projet répond la multiplicité des acteurs potentiellement intéressés par les divers résultats du projet : industriels en charge de la réalisation de grandes infrastructures de données sensibles, médecins, patients, grand public, etc. L'organisation d'une consultation de toutes ces parties prenantes dans la troisième année du projet sera un vecteur clé de la diffusion de ses résultats.

Le site web du projet sera la plateforme de diffusion des résultats du projet sous ses multiples formes : analyse et recommandations techniques sur la sécurité des bases de données, analyse du corpus juridique, etc.

Le travail effectué par les partenaires de recherche du projet prendra en outre la forme de publications scientifiques et interventions dans des colloques de leurs domaines respectifs. De plus, grâce à la confrontation des points de vue traditionnellement dissociés des chercheurs en droit et en informatique, le projet conduira à une meilleure compréhension réciproque des règles et possibilités juridiques et techniques par les deux communautés ; les partenaires s'efforceront alors de diffuser dans leurs communautés respectives une telle connaissance.

Un séminaire de fin de projet sera organisé afin de réunir les différentes communautés scientifiques autour des travaux du projet. Cela conduira sans nul doute à plus long terme à une articulation plus efficace des mécanismes techniques et juridiques.

En ce qui concerne le partenaire industriel, la diffusion des résultats concernant le système d'annotation des textes juridiques et techniques reposera sur la diffusion dès maturité suffisante de la base logicielle du système sous la licence libre Affero GPLv3. Cette diffusion viendra alimenter la stratégie industrielle générale de Sopinspace concernant les systèmes d'annotations et commentaires de textes et services associés. Cette stratégie repose sur l'utilisation conjointe d'une diffusion en logiciel libre à copyleft fort (obligation de redistribution y compris de la partie serveur en cas d'opération d'un service Web utilisant une version modifiée du code), une protection et un suivi efficace de la marque co-ment® et des modèles commerciaux diversifiés : service Web d'entrée gratuit, service « Pro » à abonnement annuel peu coûteux, service personnalisé pour des organismes, développements additionnels pour intégration à des systèmes d'information. Dans le cas des systèmes d'annotation de textes juridiques et techniques, nous estimons que ce sont les deux derniers modèles qui présentent un véritable potentiel de marché.

Tâche	Description	Livrables	Partenaire leader
T9	Diffusion et exploitation des résultats	L11, L12	Sopinspace

Tableau 12: Tâches du WP5

Livrable	Description	Date
L11	Site Web public du projet mettant en ligne l'ensemble des publications et dé livrables publics du projet DEMOTIS	M12
L12	Diffusion du code source de la base logicielle du système d'annotations de textes juridiques et techniques	M13-M36

Tableau 13: Livrables du WP5

## 1.6 Résultats escomptés et Retombées attendues. *Expected results and potential impact.* (1 à 2 pages maximum)

(Plus spécifiquement pour les programmes partenariaux organismes de recherche/entreprises)

Présenter les **résultats escomptés** en proposant si possible des critères de réussite et d'évaluation adaptés au type de projet, permettant d'évaluer les résultats en fin de projet.

Présenter les **retombées attendues** en précisant pour les partenaires concernés :

- la valorisation des résultats attendus, connaissances à protéger ou à diffuser, ...
- les retombées scientifiques, techniques, industrielles, économiques...
- la place du projet dans la stratégie industrielle de l'entreprise (ou du groupe)
- les échéances et la nature des retombées technico-économiques attendues
- l'incidence éventuelle sur l'emploi, la création d'activités nouvelles, ...

Les retombées attendues sont à la fois scientifiques, sociales et industrielles. En ce qui concerne les travaux des organismes de recherche (informaticiens comme juristes), ces travaux feront l'objet d'une large diffusion, par des publications bien sûr, mais aussi par la diffusion d'un corpus annoté et de recommandations techniques concernant la façon de prendre en compte les exigences juridiques et normatives complexes dans l'architecture de systèmes de sécurité. En ce qui concerne les travaux du partenaire industriel, ils feront l'objet d'une exploitation directe utilisant un modèle original de valorisation d'un service Web commercial à base logicielle entièrement libre. Enfin, l'opération de concertation avec des parties prenantes du domaine de la santé vise à élargir le public impliqué dans ces réflexions et à créer un terrain plus favorable pour la réalisation des grandes infrastructures d'information de santé de demain. Nous détaillons ces différents aspects ci-dessous.

