La gouvernance informationnelle et ses multiples facettes : recueil de travaux d'étudiants

Travail d'édition : Aurèle Nicolet, assistant HES

Table des matières

Résumé

La filière Information documentaire de la Haute école de gestion de Genève (HEG) propose dans le cadre de son Master en Sciences de l'information un module de spécialisation, sous la direction du Prof. Dr. Basma Makhlouf Shabou, consacré à la gouvernance des données. Comme travail personnel, il a été demandé à chaque étudiant de s'intéresser à un aspect de la gouvernance des données ou à un type de données en particulier. Au vu de la qualité de leurs travaux, nous avons proposé aux étudiants intéressés de publier leur travail sur *Ressi*, moyennant quelques ajustements[1].

Chacune des cinq sections de l'article correspond à un travail, hors introduction et conclusion. Les voici ci-dessous :

- Les actifs informationnels : définitions et évaluations. Un état de l'art entre théories et pratiques – Ágnes A. Motisi-Nagy tente de définir le concept d'actif informationnel en partant de la littérature professionnelle et des normes.
- Valeur probante du document électronique : nature et exigences – Lise Lefort s'appuie sur le droit suisse et les normes, notamment l'ISO 15489, afin de déterminer les exigences auxquelles doit se plier un document électronique afin de posséder une valeur probante.
- Le traitement des données personnelles dans les procédures d'E-Discovery : présentation des contextes suisse et européen – Sandrine Anderfuhren s'intéresse à la délicate question des données personnelles dans les procédures d'E-Discovery et présente les similitudes et différences entre les pratiques suisses et européennes.
- Etat de l'art des documents gouvernant les données de la recherche dans les Hautes écoles suisses – Tania Zuber Dutoit fait le point sur la gouvernance des données de la recherche dans les Hautes écoles au travers des documents.
- Gouvernance des données musicales électroniques : Le cas des métadonnées de Spotify – Matthieu Putallaz s'est penché sur la gestion des données musicales par Spotify et notamment son utilisation des métadonnées de description.

Introduction

Gouvernance de l'information (*information governance*), gouvernance des données (*data governance*) ou encore gouvernance des technologies de l'information (*IT governance*)… Chacune de ces expressions renvoie à la gouvernance, mais le champ auquel cette dernière s'applique peut s'avérer difficile à délimiter.

Avant de s'intéresser aux différences qui nous préoccupent, il convient de définir la notion commune à chacun des termes. Le mot « gouvernance » vient du grec *κυβερνάω* et, à l'origine, signifie « diriger un navire », mais acquiert rapidement, avec Platon et son ouvrage *République*, le sens de « gouverner » (Nicolet 2016, p. 2). Au sein d'une organisation, la gouvernance est une structure administrative de niveau supérieur qui en établit la stratégie en déterminant les rôles, les responsabilités, les processus décisionnels, les politiques et les procédures d'une part et en surveillant les résultats et la conformité d'autre part (InterPARES Trust [s. d.]).

[1] Nous remercions vivement Silas Krug, assistant HES, pour sa relecture minutieuse.

Il est difficile de distinguer « information » et « donnée », car la différence est subtile. La donnée est la forme atomique des faits et des idées, alors que l'information renvoie à des concepts plus complexes composés d'éléments de données multiples (Pearce-Moses 2016).

Au niveau des gouvernances, nous retrouvons ces distinctions. La gouvernance des données comprend les processus, les méthodes, les outils et les techniques visant à garantir que les données sont de haute qualité, fiables et uniques (non dupliquées), de sorte que leurs utilisations en aval, dans les rapports et les bases de données, soient les plus fiables et exactes possibles (Smallwood 2014). La gouvernance informationnelle, de son côté, se compose des politiques et des processus généraux visant à optimiser et à tirer parti de l'information tout en la protégeant et en respectant les obligations juridiques et les obligations en matière de protection de la vie privée, conformément aux objectifs opérationnels énoncés par l'organisation (Smallwood 2014).

Les sujets traités par nos étudiants se situent dans l'une ou l'autre de ces gouvernances.

Les actifs informationnels : définitions et évaluations. Un état de l'art entre théories et pratiques (Ágnes A. Motisi-Nagy)

Introduction

Que sont les actifs informationnels ? Pourquoi et comment les identifier ? Comment mesurer leur valeur et comment les protéger ? Ces questions se posent avec force parmi les économistes depuis la fin des années 1980. La présente section propose un bref tour d'horizon de la notion d'« actif informationnel » en partant de ses principes constitutifs identifiés dans la littérature scientifique. Nous allons ensuite confronter la théorie à la pratique actuelle par une sélection de définitions de la dernière décennie du monde européen et nord-américain de l'entreprise et de l'administration publique, disponibles en ligne. Enfin, nous tenterons de dégager quelques pistes de réflexions pour l'avenir à l'aide de la littérature professionnelle. Pour faciliter la lecture de ce dossier particulièrement dense, nous mettrons en exergue les idées saillantes par du caractère gras et en soulignant les aspects qui nous semblent fondamentaux pour appréhender la question dans toute son ampleur.

Principes constitutifs de la notion d'*actif informationnel* dans la littérature scientifique

Le vocabulaire : *Information asset(s)*, *informational asset(s)* ou actif(s) informationnel(s) ?

Aux termes français « actif informationnel » et « actifs informationnels » quatre formulations semblent correspondre en anglais : *information asset* (sing. et plur.) et *informational asset* (sing. et plur.). La question se pose d'emblée de savoir si une différence significative existe entre eux. Dans le cadre de cette section, nous avons décidé d'adopter et d'adapter l'explication du dictionnaire en ligne de l'Office québécois de la langue française (2005), *En toute sécurité informatique* qui définit **les pluriels** *informational assets* et *information assets* comme de parfaits synonymes qui **se traduisent en français par « actif informationnel » au singulier**. En anglais le pluriel désigne un ensemble, tandis que le singulier fait référence à un élément précis de l'ensemble. En français, en revanche, le singulier doit être utilisé pour l'ensemble ; pour ne désigner qu'un seul élément, le dictionnaire propose l'expression « élément d'actif informationnel ».

Nous utiliserons donc le singulier pour désigner un type d'actif dans son ensemble ainsi que la notion d'actif elle-même. Considérant qu'une organisation peut posséder **plusieurs types d'actifs informationnels**, nous réserverons l'usage du pluriel pour mettre en avant cette pluralité.

Le capitalisme de l'information

Dès la fin des années 50, H.J. Leavitt et T.L. Whisler (1958, p.41) prédisent que l'**information** prendra bientôt une **importance stratégique** dans la gestion des entreprises. Son impact devenant de plus en plus considérable, la nécessité d'appliquer un **contrôle** interne à sa gestion et **l'optimisation de son utilisation** commenceront effectivement à devenir un enjeu majeur dès les années 70. Cette attention accrue sera notamment l'un des moteurs du **développement des technologies de l'information**.

Toutefois l'idée que l'information est un **actif intangible**, et donc une **valeur comptable**, n'émergera qu'au tournant des années 90. En 1988 K.E. Boulding estime ainsi que « **l'information est à la connaissance ce que le revenu est au capital** » (cité par Cronin : 1997, p.11). Une nouvelle terminologie apparaît alors, comprenant des termes comme « actifs informationnels » (***information assets***, Cronin : 1989) et « **capital intellectuel** » (Stewart : 1997), ce qui conduit tout naturellement à l'idée du « **capital structurel** » et du « **capital organisationnel** », défini par Donald Lamberton (1997, p.77) comme « la combinaison de **dispositions institutionnelles**, de **styles de comportement** et d'**information accumulée** qui nous permet de **faire usage de l'information** ». Comme le souligne très justement Blaise Cronin (1997, p.12), ces termes sont implicitement liés à l'idée d'un « **capitalisme de l'information** ». Or, dans ce système économique les entreprises sont supposées **tirer leur profit** de l'**utilisation** ou de la **vente** d'information (Kling, Ackerman & Allen : 1996, p. 731).

Traiter l'information comme n'importe quel actif, en évaluer la valeur financière et la faire figurer au bilan de l'entreprise viseraient donc les **deux objectifs de base de tous bilans comptables** : d'un côté, **démontrer la contribution de l'information à la valeur globale d'une entreprise** pour le public externe, et de l'autre, **encourager sa meilleure utilisation** pour le public interne (Yates-Mercer & Bawden : 2001, p.20). Cette orientation a stimulé le développement de nouvelles méthodes d'identification et d'évaluation des « actifs informationnels ». Cependant, comme le reconnaît Cronin : « L'information est l'enfant terrible de la théorie économique classique : **il n'existe pas d'étalon auquel se référer pour la quantifier**, l'apprécier ou l'évaluer » (1997, p.11). Ou encore, comme le formulent Moody et Walsh (1999, p.2), l'information est un « actif commercial stratégique », qui est « un **actif précieux mais largement non valorisé** ».

Les caractéristiques comptables d'un actif

Comme le rappellent Moody et Walsh (1999, p.3.), un *assets* doit posséder trois critères spécifiques du point de vue comptable, auxquels l'information – du moins **certains types d'information** – répondent parfaitement :

1. Il est susceptible de fournir des services futurs ou des **avantages économiques**. Les avantages peuvent découler de **l'utilisation** ou de la **vente** des actifs.
2. Il est **sous le contrôle de l'organisme**.
3. Le contrôle de l'actif a été obtenu par l'**achat**, le **développement interne** ou la **découverte**.

Enfin, comme tous les actifs, l'information a un **coût** et une **valeur**. Toutefois, pour Moody et Walsh la similitude s'arrête là, car **l'information obéit à ces propres lois (cf. Annexe II.**).

Les valeurs comptables des actifs

Dans la théorie comptable classique un actif peut avoir deux types de valeurs : **valeur d'échange** (la vente) et **valeur d'usage** (utilisation) (Moody et Walsh : 1999, p.5), mais en ce qui concerne spécifiquement l'information, Doug Laney (2011, p.15) énumère pas moins de six types de valeurs : **intrinsèque** (fiabilité, exhaustivité, exclusivité), **business** (pertinence pour les objectifs commerciaux), **coût** (coûts causés par une perte), **performance** (effet sur les principaux moteurs d'activité), **économique** (contribution à la rentabilité) et de **marché** (vente des données). Reynold Leming estime de son côté qu'il existe quatre types de valeurs : **informationnelle**, **probante**, **économique** et **patrimoniale** (Mancini : 2016, p.7).

Pour Moody et Walsh les deux valeurs se mesurent sur trois aspects : le **coût** (combien l'acquisition, la gestion et le stockage coûtent à l'entreprise), le **marché** (à quel prix l'actif pourrait-il être vendu), et l'**utilité** (combien il pourrait rapporter à l'avenir). **Pour Laney l'aspect « coût » est en réalité une valeur** pour l'information qui peut être inscrite parmi les actifs du bilan. C'est la valeur de **remplacement** : de ce point de vue **l'information vaut autant que sa reconstitution coûterait à l'organisme** en cas de perte/vol, ou encore en frais de justice, amende ou dommage et intérêt en cas de non présentation de documents probants, etc. **C'est cette valeur qui est aujourd'hui au cœur des préoccupations et qui est très fortement liée à la notion du risque.**

Infonomics : au carrefour des sciences de l'information et de l'économie

En 1999, dans un article de recherche du Groupe META, Doug Laney dénonce une réalité : l'information n'est pas formellement évaluée, reconnue ou déclarée comme un actif économique dans les entreprises (Laney : 2017). C'est dans ce contexte qu'il utilise pour la première fois le terme *infonomics* pour nommer une nouvelle discipline à la croisée des sciences économiques et de la science de l'information qui affirme l'importance économique de l'information, propose de mesurer sa valeur comptable pour l'organisme, et fournit un cadre aux entreprises pour la valoriser, la gérer et l'utiliser comme un véritable atout. *L'Infonomics* est né d'un **intérêt commun des économistes et des archivistes**/records managers. Il n'est dès lors pas surprenant qu'au centre de leurs préoccupations communes se trouvent la notion de *risque* en tant que **perte de disponibilité, d'intégrité et de confidentialité,** ainsi que les **documents probatoires** (Clavier & Paganelli : 2013, pp.175-176). La **catégorisation des actifs informationnels** (CAI) qu'ils ont développée sert à bien identifier les **risques potentiels** liés à l'information afin de les prévenir ou de les accepter (si le risque est minime ou si le coût de mitigation est trop élevé). S'appuyant sur la **famille de normes ISO 27000**, la CAI est un outil de gestion qui, à terme, permet de déterminer les priorités institutionnelles en matière de rehaussement de la gouvernance informationnelle (Servais 2015, pp. 23-24).

Une définition de l'actif informationnel ?

En 2016 une équipe de trois chercheurs sudafricains, spécialistes d'IT et de gestion de risque informationnel, a mené **une enquête approfondie sur la définition de la notion d'*information assets* dans les normes et référentiels actuels** (Adesemowo, von Solms & Botha : 2016). En effet ils ont constaté que tandis qu'un grand nombre de travaux traitent des risques qui menacent les actifs informationnels, **la nature même des actifs n'est pas bien étudiée**. Ils souhaitaient donc soit trouver une définition cohérente et largement utilisable dans divers domaines économiques soit, à défaut, en proposer une à partir d'éléments des divers textes normatifs. Contrairement à leurs attentes, l'étude a conclu que **toutes les définitions actuelles étaient incohérentes et insuffisantes, y compris les normes ISO (55001, 27001, 38500 et 20000), et les référentiels ITIL et COBIT**. Or **lorsque l'actif à contrôler n'est pas correctement défini et compris, il risque de ne pas être correctement géré**. Cela implique que l'efficacité, l'efficience, la fiabilité du contrôle interne et le respect de la législation et de la réglementation applicables ne seraient pas appropriés. Selon les trois auteurs, **le plus grand risque qui menace actuellement les actifs informationnels est le manque de compréhension de ce qui les constitue et donc de ce qui doit être protégé**.

La définition que les chercheurs proposent est très intéressante car suffisamment large pour pouvoir être applicable dans des contextes divers :

> *« (Information assets are) Intangible assets consisting of information* ***having no physical form*** *that could be identified singly or collectively, which when arranged systematically or logically could,* ***give an organisation a competitive advantage and the necessary leeway to innovate*** *(p.10) »*[2].

Définitions actuelles de la notion d'actif informationnel dans le monde des entreprises et de l'administration publique

Nous nous sommes basés sur un corpus de documents afin d'identifier diverses conceptions de la notion d'*actif informationnel*, trouvables en Amérique du Nord et en Europe. Ces conceptions sont présentées ci-après.

Amérique du Nord

Les Etats-Unis : l'information organisée ou le système qui l'organise ?

Nous avons sélectionné pour ce dossier deux définitions contradictoires qui coexistent en 2017 aux Etats-Unis : celle qui définit les actifs informationnels comme de **l'information organisée** (*IAD* : 2017), et celle qui n'inclut dans la notion que les **systèmes qui l'organise** (*Clearwater compliance* : 2017). Les deux sont portées par des entreprises spécialisées en conseil et solution. IAD se focalise sur le **développement de la valeur de l'information** par **l'organisation :** il propose de créer des *assets* en rendant l'information **utile** et **facilement accessible** à ceux qui en ont besoin afin d'éviter les risques d'inefficacité, d'incohérence et de limitation. Pour IAD **les outils informatiques sont simplement le moyen d'y arriver mais ne font pas partie de l'actif proprement dit**. *Clearwater compliance,* spécialisée dans la **protection** des données sensibles, définit l'*information asset* au contraire comme une **application**, un **système** ou une **solution métier** qui sert à **gérer des informations sensibles** dont la confidentialité, l'intégrité et la disponibilité doivent être préservées dans le cadre de la **gestion globale des risques** de l'entreprise.

Le Canada : l'information, les systèmes et les équipements informatiques

Au Québec, les termes « actifs informationnels » et « actif informationnel » sont très répandus dans les règlements internes des entreprises et des administrations publiques encadrant la **sécurité informatique**. Plusieurs définitions en sont données, mais celles-ci se rejoignent presque sans exception dans les grandes lignes. Les actifs informationnels comprennent ainsi **l'information et ses supports** dans le sens large du terme. Pour les informations numériques cela inclut les **applications, logiciels, progiciels, systèmes d'information, réseaux**, ainsi que les **équipements** qui permettent de les visualiser. La définition du Secrétariat du Conseil du trésor (Québec : 2016) est particulièrement intéressante. Elle identifie un actif informationnel purement et simplement à **un document au sens de l'article 3 de la *Loi*** *concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1) : « un document est constitué d'information portée par un support ». Or il est expressément précisé plus loin qu'une banque de données, en tant qu'information *et* son support, doit être considérée comme **document**. La *Loi concernant le partage de certains renseignements de santé* (Québec : 2017), dans sa définition du terme « actif informationnel » ne fait que détailler cette acception de la notion de *support* en énumérant plusieurs éléments informatiques.

[2] (Un actif informationnel est un) actif intangible constitué d'informations n'ayant pas de forme physique pouvant être identifiées isolément ou collectivement, qui, lorsqu'il est disposé de manière systématique ou logique, peut conférer à une organisation un avantage concurrentiel et la marge de manœuvre nécessaire pour innover (trad. pers.).

Si le cœur des définitions québécoises analysées reste donc similaire, il est tout de même possible de distinguer **trois courants selon la nature du support** de l'information compté parmi les actifs informationnels. Tandis que certaines concernent **uniquement les informations numériques** (Fondation de bibliothèque et archives nationales du Québec 2016, p. 1 ; Ultima 2016, p.7) ; d'autres comprennent **également le papier** (Agence de la santé et des services sociaux de Montréal 2012 et 2015 ; Office québécois de la langue française 2005 ; Lessard 2009, p. 17). Enfin, le Groupe Canam (2007), une entreprise de métallurgie canadienne, estime que même **l'information verbale** y est comprise. Cette dernière définition, pour le moment unique dans notre corpus et relativement ancienne, semble d'ailleurs complètement contredire celle de **l'Office québécois de la langue française (2005) qui exclut expressément du périmètre des actifs informationnels les ressources humaines**.

