BYOD et innovations managériales en contexte hospitalier : mise en évidence d'une logique d'adoption inversée

BYOD and management innovations in a hospital context: highlighting a reversed adoption logic

Paméla Baillette et Yves Barlette

Édition électronique

URL : <https://journals.openedition.org/pmp/11563>
ISSN : 2119-4831

Éditeur

Institut de Management Public (IDPM)

Édition imprimée

Date de publication : 1 janvier 2018
Pagination : 49-68
ISBN : 978-2-7430-2415-4
ISSN : 0758-1726

Référence électronique

Paméla Baillette et Yves Barlette, « BYOD et innovations managériales en contexte hospitalier : mise en évidence d'une logique d'adoption inversée », *Politiques et management public* [En ligne], Vol 35/1-2 | 2018, mis en ligne le 13 novembre 2021, consulté le 15 novembre 2021. URL : <http://journals.openedition.org/pmp/11563>

BYOD et innovations managériales en contexte hospitalier : mise en évidence d'une logique d'adoption inversée

03

► **Paméla Baillette^{a*} et Yves Barlette^b**

^a Université de Perpignan Via Domitia,
Laboratoire de recherche MRM-Montpellier Recherche en Management

^b Montpellier Business School,
Laboratoire de recherche MRM-Montpellier Recherche en Management

Résumé

Cette recherche est centrée sur le BYOD-Bring Your Own Device, soit l'usage d'équipements mobiles personnels (ordinateurs portables, tablettes et smartphones) pour travailler. Le BYOD permet de travailler autrement, facilitant ainsi la génération d'innovations managériales. Pourtant, des risques existent, particulièrement en contexte hospitalier, car les données des patients sont des données sensibles. Cette recherche pose donc la question suivante : dans quelle mesure l'appréhension des risques et des opportunités du BYOD en contexte hospitalier peut-elle s'avérer source d'innovations managériales ?

Une analyse théorique est menée au regard des innovations managériales facilitées par le BYOD en intégrant les risques liés à ses pratiques. Au plan théorique, cette recherche souligne en particulier la logique d'adoption inversée des Technologies de l'Information (TI) liée au BYOD, en mettant en exergue le fait que les innovations managériales sont à la fois *facilitées* par les pratiques du BYOD et *induites* par la mise en place de solutions adaptées à leurs risques. Au plan managérial, la prise en compte des mutations auxquelles les hôpitaux sont soumis nécessite une réflexion en termes d'innovations via le BYOD capables de les aider à faire évoluer leurs pratiques et leurs politiques managériales.

© 2018 IDMP/Lavoisier SAS. Tous droits réservés

Mots clés : innovation managériale, hôpital, BYOD, logique d'adoption inversée, sécurité.

Abstract

BYOD and management innovations in a hospital context: highlighting a reversed adoption logic. This research focuses on BYOD-Bring Your Own Device, i.e. the use of personal devices (laptops, tablets and smartphones) in a professional context. BYOD

*Auteur correspondant : pamela.baillette@univ-perp.fr

doi :10.3166/pmp.35. 2018.0003 © 2018 IDMP/Lavoisier SAS. Tous droits réservés

offers the possibility of working differently and facilitates the generation of management innovations. However, BYOD involves security risks. These risks are particularly significant in hospitals, because patient data are sensitive. Consequently, the research question addressed is: to what extent may the apprehension of risks and opportunities of BYOD in a hospital context be a source of management innovations?

A theoretical analysis is conducted with regard to management innovations *facilitated* by BYOD, integrating the risks stemming from its *practices*. From a theoretical point of view, this research highlights specifically the IT reversed adoption logic related to BYOD, highlighting the fact that management innovations are both facilitated by BYOD-related practices and induced by the implementation of solutions addressing their related risks. From a practical point of view, taking into account the changes to which hospitals are confronted requires a reflection in terms of innovations via BYOD-related practices that can help them to change their practices and their management policies. © 2018 IDMP/Lavoisier SAS. Tous droits réservés

Keywords: management innovation, hospital, BYOD, reversed adoption logic, security.

Introduction

Le « *BYOD-Bring Your Own Device* » est un phénomène qui touche aujourd'hui la plupart des organisations. Il désigne l'usage d'outils mobiles personnels dans un contexte professionnel, soit l'utilisation d'ordinateurs portables, de tablettes tactiles et de téléphones mobiles appartenant aux salariés et utilisés par ces derniers aux plans privé et professionnel (Singh, 2012 ; Magruder *et al.*, 2015 ; Hovav et Putri, 2016 ; Weeger *et al.*, 2016).

Ce phénomène s'inscrit à l'intérieur d'une tendance de plus en plus affirmée de « consommation » des Technologies de l'Information (TI), c'est-à-dire l'adoption, dans un contexte de travail, des technologies du marché grand public (Harris *et al.*, 2011 ; Ortbach *et al.*, 2013 ; De Kok *et al.*, 2015 ; Mueller *et al.*, 2016). Le marché du BYOD ne cesse d'ailleurs de progresser dans le monde. Il valait en effet près de 76 milliards de dollars en 2013 et pourrait représenter quasiment 240 milliards de dollars en 2020, selon une étude réalisée par Grand View Research¹.

Pourtant, le BYOD présente des risques réels quant à la sécurité de l'information stockée dans les outils mobiles personnels. Ceci est dû à un manque de systèmes intégrés de protection de ces outils mis quotidiennement sur le marché, tout autant qu'aux comportements à risque des utilisateurs, davantage enclins à profiter des possibilités de ces outils qu'à en prévenir les risques (Dinev et Hart, 2006 ; Awad et Krishnan, 2006 ; Pras, 2012 ; Keith *et al.*, 2013 ; Sutanto *et al.*, 2013 ; Hérault et Belvaux, 2014).

En milieu hospitalier, où le BYOD se propage également (Moyer, 2013 ; Marshall, 2014 ; Keyes, 2014 ; Stephens *et al.*, 2017), ces risques sont d'autant plus importants qu'ils concernent tout particulièrement les données se rapportant aux patients. Considérées comme étant sensibles, ces données sont protégées par le Code de la santé publique. Pourtant, des fuites de données se manifestent parfois en provenance de centres hospitaliers français, notamment via l'accès par internet à des données confidentielles².

¹<http://www.grandviewresearch.com/press-release/global-bring-your-own-device>

²http://www.huffingtonpost.fr/barbara-bertholet/donnees-medicales-en-ligne_b_3162327.html

Il n'en reste pas moins que le BYOD offre des façons de travailler différentes, au-delà des frontières traditionnelles physiques et temporelles de l'organisation (Leclercq-Vandelannoite, 2014). La prise en compte réelle de ses risques induits dans les politiques hospitalières se traduit elle-même par de nouvelles façons de communiquer et de travailler. Dans un tel contexte, la génération d'innovations managériales, lesquelles comprennent le critère de nouveauté étendu à l'introduction de pratiques, de processus ou de techniques de management (Birkinshaw *et al.*, 2008), représente un intérêt manifeste. Ceci en particulier pour les hôpitaux aujourd'hui soumis à de profondes mutations induites par des exigences de rentabilité (Crémieux *et al.*, 2013 ; Bourret *et al.*, 2013 ; Bérard *et al.*, 2015 ; Valette *et al.*, 2015 ; Holcman, 2016) et qui les contraignent à innover (Djellal *et al.*, 2004 ; Djellal, 2014), en transformant leurs pratiques managériales au-delà de l'innovation thérapeutique ou technologique (Nobre, 2013a ; 2013b).

En considérant le manque de travaux menés à ce jour sur ces différents problèmes, ainsi que leur importance pour l'hôpital et pour les patients, la question de recherche posée ici est la suivante : dans quelle mesure l'appréhension des risques et des opportunités du BYOD en contexte hospitalier peut-elle s'avérer source d'innovations managériales ? Pour y répondre, cette recherche développe une analyse théorique fondée sur une revue de la littérature³. Cette analyse s'appuie sur les travaux existants, en combinant l'intérêt des pratiques du BYOD à l'hôpital et la nécessaire prise en compte de ses risques induits, pour la génération d'innovations managériales.

Au plan théorique, cette recherche met d'abord en évidence une logique nouvelle d'adoption des TI de façon à mieux comprendre les intérêts du BYOD relativement aux innovations managériales. Elle met ensuite en exergue le fait que les innovations managériales sont à la fois *facilitées* par les pratiques du BYOD et *induites* par la mise en place de solutions adaptées à leurs risques. Au plan managérial, la prise en compte des mutations auxquelles les hôpitaux sont soumis nécessite une réflexion en termes d'innovations capables de les aider à faire évoluer leurs pratiques et leurs politiques managériales. La recherche présentée ici propose une analyse orientée vers l'innovation managériale en détaillant les opportunités pratiques du BYOD face à ses risques, dans le contexte spécifique de l'hôpital, qui nécessite la protection de ses données et de celles de ses patients via le Code de la santé publique.

