HAL
open science

Une Logique pour Raisonner sur la Protection des Données Personnelles

Guillaume Piolle, Yves Demazeau

▶ **To cite this version:**

Guillaume Piolle, Yves Demazeau. Une Logique pour Raisonner sur la Protection des Données Personnelles. 16e congrès francophone AFRIF-AFIA sur la Reconnaissance de Formes et l'Intelligence Artificielle (RFIA'08), AFRIF - AFIA, Jan 2008, Amiens, France. 8p. inria-00423797

HAL Id: inria-00423797

https://inria.hal.science/inria-00423797v1

Submitted on 12 Oct 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Une Logique pour Raisonner sur la Protection des Données Personnelles

A Logic to Reason about Personal Data Protection

Guillaume Piolle[1] Yves Demazeau[2]

[1] Université Joseph Fourier - LIG,
[2] CNRS - LIG,

46 avenue Felix Viallet, 38000 Grenoble Cedex, FRANCE
{guillaume.piolle, yves.demazeau}@imag.fr

Résumé

Les agents personnels interagissant dans le cadre d'applications web, ainsi que les agents de service avec lesquels ils collaborent, ont la responsabilité d'assurer la sécurité des informations personnelles, appartenant aux utilisateurs, qui leur sont confiées. Ils sont soumis aux réglementations émanant de diverses autorités normatives (lois, réglements, instructions de l'utilisateur...) régissant la protection des données personnelles. Nous présentons ici la logique DLP, conçue pour permettre à un agent cognitif de se représenter ces normes, de raisonner dessus, de prendre en compte leur caractère composite et d'y adapter leur comportement de manière cohérente.

Mots Clef

Agent cognitif, logique déontique, vie privée, conflits d'obligations.

Abstract

Personal agents interacting in the context of web applications, as well as the service agents they collaborate with, are responsible for the security of the users' personal information that they are in charge of. Several regulations apply to them, issued from various normative authorities (laws, regulations, user instructions...) ruling personal data protection. We present here the DLP logic, designed to allow a cognitive agent to represent these norms, to reason about them, to take into account their composite nature and to adapt their behaviour to them in a consistent way.

Keywords

Cognitive agent, deontic logic, privacy, obligation conflicts.

1 Introduction

Les travaux sur les systèmes multi-agents centrés utilisateurs [11] évoquent de plus en plus des agents personnels, rattachés à des utilisateurs humains, et agissant comme des assistants au sein d'applications distribuées dans des réseaux ouverts (internet) ou dans des environnements d'informatique ambiante. Ces agents, ainsi que les agents de service avec lesquels ils devront collaborer, ont la responsabilité d'assurer la sécurité des informations personnelles, appartenant à l'utilisateur, qui leur sont confiées. De ce fait, au-delà de capacités applicatives spécifiques, ces agents doivent disposer d'outils leur permettant de se conformer au cadre réglementaire composite de leur contexte d'exécution sur la protection des données personnelles, afin d'avoir les moyens de protéger efficacement la vie privée des utilisateurs du système. Dans cette optique, nous présentons ici la logique DLP (*Deontic Logic for Privacy*) qui permet à un agent cognitif de se représenter de manière cohérente ses obligations légales, réglementaires, contractuelles ou morales en matière de protection des données personnelles, de manière à pouvoir raisonner sur ces obligations.

Précédemment [16], nous avons identifié les six dimensions qui composent la protection des données personnelles dans les textes légaux et réglementaires. Ces dimensions sont l'information de l'utilisateur, son consentement, le droit de modification et rétractation, la justification de la collecte et du traitement, la conservation des données et leur transmission à des tiers. Ces six dimensions ont été justifiées en détail dans [16], et nous allons en faire ici les six domaines de représentation de notre proposition.

Nous prévoyons d'intégrer cet outil dans un agent de type BDI, mais la logique en elle-même est indépendante de la formalisation du modèle mental de l'agent. La logique DLP permet de différencier le traitement des normes selon l'autorité normative (comme un État ou un supérieur hiérarchique) dont elles proviennent, de faire évoluer le contexte normatif de l'agent, de détecter et de gérer les conflits d'obligations entre différentes autorités normatives. À ce stade de notre travail, notre objectif est de permettre à l'agent de raisonner sur ce contexte normatif afin

de l'appliquer lui-même d'une manière satisfaisante, en respectant les données qui lui sont confiées.

2 Travaux existants

Le World Wide Web consortium a établi un jeu de standards pour la représentation des politiques de gestion des données personnelles, appelé *Platform for Privacy Preferences* (P3P, [18]). P3P fournit des schémas XML pour représenter la politique d'un site web ou les exigences d'un utilisateur. Ces travaux répondent de manière satisfaisante aux exigences des deux premiers axes de la protection des données personnelles (information et consentement de l'utilisateur), et par mesure d'interopérabilité nous ferons en sorte que nos propositions soient aisément compatibles avec ces formats.

La logique déontique [15] et les systèmes multi-agents normatifs [4, 13] constituent un outil privilégié pour la représentation et le traitement des contraintes d'obligations par des agents cognitifs. Nous accepterons pour définition des systèmes multi-agents normatifs, dans le cadre de nos travaux, une adaptation de la définition fournie par Boella, van der Torre et Verhagen [4] :

Définition 1 *Un système multi-agent normatif est un système multi-agent associé à un ensemble de normes sur le comportement des agents, permettant le choix individuel des normes à suivre, l'évolution de ces normes, la représentation et le traitement des violations.*

Dans nos précédents travaux [8], nous avons montré que l'utilisation de systèmes normatifs centralisés était inadaptée à notre problème, c'est pourquoi le système multi-agent normatif que nous construisons ici est basé sur un traitement des normes local à chaque agent, les normes elles-mêmes étant publiques.