Europe

La Grande Bretagne

En Grande Bretagne, les *Archives nationales* qui sont en première ligne dans le conseil en matière d'actif informationnel définissent celui-ci comme « un ensemble d'informations, défini et géré comme une **unité unique**, afin qu'il puisse être compris, partagé, protégé et exploité efficacement ». Elles rappellent également que les actifs informationnels ont une **valeur**, un **risque**, un **contenu** et des **cycles de vie** reconnaissables et **gérables** (The National Archives, 2017). Cette définition est bien plus proche de la vision de *IAD* que de celle de *Clearwater compliance* ou des définitions canadiennes. Toutefois une nouvelle dimension y est mise en exergue, celle de cycle de vie, signe de **l'appropriation de la notion par la science de l'information**. Cette définition des Archives nationales britanniques est devenue *de facto* la norme dans toutes les administrations publiques du pays (National Institute for Health and Care Excellence (NICE) 2015, p. 4 ; Council of Islington 2015, p.4 ; Wallace 2014, p.4 ; Oxfordshire County Council 2015, p.18). Par ailleurs, bien que ces parties du monde ne fassent pas partie de notre périmètre de recherche, il convient de mentionner que la définition susmentionnée sert également de base aux définitions du terme en Australie et en Nouvelle-Zélande (Institute of Directors in New Zealand 2017 ; Victorian Government 2018, p.8 ; Tasmanian Archives and heritage office (TAHO) 2015, p. 2 ; University of Tasmania. Records management unit 2018, p.1).

La Suisse

En Suisse il est extrêmement difficile de trouver une définition du terme « actifs informationnels » (que ce soit au singulier ou au pluriel), du moins dans les règlements d'entreprises disponibles en ligne. Si le terme est sans conteste fréquemment utilisé, **c'est pratiquement toujours sans définition** préalable comme si son sens allait de soi. Cela se vérifie de façon particulièrement emblématique dans le document intitulé « Records management et gouvernance informationnelle : Concepts et explications » de l'Université de Lausanne (2016) qui utilise le terme « actifs informationnels » dans son préambule, sans le définir. On y apprend toutefois que ces actifs devront être gouvernés **selon les principes du records management et de l'archivistique**, ce qui sous-entend qu'ils **comprennent l'information, mais pas les systèmes et les équipements informatiques**. Tenter de dégager une définition à partir du contexte donne l'impression que, dans notre corpus, **le terme « actifs informationnels » est souvent simplement synonyme de « données »**, et notamment de celles qui ont de la valeur et **qu'il faut protéger de la perte, du vol et des accès non autorisés** (Conseil d'Etat du Canton du Valais 2015 ; E-Health Suisse 2017, p. 27).

La Banque Barclays (2016) fait figure d'exception en fournissant une définition claire du terme « actif informationnel » dans un document règlementant la **sécurité informatique** destiné à ses partenaires externes. Pour Barclays, « actif informationnel » égale **information** ou **groupe d'information**. Bien que la définition ne le précise pas, il devient évident par le contexte que ce terme ne s'applique – du moins dans le périmètre du document – qu'à **l'information sur support informatique**.

Analyse et synthèse du corpus

Ce rapide tour d'horizon de définitions actuelles permet de dégager quelques constantes qui méritent réflexion :

1. D'abord, l'Amérique du Nord et les pays anglo-saxons sont bien plus avancés dans la définition des actifs informationnels que la Suisse. On note en particulier **l'intérêt de la législation pour la notion au Québec**, ainsi que l'immense **influence des archives nationales britanniques sur les administrations publiques** bien au-delà des frontières du pays. **L'absence totale d'une définition précise dans les administrations publiques suisses est en revanche très inquiétante.**

2. Ensuite, la **préoccupation sécuritaire** est prédominante : toutes les définitions du corpus proviennent de documents destinés à **gérer les risques** liés à l'information. L'importance des actifs informationnels définis par l'aspect « risque » se mesure uniquement à leurs composants légaux et sécuritaires (respect des obligations légales et administratives, protection des renseignements personnels ou sensibles, etc.). Il convient de noter que cet usage est en accord avec une partie de la littérature scientifique et professionnelle qui approche la question également sous cet angle. **Pourtant, comme l'ont déjà rappelé Moody et Walsh, un *asset* n'est pas l'évitement d'un risque : « something is only an asset from an accounting viewpoint if it is expected to provide future services or economic benefits ». L'aspect risque ne devrait donc pas être le seul angle d'approche pour comprendre, évaluer et gérer les actifs informationnels.**

3. Enfin, **le caractère IT, en tant que support** de l'information **et outil organisationnel, semble souvent indissociable** de la définition d'actif informationnel. Effectivement, le développement des technologies de l'information va de pair avec la reconnaissance de l'importance stratégique de l'information. Toutefois, de manière paradoxale, au lieu de résoudre le problème de la gestion et de la valorisation de l'information non seulement celles-ci en complexifient les processus par la quantité et la diversité phénoménale des données collectées, mais surtout **elles dévient et décentrent la question de la valeur de l'information,** et ce de deux manières dont nous retrouvons les traces dans le corpus :

    a. d'une part, elles font oublier que **l'information n'existe pas seulement sous forme numérique** ou, pire, que **l'« information » n'égale pas les « données »**. Dès lors, **leur gestion ne doit pas être le domaine exclusif des informaticiens, mais bien celui des spécialistes des sciences de l'information**. Comme le souligne l'étude des chercheurs sud-africains : **les données, l'information et la connaissance font partie intégrante des actifs informationnels** (Adesemowo, von Solms, & Botha : 2016, p.2). L'approche du Groupe Canam, qui inclut l'information verbale dans ses actifs informationnels est porteuse de cette **vision plus globale mais qui semble être très minoritaire**, tant dans la théorie que dans la pratique.

b. d'autre part, l'information étant par nature intangible, **la tentation est grande de calculer plutôt la valeur des outils qui les créent, captent, stockent et gèrent que l'information en elle-même**. Pourtant déjà Moody et Walsh (1999, p.3) révèlent la fausseté de cette approche simpliste. En effet, **le matériel informatique et les logiciels ne sont que des mécanismes** utilisés pour créer et maintenir des informations.

Quel avenir pour l'actif informationnel ?

La vision des *leaders* d'ELC et du *chief evangelist* d'AIIM

L'été 2016 l'Executive Leadership Council (ELC) et l'Association for Information and Image Management (AIIM) ont consacré un congrès à l'*infonomics* qui a réuni 86 leaders d'entreprise actifs en gestion de l'information en Amérique du Nord et en Europe. Leur constat, formulé par le *chief evangelist* d'AIIM John Mancini, est amère (Mancini : 2016). Ceux-ci observent en effet unanimement que bien que l'information soit une ressource indispensable de l'ère numérique, **les organisations ne gèrent toujours pas leurs actifs informationnels avec le même sérieux que leurs actifs financiers**, **physiques et humains**. Ils en identifient trois raisons :

1. Attribuer une valeur aux ressources informationnelles n'est pas aussi simple que cela en a l'air, car **sa valeur varie selon l'utilité** que celles-ci ont pour l'utilisateur. Autrement dit **il faut objectiver quelque chose de subjectif**.

2. En fin de compte, **la façon dont on valorise** les actifs informationnels **dépend** d'une part **du type** d'actif et d'autre part **de la façon dont il est utilisé**. Autrement dit, **on ne peut et ne doit pas gérer de la même façon les informations structurées, semi-structurées et non structurées**.

3. Le mot *infonomics* a un potentiel en tant que terme générique pour cette discipline, mais est encore **largement mal compris dans la communauté des utilisateurs**. Autrement dit, **la discipline doit encore trouver un vocabulaire qui parle aux décideurs**. Car même « gouvernance de l'information », terme pourtant destiné à élever la problématique au niveau stratégique, est souvent identifié avec la simple gouvernance documentaire, et **l'*infonomics* confondu avec le *records management***.

Les membres du congrès estiment que la solution doit venir de la **profession comptable, qui serait capable d'imposer la question** de l'évaluation des actifs informationnels. Toutefois, ils sont contraints de reconnaître **qu'actuellement ni l'information, ni les compétences en gestion de l'information n'apparaissent jamais au bilan**. Pire, parmi 48 cadres supérieurs interrogés seul un tiers d'entre eux peut imaginer que cela arrivera d'ici cinq ans…

Réflexions conclusives : données, documents ou connaissance ?

Ce bref survol de la littérature a permis de comprendre la nécessité d'évaluer l'actif informationnel. Il nous a également permis de saisir la difficulté de cette opération qui se heurte à la fois à l'absence d'une vision commune et à l'impossible dialogue entre économistes, archivistes, dirigeants d'entreprise et comptables. Mais pour conclure ce dossier, reposons-nous la question : en fin de compte, qu'est-ce qu'un actif informationnel ? Parlons-nous de données, de documents ou de la connaissance ? Parlons-nous d'outils informatiques qui permettent de les gérer ? Nous avons retenu cinq éléments fondamentaux qui constituent **notre définition personnelle de l'actif informationnel** :

1. Un actif informationnel peut être constitué d'éléments qui sont reliés à la notion d'information et qu'on peut appeler « élément informationnel » : données, documents, connaissance, savoir-faire.

2. Tous les éléments informationnels d'une entreprise ne constituent pas d'actifs informationnels, mais uniquement ceux qui représentent une valeur pour celle-ci dans une perspective d'utilisation, de vente et/ou de remplacement.

3. Cette valeur peut être considérée sous plusieurs aspects : coût/bénéfice, obligations légales, sécurité, etc.

4. Une entreprise peut posséder plusieurs types d'actifs informationnels gérés de diverses manières et représentant des valeurs différentes. La catégorisation des actifs informationnels peut être un outil intéressant pour déterminer et gérer les priorités institutionnelles, pourvu qu'elle puisse s'appuyer sur une échelle de valeur universellement acceptée dans les transactions commerciales et adaptable au domaine de l'enseignement et de l'administration publique.

5. Les outils de la technologie de l'information font partie de l'actif informationnel uniquement lorsqu'ils en constituent un support indissociable. Toutefois, plus ce support permet d'exploiter l'information, plus la valeur de l'actif augmente.

Voici pourquoi : **pour pouvoir contrôler quelque chose il faut commencer par le définir**. Cependant si l'information a certainement une valeur intrinsèque, c'est tout de même **sa pertinence, son utilité et son utilisabilité** pour les objectifs spécifiques à l'organisme **qui en font une valeur stratégique** pour celui-ci. **Ce n'est donc pas le même type d'information qui doit être traité partout comme *assets***. Si pour certains types d'institutions ce sont plutôt les données sur les clients, pour d'autres ce sont les brevets et les processus (d'acquisition, de stockage, de fabrication, etc.), et pour d'autres encore le savoir-faire des employés. **Chaque organisme doit donc définir en priorité elle-même ce qui a de la valeur pour elle**, ce qu'il entend inclure dans ses actifs informationnels.

Toutefois, il ne faut pas oublier que **l'information – comme tout actif – peut posséder plusieurs types de valeurs**, parmi lesquelles les trois les plus importantes sont celle de **l'échange**, celle de **l'usage** et celle du **remplacement**. **L'information inutilisée** – par manque d'organisation, de savoir-faire, d'outils, de capital ou simplement d'occasion – **n'est pas pour autant forcément sans valeur** : il peut s'agir d'**un actif immobilisé inoccupé**, comme un terrain en friche ou un immeuble vide. Bien que ce genre d'actif coûte en général plus à l'organisme qu'il ne rapporte, aucun ne l'omettrait de l'inclure dans son bilan. Pourquoi l'information ferait-elle exception ? **Ce n'est pas parce qu'elle n'est pas exploitée qu'elle n'est pas exploitable : à défaut d'une valeur d'usage, elle peut représenter une valeur d'échange** (et augmenter également la valeur marchande de l'organisme qui le possède), ou du moins une valeur de remplacement. **Appuyé sur une échelle de valeur universellement acceptée la catégorisation des actifs informationnels (CAI) peut jouer un rôle fondamental** pour identifier ce genre d'information. **Or pour le développement d'une telle échelle il est absolument indispensable d'établir une norme internationale dont la définition soit suffisamment large pour y inclure toutes les valeurs et tous les aspects qui peuvent faire des éléments informationnels un actif informationnel**.

Valeur probante du document électronique : nature et exigences (Lise Lefort)

Introduction

L'environnement numérique entraîne une dématérialisation des processus et un essor considérable du document électronique, défini comme « représentation numérique d'un contenu stocké et géré électroniquement » (ISO 14641-1:2012). Ce type de document peut être créé numériquement - il provient par exemple d'une GED, d'une messagerie, d'outils de bureautique, d'applications métier ou encore de bases de données - ou converti à partir d'un document analogique (numérisation).

En matière probatoire, c'est à dire pour l'établissement de la vérité d'un fait, la rupture entre l'information et son support matériel est, à première vue, problématique. En effet, la qualité d'une preuve découle en principe de « l'indissociabilité entre un support matériel durable et l'information qu'il porte » (Yante, 2004, dans Barreau, 2011). Se pose alors la question de savoir si le document numérique peut inspirer la même confiance que le document papier, dans quelle mesure et à quelles conditions.

Une approche pluridisciplinaire, partant de l'archivistique et du *records management* pour s'étendre aux domaines du droit (suisse), de l'informatique (sécurité de l'information) et du management du risque, doit permettre d'apporter à cette étude un éclaircissement supplémentaire.

Après un examen du document électronique comme élément de preuve (2), une distinction est opérée entre toutes les exigences probatoires, selon qu'elles sont générales à toutes les disciplines (3), particulières à certains domaines (4) ou complémentaires et spécifiques (5).

Le document électronique constitutif d'une preuve

Comme son homologue papier, et à certaines conditions, le document électronique est admissible en tant que preuve légale (2.1). Hors du périmètre strictement juridique, il peut également constituer la preuve d'une opération (2.2).

Preuve légale

Moyens de preuve admissibles en procédure civile, les titres sont définis comme « des documents, tels les écrits, les dessins, les plans, les photographies, les films, les enregistrements sonores, les fichiers électroniques et les données analogues propres à prouver des faits pertinents » (art. 177 CPC). La valeur probante du document électronique est donc expressément reconnue par le législateur suisse.

De la même façon, les actes de procédure devant les tribunaux civils ou pénaux peuvent prendre une forme électronique dès lors qu'ils sont dotés d'une signature électronique au sens de la loi du 18 mars 2016 (art. 130 CPC, art. 110 du CPP). L'article 2 de cette loi définit la signature électronique comme « un ensemble de données électroniques qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité ».

En ce qui concerne la forme des contrats, le Code des obligations assimile la « signature électronique qualifiée avec horodatage qualifié » à la signature manuscrite (art. 14B 2bis CO). La valeur légale du document électronique ressort également de l'Ordonnance concernant la tenue

et la conservation des livres de comptes du 24 avril 2002 (Olico), dès lors que plusieurs conditions sont remplies (authenticité, fiabilité et intégrité notamment).

Preuve d'une opération

La norme ISO 30300:2011 définit la preuve comme "information ou document prouvant un opération". La précision suivante est apportée : "preuve d'une opération dont il peut être démontré qu'elle a été créée dans le cadre normal de la conduite de l'activité de l'organisme et qu'elle est intacte et complète. Ne se limite pas au sens légal du terme." Dans cette optique, la valeur probante d'un document, papier ou électronique, dépasse le cadre strictement juridique.

La norme ISO 15489-1:2016 souligne, quant à elle, que « les documents d'activité [définis comme "informations créées, reçues et préservées comme preuve et actif par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite des opérations liées à son activité"] sont de plus en plus créés et conservés dans des environnements numériques ». Document électronique et document d'activité sont donc étroitement liés, le premier pouvant être assimilé au second pour l'étude de ses exigences probatoires.

Authenticité et intégrité : deux exigences générales

L'étude pluridisciplinaire de la valeur probante du document électronique fait apparaître l'authenticité (3.1) et l'intégrité (3.2) comme des dimensions centrales, unanimement exigées.

Authenticité

Le droit confère à l'authenticité une importance toute particulière à travers « l'acte en la forme authentique ». Document établi par un officier public compétent, rédigé selon les formalités exigées par la loi, ce type d'acte fait foi des faits qu'il atteste tant qu'il n'a pas été établi que son contenu est inexact (art. 179 CPC); il peut être dressé sur support électronique (art. 55, al.1, tit. fin. CC). Au-delà de l'acte authentique proprement dit, l'authenticité est un « critère de la preuve juridiquement admissible » (Wright, 1998 cité dans Park, 2004), rattaché à la vérité d'un fait et directement en rapport avec ce fait. Toutefois, il a pu être souligné que « le vrai problème des documents numériques n'est pas l'admissibilité mais le poids » (Duranti, 1997 citée dans Barreau, 2011). La confiance dans le document électronique peut notamment découler de l'apposition d'une signature électronique, servant à vérifier son authenticité.

L'authenticité du document électronique se trouve également au coeur de l'archivistique et du *records management*. Elle a notamment fait l'objet d'une étude approfondie menée par le groupe InterPARES (*International Research on Permanent Authentic Records in Electronic System*). Classiquement, un document authentique est ce qu'il prétend être, sans altération ni corruption, un document conservant son identité et son intégrité.

La norme ISO 15489-1:2016 fait de l'authenticité la première des caractéristiques d'un document d'activité à valeur probante. Elle définit le document d'activité authentique comme "un document dont on peut prouver qu'il est bien ce qu'il prétend être, qu'il a été créé ou envoyé par l'acteur qui prétend l'avoir créé ou envoyé et qu'il a été créé ou envoyé au moment prétendu". Le créateur doit être autorisé et identifié comme tel.

En management du risque, le défaut de contrôle de l'authenticité représente un risque à évaluer (ISO 30301:2011) ; la perte d'authenticité des documents d'activité constitue à la fois la réalisation d'un risque (ISO 18128:2014) et un critère à prendre en compte pour la valorisation des actifs (ISO 27005:2011).

En informatique enfin, la notion d'authenticité sous-tend les différentes techniques mises en œuvre en sécurité de l'information ; elle est cependant largement concurrencée par le terme d'authentification[3], renvoyant lui-aussi aux critères d'identité (du créateur) et d'intégrité (du message).

Intégrité

Le domaine informatique, plus précisément celui de la sécurité de l'information, attache une grande importance à l'exigence d'intégrité. Il s'agit de la propriété permettant de vérifier qu'une donnée n'a pas été modifiée, intentionnellement ou non, par une entité tierce. Pour s'assurer de l'intégrité d'un document électronique, et donc de sa valeur probante, diverses méthodes de cryptographie peuvent être employées, souvent conjointement : horodatage (*timestamp*), sommes de contrôle (*checksum*) et fonction de hachage[4], code d'authentification de message (*MAC*). Elles concourent à la création de signatures numériques.

L'archivistique est également très attachée à l'intégrité du document électronique, vue comme la "stabilité de son contenu à travers le temps" (Frey, 2009, cité dans Barreau, 2011). Figurant parmi les quatre caractéristiques du document d'activité à valeur probante, l'intégrité renvoie au "caractère complet et non altéré de son état" (ISO 15489-1:2016) "prouvant que celui-ci n'a subi aucun ajout, aucun retrait ni aucune modification, accidentelle ou intentionnelle, depuis sa validation" (UNIRIS, 2014). Le document électronique doit donc être "protégé contre les modifications non autorisées" (ISO 30300:2011, ISO 30301:2011), surtout si le média d'archivage n'est pas de type WORM[5] (ISO 14641-1:2012). Cela implique notamment l'adjonction de métadonnées de préservation (empreinte numérique) ainsi qu'un stockage surveillé de type coffre-fort électronique (garantissant également la pérennité par des contrôles périodiques, la confidentialité par le contrôle des accès et le cryptage, ainsi que la traçabilité).

