Vers de nouveaux modèles de partage de l'information

Manuel Munier[1,*] Camille Dubedout[2] Nouha Laamech[1]

Manuel.Munier@univ-pau.fr Camille.Dubedout@univ-grenoble-alpes.fr Laamech.Nouha@gmail.com

[1] IUT des Pays de l'Adour
LIUPPA – Mont de Marsan
Laboratoire d'Informatique de l'Université de Pau et des Pays de l'Adour

[2] Université Grenoble Alpes
CESICE – Grenoble
Centre d'Études sur la Sécurité Internationale et les Coopérations Européennes

*Le/les auteur(s) avec la marque * sont auteur(s) correspondant(s).*

Thèmes – *Informatique - Droit*

Résumé – *Dans la société numérique actuelle, la multiplication des échanges d'information soulève de nombreux défis pour les différents acteurs amenés à intervenir à l'échelle locale, à l'instar des fournisseurs privés de services numériques ou des collectivités territoriales. Ces défis qui interviennent à tous les niveaux d'un traitement de données, depuis son partage à son stockage, appellent en particulier à créer de nouvelles règles de transparence, de qualité ou encore de traçabilité des données échangées. Communément partagées, ces nouvelles règles sont en effet susceptibles de favoriser la confiance entre les différents types d'acteurs à l'égard des données échangées et encouragent un partage équitable des ressources numériques, notamment entre les acteurs publics et privés.*

Mots-clés – *gouvernance des données, communs, responsabilité, traçabilité*

Section(s) CNU pour cet article – *27, 02*

Article présenté à l'oral par un(e) doctorant(e) – *NON*

1 Introduction

Avec le développement d'Internet et des réseaux de communication, la circulation des données a acquis une place primordiale au sein de la société, en particulier au sein des villes. À travers la mise en place d'outils de captation des données et d'actionneurs, à l'instar d'objets connectés ou *"IoT"*, il est désormais possible de collecter une quantité et une diversité croissante de données ainsi que d'agir sur l'environnement en temps réel, à l'exemple de capteurs permettant d'ajuster la température dans des bâtiments publics. In fine, la captation et la diffusion de données au sein des villes donne lieu à la création de nouveaux services dans des domaines aussi divers que les transports, l'énergie, la gestion des déchets, la gestion de l'eau ou les flux de circulation. Toutefois, l'absence de contrôle sur l'usage et la fiabilité de ces données tend à constituer un frein au partage de données, tant pour le "producteur" de données que pour le "consommateur".

2 Les enjeux liés aux échanges de données

De ces échanges de données (et pas uniquement les données à caractère personnel) subvient alors un enjeu majeur : celui de la maîtrise et de la protection des données circulant entre les différents acteurs. Il ne s'agit pas de s'intéresser à la sécurité technique des différents réseaux mis en place, tels que la 4G, la 5G, ou des protocoles de communications d'objets connectés comme LoraWAN, mais d'envisager une question plus large, relevant de la gouvernance des échanges [1]. L'enjeu relève davantage de l'accès aux données par le citoyen, de leur diffusion, de leur traçabilité ou des garanties d'intégrité apportées, dans un contexte où les échanges de données deviennent aujourd'hui, et de plus en plus, des éléments essentiels au fonctionnement des villes, en France comme à travers le monde.

Aujourd'hui, un ensemble de textes légaux et réglementaires visent déjà à orienter les usages des données, par exemple en encourageant leur diffusion ou en limitant l'utilisation de certains types de données. En France notamment, la Loi pour une République Numérique du 7 octobre 2016 (LRN) a pour but d'inciter les administrations à ouvrir et à partager l'ensemble des données publiques qu'elles exploitent afin de faciliter la réutilisation de celles-ci par les entreprises et les citoyens. Dans le cadre des données à caractère personnel, citons également le Règlement Général européen sur la Protection des Données (RGPD) en vigueur depuis le 25 mai 2018. Celui-ci a pour but d'encadrer l'utilisation des données personnelles afin que cette utilisation ne porte pas atteinte aux droits et libertés des individus, en particulier leur droit à la vie privée.