Le projet DEMOTIS aboutira sur le plan de la recherche à une meilleure compréhension des règles et possibilités juridiques et informatiques, ce qui encouragera une articulation plus raisonnée et efficace des mécanismes mis en place dans les deux domaines.

Sur le plan technique, l'exploration de nouvelles solutions et les documents produits par le projet seront à même de servir de référence pour les mises en place industrielles des grandes infrastructures de gestion de données à caractères sensibles; et ce dans le domaine de la sécurité et de la prise en compte du contexte juridique et social. Nos résultats seront en effet aussi destinés aux juristes qui pourront déterminer l'effectivité des textes de loi existants et la nécessité de proposer de nouvelles règles destinées à pallier certaines impossibilités techniques. Ils contribueront dans ce sens à la construction du droit positif (c'est-à-dire applicable aujourd'hui).

Par ailleurs, l'étude juridique menée sur le DMP ainsi que l'étude d'impact social menée sous la forme d'une concertation publique associant les principales parties prenantes doit permettre d'éclairer



<b>TABLEAU des LIVRABLES et des JALONS (le cas échéant)/ Deliverables and milestones</b>			
Tâche/ Task	Intitulé et nature des livrables et des jalons/ <i>Title and substance of the deliverables and milestones</i>	Date de fourniture nombre de mois à compter de T0/ <i>Delivery date, in months starting from T0</i>	Partenaire responsable du livrable/jalon/ <i>Partner in charge of the deliverable/ milestone</i>
<b>0. Reporting</b>			
	Rapports périodiques (5)	M6 – M12 – M18 – M24 – M30	Sopinspace (1)
	Rapport final	M36	Sopinspace (1)
<b>1. Communication interne</b>			
	Intranet du projet	M3 – M36 (interne)	Sopinspace (1)
<b>2. Constitution et commentaire du corpus juridique par les équipes de recherche de juristes et d'informaticiens</b>			
	Corpus juridique commenté conjointement par les équipes de recherche de juristes et d'informaticiens	M3 – M30	CECOJI (3)
<b>3. Adaptation et développement du logiciel du système d'annotation</b>			
	Logiciel (publié sous licence libre) de commentaire de texte juridique et technique Web 2.0	M3- M24	Sopinspace (1)
<b>4. Confrontation des exigences techniques et juridiques</b>			
	Identification des carences technologiques à la mise en œuvre des textes juridiques sur les données à caractère personnel	M12	INRIA (2)
<b>5. Exploration de nouvelles solutions technologiques</b>			
	Identification et impact des technologies émergentes en base de données et cryptographie sur la sécurité des données personnelles	M36 (brouillon M30)	INRIA (2)
<b>6. Analyse des problèmes et piste de résolution</b>			
	Etat des problèmes et pistes de résolution	M12	CECOJI (3)
<b>7. Analyse du le corpus juridique relatif au traitement automatisé des données de santé</b>			
	Analyse et recommandations sur le corpus juridique relatif au traitement automatisé des données de santé	M36 (brouillon M30)	CECOJI (3)
<b>8. Préparation, organisation et animation de la concertation en ligne et de le colloque de clôture du débat</b>			
	Site support du débat, documentation grand public, site plateforme des échanges, animation des débat, synthèse des échanges	M28 - M34	Sopinspace (1)
	Organisation du colloque de clôture	M33-M34	Sopinspace (1)
	Conclusion du débat, analyse de la participation	M34	Sopinspace (1)
<b>9. Diffusion et exploitation des résultats</b>			
	Site Web public du projet : ensemble des publications et livrables publics	M12	Sopinspace (1)
	Organisation et animation du séminaire de clôture du projet	M36	INRIA (2)
	Diffusion du code source de la base logicielle du système d'annotations de textes juridiques et techniques	M13 - M36	Sopinspace (1)

## 1.8 Organisation du partenariat. *Description of the Consortium.*

### 1.8.1 Pertinence des partenaires. *Presentation of the relevance of each partner to the proposal.*

*Fournir ici les éléments permettant d'apprécier la qualification des partenaires dans le projet (le « pourquoi qui fait quoi »). Il peut s'agir de réalisations passées, d'indicateurs (publications, brevets), de l'intérêt du partenaire pour le projet...*

Le partenariat comprend la société Sopinspace (coordination), le partenaire INRIA (équipes-projets SECRET, SMIS et CACAO) et le partenaire CNRS (laboratoire CECOJI).

