Métadonnées et Aspects Juridiques: Vie Privée vs Sécurité de l'Information

Manuel Munier[1] V. Lalanne[1] P.Y. Ardoy[2] M. Ricarde[3]

[1]**LIUPPA** (informatique) Université de Pau et des Pays de l'Adour, Mont de Marsan, France

[2]**CRAJ** (droit privé) Université de Pau et des Pays de l'Adour, Pau, France

[3]**BackPlan** (entreprise) Project Communication Control, Pau, France

SARSSI 2014

Saint-Germain-Au-Mont-d'Or (Lyon), France, 13-16 mai 2014

Cet article

- La sécurité de l'information est actuellement un des enjeux majeurs pour les entreprises.
- Nouvelles technologies de l'information: ADSL, 3G/4G, BYOD, services cloud,...
  - ⇝ Les utilisateurs échangent et stockent de plus en plus d'informations
  - ⇝ Ils peuvent faire à peu près tout depuis n'importe où
  - ⇝ Les systèmes d'information sont dorénavant connectés à Internet
  - ⇝ Les données elles-mêmes sont de plus en plus complexes
    - *on parle maintenant de documents structurés*
    - *les données publiques côtoient des données "sensibles"*

⇒ Quid de la sécurité de l'information ?

Cet article

- En SSI, les nouveaux mécanismes de sécurité ont besoin d'en savoir "plus" sur les opérations exécutées
  - utilisateur & rôle, ressource, action
  - date, (géo)localisation, outils utilisés,...
  - opérations précedentes (traçabilité), obligations en attente,...

$\Rightarrow$ **Métadonnées** ("données sur les données")

$\rightsquigarrow$ ~~contrôle d'accès~~ $\rightarrow$ contrôle d'usage

$\rightsquigarrow$ contextes & politiques de sécurité dynamiques

$\rightsquigarrow$ calcul d'indicateurs (confiance, degré d'impact d'un changement, fiabilité,...)

$\Rightarrow$ Quid des aspects juridiques quant à la protection de ces (méta)données ?

Plan

Motivations pour les Métadonnées

De la "sécurité des systèmes d'information" vers la "sécurité de l'information"

- Nos travaux portaient sur le contrôle d'usage pour la gestion du travail collaboratif sur des projets inter-organisationnels
  - ▷ *"Self-Protecting Documents for Cloud Storage Security"* (TrustCom 2012)
  - ▷ Enterprise Digital Right Management (E-DRM)
  - ▷ contrôle d'usage ≡ politique de sécurité pour contrôler **comment** les utilisateurs manipulent les documents
  - ▷ politique de sécurité dynamique ≡ règles de sécurité contextuelles
  - ⇒ Le système doit collecter différentes **métadonnées** pour activer/désactiver les contextes: *localisation de l'utilisateur, confiance de l'utilisateur dans ses partenaires, statut des documents liés, respect des échéances, notes de révision,...*

Motivations pour les Métadonnées

De la "sécurité des systèmes d'information" vers la "sécurité de l'information"

- En activant/désactivant les contextes le système peut ajouter/supprimer des permissions, obligations,... en fonction des actions déjà réalisées, du contenu des métadonnées,...

NB: Documents structurés $\Rightarrow$ les métadonnées sont stockées sur les nœuds du document ($\rightsquigarrow$ granularité fine)

- Utilisation de ces métadonnées:
  - $\rightarrow$ au cours du **cycle de vie du document**: *contrôle d'usage, calcul d'indicateurs,...*
  - $\rightarrow$ **a posteriori**: *traçabilité, preuve en cas de litige,...*

Nos travaux actuels

Nous mettons l'accent sur la sécurité de l'information plutôt que sur la sécurité du système lui-même.

