Des Systèmes Normatifs comme Outils de Protection de la Vie Privée

Ludivine Crépin* — **Guillaume Piolle**** — **Olivier Boissier***** — **Yves Demazeau******

* *UJM-ENSMSE *** *ENSMSE*
158 cours Fauriel - F-42023 Saint-Étienne Cédex 2
{crepin, olivier.boissier}@emse.fr

** *UJF - LIG **** *CNRS - LIG*
46, avenue Félix Viallet - F-38031 Grenoble Cédex
{guillaume.piolle, yves.demazeau}@imag.fr

RÉSUMÉ. *Les applications web demandent de plus en plus d'informations personnelles pour l'authentification des utilisateurs et la personnalisation des services. Le besoin de nouveaux outils pour garantir la vie privée des utilisateurs se fait ainsi sans cesse plus pressant. Nous considérons ici la potentialité des systèmes normatifs, qui servent aujourd'hui principalement à modéliser et gérer les organisations et les réglementations, à devenir un des outils de représentation et gestion de cette protection des données personnelles. Nous montrons que la plupart d'entre eux ne sont pas capables de fournir une réponse adaptée à cette problématique, et que l'utilisation des systèmes normatifs ne peut avoir qu'un rôle limité dans la protection de la sphère privée.*

ABSTRACT. *Web applications request more and more personal data in order to authenticate users and personalize services. The need for novel privacy enhancing tools is thus more present everyday. We consider here the potential of normative systems, which are mainly used today for modeling and managing organizations and regulations, to become one of the representation and management tools of this privacy management. We show that most of them cannot properly address the problem, and that the use of normative systems can only have a limited role in the protection of privacy.*

MOTS-CLÉS : *Normes, vie privée, systèmes normatifs, violations, passage à l'échelle*

KEYWORDS: *Norms, privacy, normative systems, violations, scalability*

1. Introduction

Les applications web, de par les possibilités de collaboration et d'association dynamique de services, la multiplicité des acteurs et le caractère ouvert de l'environnement, deviennent conjointement un outil de personnalisation au service d'une plus grande fluidité pour l'utilisateur, et une source de risques pour la protection de ses données personnelles.

Les systèmes normatifs (Jones *et al.*, 1993) nous servent à modéliser et gérer, dans les systèmes multi-agents, les relations organisationnelles et les aspects déontiques de l'application. Ils permettent de conceptualiser la notion de norme, de violation, de récompense, de sanction. Les normes considérées dans cette étude portent sur la protection des données privées. Nous nous interrogeons ici sur la possibilité d'utiliser les systèmes normatifs pour mettre en œuvre une protection efficace des données personnelles dans les applications distribuées sur internet. Dans cette hypothèse, les réglementations en matière de protection des données personnelles seraient représentées par des normes du système, et la violation de ces normes correspondrait à la violation desdites réglementations.

2. Systèmes Normatifs et Gestion de la Sphère Privée

Dans Piolle *et al.* (2006), nous avons défini les six paramètres de la protection des données personnelles, partie constituante de la gestion de la sphère privée, réparties en propriétés locales et distantes. Les propriétés locales (information, consentement, droit d'accès) peuvent être vérifiées par l'agent utilisateur, qui peut décider en toute connaissance de cause de poursuivre sa collaboration avec son interlocuteur. En revanche, les propriétés distantes (utilisation, conservation et transmission des données) peuvent être contournées de manière silencieuse, à l'insu de l'agent utilisateur. C'est sur leur garantie que nous évaluerons ici l'impact de l'utilisation d'un système normatif car elles constituent actuellement le point dur du problème.

Les différents mécanismes concernant l'application des normes ou, plus précisément, la manière dont le système diffuse les normes, détecte/constate les violations et applique les sanctions, nous permettent de classifier les systèmes normatifs en deux groupes : ceux dont les mécanismes sont centralisés et ceux dont ils sont distribués, voire décentralisés. La centralisation de ces mécanismes implique la présence d'un tiers pour contrôler le système, comme les superviseurs (ou agents de confiance) ou les entités omnipotentes. Les mécanismes distribués n'ont pas besoin d'ajout de cette sorte, l'ordre social (Castelfranchi, 2000) permettant aux agents d'appliquer eux-mêmes les normes, sans l'intervention d'une plus haute instance. Notre étude se base sur cette différence entre les systèmes normatifs pour en définir les avantages et les inconvénients sur la protection de la sphère privée.

3. Application à la Protection des Données Personnelles

Les trois points abordés ici sont caractéristiques de la protection des données personnelles dans le cadre d'une application web, et peuvent constituer des limites à l'utilisation des systèmes normatifs.