Le principe de l'adaptation dynamique du comportement de l'agent à son contexte normatif a déjà été décrit par Gaertner *et al* dans le scénario de la "salle de bal" [10], dans lequel un agent "danseur" passe de salle en salle, en se conformant à chaque fois à l'étiquette et aux coutumes en vigueur dans la salle. Notre proposition peut être vue comme une implémentation des mécanismes en jeu dans ce scénario. Certaines logiques déontiques proposées pour des systèmes normatifs présentent des caractéristiques intéressantes pour notre problématique. C'est le cas de la logique NTL [2], qui différencie les modalités suivant les différents systèmes normatifs auxquels appartient l'agent, mais ne considère pas toutefois les conflits possibles. On notera que NTL tire parti de l'association de la logique déontique et de la logique temporelle pour des applications de *model checking*. Ce n'est pas ici notre objectif.

Les travaux de Cholvy et Cuppens sur la consistance des politiques de sécurité [6] traitent également de problématiques très proches des nôtres. Dans leur contribution, les conflits d'obligations sont gérés par un opérateur de fusion des rôles qui s'appliquent à l'agent, alors que nous nous basons sur une différenciation par autorité normative. Cholvy et Cuppens utilisent une modalité d'obligation unique, ce qui impose une définition assez restrictive de l'inconsistance et des conflits d'obligations. Nous tentons ici de dépasser cette limitation.

3 Les logiques DLP et RDLP

Les formules de la logique DLP sont destinées à être diffusées par les autorités normatives en tant que représentation des normes qu'elles édictent, puis à être traitées localement par l'agent pour lui permettre d'adapter son comportement (dans notre cas, en matière de gestion des données personnelles). Nous ne cherchons donc pas à modéliser ni à vérifier le fonctionnement d'un système multi-agent vu de l'extérieur, mais à représenter les normes de manière à obtenir une compatibilité maximale avec des modèles cognitifs classiques basés sur la logique modale (comme dans [7], [12] ou [1]). Nous construisons ici la logique DLP sur la base d'une logique multimodale normale [3], qui nous permettra de prendre en compte le caractère composite du contexte normatif.

3.1 Syntaxe

La logique déontique que nous proposons est basée sur une classe de modalités d'obligation O_i^ν. Dans cette notation, ν représente une autorité normative, c'est à dire un agent qui édicte des normes (comme un État ou un supérieur hiérarchique dans une entreprise), et i représente un agent du système qui traite les normes de ν (qui reconnaît l'autorité normative de ν). Il y a donc une modalité différente pour chaque autorité normative, et pour chaque agent interprétant ces normes. Dans un souci de simplicité, nous pourrons dans le cadre de cette présentation considérer un unique agent i, ignorer l'indice et donc considérer la classe des modalités O^ν. La figure 1 présente la syntaxe des formules bien formées de la logique DLP, qui consiste notamment en l'application éventuelle d'une modalité telle que définie plus haut sur des prédicats dont la forme est définie par la grammaire de la figure 2. On intègre également à la logique la disjonction $\vee$ et la négation $\neg$, et l'on acceptera par la suite les abréviations classiques de la conjonction $\wedge$ et de l'implication logique $\longrightarrow$. On pourra pour la notion de permission utiliser l'abréviation Per_i^ν qui vaut pour $\neg O_i^\nu \neg$ (nous acceptons donc la définition classique de la permission en tant que dual de l'obligation). On s'accorde l'usage de parenthèses pour forcer les priorités.

$$\text{WFF} = \text{PROPOSITION} \mid \text{WFF} \text{ “}\vee\text{” } \text{WFF} \mid \text{“}\neg\text{” WFF} \mid \text{“}O_i^\nu\text{” WFF} \;;$$

FIG. 1: Syntaxe des formules bien formées de la logique DLP

Dans la grammaire des propositions (figure 2), ID représente l'identifiant unique d'un traitement mettant en œuvre

PROPOSITION = PERFORMATIVE | DATA | FORMULA ;
PERFORMATIVE = "*request*(" AGENT, AGENT, DATAINFO, TIMESTAMP ")"
| "*inform*(" AGENT, AGENT, ID, ACTIONTYPE, CONTACT, TIMESTAMP ")"
| "*consent*(" AGENT, AGENT, ID, TIMESTAMP ")"
| "*tell*(" AGENT, AGENT, DATA, TIMESTAMP ")"
| "*perform*(" AGENT, ID, TIMESTAMP ")" ;
DATAINFO = "*datainfo*(" ID, DATATYPE, AGENT, EXPIRATIONDATE, FORWARDLIST ")" ;
DATA = "*data*(" ID, DATATYPE, AGENT, EXPIRATIONDATE, FORWARDLIST, DATASTRING ")" ;
FORWARDLIST = "["{AGENT}"]" ;

FIG. 2: Grammaire des propositions spécifiques à la protection des données personnelles, et sur lesquelles porteront les modalités déontiques

des données personnelles, DATASTRING les données personnelles transmises, et FORMULA une expression logique ou arithmétique, n'utilisant aucun des prédicats définis dans cette grammaire. On suppose que ACTIONTYPE et DATATYPE procèdent d'ontologies décrivant les différents types de traitements et de données personnelles, respectivement. Dans les différents prédicats performatifs de cette grammaire, on retrouve (en gras) les six dimensions des traitements et de la protection des données personnelles :