Dans une première partie, nous précisons les liens entre les pratiques du BYOD et les innovations managériales qu'elles facilitent, en nous appuyant plus spécifiquement sur le contexte hospitalier soumis actuellement à de profondes mutations. La seconde partie souligne l'importance de la prise en compte par l'hôpital des risques liés à ces pratiques ; cette prise en compte induisant elle-même de nouvelles façons de communiquer et de travailler.

1. BYOD et innovations managériales en contexte hospitalier

La génération potentielle d'innovations managériales par le BYOD suppose avant tout l'adoption par les utilisateurs de ses technologies. Les travaux en matière d'adoption des TI ont suscité de nombreuses recherches réalisées notamment par des spécialistes en management, des spécialistes de la cognition, de la communication et des économistes. De nombreux modèles

³ Voir la note méthodologique en annexe I.

coexistent tant au niveau de l'individu que de l'organisation. Dans cette recherche, nous nous centrons sur la question de l'adoption pour en examiner ses effets en termes d'innovations managériales, tout d'abord dans un contexte général, ensuite dans le milieu hospitalier spécifiquement.

1.1. Le BYOD, un cas particulier d'adoption des TI

Après avoir exposé les fondements classiques de l'adoption des TI, cette recherche s'intéresse à une logique récente, en particulier si elle est envisagée au travers de la rareté et de la nouveauté des travaux existants : la logique de l'adoption inversée.

1.1.1. La logique traditionnelle de l'adoption des TI

Traditionnellement, l'innovation technologique est perçue et analysée comme un processus descendant : elle est appréhendée et amorcée par les responsables informatiques et les spécialistes en TI dans les organisations. Dans ce cadre, l'adoption des TI, en tant que partie du processus d'appropriation, s'inscrit dans un mécanisme par lequel l'organisation décide de choisir et d'acquérir une technologie, pour la proposer, voire l'imposer, aux acteurs de l'organisation (Venkatesh *et al.*, 2003 ; Reix *et al.*, 2016). Il s'agit d'une décision d'investissement généralement planifiée et organisée par la hiérarchie. Elle est encadrée par des enjeux et des nécessités de retour sur investissement. Pourtant, la décision n'est pas toujours entière et rationnelle (Karoui et Dudezert, 2016 ; Dudezert et Portal, 2016) : elle peut être influencée par des effets de mode, des jeux de pouvoir et de lobby, des éléments affectifs. Le choix et l'acquisition dépendent ainsi en particulier d'une « vision organisante » exposée par Swanson et Ramiller (1997, 2004). Inspirés par le courant néo-institutionnaliste, ces auteurs considèrent que la décision d'adopter ou non la technologie est prise en étant orientée par une représentation ou idée focale sur la finalité de la TI et son déploiement, les conditions nécessaires à l'obtention de valeur ajoutée en utilisant cette TI, ou les changements organisationnels qu'elle suscite ; sachant que la représentation du sens à donner à la technologie, et à son usage, structure fortement les décisions prises autour de son choix et de ses modalités de déploiement (Karoui et Dudezert, 2016). La vision organisante constitue ainsi une « grille de lecture » de la technologie (Swanson et Ramiller 1997 ; Carton *et al.*, 2006) en induisant aussi bien la promotion et la légitimation d'une décision d'investissement que le ralentissement de l'adoption d'une TI par l'organisation (Karoui et Dudezert, 2016).

Le bénéfice retiré par l'organisation de l'adoption des TI dépend de ses membres quant à leur acceptation et leur appropriation des changements de pratiques de travail qui en découlent (Orlikowski et Hofman, 1997). Les travaux de recherche mobilisent les différentes théories largement utilisées en systèmes d'information comme la théorie de la diffusion (Rogers, 1962), les modèles d'acceptation des TI tels que TAM (Davis, 1989), UTAUT et UTAUT-2 (Venkatesh *et al.*, 2003, 2012), ou encore les modèles d'alignement stratégique (Henderson et Venkatraman, 1993 ; Tanriverdi *et al.*, 2010). Dans la mesure où l'adoption des TI est opérée par l'organisation, en l'occurrence sa direction en lien éventuellement avec des spécialistes en informatique, les utilisateurs sont amenés à assimiler des équipements qui leur sont « imposés » et avec lesquels ils doivent composer pour travailler.

Relativement aux outils mobiles, une illustration de cette logique traditionnelle d'adoption des TI est celle du CYOD-Choose Your Own Device, consistant pour l'organisation à choisir et à mettre à la disposition des salariés des outils mobiles professionnels (De Kok *et al.*, 2015 ;

Brodin, 2016), que ce soient des ordinateurs portables, des tablettes ou, de plus en plus, des téléphones mobiles. Dans ce cas, l'organisation est propriétaire des outils. Cela permet de limiter les risques liés à la sécurité des informations stockées dans ces outils ; notamment car l'organisation exerce un contrôle rigoureux sur un panel précis d'outils mobiles proposés aux salariés, qui de plus peuvent contenir des applications préinstallées et des systèmes de sécurité élaborés (mises en veille, mots de passe, antivirus, etc.). Pourtant, ces dispositifs soulèvent des questionnements quant à un double équipement pour les salariés avec des contraintes pratiques, et surtout des contraintes aux plans budgétaire et organisationnel pour l'organisation (investissement dans les outils, sécurisation, organisation de l'allocation des outils, etc.).

Ces contraintes sont amplifiées par la prolifération des outils personnels utilisés par les salariés en contexte professionnel, et par l'incitation plus ou moins explicite de certaines organisations auprès de leurs salariés à utiliser leurs propres matériels (Leclercq-Vandelannoitte, 2014).

1.1.2. BYOD et mise en évidence de la logique d'adoption inversée

On assiste actuellement à un phénomène dit de « *consommérisation* » des technologies mobiles dans les organisations (Harris *et al.*, 2012 ; Niehaves *et al.*, 2012 ; De Kok *et al.*, 2015 ; Weeger *et al.*, 2016). Ceci dans la mesure où certaines innovations technologiques tendent à s'imposer auprès du grand public avant de se diffuser dans les organisations. La consommérisation des TI se définit au plan professionnel comme étant l'adoption, dans un contexte de travail, des technologies du marché grand public par les employés (Harris *et al.*, 2011 ; Ortbach *et al.*, 2013).

Le BYOD, qui concerne l'usage d'outils mobiles personnels en contexte professionnel (Singh, 2012 ; Magruder *et al.*, 2015 ; Hovav et Putri, 2016 ; Weeger *et al.*, 2016), est précisément une réalisation de cette consommérisation des TI. On assiste de ce fait à la mise en place d'une « *logique d'adoption inversée* » ou « *reversed adoption logic* » (Leclercq-Vandelannoitte, 2014, 2015a, 2015b). Dans cette nouvelle logique (voir figure 1), et compte tenu de l'évolution des logiciels et des terminaux mobiles, l'usage de plus en plus autonome des équipements est devenu possible. Ceci grâce à la facilité d'utilisation de ces outils, combinée aux intérêts qu'offrent les nombreuses applications innovantes développées pour les outils mobiles (Cook *et al.*, 2013 ; Köffer *et al.*, 2015 ; Leclercq-Vandelannoitte, 2015b).

Le développement de cette autonomie permet aux utilisateurs d'être de moins en moins dépendants des directions informatiques pour l'adoption des outils utilisés en contexte professionnel. Partant « *les utilisateurs deviennent des décideurs, et des prescripteurs, pour les technologies matérielles et logicielles qu'ils utilisent* » (Reix *et al.*, 2016 : 30).

Le phénomène du BYOD, dont nous présentons une illustration dans la figure 1, provoque ainsi une inversion de la logique d'adoption des TI dans les organisations.

Figure 1 : Le BYOD : d'une adoption traditionnelle à une adoption inversée (inspiré des travaux de Leclercq-Vandelannoitte 2015a, 2015b)

On passe d'une trajectoire top-down (adoption traditionnelle) à une nouvelle trajectoire bottom-up (dite d'adoption inversée). Selon une logique facilitatrice, cette adoption inversée devient source de nombreuses innovations managériales.