Motivations pour les Métadonnées

Des "technologies de l'information" au "domaine juridique"

- Les métadonnées sont bien connues en **informatique**
  - en *data warehousing* $\rightarrow$ gestion et stockage des données
  - en *business intelligence* $\rightarrow$ tableaux de bord, analyse statistique
- Mais l'utilisation croissante des métadonnées soulève des **questions juridiques** (ex. entre partenaires sur un projet)
  - $\rightsquigarrow$ Les métadonnées impactent les contextes et modifient donc la façon dont les partenaires utilisent les documents (et donc travaillent): *ajout d'obligations, suppression de permissions,...*
  - $\rightsquigarrow$ Les métadonnées servent à calculer des indicateurs (de nouvelles métadonnées) et peuvent ainsi trahir des opinions, la qualité des partenaires et de leur travail,...
  - $\rightsquigarrow$ L'analyse des métadonnées peut conduire à appliquer des pénalités: *engagements non tenus, échéances non respectées,...*

Motivations pour les Métadonnées

Exemple d'application: projet en Génie Pétrolier

- Considérons un projet en Génie Pétrolier tel que la construction d'un pipeline ou d'une installation pétrolière
  - Un tel projet implique de nombreux partenaires et sous-traitants (souvent de plusieurs pays).
  - Le système d'information (appelé registre de documents) contient de nombreux documents
    - ⇝ *spécifications, documents de conception, plans, expertises, certifications, guides de bonnes pratiques, standards,...*
  - Un tel projet définit également de nombreux *workflows* pour la gestion du travail collaboratif
    - ⇝ *suivi des processus, documents "à jour" entre les partenaires, respect des échéances,...*

Motivations pour les Métadonnées

Exemple d'application: projet en Génie Pétrolier

- BackPlan $\rightarrow$ *project communication control*
- Le cœur de métier de BackPlan consiste à fournir:
  - des outils de travail collaboratif entre les entreprises
    - $\rightsquigarrow$ *gestion des workflows, tableaux de bord,...*
  - un service de registre de documents
    - $\rightsquigarrow$ *entrepôt de documents commun, traçabilité des modifications,...*
- BackPlan & métadonnées ?
  - ▷ améliorer la gestion des *workflows*
  - ▷ ajouter de nouveaux indicateurs (très spécifiques) aux tableaux de bord
  - ▷ "lier" les divers documents à des fins de traçabilité et de gestion des responsabilités, tant pendant qu'après le projet

$\Rightarrow$ Importance des aspects juridiques pour l'activité de BackPlan!

Motivations pour les Métadonnées

Autre application: sécurité des Architectures Orientées Services

- Nous avons adopté la même démarche pour la sécurité des SOA (SI interconnectés au travers de services) et des SdS
  - ⇝ contrôle d'usage entre clients, fournisseurs de services, sous-traitants; objectifs de niveau de service
    - ▷ *"Information Security in Business Intelligence based on Cloud"* (WOSIS 2013)
    - ▷ *"Sécurité de l'Information dans les Environnements Inter-Organisationnels"* (SARSSI 2013)
    - ▷ *"Accords de niveau de service et modèle de réputation pour le contrôle d'usage"* (FJC INFORSID 2014)
  - ⇝ métadonnées, traçabilité, indicateurs,... pour la gestion des risques liés à la sécurité de l'information (norme ISO 27005)
    - ▷ *"Information Security Risk Management in a World of Services"* (PASSAT 2013)
    - ▷ *"The Systems-of-Systems Challenge in Security Engineering"* (GPL 2014)
    - ▷ *"Challenges in Security Engineering of Systems-of-Systems"* (CIEL 2014)

Motivations pour les Métadonnées

Bilan

- Remarques:
  - Nous ne cherchons pas à éviter "à tout prix" les comportements non conformes à la politique de sécurité
  - Environnements inter-organisationnels $\Rightarrow$ pas d'organe de contrôle global
  - Nous visons plutôt à définir des objectifs de sécurité (négociés entre les partenaires), à vérifier s'ils ont été respectés et, le cas échéant, à identifier les responsabilités

$\Rightarrow$ Les questions juridiques sont incontournables dès que l'on traite de vulnérabilités, de menaces, de niveaux de service (SLA), de responsabilités,...