Sopinspace, Société pour les espaces publics d'informations est une jeune entreprise innovante créée par Philippe Aigrain (dans le cadre de la loi 99-587 sur la recherche et l'innovation). La société a une activité commerciale de services et une activité de recherche et d'innovation. Elle est un acteur de référence en France pour l'utilisation des technologies de l'information pour le débat sur les politiques publiques. Sopinspace conduit une politique de R&D visant les technologies de services Web 2.0. La valorisation des activités se fait soit par l'intégration de leur usage aux offres de services soit directement. En 2004 et 2005, l'activité de R&D s'est centrée sur les technologies de cartographie sémantique interactive des contenus du Web, ce qui a abouti au service Glinkr. En 2006 et 2007, tout en continuant des travaux sur la cartographie de débats, l'effort de R&D a principalement porté sur les technologies Web 2.0 pour l'annotation des textes ce qui a conduit à la version actuelle de l'outil comment. Sopinspace est partenaire du réseau thématique européen COMMUNIA sur les contenus de domaine public et les outils pour leur valorisation.

Dans le cadre du projet DEMOTIS, la contribution de Sopinspace se situe à 3 niveaux :

- Sopinspace apporte au projet une expérience de coordination, gestion et valorisation de projets de recherche (WP0, WP5). Voir 1.8.3 sur les compétences spécifiques.
- Sopinspace développera l'outil d'annotation utilisé dans le WP1 (adaptation de co-ment au cas des textes techniques et juridiques) et fournira le soutien opérationnel à son usage pour l'annotation du corpus juridique et normatif.
- Sopinspace concevra (en liaison avec les autres partenaires) et animera la consultation des parties prenantes et du public prévue au WP4.  
Toutes ces activités se situent dans le coeur de compétences de la société.

### Sélection de publications du partenaire Sopinspace relatives au contexte étudié

- Ph. Aigrain, R. Badin, R. Bernard, Ph. Bourlito, K. Chevalet, Livre blanc sur la démocratie participative et le débat public utilisant internet, [http://www.co-ment.net/docs/livre\\_blanc\\_sopinspace.pdf](http://www.co-ment.net/docs/livre_blanc_sopinspace.pdf)
- Ph. Aigrain, Environnement et outils pour un nouvel espace public : l'exemple de l'annotation des textes », séminaire de l'Atelier Internet, Ecole Normale Supérieure, Paris, 11 février 2008.
- Ph. Aigrain, Modes de régulation des enjeux politiques et sociaux liés à l'information et à ses outils, in Stéphanie Lacour, ed. La sécurité aujourd'hui dans la société de l'information, Editions L'Harmattan, 2007, <http://paigrain.debatpublic.net/docs/expose-250106.pdf>
- Ph. Aigrain, ICT for the public debate by citizens of policy issues, hearing by the Industry, Research and Energy Committee of the European Parliament on the i2010 initiative, 26 January 2006, <http://www.sopinspace.com/press/presentations/pha-ITRE-260106-fr-notesen.pdf>
- Ph. Aigrain, Cause commune : l'information entre bien commun et propriété, Editions Fayard, 2005. Ouvrage traduit en italien et en arabe.
- Philippe Aigrain, Libre Software Policies at European Level in Joseph Feller et al., ed., Perspectives on Free / Open Source Software, MIT press, June 2005, ISBN : 0262062461.
- Service Web co-ment®, <http://www.co-ment.net>
- Observatoire des débats publics utilisant internet et de leurs outils, <http://www.debatpublic.net>