Outre ces deux textes juridiques importants, la Commission européenne, le Parlement et le Conseil se sont accordés fin 2023 sur une proposition de règlement européen sur l'intelligence artificielle (ou *"AI Act"*) entré en vigueur en août 2024. Ce texte vise à établir un cadre pour l'utilisation des données dans les modèles d'IA en fonction de risques identifiés.

Depuis septembre 2023 également, le Règlement européen sur la gouvernance européenne des données (ou *"Data Governance Act"*) [2] apporte de nouvelles règles en matière de partage de données au sein du marché intérieur. Ce dernier a pour objectif de favoriser le libre partage des données à travers l'Union en encourageant l'instauration d'espaces communs de partage de données et la mise en place d'intermédiaires de données, notamment dans les domaines de la santé, de la mobilité, de l'énergie et de l'agriculture. Le but est ainsi de développer l'accès, la portabilité et l'interopérabilité des données au sein de l'Union, en conciliant le secret des affaires, le respect de la confidentialité des données personnelles et la libre réutilisation des données.

S'il apporte certaines avancées en matière de partage et de mise à disponibilité des données, notamment à travers les intermédiaires de données, le DGA demeure cependant lacunaire sur les formes concrètes que sont susceptibles de prendre les partages de données entre les acteurs publics et privés au sein des Etats membres. Ainsi, il tend à manquer, sur le terrain, des règles de gestion, mais aussi d'organisation des responsabilités, qui articulent de manière adéquate l'ouverture, la protection et le partage des données.

3 Une démarche "sécurité de l'information"

Pour mettre en pratique une telle gestion des responsabilités, il sera nécessaire de disposer d'un "outillage technologique" sur lequel nous pourrons nous appuyer. Il s'agit d'une vision plus technique de notre problématique, présentée cette fois en termes de politique de sécurité (les règles de partage : contrats, règles d'usage, etc.), de métadonnées (traçabilité, etc.).

Si l'on aborde cette problématique sous l'angle de la sécurité de l'information et avec une démarche de gestion des risques (ex : norme ISO/IEC 27005:2022 [3], méthode EBIOS Risk Manager [4]), l'objectif consiste à proposer et à mettre en place des mécanismes permettant de supervi-

1. La gouvernance peut être définie comme : « les formes de pilotage, de coordination et de direction des individus, des groupes, des secteurs, des territoires, et de la société, au-delà des organes classiques du gouvernement. […] avec trois points centraux : l'idée de donner une direction à la société, de mobiliser une coalition et enfin d'exercer une contrainte, soit trois dimensions essentielles du politique ». V. Patrick Le GALÈS, « Gouvernance », Dictionnaire des politiques publiques, Laurie BOUSSAGUET, Sophie JACQUOT et Pauline RAVINET, 5e édition., Paris : Presses de Sciences Po, 2018, p. 299–308

2. Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724

3. ISO/IEC 27005:2022 : Sécurité de l'information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés à la sécurité de l'information

4. EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité (ANSSI)

ser les échanges d'informations entre une multitude d'organisations (les acteurs). Ces entités sont indépendantes les unes des autres, c'est-à-dire qu'elles sont libres de mettre en place leur propre politique de sécurité (de l'information) ; il n'y a pas, à priori, d'autorité centrale. Elles ont en outre chacune leurs propres objectifs et critères d'évaluation, pouvant même éventuellement être concurrentes sur certains points : enjeux économiques, critères et niveaux de sécurité, contraintes réglementaires, etc.

Un certain nombre de technologies et de modèles existent déjà pour garantir des propriétés de sécurité sur les échanges de données entre différents systèmes d'information inter-connectés : cryptographie (chiffrement, signature, tatouage, etc.), journalisation, blockchain [1], contrôle d'accès [2] et contrôle d'usage [3], etc. Elles permettent d'acheminer "correctement" une donnée d'un point A à un point B. Mais vis-à-vis de l'information véhiculée par cette donnée, qu'en est-il de la confiance envers le système qui l'a émise, de la conformité de l'usage qui en sera fait, etc. ?