Métadonnées & Aspects Juridiques

Sécurité de l'information $\rightsquigarrow$ métadonnées $\rightsquigarrow$ préoccupations juridiques

- Questions: **informatique $\rightarrow$ droit**
  - Quelles métadonnées collecter et stocker ?
  - Quels indicateurs calculer ? (traitements automatisés)
  - Sur la base de telles informations, est-il légal d'influencer les usages "normaux" ?

- Questions: **informatique $\leftarrow$ droit**
  - Quels sont les mécanismes de sécurité requis pour pouvoir utiliser des métadonnées en tant que preuve ?
    (ex: authenticité, intégrité, stabilité)
  - Preuve par les métadonnées ? (jurisprudence)
  - Métadonnées pour la pré-constitution de preuves ?
    (ex: projet terminé conforme aux réglementations en vigueur)

Métadonnées & Aspects Juridiques

Sécurité de l'information ⇝ métadonnées ⇝ préoccupations juridiques

- Clairement, au **LIUPPA** (sécurité informatique) nous n'étions pas compétents sur ces questions

⇒ Nous avons donc pris contact avec nos collègues du **CRAJ** (*Centre de Recherche et d'Analyse Juridique*)

- Le CRAJ est le centre de recherche en droit privé de l'UPPA.
- Ils travaillent sur le droit civil, le droit des affaires, le droit pénal et la criminologie.
- L'ODJ (*Observatoire De la Jurisprudence*) analyse les décisions des juridictions locales, nationales et européennes.

Métadonnées & Aspects Juridiques

Qu'est-ce qu'une métadonnée en droit ?

Métadonnée

Le concept de métadonnée n'est pas une notion bien connue en droit.

- Le préfixe grec *méta-* renvoie à la référence à soi-même
  - ⇝ Le terme "métadonnée" fait référence à des données sur des données, des données qui décrivent d'autres données.
  - ⇝ Le droit ne définit pas, pour le moment, de régime spécifique pour les métadonnées et les traite comme des données classiques.
  - ⇝ Les métadonnées soulèvent trois types de difficultés: leur collecte, leur stockage et leur utilisation.

Métadonnées & Aspects Juridiques

Qu'est-ce qu'une métadonnée en droit ?

- Collecte des métadonnées
  - Bien souvent, cette collecte se fait sinon à l'insu, du moins dans l'ignorance des personnes concernées.
  - Du point de vue de la loi se posent deux questions:
    1. le droit d'accéder aux informations contenues dans les métadonnées
    2. le droit de savoir que l'information est collectée
- Stockage des métadonnées
  - authenticité des métadonnées ($\Rightarrow$ processus de collecte, fiabilité de la source)
  - intégrité, stabilité & disponibilité
- Utilisation des métadonnées
  - de bonne foi: implémentation de mécanismes de sécurité
  - de mauvaise foi: métadonnées détournées de leur utilisation initiale, falsification

Métadonnées & Aspects Juridiques

Droit de la preuve

- C'est essentiellement sur le terrain du droit de la preuve que se placent les rares décisions se référant aux métadonnées.
- En droit civil, la preuve d'un fait juridique peut se faire par tout moyen, à certaines conditions toutefois:
  - la preuve est rapportée avec loyauté
  - le mode de preuve est **fiable**
- Article 1316-1 du Code Civil:

  "L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions **de nature à en garantir l'intégrité**.*"*

$\Rightarrow$ Pour le moment, les rares décisions se référant aux métadonnées exigent principalement leur fiabilité.

