

---

# Transaction de données sensibles au sein de systèmes multi-agents hippocratiques

**Ludivine Crépin** \* \*\*\* — **Yves Demazeau**\* — **Olivier Boissier**\*\*  
**François Jacquenet**\*\*\*

\* CNRS - Laboratoire d'Informatique de Grenoble  
Domaine Universitaire, Maison Jean Kuntzmann, BP 53  
F-38031 Grenoble Cédex  
{Ludivine.Crepin, Yves.Demazeau}@imag.fr

\*\* Ecole Nationale Supérieure des Mines de Saint-Etienne - Centre G2I  
158 cours Fauriel  
F-42023 Saint-étienne Cédex 2  
Olivier.Boissier@emse.fr

\*\*\* Université de Lyon - Université Jean Monnet - Laboratoire Hubert Curien - CNRS  
18 rue Benoit Laurus  
F-42000 Saint-Etienne  
Francois.Jacquenet@univ-st-etienne.fr

---

*RÉSUMÉ.* L'évolution actuelle de l'informatique rend inéluctable un traitement automatique des données sensibles (l'identité des utilisateurs...). Celles-ci transitent souvent à l'insu des entités concernées. Ceci pose un ensemble de problèmes liés à la confidentialité, ou respect de la sphère privée. Nous proposons une solution à ce problème au travers du modèle HiMAS, systèmes multi-agents hippocratiques, préservant la sphère privée. Dans cet article nous nous présentons le protocole de transaction de données sensibles de ce modèle HiMAS.

*ABSTRACT.* The current evolution of IT has increased the automatic processing of sensitive data (user's identity...) in information processing systems. This information is often diffused without the consent of the entities concerned. We propose a solution to this problem with the HiMAS model aiming at privacy management. In this paper, we focus on the presentation of a protocol dedicated to the transaction of sensitive data used in a HiMAS.

*MOTS-CLÉS :* systèmes multi-agents, sphère privée, transaction de données sensibles.

*KEYWORDS:* multi-agent systems, privacy, sensitive data transaction.

---

## 1. Introduction

L'utilisation des systèmes multi-agents (SMA) pour la manipulation de données sensibles est de plus en plus fréquente. Par exemple dans le cadre d'un système de gestion d'agendas électroniques par des agents assistants (Demazeau *et al.*, 2006), les rendez-vous des utilisateurs et leurs propriétés sont des données sensibles manipulées et échangées entre des agents. Le problème de la transmission de données sensibles au sein d'un système multi-agent est d'autant plus présent qu'un utilisateur délègue ses informations sensibles à un agent autonome. Les interactions étant essentielles dans les systèmes multi-agents, ces données sont échangées et courent le risque d'être divulguées, tronquées, modifiées, etc.

Cet article se focalise sur la gestion et la protection des informations sensibles au sein des systèmes multi-agents. En anglais, le terme *privacy* permet de se référer à tout ce qui a trait aux données sensibles, à leur traitement et à leur protection. En français il n'y a pas de traduction communément acceptée (intimité, confidentialité, vie privée, etc). Dans la suite de cet article, nous utiliserons le terme *sphère privée* comme le fait le sociologue P. Demeulenaere (Demeulenaere, 2002) pour faire référence aux problématiques attachées à la *privacy*.

Notre travail s'inscrit dans le cadre du modèle de systèmes multi-agents hippocratiques (HiMAS), modèle prenant en compte la sphère privée (Crépin *et al.*, 2008). Ce modèle définit le concept de sphère privée ainsi que neuf principes normatifs à respecter pour assurer la protection des données sensibles. Le terme *hippocratique*, en référence à Hippocrate, implique que ce modèle traite des aspects moraux et éthiques du respect de la sphère privée en imposant aux agents du système multi-agent de se plier à un ensemble de principes tels le médecin envers son patient.

Dans cet article, nous nous intéressons plus particulièrement à une étape précise de la préservation de la sphère privée : la protection des informations sensibles échangées lors des communications entre agents. Une telle communication est appelée par la suite *transaction de données sensibles*. Nous proposons ici un protocole de transaction de données sensibles, inspiré du P3P (W3C, 2002; Cranor, 2002), dans le cadre de ce modèle de systèmes multi-agents hippocratiques.

La prochaine section présente différentes visions du concept de sphère privée que l'on peut rencontrer dans différents domaines. La section 3 présente le modèle HiMAS en commençant par la gestion de la sphère privée pour finir par les neuf principes normatifs de ce modèle. La section suivante se consacre au protocole de transaction de données sensibles qui s'appuie sur les principes intervenant lors d'une transaction de données sensibles. Finalement nous concluons et proposons quelques perspectives.

## 2. Sphère privée : définitions, approches et besoins

La sphère privée en informatique concerne cinq types d'applications selon (Deswarte *et al.*, 2006) (i) la protection des adresses IP, (ii) la protection de la localisa-

tion, (iii) la gestion de l'anonymat, (iv) les autorisations respectant la vie privée et (v) l'accès aux données et leur gestion. Notre travail relevant de ce dernier type d'applications, nous présentons dans cette section un panorama des différentes visions relatives à l'accès et à la gestion de données sensibles sur internet, dans les bases de données et également dans les systèmes multi-agents.

### **2.1. Plate-forme pour les préférences de confidentialité (P3P)**

La plate-forme pour les préférences de confidentialité (P3P) (W3C, 2002; Cranor, 2002) est une initiative du consortium W3C visant à développer un standard pour gérer les informations de la sphère privée des côtés client et serveur.

Dans ce contexte, un utilisateur définit ses préférences pour la gestion de ses données personnelles sensibles. Une *préférence* définit les contraintes que les utilisateurs souhaitent imposer sur la gestion et la manipulation des données personnelles. De son côté, le serveur ayant à gérer ces données définit une politique à cet effet, et s'engage à s'y tenir. Une *politique* spécifie les objectifs de la collecte de données qui va être réalisée, l'utilisation ainsi que la durée de conservation des données privées recueillies.

Ce standard permet donc de spécifier des contraintes sur la gestion de données sensibles. Il fait cependant l'objet de plusieurs critiques (Thibadeau, 2000). On lui reproche notamment de ne fournir qu'une description des accords passés entre un client et un serveur sur une transaction mettant en œuvre des données sensibles, sans se préoccuper de la vérification de l'engagement du serveur.

### **2.2. Bases de données et respect de la sphère privée**

Le contrôle d'accès à base de rôles (RBAC) (Sandhu *et al.*, 1996) a été développé dans le but de permettre le contrôle dynamique des accès aux données dans les organisations dynamiques et les systèmes d'information complexes.

La notion de rôle est définie ici comme étant un ensemble de permissions d'accès attachées à des types d'utilisateurs. Pour assurer une gestion dynamique et flexible de l'accès aux données, le contrôle d'accès à base de rôles utilise des sessions. Chaque session représente une mise en correspondance entre un utilisateur et un rôle. Cela permet d'attribuer un ensemble de permissions pour chaque utilisateur lors de chaque requête.

Cette technologie ne s'intéresse pas à la phase de collecte des informations sensibles mais uniquement à la consultation de ces dernières après leur collecte. Même si le contrôle d'accès à base de rôles impose plus de contraintes sur l'utilisation de données sensibles que le P3P, nous pouvons regretter l'absence de contrôle sur le devenir de ces informations après leur accès.

Englobant les principes du P3P et du contrôle d'accès à base de rôles, le modèle de bases de données hippocratiques (Agrawal *et al.*, 2002; LeFevre *et al.*, 2004; Agrawal *et al.*, 2005) renforce le contrôle d'accès à base de rôles dans le domaine des bases de données en définissant un ensemble de dix principes intégrant ceux du P3P. Ces travaux de recherche définissent un modèle de système de gestion de bases de données prenant en compte la gestion et la protection de la sphère privée des utilisateurs en imposant le respect des dix principes suivants :

1) **Consentement de l'utilisateur** : un utilisateur doit donner son accord pour chacune des données propres qui sont recueillies.

2) **Connaissance des différents objectifs** : afin de donner son consentement sur la collecte de données, un utilisateur doit être au courant des objectifs dans lesquels cette collecte est réalisée.

3) **Limitation de la collecte de données** : un système de gestion de bases de données hippocratiques s'engage à limiter le nombre de données qu'il recueille pour un objectif donné.

4) **Limitation de l'utilisation des données** : un système de gestion de bases de données hippocratiques s'engage à restreindre l'utilisation des données recueillies aux objectifs transmis à l'utilisateur (cf principe 2).

5) **Limitation de la diffusion des données** : un système de gestion de bases de données hippocratiques s'engage à diffuser le moins possible les informations sensibles des utilisateurs.

6) **Limitation de la rétention des données** : un système de gestion de bases de données hippocratiques s'engage à ne conserver les données seulement pendant le laps de temps correspondant au délai nécessaire à leur utilisation.

7) **Sécurité** : un système de gestion de bases de données hippocratiques assure un niveau élevé de sécurité afin d'éviter toute collection frauduleuse. La mise en place d'un tel niveau de sécurité intervient lors des accès aux bases et lors du stockage des informations sensibles.

8) **Transparence des données** : au sein d'un système de gestion de bases de données hippocratiques, l'utilisateur doit avoir accès aux informations qui lui sont propres afin de connaître celles qui sont encore stockées. L'utilisateur doit pouvoir effectuer des mises à jour de ces informations.

9) **Exactitude des données** : un système de gestion de bases de données hippocratiques impose le fait que les données stockées dans une base de données hippocratique doivent être exactes pendant leur durée de rétention.

10) **Conformité** : un système de gestion de bases de données hippocratiques permet à tout utilisateur d'avoir la possibilité de vérifier le respect de chacun des principes précédents.

Dans un système de gestion de bases de données hippocratiques, les informations sensibles sont préservées lors de leur stockage, lors des communications, et leur de-

venir est également pris en considération. Aucun mécanisme de sanction envers les systèmes ne répondant pas à ces principes n'est cependant abordé dans ces travaux.

### 2.3. Systèmes multi-agents et sphère privée

Du fait des nombreuses interactions, et donc des nombreuses communication de données sensibles, entre agents logiciels autonomes, le respect de la sphère privée est devenu un aspect important dans le domaine des systèmes multi-agents.