Comme en matière d'authenticité, le management du risque considère une atteinte potentielle à l'intégrité comme un risque, et les frais générés par une perte d'intégrité comme un critère de valorisation des actifs.

Quant au droit, moins attaché ici à la terminologie, il appréhende la question de l'intégrité sous l'angle technique, à travers la signature électronique avancée (au sens de la loi du 18 mars 2016), les certificats numériques, les cachets électroniques ou l'horodatage, visant à détecter toute modification du document et à assurer la fiabilité d'échanges.

Fiabilité et exploitabilité : deux exigences particulières

Les notions de fiabilité (4.1) et d'exploitabilité (4.2) du document électronique apparaissent essentielles en archivistique comme en management du risque, mais marginales voire ignorées dans les autres domaines.

[3] « Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel » (Office québécois de la langue française, 2013)

[4] « Fonction qui, à partir d'une donnée arbitraire, calcule une empreinte servant à condenser et identifier rapidement la donnée initiale » (Nitulescu, 2016). Elle rend plus aisée la détection d'éventuelles modifications.

[5] Write Once Read Many : Support permettant l'écriture de données mais pas leur effacement.

Fiabilité

Le droit et l'informatique n'emploient guère ou pas le terme de fiabilité, se concentrant sur les exigences d'intégrité ou de traçabilité.

En revanche, l'archivistique et le *records management* font de la fiabilité du document probant une de ses dimensions essentielles, directement liée à l'authenticité. Pour le groupe InterPARES, « le concept de fiabilité (authenticité diplomatique) renvoie à l'autorité et la qualité du document d'archives d'être digne de confiance en tant que représentation des faits auxquels il se rapporte » (Banat-Berger, Borgeaud, Nougaret, 2016). Il implique une proximité entre l'observateur et les faits enregistrés. La norme ISO 15489-1:2016 indique ainsi : « un document d'activité fiable est un document dont le contenu peut être considéré comme la représentation complète et exacte des opérations, activités ou faits qu'il atteste, sur lequel on peut s'appuyer lors d'opérations ou d'activités ultérieures. Il convient que les documents d'activité soient créés au moment de l'événement auquel ils se rapportent ou immédiatement à sa suite, par des personnes qui ont une connaissance directe des faits ou par des systèmes utilisés systématiquement pour réaliser l'opération ». La fiabilité est donc liée à la qualité des données contenues dans le document, alors que l'authenticité est liée « à la transmission et à la maintenance du document » (Banat-Berger, Borgeaud, Nougaret, 2016).

En matière de gestion des risques, la fiabilité est traitée sur le même plan que l'intégrité et l'authenticité. Elle est rattachée à la notion d'utilisabilité qui implique notamment de « maintenir la fiabilité et l'authenticité des documents d'activité dans le temps » (ISO 18128:2014).

Exploitabilité

La notion d'exploitabilité du document électronique à valeur probante ne ressort ni en droit, ni en informatique.

En revanche, elle figure en bonne place dans la norme ISO 15489-1:2016: « un document d'activité exploitable est un document qui peut être localisé, récupéré, communiqué et interprété dans une période de temps jugée raisonnable par les parties prenantes », y compris en dehors de son contexte de création. Il doit être relié au processus ou à l'opération à l'origine de sa création, le tout étant documenté de manière rigoureuse. La norme ISO 30300:2011 préfère au terme « exploitable », le terme « utilisable », tout en en livrant une définition similaire. La norme ISO 30301:2011 recommande que « les moyens employés pour conserver/stocker les documents d'activité [satisfassent] aux normes pertinentes relatives au support et à la technologie employés afin de s'assurer qu'ils demeurent exploitables aussi longtemps que nécessaire ».

Le management du risque s'intéresse quant à lui aux risques associés au défaut de contrôle de l'exploitabilité des documents d'activité dans le cadre des processus opérationnels de l'organisme (ISO 30301:2011).

Traçabilité, imputabilité et non répudiation : des exigences complémentaires

Plusieurs exigences connexes viennent compléter, dans certains domaines, les contours du document électronique à valeur probante. Il s'agit de la traçabilité (5.1), de l'imputabilité et de la non répudiation (5.2).

Traçabilité

En *records management,* la traçabilité est définie comme « la faculté de pouvoir présenter l'historique des traitements opérés sur un document durant tout le cycle de vie » (UNIRIS, 2014) ; elle est incontournable en matière d'archivage électronique à valeur probante. La norme ISO 15489-1:2016 en livre la définition suivante : « fait de créer, d'enregistrer et de préserver les données relatives aux mouvements et à l'utilisation des documents d'activité ». Cette notion est en étroite relation avec l'exigence d'intégrité puisque, dans cette perspective, il est recommandé que « toute annotation, tout ajout ou suppression autorisée apporté à un document d'activité soit explicitement indiqué et traçable ».

En matière de gestion du risque, l'idée de traçabilité est également présente, même sans que le terme ne figure. Ainsi, la « préservation dans le temps des enregistrements des personnes ayant consulté ou modifié les documents » est un risque identifié, tout comme la « maintenance de l'utilisabilité », impliquant la conservation de « l'historique des événements liés aux documents d'activité, pour étayer la pertinence des documents d'activité » (ISO 18128:2014).

En droit et en sécurité de l'information, la traçabilité est inhérente aux moyens techniques mis en œuvre pour assurer l'authenticité et l'intégrité du document (signature électronique, certificats, horodatage, etc.).

Imputabilité et non-répudiation

Les concepts d'imputabilité et de non-répudiation sont liés à celui de traçabilité. Leur utilisation semble néanmoins limitée au domaine de la sécurité de l'information et de la gestion des risques afférente.

L'imputabilité revient à attribuer à une personne l'accès à un objet ou une opération donnée afin de rendre traçable toute violation d'une règle de sécurité. De fait, chaque action donne lieu automatiquement à un enregistrement. L'imputabilité, aussi appelée « gestion de la preuve », rejoint la question de l'intégrité du document électronique.

La non-répudiation constitue une dimension de l'authentification, au même titre que la validation de l'identité de l'auteur et la protection de l'intégrité du message. Elle vise à empêcher une personne engagée dans une communication informatique de nier avoir reçu ou émis un message. Reposant sur des techniques de cryptographie asymétrique, la signature numérique apposée sur un document électronique permet de garantir la non-répudiation de l'origine.

Conclusion

La valeur probante (entendue au sens large) du document électronique est au cœur d'un faisceau d'exigences plus ou moins imbriquées et complémentaires. L'approche pluridisciplinaire de la question souligne le caractère incontournable des exigences d'authenticité et d'intégrité, sans toutefois amoindrir l'importance des autres dimensions.

Si ces exigences sont, pour la plupart, applicables au document papier, elles s'appuient, en matière numérique, sur des moyens techniques avancés (cryptographie, coffre-fort électronique) destinés à garantir la confiance dans le document électronique, y compris sur la durée.

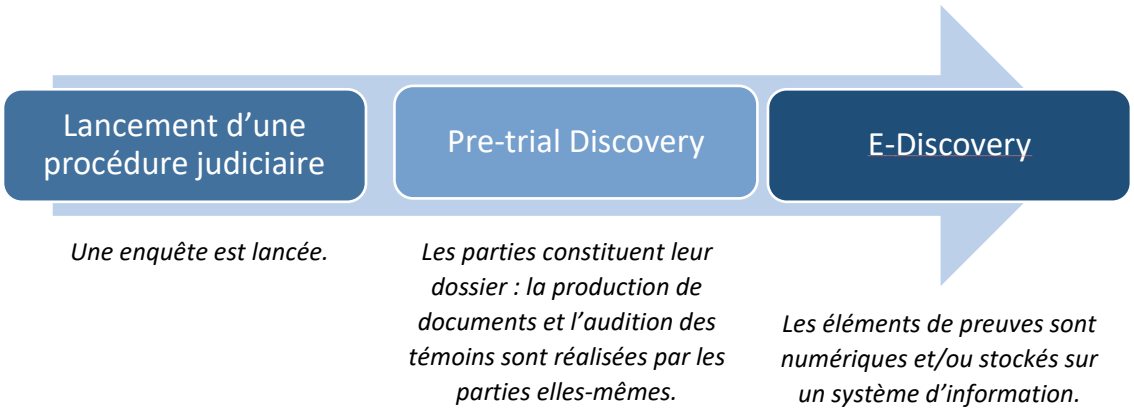
Le traitement des données personnelles dans les procédures d'E-Discovery : présentation des contextes suisse et européen (Sandrine Anderfuhren)

Définition et contexte de l'E-Discovery

L'Electronic Discovery fait partie d'un ensemble de mesures juridiques appelées Discovery : indispensable à la recherche de preuve, cette procédure constitue la phase préalable au procès civil ou commercial et s'avère quasi-systématique dans les pays du Common Law, notamment aux Etats-Unis.

Le but d'une procédure de Discovery est d'obliger chacune des parties à livrer à la partie adverse l'ensemble des éléments de preuve dont elle dispose en cas de litige pour, d'une part, réduire les temps et coûts du procès et, d'autre part, garantir une certaine égalité et justice entre elles. Ce processus se déroule de la manière suivante :

Figure 1: Processus de Discovery



Dans le cas de l'E-Discovery, la procédure se concentre principalement sur les éléments de preuve stockés sur des systèmes d'information[6]. Selon Mathias (2016, p.3) :

> *« La nature des données électroniques est particulièrement intéressante dans le cadre d'un procès. Ces données peuvent en effet être recherchées beaucoup plus facilement que les informations se trouvant sur un format papier. Cela d'autant plus qu'il est plus complexe de détruire ces données sans laisser de traces. ».*

La règle d'E-Discovery est récente : Burton et Proust expliquent qu'en 2006 une réforme des règles de procédures civiles aux Etats-Unis oblige désormais les entreprises américaines à « conserver et produire tous les documents et informations conservés sous forme électronique » (Burton et Proust 2009, p. 80). Cette exigence, bien que contraignante, permet aux entreprises d'anticiper tous problèmes judiciaires et protège les intérêts des producteurs d'information : pour Exterro (2016, p.3) « Electronic discovery (…) preserve, collect, review and exchange information in

[6] Comme, à titre d'exemple, les ordinateurs, les serveurs web ou encore les réseaux d'entreprise.

electronic formats for the purpose of using it as evidence in the case »[7]. En effet, en systématisant le traitement des données dans un but juridique, on délimite beaucoup plus facilement l'objet du conflit et on évite ainsi de devoir transmettre des informations qui ne seraient pas indispensables lors d'une enquête.

Ce dernier point est le principal challenge de l'E-Discovery : pour sélectionner les données nécessaires, il faut avoir une bonne capacité d'évaluation de l'information. Cette analyse va influencer les autres étapes du Discovery ainsi que l'issue du procès ; pour aider les entreprises à y voir plus clair, EDRM a mis au point en 2005 un modèle de référence divisé en 9 étapes, dont une partie concerne la gouvernance de l'information et la seconde la gestion des données. Ce modèle sert essentiellement de cadre et non de *workflow* à suivre à la lettre.

En outre, appliquer des procédures d'E-Discovery implique une sensibilisation à la préservation des données : qu'elles soient physiques ou numériques, la conservation des informations doit être maitrisée pour répondre aux besoins de l'E-Discovery.

Pour résumer, l'E-Discovery est une règle indispensable à suivre en cas de procédure judiciaire : elle permet d'anticiper tout risque juridique, de protéger les intérêts des parties concernées et de délimiter l'objet du litige. Elle requiert une évaluation de l'information et une bonne maitrise de sa préservation.

Définition de la notion de donnée personnelle et sa place dans le processus d'E-Discovery

Dans le cadre de ce travail, nous nous intéressons exclusivement au traitement des données personnelles : à travers notre analyse, nous allons à présent tenter de comprendre comment ces dernières sont considérées dans les contextes suisse et européen, et quel impact cela peut avoir au niveau international.

La donnée personnelle se définit comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (article 2 de la loi informatique et liberté). » (Wikipédia, 2017). Il est important de relever qu'une donnée dite personnelle n'est pas automatiquement une donnée sensible : cette dernière fait apparaitre les origines raciales ou ethniques, les opinions politiques ou religieuses, ou encore des informations sur la santé de la personne concernée. Ici, nous ne traiterons pas de ce type de données.

Burton et Gufflet (2012, p.116) présentent le traitement des données personnelles comme :

> *« Toutes opérations (…) appliquées à des données à caractères personnelles telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement et la destruction ».*

[7] L'Electronic Discovery (…) préserve, collecte, révise et échange l'information existant en formats électroniques, dans le but de l'utiliser comme preuve lors d'une procédure juridique. (trad. par Silas Krug)

Comme indiqué au chapitre précédent, les procédures de Discovery concernent l'exploitation de toutes informations utiles et exploitables lors d'un procès ; les informations personnelles en font partie. A titre d'exemple, il est possible d'exiger l'ordinateur d'un ou plusieurs employés, ou encore leur disque dur.

Aux Etats-Unis, on estime que « tous les documents et fichiers des salariés sont la propriété de l'entreprise et sont donc accessibles à l'employeur, car ils sont considérés comme relevant de la sphère professionnelle. » (Swan, 2013) : dans son article, Burton (2009, p.82) désigne ces documents comme des *business documents*. En outre, la Discovery étant systématique, la gestion de ces informations est le plus souvent automatisée, étant donné que tout ce qui concerne les données numériques doit répondre à des exigences légales en matière de conservation et de traitement.

En Suisse et dans l'Union Européenne (UE), l'approche est toute autre : en effet, il y a une distinction entre les documents d'entreprise et ceux produits par les employés. Contrairement aux Etats-Unis, la Suisse et l'UE sont dotées de lois et règlements qui régissent la protection des données, dont l'utilisation des informations dans le cadre d'une procédure judiciaire. Dans ce contexte, le traitement des données personnelles doit répondre à deux principes qui sont

- La légitimité, qui exige notamment le consentement de la personne concernée.
- La proportionnalité, obligeant à avoir un véritable contrôle et une analyse précise des informations pour définir si le transfert des données personnelles est indispensable à la résolution du litige (Matthias, 2016, p. 14). S'il est bien appliqué, ce principe permet de « garantir un équilibre entre les intérêts en présence et de limite l'atteinte à la vie privée en traitant le moins de données possible » (Burton et Gufflet, 2012, p.116).

On constate dès lors une incompatibilité entre la vision des Etats-Unis et celle du continent européen : dans un contexte de mondialisation toujours plus important, cette friction donne lieu à des tensions de la part des deux parties. Ces tensions donnent par exemple naissance à des lois suisses et européennes de blocages qui limitent la mise en œuvre d'une procédure de Discovery. La protection des données personnelles étant un droit fondamental en Europe et en Suisse[8], ni l'une ni l'autre ne pourrait songer à en systématiser l'échange, surtout avec un pays qui n'a aucune réglementation en la matière.

La transmission des données personnelles en Suisse et dans l'Union Européenne

Le contexte suisse

En Suisse, le transfert des données personnelles s'effectue de façon distincte selon deux destinations : la Suisse uniquement, ou d'autres pays.

La protection de ces informations est une préoccupation majeure : elle est d'ailleurs considérée comme un droit fondamental et figure à l'article 13 de la Constitution suisse[9]. Les cantons suisses ont chacun leur réglementation en matière de données personnelles. Néanmoins, leurs pratiques

[8] Il est présent dans la constitution suisse, dans la charte des droits fondamentaux et dans le Traité de fonctionnement de l'Union Européenne.

[9] « Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.2 Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent. »

sont encadrées au niveau fédéral par la « Loi sur la protection des données (LPD) » et par le Préposé fédéral à la protection des données, qui surveille l'utilisation de ces données par les organes fédéraux, les particuliers et les organisations. En plus du principe de proportionnalité qui doit être appliqué, Winkler (2011, p.111) indique que le traitement et l'exploitation de ces informations n'est autorisé que dans un but clairement indiqué lors de leur récolte. Le principe de transparence des données est donc un élément essentiel à respecter en cas de transmission de données personnelles[10].

En 2015, le Conseil Fédéral a mis en place la « Stratégie Suisse numérique », qui a pour but d'assurer une sécurité numérique aussi importante et fiable que celle du monde physique : elle poursuit l'objectif de « Transparence et Sécurité » pour le stockage des données et agit dans différents domaines tels que l'économie numérique, la cyberadministration, la cybersanté, la sécurité et la confiance.

Au niveau de ses échanges avec l'étranger, la Suisse est l'un des pays les plus sévères quant aux conditions de transfert, et plus particulièrement pour les données personnelles. Les modalités sont définies à l'article 6 de la LPD (« Communication transfrontière de données ») et par les articles 271 à 274 du Code Pénal suisse : il est indispensable que le pays exigeant des données personnelles à la Suisse assure un niveau de protection adéquat. En outre, et c'est le plus gros obstacle à franchir pour les autres états, la Suisse considère que toute exploitation d'information suisse par un pays étranger est assimilée à de l'espionnage, et se trouve par conséquent interdite et sanctionnée[11]. On peut dès lors considérer que le Code pénal fait office de blocage envers les autres états. Face à cette résistance, il est difficile d'établir des consensus acceptables dans l'échange de données personnelles internationales.

De plus, comme mentionné plus haut, le principe de transparence doit être appliqué à toute procédure visant le traitement de ces informations : l'E-Discovery ne déroge pas à la règle. Ainsi, la Suisse applique un filtre quasi systématique à toute information sortant du pays. En raison de son emprise totale sur les données et de ses lois très contraignantes, cet Etat est l'un des plus redoutés mais est aussi considéré comme le lieu le plus sécurisé au monde pour la protection des données (Gautschi, Gianluigi, Tucci, 2016, pp.18-26).