Métadonnées & Aspects Juridiques

Droit de la preuve: quelques exemples

- Enquête sur email (2011)
  - Si le problème juridique ne portait pas directement sur la question des métadonnées, la Cour entérine cependant l'argumentaire suivant:

    "La structure particulière d'un fichier de messagerie Outlook et l'obligation de ne modifier ni l'état de l'ordinateur visité, ni les attributs des fichiers (métadonnées contenues dans le fichier lui-même: titre, auteur taille, dates, localisation, signature...) impliquent nécessairement la saisie globale du fichier de messagerie, après avoir vérifié qu'il contient des éléments entrant dans le champ de l'autorisation."

  $\Rightarrow$ Dans tous les cas l'accent est mis sur l'exigence selon laquelle il convient de saisir l'intégralité de messageries Outlook afin de ne pas altérer la fiabilité de la saisie par une altération des métadonnées contenues dans les messages.

Métadonnées & Aspects Juridiques

Droit de la preuve: quelques exemples

- Métadonnées contenues dans des photographies (2010)
  - Un requérant s'appuie sur les métadonnées contenues dans des photographies pour démontrer sa qualité d'auteur des photographies.
  - La Cour retient les métadonnées (données EXIF) comme éléments de preuve en relevant que celles-ci comportent l'identité de l'auteur, la date et l'heure des prises de vues, le nom du fabriquant de l'appareil, le modèle de celui-ci, ainsi que le détail des réglages de l'appareil.
  - Si les métadonnées ne peuvent en soi démontrer l'originalité des photographies, elles sont toutefois des éléments permettant d'en établir la paternité et peuvent s'avérer fort utiles dans le cadre d'un procès en contrefaçon comme en l'espèce.

NB: Notes que la fiabilité des métadonnées n'a pas été abordée !

Métadonnées & Aspects Juridiques

Travaux actuels

- Mémoire de recherche de Camille Drouiller (juillet 2013)
  - "*La preuve par les métadonnées*"
  - Master recherche, droit privé général et appliqué
  - encadré par Pierre-Yves Ardoy
  - quelques éléments de la conclusion:
    - ⇝ Rien ne s'oppose à ce que les métadonnées soient utilisées, ou tout du moins examinées, lors d'un procès.
    - ⇝ Les métadonnées renouvellent les exigences d'imputabilité et de fiabilité des données collectées: retenir une preuve impose de croire en sa véracité.
    - ⇝ L'émergence de technologies a toujours eu pour effet de susciter des craintes quant à leur admission en justice à titre de preuve (comme la photocopie ou les enregistrements sonores au milieu du $20^{\text{ème}}$ siècle).

Métadonnées & Aspects Juridiques

Travaux actuels

- La première étape était de vérifier si les métadonnées pouvaient bien servir de preuves
  - ▷ Les investigations numériques deviennent de plus en plus fréquentes.
  - ⚠ La Cour prononce un jugement sur la base des arguments avancés par chaque partie, mais ne recherche pas la vérité absolue
    - ⇒ Si personne ne proteste, même des données "peu fiables" peuvent parfois servir de preuves !
    - ⇒ C'est le travail des experts en investigation numérique.
- L'investigation numérique implique également de considérer la protection des données
  - ▷ données personnelles $\rightsquigarrow$ vie privée et libertés individuelles
  - ▷ données confidentielles en entreprise $\rightsquigarrow$ préoccupations socio-économiques

Métadonnées & Aspects Socio-Économiques

Protection des données

Société numérique

Dans la société de l'information actuelle, les métadonnées deviennent parfois plus importantes que les données auxquelles elles sont associées.

- Que ce soit dans le domaine de la vie privée (données personnelles) ou professionnelle (données métier d'une entreprise), de nombreuses sociétés en ont fait leur *business*.
- Les médias s'agitent autour de grandes multinationales telles que Google, Facebook ou Microsoft quant à la protection de la vie privée et des données personnelles.
  - C'est un thème d'actualité qui fait peur au public.
- Dans le monde professionnel les problèmes sont identiques avec, cette fois, les données stratégiques de l'entreprise.
  - recherche & développement, stratégie commerciale,...