- Le prédicat *request* décrit la demande d'informations personnelles pour un traitement (comprenant des propriétés attachées aux informations demandées, comme le propriétaire des données, la durée de conservation et la liste des agents autorisés à y accéder) ;
- Le prédicat *inform* encapsule des **informations sur le traitement** à destination de l'utilisateur, dont le type de traitement (**usage des données**), le contact du responsable (pour le **droit d'accès et de modification**), la date limite de **conservation des données** et la liste des agents destinataires d'une éventuelle **transmission des données** ;
- Le prédicat *consent* représente le **consentement de l'utilisateur** pour un traitement donné ;
- Le prédicat *tell* représente la transmission des données par l'utilisateur (avec les informations relatives attachées) ;
- Le prédicat *perform* représente un traitement effectif impliquant des données personnelles.

A partir de la syntaxe de la syntaxe DLP, nous définissons une version restreinte du langage, RDLP (*Restricted DLP*), constituée de formules de la forme $P \longrightarrow O_i^\nu Q$ ou $P \longrightarrow Per_i^\nu Q$, où P et Q sont des formules DLP bien formées ne contenant pas de modalité d'obligation. Éventuellement P et Q peuvent avoir pour valeur vrai ($\top$) ou faux ($\bot$). Les normes que nous traitons dans le cadre de nos travaux actuels sont des formules RDLP bien formées. Cette restriction sur la syntaxe, également jugée acceptable pour la spécification de politiques de sécurité [6], est déterminante pour le bon fonctionnement des algorithmes que nous présentons par la suite (l'amélioration future de ces algorithmes pourrait éventuellement permettre de lever ou de limiter cette restriction).

L'analyse d'une politique P3P [18] permet de générer des mots du langage défini en figure 2, et les expressions déontiques sur ce langage (formules RDLP) permettent de représenter des exigences sur les politiques P3P. La logique DLP est donc un moyen de raisonner à la fois sur ces politiques (P3P ou autres éventuellement) et sur des jeux de réglements. Les formules sous la forme RDLP, qui sont celles émises par les autorités normatives dans notre cadre applicatif, sont donc par exemple de la forme de (1), qui signifie que si l'agent i effectue un traitement ID impliquant une information de type "nom" appartenant à un autre agent, alors d'après la loi, i ne doit pas conserver ladite information plus de trente jours.

$$\begin{aligned} &perform(i, ID, T_0) \wedge datainfo(ID, nom, _, T_{exp}, _) \\ &\quad \longrightarrow O_i^{loi}(T_{exp} - T_0 < 30 * 24 * 3600) \end{aligned} \tag{1}$$

3.2 Axiomatique

Nous avons accepté plus haut la notion de permission comme le dual de celle d'obligation ($Per_i^\nu P \stackrel{def}{=} \neg O_i^\nu \neg P$). Ce choix nous force à renoncer à plusieurs axiomes courants des logiques modales normales [3, 5], comme $\mathbf{O_i^\nu}$-5 ($Per_i^\nu P \longrightarrow O_i^\nu Per_i^\nu P$), qui permettrait à une autorité normative de générer mécaniquement des obligations sur un domaine qui ne relève pas de sa compétence. L'axiomatique que nous proposons évite cet écueil causé par la dualité de l'obligation et de la permission.

La logique DLP est construite sur l'axiomatique et les règles d'inférence suivantes, où P et Q représentent des formules DLP bien formées :

$$\frac{P, P \rightarrow Q}{Q} \tag{MP}$$

$$\frac{P}{O_i^\nu P} \tag{$\mathbf{O_i^\nu}$-RN}$$

$$\text{WFF tautologiques du langage} \qquad \text{(TAUT)}$$
$$O_i^\nu(P \to Q) \longrightarrow (O_i^\nu P \to O_i^\nu Q) \qquad (\mathbf{O_i^\nu}\text{-K})$$
$$O_i^\nu P \longrightarrow Per_i^\nu P \qquad (\mathbf{O_i^\nu}\text{-D})$$
$$O_i^\nu P \longrightarrow O_i^\nu O_i^\nu P \qquad (\mathbf{O_i^\nu}\text{-4})$$
$$O_i^\nu(O_i^\nu P \longrightarrow P) \qquad (\mathbf{O_i^\nu}\text{-}\Box M)$$

Cette axiomatique est basée sur la logique SDL (logique déontique standard, [15]), assortie des axiomes ($\mathbf{O_i^\nu}$-4) et ($\mathbf{O_i^\nu}$-$\Box M$). ($\mathbf{O_i^\nu}$-$\Box M$) impliquant ($\mathbf{O_i^\nu}$-4c), avec ($\mathbf{O_i^\nu}$-4) il fait de ($\mathbf{O_i^\nu}$-4!) un théorème du langage, qui nous permet de réduire les chaînes d'obligations d'une même autorité normative, la notion étant peu porteuse de sens. Nous rejoignons donc Chellas [5] sur ces considérations.

$$O_i^\nu O_i^\nu P \longrightarrow O_i^\nu P \qquad (\mathbf{O_i^\nu}\text{-4c})$$
$$O_i^\nu P \longleftrightarrow O_i^\nu O_i^\nu P \qquad (\mathbf{O_i^\nu}\text{-4 !})$$

Au-delà de ces raisons quelque peu mécaniques, nous pouvons justifier l'ajout de ($\mathbf{O_i^\nu}$-$\Box M$) en le voyant comme un axiome fondant l'autorité normative : il nous dit en effet que toute autorité normative ν impose (au sens d'une norme, et non mécaniquement) que les obligations édictées par elle soient respectées.