Néanmoins, les procédures judiciaires internationales se multiplient et la Suisse n'est pas épargnée. Malgré cette constatation, son absence d'efforts et de consensus de sa part devient véritablement problématique. Les Etats-Unis ont donc exigé plus de coopération au travers de mesures et règlements clairs, derrière lesquels la Suisse ne pourra pas se retrancher : le premier est le « Swiss Bank Programm », lancé en 2013. Sous forme d'ultimatum, cet accord force la Suisse à favoriser l'échange des données financières avec les Etats-Unis dans les procédures pénales liées aux impôts (Burrus, 2017, p. 4). En 2017, Le « Swiss-US Privacy Shield » est instauré : il régit la transmission des données personnelles de la Suisse vers les Etats-Unis. Pour le préposé à la protection des données (2017) :

> *« Il garantit aux personnes concernées en Suisse une bien meilleure protection, en particulier dans le domaine commercial, notamment grâce à un renforcement de l'application des principes de protection des données par*

[10] Cet élément est énoncé à l'art. 8 al. 2 let. B de la LPD : « 2. Le maître du fichier doit lui communiquer : (…) b. Le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données. »

[11] Les peines privatives de liberté peuvent aller jusqu'à plus de 3 ans (art. 273 2. Code Pénal Suisse)

> *les entreprises participantes et par une amélioration de la gestion et de la surveillance par les autorités américaines. (…) Grâce au Privacy Shield, les données personnelles exportées de Suisse vers les États-Unis bénéficieront des mêmes normes que celles provenant de l'Union européenne, un point fondamental pour la sécurité juridique des échanges économiques et en particulier aussi pour le libre échange des données entre la Suisse et l'UE (précisément dans le domaine commercial). »*

La Suisse a une position ambivalente en cas de procédure d'E-Discovery : elle est peu conciliante et protège au maximum ses informations, mais cette méfiance et ce niveau de protection en fait un pays sûr et fiable, qui attire la confiance du monde entier. Elle pourrait tirer parti de cette qualité en mettant en place une réflexion autour des processus de Discovery qui pourrait à terme conduire la Suisse à avoir des politiques et procédures précises et intégrant ses exigences au niveau de la protection des données. Elle pourrait dès lors servir d'exemple et assurer sa réputation de place forte dans le domaine de la gestion des données.

Le contexte européen

Comme pour la Suisse, les échanges de données dans le contexte européen se font à deux niveaux : l'interne, qui concerne les états membres de l'UE, et l'externe, qui régule les échanges de données personnelles avec les autres pays.

Les échanges de données personnelles au sein de l'UE sont principalement encadrés par la « Directive sur la protection des données 95/46/Ce » : cette règlementation permet d'harmoniser les pratiques des pays membres, de définir ce qu'est une donnée personnelle et le traitement qui lui convient, ainsi que de mettre en avant les deux principes essentiels à respecter dans le contexte de l'échange, c'est-à-dire la proportionnalité et la légitimité. Bien qu'il existe un règlement commun, chaque état membre est responsable du traitement des données personnelles sur son territoire : cet aspect est organisé dans les articles 16 du Traité de fonctionnement de l'Union Européenne et 39 du traité de l'UE.

Comme précisé dans le chapitre précédent, la protection des données personnelles fait partie des libertés fondamentales de l'UE sur la vie privée : on la retrouve dans l'article 8 de la charte des droits fondamentaux[12] et à l'article 16 du traité de fonctionnement de l'UE, qui indique quel rôle joue le parlement européen dans l'application des règles relatives à la protection des données personnelles[13].

Lors des procédures d'E-Discovery, le traitement de la correspondance électronique privée doit également répondre au « droit du secret » car on considère que toute communication privée est protégée par le secret de correspondance et de communication.

---

[12] « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

[13] « 2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes. »

L'Union européenne, faisant face à une demande de réglementation toujours plus grande en matière d'E-Discovery, elle a mis en place le « Groupe de Travail de l'article 29 » ; constitué pour répondre aux besoins de l'économie numérique, il traite notamment des procédures en cas de litiges civils ou commerciaux, et propose des recommandations fondées sur l'importance du consentement, le respect des obligations légales et la légitimité des intérêts de chaque partie.

Tout comme la Suisse, l'Union Européenne refuse d'établir une base pour le transfert des données personnelles avec les autres pays non-membres, sauf si le niveau de protection des données est adéquat selon ses normes. Ainsi que nous l'avons constaté, l'échange de ce type de données est problématique. Afin d'avoir des dispositions légales internationales protectrices, la Convention de La Haye de 1970 a eu pour objectif d'organiser la communication des preuves entre ses états membres en cas de procédures judiciaires nationales : « L'autorité judiciaire d'un État peut demander, par commission rogatoire, à l'autorité compétente d'un autre État de faire, notamment, tout acte d'instruction. L'État requis examinera l'existence avérée d'un lien précis et direct avec l'objet du litige, et les documents sollicités devront être limitativement énumérés dans la commission rogatoire. » (Fondation Prometheus, 2011). Toutefois, cette convention a un point faible, exploité par les Etats-Unis. En effet, l'article 23 stipule que les pays membres ne sont pas obligés d'exécuter la procédure dite de « pre-trial discovery of document ». Dès lors, il était difficile de trouver un compromis entre l'UE (souhaitant avoir une règlementation en accord avec sa politique de protection des données) et les Etats-Unis (considérant les données personnelles comme inexistantes dans le cadre d'une entreprise) : différents pays de l'UE ont mis en place des lois de blocage pour limiter au maximum la marge de manœuvre des Etats-Unis en cas de procédure judiciaire[14].

Dans le but de trouver un terrain d'entente entre l'UE et les Etats-Unis, deux réglementations ont été élaborées :

- La « Data Umbrella Agreement » : il s'agit d'un cadre global assurant un haut niveau de protection des données et fournissant une garantie légale pour le transfert de données ainsi qu'une égalité de traitement entre les adhérents.
- L'« EU-US Privacy Shield » : elle règlemente la protection des données personnelles depuis un état membre vers les USA. Pour en faire partie, les entreprises doivent apparaître dans une liste certifiée. Cette initiative remplace le « Safe Harbor » auparavant en vigueur.

[14] Comme la France avec la loi n°80-538 du 16 juillet 1980 relative à la communication de documents et renseignements d'ordre économique, commercial ou techniques à des personnes physiques ou morales étrangères. (Mathias, 2016)

Comparaison

Tableau 1: récapitulatif des règlements et normes suisses et européens

	Suisse	Union Européenne
Intérieur	Loi fédérale sur la protection des données (LPD) (MAJ en cours) Préposé fédéral à la protection des données Constitution fédérale de la confédération suisse Loir sur le travail (LTr) Initiative "Suisse numérique"	Directive sur la protection des données 95/46/Ce (MAJ 2016) Groupe de travail de l'article 29 Charte des droits fondamentaux de l'UE Traité sur le fonctionnement de l'UE 2012/C 326/01
Extérieur	Swiss Bank Programm Swiss-US Privacy Shield Code pénal suisse	Data Umbrella Agreement EU-US Privacy Shield
En commun	Convention de la Haye 1970 Avoir un niveau de protection des données suffisant Principe de proportionnalité Liberté fondamentale Loi de blocage Pas de partage avec les autres pays	

L'Union Européenne ainsi que la Suisse partagent des points communs en termes de transferts des données personnelles : tout d'abord, la protection de ces informations, érigée en liberté fondamentale, est encadrée par des lois spécifiques. En outre, tous deux refusent le transfert automatique des données personnelles aux autres pays, ou uniquement si ces derniers ont un niveau de protection suffisant, répondant aux normes définies. Dans ce dernier cas, le principe de proportionnalité doit alors impérativement être respecté. Face à des pays ne correspondant pas à ces critères ou n'ayant pas la même vision des données personnelles, des lois de blocage ont été mises en place pour assurer une certaine protection des intérêts des individus et pour réduire au possible le pouvoir d'action de ces états. Enfin, la Suisse et l'UE ont signé la « Convention de la Haye » de 1970.

On note toutefois une approche différente entre ces deux entités. En effet, avec la constitution du « Groupe de Travail de l'article 29 », l'UE manifeste une véritable prise de conscience autour de l'E-Discovery et mène une importante réflexion autour des politiques et procédures qui l'incluraient dans les pratiques professionnelles.

La Suisse reste excessivement protectrice. Bien qu'elle mette l'accent sur l'importance des consensus, elle-même semble peu encline à faire le moindre pas dans ce sens : l'ultimatum lancé au travers du « Swiss Bank Programm » en est un bon exemple. Néanmoins, si elle veut continuer à évoluer dans un contexte de plus en plus mondialisé, la Suisse se doit de faire des efforts en matière d'E-Discovery. Un premier pas en avant est la mise à jour de la LPD, dont l'objectif est d'être en adéquation avec la réforme du règlement européen sur la protection des données personnelles et ratifier la nouvelle convention STE 108 du Conseil de l'Europe concernant l'espace Schengen[15]. La « Tribune de Genève » et le « 24 heures » indiquent également qu'en novembre 2017 le Conseil des Etats a donné son feu vert pour l'échange automatique des informations fiscales avec certains pays… à certaines conditions. Même si cet exemple ne touche pas forcément les données personnelles, il démontre que la Suisse avance en faveur d'une meilleure collaboration avec les autres pays.

[15] DUBOIS, Camille, 2015.Révision de la loi fédérale sur la protection des données : mettre l'accent sur la transparence et le contrôle. *La vie économique* [en ligne]. 26 octobre 2015. [Consulté le 15 novembre 2017]. Disponible à l'adresse : http://dievolkswirtschaft.ch/fr/2015/10/dubois-11-2015-franz/

Conséquences de la gestion suisse et européenne dans la transmission des données personnelles dans le processus d'E-Discovery

À l'heure actuelle, où l'économie se mondialise, les procédures d'E-Discovery ont besoin de se concorder pour permettre une collaboration égale et juste entre Etats. Cependant, comme nous l'avons explicité dans les chapitres précédents, il semble difficile de trouver des compromis, notamment dans le respect des exigences légales de chaque partie.

Burton et Gufflet (2012, p.130) estiment que « le droit reste peu harmonisé et les multinationales se retrouvent fréquemment dans une impasse juridique ».

De la part de l'UE et de la Suisse, où le traitement des données personnelles est un droit fondamental, on recherche surtout la garantie que chaque partie prenante puisse assurer la sécurité et la bonne utilisation de ces informations, dans un souci de protection des intérêts et d'égalité de traitement de chacun. Néanmoins, alors que l'E-Discovery a des exigences en matière de traitement et de conservation des données, les procédures de l'UE et de la Suisse en la matière sont assez opaques : la plupart du temps, la tendance est à l'examen au cas par cas, ce qui entraîne lenteur, coût et difficulté pour les autres Etats lorsqu'ils s'affairent à répondre aux obligations suisses et européennes.

Les lois de blocage mises en place par le continent européen, même si leurs intentions sont louables, peuvent mettre en péril les intérêts de ceux qu'ils cherchent à protéger. Face aux Etats-Unis, le refus des procédures d'E-Discovery peut coûter très cher, spécifiquement au niveau des sanctions infligées : on parle d'un fort pourcentage du chiffre d'affaire ou même de l'issue du jugement, qui peut être défavorable envers la partie qui s'est opposée aux règles d'E-Discovery.

Ne pas vouloir intégrer la Discovery en général conduit immanquablement les Etat à s'isoler des autres. Ce risque étant réel, on note de la part de la Suisse et de l'UE une volonté de prendre en compte l'E-Discovery dans leurs lois – une révision de la LPD suisse, lui permettant de mieux répondre au cadre de l'UE, est d'ailleurs en cours – et de trouver des consensus. Le Swiss-US Privacy Shield et le EU-US Privacy Shield en sont de bons exemples.

Propositions de bonnes pratiques

En termes d'E-Discovery, il existe des recommandations qui peuvent être intégrées dans les pratiques, sans pour autant empiéter sur l'espace personnel de chacun.

Mettre en place une politique de gestion de l'information pour répondre aux exigences de l'E-Discovery

Dans le but d'anticiper des conflits et de retreindre au possible le champ d'une procédure de Discovery, élaborer une politique aide à délimiter pour chaque opération de conservation, d'archivage, d'analyse, de transfert et de communication la quantité et le type de données traitées. De plus, avoir une procédure interne claire et accessible permet de limiter les différences de traitement entre les services et diminuer les risques en termes de protection des données.

Collaborer

La procédure d'E-Discovery concerne tous les collaborateurs d'une entreprise : il est donc important de les sensibiliser à la question des données personnelles, pour leur permettre de gérer ce qui relève de leur sphère privée et pour les responsabiliser lors de la production de leurs informations et documents. Cette pratique se fait avec le soutien de la politique définie

préalablement : elle est un outil concret qui donne du sens aux nouvelles pratiques de gestion de l'information.

Coordonner

L'E-Discovery, tout comme la gouvernance de l'information, touche plusieurs secteurs d'une organisation, notamment les juristes, la direction et les services informatiques : coordonner ces services permet de connaitre les besoins légaux et techniques lors d'une procédure judiciaire et d'anticiper efficacement chaque demande juridique.

État de l'art des documents gouvernant les données de la recherche dans les Hautes écoles suisses (Tania Zuber Dutoit)

Introduction

Ce travail a pour but de recenser les documents traitant des données de la recherche[16] dans les hautes écoles suisses, de constater leur diversité, ainsi que d'observer leur existence. Ont été pris en compte les documents 'publics', c'est-à-dire publiés sur les sites internet des écoles. Si un document existe mais n'est disponible qu'à l'interne, il ne figurera pas dans l'état des lieux.

Méthodologie

Les sites internet des hautes écoles suisses ont été passés en revue, afin de trouver les pages, services, directives ou autres documents gouvernant les données de la recherche. Dans quelques cas, il n'était pas possible de les identifier par ce moyen ; des recherches complémentaires ont alors été faites par des requêtes dans Qwant et Google. Les documents repérés n'ont pas été annexés, mais figurent dans la bibliographie.

Situation en Suisse

Typologie des institutions

Les hautes écoles considérées sont de plusieurs types :

- 2 écoles polytechniques : Lausanne (EPFL) et Zurich (ETHZ)
- 10 universités : Bâle, Berne, Fribourg, Genève, Lausanne, Lucerne, Neuchâtel, Saint-Gall, Suisse Italienne, Zurich
- 8 hautes écoles spécialisées : Fachhochschule Nordwestschweiz (FHNW), Fachhochschule Ostschweiz (FHO), Haute école spécialisée bernoise (BFH), Haute Ecole Spécialisée de Suisse occidentale (HES-SO), Hochschule Luzern (HSLU), Kalaidos Fachhochschule Schweiz, Scuola universitaria professionale della Svizzera italiana (SUPSI), Zürcher Fachhochschulen (ZFH)

Concernant les universités : la faculté de médecine de l'Université de Lausanne a été considérée comme une institution, car elle a mis en place des services et un espace de stockage des données de manière autonome.

Concernant les HES : elles ont été étudiées dans leur globalité. Les sites des écoles les composant ont été passés en revue, mais comme rien de significatif n'a été trouvé, elles n'ont pas été retenues dans le comparatif.

Les Hautes écoles pédagogiques n'ont pas été prises en compte dans ce travail.

Typologie des documents

Aucune des institutions étudiées n'a de politique propre aux données de la recherche. Dans un travail de recherche, effectué il y a deux ans dans le cadre du master en sciences de l'information, (Fachinotti et al., 2016), certaines institutions semblaient avoir établi ou étaient en train d'établir

[16] Plus loin aussi appelées « DR »

des politiques de gouvernance des données. Soit ces documents n'ont pas été rendus publics, soit ils n'ont pas été validés par les directions, soit la question n'avait pas été comprise, comme le suggéraient les trois étudiantes qui se sont penchées sur la question à l'époque.

A défaut de politique, les données de la recherche peuvent être gouvernées par d'autres types de documents[17]. Ceux trouvés dans le cadre de ce travail sont principalement des directives sur l'intégrité de la recherche (dans huit écoles[18]), mais également le plan d'intentions d'une université, une « politique de records management et d'archivage pour une gouvernance informationnelle » et un « compliance guide ».

Lors de la recherche de ces documents, d'autres politiques concernant l'Open Access (OA) ont été trouvées. Il est frappant de constater que les politiques OA existent dans neuf institutions, alors qu'il n'y en a pas (encore) pour les données de la recherche :

Nom de la Haute école	Politique DR	Autre document DR	Politique OA	Autre document OA
EPFL	Non	Compliance Guide / Directive pour l'intégrité dans la recherche et pour une bonne pratique scientifique à l'EPFL LEX 3.3.2	Non	Compliance Guide
ETHZ	Non	Guidelines for research integrity	Oui	
Université de Bâle	Non	-	Oui	-
Université de Berne	Non	Stratégie de la bibliothèque / Regulations concerning scientific integrity	Oui	-
Université de Fribourg	Non	-	Non	-
Université de Genève	Non	Intégrité dans la recherche scientifique	Oui	Directives par facultés
Université de Lausanne	Non	Directive de la Direction 4.2. Intégrité scientifique dans le domaine de la recherche et procédure à suivre en cas de manquement à l'intégrité Plan d'intentions de l'Université de Lausanne 2017-2021 Politique de records management et d'archivage pour une gouvernance informationnelle et feuille de route	Non	
Université de Lucerne	Non	Reglement über die wissenschaftliche Integrität in der Forschung und die gute wissenschaftliche Praxis	Oui	
Université de Neuchâtel	Non	-	Non	-
Université de St-Gall	Non	Richtlinien zur Integrität wissenschaftlichen Arbeitens	Oui	OA Regulations
Université de Suisse italienne	Non	-	Non	
Université de Zurich	Non	Directive Académie Suisse des Sciences	Oui	

[17] Les documents français ont été retenus prioritairement, puis ceux en anglais et finalement en allemand
[18] D'autres écoles ont des directives sur l'intégrité, mais n'y parlent pas des données de la recherche.

FHNW	Non	-	Non	-
FHO	Non	-	Non	-
BFH	Non	-	Non	Stratégie des bibliothèques
HES-SO	Non	-	Non	Open HES-SO
Hochschule Luzern	Non	Reglement zur wissenschaftlichen Integrität und zur guten wissenschaftlichen Praxis	Oui	
Kalaidos Fachhochschule Schweiz	Non	-	Non	-
SUPSI	Non	-	Non	-
ZHAW	Non	-	Oui	

Typologie des contenus

Vu leur non-existence, le contenu des politiques gérant les données de la recherche ne seront pas analysées.

Il est cependant intéressant à relever que pour pallier à cette absence, ce sont les directives sur l'intégrité académique qui fixent les objectifs à atteindre et parfois les moyens pour y arriver. Le contenu des directives n'étant pas significativement différent entre elles, elles n'ont pas été étudiées.

Services gérant les données de la recherche dans les institutions étudiées

S'il n'y a pas de politique établie, les institutions et leurs services se préoccupent bien des données de la recherche. Ce sont souvent des partenariats entre différents services, les bibliothèques en faisant souvent partie :

Institution[19]	**Services s'occupant des DR**
EPFL	Bibliothèque et Research office
ETHZ	Bibliothèque, Digital Curation Office
Université de Bâle	RDM-Network Basel : groupe transversal, comprenant la bibliothèque, le service informatique et d'autres services de l'université
Université de Berne	Bibliothèque
Université de Fribourg	Service promotion recherche et Bibliothèque
Université de Genève	Bibliothèque et Service recherche
Université de Lausanne	Uniris - Service des ressources informationnelles et archives
Université de Lausanne - CHUV	Bibliothèque
Université de Lucerne	Bibliothèque
Université de St-Gall	Externe (FORS)
Université de Zurich	Bibliothèque et Service informatique
HES-SO	Dicastère recherche innovation

[19] Les institutions pour lesquelles rien n'a été trouvé sur leurs sites internet ne figurent pas dans le tableau par souci de confort de lecture.