Métadonnées & Aspects Socio-Économiques

Protection des données

- Exemples:
  - Facebook & tags sur les photos
    - $\Rightarrow$ Une photo d'un groupe d'amis publiée sur Internet peut contenir les noms des personnes sur la photo, le lieu où elle a été prise, la date et l'heure du cliché.
  - Google
    - $\Rightarrow$ Interactions entre GMail, Calendar, Drive, Maps, Search, équipements Android,...
  - BackPlan
    - $\Rightarrow$ Son activité consiste à utiliser les métadonnées associées aux informations échangées entre les participants pour assurer la gestion des projets.

Métadonnées & Aspects Socio-Économiques

Les données, puissance du futur

- Nous vivons une période de rupture, celle de la numérisation de tout: l'homme, la société, les organisations, le savoir, les interactions,...
- Les données constituent les briques de base de la société de l'information.
- Les données sont au cœur de l'économie.
  - données personnelles produites par les usagers (textes, photos, vidéos,...)
  - données générées par les systèmes que nous utilisons (souvent à notre insu)
- La captation de données est la priorité absolue de certains pays tels que les États-Unis ou la Chine... mais pas que...!

Métadonnées & Aspects Socio-Économiques

Localisation des données

- Les services externalisés (comme le stockage ou le traitement dans le *cloud*) peuvent être situés n'importe où dans le monde, parfois sans aucune possibilité de choisir le pays.

ex: USA PATRIOT Act $\Rightarrow$ la loi américaine permet à ses services de sécurité d'accéder:

- aux données de sociétés américaines, même si ces données sont stockées physiquement sur le territoire européen
- aux données de leurs filiales, même si elles sont implantées dans un autre pays du monde
- aux données stockées sur des serveurs hébergés aux États-Unis, y compris si la société qui possède ces serveurs est d'une autre nationalité

Métadonnées & Aspects Socio-Économiques

Localisation des données

- USA PATRIOT Act ⇒ scandale **PRISM**
  - PRISM est un programme d'exploration de données et de surveillance électronique de masse exploité par la NSA (United States National Security Agency) depuis 2007.
  - Son existence a été révélée six ans plus tard par Edward Snowden (juin 2013)
    - → *"The extent of mass data collection was far greater than the public knew."*
  - PRISM consiste à recueillir les données **"directement sur les serveurs"** de plusieurs grands fournisseurs de services Internet: Google, Facebook, Microsoft, Apple,...
    - → *Le chiffrement des données est inutile puisque que les données doivent être déchiffrées sur le serveur avant d'être traitées !*

Métadonnées & Aspects Socio-Économiques

Internet sur écoute

- USA PATRIOT Act ⇒ PRISM ⇒ **Bullrun**
  - Le chiffrement des contenus n'est plus une protection efficace.
  - La NSA a lancé il y a plusieurs années Bullrun, un programme clandestin pour casser la protection par chiffrement via l'affaiblissement des normes, l'introduction de portes dérobées et même le vol de clés de chiffrement.
    - → *"This includes SSL, VPN and security of GSM networks."* (New York Times)
  - La NSA se justifie en faisant appel à la sécurité nationale et explique que le pays ferait face à de graves risques si les messages des espions étrangers, des terroristes,... ne pouvaient pas être piratés.