3.3 Sémantique

Dans la plupart des modèles cognitifs basé sur une modalité de croyance [7, 12, 1], la sémantique de Kripke correspondant à cette modalité associe à chaque monde possible une succession envisageable d'actions, décrivant l'évolution possible du système depuis son initialisation jusqu'à la fin de l'exécution. Dans un souci de compatibilité, nous retenons cette conception de la sémantique des mondes possibles, qui s'accorde avec l'axiomatique présentée plus haut. Nous nommerons $\mathcal{W}$ l'ensemble des mondes possibles, et nous noterons w, w', w'' et à suivre, des éléments de $\mathcal{W}$. À chaque modalité O_i^ν, nous associons une relation d'accessibilité $\mathbb{O}_i^\nu$, pourvue de la même différenciation par agent et par autorité normative. Conséquemment à l'axiomatique choisie pour O_i^ν, les relations $\mathbb{O}_i^\nu$ ont les propriétés de sérialité, de transitivité et de réflexivité secondaire (2). Cette dernière propriété nous promet que tout monde possible respectant les normes du monde courant, respecte les normes s'appliquant à ce monde. Elle assure donc une certaine qualité, en matière de respect des normes, des mondes désirables au sens des normes d'une autorité ν.

$$\forall w, w' \in \mathcal{W} \qquad w\mathbb{O}_i^\nu w' \longrightarrow w'\mathbb{O}_i^\nu w' \qquad (2)$$

Nous pouvons maintenant définir la classe $\mathcal{K}_i^\nu$ des cadres $\mathcal{F} = \{\mathcal{W}, \mathbb{O}_i^\nu\}$ associée à chaque modalité O_i^ν. D'après le théorème de complétude de Sahlqvist [3], la logique DLP pour la modalité O_i^ν est fortement complète par rapport à la classe de cadres de Kripke $\mathcal{K}_i^\nu$, de part la nature des axiomes et leur correspondance avec les propriétés de $\mathbb{O}_i^\nu$.

La correction de la logique DLP par rapport à cette classe se montre aisément.

Nous venons de présenter la syntaxe, l'axiomatique et la sémantique de la logique DLP, et nous allons maintenant voir comment elle peut être utilisée par un agent cognitif.

4 Interprétation des normes

L'objectif initial de la logique DLP est de représenter les normes du système d'une manière efficace. La classe de modalités O_i^ν que nous avons introduite pourrait être intégrée à un modèle complet d'agent logique [12, 1], mais cela dépasse le cadre de cette présentation. Nous supposerons disposer d'un agent cognitif de type BDI, et nous allons montrer comment fournir à cet agent un ensemble de formules DLP cohérent, et comment ce dernier peut être utilisé pour prendre en compte le contexte normatif de manière efficace.

4.1 Acceptabilité des normes

Dans les cas réels, où l'édition des normes est de la responsabilité d'autorités indépendantes et éventuellement sujettes à l'erreur, les normes à prendre en compte peuvent poser deux types de problèmes logiques. L'ensemble des normes peut être inconsistant, et des conflits d'obligations peuvent apparaître. Concernant l'inconsistance, ses effets sont réduits par la différenciation des modalités en fonction de l'autorité normative. L'ensemble de normes $\{O_i^{\nu_1} P, O_i^{\nu_2} \neg P\}$, par exemple, n'est pas inconsistant, il exprime un contradiction entre une obligation édictée par ν_1 et une obligation édictée par ν_2. Ainsi, les seules inconsistances possibles entre obligations mettent en jeu des formules faisant référence à une même autorité normative. A ce titre, l'ensemble de normes $\{O_i^\nu P, O_i^\nu \neg P\}$ est lui inconsistant en logique DLP, comme en SDL d'une manière générale. De la même manière, la différenciation par agent (indice i) restreint la notion d'inconsistance à l'échelle d'un seul agent. À ce stade de nos travaux, nous choisissons de ne pas accepter l'inconsistance au sens strict. Si une autorité normative édicte des obligations inconsistantes, l'agent choisira d'ignorer cette autorité normative, jusqu'à ce que l'ensemble des normes qu'elle publie redevienne consistant.

La gestion des conflits d'obligations est plus subtile. La raison principale en est qu'en logique déontique standard, un conflit d'obligations ne peut jamais être représenté, parce qu'il rend l'ensemble des normes inconsistant (à cause de l'axiome ($\mathbf{O_i^\nu}$-D)). C'est le dilemme de Sartre, tel que décrit en logique déontique par McNamara [15]. Nous verrons comment la différenciation des modalités peut encore une fois nous permettre de contourner ce problème fondamental inhérent à l'utilisation d'une logique modale normale pour la logique déontique.