Le CECOJI (Centre d'Etudes sur la Coopération Juridique Internationale, [www.cecoji.cnrs.fr](http://www.cecoji.cnrs.fr)) est une Unité Mixte de Recherche composée de quatre équipes internes déployant des activités diverses dont la complémentarité est soulignée par des actions transversales. Ses compétences en droit de la santé, droit des propriétés intellectuelles, droit des données à caractère personnel lui permettront de réaliser la constitution du corpus juridique à étudier et d'encadrer le travail commun d'annotation. L'équipe interne « Normativités et nouvelles technologies » développe depuis de longues années des travaux sur la régulation de la société de l'information, qui se sont manifestés par des études sur le métissage des normes (en coopération avec l'Université de Montréal), sur les questions juridiques liées à la numérisation (étude Persée, [www.persee.fr](http://www.persee.fr)), ainsi qu'aux modes alternatifs de règlement des différends, par l'intermédiaire, notamment, du forum des droits sur l'Internet. Cette équipe a également coordonné le programme Asphales, de l'ACI Sécurité et Informatique (<http://www.asphales.cnrs.fr/>) qui se termine en 2007. Elle associera à ses travaux, dans le cadre de ce nouveau projet interdisciplinaire, les compétences juridiques d'un enseignant chercheur spécialiste du droit de la santé et de la sécurité sociale de l'Université de Nanterre, Anne-Sophie Ginon. Stéphanie Lacour est en outre, avec Anne-Sophie Ginon, l'un des membres fondateurs du réseau Droit Sciences et Techniques promouvant la recherche juridique française sur les questions liées aux sciences et aux techniques.

### Sélection de publications du partenaire CECOJI relatives au contexte étudié

- A.-S. Ginon, « Organisation mondiale de la santé – La norme internationale comme ressource pour le droit communautaire », Chronique de droit européen n°11, Questionnement sur la place des normes internationales dans l'ordre juridique, Les Petites Affiches, 2002, n° 149, p. 15-17.
- A.-S. Ginon, « Le médecin traitant, révélateur des nouvelles fonctions de la protection sociale complémentaire », Revue du droit de la sécurité sociale, nov.-déc. 2005 p. 907 et s.
- B. Gleize et S. Lacour, Note sous Paris, 6 mars 1931 et Civ 1ère, 20 décembre, De

l'indépendance des propriétés incorporelle et corporelle, in Les grands arrêts de la propriété intellectuelle, Dalloz, 2004, p. 101.

- B. Gleize et S. Lacour, Note sous OEB, Grande Chambre des Recours, 5 décembre 1984 ; Com. 26 octobre 1993, Brevetabilité des secondes applications thérapeutiques in Les grands arrêts de la propriété intellectuelle, Dalloz, 2004, p. 251.
- A.-S. Ginon, T. de Rochegonde, « L'encadrement méconnu de la recherche biomédicale en France », Revue Esprit, 2005, p. 130-144.
- S. Lacour, Le temps dans les propriétés intellectuelles. Contribution à l'étude du droit des créations, Editions Litec, Bibliothèque du droit de l'entreprise, n° 65, 2004.
- S. Lacour, L'identification par radiofréquence (RFID), une technologie en mal de régulation juridique, à paraître aux Annales des télécommunications, n° spécial, 2007, sur la Sécurité du monde numérique.

**L'INRIA - équipes-projets SMIS, SECRET et CACAO** : L'INRIA (Institut National de Recherche en Informatique et Automatique, <http://www.inria.fr/>) a pour vocation d'entreprendre des recherches fondamentales et appliquées dans les domaines des sciences et technologies de l'information et de la communication (STIC). Les équipes-projets intervenant dans DEMOTIS sont SMIS (Secured and Mobile Information Systems), SECRET (Sécurité, Cryptologie et Transmissions) et CACAO (Courbes, Algèbre, Calculs, Arithmétique des Ordinateurs).