Métadonnées & Aspects Socio-Économiques

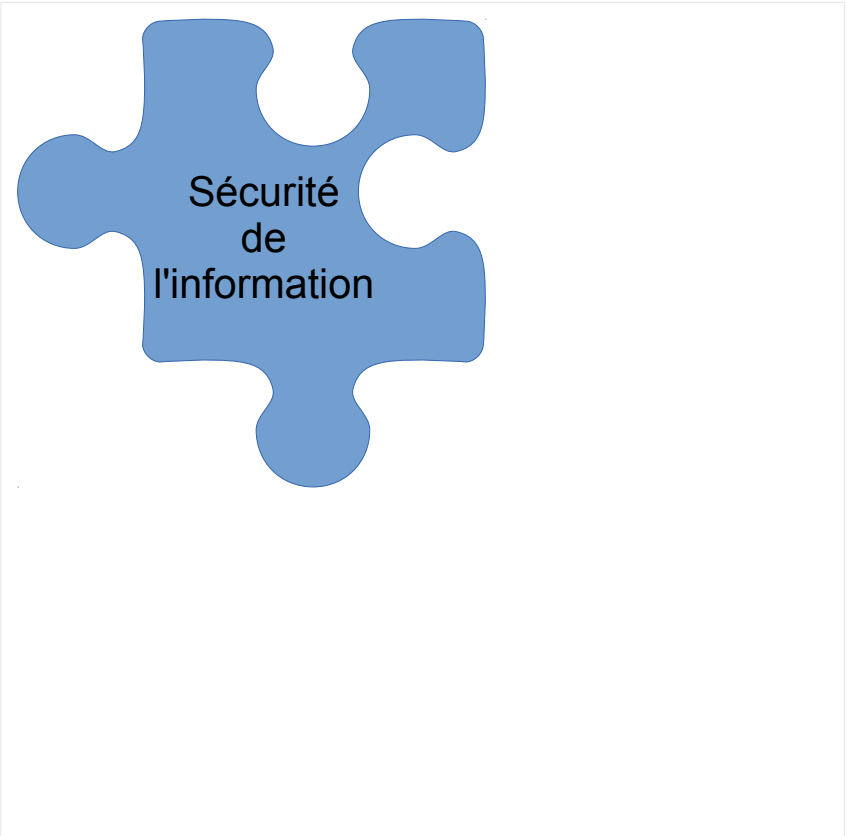
Retour à la gestion des risques liés à la sécurité de l'information

- Notre objectif n'est pas de porter un jugement sur le "USA PATRIOT Act" et autres projets secrets.
- Simplement, dans l'état actuel des législations, une entreprise (ex: européenne) ayant des contraintes fortes sur la confidentialité de ses données **doit donc être vigilante quant au choix de son prestataire de services** (localisation des données et nationalité du prestataire).
  - → pour se conformer aux lois en vigueur
  - → pour garantir la protection des données personnelles de ses clients et de ses employés
  - → pour protéger ses données stratégiques
  - → pour garder secrètes ses relations avec ses partenaires et ses sous-traitants

⇒ Nous en revenons donc à la **gestion des risques liés à la sécurité de l'information**