1.2. Les innovations managériales découlant du BYOD

Le BYOD, via la logique d'adoption inversée, permet de favoriser les innovations managériales à un rythme plus soutenu que ne le permettrait l'adoption classique via les outils mis à la disposition des collaborateurs par l'organisation.

En effet, à travers leur volonté d'utiliser leurs équipements personnels pour travailler (Reix *et al.*, 2016), les collaborateurs procèdent à une adoption choisie de l'outil, puis à une utilisation volontaire de l'outil qu'ils ont eux-mêmes sélectionné et acquis avec leurs propres ressources financières. L'utilisation des équipements personnels, à la fois pour leur vie personnelle et pour travailler, permet aux collaborateurs de les assimiler plus facilement et par conséquent de les utiliser dans de meilleures conditions.

Les collaborateurs sont alors davantage susceptibles d'introduire des changements de pratiques dans leur organisation. Ils peuvent initier dans les organisations des changements capables d'améliorer, de revoir et de repenser certains de leurs processus (Leclercq-Vandelannoitte, 2014); ceci notamment grâce à l'utilisation d'applications à partir des équipements personnels, par exemple les applications de cartographie, de géolocalisation, ou des applications plus généralistes telles que Google Docs et Yahoo! Messenger, qui peuvent en outre servir les objectifs de l'entreprise en termes de performance dans le travail effectué.

Ces phénomènes apparaissent d'ailleurs amplifiés par le fait que certaines organisations laissent plus ou moins explicitement les salariés utiliser leurs propres matériels. On assiste ainsi à une sorte de délégation de l'adoption des outils utilisés par le personnel. Pour les directions d'organisations, les intérêts reposent en particulier sur la gestion de leurs ressources. En effet, le BYOD permet aux organisations de bénéficier de nombreuses innovations technologiques intégrées dans ces outils (Cook *et al.*, 2013; Köffer *et al.*, 2015). Ceci sans avoir besoin ni de les financer, ni de gérer leur fonctionnement. Dans ce contexte, si le BYOD ne représente pas une panacée, car il entraîne des risques, il permet de compenser certaines faiblesses de l'organisation en termes de ressources. Les bénéfices du BYOD reposent en effet sur la réduction des coûts pour l'organisation grâce à l'utilisation d'équipements appartenant aux employés, ainsi que sur une productivité améliorée grâce au traitement quasi instantané des dossiers et des emails (Miller *et al.*, 2012; Morrow, 2012; Singh, 2012).

Partant, si la question même de la réaction des organisations à ces nouvelles logiques d'adoption reste complexe (Gens *et al.*, 2011), il apparaît possible d'identifier différents comportements relativement à l'emploi par les collaborateurs de leurs propres équipements au travail. À travers plusieurs études de cas, Leclercq-Vandelannoitte (2014) identifie des réactions provenant des directions d'organisations. Parmi ces réactions, l'incitation, soit l'encouragement des collaborateurs, par la direction, à utiliser leurs outils personnels pour initier des changements technologiques et organisationnels dont ils sont eux-mêmes les porteurs, illustre particulièrement la possibilité offerte par la hiérarchie de générer des changements de pratiques grâce au BYOD.

En se focalisant sur les demandes et attentes des collaborateurs quant au désir d'utiliser leurs propres équipements, l'organisation encourage ces derniers à utiliser ouvertement

les outils de leur choix pour travailler, permettant ainsi d'introduire des changements de pratiques capables d'améliorer à la fois la performance des collaborateurs et celle de l'entreprise. De ce fait, les initiatives de certains collaborateurs peuvent générer des innovations de pratiques donnant aux organisations la possibilité de les formaliser, de les élargir, de les enrichir (ou au contraire de les inhiber) afin d'améliorer leurs processus et leur productivité (Leclercq-Vandelannoite, 2014).

Ces innovations de pratiques par le BYOD, en logique d'adoption inversée, font référence au concept d'innovation managériale. Ce concept apparaît d'ailleurs comme polymorphe et polysémique, et inclut de multiples réalités (Mignon *et al.*, 2017), ainsi qu'en témoignent les différents termes utilisés pour le nommer : innovation organisationnelle, administrative, changement organisationnel, etc.

Le concept d'innovation managériale a fait l'objet depuis le début des années 2000 d'une attention renouvelée et d'une redéfinition (Hamel, 2006 ; Mol et Birkinshaw, 2009 ; Le Roy *et al.*, 2013 ; Mignon *et al.*, 2017). Cette attention renouvelée a surtout visé à reconnaître la dimension immatérielle de l'innovation (Mignon et Walliser, 2015) et le caractère non technologique de la nouveauté introduite dans l'organisation (Damanpour, 2014). La troisième édition du Manuel d'Oslo (OCDE) de 2005 tient d'ailleurs particulièrement compte des progrès réalisés et analyse pour la première fois l'innovation non technologique et les liens entre les différents types d'innovation⁴. Dans cette mouvance, la littérature soutient l'idée que ces innovations, nouvellement considérées et largement sous-étudiées, seraient non seulement un vecteur essentiel du succès de nombreuses organisations, mais qu'elles permettraient également des avancées décisives en termes de performance (Hamel, 2006 ; Birkinshaw et Mol, 2006 ; Birkinshaw *et al.*, 2008 ; Mol et Birkinshaw, 2009 ; Damanpour et Aravind, 2012 ; Jaouen et Le Roy, 2013 ; Le Roy *et al.*, 2013 ; Dubouloz, 2014 ; Mignon *et al.*, 2017).

L'innovation managériale intègre tout particulièrement le critère de nouveauté en l'étendant à l'introduction de pratiques, de processus ou de techniques de management (Birkinshaw *et al.*, 2008). En ce sens, la nouveauté est entendue au sens large relativement à l'innovation managériale, laquelle peut être l'adoption par une organisation d'une pratique ou d'une méthode de management qui existe déjà mais qui est nouvelle par rapport à ses pratiques et méthodes de management actuelles (Le Roy *et al.*, 2013). La nouveauté de l'innovation est finalement liée à un écart relatif à des normes et à des pratiques traditionnelles généralement utilisées par les organisations ; ceci rejoint la conception de Birkinshaw et Mol (2006) et de Hamel (2006) pour lesquels l'innovation managériale relève de pratiques, de techniques de management ou de processus nouveaux, qui sont significativement différents des normes habituelles. Exprimé simplement, « *l'innovation managériale change la façon dont les managers font ce qu'ils font*⁵ » (Hamel, 2006 : 3).

Les nombreuses applications numériques constituent une illustration prégnante d'opportunité de développement des formes d'innovations managériales (Autissier *et al.*, 2016). Certaines applications permettent l'animation d'ateliers participatifs via des tablettes en lieu et place des tableaux blancs traditionnels et des post-it. Le support numérique permet une diffusion plus importante de ces nouvelles pratiques et offre la possibilité d'une propagation

⁴ <http://www.oecd.org/fr/science/inno/manueldosloprincipesdirecteursproposespourlerecueil etlinterpretationdesdonneesurlinnovationtechnologique2eedition.htm>

⁵ « *Put simply, management innovation changes how managers do what they do* » (Hamel, 2006 : 3).

massive. La logique des *apps*, correspondant à des applications accessibles directement à partir de son téléphone mobile, représente une opportunité pour ces nouvelles pratiques. Grâce à ces *apps*, il sera possible de coordonner des projets ou des services : finalement, l'appliquatif devient l'outil et la base de nouvelles formes de coopération entre les personnes et entre les organisations (Autissier *et al.*, 2016). En logique d'adoption inversée, nous rappelons que le BYOD permet une adoption choisie de l'outil, suivie d'une utilisation volontaire capable d'entraîner une meilleure assimilation de ses fonctionnalités (Venkatesh *et al.*, 2003). Le BYOD facilite de ce fait les innovations managériales.

Le milieu hospitalier est particulièrement concerné par le phénomène du BYOD et devient donc le siège de nombreuses innovations managériales. Ces innovations sont d'autant plus importantes à considérer que l'hôpital, mû par des logiques de rentabilité (Crémieux *et al.*, 2013 ; Bourret *et al.*, 2013 ; Bérard *et al.*, 2015 ; Valette *et al.*, 2015 ; Holcman, 2016), est amené à innover en transformant ses pratiques managériales (Djellal *et al.*, 2004 ; Djellal, 2014), dépassant ainsi l'innovation thérapeutique ou technologique (Nobre, 2013a ; 2013b).

