GESTION DES USAGES DES TECHNOLOGIES NUMÉRIQUES DANS LES ORGANISATIONS : UNE APPROCHE QUALITATIVE PAR LE CONTRÔLE ORGANISATIONNEL ET LES CHARTES INFORMATIQUES

Étienne Thenoz

ESKA | « Systèmes d'information & management »

2020/3 Volume 25 | pages 51 à 86

ISSN 1260-4984
ISBN 9782747231091

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-systemes-d-information-et-management-2020-3-page-51.htm

Gestion des usages des technologies numériques dans les organisations : une approche qualitative par le contrôle organisationnel et les chartes informatiques

Étienne THENOZ

IAE, Université de Nantes, France

RÉSUMÉ

L'ouverture et la connectivité des technologies numériques basées sur Internet offrent un potentiel informatique inédit, mais conduisent néanmoins à une diversification et à un accroissement importants des risques et tensions liés à leur usage. Pour les organisations, ces risques soulèvent le problème de l'ajustement de leurs politiques de gestion des usages à ces technologies numériques, et notamment à l'usage de l'Internet relationnel, du cloud computing et des outils de mobilité. À partir d'une analyse qualitative d'entretiens avec des Directeurs des Systèmes d'Information, de chartes informatiques, de décisions de justice et des délibérations de la CNIL, nous examinons pourquoi les contrôles par les comportements, par les résultats, ou par socialisation sont plus ou moins adaptés à la gestion des usages de ces technologies numériques basées sur Internet et à leurs particularités. En particulier, nous analysons leur capacité à concilier contrôle et autonomie, stabilité et flexibilité, pratiques organisationnelles et culture numérique émergente. Nos résultats suggèrent une meilleure adéquation des contrôles par socialisation à la gestion des usages de ces technologies et soulignent les effets potentiellement délétères des contrôles comportementaux. Ils nous conduisent à proposer d'exploiter en premier lieu des contrôles par socialisation décentralisés et d'impliquer fortement les utilisateurs dans le développement de leurs compétences numériques et dans la conception de leurs usages.

Mots-clés : *Gestion des usages, Chartes informatiques, Technologies numériques, Contrôle organisationnel, Culture numérique.*

ABSTRACT

The openness and connectivity of Internet-based digital technologies provide an unprecedented computational power. Nevertheless, a greater amount and variety of risks and tensions stem from their use, hence calling for adjustments in organizations' digital technologies use policies, in particular to manage the use of social web, cloud computing and mobile computing. Through a qualitative analysis of interviews with CIOs, ICT codes of ethics, court decisions and the French Data Protection Authority's deliberations, we examine how results, behavior, or socialization-based control modes are more or less suited to managing Internet-based digital technologies uses and their particularities. In particular, we analyze the capacity of these control modes to reconcile control and autonomy, stability and flexibility, organizational practices and an emerging digital culture. Our results suggest that social controls are more appropriate for managing Internet-based digital technologies uses and highlight the potential counterproductive effects of behavioral controls. For practitioners, we therefore propose prioritizing the use of decentralized social controls as well as a strong involvement of users in the development of their digital skills and in the design of their practices.

Keywords: *Use management, ICT codes of ethics, Digital technologies, Organizational control, Digital culture.*