Massacci *et al.* répondent à quelques-unes des limites, dont l'absence de mécanismes de sanction, dont souffrent les travaux portant sur les systèmes de gestion de bases de données hippocratiques (Massacci *et al.*, 2007). Ils proposent d'intégrer les bases de données hippocratiques dans TROPOS, une méthode de développement de logiciel orientée agent prenant en compte les besoins non fonctionnels, afin de protéger la sphère privée lors des échanges entre deux bases de données. Pour ce faire, ils introduisent la notion de confiance pour chacune des bases de données. La confiance est utilisée ici pour augmenter le niveau de sécurité entre les différentes bases. Cependant, ces travaux ne prennent pas en considération le lien entre les utilisateurs et la base de données comme le font Agrawal *et al.*, aspect très important dans le cadre du respect de la sphère privée.

Dans les problèmes de satisfaction de contraintes distribuées, le respect de la sphère privée est assimilé à la protection de données lors du partage de connaissance entre agents. Ce respect est assuré par la diminution du partage et donc par l'augmentation des secrets (états courants cachés des agents) entre les agents. Avec cette approche, les algorithmes des solveurs sont de moins en moins efficaces pour un respect de plus en plus complet, comme le remarque (Freuder *et al.*, 2001). Un premier type d'approche dans ce domaine pour la préservation de la sphère privée consiste en un ensemble de techniques cryptographiques (Yokoo *et al.*, 2005) mais ces algorithmes s'avèrent trop coûteux. Pour diminuer ce coût, de nombreuses approches proposent d'utiliser des algorithmes de permutation aléatoire entre les agents pour assurer le respect de la sphère privée comme par exemple (Silaghi *et al.*, 2004; Greenstadt *et al.*, 2006) ce qui permet de diminuer l'utilisation de techniques cryptographiques tout en aboutissant à un résultat acceptable.

Ces travaux soulèvent la question de la sécurité informatique des données sensibles lors du respect de la sphère privée. Les méthodes cryptographiques sont nécessaires à ce respect mais, étant trop coûteuses, elle doivent être assistées par d'autres méthodes de plus haut niveau. Ces approches s'occupent principalement du traitement des informations sensibles sans attacher d'importance aux problématiques liées à la collection et au devenir de ces informations ce qui est pourtant primordial dans le contexte du respect de la sphère privée.

Dans le cadre des systèmes multi-agents, en plus d'un niveau de sécurité élevé lors du stockage et des communications, (Bergenti, 2005) propose l'intervention d'un agent garant pour la transmission d'une information sensible entre deux agents afin

d'assurer le respect de leur sphère privée. Cet agent représente en fait un intermédiaire entre les deux autres agents de la communication des données, il garantit les informations transmises ainsi que le respect des volontés des deux parties. L'avantage majeur de cette technique réside dans le fait que les agents peuvent concentrer leur confiance en une seule entité, l'agent garant.

(Rezgui *et al.*, 2002) propose un modèle permettant d'assurer le respect de la sphère privée au sein des services web. Pour ce faire, il définit plusieurs éléments essentiels à la communication d'informations sensibles entre un utilisateur et un service web et entre service web. L'utilisateur définit un profil dynamique pour gérer sa sphère privée. Ce profil permet de qualifier les données en termes de protection. Ensuite, le service définit une politique pour les données qu'il souhaite recueillir. La communication entre l'utilisateur et le service web passe par un agent intermédiaire. Cet agent crée des filtres à partir des profils de l'utilisateur afin de garantir la protection de ses informations sensibles lors de chaque communication en vérifiant si la politique du service correspond bien aux souhaits de l'utilisateur. Ce type d'approche est également utilisé dans (Cissée *et al.*, 2007) qui propose d'utiliser un agent garant avec des techniques de filtrage et des profils utilisateurs pour préserver la sphère privée lors des interactions entre les agents.

#### **2.4. Synthèse : besoins du respect de la sphère privée**

Ces différents travaux sur le problème de la préservation de la sphère privée nous permettent de constater que les problématiques liées à la préservation de la sphère privée ne relèvent pas uniquement du domaine de la sécurité en termes de cryptographie. De plus, ces études nous indiquent que la manière de recueillir des données sensibles ou leur traitement ne constituent pas les principales étapes à prendre en considération. En effet, le respect de la sphère privée demande à être étudié lors de trois phases critiques : le stockage des données sensibles, la transaction de données sensibles et le comportement de l'entité qui reçoit de telles données.

##### **2.4.1. Stockage**

Le stockage des données sensibles contenues dans la sphère privée demande un niveau de sécurité élevé afin de prévenir les attaques possibles et d'en contrôler les accès comme le souligne (Agrawal *et al.*, 2002) avec le septième principe des bases de données hippocratiques.

##### **2.4.2. Transaction**

Lors de la transaction de données sensibles, les agents doivent utiliser un support de communication sécurisé afin que de telles données ne soient pas interceptées (Sandhu *et al.*, 1996; Agrawal *et al.*, 2002; Rezgui *et al.*, 2002; Bergenti, 2005; Cissée *et al.*, 2007). De plus, l'entité qui fournit de telles données doit être en mesure de déterminer les impacts futurs d'une telle transaction en termes de diffusion, d'utilisation et de rétention (W3C, 2002; Cranor, 2002; Agrawal *et al.*, 2002).

### 2.4.3. Comportement

Afin que l'entité (l'utilisateur ou le serveur) qui fournit les données sensibles puisse déterminer les impacts de la diffusion de ses données sensibles, l'entité qui reçoit ces données doit fournir une description des manipulations qu'elle envisage de réaliser sur ces données. De plus, cette dernière entité doit s'engager à ne pas exécuter d'autres manipulations hormis celles décrites (W3C, 2002; Cranor, 2002; Agrawal *et al.*, 2002). Une fois la transaction de données sensibles terminée, les agents doivent être capables de vérifier la sincérité sur cet engagement de l'entité qui reçoit les données (Agrawal *et al.*, 2002). Pour finir, son comportement doit être garanti : détection des violations de cet engagement, application des sanctions et prévention des utilisateurs sur les comportements suspicieux<sup>1</sup>.

Dans la suite de cet article, notre travail se focalise sur la deuxième phase du respect de la sphère privée : la transaction de données sensibles. Avant d'aborder cette problématique, nous présentons dans la prochaine section le modèle des systèmes multi-agents hippocratiques.

## 3. HiMAS : systèmes multi-agents hippocratiques

L'étude des différents travaux présentés dans la section précédente nous ont conduit à définir les problématiques attachées à la sphère privée et à présenter un modèle opérationnel, que nous appelons HiMAS (hippocratic multi-agent systems) (Crépin *et al.*, 2008). Il modélise le concept de sphère privée, sa gestion et sa protection, en prenant en compte les trois phases impliquées dans sa gestion avec l'ensemble des exigences qui en découle.

Dans la suite de cet article, nous considérons une application concrète de gestion d'agendas distribués (Demazeau *et al.*, 2006) comme domaine permettant d'illustrer le modèle HiMAS. Dans cette application, un rendez-vous est caractérisé par un nom, les participants, une date de début, une date de fin, un niveau d'importance et un niveau d'urgence (ces deux dernières propriétés sont subjectives à chaque utilisateur). Chaque utilisateur est assisté par un agent logiciel ayant en charge son agenda. L'agenda peut être partagé avec les autres agents. Pour fixer un rendez-vous entre plusieurs utilisateurs, cette application propose deux méthodes. La première est fondée sur le partage des agendas, ce qui permet aux agents d'avoir un accès direct aux données. La seconde utilise un système de négociation afin de ne pas divulguer les données dans le cas où les agendas ne sont pas partagés. Nous nous focalisons dans notre travail sur la première méthode impliquant un partage des agendas car il s'agit de communication de données sensibles relatives aux calendriers des utilisateurs entre deux agents.

---

1. Agent violant la sphère privée des autres agents du système en accédant, en altérant, en endommageant ou en détruisant des données sensibles de la sphère privée d'un autre agent sans autorisation (Baase, 2002).

Nous définissons d'abord notre modèle de la sphère privée puis nous développons les neuf grands principes normatifs du modèle HiMAS.

### 3.1. *Sphère privée*

Comme nous l'avons vu en section 2, nous considérons que la sphère privée d'un agent concerne toutes les données qu'il désire protéger des autres. Seul l'agent concerné par les données sensibles détient les droits de propriété sur ces données (Thomson, 1975). La sphère privée est personnelle (Demeulenaere, 2002; Baase, 2002), personnalisable (l'agent concerné juge de ce qu'elle doit contenir) (Westin, 1967; Warren *et al.*, 1985; Lessig, 2000) et contextuelle (elle dépend du contexte courant dans lequel l'agent interagit avec les autres agents) (Bellotti *et al.*, 1993; Palen *et al.*, 2003).

Les agents d'un HiMAS construisent, font évoluer et protègent la représentation de leur sphère privée.

Afin de donner une vision globale de la sphère privée, nous définissons la sphère privée d'un agent, notée *SP*, par un quadruplet de quatre ensembles<sup>2</sup> :

$$SP ::= \langle \textit{Eléments}, \textit{Autorisations}, \textit{Règles}, \textit{Normes} \rangle$$

#### 3.1.1. *Eléments de la sphère privée*

Nous définissons un élément de la sphère privée, *élément*, comme un sextuplet :

$$\textit{élément} \in \textit{Eléments}$$

*élément* ::=  $\langle id, \textit{donnée}, \textit{Propriétaires}, \textit{contexte}, \textit{Sujets}, \textit{Références} \rangle$  avec :

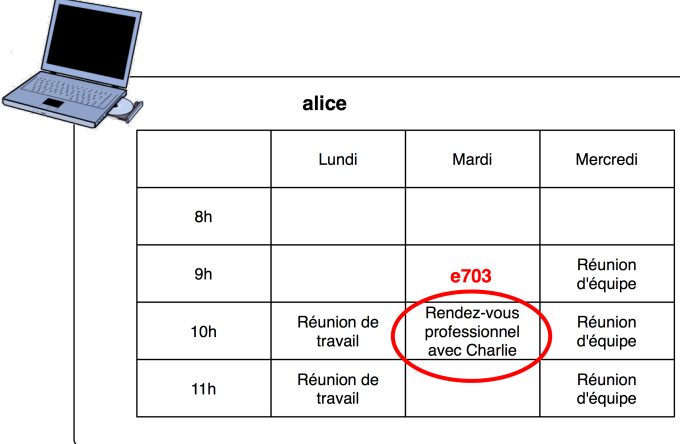
- *id* : identifiant de l'élément,
- *donnée* : donnée sensible contenue dans l'élément de la sphère privée,
- *Propriétaires* : ensemble des identifiants des agents connus possédant la donnée sensible à un instant donné,
- *contexte* : contexte représentant les éléments de la donnée sensible propres au domaine,
- *Sujets* : ensemble des agents concernés par la donnée sensible,
- *Références* : ensemble des références vers les données sensibles qui peuvent être déduites à partir de la connaissance de *donnée*.