1.3. La génération d'innovations managériales en contexte hospitalier

Suivant la tendance à la consumérisation des TI, les pratiques liées au BYOD se développent aussi en milieu hospitalier (Moyer, 2013 ; Marshall, 2014 ; Keyes, 2014 ; Stephens *et al.*, 2017). Au travers du prisme théorique de l'adoption inversée, cette recherche a mis en évidence le fait que les outils personnels (BYOD) favorisent davantage les innovations managériales que les outils mobiles proposés par l'organisation, car non seulement ils sont mieux maîtrisés et présentent de nombreux atouts pour les salariés, mais de plus, ils constituent un palliatif des lacunes organisationnelles. En milieu hospitalier particulièrement, la lourdeur administrative des hôpitaux, le manque de ressources financières et le taux de rotation du personnel médical⁶ limitent l'investissement via les politiques hospitalières dans des outils mobiles, ce qui renforce la motivation des acteurs à utiliser leurs propres outils (Ciborra, 2002 ; Ferneley et Bell, 2006).

Le développement du BYOD présente des intérêts, tout spécifiquement dans ce milieu, pour favoriser des innovations managériales, grâce à une adoption choisie de leurs outils personnels, par les salariés de l'hôpital. Motulsky *et al.* (2017) exposent par exemple le cas d'une application innovante déployée via les outils mobiles personnels des salariés d'un hôpital pour fournir une vue des données des patients et entrer de courtes notes. L'expérience a mobilisé 253 professionnels hospitaliers d'octobre 2013 à mars 2015 dans les unités de soins intensifs pédiatriques et néonataux avec une médiane de 26 notes saisies par utilisateur et par jour. Les résultats obtenus via un questionnaire de satisfaction ont permis de constater pour 57 % des répondants une amélioration des soins aux patients grâce à cette application innovante. De plus, la plupart des répondants (86 %) a souhaité continuer à l'utiliser. C'est ainsi que cette application innovante, destinée initialement à aider le personnel à gérer une partie des dossiers via leur téléphone mobile personnel, a finalement été adaptée aux pratiques locales et élargie pour gérer les dossiers plus formellement.

⁶ L'ATIH-Agence Technique de l'Information sur l'Hospitalisation indique pour 2014 un taux de rotation (sur 352 établissements) de 23,3 % pour le personnel médical. Source : <http://www.atih.sante.fr/thematique/ressources-humaines>

Du fait de cette adoption choisie d'outils personnels, les pratiques du BYOD facilitent la génération d'innovations managériales à l'hôpital. Ces pratiques créent en effet un nouvel environnement professionnel empreint de plus de souplesse, de liberté, et surtout de réactivité pour les acteurs hospitaliers confrontés à la gestion de l'urgence auprès des malades, tout autant qu'aux limitations budgétaires affectant notamment les investissements dans les outils mobiles qui n'entrent généralement pas dans les priorités stratégiques de l'hôpital.

Plus encore, dans ses travaux menés en contexte hospitalier, Marshall (2014) révèle l'influence favorable du BYOD sur la performance du travail réalisé. Par exemple, les médecins ne sont plus obligés de revenir à leur bureau pour travailler depuis l'ordinateur fixe de l'hôpital, ce qui réduit la probabilité de retards dus à des interruptions, des appels d'urgence, etc. Également, maîtrisant bien leur mobile personnel, ils peuvent instantanément approuver des tests, en commander eux-mêmes, et ainsi minimiser à la fois le temps d'attente des patients, particulièrement ceux en situation d'urgence médicale, et celui des infirmiers(ères). Plus encore, l'accès à l'information en temps réel stockée dans leur mobile peut également leur assurer la possibilité de disposer des données les plus récentes de façon à améliorer l'efficacité des décisions prises. Du côté des patients, ces appareils ont également de l'intérêt, car il est de ce fait possible de leur montrer des images actualisées dans un délai très court, de façon à ce qu'ils comprennent mieux leur état présent. Harris *et al.* (2011 : 102) exposent quant à eux le cas d'un hôpital canadien signalant l'utilisation innovante par une infirmière de l'appareil photo de son propre téléphone mobile générant une réduction des coûts, l'amélioration des soins aux patients et la baisse du sentiment de frustration du personnel médical, par exemple grâce à des photos montrant le travail réalisé sur des plaies.

Si le BYOD peut favoriser l'apparition d'innovations managériales en milieu hospitalier, il génère aussi des risques supplémentaires, d'autant plus préoccupants s'ils ne sont pas pris en compte dans les politiques hospitalières, que l'on touche aux données des patients, considérées comme sensibles.

2. Innovations managériales et prise en compte des risques liés au BYOD

Les risques générés par les pratiques du BYOD sont d'abord énoncés au regard de la sécurité de l'information qui transite via les outils mobiles personnels. Cette recherche se focalise ensuite sur les risques spécifiques liés à la sécurité des données des patients à l'hôpital. Elle souligne enfin l'intérêt pour l'hôpital de les prendre en compte pour protéger ces données, ce qui induit de nouvelles façons de communiquer et de travailler.

2.1. Les risques pour les organisations induits par le BYOD

Les évolutions rapides des pratiques du BYOD génèrent des changements réels dans la conception et l'exécution du travail dans les organisations. Elles suscitent cependant des inquiétudes sérieuses relativement à la sécurité de l'information découlant de ces pratiques (Reix *et al.*, 2016 ; Hovav et Putri, 2016). Ces risques accrus de sécurité de l'information font partie des défis les plus importants à relever quant aux programmes BYOD (Ansaldi, 2013) car les spécialistes de la sécurité considèrent le BYOD comme l'une des plus grandes menaces pour la sécurité des informations (Timms, 2017).

La sécurité dont il est fait état ici correspond à l'intégrité, à la disponibilité et à la confidentialité des informations. La *disponibilité* fait référence au fait que les informations doivent être accessibles au moment où l'organisation en a besoin. L'utilisation des appareils personnels pour travailler augmente également le risque pour l'outil d'être perdu ou volé (Jones et Chin, 2015). L'*intégrité* concerne le fait que les informations ne soient pas effacées ou altérées. Un défaut de disponibilité ou d'intégrité peut s'avérer catastrophique car il entraîne souvent une perte de chiffre d'affaires et peut même conduire à une interruption de la continuité d'affaires. La *confidentialité* renvoie à l'interdiction d'accès aux informations par des personnes ou par des systèmes non autorisés. Un défaut de confidentialité affectant les informations manipulées par les organisations va avoir deux conséquences majeures : la première concerne les secrets d'affaires de l'entreprise (stratégie, R&D, projets, etc.), ce qui va pouvoir porter atteinte à sa réputation ou bien avoir un impact négatif sur sa position concurrentielle (Sangani et Vijaykumar, 2012). La deuxième peut conduire à un dépôt de plainte : en effet, une part importante des informations va concerner les employés et les clients, qui peuvent demander réparation en cas de divulgation de leurs données personnelles à des tiers sans leur consentement (Hong et Thong, 2013).

La sécurité relative au BYOD correspond à un marché très prometteur : Allied Market Research indique en effet que cette industrie pourrait atteindre 24,6 milliards de dollars d'ici 2020⁷. La sécurité de l'information peut en particulier être affectée au niveau de l'organisation car les équipements personnels créent un nouveau potentiel de violations de sécurité (Baillette et Barlette, 2016, 2017). En effet, dans le cas de l'adoption du BYOD par les salariés d'une organisation, de nombreux facteurs de risques supplémentaires vont apparaître : une perte de contrôle du fait d'une possession des outils transférée aux salariés, des téléphones mobiles attractifs pour les cybercriminels, des ouvertures du réseau informatique de l'organisation difficiles à contrôler, et finalement des risques accrus de perte par les employés de leurs outils personnels entraînant des conséquences néfastes pour les organisations.

Tout d'abord, l'organisation va perdre une part du contrôle de la gestion de sa sécurité, car les outils sont désormais la propriété des employés. Ces outils contiennent des applications personnelles qui peuvent entraîner des accès spécifiques aux données sur l'outil de l'employé, incluant les données de l'organisation. De plus, les comportements des employés utilisant leurs outils personnels sont souvent plus risqués que ceux impliquant des outils appartenant à l'entreprise (Hovav et Putri, 2016), d'autant qu'ils utilisent ensuite ces mêmes outils à leur domicile. Pourtant, contrôler l'utilisation des outils personnels des employés s'avère plus complexe, et *a fortiori* le fait de demander aux employés de respecter les règles ou politiques de sécurité de l'organisation (Hovav et Putri, 2016). Ce problème est d'autant plus inquiétant que 71 % des organisations qui autorisent le BYOD n'ont pas mis en place de politiques ou de procédures spécifiques au BYOD pour assurer leur sécurité (Ansaldi, 2013), ce qui s'explique en partie par le manque de guides concernant les bonnes pratiques ou les procédures à mettre en place.