Si nous reprenons notre exemple de la formule (1), la loi impose à l'agent i de supprimer les informations personnelles de type nom trente jours au plus après le traitement. Supposons que i soit soumis au réglement interne

de son entreprise qui lui impose la norme (3) (autorisant la conservation des mêmes données au-delà de trente jours), et à un ordre direct de son supérieur hiérarchique (demandant la conservation des donnée nom de l'agent $client$ pendant une durée de soixante jours minimum) représenté par la formule (4). On suppose que les prémisses des trois formules sont vérifiées, et donc que i doit théoriquement se conformer aux trois modalités déontiques exprimées. Schématiquement, les formules (1), (3) et (4) sont respectivement de la forme $(A \rightarrow O_i^\nu P)$, $(A \rightarrow Per_i^\nu \neg P)$ et $(A' \rightarrow O_i^\nu Q)$, avec $A' \rightarrow A$ et $\{P, Q\} \vdash \bot$.

$$perform(i, ID, T_0) \wedge datainfo(ID, nom, _, T_{exp}, _) \longrightarrow O_i^{loi}(T_{exp} - T_0 < 30 * 24 * 3600) \quad (1)$$

$$perform(i, ID, T_0) \wedge datainfo(ID, nom, _, T_{exp}, _) \longrightarrow Per_i^{entreprise}(T_{exp} - T_0 \geq 30 * 24 * 3600) \quad (3)$$

$$perform(i, ID, T_0) \wedge datainfo(ID, nom, client, T_{exp}, _) \longrightarrow O_i^{patron}(T_{exp} - T_0 > 60 * 24 * 3600) \quad (4)$$

Cholvy et Cuppens [6] définissent les conflits de normes par l'existence d'un monde accessible où l'on peut déduire $\bot$. Ne différenciant pas les modalités déontiques dans le cadre de [6], ils considèrent que l'ensemble de normes $\{O_i^{\nu_1} P, \wedge O_i^{\nu_2} \neg P\}$ est inconsistant, et ils se trouveraient donc à devoir prononcer un arbitrage entre les normes (1) et (3). Or ces deux normes ne sont pas fondamentalement incompatibles, (1) étant simplement une restriction par rapport aux permissions accordées par (3)[1]. En fixant une durée d'expiration inférieure à trente jours, l'agent i peut se conformer de manière simple à ces deux normes. Nul besoin donc d'un traitement spécifique dans ce cas-là, et nous tâcherons en conséquence de donner un rôle particulier aux modalités de permission, qui par essence ne restreignent pas le comportement de l'agent[2]. La différenciation des modalités nous évite donc ici de considérer abusivement un ensemble de normes comme contenant un conflit d'obligations, en limitant la portée de l'inconsistance logique. En effet dans notre exemple, au lieu de considérer l'inconsistance qui pourrait dériver de la permission (3) et de l'obligation (1), nous les traitons séparément, de par leurs sources distinctes, nous constatons qu'elles ne sont en fait pas contradictoires, et qu'un agent pourrait avoir un comportement ne violant aucune de ces deux normes.
Les normes (1) et (4), par contre, posent un réel problème : il n'y a aucun moyen pour i de se conformer simultanément aux deux normes. D'un point de vue logique, si l'on fait abstraction de la différenciation par autorité normative, on peut déduire $\bot$ dans tous les mondes accessibles. Ce serait à notre sens une définition plus correcte de la notion de conflit d'obligations, la différenciant de la restriction de permission (ou durcissement des contraintes d'obligation). Dans cette situation de conflit d'obligations, notre agent humain devra donc choisir de se conformer soit à la loi, soit à l'ordre de son supérieur. Ce choix subjectif relèvera de ses valeurs morales, c'est le "dilemme moral" également accepté comme situation de conflit par Cholvy et Cuppens [6].

[1]Émises par une même autorité normative, ces deux formules seraient toutefois inconsistantes entre elles, et dans ce cas nous l'avons dit, l'agent i choisira d'ignorer l'autorité en question.

[2]Ce n'est pas toujours le cas dans les logiques déontiques incluant $\mathbf{O_i^\nu}$-5.

4.2 Définition du conflit d'obligations

Nous allons maintenant formaliser cette intuition de la notion de conflit d'obligations. Nous définissons la fonction d'agrégation γ, qui à une formule sous la forme RDLP associe une formule DLP, mais avec une autorité normative commune ν_0, fictive. Cette fonction est destinée à représenter momentanément un ensemble de normes en faisant abstraction de la différenciation par autorité normative, et en donnant un rôle particulier à la modalité de permission. La figure 3 décrit le fonctionnement de la fonction d'agrégation.

$$\gamma : RDLP \longrightarrow DLP$$
$$\gamma : (P \rightarrow Ob_i^\nu Q) \longmapsto (P \rightarrow Ob_i^{\nu_0} Q)$$
$$\gamma : (P \rightarrow Per_i^\nu Q) \longmapsto (P \rightarrow \top)$$

FIG. 3: Définition de la fonction d'agrégation γ

Par extension si Δ est un ensemble de formules RDLP, on notera $\Gamma(\Delta)$ la fermeture des formules de Δ agrégées au moyen de la fonction γ. Cette fonction d'agrégation nous permet maintenant de définir la notion de conflit d'obligations dans RDLP :

Définition 2 *L'ensemble de formules RDLP Δ comporte un conflit d'obligations si l'ensemble de formules DLP $\Gamma(\Delta)$ est inconsistant (soit $\Gamma(\Delta) \vdash_{DLP} \bot$).*

Cette définition est bien cohérente avec les exigences intuitives que nous avons formulées pour la notion de conflit d'obligations. Elle nous permet d'inclure les incompatibilités entre obligations, et d'exclure les incompatibilités mettant en œuvre des permissions. On pourra noter que c'est la structure de l'opérateur d'agrégation qui conditionne la restriction syntaxique de RDLP par rapport à DLP. En appliquant notre définition à des formules DLP, on devrait considérer que l'ensemble des normes (5) et (6) constitue un conflit d'obligations, ce qui n'est pas le cas. L'affinement de la définition de γ pour permettre la levée de cette restriction pourra faire l'objet de développements futurs.

$$Per_i^{\nu_1} P \longrightarrow Ob_i^{\nu_1} P \quad (5)$$
$$Ob_i^{\nu_1} \neg P \quad (6)$$

Nous avons donc dans RDLP, grâce à la différenciation et à l'agrégation, un moyen de représenter et de détecter les conflits d'obligations tout en conservant une logique modale normale. Nous nous affranchissons donc ici du dilemme de Sartre, intrinsèque à la logique déontique standard.