---

2. Par convention, nous notons les ensembles avec une majuscule et les éléments appartenant à ces ensembles par une minuscule.

## Exemple

Soit  $e703$  l'identifiant de l'élément concernant la donnée sensible  $rdv$  représentant le rendez-vous de l'agenda de l'agent *alice*, figure 1.

$$\langle e703, rdv, \{alice, charlie\}, professionnel, \{alice, charlie\}, \{mardi - 10h, \{alice, charlie\}, important, urgent\} \rangle$$


alice			
	Lundi	Mardi	Mercredi
8h			
9h		e703	Réunion d'équipe
10h	Réunion de travail	Rendez-vous professionnel avec Charlie	Réunion d'équipe
11h	Réunion de travail		Réunion d'équipe

**Figure 1.** Agenda de l'agent *alice*

Ce rendez-vous a lieu à une date précise, *mardi* – 10h. Les agents *alice* et *charlie* sont les participants et sont les seuls à connaître cette information sensible.

Une donnée sensible peut faire référence à d'autres données sensibles :  $rdv$  fait référence à la date *mardi* – 10h, au niveau d'importance et d'urgence de la réunion ou encore aux participants  $\{alice, charlie\}$ .

Afin qu'un agent puisse raisonner sur la diffusion des données sensibles, un élément est associé à un ensemble de propriétaires. Dans le cas de l'élément  $e703$ , les propriétaires de l'information sensible  $rdv$  sont les agents *alice* et *charlie*.

Un élément de la sphère privée contient également l'ensemble des *sujets* de l'information sensible. Pour  $e703$ , les *sujets* sont les agents participant à la réunion, soit *alice* et *charlie*.

Un élément appartient également à un certain contexte : par exemple, un rendez-vous de travail est associé au milieu professionnel, donc le contexte de  $e703$  est *professionnel*.

### 3.1.2. Autorisations d'un élément de la sphère privée

Les autorisations d'un élément de la sphère privée permettent à un agent de définir les opérations qu'il autorise sur une information sensible. Nous avons défini cinq autorisations représentant les manipulations possibles des éléments de la sphère privée relatives au modèle dans lequel notre travail s'inscrit : utiliser, supprimer, diffuser, changer et mentir sur un élément de la sphère privée<sup>3</sup>.

Nous définissons une autorisation par :

$$\begin{aligned} \text{autorisation} \in \text{Autorisations} = \\ \{ \text{utiliser}, \text{supprimer}, \text{diffuser}, \text{changer}, \text{mentir sur} \} \end{aligned}$$

#### Exemple

Soit  $e703$  l'élément défini précédemment, nous pouvons définir les cinq autorisations suivantes :

–  $\text{utiliser}(e703)$

La donnée sensible contenue dans l'élément  $e703$  peut être utilisée par l'agent.

–  $\text{supprimer}(e703)$

Cette autorisation permet à un agent de supprimer l'élément  $e703$  de sa sphère privée.

–  $\text{diffuser}(e703)$

L'agent possédant l'élément  $e703$  dans sa sphère privée a le droit de diffuser la donnée sensible de  $e703$ .

–  $\text{changer}(e703)$

Cette autorisation permet à un agent de modifier l'élément  $e703$ , afin de mettre à jour une donnée sensible par exemple.

–  $\text{mentir sur}(e703)$

L'agent a le droit de mentir sur la donnée sensible de  $e703$  pour en assurer sa protection. L'explication de cette autorisation est fournie dans la sous-section suivante pour plus de clarté.

### 3.1.3. Règles de la sphère privée d'un agent

Du fait que la sphère privée est définie de manière contextuelle, qu'elle évolue dynamiquement au cours du temps et qu'elle est intrinsèquement personnelle, nous lui associons un ensemble de règles permettant de spécifier les conditions d'activation des autorisations présentées précédemment.

Une règle de la sphère privée est définie de la façon suivante :

$$\begin{aligned} \text{règle} \in \text{Règles} \\ \text{règle} ::= \text{autorisation}(id) \leftarrow \text{condition} \end{aligned}$$

3. Selon le domaine du système multi-agent hippocratique, l'ensemble de ces autorisations peut être modifié par l'ajout ou la suppression d'une ou de plusieurs manipulations possibles.

Les conditions de type *condition* sont relatives à l'état de l'environnement dans lequel se trouve l'agent et à celui de l'élément de la sphère privée. De plus, lorsqu'un agent envoie des données sensibles de sa sphère privée à un autre, cette transaction a pour but de satisfaire un objectif donné. De ce fait, les conditions sont également relatives aux objectifs de la transaction.

#### Exemple

Soit  $e703$  l'élément défini précédemment, *professionnel* le contexte relatif aux rendez-vous de travail et  $fixerUneReunion_{professionnel}$  un objectif donné représentant la fait de fixer une réunion de travail.

$$utiliser(e703) \leftarrow fixerUneReunion_{professionnel}$$

Cette règle permet à l'agent d'utiliser la donnée sensible de  $e703$  afin de prendre un autre rendez-vous seulement dans le contexte professionnel .

Les règles d'une sphère privée permettent à un agent de définir la dynamique interne de celle-ci selon ses désirs et donc de prendre en compte le caractère personnel de la sphère privée.

L'ensemble des règles est dynamique : son contenu est influençable par les différents événements qui se produisent. Par exemple, une règle peut permettre à un agent de diffuser un rendez-vous professionnel, et, suite à l'ajout d'un nouveau participant à cette réunion, cette donnée ne pourra plus être diffusée afin de respecter les préférences de ce dernier participant. En plus des changements dus à l'évolution temporelle, les règles de la sphère conduisent également à une évolution personnelle, selon les préférences de l'agent propriétaire de la sphère privée.

#### 3.1.4. Normes de la sphère privée

Le dernier point abordé au niveau de la représentation d'une sphère privée concerne l'impact que peut avoir la société dans laquelle se trouve l'agent.

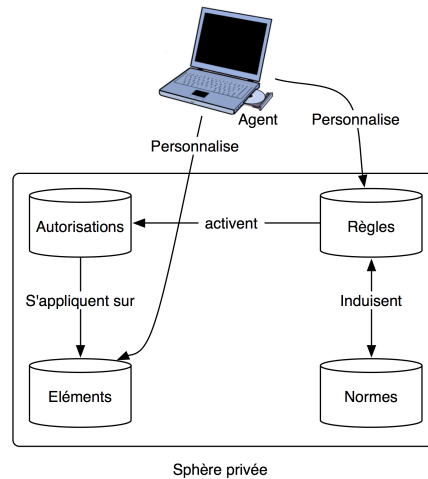
Nous définissons les normes (Boella *et al.*, 2007) relatives à la sphère privée de manière similaire aux règles associées à la sphère privée.

$$norme \in Normes$$

$$norme ::= autorisation(id) \leftarrow condition$$

#### 3.1.5. Relations internes entre objets de la sphère privée

Un agent personnalise sa sphère privée en choisissant l'ensemble des éléments qui la constitue et donc l'ensemble des données qu'il estime être sensibles. Il personnalise également l'ensemble des règles qui se rapportent aux autorisations sur les éléments de sa sphère privée selon ses préférences, comme le montre la figure 2. Cette personnalisation permet de prendre en considération l'ensemble des souhaits de l'utilisateur,



**Figure 2.** *Sphère privée d'un agent*

que ce soit en termes de sensibilité de l'information ou en termes de gestion de telles données.

Au niveau du raisonnement de l'agent, les autorisations représentent les manipulations possibles des éléments de la sphère privée par les agents et elles sont activées selon les conditions des règles. Les normes peuvent imposer aux agents de nouvelles règles de la sphère privée dans le but d'être respectées et les règles peuvent modifier l'ensemble des normes de la société. En effet, lorsque l'ensemble des agents respectent les mêmes règles, la société d'agents peut alors décider d'imposer de nouvelles normes correspondant à ces règles. Ce dynamisme est un aspect essentiel pour le respect de la sphère privée car il intervient directement sur la gestion de la sphère privée par les agents (Piolle, 2009).

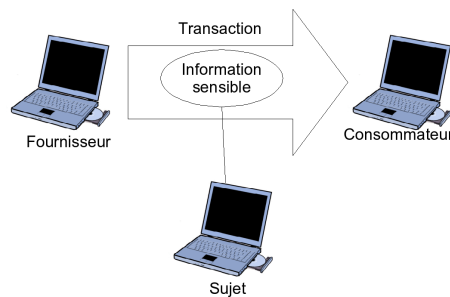
La sphère privée étant définie, nous pouvons maintenant présenter les neuf principes normatifs qui permettent aux agents d'assurer le respect de cette sphère.

### 3.2. *Les neuf principes des HiMAS*

Le modèle de systèmes multi-agents hippocratiques, HiMAS, est inspiré de celui proposé par Agrawal *et al.* dans le cadre des bases de données hippocratiques (Agrawal *et al.*, 2002). Les systèmes multi-agents hippocratiques adaptent neuf des dix principes des systèmes de gestion de bases de données hippocratiques en prenant en considération des mécanismes de sanction pour les agents suspicieux afin de préserver de la sphère privée.

Pour représenter les positionnements possibles d'un agent par rapport à la sphère privée, trois rôles ont été définis (cf. figure 3) :

- Le rôle de *consommateur* caractérise l'agent qui demande la donnée sensible.
- Le rôle de *fournisseur* décrit l'agent qui reçoit cette demande<sup>4</sup>.
- L'agent concerné par une donnée sensible incarne le rôle *sujet*.