Deuxièmement, les outils BYOD les plus répandus sont les smartphones, qui sont devenus une cible lucrative pour les cybercriminels : les infections de smartphones se sont accrues de 400 % en 2016 (Nokia, 2016). Ainsi, les outils personnels créent de nouvelles failles

⁷ <https://www.alliedmarketresearch.com/press-release/global-BYOD-security-market-is-expected-to-reach-24-6-billion-by-2020-allied-market-research.html>

de sécurité. Les informations de l'organisation peuvent être corrompues par des attaques provenant d'un smartphone piraté ou infecté par un logiciel malveillant tel qu'un virus et de plus en plus par des logiciels rançonneurs⁸. Ces derniers ont représenté la plus importante menace pour les organisations en 2016 (Malwarebytes, 2017). De plus, les outils mobiles contenant des logiciels non à jour sont de plus en plus la source de failles de sécurité.

Troisièmement, l'utilisation du cloud computing se développe au travers du BYOD, principalement pour accéder à de gros espaces de stockage et à des applications en ligne au travers d'un navigateur internet, ce qui va aussi occasionner de nouvelles failles de sécurité (Morrow, 2012). De plus, les outils mobiles des employés peuvent se connecter à de nombreux types de réseaux (3G-4G, Wi-Fi, Bluetooth, etc.), rendant ainsi la sécurisation du réseau de l'organisation encore plus complexe.

Enfin, le fait que les employés utilisent leur outil personnel à la fois sur le lieu de travail et dans le cadre personnel (chez soi, en déplacement, en congés, etc.) est source de risques accrus de perte de ces outils personnels, ce qui va entraîner des possibilités d'accès aux données figurant sur les outils, mais aussi constituer des ouvertures pour des accès distants à l'organisation. Ceci va s'ajouter aux vulnérabilités des informations de l'organisation, en incluant des informations potentiellement très sensibles (CNIL, 2010). Les informations seront aussi mises en danger quand le salarié va quitter l'entreprise après un renvoi ou un départ à la retraite, sans avoir effacé de son outil personnel les informations de son organisation.

La sécurité représente donc bien un problème majeur, à la fois au plan de la protection des données organisationnelles et à celui des données personnelles manipulées par les organisations. En intégrant des innovations technologiques régulièrement renouvelées, le BYOD évolue vite : s'il génère des mutations réelles dans les pratiques de travail et facilite les innovations managériales en logique d'adoption inversée, il expose les organisations et les personnes à de nouvelles vulnérabilités et à des violations potentielles de la sécurité. Ces risques accrus vont prendre une autre mesure dans le milieu hospitalier, où les données des patients constituent des données sensibles.

2.2. Les risques découlant du BYOD pour la sécurité des données des patients en milieu hospitalier

Les applications de santé et les objets connectés s'intègrent petit à petit dans les établissements de santé. Dans la plupart des cas, ce sont les acteurs hospitaliers eux-mêmes qui impulsent le mouvement en utilisant leurs propres équipements nomades. Pourtant, les données des patients ne sont pas des données comme les autres et ces pratiques soulèvent des questions à différents niveaux. Comme le souligne Marshall (2014 : 14), malgré les avantages potentiels, tant pour l'organisation que pour les acteurs hospitaliers, l'utilisation des dispositifs appartenant à ces derniers soulève des questions liées à la sécurité, à la gouvernance, aux processus et même à la culture de l'organisation. Ou encore, selon le même auteur (2014 : 15), il apparaît un certain nombre de défis à surmonter quand les employés utilisent leurs propres outils, y compris des problèmes de sécurité, de compatibilité et de partage des données.

⁸ Un *logiciel rançonneur* va empêcher ou limiter l'accès aux données à un système informatique, soit en verrouillant l'écran de l'outil, soit en cryptant l'accès aux données, à moins qu'une rançon ne soit payée par l'utilisateur.

Il existe des risques importants quant à la protection des données des patients, en particulier dans les hôpitaux (Cher *et al.*, 2017), car ces données sont considérées comme étant des données sensibles au sens de la CNIL. Leur utilisation est donc très encadrée⁹. L'accès possible aux données des patients et leur diffusion constituent un risque majeur, et accru du fait des pratiques découlant du BYOD qui soulèvent des problèmes à la fois éthiques et juridiques. Ces risques sont d'autant plus prégnants que l'ouverture et le partage d'informations sous différentes formes de supports connectés représentent un phénomène qui prend de l'ampleur via la numérisation de nombreux processus et données : par exemple, les résultats d'examens diffusés en ligne ou les rappels de rendez-vous par sms. Les médias relaient ce problème auprès du grand public avec par exemple la mise en évidence de fuites de données des patients concernant une quarantaine de Centres Hospitaliers Français¹⁰, ou encore l'accès via Internet à une centaine de données confidentielles relatives aux patients¹¹.

Juridiquement pourtant, la confidentialité des données de santé est protégée aussi bien par le secret médical que par les règles de protection des données personnelles. Ainsi, en vertu de l'article L1110-4 du Code de la santé publique : « *Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations le concernant* ».

Les établissements de santé sont donc dans l'obligation de prendre toutes les précautions nécessaires pour que des tiers non autorisés ne puissent avoir accès aux données des patients. Cette obligation de sécurité est posée par l'article 34 de la loi informatique et libertés du 6 janvier 1978 modifiée¹². La CNIL est chargée d'effectuer des contrôles quant à la satisfaction par les établissements de santé de cette obligation. Le processus comprend en premier lieu une mise en demeure qui est parfois rendue publique si le cas s'avère particulièrement grave. Si l'organisation de santé ne se met pas en conformité, la CNIL prononce finalement une sanction, ou bien clôture la procédure dans le cas inverse.

La CNIL cite par exemple le cas d'un centre hospitalier ayant accordé l'accès à l'un de ses prestataires informatiques aux dossiers médicaux de plusieurs centaines de patients, en méconnaissance des dispositions du Code de la santé publique et de la loi informatique et libertés relatives au respect de la vie privée des patients ainsi qu'à la sécurité de leurs données médicales. Dans un communiqué du 17 octobre 2013, la CNIL a annoncé que le centre hospitalier contrôlé s'était finalement mis en conformité¹³. Ceci grâce à la mise en œuvre de mesures comme la suppression de l'accès par le prestataire informatique aux dossiers médicaux des patients, lesquels demeurent désormais sous la responsabilité du

⁹ <https://www.cnil.fr/fr/cnil-direct/question/424>

¹⁰ <https://www.datasecuritybreach.fr/fuite-de-donnees-concernant-une-quarantaine-de-centres-hospitaliers-francais/>

¹¹ http://www.huffingtonpost.fr/barbara-bertholet/donnees-medicales-en-ligne_b_3162327.html

¹² <https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee>

¹³ Délibération CNIL n° 2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo, et Communiqué CNIL intitulé "Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo" du 17 octobre 2013.

médecin en charge de l'information médicale de l'établissement, ainsi qu'à la formalisation d'une politique stricte de sécurité des systèmes d'information.

Néanmoins, au regard des spécificités exposées, la gestion des pratiques liées au BYOD apparaît particulièrement essentielle en milieu hospitalier ; ceci permettant de limiter les risques du BYOD en générant aussi de nouvelles façons de communiquer et de travailler.

2.3. Innovations managériales induites par les risques du BYOD en milieu hospitalier

Marshall (2014) liste cinq défis majeurs à relever dans le domaine médical en liaison avec le BYOD : (1) l'atteinte à la sécurité avec le risque de violation des données confidentielles des patients ; (2) la gouvernance nécessaire du BYOD avec des protocoles standardisés et des lignes directrices claires ; (3) la législation stricte en matière de santé avec l'observation nécessaire des règles ; (4) la limitation et l'encadrement des pratiques liées au BYOD, avec par exemple le choix des types d'appareils qu'il est possible de connecter avec ceux de l'hôpital ; (5) la limitation de la dépendance à Internet afin de pouvoir réagir en cas d'urgence auprès des patients.

Pour relever ces défis, il apparaît nécessaire pour la direction de l'hôpital de considérer un ensemble de critères tels que le contexte de l'hôpital, ses choix en matière d'investissement, de gestion des coûts et surtout de sécurité ; d'autant plus que chaque hôpital a des besoins, des ressources et des capacités différentes (Moyer, 2013).