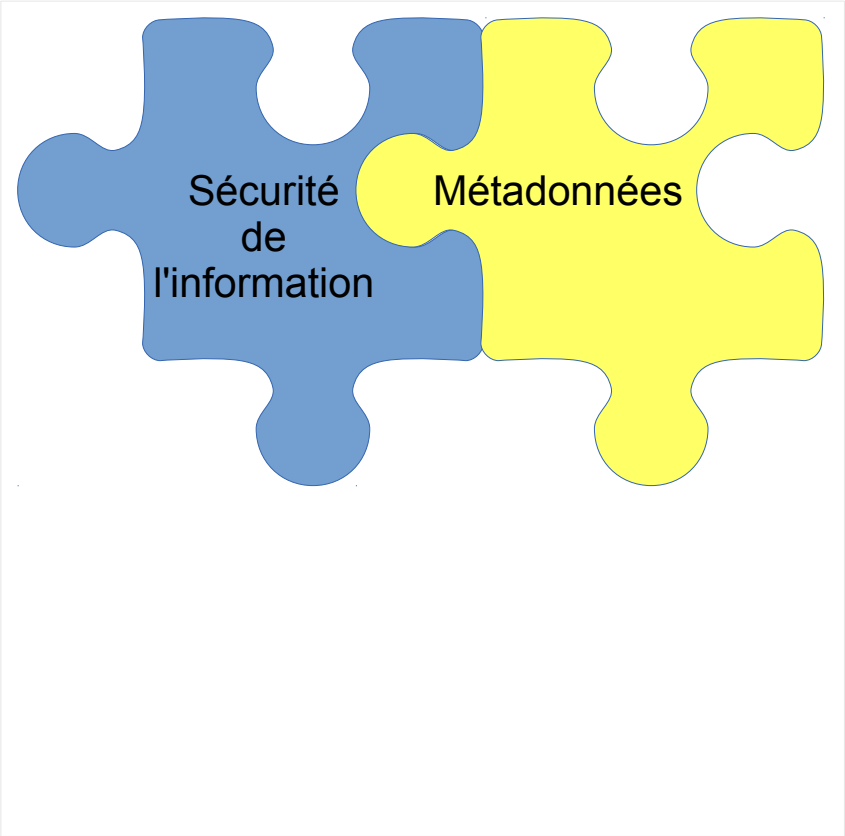
Plan

Conclusion
Synthèse



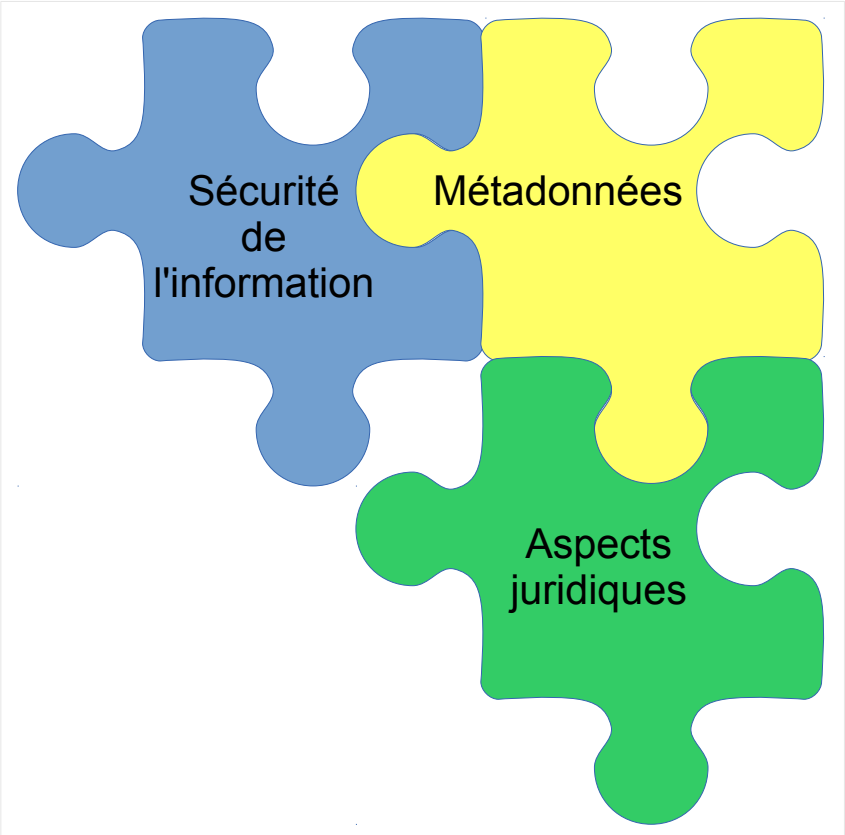
→ Nous travaillons sur la sécurité informatique et la gestion des risques liés à la sécurité de l'information.