**Figure 3.** Rôles des agents

Selon le modèle HiMAS, un système multi-agent hippocratique doit respecter les neuf principes normatifs suivants.

1) **Consentement** : un système multi-agent hippocratique impose que chaque transaction de données sensibles doit requérir le consentement du fournisseur. Par exemple, lorsqu'un consommateur demande à un fournisseur son planning à une date précise, le fournisseur doit donner son accord. Dans le cas où le fournisseur et le sujet ne sont pas le même agent, ce consentement est également demandé et doit respecter les préférences du sujet. Par exemple, si le consommateur demande à un fournisseur le planning d'un troisième agent (représentant le sujet), le fournisseur transmettra cette donnée seulement à condition que le sujet et lui-même soient consentants.

2) **Connaissance des objectifs** : dans un système multi-agent hippocratique, le fournisseur doit connaître les objectifs motivant la collecte des données sensibles. Ainsi, s'il le souhaite, il a la possibilité de calculer les conséquences de cet échange. Par exemple, le consommateur indique que s'il désire avoir le planning du fournisseur, c'est dans l'objectif de prendre un rendez-vous avec lui. Le fournisseur peut ainsi décider dans de meilleures conditions s'il transmet ou non la donnée sensible.

3) **Collection minimale** : un système multi-agent hippocratique impose à tout consommateur de s'engager à se restreindre à une quantité minimale de données pour la réalisation d'un même ensemble d'objectifs. Par exemple, lorsque le consommateur

4. Cette vision centrée utilisateur est à l'opposé de celle centrée service en termes de consommateur et de fournisseur.

demande son planning au fournisseur pour fixer un nouveau rendez-vous, le consommateur a uniquement besoin de connaître les plages horaires libres et occupées du fournisseur. Il ne doit pas chercher à obtenir plus de données comme par exemple l'objet des rendez-vous ou les participants.

4) **Utilisation minimale** : un système multi-agent hippocratique demande à tout consommateur de s'engager à n'utiliser une donnée sensible demandée à un fournisseur que pour satisfaire les objectifs qu'il a spécifiés et rien de plus. Dans le contexte de la gestion d'agendas, le consommateur doit par exemple utiliser le planning demandé uniquement pour fixer un nouveau rendez-vous entre lui et le fournisseur. Le consommateur ne peut pas demander à utiliser cette donnée sensible pour la communiquer à un tiers par exemple car cela ne fait pas partie de ses objectifs.

5) **Diffusion minimale** : un système multi-agent hippocratique impose à tout consommateur de s'engager à ne diffuser une donnée sensible que si ses objectifs l'exigent et ce, le moins de fois possible et au minimum d'agents possible. La valeur de cette limitation dépend des objectifs de la transaction. Dans l'exemple de la prise de rendez-vous, le consommateur n'a nullement besoin de diffuser le planning du fournisseur pour prendre un rendez-vous.

6) **Rétention minimale** : dans un système multi-agent hippocratique, tout consommateur s'engage à ne conserver une donnée sensible que pendant un certain laps de temps. Celui-ci doit être fixé au plus petit délai requis pour la réalisation des objectifs du consommateur. Par exemple, pour la prise de rendez-vous, le consommateur s'engage à effacer le planning du fournisseur une fois le rendez-vous pris ou, le cas échéant, la date du rendez-vous dépassée.

7) **Sécurité** : un système multi-agent hippocratique doit garantir la sécurité des données sensibles pendant leur stockage et les transactions.

8) **Transparence** : dans un système multi-agent hippocratique, la donnée sensible transmise doit rester accessible au sujet et/ou fournisseur pendant la durée de rétention. La transparence permet au fournisseur de mettre à jour les données sensibles qu'il a pu transmettre. Par exemple, si le planning du fournisseur change et que le nouveau rendez-vous n'a pas encore été pris, il doit avoir la possibilité de mettre à jour le planning connu par le consommateur, et ce afin que la prise de rendez-vous se base sur des données exactes.

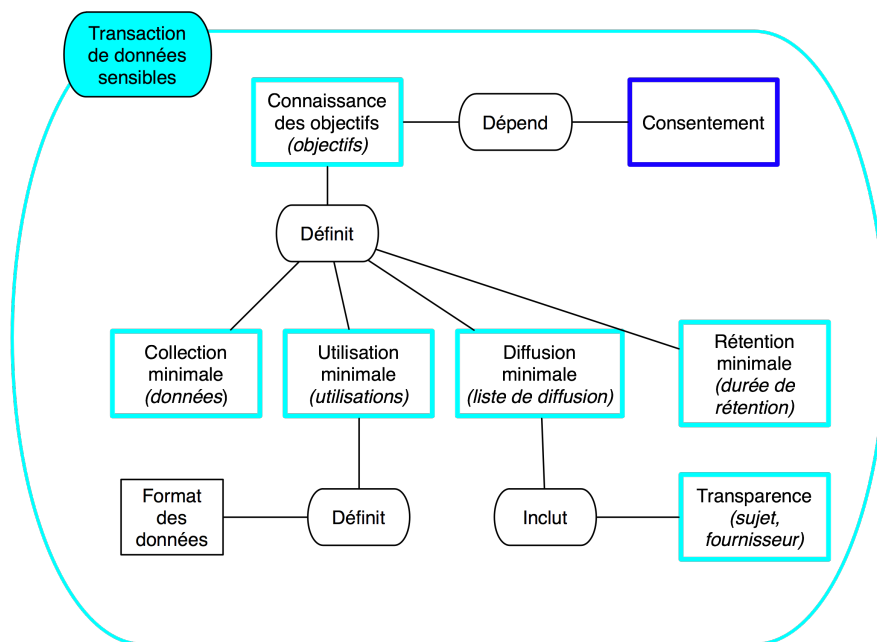
9) **Conformité** : un système multi-agent hippocratique impose à tout agent d'être capable de vérifier le respect des principes précédents et de prévenir tout comportement suspicieux (ou déviant).

Notons qu'un principe des bases de données hippocratiques n'a pas été retenu pour les HiMAS : celui qui impose l'exactitude des données sensibles. En effet, dans le contexte des systèmes multi-agents, un agent doit avoir la possibilité de mentir (i.e. altérer la donnée) pour protéger sa sphère privée. Par exemple, le fait de refuser de donner une donnée sensible à un agent suspicieux peut souvent révéler cette donnée ou du moins une partie. Lorsqu'un fournisseur juge un consommateur comme suspicieux, deux possibilités s'offrent à lui. La première consiste à ignorer la requête du consommateur. La deuxième consiste à mentir sur la donnée sensible demandée.

L'utilisation du mensonge permet de ne pas dévoiler au consommateur qu'il est jugé comme suspicieux. Cette solution permet de ce fait de discréditer le consommateur suspicieux auprès des autres agents lorsqu'il dévoilera une donnée sensible erronée. Une première piste de travail pour que les agents d'un HiMAS puissent juger de la fiabilité des autres agents consiste à utiliser des processus de construction et de gestion de la confiance comme par exemple (Castelfranchi, 2000; Castelfranchi *et al.*, 1998; Muller, 2006; Sabater, 2002). Pour l'instant, cet axe de recherche représente une des perspectives de notre travail.

### 3.3. Expression sémantique des principes d'un HiMAS

Afin de définir plus précisément les principes d'un HiMAS, nous les étudions sous un aspect sémantique et déterminons les différents liens qui existent entre eux, figure 4. Cette étude commence par le regroupement des principes en trois groupes intervenant à différentes étapes dans le raisonnement des agents d'un HiMAS : ceux qui entrent en jeu lors de la transaction de données sensibles, ceux qui interviennent lors des interactions entre agents et finalement ceux qui sont en lien avec le système.



**Figure 4.** Graphique conceptuel de la sémantique des neuf principes d'un HiMAS

Cette étude sémantique nous permet d'exclure deux principes qui n'interviennent pas dans une transaction de données sensibles. Le premier est en relation avec les

interactions qui permettent la définition du neuvième principe : la conformité (principe 9). De plus, le principe de sécurité (principe 7) ne concerne pas directement le raisonnement des agents d'un HiMAS. Ce principe intervient lors de la conception du système multi-agent et ne fait donc pas partie de la formalisation présentée dans ce document car il est indépendant du raisonnement des agents d'un HiMAS.

Lors d'une transaction de données sensibles, le fournisseur définit une *politique* et le consommateur une *préférence* afin que chaque agent puisse définir ses autorisations sur les manipulations des données sensibles.

La politique du consommateur et la préférence du fournisseur sont semblables à celles définies dans (W3C, 2002). Elles comportent les objectifs<sup>5</sup> de la transaction, la date de suppression des données recueillies, une liste de diffusion des agents susceptibles de recevoir ces données et le format de la donnée.

Afin de pouvoir mettre en correspondance une politique et une préférence (voir 4.4.3.), une transaction de données sensibles est constituée des données sensibles à transmettre, de la politique et du consentement du fournisseur (représenté par une mise en correspondance de la préférence et de la politique).

Sept des neuf principes des HiMAS doivent être respectés pour qu'une transaction de données sensibles puisse se dérouler dans un tel système (figure 4) :

– **2. Connaissance des objectifs** : le consommateur demande des données sensibles à un fournisseur afin de réaliser certaines tâches. Celles-ci permettent de définir les objectifs du consommateur qui peut alors les transmettre au fournisseur.

– **3. Collection minimale** : une fois que le consommateur a défini ses objectifs, il peut alors sélectionner les données sensibles dont il a besoin pour les réaliser.

– **4. Utilisation minimale** : les objectifs étant définis, le consommateur peut déterminer les utilisations possibles des données recueillies.

– **5. Diffusion minimale** : la spécification des objectifs permet au consommateur de déterminer les agents pouvant recevoir les données sensibles recueillies.

– **6. Rétention minimale** : la spécification des objectifs définit combien de temps le consommateur va pouvoir garder en mémoire les données sensibles.

– **8. Transparence** : la transparence implique que le fournisseur et/ou le sujet appartiennent à la liste de diffusion.