Au-delà, l'aspect humain constitue un critère majeur, par l'importance qu'il s'agit d'accorder dans les politiques hospitalières à l'adaptation des outils aux besoins du personnel (De Kok *et al.*, 2016). La question se pose finalement de savoir si une interdiction du BYOD dans les hôpitaux serait bien réaliste, dans la mesure où ses outils sont déjà largement adoptés et utilisés fréquemment au cours de la journée de travail par les acteurs hospitaliers.

D'où l'importance d'une réflexion menée, ou à envisager de mener, dans les politiques hospitalières sur les mesures possibles pour limiter les risques liés au BYOD. En ce sens, les grandes entreprises de l'édition logicielle (Google et Microsoft en particulier) travaillent actuellement sur le développement d'offres dites « globales », en définissant des systèmes d'exploitation permettant de séparer les utilisations, privées ou professionnelles, et en créant des logiciels de gestion de la sécurité des outils mobiles utilisés en mode BYOD. Ces offres en émergence visent d'une part à assurer la sécurité des outils personnels des salariés sans porter atteinte à la sécurité et à la confidentialité de leurs données personnelles ; et d'autre part à mieux sécuriser les informations « professionnelles » (les informations sensibles touchant aux patients, dans ce contexte), de façon à satisfaire les attentes à la fois privées et organisationnelles.

Il n'en reste pas moins qu'il est difficile de forcer les acteurs hospitaliers à se conformer à la politique de sécurité de l'hôpital, en étant soumis à des obligations, surtout quand il s'agit d'outils dont ils sont propriétaires (Hovav et Putri, 2016). Il peut aussi arriver que le logiciel de sécurité installé sur leur appareil personnel soit restrictif. Dans ce cas, les dispositifs personnels ne sont pas autorisés à se connecter au réseau de l'entreprise, ce qui signifie que les employés peuvent seulement accéder à un réseau restreint « invités » à partir de leur outil personnel (De Kok *et al.*, 2015).

La facilitation des innovations managériales via le BYOD, aménagé ou non par ces nouvelles offres « globales », passe alors par une observation fine des comportements en interne, et par une entente réciproque des acteurs hospitaliers avec la direction de l'hôpital et la direction des systèmes d'information-DSI.

En ce sens, les mesures à prendre en termes de politiques hospitalières ne sont pas uniquement techniques. Elles relèvent à la fois de l'organisation et du contrôle. Elles dépassent les attributions des spécialistes en SI et concernent directement le management de l'hôpital. Pour cela, une réflexion organisationnelle doit être menée (Barlette, 2008 ; Brodin, 2016) et comporter une sensibilisation et une formation des acteurs hospitaliers. Partant, la sécurité ne réussit que par le biais d'une modification des attitudes et des comportements : *« il est nécessaire que chaque membre de l'organisation soit convaincu de l'importance du problème stratégique qu'est celui de la sécurité de l'information, problème qui englobe et dépasse largement celui de la seule sécurité du fonctionnement des systèmes d'information »* (Reix *et al.*, 2016 : 448).

En milieu hospitalier, le but est d'introduire collégialement et de manière formelle, avec un accompagnement aussi bien au plan humain que juridique, une culture de confidentialité des informations numérisées adaptée au BYOD. En effet, les acteurs hospitaliers ont souvent une forte culture de la confidentialité au sujet des risques de divulgation sous forme écrite ou orale, mais cette culture reste souvent insuffisante au plan des informations numérisées (Barlette, 2008), du fait d'une nature des informations plus « impersonnelle » et « virtuelle » (Harrington, 1996).

Dans les politiques hospitalières, l'évolution de cette culture pourra passer par la mise en place de campagnes de sensibilisation des acteurs hospitaliers, incluant notamment les managers, vecteurs majeurs de l'implication de tous dans la diffusion des bonnes pratiques (Barlette, 2012). En parallèle à ceci, la signature d'une charte (Harrington, 1996) spécifique au BYOD s'avère indispensable, tout particulièrement en milieu hospitalier. Cette charte doit préciser les risques particuliers découlant de ce type d'utilisation des outils mobiles personnels, et permet de préciser les responsabilités ainsi que les cas spécifiques, par exemple les mots de passe à renforcer, les mises à jour, les solutions en cas de perte ou de panne de l'outil, etc.

En ce sens, la prise en compte réelle des risques importants du BYOD à l'hôpital génère des modifications dans les façons de travailler et de communiquer entre les différents acteurs de l'hôpital, i.e. la direction, les informaticiens et les praticiens, afin d'améliorer la performance globale de ce type d'organisation, ce qui se traduit par une innovation managériale provoquée ou induite. Rappelons que les hôpitaux doivent actuellement faire face à de profondes mutations, engendrées par des logiques de rentabilité, qui les obligent à innover en transformant leurs pratiques managériales, au-delà de l'innovation thérapeutique ou technologique.

La synthèse de cette recherche théorique, dont nous présentons une illustration dans la figure 2, permet de mettre en évidence deux types d'effets générés par le BYOD sur les innovations managériales.

Figure 2 : Les effets du BYOD sur les innovations managériales

En termes d'innovations managériales, l'adoption inversée des TI via le BYOD provoque des effets facilitateurs, mais aussi des effets induits en raison de la gestion nécessaire des risques liés à ces pratiques.

Conclusion

Considérant la logique d'adoption inversée des TI, cette recherche fondée sur une synthèse de l'état de l'art a permis d'exposer l'intérêt des pratiques liées au BYOD pour travailler autrement et faciliter la génération d'innovations managériales. Au regard de leur volonté d'utiliser leurs équipements personnels pour travailler, il a été rappelé que les acteurs procèdent à une adoption choisie de l'outil qu'ils ont acquis avec leurs propres ressources financières. Pourtant, en contexte hospitalier particulièrement, ces pratiques augmentent les risques d'atteintes à la confidentialité des données des patients, ce qui entraîne des conséquences principalement éthiques et juridiques. Dans ce contexte, le rôle essentiel de la direction de l'hôpital a été mis en évidence pour prendre tout particulièrement en compte ces risques dans ses politiques, par la mise en place de solutions adaptées, ce qui se traduit par une innovation managériale provoquée ou induite via de nouvelles façons de communiquer et de travailler.

Plusieurs limites peuvent être identifiées dans cette recherche. Elles portent d'abord sur les limites inhérentes à un travail théorique. Il s'agira de compléter et d'enrichir cette recherche par des études menées sur le terrain en contexte hospitalier. Les limites de cette recherche portent également sur l'étendue des risques exposés quant à la sécurité des informations découlant du BYOD. Il a majoritairement été fait référence aux risques éthiques et juridiques en lien avec la littérature existante. Or d'autres risques interviennent aussi, de nature principalement économique, managériale et sociologique, qu'il s'agira d'identifier et d'étudier sur le terrain. Partant, une piste intéressante de recherche future préciserait les réactions des directions d'hôpitaux à ces pratiques du BYOD et à leurs risques en termes de politiques, ainsi que les actions engagées par les acteurs hospitaliers relativement à ces pratiques. Ceci afin de faciliter les innovations managériales en lien avec les innovations technologiques, et répondre ainsi aux nouvelles logiques engagées dans le secteur hospitalier.

Les principales contributions théoriques portent sur la mise en lumière de la « *logique d'adoption inversée* » des TI (face à la logique traditionnelle d'adoption) permettant de laisser librement les acteurs hospitaliers choisir puis utiliser volontairement les fonctionnalités de leurs outils, pour faciliter les innovations managériales, notamment quand l'organisation a des difficultés pour fournir les outils nécessaires. Cette nouvelle logique entraîne des risques auxquels l'hôpital doit faire face dans ses politiques, ce qui induit des innovations managériales. Ainsi, la mise en évidence d'innovations managériales d'une part *facilitées* par les pratiques du BYOD et d'autre part *induites* par la mise en place de solutions adaptées à leurs risques, représente également un intérêt théorique modélisé dans la figure 2.

Au plan managérial, il est utile pour les hôpitaux de considérer ces phénomènes, dans la mesure où ils sont soumis aujourd'hui à de profondes mutations. La nécessité de mettre en œuvre de nouvelles méthodes de travail, en prenant en compte l'adaptation des outils aux besoins des salariés, constitue une clé d'entrée pour aider les hôpitaux à innover en transformant leurs pratiques et politiques managériales. Cette transformation devra aussi

s'accompagner d'une évolution de la culture organisationnelle qui permette aux organisations de protéger leurs informations et celles de leurs patients en profitant des innovations managériales ainsi générées en milieu hospitalier.