L'équipe-projet SMIS (<http://www-smis.inria.fr/>) est spécialisée dans la gestion de données embarquées dans des calculateurs ultra-légers (notamment les cartes à puce) ainsi que dans la protection de la confidentialité des bases de données par la définition de nouveaux modèles de contrôle d'accès, le chiffrement des données et l'usage de composants matériels sécurisés. Ses travaux dans le domaine ont récemment été récompensés par plusieurs distinctions académiques, prix logiciels et brevets. La protection de la confidentialité des données personnelles de santé est un des domaines d'application privilégiés de SMIS. SMIS est notamment coordinateur du projet RNTL'2006 PlugDB., en association avec Santeos (hébergeur de données médicales), l'ALDS (coordination gérontologique), Gemalto (leader mondial des cartes à puce) et l'Université de Versailles. PlugDB vise la conception d'un dossier portable sécurisé et nomade (embarqué dans une clé USB sécurisée matériellement) permettant l'échange de données médico-sociales au chevet du patient avec de fortes garanties de confidentialité. La protection de données personnelles hébergées sur un terminal non sécurisé (typiquement celui du médecin) fait également partie de l'étude.

Les équipes-projets SECRET (<http://www-rocq.inria.fr/secret/>, anciennement CODES) et CACAO (<http://www.loria.fr/equipes/cacao/>) sont spécialisées dans le domaine de la cryptographie ; un de leurs principaux thèmes de recherche est la conception et l'analyse des algorithmes de chiffrement. Leur contribution se situe tant dans le domaine de l'évaluation de la sécurité des systèmes existants que dans la conception de nouveaux algorithmes. Par exemple, l'équipe-projet SECRET, à travers sa participation au réseau d'excellence européen ECRYPT, intervient dans le projet eSTREAM consacré à la définition de nouveaux chiffrements à flot. La recherche d'algorithmes de chiffrement sûrs et efficaces dans des environnements matériels extrêmement contraints fait également l'objet du projet RAPIDE (<http://rapide-anr2006.gforge.inria.fr/>) sélectionné par l'ANR dans le cadre de l'appel SETIN'06. Par ailleurs, Anne Canteaut (équipe SECRET) et Marion Videau (équipe CACAO) ont mené des recherches pluridisciplinaires sur le thème de la conservation des documents électroniques, en abordant conjointement les aspects informatiques et juridiques, dans le cadre du projet Asphales de l'ACI Sécurité et Informatique (<http://www.asphales.cnrs.fr/>).

### **Sélection de publications du partenaire INRIA relatives au contexte étudié**

- N. Ancaux, M. Benzine, L. Bouganim, P. Pucheral, D. Shasha, "GhostDB: Querying Visible and Hidden data without leaks", 26th ACM SIGMOD International Conference on Management of Data, Beijing, China, 2007.
- N. Ancaux, L. Bouganim, P. Pucheral, "Data confidentiality: to which extent cryptography and secured hardware can help", Annals of telecom, 2006.