– **1. Consentement** : la mise en correspondance entre une politique et une préférence représente le principe du consentement, établi après le respect des précédents principes.

Dans cet article, nous nous focalisons sur la problématique de la transaction de données sensibles dans un HiMAS. La section suivante présente ainsi une formalisa-

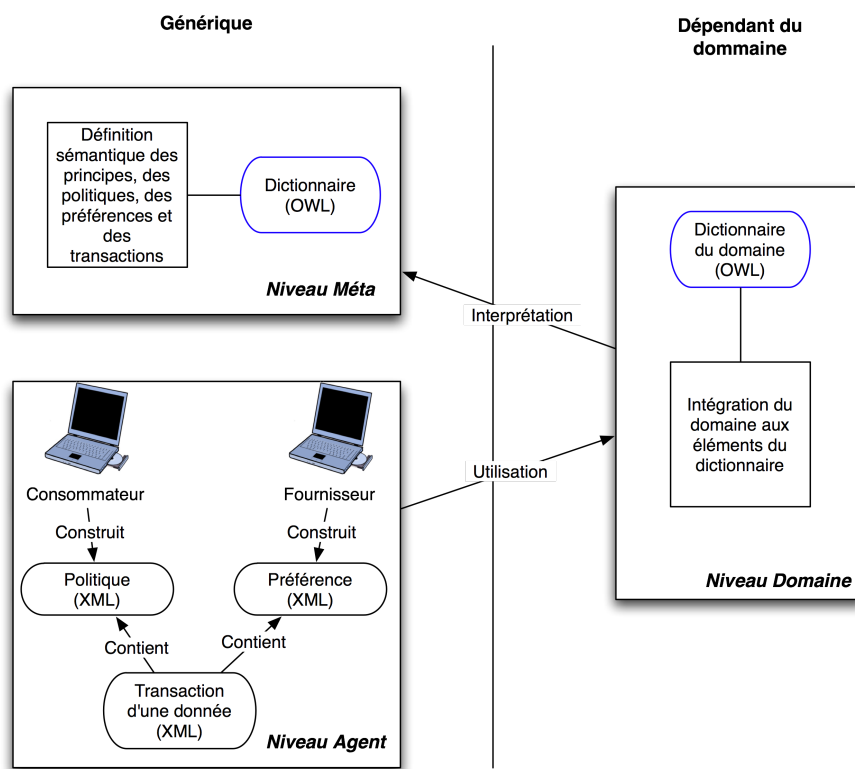
---

5. Les objectifs se rapprochent de la notion de désir, comme par exemple dans le modèle BDI (Bratman, 1987).

tion des principes intervenant lors d'une telle transaction, nous amenant à définir notre protocole de transaction de données sensibles.

#### 4. Protocole de transaction de données sensibles

Les principes qui nous intéressent ici permettent aux agents de définir leur politique et leur préférence pour une transaction de données sensibles. Cette vision des principes requiert l'étude préalable des travaux existants sur les politiques portant sur des politiques, les métapolitiques. Ces principes ne s'appliquant qu'aux transactions de données sensibles, nous proposons de formaliser un protocole de transaction de données sensibles s'appuyant sur des métapolitiques pour les décrire formellement et les implémenter au sein d'un HiMAS.



**Figure 5.** Architecture de modélisation et d'implémentation du protocole de transaction de données sensibles

Nous proposons de définir ces métapolitiques dans un dictionnaire qui définit les principes à respecter lors d'une transaction de données sensibles en guidant la concep-

tion d'une politique et d'une préférence à un niveau méta. Un dictionnaire du domaine est également considéré afin d'inclure les éléments contextuels pour le raisonnement des agents. Ces derniers construisent alors leur préférence et leur politique, et donc une transaction de données sensibles, en se référant au dictionnaire du domaine.

Ces dictionnaires doivent être communs aux agents d'un HiMAS afin que chaque agent fonde son raisonnement sur un même vocabulaire et une même sémantique. Nous choisissons de modéliser ces deux dictionnaires par des ontologies extérieures aux agents et consultables par l'ensemble de ces derniers. De cette manière, les modifications apportées aux dictionnaires ne posent pas de problème de propagation et requièrent uniquement l'intervention d'une seule entité de contrôle. De plus, avec cette approche, plusieurs HiMAS relatifs à un domaine commun peuvent se référer aux mêmes dictionnaires, ce qui nous permet de considérer l'ouverture entre plusieurs HiMAS ayant le même domaine.

L'architecture permettant de modéliser et implémenter le protocole de transaction de données sensibles que nous proposons est résumée dans la figure 5. L'avantage d'un tel procédé vient de la possibilité de vérifier les contraintes exprimées dans les principes d'un HiMAS grâce aux dictionnaires.

Nous commençons par présenter un panorama des principaux travaux existant dans le domaine des métapolitiques. Nous présentons ensuite une formalisation du protocole que nous proposons en étudiant d'abord le niveau méta, puis le niveau domaine et finalement le niveau agent. Une implémentation de ce protocole est présentée dans la section suivante.

#### **4.1. Métapolitiques**

Cette section présente brièvement les principaux travaux existant dans le domaine des métapolitiques afin d'en fournir une vision générale.

Les métapolitiques ont été introduites par Hosmer dans (Hosmer, 1991; Hosmer, 1992). Ces articles décrivent des politiques qui portent sur des politiques. Ces métapolitiques permettent de définir des règles de coordination sur les politiques de sécurité d'un système. Les travaux de Kühnhauser (Kühnhauser, 1995) les utilisent pour l'interface de politiques complexes coexistantes et pour la coopération et la résolution de conflits entre politiques. Dans le système PONDER (Lupu *et al.*, 2000; Twidle *et al.*, 2007), elles sont utilisées pour décrire les politiques de sécurité et résoudre les conflits.

Pour résumer, les métapolitiques ont en général pour objectif de gérer l'ensemble des politiques de sécurité d'un système en garantissant leur définition et la détection de conflits.

Les principes des HiMAS définissent des lignes directrices pour le raisonnement des agents et donc pour leurs politiques et préférences. Ainsi ces principes représentent

des métapolitiques pour le comportement des agents en relation avec la communication et les manipulations des données sensibles.

Cependant, dans notre cas d'étude, la notion de politique n'est pas la même que dans les travaux portant sur la sécurité. Les principes d'un HiMAS permettent aux agents de raisonner sur un ensemble de contraintes sur leur comportement et non de gérer l'ensemble des politiques des agents. Nous proposons donc d'étudier les métapolitiques comme une spécialisation des métaconnaissances introduites par Pitrat (Pitrat, 1990) : elles portent sur des connaissances représentant uniquement les politiques des consommateurs d'un HiMAS.

Cette différence nous amène également à représenter autrement les principes d'un HiMAS. Sachant que la sphère privée est contextuelle, ces principes doivent donner une définition formelle et générique des lignes directrices de comportement que les agents prennent en compte lors d'une transaction de données sensibles. Afin de permettre aux agents de raisonner sur ces principes, nous les définissons dans un dictionnaire sous forme de graphe conceptuel (Sowa, 1984) où chaque concept représente l'élément majeur d'un principe relié sémantiquement à un autre par une relation binaire, voir figure 4.

#### 4.2. Niveau méta

Le deuxième principe des HiMAS est au cœur du raisonnement relatif à la transaction de données sensibles (cf figure 4). Ce principe permet aux agents de définir la durée de rétention, la collection de données, la liste de diffusion incluant le principe de transparence, les différentes utilisations possibles ainsi que le format de la donnée demandée (liste des références requises). A partir de la connaissance des objectifs, le fournisseur est également apte à donner ou non son consentement.

$\forall x \text{ objectifs}(x)$	$\rightarrow \exists y \text{ définit}(x, y) \wedge \text{données}(y)$
$\forall x \text{ objectifs}(x)$	$\rightarrow \exists y \text{ définit}(x, y) \wedge \text{utilisations}(y)$
$\forall x \text{ objectifs}(x)$	$\rightarrow \exists y \text{ définit}(x, y) \wedge \text{listeDiffusion}(y)$
$\forall x \text{ objectifs}(x)$	$\rightarrow \exists y \text{ définit}(x, y) \wedge \text{duréeRétention}(y)$
$\forall y \text{ utilisations}(y)$	$\rightarrow \exists z \text{ définit}(y, z) \wedge \text{format}(z)$
$\forall y \text{ listeDiffusion}(y)$	$\rightarrow \exists z \text{ inclut}(y, z) \wedge \text{sujet}(z)$
$\forall y \text{ listeDiffusion}(y)$	$\rightarrow \exists z \text{ inclut}(y, z) \wedge \text{fournisseur}(z)$
$\forall w \text{ consentement}(w)$	$\rightarrow \exists x \text{ dépend}(w, x) \wedge \text{objectifs}(x)$

**Tableau 1.** Formalisation des principes en logique du premier ordre

Chaque principe et le format représentent un concept relié à un autre selon un lien sémantique. Afin d'obtenir une définition formelle, nous utilisons un fragment de la logique existentielle, positive et conjonctive du premier ordre afin de ne pas obtenir de données logiques contradictoires. Nous représentons ainsi chacun de ces concepts

par un prédicat atomique et chaque relation par un prédicat binaire. La description formelle du graphe conceptuel de la figure 4 est décrite dans le tableau 1.