Bibliographie

- Ansaldi H., 2013. Addressing the Challenges of the "Bring Your Own Device" Opportunity. *The CPA Journal*, novembre, 62-65.
- Autissier D., Johnson K.J., Moutot J.M., 2016. L'innovation managériale : rupture ou évolution du management. *Question(s) de management* 2 (13), 25-33.
- Awad N.F., Krishnan M.S., 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly* 30 (1), 13-28.
- Baillette P., Barlette Y., 2016. Identification of the "Security Paradox" in SMEs: Application to BYOD-Related Practices. *Pre-ICIS Workshop on Information Security and Privacy (WISP)*, 10 december, Dublin, Irlande.
- Baillette P., Barlette Y., 2017. Security Paradox Situations Related to the BYOD Phenomenon in SMEs: Insights from the Coping Model of User Adaptation. *22e Conférence de l'AIM - Association Information et Management*, 19 mai, Paris.
- Barlette Y., 2008. Une étude des comportements liés à la sécurité des systèmes d'information en PME. *Systèmes d'Information et Management* 13 (4), 7-30.
- Barlette Y., 2012. Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME. *Systèmes d'Information et Management* 17 (2), 115-149.
- Bérard, E., Flachère, I., Saulpic, O., Zarlowski, P., 2015. Les outils financiers dans les hôpitaux : penser leur déploiement au-delà de la dimension technique. *Journal de gestion et d'économie médicales* 33 (7), 409-427.
- Birkinshaw J., Mol M.J., 2006. How Management Innovation Happens. *Sloan Management Review* 47 (4), 81-88.
- Birkinshaw J., Hamel G., Mol M.J., 2008. Management Innovation. *Academy of Management Review* 33 (4), 825-845.
- Bourret R., Martinez E., Vert M., Vernhet A., Naro G., 2013. La certification des comptes des hôpitaux publics à l'horizon 2014 : un état de l'art au travers du témoignage du CHRU de Montpellier. *Politiques et Management Public* 30 (4), 571-581.
- Brodin M., 2016. BYOD vs. CYOD: What is the Difference? *9 th IADIS International Conference Information Systems 2016*. IADIS Press, 55-62.
- Carton S., De Vaujany F.-X., Perez M., Romeyer C., 2006. Vers une théorie de l'appropriation des outils de gestion informatisés : une approche intégrative. *Management & Avenir* (9), 159-179.
- Ciborra C., 2002. *The Labyrinths of Information: Challenging the Wisdom of Systems*. Oxford University Press, Oxford.
- CNIL, 2010. *Guide. La sécurité des données personnelles*. https://www.cnil.fr/sites/default/files/typo/document/Guide_securite-VD.pdf, (accédé le 8 mars 2018).
- Cook T., Jaramillo D., Katz N., Bodin W., Cooper S., Becker C., Smart R., Lu C., 2013. Mobile Innovation Applications for the BYOD Enterprise User. *IBM Journal of Research and Development* 57 (6), 6-10.
- Crémieux F., Saulpic O., Zarlowski P., 2013. Comment diffuser une logique médico-économique à l'hôpital ? Éléments d'analyse et propositions à partir d'une étude de cas *In t. Noble, L'innovation managériale à l'hôpital : 14 cas de mise en œuvre*, Dunod, Paris, 167-182.
- Damanpour F., 2014. Footnotes to Research on Management Innovation? *Organization Studies* 35 (9), 1265-1285.
- Damanpour F., Aravind D., 2012. Managerial Innovation: Conceptions, processes, and antecedents. *Management and Organization Review* 8 (2), 423-454.

- Davis F.D., 1989. Perceived Usefulness, Perceived Ease of Use, and user Acceptance of Information Technology. *MIS Quarterly* 13 (3), 319-340.
- De Kok A., Lubbers Y., Helms R.W., 2015. Mobility and Security in the New Way of Working: Employee Satisfaction in a Choose Your Own Device (CYOD) Environment. *Information Systems in a Changing Economy and Society, 9th MCIS-Mediterranean Conference on Information Systems*, Greece, 73-92.
- De Kok A., Van Zwieten J., Helms R., 2016. Attitude towards NWOW and Activity Based Working: Activity Patterns and Change Perspectives. *Proceedings of the 17th European Conference on Knowledge Management*, Ulster University Northern Ireland, UK, 1-2 September 2016.
- Dinev T., Hart P., 2006. An-extended Privacy Calculus Model for e-commerce Transactions. *Information Systems Research* 17 (1), 61-80.
- Djellal F., 2014. Les logiques d'innovation à l'hôpital. *Revue Soins cadres* 91, 16-20.
- Djellal F., Gallouj C., Gallouj F., Gallouj K. (2004). *L'hôpital innovateur : de l'innovation médicale à l'innovation de service*. Paris, Masson.
- Dubouloz S., 2014. Innovation organisationnelle et pratiques de mobilisation des RH. *Revue Française de Gestion* 40 (238), 59-85.
- Dudezert A., Portal M., 2016. *La controverse dans l'appropriation des outils de gestion : Contes de connaissance*. Éditions L'Harmattan, Paris.
- Ferneley E., Bell F., 2006. Using Bricolage to Integrate Business and Information Technology Innovation in SMEs. *Technovation* 26, 232-241.
- Gens F., Levitas D., Segal R., 2011. *Consumerization of IT Study: Closing the Consumerization Gap*. Framingham, MA, IDC.
- Hamel G., 2006. The Why, What, and How of Management Innovation. *Harvard Business Review* 84 (2), 1-16.
- Harrington S.J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly* 20 (3), 257-278.
- Harris J.G., Ives B., Junglas I., 2011. The Genie is out of the Bottle: Managing the Infiltration of Consumer IT into the Workforce. *Accenture Institute for High Performance*, (accédé le 8 mars 2018).
- Harris J.G., Ives B., Junglas I., 2012. IT Consumerization: When Gadgets Turn into Enterprise IT Tools. *MIS Quarterly Executive* 11 (3), 99-112.
- Henderson J., Venkatraman N., 1993. Strategic Alignment: Leveraging Information Technology for Transforming Organizations – Technical. *IBM Systems Journal* 32 (1), 4-16.
- Herault S., Belvaux B., 2014. Privacy paradox et adoption de technologies intrusives. Le cas de la géolocalisation mobile. *Décision Marketing* 74, 67-82.
- Holcman R., 2016. Hôpital public et redditions de comptes. *Revue Française d'Administration Publique* 4 (160), 1109-1122.
- Hong W., Thong J.Y.L., 2013. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly* 37 (1), 275-298.
- Hovav A., Putri F.F., 2016. This is my Device! Why Should I Follow your Rules? Employees' Compliance with BYOD Security Policy. *Pervasive and Mobile Computing* 32, 35-49.
- Jaouen A., Le Roy F., 2013. *L'innovation managériale*. Dunod, Paris.
- Jones B.H., Chin A.G., 2015. On the Efficacy of Smartphone Security: A Critical Analysis of Modifications in Business Students' Practices over Time. *International Journal of Information Management* 35, 561-571.
- Karoui M., Dudezert A., 2016. Transformation digitale : De l'assimilation des technologies de collaboration à la mise en usage. *21e Colloque de l'AIM - Association Information et Management*, mai 2016, Lille.
- Keith M.J., Thompson S.C., Hale J., Lowry P.B., Greer C., 2013. Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior. *International Journal of Human Computer Studies* 71 (12), 1163-1173.
- Keyes J., 2014, *BYOD for Healthcare*. CRC Press, Boca Raton.