4.3 Arbitrage des conflits d'obligations

Nous nous plaçons tout d'abord dans le cas où un agent est tenu de respecter un ensemble de normes Δ comprenant des conflits d'obligations. Nous prendrons comme premier exemple l'ensemble Δ_1 constitué des normes (1) et (4). Dans le cas d'un agent humain, celui-ci se réfèrera à l'importance relative des autorités normatives. Cette importance relative est différente suivant les personnes, elle procède d'un classement des autorités basé sur la morale, les valeurs sociales de chacun. Il nous faut donc tenir compte de cette subjectivité dans l'arbitrage des conflits d'obligations. Pour cela, nous allons introduire la notion de prévalence normative, qui est une relation d'ordre total $\succeq_i$ entre les autorités normatives connues par l'agent i[3]. La relation est indicée par i pour signifier qu'elle est locale à l'agent. Informellement, si $\nu_1 \succeq_i \nu_2$ alors l'agent i préfèrera les normes édictées par ν_1 à celles édictées par ν_2 en cas de conflit d'obligations entre les deux. On dira que ν_1 prévaut sur ν_2 pour l'agent i. Dans le cadre de notre exemple, nous avons supposé que les autorités normatives sont ordonnées, pour i, comme dans (7).

$$self \succeq_i loi \succeq_i entreprise \succeq_i patron \tag{7}$$

On notera que l'agent lui-même est l'autorité normative qui prévaut sur toutes les autres. Dans le cas d'un agent humain, c'est ce qui permet de considérer qu'un ordre (ou même une loi) est immoral, et d'avoir sur ce dernier un point de vue critique. Pour un agent personnel, cette autorité normative interne reflète dans l'idéal les directives de l'utilisateur humain. En effet, la correspondance des actions d'un agent personnel avec la volonté de son utilisateur est une condition nécessaire pour engager la responsabilité de ce dernier [14].

Le principe de notre algorithme d'arbitrage des conflits d'obligations est le suivant : à partir de Δ (tel que $\Gamma(\Delta) \vdash_{DLP} \bot$), l'agent essaie de construire un ensemble Δ' exempt de conflits ($\Gamma(\Delta') \nvdash_{DLP} \bot$), en supprimant un nombre minimal de normes édictées par des autorités normatives de prévalence la plus faible possible. Dans notre exemple Δ_1 limité à deux normes, la solution est évidente, l'agent i va ignorer la norme (4) et respecter (1) (soit $\Delta'_1 = \{(1)\}$), car il considère que la loi prévaut sur les directives de son supérieur. Dans un ensemble de normes plus important, l'agent va devoir supprimer un certain nombre de normes, jusqu'à ce que l'ensemble restant devienne exempt de conflits.

[3]Le fait que $\succeq_i$ soit un ordre total est une hypothèse de travail simplificatrice. Lors de travaux futurs pourra être examinée la possibilité qu'elle soit un préordre et/ou une relation partielle.

arbitrer(Δ) :
  $\Delta' \leftarrow \Delta$
  tant que $\Gamma(\Delta') \vdash_{DLP} \bot$:
    $\Delta'' \leftarrow$ *ssensemble_conflictuel_minimal*(Δ')
    ordonner_prevalence_croissante(Δ'')
    $\Delta' \leftarrow \Delta' \backslash \{\Delta''[0]\}$
  fin tant que
  renvoyer Δ'
fin arbitrer

FIG. 4: Algorithme d'arbitrage des conflits d'obligations

A chaque étape de l'algorithme d'arbitrage des conflits d'obligations (détaillé figure 4), l'agent identifie un sous-ensemble conflictuel de normes de cardinal minimal (par exemple par un parcours arborescent en largeur, en marquant les sous-ensembles déjà visités), et en supprime la norme édictée par l'autorité normative de prévalence la plus faible. Au final, on aura évincé un nombre de normes le plus faible possible, et on aura préservé au mieux les obligations des autorités normatives de prévalence forte.

L'introduction de la notion de prévalence, l'utilisation de la différenciation par autorité normative et de notre définition du conflit d'obligations, permettent de contourner la version déontique du dilemme de Platon [15], une extension du dilemme de Sartre qui met en avant l'impossibilité de représenter et de gérer les conflits entre une norme prioritaire et une norme non prioritaire dans le cadre d'une logique déontique monomodale normale. Nous avons ici conservé le caractère normal de la logique, et grâce à l'opérateur d'agrégation γ nous serions en mesure de reconstituer à partir de Δ' un ensemble de normes monomodales cohérent après cet arbitrage des conflits.

Notons qu'à la mise en œuvre de l'arbitrage des conflits, les normes marginales écartées par l'algorithme devraient être mises à part, et non supprimées du système. Elles devraient en effet être reconsidérées lors d'une modification ultérieure de l'ensemble des normes, de la liste des autorités normatives ou d'une mise à jour de la relation de prévalence de l'agent.