- L. Bouganim, C. Cremarenco, F. Dang Ngoc, N. Dieu, P. Pucheral, "Data Sharing and Data Dissemination on Smart Devices", 24th ACM SIGMOD International Conference on Management of data, Maryland, USA, juin 2005.
- L. Bouganim, F. Dang Ngoc, P. Pucheral, L. Wu, "Chip-Secured Data Access: Reconciling Access Right with Data Encryption", 29th International Conference on Very Large Data Bases (VLDB), Berlin, Germany, 2003.
- L. Bouganim, F. Dang Ngoc, P. Pucheral, "Client-Based Access Control Management for XML documents". 30th International Conference on Very Large Data Bases (VLDB), septembre 2004.
- L. Bouganim, F. Dang Ngoc, P. Pucheral, "Chip-Secured XML Access". Silver Award of the e-gate open 2004 international software contest (80 participating teams).
- L. Bouganim, N. Dieu, P. Pucheral, "MobiDiQ: Mobile Digital Quietude". Gold Award of the SIMagine 2005 international software contest (300 participating teams).
- L. Bouganim, F. Dang Ngoc, P. Pucheral, "Tamper-Resistant Ubiquitous Data Management". International Journal of Computer Systems Science and Engineering (IJCSSE), Special Issue on Mobile Databases, Vol.20, n°2, 2005.
- L. Bouganim, P. Pucheral, "Chip-Secured Data Access: Confidential Data on Untrusted Servers", 28th International Conference on Very Large Data Bases (VLDB), Hong Kong, China, août 2002.
- L. Bouganim, P. Pucheral, « Procédé de sécurisation de bases de données », Dépôt par le CNRS du brevet français n°01/10552 le 07/08/2002, délivré le 30/01/04. Demande de PCT (brevet international) « Method for Making Database Secure » n° PCT/FR02/02824 pour USA, Europe, Canada, Japon, 07/08/02.
- F. Banat-Berger et A. Canteaut. « Intégrité, signature et processus d'archivage ». La Sécurité aujourd'hui dans la société de l'information, L'Harmattan, 213--235, 2007.
- A. Canteaut (ed.), D. Augot, C. Cid, H. Englund, H. Gilbert, M. Hell, T. Johansson, M. Parker, T. Pornin, B. Preneel, M. Robshaw. D.STVL.5 -- Ongoing Research Areas in Symmetric Cryptography. ECRYPT Report, Mars 2007, 93 pages.
- C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. Decim, a new stream cipher for hardware applications. Chapter in: The eSTREAM Finalists, Lecture Notes in Computer Science 4986. Springer Verlag, 2008.
- C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. Sosemanuk, a fast software-oriented stream cipher. Chapter in: The eSTREAM Finalists, Lecture Notes in Computer Science 4986. Springer Verlag, 2008.
- A. Canteaut, "Analyse et conception de chiffrements à clef secrète", habilitation à diriger des recherches, Université Pierre et Marie Curie, Paris, septembre 2006.
- F. Cuppens, P. Pucheral, "Sécurité des bases de données", chapitre de l'encyclopédie informatique Vuibert, éditions Vuibert, ISBN : 2-7117-4846-4, 2006.
- Forum des Droits sur l'Internet, "La conservation électronique des documents", <http://www.foruminternet.org/telechargement/documents/reco-archivage-20051201.pdf>, décembre 2005.
- B. Finance, S. Medjdoub, P. Pucheral, "The Case for Access Control on XML Relationships", 14th ACM International Conference on Information and Knowledge Management (CIKM), Bremen, Germany, novembre 2005.
- I. de Lamberterie et M. Videau, « Regards croisés de juristes et d'informaticiens sur la sécurité informatique », Actes du Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC'06), pages 76-87, 2006.
- S. Lacour et M. Videau, « Légistique de l'écrit électronique », La Sécurité aujourd'hui dans la société de l'information, L'Harmattan, 183--208, 2007.
- P. Pucheral, L. Bouganim, P. Valduriez, C. Bobineau, « PicoDBMS: Scaling down Database

Techniques for the Smartcard », Very Large Data Bases Journal (VLDBJ), Vol.10, n°2-3, extended version of the Best Paper Award of VLDB'00, octobre 2001.

- P. Pucheral, "Ubiquité et confidentialité des données", chapitre du livre « Paradigmes et enjeux de l'informatique » édité par le département STIC du CNRS, éditions Hermès, 2005.
- M. Videau, « Critères de sécurité des algorithmes de chiffrement à clé secrète », thèse de doctorat d'informatique, Université Pierre et Marie Curie, Paris 6, novembre 2005.
- M. Videau, "How cryptography interacts with legal safeguards", Seminar Symmetric Cryptography, Dagstuhl, Allemagne, janvier 2007.
- M. Videau, « Cryptographie, nouveaux usages, nouveaux défis : l'exemple du Dossier Médical Personnel (DMP) », Computer & Electronics Security Applications Rendez-vous, Rennes, 2007.

### 1.8.2 Complémentarité des partenaires. *Description of complementarity within the consortium.*

*Montrer la complémentarité et la valeur ajoutée des coopérations entre les différents partenaires. L'interdisciplinarité et l'ouverture à diverses collaborations seront à justifier en accord avec les orientations du projet.*

L'interdisciplinarité est au coeur du projet DEMOTIS. Son originalité tient précisément à la mise en oeuvre concrète et structurée d'un travail commun entre juristes et informaticiens. Par ailleurs la complémentarité des partenaires de recherche du projet a déjà été éprouvée avec succès dans le cadre du projet Asphalès. Le coordinateur du projet a également participé aux travaux d'Asphalès par une intervention dans son séminaire, publiée dans les actes de celui-ci [insérer ref.].