Conclusion
Synthèse



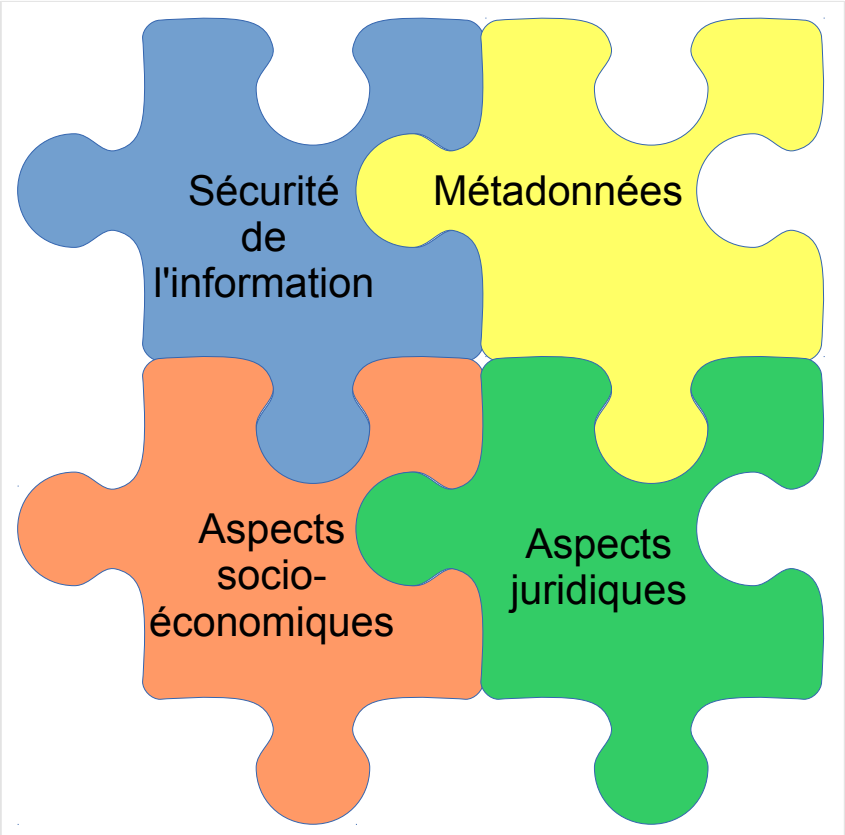
→ Pour améliorer et définir de nouveaux mécanismes de sécurité nous avons besoin de métadonnées (ex: contrôle d'usage).

Conclusion
Synthèse



→ Mais la collecte, le stockage et l'utilisation de ces métadonnées soulève des questions juridiques.

Conclusion
Synthèse



→ Et travailler dans la société de l'information actuelle exige d'être conscient des risques liés à la sécurité de l'information.

Conclusion
Perspectives

- La confiance dans les données que nous traitons chaque jour est l'un des principaux défis de la société de l'information.
- Il existe beaucoup de mécanismes qui nous permettent de recueillir, stocker et traiter d'énormes quantités de données, et en particulier des données sur ces données: métadonnées.
- Les métadonnées deviennent un outil essentiel pour la sécurité de l'information: contrôle d'usage pour le partage de documents et la sécurité du *cloud*, investigation numérique, preuve en cas de litige,...
- Mais les possibilités de la technologie de l'information ne doivent cependant pas nous faire oublier les questions juridiques.

Conclusion
Perspectives

- Vers une "CNIL Européenne"
  - L'Union Européenne a l'ambition de devenir la référence mondiale pour la protection des données.
  - Cela nécessitera la création d'une Autorité Européenne de Protection des Données (en tant qu'autorité administrative indépendante)
- Pour la communauté juridique, les métadonnées doivent-elles recevoir un régime juridique spécifique ?
- Pour la communauté informatique:
  - Comment définir une classification des métadonnées ?
  - Comment utiliser les métadonnées dans les SLA ?
  - Comment les métadonnées peuvent-elles améliorer la gestion des risques liés à la sécurité de l'information ? (ex: nouveau critère de sécurité tel que la maîtrisabilité)

Métadonnées et Aspects Juridiques: Vie Privée vs Sécurité de l'Information

Manuel Munier, Vincent Lalanne, Pierre-Yves Ardoy, Magali Ricarde

Merci pour votre attention.

manuel.munier@univ-pau.fr

http://www.univ-pau.fr/

http://www.backplan.fr/