On pourra noter également que si les permissions sont ignorées (par le fait de l'opérateur d'agrégation γ) lors de la recherche de conflits, elles sont conservées dans l'ensemble de normes Δ' confié à l'agent. Si notre opinion est que les normes de nature permissive ne doivent pas contraindre le fonctionnement de l'agent, et si nous ne proposerons pas de règle associée, un agent a toutefois la possibilité de les traiter comme il l'entend s'il en a l'utilité.

4.4 Lien avec le modèle mental de l'agent

L'agent prend connaissance des formules RDLP édictées par l'ensemble des autorités normatives qui le concernent ; cette phase peut par exemple être mise en œuvre par une diffusion des normes, ou par des requêtes sur un serveur de l'autorité normative. Une fois terminé un éventuel arbitrage des conflits d'obligations, l'agent i dispose d'un ensemble de normes cohérent Δ'. Cet ensemble, consistant et exempt de conflits, est intégré dans la base de croyances de l'agent et pris en compte pour adapter son comportement. Afin de respecter les réglementations qu'il reconnaît, l'agent génère ensuite à partir de Δ' des buts persistants et des intentions, de manière à ce qu'il ait en permanence la volonté de respecter chacune des normes.

A titre d'exemple, nous choisissons de nous placer dans un cadre où les intentions dérivent d'une modalité de choix $Choice_i$ (nous supposons bien sûr disposer d'une modalité de croyance Bel_i). Nous utiliserons également les modalités usuelles de la logique temporelle ($\mathcal{F}A$ si et seulement si A sera vrai à un moment dans le futur, $\mathcal{G}A$ si et seulement si A sera vrai à tout moment du futur, $A\mathcal{U}B$ si et seulement si A est vrai jusqu'à ce que B le devienne). Le modèle proposé par Adam *et al* [1] correspond typiquement à notre exemple. Les formules RDLP y seraient probablement représentées par des croyances particulières, mais pour des raisons de lisibilité nous ferons abstraction de la modalité correspondante. Les règles d'inférence (8) et (9) constituent selon nous la base d'une interface entre une base cohérente de formules RDLP et le modèle mental de l'agent.

$$\frac{A \rightarrow O_i^{\nu} B, Bel_i A, Bel_i B}{Choice_i \mathcal{G} B} \tag{8}$$

$$\frac{A \rightarrow O_i^{\nu} B, Bel_i A, Bel_i \neg B}{Choice_i \mathcal{F}\mathcal{G} B} \tag{9}$$

La règle (8) permet, dans le cas où l'obligation est déjà respectée, de générer un choix sur une formule logique, de manière à ce que l'agent considère le maintien de cet état de fait comme effectivement désirable. La règle (9), quant à elle, s'applique lorsque l'obligation n'est pas encore respectée. À cause de la nécessité de réalisme des choix ($Bel_i A \rightarrow Choice_i A$), l'agent ne peut pas dériver $Choice_i B$ ni $Choice_i \mathcal{G} B$ sans inconsistance de son modèle mental. Par contre, il fera le choix de la réalisation (et du maintien) de B à un instant du futur. Comme $\neg BelB$, ce choix va permettre de dériver un but à réaliser, un but persistant puis une intention. Lorsque B sera réalisé, $Choice_i \mathcal{G} B$ sera dérivé logiquement grâce à (8), et l'agent fera le choix de maintenir cet état de fait.

L'interaction entre la base de normes et le modèle mental de l'agent nécessiterait un travail d'approfondissement, comprenant notamment une axiomatique complète entre les deux parties. Ce travail dépasse le cadre de cette présentation, qui vise à fournir des outils indépendants de tout présupposé sur le modèle cognitif de l'agent, et les règles d'inférence (8) et (9) sont données à titre d'exemple.

5 Conclusion

Dans cet article, nous présentons RDLP, une logique déontique multimodale pour la représentation cohérente d'un contexte normatif composite. Nous proposons une nouvelle définition de la notion de conflits d'obligations, et nous montrons que ces conflits sont représentables en RDLP, dépassant ainsi certaines limitations connues de la Logique Déontique Standard, et des logiques déontiques normales en général. Nous présentons également un mécanisme d'arbitrage de ces conflits, basé sur une relation de précédence entre autorités normatives locale et spécifique à chaque agent, permettant de fournir une base de normes saines et cohérente tout en conservant la possibilité de la réactualiser lors des futures évolutions du contexte normatif. A titre d'exemple, nous donnons également un jeu de règles qui permet d'intégrer ces normes RDLP dans le modèle mental d'un agent BDI.

À un niveau applicatif, les outils que nous avons formalisés pour la protection des données personnelles permettent d'apporter des fonctionnalités cognitives supplémentaires aux agents gérant les données des utilisateurs. Les réseaux de terminaux centrés utilisateur gérant des profils de personnalisation, tels que proposés par Riché *et al* [17], ou les applications d'agendas collaboratifs [9] sont notamment des cibles applicatives privilégiées pour nos travaux.

Cependant, si la grammaire que nous avons proposé pour la logique DLP est spécifique à la protection des données personnelles, son extension permettrait l'intégration de nouveaux champs réglementaires à cette gestion rationnelle des normes. En effet, les mécanismes présentés ici sont adaptés, mais non exclusivement spécifiques à la protection des données personnelles, et constituent des outils d'informatique légale adaptés à des domaines d'applications variés et composites. Notre modèle permet de gérer de multiples autorités normatives, édictant des normes contextualisées, concernant possiblement de multiples domaines.