La complémentarité des partenaires se traduit par un plan de travail équilibré, chacun des partenaires académiques ayant la responsabilité du work package coeur de son activité (sécurité et bases de données pour l'INRIA, analyse juridique pour le CECOJI). Sopinspace a la responsabilité des work packages support (coordination, diffusion des résultats, organisation de la concertation) et du développement de l'outil d'annotation base du travail commun. L'implication des partenaires dans les tâches de WP placés sous la responsabilité d'autres partenaires est justifiée par d'authentiques besoins de collaboration (lecture croisée des textes dans le WP1, préparation de la concertation dans le WP4 et diffusion des résultats d'ensemble dans le WP5).

### 1.8.3 Qualification du coordinateur du projet. *Principal investigator: skills and CV.*

*(Plus spécifiquement pour les programmes destinés principalement à la communauté académique)*

*Fournir une biographie du coordinateur et des informations sur son expérience passée de coordination.*

Le chef de projet pour la coordination sera Philippe Aigrain. Philippe Aigrain est titulaire d'un doctorat de 3ème cycle en informatique théorique et de l'habilitation à diriger les recherches (Université Paris 7). Il est le directeur et fondateur de Sopinspace. Après une carrière de chercheur aussi bien dans des laboratoires industriels qu'au CNRS (responsable d'équipe à l'IRIT Toulouse de 1986 à 1996), il a rejoint de 1996 à 2003 les programmes de recherches européens, où il fut notamment chef du secteur « technologies du logiciel ». Il a été responsable du suivi de plusieurs dizaines de projets de recherche collaborative européens, et a participé à la préparation des 5ème et 6ème PCRD. Initiateur et coordinateur des politiques de soutien à l'innovation en logiciels libres, il a été l'interlocuteur européen du RNTL sur ces questions pendant la réalisation du rapport Conchon-Giraudon. Il représente Sopinspace au sein du groupe thématique « Logiciels libres » du pôle de compétitivité [System@TIC](#). Philippe Aigrain siège au Board of Directors du Software Freedom Law Center, fondation américaine active dans le domaine de l'environnement juridique des logiciels libres au niveau mondial. Il est l'auteur de plus de 120 publications scientifiques, techniques ou de sciences sociales.

### 1.9 Stratégie de valorisation et de protection des résultats. *Data management, data sharing, intellectual property strategy, and exploitation of project results.* (1 page maximum)

*(Plus spécifiquement pour les programmes partenariaux organismes de recherche/entreprises)*

*Pour les projets partenariaux organismes de recherche/entreprises, les partenaires devront conclure, sous l'égide du coordinateur du projet, un accord de consortium dans un délai de un an si le projet est retenu pour financement. Indiquer les grandes lignes de la répartition entre partenaires de la propriété intellectuelle, des droits d'exploitation etc.,*

*Pour les projets académiques, l'accord de consortium n'est pas obligatoire mais conseillé.*

La stratégie de valorisation des résultats est fortement axée sur la diffusion publique de ceux-ci, assortis de mécanismes de protection adaptés dans le cas du partenaire industriel. De manière générale, les connaissances nouvelles qui résultent de la recherche menée dans le cadre du projet seront publiées et ouvertes à d'autres acteurs.

Les connaissances antérieures au projet restent la propriété de leur détenteur et seront mises à disposition des autres partenaires pour la réalisation du projet et pour les besoins de la diffusion de ses résultats, sans que cela implique aucun transfert de propriété ou licence au-delà de ces besoins. L'accord de consortium qui sera élaboré rapidement (et finalisé au plus tard à M12) inclura en annexe une liste de ces connaissances antérieures.

A l'exception des développements logiciels réalisés par le partenaire industriel, les connaissances nouvelles obtenues dans le cadre du projet seront la propriété commune des partenaires. Les modalités de dépôt, de gestion de copropriété et de valorisation feront l'objet d'une discussion au cas par cas, qui n'impliqueront aucun transfert ou licence exclusive à destination du partenaire industriel (pas d'aide indirecte).

Les développements logiciels réalisés par le partenaire industriel (Sopinspace) seront diffusées sous une licence libre (Affero GPLv3, déjà utilisée pour les développements existants). L'exploitation de ces résultats repose à la fois sur les protections offertes par la licence contre la réappropriation et sur la protection par la marque européenne et américaine co-ment®. L'utilisation d'une licence libre garantit la pérennité de la disponibilité des résultats correspondants.