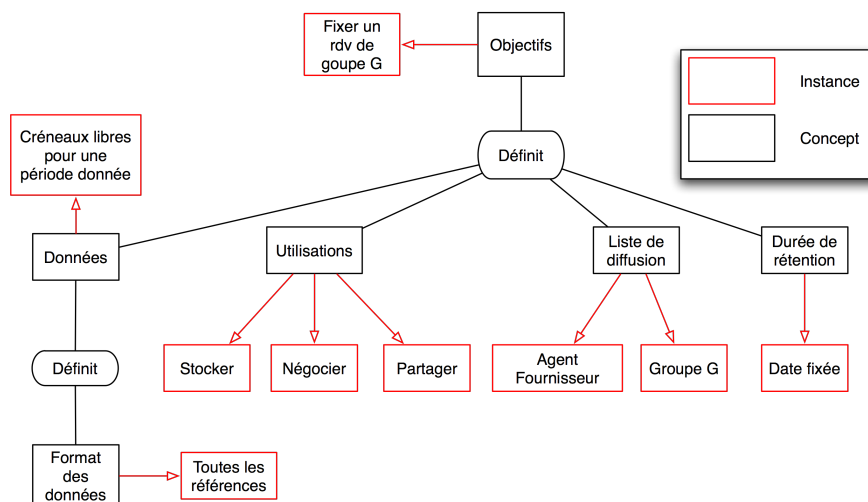
L'implémentation de ce graphe conceptuel se fait par le biais d'une ontologie définie en OWL (W3C, 2004). Ce procédé permet de définir les principes comme un ensemble de classes instanciables (*Objectifs* pour le principe de connaissance des objectifs, *Données* pour le principe de collection minimale, *Utilisations* pour le principe d'utilisation minimale, *ListeDiffusion* pour le cinquième principe de diffusion minimale et *DuréeRétention* pour de principe de rétention minimale) reliées par les relations sémantiques (*définit*, *inclut*).

### 4.3. Niveau domaine

Les principes d'un HiMAS définissent à un niveau méta les différentes relations entre les principes que les agents doivent appliquer pour préserver la sphère privée. Ce niveau méta est à mettre en relation avec le domaine du HiMAS du fait de la contextualité de la sphère privée.

Le dictionnaire au niveau méta définit un vocabulaire pour le dictionnaire du domaine. Ce dernier instancie le dictionnaire du niveau méta en donnant toutes les valeurs possibles aux classes selon le domaine et en mettant en relation ses valeurs.

Nous avons choisi un cas simple de transaction de données sensibles : fixer un rendez-vous de groupe. Nous considérons les créneaux horaires et leurs caractéristiques comme les données sensibles.



**Figure 6.** Instanciation du dictionnaire du domaine pour l'objectif « fixer un rendez-vous de groupe »

Dans cet exemple, un consommateur veut fixer un rendez-vous avec un fournisseur et d'autres agents d'un même groupe (groupe G) dans une période donnée (un intervalle de temps borné par deux créneaux de temps). La figure 6 illustre ce cas d'étude. Nous considérons ici que le fournisseur incarne également le rôle de sujet.

Pour fixer un tel rendez-vous, nous définissons les contraintes suivantes :

- Les données sensibles que le consommateur peut collecter sont les créneaux libres pour une période donnée.
- Les données sensibles peuvent être fournies avec toutes les références que le fournisseur permet de diffuser.
- Les données recueillies par le consommateur ne peuvent pas être conservées en mémoire au-delà d'une date fixée.
- Le consommateur peut diffuser ces données sensibles aux agents du groupe G et il doit en garantir l'accès au fournisseur.
- Les utilisations possibles des données sensibles dans le contexte de la détermination d'un rendez-vous de groupe sont de stocker les données recueillies, de les utiliser pour négocier un rendez-vous avec le fournisseur et de partager ces données avec les agents du groupe G.

Le dictionnaire du domaine s'implémente en instanciant les classes de fichier OWL avec les valeurs fournies dans la figure 6. Pour notre exemple, la classe *Objectifs* s'instancie par la valeur « fixer-un-rendez-vous-de-groupe » et cette valeur définit les valeurs « créneaux-libres », « négocier, stocker, partager », « date-fixée » et « agent-fournisseur, groupe G » pour les classes *Données*, *Utilisations*, *DuréeRétention* et *ListeDiffusion*.

Ces deux dictionnaires définissent les sept principes d'un HiMAS liés au raisonnement des agents lors d'une transaction de données sensibles. Ils représentent le vocabulaire contextuel nécessaire aux agents pour se comprendre et envisager les différents impacts d'une transaction de données sensibles.

#### 4.4. Niveau agent

Nous nous intéressons ici à l'utilisation que peuvent faire les agents d'un HiMAS des deux dictionnaires présentés précédemment.

Nous définissons un protocole de transaction pour les données sensibles. Celui-ci est fondé sur ces deux dictionnaires et il spécifie la façon dont se déroulent les transactions de données au sein d'un HiMAS.

Lors d'une transaction de données sensibles, le consommateur construit sa politique en fonction de ses besoins et du dictionnaire de domaine et selon le dictionnaire du domaine (figure 5). Le fournisseur définit sa préférence à partir des règles de sa sphère privée tout en respectant le dictionnaire du domaine. Avant d'effectuer une transaction de données sensibles, les agents d'un HiMAS émettent un jugement les

uns sur les autres pour juger de leur fiabilité (Crépin *et al.*, 2008). Lorsque celle-ci est jugée satisfaisante, la transaction peut alors commencer. Cette fonction peut être implémentée par un processus de gestion de la confiance comme dans (Damiani *et al.*, 2004).

La préférence du fournisseur et la politique du consommateur sont spécifiées sous forme de fichiers XML devant se conformer à un schéma XSD prédéfini. Pour que le protocole soit mené à terme, une première contrainte impose donc que le fichier XSD valide le fichier XML.

Un agent ne doit pas transmettre une donnée sensible sans prendre conscience des impacts que cette transaction pourrait avoir. Un agent doit posséder une représentation de son contexte (par exemple, professionnel ou personnel pour un rendez-vous) en plus de sa propre sphère privée afin de la protéger.

Les agents appartenant au HiMAS doivent également pouvoir émettre un jugement sur les autres agents afin de déterminer la prise de risque encourue à diffuser un élément de leur sphère privée. Cette prise de risque peut se calculer par exemple à travers la confiance accordée et le réseau de confiance de l'agent auquel la donnée est transmise, comme dans (Damiani *et al.*, 2004; Massacci *et al.*, 2007).

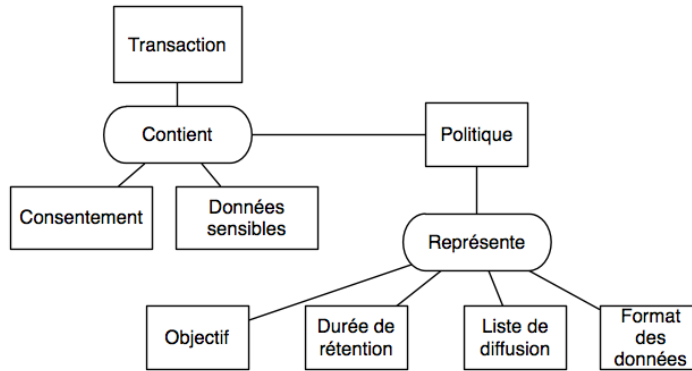
#### 4.4.1. Politique

Un consommateur construit sa politique en fonction des objectifs qu'il doit atteindre. La connaissance de ceux-ci permet donc à un agent de construire sa politique en utilisant le dictionnaire du domaine afin qu'il soit compris des autres agents et que son comportement soit respectueux de la sphère privée.

Dans notre dictionnaire du domaine, les objectifs du consommateur sont reliés sémantiquement à tous les autres principes utilisés dans une transaction de données sensibles. Le dictionnaire du domaine contient, pour chaque objectif, toutes les valeurs possibles pour les classes représentant ces principes. Ainsi un consommateur peut savoir s'il viole la sphère privée ou non en vérifiant que les éléments de sa politique soient contenus dans le dictionnaire du domaine et qu'ils respectent les relations sémantiques.

Afin de définir entièrement notre protocole, il faut que cette politique soit syntaxiquement correcte vis-à-vis du schéma XSD. Une politique doit donc contenir la spécification des objectifs, la date de suppression des données sensibles collectées, la liste de diffusion de ces données et l'ensemble des références demandées pour chaque donnée, figure 7.

Une fois que le consommateur a déterminé ses objectifs, il choisit donc les concepts relatifs à ce dernier et construit une politique syntaxiquement correcte grâce au schéma prédéfini XSD et sémantiquement correcte grâce au dictionnaire du domaine. Par exemple, un consommateur peut demander un agenda à un fournisseur « user.magma2 » pour fixer un rendez-vous avec un groupe de travail en incluant toutes les instances du graphe conceptuel correspondant (voir figure 8).



**Figure 7.** Description d'une transaction de données sensibles

#### 4.4.2. Transaction de données sensibles

Une fois que le consommateur a défini et validé sa politique, la transaction de données sensibles peut se réaliser à son initiative.

Nous avons défini une transaction de données sensibles comme un ensemble contenant une politique, une préférence, le consentement du fournisseur et les données sensibles demandées par le consommateur.

Chacune des valeurs possibles pour les éléments d'une transaction de données sensibles est définie dans le dictionnaire du domaine afin que le consommateur construise une transaction valide pour le respect de la sphère privée d'un point de vue sémantique comme dans l'exemple présenté dans la figure 8.

<pre> &lt;TransactionDonneesSensibles&gt;   &lt;ID value="8"/&gt;   &lt;consent value="false"/&gt;   &lt;objectif value="FixerRdvGroupe"&gt;     &lt;collection&gt;       &lt;donneeSensible id="CréneauxLibres" value="null"/&gt;     &lt;/collection&gt;   &lt;/collection&gt;   &lt;listeDiffusion&gt;     &lt;Sujet ID="user.magma2"/&gt;     &lt;Fournisseur ID="user.magma2"/&gt;     &lt;Groupe ID="travail"/&gt;   &lt;/listeDiffusion&gt; </pre>	<pre> &lt;utilisations&gt;   &lt;utilisation value="Stocker"/&gt;   &lt;utilisation value="Négociier"/&gt;   &lt;utilisation value="Partager"/&gt; &lt;/utilisations&gt; &lt;dureeRetention value="FinDeSession"/&gt; &lt;format&gt;   &lt;reference value="Importance"/&gt;   &lt;reference value="Urgence"/&gt; &lt;/format&gt; &lt;/objective&gt; &lt;/TransactionDonneesSensibles&gt; </pre>
---	--

**Figure 8.** Exemple de fichier de transaction de données sensibles

Pour construire une transaction de données sensibles correcte d'un point de vue syntaxique, nous adoptons le même procédé que pour une politique. Nous définissons une transaction de données sensibles d'un point de vue formel (figure 7). Notons

que ce formalisme ne fait pas référence à la préférence du fournisseur. En effet, une préférence et une politique s'appuyant sur les mêmes concepts, nous modélisons la préférence du fournisseur par les modifications qu'il induit à la politique du consommateur si elle ne lui convient pas.