- Köffer S., Ortbach K., Junglas I., Niehaves B., Harris J., 2015. Innovation through BYOD? – The Influence of IT Consumerization on Individual IT Behavior. *Business & Information Systems Engineering* 57 (6), 363-375.
- Leclercq-Vandelannoitte A., 2014. Consumérisation IT et BYOD : changements de pratiques et réactions organisationnelles. *XIX^e Colloque de l'AIM - Association Information et Management*, mai 2014, Aix-Marseille.
- Leclercq-Vandelannoitte A., 2015a. Leaving employees to their own devices: new practices in the workplace. *Journal of Business Strategy* 36 (5), 18-24.
- Leclercq-Vandelannoitte, A., 2015b. Managing BYOD: how do organizations Incorporate User-Driven IT Innovations? *Information Technology & People* 28 (1), 2-33.
- Le Roy F., Robert M., Giuliani P., 2013. L'innovation managériale. Généalogie, défis et perspectives. *Revue Française de Gestion* 39 (235), 77-90.
- Magruder J.S., Lewis S.X., Burks E.J., Smolinski C., 2015. Bring Your Own Device (BYOD) – Who Is Running Organizations? *Journal of Accounting and Finance* 15 (1), 55-61.
- MALWAREBYTES, 2017. *State of Malware Report*
<https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf>, (accédé le 8 mars 2018).
- Marshall S., 2014. IT Consumerization: A Case Study of BYOD in a Healthcare Setting. *Technology Innovation Management Review*, 14-18.
- Mignon S., Chapellier P., Mazars-Chapelon A., Villeseque-Dubus F. (sous la dir. de), 2017. *L'innovation managériale, enjeux et perspectives*. Éditions EMS Management & Société.
- Mignon, S., Walliser, E., 2015. Connaissances, capital intellectuel et management de l'innovation. *Innovations, Revue d'Économie et de Management de l'Innovation* 2 (47), 5-13.
- Miller K.W., Voas J., Hurlburt G.F., 2012. BYOD: Security and Privacy Considerations. *IT Professional* 14, 53-55.
- Mol M.J., Birkinshaw J., 2009. The Sources of Management Innovation: When Firms Introduce new Management Practices. *Journal of Business Research* 62 (12), 1269-1280.
- Morrow B., 2012. BYOD Security Challenges: Control and Protect your Most Sensitive Data. *Network Security*, 5-8.
- Motulsky A., Wong J., Cordeau J.P., Pomalaza J., Barkun J., Tamblyn R., 2017. Using Mobile Devices for Inpatient Rounding and Handoffs: an Innovative Application Developed and Rapidly Adopted by Clinicians in a Pediatric Hospital. *Journal of the American Medical Informatics Association* 24 (1), e69-e78
- Moyer J.E., 2013. Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. *Journal of Hospital Librarianship* 13 (3), 197-208.
- Mueller M., Klesel M., Heger O., Niehaves B., 2016. Empirical Insights on Individual Innovation Behavior: A Qualitative Study on IT-Consumerization. *PACIS-Pacific Asia Conference on Information Systems*, Summer 6-27-2016.
- Niehaves B., Köffer S., Ortbach K., 2012. IT Consumerization – A Theory and Practice Review. *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, USA.
- Nobre T. (2013 a). L'innovation managériale à l'hôpital. Changer les principes du management pour que rien ne change? *Revue Française de Gestion* 6 (235), 113-127.
- Nobre T. (2013b). *L'innovation managériale à l'hôpital : 14 cas de mise en œuvre*. Dunod, Paris.
- NOKIA, 2016. *Threat Intelligence Report*. <https://pages.nokia.com/8859.Threat.Intelligence.Report.html>, (accédé le 8 mars 2018).
- Orlikowski W.J., Hofman J.D., 1997. An Improvisational Model for Change Management: the Case of Groupware Technologies. *Sloan Management Review*, 11-21.
- Ortbach K., Köffer S., Bode M., Niehaves B., 2013. Individualization of Information Systems-Analyzing Antecedents of IT Consumerization Behavior. *Thirty Fourth International Conference on Information Systems-ICIS*, Milan.
- Pras B., 2012. Entreprise et vie privée: le « privacy paradox » et comment le dépasser? *Revue Française de Gestion* 224, 87-94.

- Reix R., Fallery B., Kalika M., Rowe F., 2016. *Systèmes d'Information et Management*. 7^e éd. Vuibert, Paris.
- Rogers E.M., 1962. *Diffusion of Innovations*. The Free Press of Glencoe, New York.
- Sangani N.K., Vijaykumar B., 2012. Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informática Económica* 16 (2), 58-71.
- Sher M.L., Talley P.C., Cheng T.J., Kuo K.M., 2017. How can Hospitals better Protect the Privacy of Electronic Medical Records? Perspectives from Staff Members of Health Information Management Departments. *Health Information Management Journal* 46 (2), 87-95.
- Singh N., 2012. B.Y.O.D. Genie Is Out Of The Bottle – ‘Devil Or Angel’. *Journal of Business Management & Social Sciences Research* (1) 3, 1-12.
- Stephens K., Zhu Y., Harrison M., Iyer M., Hairston T., Luk J., 2017. Bring Your Own Mobile Device (BYOD) to the Hospital: Layered Boundary Barriers and Divergent Boundary Management Strategies. *Proceedings of the 50 th Hawaii International Conference on System Sciences*.
- Subianto J., Palme E., Tan C.-H., Phang C.W., 2013. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly* 37 (4), 1141-1164.
- Swanson E.B., Ramiller N.C. (1997). The Organizing Vision in Information Systems Innovation. *Organization Science* 8 (5), 458-474.
- Swanson E.B., Ramiller N.C., 2004. Innovating Mindfully with Information Technology. *MIS Quarterly* 28 (4), 553-583.
- Tanriverdi H., Rai A., Venkatraman V., 2010. Research Commentary-Reframing the Dominant Quests of Information Systems Strategy Research for Complex Adaptive Business Systems. *Information Systems Research* 21 (4), 822-834.
- Timms K., 2017. *SMEs Must Better Understand the Cyber Security Threat in 2017*. <http://www.streamwire.co.uk/jan-17/smes-must-better-understand-the-cyber-security-threat-in-2017-2/> (accédé le 8 mars 2018).
- Valette A., Grenier C., Saulpic O., Zarlowski P., 2015. La fabrication du « médico-économique » à l'hôpital français : une analyse de la littérature. *Politiques et Management Public* 32 (3), 241-264.
- Venkatesh V., Morris M.G., Davis G.B., Davis F.D., 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* 27 (3), 425-478.
- Venkatesh V., Thong J.Y.L., Xu X., 2012. Consumer Acceptance and Use of Information technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly* 36 (1), 157-178.
- Weeger A., Wang X., Gewald H., 2016. IT Consumerization: BYOD-Program Acceptance and its Impact on Employer Attractiveness. *Journal of Computer Information Systems* 56 (1), 1-10.

Annexe I : Note méthodologique

Cet article est avant tout conceptuel et se fonde sur l'expérience des deux auteurs. Si ces derniers ont des bases communes au plan des technologies de l'information et de leur adoption, un auteur est plus spécialisé dans les comportements dans le domaine de la sécurité et l'autre auteur est plus centré sur l'innovation managériale. Après avoir étudié le BYOD depuis plus de deux ans, et être intervenus auprès du Centre Hospitalier Universitaire-CHU de Montpellier, les auteurs ont contextualisé leur travail dans le domaine hospitalier dans le cadre de cet article.

Les auteurs ont aussi effectué une revue de littérature pour étayer leur discours. On trouvera ci-dessous les principales étapes suivies.

Processus d'identification du corpus

Consultation des bases de données scientifiques :

- EBSCO, ABI Inform/Proquest, Science Direct et Google Scholar.

Prise en compte de l'actualité sur la base de sites web, d'articles professionnels, d'études de cabinets de consulting.

Utilisation de mots-clés combinés¹⁴, à partir de quatre thèmes principaux :

1. La sécurité : vie privée, données sensibles, confidentialité, sécurité, CNIL, législation, protection, charte, etc.
2. L'hôpital : organisation, hôpitaux, patients, malades, médecins, infirmiers, etc.
3. Les outils et les comportements associés : BYOD, CYOD, smartphones, outils mobiles, technologies, adoption, adoption inversée, consommerisation, etc.
4. L'innovation : nouvelles pratiques, innovation, innovation managériale, nouveaux processus, etc.

Un corpus de plus d'une centaine d'articles a été constitué, dont les 80 plus marquants figurent en référence.

Classification

Des priorités ont été affectées aux articles selon leur provenance (classement CNRS/FNEGE de la revue, presse, etc.). Les éléments rencontrés les plus fréquemment ont pu être identifiés, ainsi que les nouveaux concepts liés au BYOD (ex : l'adoption inversée et ses spécificités), puis au BYOD en contexte hospitalier, notamment les problèmes liés aux données médicales sensibles.

Une synthèse a été réalisée pour chaque thème étudié.

Choix d'organisation et de présentation des résultats

Le choix résulte d'une concertation entre les auteurs. Il s'agissait de dissocier l'aspect technologique (le BYOD) de son mode d'adoption (inversé), qui est la source réelle des innovations organisationnelles résultantes. Le corpus a peu à peu laissé apparaître les innovations facilitées (ou émergentes), et celles induites (rendues nécessaires) par ce mode d'adoption original. Ce travail a résulté en une dichotomie entre les nouveaux usages facilités par l'utilisation des outils personnels et ceux résultant de la nécessité, en contrepartie, de protéger les organisations (les hôpitaux dans cet article) et les acteurs (personnels et patients).

¹⁴ Termes français, il faut ajouter les termes anglais correspondant. Seuls les principaux termes français figurent ici.