Infrastructures mises en place

Quelques institutions ont mis en place une infrastructure dédiée pour leurs chercheurs, d'autres ont créé des communautés propres sur des plateformes communes, comme Zenodo.

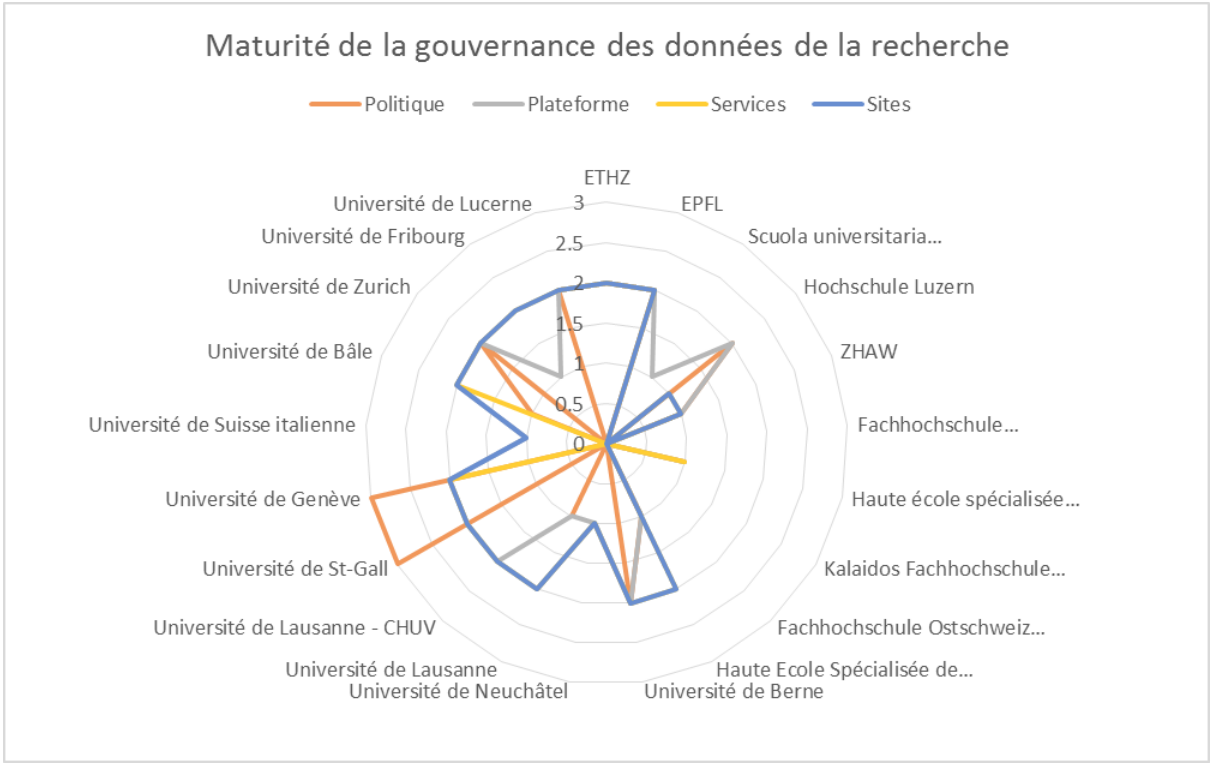
Institution	Nom de l'archive	URL de l'archive
ETHZ	ETH Data Archive	http://data-archive.ethz.ch
Université de Berne	Bern Open Repository and Information System (BORIS)	boris.unibe.ch
Université de Lausanne - CHUV	Zenodo-FBM/CHUV community (https://zenodo.org/communities/fbm_chuv), Dryad ou figshare	zenodo.org/communities/fbm_chuv
Université de Lucerne	Lory, sur Zenodo	zenodo.org/communities/lory
Université de St-Gall	DARIS (FORS)	https://forsbase.unil.ch/project/study-public-list
Hochschule Luzern	Lory, sur Zenodo	zenodo.org/communities/lory

L'EPFL et les universités de Bâle, Genève et Zurich renvoient leurs chercheurs à des plateformes existantes, soit précisément en les nommant, soit en passant par re3data[20], le registre des archives de données.

Les institutions non mentionnées, principalement les HES, n'ont pas de référence à une archive. La HES de Lucerne profite du développement commun de services et d'infrastructure avec l'Université de Lucerne

Maturité

Le niveau de maturité est donc très différent d'une institution à l'autre, voire entre types d'institutions, comme on peut le visualiser dans le graphique récapitulatif ci-dessous :



[20] Re3data.org

Autres institutions s'occupant des données de la recherche

Si les Ecoles n'ont pas (encore) de politique propre relative aux données de la recherche, les instituts de financement ou les académies ont fait le pas, et depuis longtemps pour certaines organisations.

Nom de l'institution	Politique DR	Date politique DR	Politique OA	Date politique OA
Fonds national pour la recherche scientifique	Déclaration de principe	11.05.2017	Stratégie nationale suisse sur l'Open Access	31.01.2017
Commission pour la technologie et l'innovation CTI (Innosuisse dès 2018)	-	-	-	-
Académie suisse des sciences	L'intégrité dans la recherche scientifique	01.01.2008	-	-
Académie suisse des sciences humaines et sociales	Mandat DaSCH	04.06.2016	oui	27.09.2016
Académie suisse des sciences médicales	Feuille de route «Open Access»: pour un accès libre aux résultats de la recherche scientifique	01.01.2014	Feuille de route	01.01.2014
Académie suisse des sciences naturelles6F[21]	-	-	-	-
Académie suisse des sciences techniques	Brochure pour les citoyens	2017 ?	-	-

Ces politiques par les instituts de financement ou par domaine de recherche permettent de combler, provisoirement, la non-existence de politiques par institution. Mais idéalement, tous les organismes intervenant dans la recherche devraient disposer *a minima* d'informations ou d'orientations claires sur le devenir des données de la recherche qu'elles subventionnent ou encadrent.

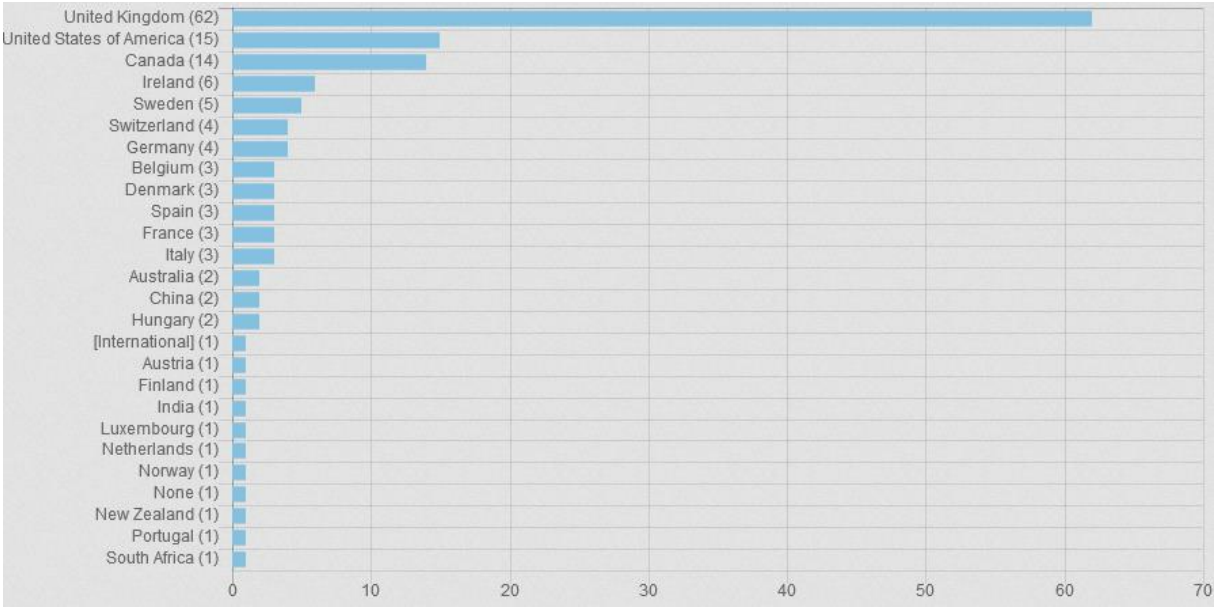
L'Académie des sciences humaines et sociales va déjà plus loin, puisqu'elle a créé un « *Data and Service Center for humanities (DaSCH)* »[22] pour gérer les données dans ces domaines.

Certains éditeurs commencent également à demander la publication des données liées aux articles. Pour rester en Suisse, l'éditeur Open Access *Frontiers* [23] demande la publication des données dans les recommandations aux auteurs.

[21] L'ASSN n'a pas de politique ou d'infos sur son site internet. Cependant, elle a organisé en janvier 2017 un congrès sur plusieurs jours "We Scientists Shape Science" à Berne
[22] http://dasch.swiss
[23] https://www.frontiersin.org

Perspectives

Il serait intéressant de comparer ce travail sur les documents gérant les données de la recherche en Suisse avec les autres pays. Le site Sherpa Juliet recense par exemple les politiques des financeurs de la recherche :



24

Pour la Suisse, les quatre mentionnés comme ayant une politique sont le CERN, l'OMS, l'Académie des sciences humaines et sociales ainsi que le FNS.

Conclusion

Aucune politique de gouvernance des données n'existe à l'heure actuelle dans les hautes écoles suisses analysées … mais tout est en développement. A l'instar des politiques sur l'Open Access[25], celles sur les données de la recherche vont fleurir ces prochains mois ou prochaines années. Le mouvement est lancé, le FNS obligeant désormais une grande partie des chercheurs suisses à établir un *Data Management Plan*.

Le projet DLCM propose un outil d'aide pour rédiger une politique institutionnelle, fournit un processus type pour l'établir, mentionne les parties prenantes et les contenus qui devraient y figurer ainsi que de nombreux exemples repris des politiques existantes internationales. Ce site en développement pourrait également accueillir les politiques au fur et à mesure de leur établissement, afin de les faire connaître plus largement que sur les sites des institutions.

Les chercheurs sont également appelés à participer : les initiatives doivent venir des instances de gouvernance institutionnelles, mais également depuis la base. Ce n'est qu'ainsi que les données seront réellement libérées.

[24] http://v2.sherpa.ac.uk/view/funder_visualisations/1.html
[25] Un aperçu est donné par le site Roarmap, qui recense les politiques Open Access du monde entier, par type d'organisation : institut de recherche, organisme de financement, …

Gouvernance des données musicales électroniques : le cas des métadonnées de Spotify (Matthieu Putallaz)

Introduction

Les données précèdent l'argent. S'il est un domaine dans lequel cela a été bien compris, c'est celui de la musique, où les données musicales sont désormais monétisées et les accès à un large public sont désormais possibles grâce au streaming. Il y a 20 ans, la musique était fragmentée, dispersée et éparpillée sur de nombreux supports et dans des formats différents. L'enjeu de l'interopérabilité était alors à son paroxysme tant les types d'appareils de lecture étaient différents.

Avec les nouvelles habitudes de consommation de la musique qu'a apportées internet, des entreprises se sont positionnées en faveur d'un accès pratiquement exhaustif, légal et à un prix abordable à la musique et dont aucune donnée n'est à stocker par l'utilisateur final. Il s'agit là d'une nouvelle approche marketing qui change la manière de consommer la musique.

Ces données musicales sont par conséquent absolument cruciales et représentent le matériau de base d'exploitation financière d'une entreprise qui propose de la musique en streaming. Toutefois, cette technique est encore jeune et souffre de faiblesses, notamment en ce qui concerne la gouvernance des données. Pour explorer plus avant cet aspect, nous nous intéresserons à la plateforme de streaming Spotify : quel est le cycle de vie des données et quels sont les risques et opportunités liés aux métadonnées musicales qui peuvent influencer l'expérience utilisateur.

La musique en streaming

L'une des principales manifestations de ce changement est la mise à disposition de services de musique en streaming, accessibles grâce à une connexion internet. « [...] le streaming audio [...] est une révolution déjà plus importante que le CD, la cassette audio ou le disque microsillon. C'est la réinvention de la musique la plus cruciale depuis [...] le gramophone et la radio [...] au début du XXe siècle. » (S.Fanen, Boulevard du stream, 2017, p.208)

Le streaming (de stream en anglais qui signifie « courant », « flux » ou « flot ») est une technologie de lecture de contenu en direct, ou en flux direct. Le contenu en question n'est pas hébergé localement, mais accessible simultanément par plusieurs utilisateurs via internet, au moyen d'un site ou d'une application client.

Les exemples de cette technologie sont nombreux : Youtube (pour la vidéo), Netflix (pour les films et les séries), Spotify ou Deezer (pour la musique), etc.

L'intérêt du streaming

L'intérêt des services de streaming est l'accès légal à un catalogue de très grande envergure, immédiatement utilisable, mobile, sans avoir à en gérer les données et le stockage. En effet, c'est pour la musique, des dizaines de millions de titres accessibles instantanément par l'utilisateur. Pour qu'un tel service puisse être légal, il doit être conforme aux lois sur le droit d'auteur et utiliser des DRM (Data Right Management) pour limiter les usages des clients.

Spotify, créé en 2006 en Suède, est sans doute l'une des plateformes les plus emblématiques. Ce service compte aujourd'hui 140 millions d'utilisateurs qui peuvent accéder à plus de 30 millions de titres musicaux, même les plus récents. Le service est soit distribué par une application client à

installer sur le dispositif de son choix (ordinateur, smartphone, tablette, etc…), soit par un lecteur web HTML. Il faut alors créer un compte spécifique ou se connecter avec un compte Facebook pour s'authentifier et utiliser ce service.

Le modèle économique repose sur un système d'abonnement (9,99 euros par mois dans l'Union Européenne, 12,95 CHF en Suisse). Si l'utilisateur ne souhaite pas payer, le service est accessible gratuitement, mais entrecoupé de publicités et certaines possibilités en sont retirées telles que la sélection d'un morceau particulier dans un album. Cela sert à inciter les usagers à souscrire à un abonnement, mais aussi à créer des recettes grâce à cette publicité. Tous les services de musique en streaming n'ont pas nécessairement le même modèle économique. Ainsi, Apple Music ne propose pas la possibilité d'une utilisation partielle hors abonnement.

Les métadonnées musicales sur Spotify

La raison première des métadonnées est l'identification d'une œuvre et des personnes qui y ont contribué. N'étant ni une connaissance, ni un savoir, la musique est par conséquent un terrain propice au développement des métadonnées : vecteur d'émotion, le fichier musical doit être enrichi de métadonnées pour être indexé, classé et relié à un genre et une époque. Il existe beaucoup de standards et de normes qui régissent les métadonnées musicales. On retiendra par exemple le standard de catalogage ISBD pour les bibliothèques, l'ISRC (International Standard Recording Code), qui caractérise les enregistrements et leurs producteurs, l'IPI (Interested Parties Information Code) qui attribue un code unique aux artistes (ou autres) pour se prémunir contre les copies illégales ou encore la norme ISO 15707 : 2001 : Code international normalisé des œuvres musicales (ISWC International Standard Musical Work Code), qui caractérise une œuvre (par opposition aux enregistrements).

Bien qu'elles soient nombreuses, ces normes n'ont pas de caractère obligatoire et n'intéressent que peu Spotify car celui-ci ne rémunère pas directement les auteurs mais externalise cette étape. Ce sont les prestataires externes qui ont besoin de toutes les informations permettant de rémunérer les ayants droits. De plus, afin de garantir une expérience utilisateur efficace et de rendre les données interopérables, Spotify cherche à exploiter le minimum d'informations nécessaires. Ce sont les raisons pour lesquelles l'utilisateur n'a à sa disposition que peu de métadonnées lors d'une écoute.

Droit applicable et modification des métadonnées.

Pour la majorité des pays qui ont accès à Spotify, le droit applicable est celui de la Suède (à l'exception du continent américain et de l'Espagne). C'est par conséquent la loi suédoise sur les droits d'auteur qui est applicable.

S'il est un aspect important à relever concernant les droits d'auteur, c'est que les métadonnées produites par les artistes sont également protégées par le droit d'auteur. Il est donc pratiquement impossible de modifier ces données si ce n'est par l'auteur lui-même qui souhaite les modifier (au sens de l'article 2 de la loi relative au droit d'auteur sur les œuvres littéraires et artistiques suédoise).

C'est là l'une des raisons pour lesquelles il n'est pas possible pour la communauté utilisant Spotify de modifier les éventuelles fautes dans ces métadonnées (dont nous discuterons plus loin), malgré de nombreuses demandes.

Le cycle de vie des données musicales sur Spotify

Pour commencer, ce sont les producteurs de musique qui transmettent à Spotify les données et les métadonnées musicales. Par producteurs de musique, il faut comprendre les artistes, les musiciens, les éditeurs et maisons de disques et enfin les distributeurs.

La maison de disque ou le distributeur peut posséder un arrangement avec Spotify et lui transmettre directement ses données. Dans d'autres cas, soit la musique est déposée au moyen d'un agrégateur qui va se charger de distribuer la musique à toutes les principales plateformes de musique en ligne et en streaming, dont Spotify. Les agrégateurs compatibles avec Spotify sont au nombre de 10[26], différents dans leurs approches marketing et de distribution. C'est sur ces plateformes que les métadonnées sont renseignées. Toutes ne proposent pas les mêmes champs de saisie de métadonnées, mais elles sont tout de même assez complètes. Il faut remplir les métadonnées de propriétés intellectuelles et de gestion (noms des ayants droits, des structures impliquées, des contrats de diffusion, etc.), les métadonnées descriptives (titre de l'album, titres des pistes, images de la pochette du CD, tonalité, années de production, genre musical, types d'instruments utilisés etc.) et enfin les métadonnées associées (contenu biographique, paroles d'une chanson, dates de concerts, etc.).

L'intérêt pour un artiste d'utiliser l'un de ces agrégateurs est de confier la gestion de leurs droits d'auteur et leur rémunération à une structure spécialisée et de communiquer directement avec les sociétés de collecte et de gestion des droits d'auteur et droits voisins[27], comme le fait un distributeur classique. Leur modèle économique repose sur une commission des recettes ainsi créées ou un système d'abonnement mensuel. Aussi, ce sont ces agrégateurs (ou distributeurs) qui vont s'occuper de transmettre les données aux différents services musicaux avec lesquels ils entretiennent un partenariat.