4 Notre approche

Le défi est de proposer des mécanismes pour mettre en pratique une politique de gouvernance des données et une gestion des responsabilités qui en découlent. L'idée est de pouvoir vérifier automatiquement si les règles de partage qui auront été définies sont bien respectées, ou encore que ces outils soient capables de raisonner pour identifier les causes d'une éventuelle violation et d'en déduire par exemple les responsabilités des différents acteurs.

Ceci nécessite de pouvoir spécifier formellement les règles de partage (dans une "logique mathématique") et d'utiliser ensuite des techniques d'inférence pour le raisonnement. Les "règles" sont exprimées sous la forme de prédicats logiques sur lesquels il sera possible de "raisonner", c'est-à-dire de déduire (notion d'inférence en logique) de nouvelles connaissances (des faits) sur la base des connaissances déjà exprimées. Intuitivement ces règles sont écrites sous la forme "si… alors…". On parle de règles de contrôle d'accès (à l'information) ou de contrôle d'usage (de l'information). Exprimer ces règles dans un langage formel permet ensuite d'automatiser leur traitement au travers d'outils tels que les raisonneurs ou les moteurs d'inférence.

Cette approche est parfaitement réaliste. Dans [4, 5] nous présentons une telle architecture pour le partage des informations basée sur les ontologies. Dans une approche orientée autodétermination informationnelle, et grâce aux outils du Web sémantique, les producteurs de données peuvent ainsi exprimer les règles de contrôle d'usage qu'ils souhaitent voir appliquées, ceci sous la forme de licences (OWL pour exprimer les entités, SWRL pour les règles). Il n'y a pas de "site central" qui imposerait la même politique de partage à tous les acteurs ; les producteurs et les consommateurs de données n'ont pas non plus besoin de communiquer directement les uns avec les autres. Le producteur publie ses données accompagnées de leur licence ; ces données sont alors diffusées, peu importe les moyens utilisés ; le consommateur qui souhaite utiliser une donnée aura alors la responsabilité de vérifier au préalable si l'usage qu'il souhaite en faire est conforme à la licence accompagnant la donnée.

5 Conclusion

Dans le contexte des échanges de données, nos travaux visent donc à mettre en place une gouvernance des données pour contrôler le partage de l'information afin de rassurer les détenteurs de données et les inciter à les mettre à disposition de la communauté. Notre problématique est ainsi orientée vers des aspects tels que la provenance, le contrôle d'usage, la qualité des données, les stratégies de partage.

À noter que cette vision du partage de l'information est en parfaite adéquation avec la stratégie européenne pour les données qui se concrétise au travers du DGA, du *"Data Act"*, etc. Elle nous permettrait également d'opérationnaliser des modèles de gestion des données par les "Communs" tels qu'envisagés dès la fin des années 1970 l'économiste Elinor Ostrom [6].

Références

[1] Riya Sapra and Parneeta Dhaliwal. Blockchain : The new era of Technology. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pages 495–499, 2018.

[2] Pierangela Samarati and Sabrina Capitani de Vimercati. Access control : Policies, models, and mechanisms. In *International school on foundations of security analysis and design*, pages 137–196. Springer, 2000.

[3] Jaehong Park and Ravi Sandhu. Towards usage control models : beyond traditional access control. In *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies*, SACMAT '02, page 57–64, New York, NY, USA, 2002. Association for Computing Machinery.

[4] Nouha Laamech, Manuel Munier, and Congduc Pham. IdSM-O : An IoT Data Sharing Management Ontology for Data Governance. In *Proceedings of the 14th International Conference on Management of Digital EcoSystems*, MEDES '22, page 88–95, NY, USA, 2022. Assoc. for Computing Machinery.

[5] Nouha Laamech, Manuel Munier, and Congduc Pham. Translating Usage Control Policies to Semantic Rules : A Model using OrBAC and SWRL. *Procedia Computer Science*, 225 :1881–1890, 2023. KES 2023.

[6] Vincent Ostrom and Elinor Ostrom. Public goods and public choices. *Alternatives for Delivering Public Services*, 1977.