Ces travaux ouvrent de nombreuses pistes de recherche intéressantes. Parmi celles qui sont prioritaires, nous travaillons actuellement sur la mise en œuvre efficace d'une gestion des croyances sensibles (i.e. portant sur des données personnelles) soumises aux croyances normatives que nous fournissons ici, de manière à traiter de manière rationnelle, systématique et respectueuse des réglementations, les informations confiées à l'agent. Ces développements pourront faire l'objet d'une proposition d'intégration de RDLP dans un modèle cognitif complet basé sur la logique modale, comme par exemple celui présenté dans [1]. Nous travaillons également à améliorer plusieurs points techniques de notre contribution, notamment l'optimisation de l'algorithme d'arbitrage des conflits d'obligations (par exemple par l'utilisation d'heuristique pour la recherche des sous-ensembles conflictuels minimaux, qui est le point sensible de l'algorithme au niveau complexité), ou la définition d'une notion de prévalence abso-

lue d'une autorité normative, trop sensible pour qu'aucune de ses normes soit dominée. À un horizon plus large, nous prévoyons de permettre à un agent cognitif de raisonner conjointement sur les normes et sur les caractéristiques des mécanismes transactionnels proposés dans le cadre d'une collaboration entre agents, afin d'étendre le raisonnement sur la protection des données personnelles à un ensemble d'agents.

Remerciements

Ces travaux ont été menés dans le cadre du projet Web Intelligence du cluster ISLE de la région Rhône-Alpes. Nous remercions également Frédéric Cuppens pour ses remarques constructives, Joris Deguet pour sa relecture critique et les relecteurs anonymes, dont les questions ont contribué à clarifier notre exposé.

Références

[1] C. Adam, F. Évrard, B. Gaudou, A. Herzig et D. Longin, Modélisation Logique d'Agents Rationnels pour l'Intelligence Ambiante, *Actes des 14èmes Journées Francophones des Systèmes Multiagents (JFSMA'06)*, Annecy, France, Hermès, 2006.

[2] T. Ågotnes, W. van der Hoek, J. A. Rodríguez-Aguilar, C. Sierra et M. Wooldridge, On the Logic of Normative Systems, *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI'07)*, Hyderabad, Inde, 2007.

[3] P. Blackburn, M. de Rijke et Y. Venema, *Modal Logic*, Cambridge University Press, 2001.

[4] G. Boella, L. van der Torre et H. Verhagen, Introduction to Normative Multiagent Systems, *Computational & Mathematical Organization Theory 12*, 2-3, pp. 71–79, 2006.

[5] B. F. Chellas, Deontic Logic, *Modal Logic, an Introduction*, pp. 190–203 Cambridge University Press, 1980.

[6] L. Cholvy et F. Cuppens, Analyzing Consistency of Security Policies, *Proceedings of the 18th IEEE Symposium on Research in Security and Privacy*, Oakland, CA, USA, 1997.

[7] P. R. Cohen et H. J. Levesque, Intention is Choice with Commitment, *Artificial Intelligence 42*, 2-3, pp. 213–261, 1990.

[8] L. Crépin, G. Piolle, O. Boissier et Y. Demazeau, Des Systèmes Normatifs comme Outils de Protection de la Vie Privée, *Intelligence Artificielle et Web Intelligence (atelier IAWI de la plate-forme AFIA 2007)*, AFIA, Grenoble, France, 2007.

[9] Y. Demazeau, D. Melaye et M.-H. Verrons, A Decentralized Calendar System Featuring Sharing, Trusting and Negotiating, *Advances in Applied Artificial Intelligence, 19th International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE 2006)*, LNCS 4031, pp. 731–740, Springer, 2006.

[10] D. Gaertner, K. L. Clark et M. J. Sergot, Ballroom Etiquette : a Case Study for Norm-Governed Multi-Agent Systems. *Proceedings of the AAMAS06 Workshop on Coordination, Organization, Institutions and Norms in Sgent Systems (COIN 2006)*, Hakodate, Japon, 2006.

[11] Y. Haradji, N. Ferrand et H. Li, *Systèmes Multi-Agents*, ch. Relations à l'Utilisateur et Nouveaux Usages, pp. 215–260, Observatoire Français des Techniques Avancées, 2004.

[12] A. Herzig et D. Longin, C&L Intention Revisited, *Proceedings of the Ninth International Conference on Principles of Knowledge Representation and Reasoning (KR2004)*, D. Dubois, C. A. Welty, and M.-A. Williams, Eds., AAAI Press, pp. 527–535, Whistler, Canada, 2004.

[13] A. J. Jones et M. J. Sergot, *Deontic Logic in Computer Science : Normative System Specification*, ch. On the Characterisation of Law and Computer Systems : The Normative Systems Perspective, pp. 275–307, John Wiley and Sons, Chichester, Grande-Bretagne, 1993.

[14] M. Martinez Ribas, *Systèmes Multi-Agents et Loi*, Observatoire Français des Techniques Avancées - groupe Systèmes Multi-Agents, 2003.

[15] P. McNamara, Deontic Logic, *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed., Stanford University, 2006.

[16] G. Piolle, Y. Demazeau et J. Caelen, Privacy Management in User-Centred Multi-Agent Systems, *Proceedings of the 7th Annual International Workshop "Engineering Societies in the Agents World" (ESAW 2006)*, Dublin, Irlande, 2006.

[17] S. Riché, G. Brebner et M. Gittler, Client-Side Profile Storage, *NETWORKING 2002 Workshops on Web Engineering and Peer-to-Peer Computing*, pp. 127–133, Pise, Italie, 2002.

[18] World Wide Web Consortium, Platform for Privacy Preferences Specification 1.1, `http://www.w3.org/P3P/`.