En ce qui concerne les plateformes de musique en streaming, elles présentent pour l'artiste l'avantage de s'occuper directement des questions de droit et de rémunération. Leur tâche est de reverser les sommes dues (en fonction du nombre d'écoutes par artiste) aux agrégateurs et distributeurs, et de les laisser s'occuper de la rémunération des artistes par le biais des sociétés nationales de gestion des droits.

Au bout de cette chaine, un service comme Spotify récupère les données musicales et encode les fichiers audio dans un format propriétaire (afin d'éviter à la musique d'être massivement copiée). D'un point de vue « utilisateur », les métadonnées disponibles sont bien plus rares que celles demandées par les agrégateurs. On y trouve : un numéro d'identification unique attribué par Spotify, le nom et le numéro de l'album et des titres, leurs durées, le genre musical, le nom du/des artistes, l'image de la pochette de CD, etc. De plus, seuls les différents titres et les artistes sont exploitables par le moteur de recherche de Spotify pour l'utilisateur. Mais plus la description des fichiers musicaux est complexe, plus il est difficile de rendre les données interopérables dans un système.

Pour le sort final des données, dans le cas où un album est retiré de Spotify par son artiste ou par une action en justice, plus aucune donnée n'est accessible par l'utilisateur, il n'est pas possible de savoir si Spotify les conserve.

[26] https://artists.spotify.com/faq#how-do-i-get-a-podcast-on-spotify
[27] La SUISA pour la Suisse

La limite de l'utilisabilité des métadonnées sur Spotify

Dans l'usage, Spotify est un outil efficace. Toutefois, l'utilisabilité des données pose de sérieux problèmes dans certains cas. En effet, lors d'une recherche, la distinction entre l'interprète et l'artiste (ou compositeur) est floue.

Considérons à titre d'exemple une chanson de Georges Brassens : « Supplique pour être enterré à la plage de Sète ». Les métadonnées disponibles sur Spotify sont les suivantes :

Track Name	**Artist Name**	**Album Name**	**Track Number**	**Track Duration (ms)**
Supplique pour être enterré à la plage de Sète	Georges Brassens	Supplique Pour Être Enterré A La Plage De Sète (Version 2011 Avec Deuxième Guitare)	1	434346

Nonobstant le peu de données disponibles, elles sont correctes. En revanche, si l'on cherche un autre artiste qui aurait fait une autre interprétation de cette même chanson, on peut trouver :

Track Name	**Artist Name**	**Album Name**	**Track Number**	**Track Duration (ms)**
Supplique pour être enterré sur la plage de Sète - Live	Maxime Le Forestier	Le Forestier Chante Brassens - Chansons De Rappel	14	384661
Supplique pour être enterré sur la plage de Sète	Sanseverino	Le petit bal perdu	9	318133

Ici, dans la colonne dédiée aux artistes, il n'est même pas possible de rattacher la chanson au le compositeur original, la paternité de l'auteur est complétement oubliée. Si cette information n'est pas disponible dans le titre de l'album, il n'y a alors aucun moyen de retrouver cette chanson par le nom du compositeur. On note également une erreur dans le titre où « à » est remplacé par « sur ».

S'il s'agit d'une opportunité manquée assez importante pour Spotify, cela l'est d'autant plus en ce qui concerne la musique classique. En effet, cette une musique est rarement exécutée par son compositeur, dont la même œuvre fait l'objet de plusieurs versions, interprétées par des artistes différents.

Il est par conséquent fréquent de trouver une pièce de musique, sans que le nom du compositeur n'apparaisse dans le champ « artiste ».

Track Name	**Artist Name**	**Album Name**	**Track Number**	**Track Duration (ms)**
String Quartet in B Minor, Op. 33 No. 1: Finale. Presto	Quatuor Terpsycordes	Joseph Haydn: String Quartets Op. 33	1	714893

En menant une recherche par auteur, il est impossible de retrouver ce titre. Malheureusement, ce phénomène est très largement répandu.

Heureusement, il est possible de mettre plus d'un artiste dans ce champ, comme dans l'exemple suivant :

Track Name	Artist Name	Album Name	Track Number	Track Duration (ms)
String Quartet In G Major, Hob.III:66, (Op.64 No.4): 1. Allegro con brio	Franz Joseph Haydn, Amadeus Quartet	Haydn: String Quartets, Opp.51, 54, 55, 64, 71 & 74	5	273813

Cela permet de rattacher l'œuvre à son compositeur, mais sans déterminer la distribution des rôles.

Pourtant, il existe des méthodes de classification de la musique classique afin d'identifier les œuvres. Il s'agit du numéro d'opus, qui vient numéroter les œuvres des compositeurs en fonction de l'édition de leurs musiques, ou le catalogue thématique, qui est une combinaison unique de chiffres et de lettres pour chaque composition d'un artiste donné (par exemple BWV 106 pour la cantate *Gottes Zeit ist die allerbeste Zeit (Actus Tragicus)*, de Jean-Sébastien Bach. Il existe aussi beaucoup de numéros normalisés, exploitables, comme décrit plus haut.

En définitive, pour que le système soit le plus adapté, il devrait devenir plus riche, plus complexe et maintenu par des personnes spécialistes de ces questions.

Les données utilisateur

Un autre pan important des activités de Spotify, sont les données personnelles des utilisateurs, et des musiques qu'ils écoutent.

En plus des données que l'utilisateur transmet lors de sa création de compte, Spotify collecte les habitudes d'écoute et en détermine des profils pour deux principales raisons [28]:

- Créer des liens entre les musiques (en plus du genre) pour déterminer les suggestions d'écoute De cette manière il leur est possible de proposer de la musique entre les utilisateurs qui ont le même profil.[29]
- Vendre de la publicité adaptée à un public ciblé[30].

Aucune mention n'est faite de la suppression de ces données utilisateurs. La seule mention est faite pour les résidents californiens mineurs… L'auteur du présent du présent article s'est permis de contacter Spotify sur cette question. Il a reçu pour réponse qu'aucune mesure n'était prise pour supprimer les préférences d'écoute. Quand il a demandé si cet état de fait allait changer avec les nouvelles lois de protection des données personnelles de l'Union Européenne, on lui a répondu affirmativement. Le for juridique compétent pour la majorité des utilisateurs de Spotify se trouve en Suède, pays européen, et sera donc soumis à la RGPD[31] dès le 25 mai 2018.

[28] La liste complète des informations collectées est disponible sur le site : https://www.spotify.com/ch-fr/legal/privacy-policy/?language=fr&country=ch
[29] Le profil est visible sur le site www.spotify.me
[30] Explications sur https://spotifyforbrands.com/ch-fr/feature/streaming-habits/
[31] Règlement général sur la protection des données (RGPD) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

Conclusion

Pour conclure, on remarque que les métadonnées proviennent directement des producteurs de musique, et sont donc protégées par le droit d'auteur. Cependant, Spotify pourrait parfaitement ajouter des métadonnées supplémentaires, au risque de complexifier son système et de rendre l'interopérabilité des données plus difficile. Pour ce faire, la société devrait engager des spécialistes de ces questions, prêts à considérer une importante masse de données.

Il y aurait un réel avantage à augmenter le nombre de métadonnées exploitables par l'utilisateur. En effet, il existe un fort potentiel d'accroissement du référencement de la musique. Aussi, pourrait-on faire apparaitre le nom de personnes (ou groupes de personnes) qui ont contribué à la création d'une œuvre, car dans certains cas la paternité d'une œuvre n'est même pas disponible… Il semblerait qu'ajouter quelques données supplémentaires amélioreraient l'expérience utilisateur sur cette plateforme.

Toutefois, Spotify devrait investir massivement dans une opération chronophage d'enrichissement des métadonnées et mettre en danger l'interopérabilité des données au sein de son système.

Le symptôme de l'éparpillement de la musique est encore très visible dans ce mode de distribution en streaming, pour lequel il conviendrait de chercher une unification et une standardisation des métadonnées. Il s'agirait peut-être d'une nouvelle opportunité de travail pour les différents distributeurs de musique.

Conclusion

Pour mener proprement leurs missions et leurs activités, les organisations sont confrontées aux diverses exigences techniques, technologiques, administratives et règlementaires de la gestion des ressources informationnelles. La volumétrie grandissante et les formats et supports diversifiés ajoutent un niveau supplémentaire à ce défi. Cependant, si les informations constituent un bien précieux, toutes ne possèdent pas une valeur uniforme et il appartient aux organisations de bien définir ce qu'elles considèrent comme un actif informationnel à protéger et valoriser.

La conformité avec les textes légaux, réglementaires et normatifs est également un enjeu important pour les organismes aussi bien privés que publics. Le développement des technologies de l'information et de la communication pose la question de la valeur probante d'un document numérique. Pour y répondre, plusieurs exigences, notamment l'authenticité et l'intégrité, s'appliquent, pour la plupart également aux documents papier, mais qui, pour les documents numériques, nécessitent des moyens techniques relativement avancés, tels que la cryptographie ou l'usage d'un coffre-fort électronique. Cette problématique de la conformité peut aussi créer des tensions, lorsque des exigences semblent contradictoires, ou du moins difficiles à concilier, comme la protection des données personnelles face à une procédure de *e-discovery*. S'ajoute à cela, les considérations spécifiques liées aux différentes typologies de données (données de la recherche, données publiques, données médicales, données bancaires, etc.).

Pour répondre à ces problématiques complexes, le concept de gouvernance de l'information a peu à peu émerger ; mais il n'a pas encore été adopté par toutes les organisations, car il demande du temps et de l'énergie pour se mettre en place.

Bibliographie

Introduction

NICOLET, Aurèle, 2016. *Vers une approche de gouvernance informationnelle pour une PME high-tech* [en ligne]. Carouge : Haute école de gestion de Genève. Mémoire de master. [Consulté le 7 mars 2019]. Disponible à l'adresse: http://doc.rero.ch/record/277982?ln=fr

INTERPARES TRUST, [s. d.]. Governance (English). *ITrust Terminology* [en ligne]. [Consulté le 8 novembre 2018]. Disponible à l'adresse : http://arstweb.clayton.edu/interlex/en/term.php?term=governance

PEARCE-MOSES, Richard, 2016. Information. *A Glossary of Archival and Records Terminology* [en ligne]. Chicago : the Society of American Archivists. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://www2.archivists.org/glossary/terms/i/information

SMALLWOOD, Robert F., 2014. *Information governance: concepts, strategies and best practices*. Hoboken : Wiley. Wiley CIO series. ISBN 9781118218303.

Les actifs informationnels : définitions et évaluations

ADESEMOWO, Adeniji K., VON SOLMS, Rossouw & BOTHA, Reinhard A. (2016). Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond?. *South African Journal of Information Management* [en ligne]. Vol. 18, n° 1. [Consulté le 8 novembre 2018]. Disponible à l'adresse : http://dx.doi.org/10.4102/sajim.v18i1.706

AGENCE DE LA SANTÉ ET DES SERVICES SOCIAUX DE MONTRÉAL, 2012. *Bilan de la sécurité des actifs informationnels 2005-2011* [en ligne]. Québec, 14 février 2012. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://santemontreal.qc.ca/fileadmin/user_upload/Uploads/tx_asssmpublications/pdf/publications/isbn978-2-89510-618-0.pdf

AGENCE DE LA SANTÉ ET DES SERVICES SOCIAUX DE MONTRÉAL, 2015. *Bilan de la sécurité des actifs informationnels 2013-2015* [en ligne]. Québec, 30 mars 2015. [Consulté le 8 novembre 2018]. Disponible à l'adresse : http://collections.banq.qc.ca/ark:/52327/bs2460689

BARCLAYS, 2016. Obligations de contrôle pour les fournisseurs externes : Sécurité des informations [en ligne]. Décembre 2016. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://home.barclays/content/dam/home-barclays/documents/who-we-are/our-suppliers/french/fr-Information-Security-v7.0.pdf

CHAMBRE DES NOTAIRES DU QUÉBEC, 2016. Cadre de sécurité des actifs informationnels [en ligne]. Québec, 8 septembre 2016. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.cnq.org/DATA/TEXTEDOC/cadre-secur-actifs-inform.pdf

CLAVIER, Viviane, & PAGANELLI, Céline (dir.), 2013. *L'information professionnelle*. Paris : Lavoisier. Systèmes d'information et organisations documentaires.

CLEARWATER COMPLIANCE, 2015. *The Clearwater Definition of an Information Asset (with Examples for different organizations)* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://clearwatercompliance.com/wp-content/uploads/2015/11/Clearwater-Definition-of-Information-Assets-with-Examples_V8.pdf

CONSEIL D'ÉTAT DU CANTON DU VALAIS, 2015. *Message accompagnant le projet de décision pour l'octroi d'un crédit d'engagement pour la mise en application de la « Stratégie informatique 2015 – 2024 de l'Etat du Valais »* [en ligne]. Sion, 21 août 2015. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://parlement.vs.ch/common/idata/parlement/vos/docs/2015/10/2015.11_Informatikstrategie%202015-2024_BOT_SR.pdf

COUNCIL OF ISLINGTON, 2015. *Islington Information Asset Owners: A council-wide information management policy* [en ligne]. Janvier 2015. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.islington.gov.uk/~/media/sharepoint-lists/public-records/informationmanagement/businessplanning/policies/20162017/20160418informationassetowners.pdf

CPA, ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DE QUÉBEC, 2014. *Politique de sécurité de l'information* [en ligne]. Montréal, 29 MAI 2014. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://cpaquebec.ca/~/media/docs/profession-ordre/a-propos/gouvernance/politiques/politique-securite-information.pdf

CRONIN, Blaise, 1989. Value for money: finding and taking fresh opportunities. In Myers, J. (éd), *Information and library services: policies and perspectives, Proceeding of a conference organized by the Institute of Information Scientists*. London : Aslib, pp. 56-65.

CRONIN, Blaise, Davenport, Elisabeth, 1991. *Elements of information management*. Metuchen, NJ : Scarecrow.

CRONIN, Blaise, 1997. Préface : La société informationnelle : enjeux sociaux et approches économiques. In : Mayère, Anne (dir.), *La société informationnelle : enjeux sociaux et approches économiques*. Paris : L'Harmattan, pp. 7-20.

E-HEALTH SUISSE, 2017. *Aide la mise en œuvre concernant la protection et la sécurité des données dans le cadre du DEP* [en ligne]. Berne, 21 juin 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/F/170627_Umsetzungshilfe_Datenschutz-Datensicherheit_f.pdf

FONDATION DE BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, 2016. *Politique de la fondation de bibliothèque et archives nationales du Québec en matière de sécurité informatique des actifs informationnels et de l'information* [en ligne]. 11 février 2016.

[Consulté le 13 novembre 2018]. Disponible à l'adresse : https://fondation.banq.qc.ca/wp-content/uploads/2016/06/FBAnQ_Sécurité-de-linformation_Politique_Révision_Final.pdf

GROUPE CANAM, 2007. Politique de sécurité des actifs informationnels [en ligne]. 31 octobre 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.groupecanam.com/wp-content/uploads/2013/11/Politique-securite-actifs-informationnels.pdf

HEC MONTRÉAL, 2011. Politique de sécurité de l'information [en ligne]. 10 novembre 2011. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://www.hec.ca/direction_services/secretariat_general/juridique/reglements_politiques/documents/politique_securite_information.pdf

INFORMATION ASSET DEVELOPMENT, 2018. What is an Information Asset?. *Information Asset Development* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.informationassetdevelopment.com/what.html

INSTITUTE OF DIRECTORS IN NEW ZEALAND, [s. d.]. Technology terms. *Technology governance* [en ligne. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.iod.org.nz/Governance-Resources/Resource-library/Risk/Technology-governance

KLING, R. ACKERMAN, M. S., ALLEN, J.P. 1996. Information entrepreurnialism information technologies and the continuing vulnerability to privacy. In : *Information entrepreneurialism and controversy: value conflicts and social choices*. San Diego : Academic Press, pp. 727-743.

LAMBERTON, Donald, 1997. Pour une taxonomie de l'information. In MAYÈRE, Anne (dir.), *La société informationnelle : enjeux sociaux et approches économiques*. Paris : L'Harmattan, pp. 69-86.

LANEY, Doug, 2017. Why a book on infonomics?. *Gartner Blog Network* [en ligne]. 23 août 2017. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://blogs.gartner.com/doug-laney/why-a-book-on-infonomics/

LANEY, Doug, 2011. Infonomics: The Economics of Information and Principles of Information Asset Management. In : *The Fifth MIT Information Quality Industry Symposium, Cambridge, MA, USA, July 13-15 2011* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://mitiq.mit.edu/IQIS/Documents/CDOIQS_201177/Papers/05_01_7A-1_Laney.pdf

LANEY, Doug, 2012. Infonomics: The Practice of Information Economics. *Forbes* [en ligne]. 22 mai 2012. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://www.forbes.com/sites/gartnergroup/2012/05/22/infonomics-the-practice-of-information-economics/#21e491916ee4

LEAVITT, Harold J., WHISLER, Tomas L., 1958. Management in the 1980's. *Harvard Business Review* [en ligne]. November-December 1958. Vol. 36, n° 6, pp. 41–48. [Consulté le 8

novembre 2018]. Disponible à l'adresse : https://stacks.stanford.edu/file/druid:fv912fw0448/fv912fw0448.pdf

LESSARD, Benoît, 2009. *Politique concernant la sécurité de l'information* [en ligne]. Québec : Ministère des Ressources naturelles et de la Faune, 31 mars 2009. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.mffp.gouv.qc.ca/publications/ministere/politique/securite-information.pdf

Loi concernant le partage de certains renseignements de santé (P-9.0001). *LégisQuébec* [en ligne]. 4 juillet 2012. Mise à jour le 12 juillet 2018. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://legisquebec.gouv.qc.ca/fr/showDoc/cs/P-9.0001?&digest=

MANCINI, John, 2016. *Infonomics: How do you measure the value of information?* [en ligne]. Executive Leadership Council (ELC), été 2016. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.project-consult.de/files/AIIM_Studies_Fall_2016/AIIM_IW_Value_of_Information_2016_Sep16.pdf

Moody, Daniel, Walsh, Peter, 1999. Measuring the value of information: An asset valuation approach. In : *7th European Conference on Information Systems (ECIS'99), Copenhagen Business School, Frederiksberg, Denmark, 23-25 June 1999* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://si.deis.unical.it/zumpano/2004-2005/PSI/lezione2/ValueOfInformation.pdf

THE NATIONAL ARCHIVES, 2017. *Information assets factsheet* [en ligne]. Février 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

NATIONAL INSTITUTE FOR HEALTH AND CARE EXCELLENCE (NICE), 2016. Information Governance Management Framework [en ligne]. Janvier 2015. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.nice.org.uk/Media/Default/About/Who-we-are/Policies-and-procedures/Information-governance-policy-and-management-framework.pdf

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, 2005. Actif informationnel. Le grand dictionnaire terminologique [en ligne]. [Consulté le 8 novembre 2018]. Disponible à l'adresse : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8365500

OXFORDSHIRE COUNTY COUNCIL, 2015. Security Incident Management Policy [en ligne]. 27 janvier 2015. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.oxfordshire.gov.uk/cms/sites/default/files/folders/documents/business/providers/securityincidentmanagementpolicy.pdf

SAPIR, Jacques, 2005. *Quelle économie pour le XXIe siècle ?*. Paris : Odile Jacob.