Une fois le fichier de la transaction de données sensibles créé et validé, le consommateur l'envoie au fournisseur afin que ce dernier prenne connaissance de sa requête.

#### 4.4.3. *Préférence*

A partir des règles de sa sphère privée portant sur l'utilisation, la diffusion et la rétention de ses données sensibles, un fournisseur est en mesure de déterminer sa préférence en accord avec le dictionnaire du domaine. Une fois qu'il a reçu un fichier de transaction de données sensibles, cette préférence lui permet d'accepter ou non la politique du consommateur.

Avant de s'intéresser à la politique du consommateur, le fournisseur doit en premier lieu vérifier la validité de la transaction d'un point syntaxique (vérification des schémas) et d'un point de vue sémantique (vérification du dictionnaire du domaine). Ces deux validations permettent de déterminer si un consommateur a un comportement suspicieux sur les limitations imposées par les principes d'un HiMAS et sur le protocole de transaction de données sensibles.

Si la transaction de données sensibles est validée, le fournisseur peut alors mettre en correspondance sa préférence avec la politique du consommateur. Pour ce faire, le fournisseur vérifie que les instances de la politique reçue sont des instances ou des sous-instances de sa préférence dans le dictionnaire du domaine. Dans le cas où cette mise en correspondance échoue, le fournisseur peut proposer des adaptations de la politique du consommateur et la lui renvoyer. Par exemple, suite à la réception du fichier présenté dans la figure 8, le fournisseur « user.magma2 », ne désirant pas pouvoir négocier ses rendez-vous, enlève l'utilisation possible « Négocier » du fichier XML et le renvoie au consommateur.

Une fois le consommateur et le fournisseur en accord sur les termes de la politique, le fournisseur complète la transaction de données sensibles avec les valeurs des données sensibles demandées. Le consommateur inclut donc dans sa sphère privée des éléments nouveaux relatifs aux données sensibles recueillies ainsi que les règles traduisant la préférence du fournisseur sur les manipulations de ces données. Si aucun accord n'est trouvé, la transaction n'aboutit pas et le fournisseur ne peut pas satisfaire la requête du consommateur.

#### 4.5. *Protocole de communication de données sensibles*

La figure 9 présente le protocole de transactions de données sensibles que nous venons de présenter sous un formalisme UML.

Ce protocole de transaction est centré utilisateur et se place à l'opposé des protocoles de communication rencontrés dans la littérature qui sont essentiellement centrés service tout en reprenant les principes de (W3C, 2002). Pour que le respect de la sphère privée soit complet, ce protocole doit être intégré à un média de communication sécurisé (principe de sécurité).

## 5. Implémentation

Afin de valider notre protocole, nous présentons dans cette section l'extension d'une application de gestion d'agendas distribués (Demazeau *et al.*, 2006) intégrant la capacité à effectuer des transactions de données sensibles au sein d'un HiMAS.

### 5.1. Gestion d'agendas distribués

L'architecture de cette application permet à chaque agent de gérer le calendrier d'un utilisateur. Chaque agenda est constitué de ressources, représentant les créneaux horaires. Ces ressources peuvent être libres ou occupées par un rendez-vous, caractérisées par un nom, les participants, un niveau d'urgence et d'importance, subjectifs aux utilisateurs.

L'application propose également l'utilisation d'un agent spécifique, l'agent serveur, qui a pour rôle d'inscrire chaque nouvel agent et de mettre en relation l'ensemble des agents du système. Cet agent a donc pour but de gérer les envois de message selon leur type (négociation de rendez-vous ou partage d'agendas).

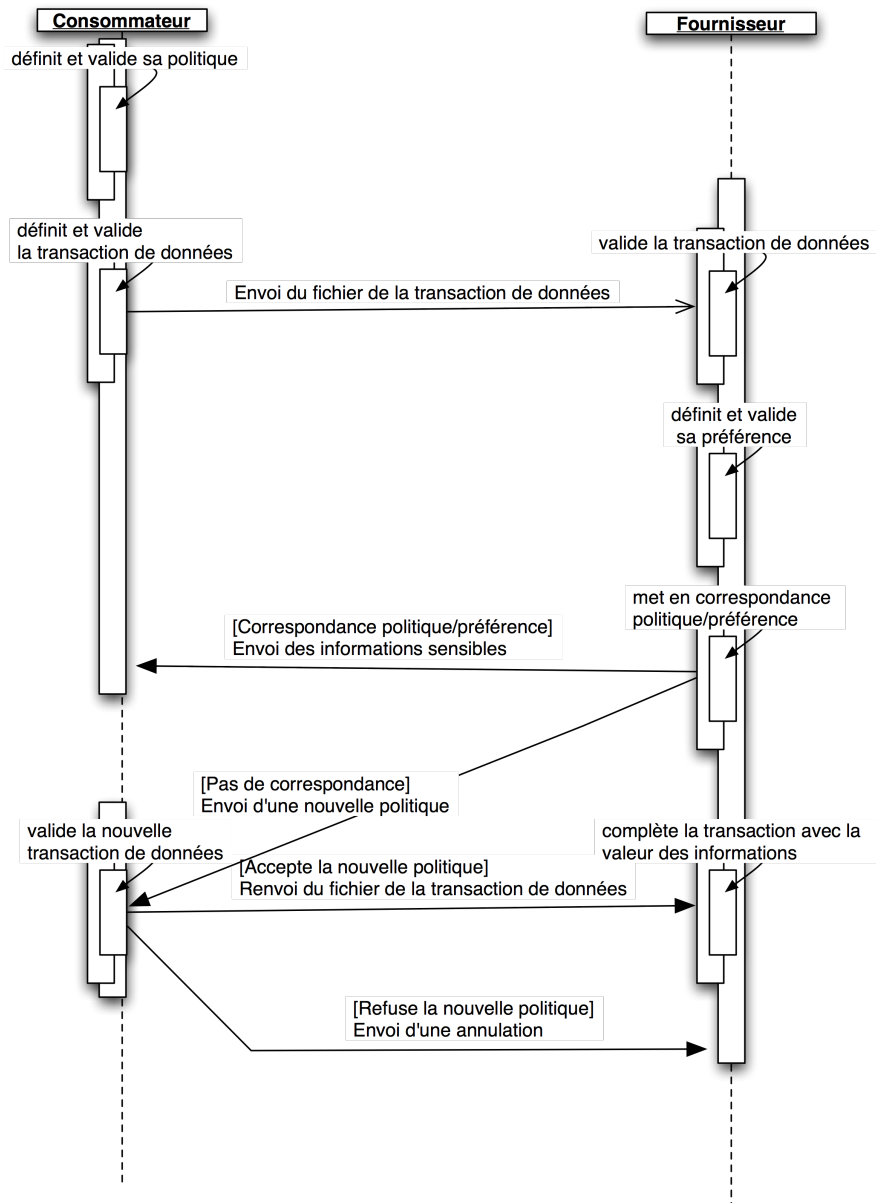
L'envoi de messages s'effectue grâce à un serveur GMAIL utilisant le protocole de communication Jabber. Ce protocole permet d'assurer la sécurité et la confidentialité des communications ainsi que la décentralisation de l'application.

### 5.2. Extensions hippocratiques

La première étape de l'évolution de cette application vers un système multi-agent hippocratique consiste à intégrer notre protocole de transaction de données sensibles lors des partages d'agendas dans (Demazeau *et al.*, 2006). Pour ce faire, nous avons développé trois objectifs possibles pour les partages de calendriers : s'informer, fixer un rendez-vous entre deux agents, fixer un rendez-vous avec un groupe d'agents.

Pour implémenter notre protocole, nous interprétons le dictionnaire du domaine selon les trois objectifs cités précédemment (cf section 4.3. et figure 6). Ce dictionnaire est implémenté en OWL et accessible par l'ensemble des agents de l'application.

Au niveau du raisonnement des agents, lorsqu'un utilisateur désire recevoir l'agenda d'un tiers, il indique à l'agent en charge de son propre agenda les objectifs du partage. Cet agent analyse alors le dictionnaire du domaine afin de créer une



**Figure 9.** *Protocole de transaction de données sensibles*

politique en accord avec le respect de la sphère privée. Dans le cas où l'utilisateur souhaite personnaliser la politique, nous lui permettons de restreindre les valeurs définies dans le dictionnaire du domaine, tout en vérifiant la préservation de la sphère privée. Une fois la politique créée, l'agent consommateur l'envoie à l'agent fournisseur.

Le fournisseur prend connaissance de la politique et vérifie s'il existe une relation de confiance avec le consommateur<sup>6</sup>. Si cette relation existe, le consommateur poursuit la transaction de données sensibles, sinon il l'annule.

Ensuite, selon les préférences de l'utilisateur, le fournisseur accepte ou non la politique du consommateur. Les préférences de l'utilisateur représentent des restrictions des ensembles du dictionnaire du domaine. Chaque changement est vérifié par l'agent afin de respecter la sphère privée. Dans le premier cas, le fournisseur envoie l'agenda demandé. Dans le second, il envoie automatiquement au consommateur une nouvelle politique correspondant aux préférences de l'utilisateur. Le consommateur choisit alors d'accepter ou non cette nouvelle politique selon les souhaits de l'utilisateur qu'il représente.

## 6. Conclusion et perspectives

Nos recherches s'inscrivent dans un cadre spécifique, les systèmes multi-agents hippocratiques (HiMAS). De tels systèmes se doivent de respecter neuf principes fondamentaux qui leur permettent d'assurer la gestion et la protection de la sphère privée au sein de leurs agents.

Un agent d'un HiMAS doit être en mesure de représenter sa sphère privée en mémorisant ses caractéristiques (personnelles et contextuelles) et en la gérant seul. Néanmoins, une fois qu'une donnée sensible de cette sphère vient à être diffusée, la société d'agents doit entrer en jeu afin de détecter les manipulations frauduleuses éventuelles de cette donnée et donc les manquements au respect de la sphère privée.

En adaptant neuf des principes des bases de données hippocratiques (Agrawal *et al.*, 2002) aux systèmes multi-agents, les HiMAS garantissent la communication d'une donnée sensible et fournissent également une surveillance sur le devenir de cette donnée dans le système, contrairement aux modèles à agents ou au P3P (W3C, 2002).