Détection des violations de normes : Dans les systèmes normatifs centralisés et omniscients, tous les types de violations peuvent être détectés et évalués, et les évaluations rendues publiques. On peut donc bâtir une société artificielle dans laquelle les stratégies basées sur la violation des normes sont perdantes. Cependant, l'hypothèse de l'omniscience se heurte à la spécificité de la violation des normes dans le domaine de la protection de la vie privée. En effet, les propriétés distantes (utilisation, conservation et transmission de données) peuvent être enfreintes sans aucun signe extérieur décelable pour un agent observateur. Des méthodes alternatives peuvent être utilisées pour la détection de ces violations, impliquant une personnalisation des informations transmises en fonction de l'interlocuteur (de type *watermarking*) et une veille des données disponibles dans l'environnement. Cependant de telles sondes sont forcément très dépendantes de l'application et de son contexte d'exécution, et la détection n'est jamais garantie.

Passage à l'échelle : Les systèmes normatifs centralisés semblent principalement utilisés pour formaliser le fonctionnement de systèmes à l'état de modèles théoriques ou de simulateurs. Le passage à l'échelle d'une application coopérative sur le web impliquerait l'instauration d'une autorité normative compétente sur l'ensemble du réseau, des hôtes et des juridictions. Il devient évident au vu de la réalité du web qu'une telle autorité ne saurait exister, c'est pourquoi les systèmes centralisés se heurtent ici à une limitation majeure.

Subjectivité des normes : Sur le web, des normes différentes s'appliquent aux différents agents logiciels et humains, suivant la juridiction dont ils dépendent et leur affiliation à diverses autorités. Des normes multiples et parfois contradictoires peuvent de plus s'appliquer à un même agent, et leur arbitrage peut être différent suivant les utilisateurs. Un traitement peut en effet être considéré comme acceptable par un agent, délictueux par un autre, ce qui est incompatible avec une évaluation partagée des violations. L'évaluation conjointe des actions et des normes se doit donc d'être distribuée et locale à chaque agent, afin de prendre en compte la richesse et l'ouverture de l'environnement du web.

4. Conclusion

D'après notre étude, les systèmes normatifs permettent une bonne modélisation des contraintes imposées par la protection de la vie privée : ils offrent la possibilité de les formaliser et de les appliquer. Mais, dans un milieu décentralisé et ouvert tel que le web, nous constatons certaines limites aux implémentations actuelles qui sont centralisées, telles que le passage à l'échelle, la détection des violations et la subjectivité des normes.

Dans la plupart des types de systèmes normatifs étudiés, une propriété intrinsèque empêche le système d'être un bon candidat pour une mise en œuvre de la protection des données personnelles, dans un cas réel à l'échelle d'une application web. La meilleure application qui semble pouvoir être faite des systèmes normatifs consiste en une déportation dans chaque agent du raisonnement sur les normes. Ce type de mise en œuvre permettrait aux agents de gérer de manière cohérente au regard de leurs obligations les données qui leur sont confiées, de raisonner (d'une manière limitée par leurs croyances) sur les normes et les actions d'autres agents, et éventuellement d'élaborer des stratégies dans leurs actions collaboratives. Nous avons vu que même une architecture de ce type reste structurellement limitée par l'impossibilité de détecter toutes les violations, de s'accorder sur un ensemble de normes commun et donc d'organiser des évaluations partagées, des récompenses ou des sanctions. Ce type de système doit donc être complété par des technologies de plus bas niveau (Deswarte *et al.*, 2006) qui auront à charge de fournir les informations nécessaires pour raisonner sur le niveau de sécurité de l'application ou du protocole utilisé. Nos futurs travaux consisteront à spécifier de manière formelle un tel système normatif.

Remerciements

Ce travail a été financé par le projet Web Intelligence du cluster ISLE de la région Rhône-Alpes, et le premier auteur bénéficie d'une allocation de recherche de la région Rhône-Alpes.

5. Bibliographie

Deswarte Y., Aguilar Melchor C., *Sécurité des Systèmes d'Information*, Hermès, Paris, France, chapitre Technologies de Protection de la Vie Privée sur Internet, p. 49-71, 2006.

Jones A. J., Sergot M., *Deontic Logic in Computer Science : Normative System Specification.*, John Wiley and Sons, Chichester, England, chapitre On the Characterisation of Law and Computer Systems : The Normative Systems Perspective, p. 275-307, 1993.

Piolle G., Demazeau Y., Caelen J., « 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, Septembre 2006.

Castelfranchi C., « Engineering Social Order », *Proceedings of the 5th Annual International Workshop "Engineering Societies in the Agent World" (ESAW 2000)*, Berlin, Allemagne, Aout 2000.