SECRÉTARIAT DU CONSEIL DU TRÉSOR, 2016. *Guide de catégorisation de l'information* [en ligne]. Québec, juillet 2016. [Consulté le 13 novembre 2018]. Disponible à l'adresse :

https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/categorisation_information.pdf

SERVAIS, Paul (eds), 2015. *Archivistes de 2030 : Réflexions prospectives*. Louvain-la-Neuve : Academia. Publications des Archives de l'Université catholique de Louvain, 32.

STEWART, Thomas A., 1997. *Intellectual capital: The new wealth organization*. Doubleday Dell : New York.

TASMANIAN ARCHIVE + HERITAGE OFFICE (TAHO), 2015. *38Information Management Advice 38 Information Asset Owner and Digital Continuity* [en ligne]. Tasmania: Department of Education, mars 2015. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Advice%2038%20Information%20Asset%20owner%20and%20Digital%20Continuity.pdf

ULTIMA, 2016. *Politique sur la gestion et la sécurité de l'information* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.ultima.qc.ca/wp-content/uploads/2016/11/Politique-sur-la-gestion-et-la-sécurité-de-linformation-2016-REV_nov2016.pdf

UNIRIS - SERVICES DES RESSOURCES INFORMATIONNELLES ET ARCHIVES, 2016. *Records management et gouvernance informationnelle : Concepts et explications* [en ligne]. Université de Lausanne, 26 janvier 2016. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.unil.ch/uniris/files/live/sites/uniris/files/documents/references/UNIL_RM_Gouvernance_Info_concepts_explications_VF-1.pdf

UNIVERSITÉ LAVAL, 2012. *Règlement de sécurité de l'information sur l'utilisation des actifs informationnels* [en ligne]. 28 novembre 2012. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.bsi.ulaval.ca/sites/default/files/cadre/publics/reglement_de_sdi_sur_utilisation_des_actifs_informationnels.pdf

UNIVERSITY OF TASMANIA - RECORDS MANAGEMENT UNIT (RMU), 2018. *RMU Information Sheet 18* [en ligne]. 6 octobre 2017. Mis à jour le 6 février 2018. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.utas.edu.au/__data/assets/pdf_file/0020/1046243/RMU-Information-Sheet-18-Information-Assets.pdf

VICTORIAN GOVERNMENT, 2018. *Information Management Glossary* [en ligne]. Mai 2018 [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2018/05/IM-GUIDE-03-Information-Management-Glossary1-1-1.pdf

WALLACE, Chris, 2014. *Information Governance: Framework and Strategy* [en ligne]. Hambleton, Richmondshire and Whitby Clinical Commissioning Group, juillet 2014. [Consulté le 13 novembre 2018]. Disponible à l'adresse :

https://www.hambletonrichmondshireandwhitbyccg.nhs.uk/documents/59993/91161/HRWCCG+IG+Framework/56a42479-4b79-490b-ac80-ab8996f1ff05?version=1.1

WOODS, Bernard, 1992. The evaluation of marketing information: some current practices and trends. *Aslib Proceedings* [en ligne]. Vol. 44, n° 10, pp. 361-364. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://doi.org/10.1108/eb051297

YATES-MERCER, Penelope, BAWDEN, David, 2002. Managing the paradox: the valuation of knowledge and knowledge management. *Journal of Information Science* [en ligne]. Vol. 28, n° 1, pp. 19-29. [Consulté le 8 novembre 2018]. Disponible à l'adresse : https://doi.org/10.1177/016555150202800103

Valeur probante du document électronique

BANAT-BERGER, Françoise, BORGEAUD, Emily, NOUGARET, Christine, 2016. Les concepts de fiabilité, d'exactitude et d'authenticité revus à cette aune. In: *Archivistique et diplomatique numériques : une traduction en français d'une partie des livrables du projet InterPARES 2* [en ligne]. Paris : Editions en ligne de l'Ecole des Chartes. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://elec.enc.sorbonne.fr/interpares2/revision

BARREAU, Ivan, 2011. *L'écrit comme meilleure preuve : toujours une vérité à l'ère numérique ?* [en ligne]. Montréal : Université de Montréal - EBSI. Travail de recherche. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/5079/barreau-i-ecrit-preuveere-numerique.pdf?sequence=7

CANTON DE VAUD, 2017. Archiver les documents numériques. *Site officiel du Canton de Vaud* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.vd.ch/themes/etat-droit-finances/communes/administration-generale/archives-communales/archivage-electronique/

CASTEX, Eric, 2016. Les critères d'authenticité d'une archive électronique. *Portail international archivistique francophone* [en ligne]. 24 mars 2016. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.piaf-archives.org/actualites/les-criteres-dauthenticite-dune-archive-electronique

Code de procédure civile (RS 272). *Recueil systématique du droit fédéral (RS)* [en ligne]. 19 décembre 2008. Mise à jour le 1er janvier 2018. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/20061121/index.html

Code de procédure pénale suisse (RS 312.0). *Recueil systématique du droit fédéral (RS)* [en ligne]. 05 octobre 2007. Mise à jour le 1er mars 2018. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/20052319/index.html

CONFÉDÉRATION SUISSE, 2017. Signature électronique. *egovernment schweiz suisse svizzera.* [Consulté le 13 novembre 2018]. Disponible à l'adresse :

https://www.egovernment.ch/fr/dokumentation/questions-juridiques/signature-electronique/

DUMONT, Renaud, 2009-2010. *Cryptographie et Sécurité informatique* [en ligne]. Support de cours : Cours « Cryptographie et sécurité informatique », Université de Liège, Faculté des Sciences appliquées, année académique 2009-2010. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.montefiore.ulg.ac.be/~dumont/pdf/crypto.pdf

DUNANT GONZEBACH, Anouk, 2013. La gouvernance des documents électroniques dans l'administration cantonale genevoise: genèse et mise en oeuvre. *Ressi* [en ligne]. N°14, 18 décembre 2013. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.ressi.ch/num14/article_93

DUNANT GONZEBACH, Anouk, DUCRY, Emmanuel, 2014. *La gouvernance des documents électroniques- Cycle pratique archivistique suisse 2014* [en ligne]. 3 octobre 2014. Genève: Département présidentiel. Archives d'Etat. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.bar.admin.ch/dam/bar/it/dokumente/veranstaltungen/regelwerke_zum_umgangmitdigitalendokumentenwaehrendihresadminist.pdf.download.pdf/la_gestione_dei_documentidigitalinelcorsodellaloroesistenzaammin.pdf

Loi fédérale complétant le Code civil suisse (RS 220). *Recueil systématique du droit fédéral (RS)* [en ligne]. 30 mars 1911. Mise à jour le 1er avril 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19110009/index.html

Loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (RS 943.03). *Recueil systématique du droit fédéral (RS)* [en ligne]. 18 mars 2016. Mis à jour le 1er janvier 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse: https://www.admin.ch/opc/fr/classified-compilation/20131913/index.html

NITULESCU, Anca, 2016. *Authentification et Intégrité : Signature numérique et hachage* [en ligne]. Support de cours : Cours « Introduction à la cryptographie », Université Paris 13 Villetaneuse, année académique 2015-2016. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.di.ens.fr/~nitulesc/files/CRYPTO13/cours8.pdf

Ordonnance concernant la tenue et la conservation des livres de comptes (Olico) (RS 221.431). *Recueil systématique du droit fédéral (RS)* [en ligne]. 24 avril 2002. Mise à jour le 1er janvier 2013. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/20001467/index.html

ORGANISATION INTERNATIONALE DE NORMALISATION, 2009. *Risk management — Principles and guidelines = Management du risque — Principes et lignes directrices*. 1ère éd. Genève : ISO, 15 novembre 2009. ISO 31000.

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011. *Information technology — Security techniques — Information security risk management = Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information*. 2e éd. Genève : ISO. 1er juin 2011. ISO/IEC 27005.

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011. *Information and documentation — Management systems for records — Requirements = Information et documentation — Systèmes de gestion des documents d'activité — Exigences*. 1ère éd. Genève : ISO, 15 novembre 2011. ISO 30301.

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011. *Information and documentation — Management systems for records — Fundamentals and vocabulary = Information et documentation — Systèmes de gestion des documents d'activité — Principes essentiels et vocabulaire*. 1ère éd. Genève : ISO, 15 décembre 2011. ISO 30300.

ORGANISATION INTERNATIONALE DE NORMALISATION, 2012. *Electronic archiving — Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation = Archivage électronique — Partie 1: Spécifications relatives à la conception et au fonctionnement d'un système d'informations pour la conservation d'informations électroniques*. 1ère éd. Genève : ISO, 1er février 2012. ISO 14641-1.

ORGANISATION INTERNATIONALE DE NORMALISATION, 2014. *Information and documentation — Risk assessment for records processes and systems = Information et documentation — Evaluation du risque pour les processus et systèmes d'enregistrement*. 1ère éd. Genève : ISO, 15 mars 2014. ISO/TR 18128.

ORGANISATION INTERNATIONALE DE NORMALISATION, 2016. *Information and documentation — Records management — Part 1: Concepts and principles = Information et documentation — Gestion des documents d'activité — Partie 1: Concepts et principes*. 2e éd. Genève : ISO, 15 avril 2016. ISO 15489-1.

PARISCOAT, Jérôme, 2016. Archivage de documents dématérialisés, contraintes légales et sécurité des données : Comment protéger au mieux ses documents? *Archimag* [en ligne]. 09 mai 2016. [Consulté le 30 novembre 2017]. Disponible à l'adresse : http://www.archimag.com/demat-cloud/2016/05/09/archivage-documents-dematerialises-securite-donnees-proteger

PARK, Eun G., 2004. Rôle de l'authenticité dans le cycle de vie des documents numériques. In : SAVARD, Réjean (dir.). *Le numérique : impact sur le cycle de vie du document, Université de Montréal, 13 au 15 octobre 2004* [en ligne]. Lyon : école nationale supérieure des sciences de l'information et des bibliothèques, pp. 200-205. [Consulté le 13 novembre 2018]. Disponible à l'adresse: http://www.enssib.fr/bibliotheque-numerique/documents/1223-lenumerique-impact-sur-le-cycle-de-vie-du-document.pdf

ROGERS, Corinne, 2015. *Virtual authenticity: authenticity of digital records from theory to practice*. [en ligne]. Vancouver : University of British Columbia. Thèse de doctorat.

[Consulté le 13 novembre 2018]. Disponible à l'adresse: https://open.library.ubc.ca/media/stream/pdf/24/1.0166169/1

UNIRIS - SERVICES DES RESSOURCES INFORMATIONNELLES ET ARCHIVES, 2014. *Politique de Records management - Glossaire* [en ligne]. 12 mars 2013. Mis à jour le 11 juin 2014. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.unil.ch/uniris/files/live/sites/uniris/files/documents/references/UNIL_POL_RM_Glossaire_VF.pdf

Le traitement des données personnelles dans les procédures d'E-Discovery

ALLISON, Peter Ray, 2017. UK Data Protection Bill vs EU General Data Protection Regulation. *Computer Weekly* [en ligne]. Novembre 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.computerweekly.com/feature/UK-Data-Protection-Bill-vs-EU-General-Data-Protection-Regulation

BURRUS, Louis, 2017. US DoJ Program for Swiss Banks: Lessons Learned and Perspectives. *Institut suisse de droit comparé* [en ligne]. 23 juin 2017. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.isdc.ch/media/1409/dip2017burrus.pdf

BURTON, Cédric, GUFFLET, Myriam, 2012. Procédure d'E-discovery et protection des données : entre le marteau et l'enclume. In : DEMOULIN, Marie (dir.). *L'archivage électronique et le droit*. Bruxelles : Larcier, 2012, pp.105-131. Collection du CRIDS, 34. ISBN 9782804452001.

BURTON, Cédric, PROUST, Oliver, 2009. Le conflit de droits entre les règles américaines d'e-discovery et le droit européen de la protection des données à caractère personnel...entre le marteau et l'enclume. *Revue Lamy droit de l'immatériel* [en ligne]. N° 46, février 2009. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.wsgr.com/attorneys/BIOS/PDFs/burton-ediscovery-0209.pdf

Charte des droits fondamentaux de l'union européenne (2000/C 364/01). *Journal officiel des Communautés européennes* [en ligne]. 18 décembre 2000. [Consulté le 14 novembre 2018]. Disponible à l'adresse : www.europarl.europa.eu/charter/pdf/text_fr.pdf

Code pénal suisse du 21 décembre 1937 (RS 311.0). *Recueil systématique du droit fédéral (RS)* [en ligne]. 21 décembre 1937. Mise à jour le 1er mars 2018. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html

COMMISSION EUROPEENNE, 2016. European Commission - Fact Sheet: Questions and Answers on the EU-U.S. Data Protection "Umbrella Agreement". *Commission européenne* [en ligne]. 1er décembre 2016. [Consulté le 5 octobre 2017]. Disponible à l'adresse : http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm

CONFÉDÉRATION SUISSE, 2016. *Stratégie Suisse numérique* [en ligne]. Avril 2016. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.bakom.admin.ch/dam/bakom/fr/dokumente/informationsgesellschaft/strategie/strategie_digitale_schweiz.pdf.download.pdf/strategie_digitale_schweiz_FR.pdf

Convention sur l'obtention des preuves à l'étranger en matière civile et commerciale. *Conférence de la Haye de droit international privé* [en ligne]. 18 mars 1970. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://assets.hcch.net/docs/41558329-d3e0-44ce-94ec-e827a1feff20.pdf

Constitution fédérale de la Confédération suisse du 18 avril 1999 (101). *Recueil systématique du droit fédéral (RS)* [en ligne]. 18 avril 1999. Mise à jour le 1er janvier 2018. [Consulté le 14 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19995395/index.html

LE COURRIER, 2017. Mieux protéger les données des Suisses. *Le Courrier* [en ligne]. 15 septembre 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.lecourrier.ch/152619/mieux_proteger_les_donnees_des_suisses

Directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil. *Journal officiel de l'Union européenne* [en ligne]. 4 mai 2016. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:32016L0680&from=EN

DUBOIS, Camille, 2015.Révision de la loi fédérale sur la protection des données : mettre l'accent sur la transparence et le contrôle. *La vie économique* [en ligne]. 26 octobre 2015. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://dievolkswirtschaft.ch/fr/2015/10/dubois-11-2015-franz/

EDRM. Quick Reference EDRM Workflow Poster — A Training Tool for Legal Professionals and E-Discovery Practitioners. *EDRM Duke Law* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.edrm.net/frameworks-and-standards/edrm-model/edrm-wall-poster/

EXTERRO, 2016. The basics of e-discovery. *Exterro* [en ligne]. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.exterro.com/basics-of-e-discovery/

FONDATION PROMETHEUS, 2011. La procédure dite de Discovery. *Fondation Prometheus* [en ligne]. Mai 2011. [Consulté le 14 octobre 2017]. Disponible à l'adresse : http://www.fondation-prometheus.org/wsite/publications/newsletter/201105/la-proc%C3%A9dure-dite-de-discovery/

FTI CONSULTING, 2010. E-Discovery and Legal Frameworks Governing Privacy and Data Protection in European Countries: Part 1 – Implications. *FTI Consulting Technology* [en ligne]. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://www.ftitechnology.com/resources/white-papers/rand-global-privacy-and-data-protection-part-1

GAUTSCHI, Heidi, GIANLUIGI, Viscusi, TUCCI, Christopher L, 2016. *Switzerland's digital future : facts, Challenges, Recommandations* [en ligne]. Rapport de l'Ecole Polytechnique Fédérale de Lausanne (EPFL) [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.egovernment.ch/index.php/download_file/force/821/3343/&usg=AOvVaw33SnjoCx00OU67Y0sJ4iLg

GREENBERG, Michael, LYNSKEY, Orla, ROBINSON, Neil, 2010. E-Discovery and legal frameworks governing Privacy and Data Protection in European countries. *FTI Consulting Technology* [en ligne]. Novembre 2010. [Consulté le 14 novembre 2018]. Disponible à l'adresse : https://static.ftitechnology.com/docs/white-papers/white-paper-rand-implications-part-two-2010.pdf

HILGARD, Mark C., LEFFERT, Kim A., SAUTTER, Edmund, 2013. European Union: E-Discovery In The European Union. *Mondaq* [en ligne]. 5 novembre 2013. [Consulté le 13 octobre 2018]. Disponible à l'adresse : http://www.mondaq.com/unitedstates/x/273078/disclosure+electronic+discovery+privilege/EDiscovery+In+The+European+Union

Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; 235.1). *Recueil systématique du droit fédéral (RS)* [en ligne]. 19 juin 1992. Mise à jour le 1er janvier 2014. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html

Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce du 13 mars 1964 (LTr ; 822.11). *Recueil systématique du droit fédéral (RS)* [en ligne]. 13 mars 1964. Mise à jour le 1er décembre 2013. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19640049/index.html

MATHIAS, Garance, 2016. Discovery & transfert de données. *Mathias Avocats* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.avocats-mathias.com/wp-content/uploads/2016/02/Discovery-Transfert-de-donn%C3%A9es-Mathias-Avocats-F%C3%A9vrier-2016.pdf

Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD ; 235.11). *Recueil systématique du droit fédéral (RS)* [en ligne]. 14 juin 1993. Mise à jour le 16 octobre 2012. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19930159/index.html

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, [s. d.]. Protection des données. *Confédération suisse* [en ligne]. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/generalites/protection-des-donnees.html

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, 2014. *Guide pour le traitement des données personnelles dans le secteur du travail : traitement par des personnes privées* [en ligne]. Berne, 2 octobre 2014. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/traitement-des-donnees-personnelles-dans-le-secteur-du-travail.html

QUIQUEREZ, Florent, 2017. « Les contribuables ont droit à leur sphère privée ». *Tribune de Genève* [en ligne]. 16 novembre 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.tdg.ch/suisse/contribuables-droit-sphere-privee/story/17947873

Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). *Cnil* [en ligne]. 23 mai 2018. [Consulté le 14 novembre 2018]. Disponible à l'adresse : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

SAFFADY, William, 2013. *E-mail retention and archiving: issues and guidance for compliance and discovery*. Overland Park : ARMA International, 2012. ISBN 9781936654260

SAUNOIS, Lucie, 2017. LPD – Loi fédérale sur la Protection des Données : qu'est-ce qui change ? *Net4All* [en ligne]. 20 avril 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.net4all.ch/blog/lpd-loi-federale-protection-donnees-quest-change/

SWAN, Carole, 2013. L'enjeu de la protection des données personnelles lors de l'utilisation de la procédure d'E-Discovery. *Dalloz Actualité : le quotidien du droit* [en ligne]. 21 juin 2013. [Consulté le 12 novembre 2018]. Disponible à l'adresse : https://www.dalloz-actualite.fr/chronique/l-enjeu-de-protection-des-donnees-personnelles-lors-de-l-utilisation-de-procedure-de-e-dis#.Web-GVt-q70

LE TEMPS, 2017. La Suisse étend l'échange automatique à la Russie et la Chine. *Le Temps* [en ligne]. 16 juin 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.letemps.ch/economie/2017/06/16/suisse-etend-lechange-automatique-russie-chine

THARIN, Arien, WILLI, Anna, 2017. Protection des données : évolution du panorama Suisse et Européen. *Altenburger* [en ligne]. Avril 2017. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://www.altenburger.ch/fr/actualites/newsletter/protection-des-donnees-evolution-du-panorama-suisse-et-europeen/

Traité sur le fonctionnement de l'Union européenne (version consolidée). *Journal officiel de l'Union européenne* [en ligne]. 26 octobre 2012. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A12012E%2FTXT

TRIBUNE DE GENÈVE, 2017a. Feu vert à l'échange automatique avec 40 pays. *Tribune de Genève* [en ligne]. 18 octobre 2017. [Consulté le 12 novembre 2018]. Disponible à l'adresse : https://www.tdg.ch/suisse/feu-vert-echange-automatique-40-pays/story/29137478

TRIBUNE DE GENÈVE, 2017b. Le secret bancaire pour les Suisses sauve sa peau. *Tribune de Genève* [en ligne]. 16 novembre 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.tdg.ch/suisse/secret-bancaire-suisses-sauve-peau/story/14375804

UEBERSCHLAG, Leila, 2017. Législation européenne sur la protection des données : les entreprises suisses en retard. *Economie Digitale : Dé-cryptage* [en ligne]. 3 avril 2017. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://blogs.letemps.ch/leila-ueberschlag/2017/04/03/legislation-europeenne-sur-la-protection-des-donnees-les-entreprises-suisses-en-retard/

THE UNITED STATES DEPARTMENT OF JUSTICE, 2013. Joint Statement between the U.S. Department of Justice and the Swiss Federal Department of Finance. *The United States Department of Justice [*en ligne]. Février 2009. [Consulté le 13 novembre 2018]. Disponible à l'adresse : https://www.justice.gov/tax/file/631356/download

24 HEURES, 2017. Berne défend l'échange d'infos avec Wellington. *24 heures* [en ligne]. 3 novembre 2017. [Consulté le 12 novembre 2018]. Disponible à l'adresse : https://www.24heures.ch/suisse/berne-defend-echange-dinfos-wellington/story/22065478

WINKLER, Maria, 2011. La protection des données dans l'entreprise – Un mode d'emploi pour sa mise en œuvre. *TREX L'expert fiduciaire* [en ligne]. 2011, n° 2 [Consulté le 13 novembre 2018]. Disponible à l'adresse : http://www.itandlaw.ch/fileadmin/user_upload/Publikationen/2_11_Fachb_Winkler_Datenschutz_fr_Druckdatei.pdf

Etat de l'art des documents gouvernant les données de la recherche dans les Hautes écoles suisses

ACADÉMIE SUISSE DES SCIENCES HUMAINES ET SOCIALES, 2016a. Mandat de la Commission « Data and Service Center for the Humanities » de l'Académie suisse des sciences humaines et sociales. *Data and Service Center for the Humanities (DaSCH)* [en ligne]. 4 juin 2016. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://www.sagw.ch/dms/sagw/unternehmen/dasch/Mandat-DaSCH-fr/Mandat%20DaSCH%20fr.pdf

ACADÉMIE SUISSE DES SCIENCES HUMAINES ET SOCIALES, 2016b. *Stratégie Open Access de l'Académie suisse des sciences humaines et sociales* [en ligne]. 23 septembre 2016. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.assh.ch/dms/sagw/open_access/Open-Access_Strategie_def_fr

ACADÉMIE SUISSE DES SCIENCES MÉDICALES, 2014. « Open Access » : pour un accès libre aux résultats de la recherche scientifique. *Swiss academies communications* [en ligne]. Vol. 9, n° 1. [Consulté le 14 novembre 2018]. Disponible à l'adresse : https://www.assm.ch/dam/jcr:4a725c9b-958e-45f6-9c4c-658e4ba88a8b/feuille_de_route_assm_open_access.pdf

BERNER FACHHOCHSCHULE. FACHGRUPPE BIBLIOTHEKEN, 2015. Strategische Ausrichtung der BFH - Bibliotheken als Informations -, Medien - und Lernzentren. In : *Bibliothèques BFH* [en ligne]. 25 novembre 2015. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.bfh.ch/fileadmin/docs/campus/bibliotheken/Strategiepapier_BFH-Bibliotheken.pdf

DLCM, 2016. *Research Data Management Policy Template : version 1.3* [en ligne]. S.l. : Swissuniversities septembre 2016. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.dlcm.ch/download_file/force/68/276

ETH ZÜRICH, 2008. ETH Zurich's Open-Access Policy. In : *Wissensportal ETH-Bibliothek* [en ligne]. juillet 2008. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.library.ethz.ch/en/ms/Open-Access-at-ETH-Zurich/ETH-Zurich-s-Open-Access-Policy

FACHINOTTI, Elena, GOZZELINO, Eva, LONATI, Sara, 2016. *Les bibliothèques scientifiques et les données de la recherche : défis et enjeux* [en ligne]. Carouge : Haute école de gestion de Genève. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://doc.rero.ch/record/258991

FRONTIERS, s.d. Author Guidelines. *Frontiers - Peer Rewieved Articles Journals* [en ligne]. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.frontiersin.org/about/author-guidelines

GAILLARD, Rémi, 2014. *De l'Open data à l'Open research data : quelle(s) politique(s) pour les données de recherche ?* [en ligne]. Master thesis. Lyon : Ecole Nationale Supérieure des Sciences de l'Information et des Bibliothèques. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://eprints.rclis.org/22746

HÄMMERLI, Bernhard (éd.), 2017. Comment gérer des données de manière sûre et durable ? [en ligne]. Académie suisse des sciences techniques [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/03_Cyber/SATW_Brochure_Cyber_FR.pdf

HES-SO, [sans date]. Open HES-SO. In : *HES-SO Haute école spécialisée de Suisse occidentale* [en ligne]. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.hes-so.ch/fr/open-hes-so-10501.html

HOCHSCHULE LUZERN, 2014. Reglement zur wissenschaftlichen Integrität und zur guten wissenschaftlichen Praxis. In : *Systematische Rechtssammlung - Hochschule Luzern* [en ligne]. 13 juin 2014. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.hslu.ch/-/media/campus/common/files/dokumente/h/ueber%20uns/systematische%20rechtssammlung/1%20hochschule%20luzern/h%20115%20reglement%20wissenschaftsethos.pdf?la=en

JAMBÉ, Carmen, 2015. *La gestion des données de recherche à l'Université de Lausanne : enjeux transdisciplinaires* [en ligne]. Carouge : Haute école de gestion de Genève. [Consulté le 14 novembre 2018]. Disponible à l'adresse : http://doc.rero.ch/record/258023

KILLIAS, Susan, CHAMBAZ, Marc, GOZEL, David et GUÉDON, Géraldine (éd.), 2018. Compliance guide : Code de bonnes pratiques. [en ligne]. Lausanne : EPFL, juin 2018. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://polylex.epfl.ch/files/content/sites/polylex/files/recueil_pdf/ComplianceGuideEPFL_FR.pdf

SALATHÉ, Michelle, 2008. L'intégrité dans la recherche scientifique : principes de base et procédures. [en ligne]. Académies suisses des sciences [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.akademien-schweiz.ch/dms/F/Publications/Directives_Recommandations/Integritaet/Directive.pdf

STAB WISSENSCHAFTSKOORDINATION, RECHTSDIENST, 2011. *Richtlinien für integrität in der Forschung = Guidelines for research integrity* [en ligne]. ETHZ, décembre 2011. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.ethz.ch/content/dam/ethz/main/research/pdf/forschungsethik/Broschure.pdf

SWISSUNIVERSITIES et FONDS NATIONAL SUISSE DE LA RECHERCHE SCIENTIFFIQUE, 2017. Stratégie nationale suisse sur l'Open Access. In : *Open access to publications - SNF* [en ligne]. 31 janvier 2017. [Consulté le 13 décembre 2018]. Disponible à l'adresse :

https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/Open_Access/Open_Access_strategy_final_f.pdf

UNIVERSITÄT BASEL, 2013. Open Access Policy of the University of Basel. In : [en ligne]. 19 mars 2013. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.ub.unibas.ch/fileadmin/redaktion/ub/publizieren/REGL_Open-Access-Policy_eng_20130419_pub.pdf

UNIVERSITÄT BERN, 2012. Regulations concerning scientific integrity. In : *Integrity - University of Bern* [en ligne]. 16 octobre 2012. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.unibe.ch/e1133/e2828/e38316/e38317/e50871/section50872/files251888/rgl_regulations_integrity_121016_ger.pdf

UNIVERSITÄT LUZERN, 2015. Reglementüber die wissenschaftliche Integrität in der Forschung und die gute wissenschaftliche Praxis an der Universität Luzern. In : *Personalgesetz, Verordnungen und Reglemente - Universität Luzern* [en ligne]. Dezember 2015. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://srl.lu.ch/frontend/versions/2607/download_pdf_file

UNIVERSITÄT LUZERN, 2016. Richtlinien zur Open Access Policy der Universität Luzern. In : *Personalgesetz und Reglemente - Universität Luzern* [en ligne]. 15 juin 2016. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.unilu.ch/fileadmin/universitaet/personal/pd/Reglemente_und_Richtlinien/Richtlinien_zur_Open_Access_Policy_der_Universitaet_Luzern.pdf

UNIVERSITÄT ST.GALLEN, 2007. Open Access Policy der Universität St.Gallen. In : *Universität St.Gallen* [en ligne]. 12 novembre 2007. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.unisg.ch/-/media/dateien/unisg/forschung/forschungsplattformalexandria/2007-11-12_unisg_open_access_policy.pdf

UNIVERSITÄT ST.GALLEN, 2008. Regulations concerning the Open Access Policy. In : *Universität St.Gallen* [en ligne]. 15 décembre 2008. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.unisg.ch/-/media/dateien/unisg/forschung/forschungsplattformalexandria/2008-12-15_university_st_gallen_regulations_open-access-policy.pdf

UNIVERSITÄT ST.GALLEN, 2015. Richtlinien zur Integrität wissenschaftlichen Arbeitens (Wissenschaftliche Integrität). In : *Universität St.Gallen* [en ligne]. 24 février 2015. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.unisg.ch/-/media/dateien/unisg/forschung/forschen-an-der-hsg/richtlinien-integrit%C3%A4t-wissenschaft20150224.pdf

UNIVERSITÄT ZÜRICH, 2017. UZH Policy. In : *Main library* [en ligne]. 21 novembre 2017. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.hbz.uzh.ch/en/open-access-und-open-science/open-access/policy.html

UNIVERSITÄTSBIBLIOTHEK BERN, 2017. Strategie 2017 - 2020. In : *Strategie 2017-2020 - Universität Bern* [en ligne]. 22 février 2017. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.unibe.ch/unibe/portal/content/e809/e962/e963/e6382/e6386/e552940/Strategie_A5_Web_ger.pdf

UNIVERSITÉ DE GENÈVE, 2009. Directive sur le dépôt et la diffusion des documents scientifiques dans l'Archive ouverte UNIGE. In : *Université de Genève* [en ligne]. 18 mai 2009. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://web.archive.org/web/20160914033857/http://www.unige.ch/biblio/openaccess/files/3814/3989/9799/Directive_Archive_ouverte_UNIGE.pdf

UNIVERSITÉ DE GENÈVE, 2012. Directive relative à l'intégrité dans le domaine de la recherche scientifique et à la procédure à suivre en cas de manquement à l'intégrité (Chercheurs-euses). In : *Mémento* [en ligne]. 12 avril 2012. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://memento.unige.ch/doc/0003

UNIVERSITÉ DE LAUSANNE, 2017. *Plan d'intentions de l'Université de Lausanne 2017 - 2021* [en ligne]. 9 mars 2017. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.unil.ch/central/files/live/sites/central/files/docs/plan_intentions_unil_17_21.pdf

UNIVERSITÉ DE LAUSANNE. DIRECTION, 2006. Intégrité scientifique dans le domaine de la recherche et procédure à suivre en cas de manquement à l'intégrité. In : *Directives internes de l'Université de Lausanne - Unil interne* [en ligne]. 1 septembre 2006. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://www.unil.ch/interne/files/live/sites/interne/files/textes_leg/4_rech/dir4_2_integrite_scientifique3.pdf

UNIVERSITÉ DE LAUSANNE. UNIRIS, 2014. *Politique de records management et d'archivage pour une gouvernance informationnelle* [en ligne]. 30 juin 2014. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://www.unil.ch/uniris/files/live/sites/uniris/files/documents/references/UNIL_POL_Records_management_archivage_VF.pdf

UNIVERSITÉ DE LAUSANNE. UNIRIS, 2017. Gestion des données de la recherche : feuille de route 2017-2021. *uniris.unil.ch/researchdata* [en ligne]. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://uniris.unil.ch/files/researchdata/image/UNIRIS-Infographie_Gestion17-21.png

ZHAW. BIBLIOTHEK, 2015. ZHAW Open Access Policy. In : *Publishing and Open Access - ZHAW University library* [en ligne]. 22 octobre 2015. [Consulté le 13 décembre 2018]. Disponible à l'adresse : https://gpmpublic.zhaw.ch/GPMDocProdZPublic/1_Management/1_04_Governance/1_04_01_Fuehrungsgrundlagen/Z_PY_Open_Access_Policy_ZHAW_engl.pdf

Gouvernance des données musicales électroniques

BAUMANN, Alexandre, 2015. *L'impact économique du téléchargement illégal sur le marché de la musique*. Paris : L'Harmattan. ISBN 23-430-5233-6

BERT, Jean-François, 2012 Un concert de métadonnées. *Arabesques* [en ligne]. Juillet - août - septembre 2012, n°67, pp. 14-17. [Consulté le 8 novembre 2018] Disponible à l'adresse : http://www.abes.fr/content/download/2378/10090/version/2/file/ABES+N67+sommaire.pdf

BOUTON, Rémi, 2011. L'enjeu des métadonnées musicales : la musique n'est pas qu'un fichier son. *Centre d'information et de ressources pour les musiques actuelles* [en ligne]. 4 avril 2011. [Consulté le 8 novembre 2018. Disponible à l'adresse : http://www.irma.asso.fr/L-ENJEU-DES-METADONNEES-MUSICALES

FANEN, Sophian, 2017. *Boulevard du stream : du MP3 à Deezer, la musique libérée*. [Bègles] : Le Castor Astral. ISBN 979-10-278-0133-6

FÉDÉRATION INTERNATIONALE DES ASSOCIATIONS DE BIBLIOTHÉCAIRES ET DES BIBLIOTHÈQUES, *Description bibliographique internationale normalisée des "non-livres" (ISBD for non-book material)* [en ligne], traduction française, 2010, [en ligne] disponible à l'adresse : http://www.bnf.fr/documents/Isbd_nbm.pdf

HAUPT, John, 2012. Spotify (review). *Notes* [en ligne]. Septembre 2012. Vol. 69, n° 1, pp. 132-138. [Consulté le 8 novembre 2018. Disponible à l'adresse : https://doi.org/10.1353/not.2012.0115

Loi relative au droit d'auteur sur les œuvres littéraires et artistiques, (loi n° 729 du 30 décembre 1960, modifiée en dernier lieu par la loi n° 1274 du 7 décembre 1995), 7.12.1995, [Suède], [trad. française]

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *eur-lex* [en ligne]. 27 avril 2016. [Consulté le 13 décembre 2018]. Disponible à l'adresse : http://eur-lex.europa.eu/eli/reg/2016/679/oj

ROBERGE, Marc-André, 2018. Titres d'œuvres, d'ouvrages et de périodiques. *Guide des difficultés de rédaction en musique* [en ligne]. 2 novembre 2018. [Consulté le 8 novembre 2018. Disponible à l'adresse : https://www.mus.ulaval.ca/roberge/gdrm/03-categ.htm

SPOTIFY, 2016, Conditions générales d'utilisation de Spotify. *Spotify.com* [en ligne], 1er novembre 2016. [Consulté le 8 novembre 2018. Disponible à l'adresse : https://www.spotify.com/ch-fr/legal/end-user-agreement/

SPOTIFY, 2018, Politique de confidentialité de Spotify. *Spotify.com* [en ligne]. 25 mai 2018. [Consulté le 8 novembre 2018. Disponible à l'adresse : https://www.spotify.com/ch-fr/legal/privacy-policy/

TANG, Muh-Chyun, YANG, Mang-Yuan, 2017. Evaluating Music Discovery Tools on Spotify: The Role of User Preference Characteristics. *Journal of Library and Information Studies* [en ligne]. Juin 2017. Vol. 15, n° 1, pp. 1-16. [Consulté le 8 novembre 2018. Disponible à l'adresse : https://jlis.lis.ntu.edu.tw/article/v15-1-1.pdf

WLÖMERT, Nils, PAPIES, Dominik, 2016. On-demand streaming services and music industry revenues: Insights from Spotify's market entry. *International Journal of Research in Marketing* [en ligne]. Juin 2016. Vol. 33, pp. 314-327. [Consulté le 8 novembre 2018. Disponible à l'adresse : https://doi.org/10.1016/j.ijresmar.2015.11.002

Conclusion

ACCART, Jean-Philippe, 2004. Le Sommet mondial sur la société de l'information : Caractéristiques et enjeux pour les professionnels de l'information. *Bulletin des bibliothèques de France (BBF)* [en ligne]. Novembre 2004. N° 6, pp. 68-73. [Consulté le 14 décembre 2018]. Disponible à l'adresse : http://bbf.enssib.fr/consulter/bbf-2004-06-0068-010