Notre protocole de transaction de données sensibles permet d'appliquer sept principes d'un HiMAS : 1. Consentement, 2. Connaissance des objectifs, 3. Collecte minimale, 4. Utilisation minimale, 5. Diffusion minimale, 6. Rétention minimale et 8. Transparence.

Le respect de ces principes s'effectue en considérant notre protocole selon trois niveaux. Au niveau méta, les principes sont définis dans un dictionnaire les reliant. Le niveau domaine représente l'instanciation de ce dictionnaire selon le domaine. Au

---

6. Pour plus d'informations sur le modèle de confiance implémenté, nous renvoyons le lecteur à l'article (Demazeau *et al.*, 2006).

niveau agent, les agents utilisent le dictionnaire du domaine pour construire une transaction de données sensibles.

En associant sémantiquement les principes, nous déterminons dans le dictionnaire du domaine l'ensemble maximal des manipulations de données sensibles qu'un consommateur peut exécuter sur celles qu'il recueille. Un fournisseur peut alors vérifier qu'un consommateur respecte les principes limitatifs en se référant à ce dictionnaire. Afin qu'aucun principe ne soit omis, nous formalisons également cette interaction spécifique, ce qui contribue également à la détection d'un agent suspicieux.

Le fait d'inclure un dictionnaire du domaine dans notre protocole permet de ne pas être confronté au même problème que le P3P (Thibadeau, 2000) : la mise en correspondance entre une politique et une préférence se fait en fonction du dictionnaire du domaine, ce qui permet aux agents de comprendre les intentions des consommateurs. Un autre avantage de l'introduction d'un dictionnaire du domaine réside en la possibilité de définir les limitations imposées par les principes d'un HiMAS.

Les principes liés à une transaction de données sensibles étant définis, nos perspectives de travail se portent maintenant sur le principe de conformité qui est relié à la problématique de l'interaction entre agents. Une première piste consiste à instaurer un contrôle social (Castelfranchi, 2000) en relation avec la fonction de jugement des agents. Nous envisageons de modéliser cette fonction par un processus de construction et de gestion de la confiance (Castelfranchi *et al.*, 1998).

#### Remerciements

Ce travail a bénéficié du soutien du projet web intelligence, financé par le cluster ISLE de la région Rhône-Alpes.

## 7. Bibliographie

- Agrawal R., Bird P., Grandison T., Kiernan J., Logan S., Rjaibi W., « Extending Relational Database Systems to Automatically Enforce Privacy Policies. », *Proceedings of the International Conference on Data Engineering*, IEEE Computer Society, p. 1013-1022, 2005.
- Agrawal R., Kiernan J., Srikant R., Xu Y., « Hippocratic Databases. », *Proceedings of the International Conference on Very Large Data Bases*, Morgan Kaufmann, p. 143-154, 2002.
- Baase S., *A Gift of Fire : Social, Legal, and Ethical Issues in Computing*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2002.
- Bellotti V., Sellen A., « Design for Privacy in Ubiquitous Computing Environments », *Proceedings of the European Conference on Computer Supported Cooperative Work*, Kluwer Academic Publishers, p. 77-92, 1993.
- Bergenti F., « Secure, Trusted and Privacy-aware Interactions in Large-Scale Multiagent Systems », *Proceedings of the Workshop From Objects to Agents*, Pitagora Editrice Bologna, p. 144-150, 2005.
- Boella G., van der Torre L. W. N., Verhagen H., « Introduction to Normative Multiagent Systems », *Normative Multi-agent Systems*, vol. 07122 of *Dagstuhl Seminar Proceedings*,

- Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2007.
- Bratman M. E., *Intention, Plans, and Practical Reason*, O'Reilly, Harvard University Press : Cambridge, MA, 1987.
- Castelfranchi C., « Engineering Social Order », *Proceeding of the International Workshop Engineering Societies in the Agent World*, vol. 1972 of *Lecture Notes in Computer Science*, Springer, p. 1-18, 2000.
- Castelfranchi C., Falcone R., « Principles of Trust for MAS : Cognitive Anatomy, Social Importance, and Quantification », *Proceedings of the International Conference on Multiagent Systems*, IEEE Computer Society, p. 72-79, 1998.
- Cissée R., Albayrak S., « Experimental analysis of privacy loss in DCOP algorithms », *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems*, ACM, p. 1424-1426, 2007.
- Cranor L. F., *Web Privacy with P3P*, O'Reilly, 2002.
- Crépin L., Vercouter L., Jacquenet F., Demazeau Y., Boissier O., « Hippocratic Multi-Agent Systems », *Proceedings of the 10th International Conference of Enterprise Information Systems*, p. 301-308, 2008.
- Damiani E., di Vimercati S. D. C., Paraboschi S., Samarati P., « P2P-Based Collaborative Spam Detection and Filtering », *Proceedings of the International Conference on Peer-to-Peer Computing*, IEEE Computer Society, p. 176-183, 2004.
- Demazeau Y., Melaye D., Verrons M.-H., « A Decentralized Calendar System Featuring Sharing, Trusting and Negotiating. », *Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, vol. 4031 of *Lecture Notes in Computer Science*, Springer, p. 731-740, 2006.
- Demeulenaere P., « Les difficultés de la caractérisation de la notion de la vie privée d'un point de vue sociologique », *La protection de la vie privée dans la société d'information*, vol. 11, 2002. Groupe d'études Société d'information et vie privée.
- Deswarte Y., Melchor C. A., « Current and future privacy enhancing technologies for the Internet », *Annales des Télécommunications*, vol. 61, p. 399-417, 2006.
- Freuder E. C., Minca M., Wallace R. J., « Privacy/efficiency tradeoffs in distributed meeting scheduling by constraint-based agents », *Notes of the International Joint Conference on Artificial Intelligence Workshop on Distributed Constraint Reasoning*, p. 63-71, 2001.
- Greenstadt R., Pearce J. P., Bowring E., Tambe M., « Experimental analysis of privacy loss in DCOP algorithms », *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems*, ACM, p. 1424-1426, 2006.
- Hosmer H. H., « Metapolicies I », *ACM SIGSAC Data Management Workshop*, vol. 10, n° 2-3, p. 18-43, 1991.
- Hosmer H. H., « Metapolicies II », *Proceeding of the National Computer Security Conference*, Elsevier Advanced Technology Publications, p. 369-378, 1992.
- Kühnhauser W. E., « A Paradigm for User-Defined Security Policies », *Symposium on Reliable Distributed Systems*, p. 135-144, 1995.
- LeFevre K., Agrawal R., Ercegovac V., Ramakrishnan R., Xu Y., DeWitt D. J., « Limiting Disclosure in Hippocratic Databases. », *Proceedings of the International Conference on Very Large Data Bases*, Morgan Kaufmann, p. 108-119, 2004.

- Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 2000.
- Lupu E., Sloman M., Dulay N., Damianou N., « Ponder : Realising Enterprise Viewpoint Concepts », *Proceedings of the International Enterprise Distributed Object Computing Conference*, IEEE Computer Society, p. 66-75, 2000.
- Massacci F., Mylopoulos J., Zannone N., « From Hippocratic Databases to secure Tropos : a computer-aided re-engineering approach », *International Journal of Software Engineering and Knowledge Engineering*, vol. 17, p. 265-284, 2007.
- Muller G., Utilisation de normes et de réputations pour détecter et sanctionner les contradictions, PhD thesis, Ecole Nationale Supérieure des Mines, Saint-Etienne, 2006.
- Palen L., Dourish P., « Unpacking "privacy" for a networked world », *Proceedings of the International Conference on Human Factors in Computing Systems*, ACM, p. 129-136, 2003.
- Piolle G., Agents utilisateurs pour la protection des données personnelles : modélisation logique et outils informatiques, PhD thesis, Université Joseph Fourier - Grenoble I, Grenoble, France, 2009.
- Pitrat J., *Métacognition, Futur de l'Intelligence Artificielle*, Hermès, 1990.
- Rezgui A., Ouzzani M., Bouguettaya A., Medjahed B., « Preserving privacy in web services », *Proceedings of the Workshop on Web Information and Data Management*, p. 56-62, 2002.
- Sabater J., Trust and Reputation for Agent Societies, PhD thesis, Universitat Autònoma de Barcelona, Spain, 2002.
- Sandhu R. S., Coyne E. J., Feinstein H. L., Youman C. E., « Role-Based Access Control Models », *IEEE Computer*, vol. 29, n° 2, p. 38-47, 1996.
- Silaghi M.-C., Rajeshirke V., « The Effect of Policies for Selecting the Solution of a DisCSP on Privacy Loss », *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems*, IEEE Computer Society, p. 1396-1397, 2004.
- Sowa J. F., *Conceptual Structures : Information Processing in Mind and Machine*, Addison-Wesley, 1984.
- Thibadeau R., « A critique of P3P : Privacy on Web », 2000, [dollar.ecom.cmu.edu/p3pcritique/](http://dollar.ecom.cmu.edu/p3pcritique/).
- Thomson J. J., « The Right of Privacy », *Philosophy and Public Affairs* 4 : 295-314, 1975.
- Twidle K. P., Lupu E., « Ponder2 - Policy-Based Self Managed Cells », *Proceedings of the International Conference on Autonomous Infrastructure, Management and Security*, vol. 4543 of *Lecture Notes in Computer Science*, Springer, p. 230, 2007.
- W3C, « Platform for Privacy Preferences », 2002, <http://www.w3.org/P3P/>.
- W3C, « OWL Web Ontology Language », 2004, <http://www.w3.org/TR/owl-features/>.
- Warren S. D., Brandeis L. D., *The right to privacy*, Wadsworth Publ. Co., Belmont, CA, USA, 1985.
- Westin A. F., « Special report : legal safeguards to insure privacy in a computer society », *Commun. ACM*, vol. 10, n° 9, p. 533-537, 1967.
- Yokoo M., Suzuki K., Hirayama K., « Secure distributed constraint satisfaction : reaching agreement without revealing private information », *Artificial Intelligence*, vol. 161, n° 1-2, p. 229-245, 2005.