INTRODUCTION

En 2008, des employés d'une entreprise de services numériques communiquèrent à leur direction une copie de messages échangés sur Facebook par trois de leurs collègues. Ces derniers avaient formé le « *club des néfastes* » dont l'objet était de se moquer « avec humour » de leur directrice. Le conseil des Prud'hommes confirma leur licenciement pour incitation à la rébellion et dénigrement envers leur entreprise, estimant que la page accessible « aux amis des amis » revêtait un caractère public (CPH Boulogne-Billancourt, 19 nov. 2010). Les litiges liés à l'usage des technologies numériques ne se limitent pas à l'usage des réseaux sociaux. En 2017, un employé d'une société d'analyse de données commit une négligence dans la configuration du service de stockage cloud sur lequel la société hébergeait son entrepôt de données entier. La base fut alors rendue accessible à toute personne pouvant en trouver l'adresse URL. Cette base de données contenait les noms, adresses, dates de naissance et numéros de téléphone de 99% des électeurs américains, ainsi qu'une modélisation de leurs origines ethniques, religions, votes et opinions présumées sur une cinquantaine de sujets tels que le port d'arme, les impôts, l'écologie, l'avortement, et bien d'autres (Upguard, 2018). Le développement des technologies de mobilité contribue également à l'émergence de tensions autour de l'usage des technologies en entreprise. En 2015, une décision de Justice reconnût les SMS envoyés depuis un téléphone fourni par l'entreprise comme présumés professionnels, et donc consultables par l'employeur et la Justice (Cass, Ch. Co., 10 fév. 2015), tandis qu'outre-Atlantique, des litiges apparaissent suite à l'effacement de données personnelles des employés sur des téléphones

utilisés dans le cadre de politiques Bring Your Own Device (BYOD) (Southern District of Texas, 2014). En réaction, les opportunités de contrôle offertes par les technologies numériques sont parfois exploitées par les entreprises et leurs responsables jusqu'à les placer dans l'illégalité (CA Versailles, 4 fév. 2015 ; Cass. Ch. Soc., 19 déc. 2018).

Ces cas illustrent la diversité des problèmes liés à la gestion des usages des technologies numériques basées sur Internet, qui dépassent désormais les questions de productivité et de sécurité informatique et soulèvent des problématiques variées liées par exemple à la vie privée des individus, la responsabilité légale de l'organisation, sa réputation, ou encore la propriété intellectuelle. En effet, l'évolutivité, l'ouverture et le caractère générique de l'architecture Internet sur laquelle reposent ces technologies numériques offrent une forte flexibilité d'usage. Permettant d'agir hors des frontières traditionnelles de l'organisation, fortement utilisées dans un cadre personnel plus libre qu'en entreprise (Rodhain & Agarwal, 2001) et nécessitant par ailleurs une moindre médiation par des « experts » techniques, ces technologies permettent une autonomie qui rend les usages plus malléables (Leclercq-Vandelannoitte & Bertin, 2018). La flexibilité interprétative (Orlikowski, 1992) qui résulte des relations entre particularités de ces technologies, leurs utilisateurs désormais plus avertis, et leur usage, dans des contextes à la fois professionnels et personnels, produit des usages variés et imprévisibles que les organisations peinent à contrôler. En émergent des tensions importantes entre exploitation et maîtrise du potentiel offert par ces technologies numériques, soulevant pour les organisations la question suivante : comment adapter leurs politiques de gestion des usages informatiques aux technologies basées sur Internet ? En dépit de pistes théoriques liées à l'émergence de nouvelles formes de gouvernance des technologies, les données empiriques manquent pour comprendre comment réaliser cette adaptation (Leclercq-Vandelannoitte & Bertin, 2018).

Le contrôle des usages peut en effet réduire leurs effets positifs et générer des conséquences négatives non anticipées (Markus, 1994), conduire à l'émergence de solutions de contournement, au développement du shadow IT ou à l'usage non autorisé de ressources personnelles (Leclercq-Vandelannoitte & Bertin, 2018). Toutefois, bien que de nombreuses recherches aient exploré la gestion des usages informatiques, leurs résultats souvent contradictoires et focalisés sur la sécurité informatique au détriment d'autres variables tiennent peu compte des particularités de ces nouvelles technologies, de leurs utilisateurs, et des dynamiques organisationnelles au sein desquelles se forment les usages. Nous adoptons dans cet article une perspective émergente considérant les usages comme le produit d'interactions complexes entre organisation, technologies, et utilisateurs (Markus & Robey, 1988). À partir d'entretiens semi-directifs avec des Directeurs des Systèmes d'Information (DSI), d'un corpus de 60 chartes informatiques, de décisions de justice, et de sanctions de la CNIL, nous analysons l'adéquation des contrôles par les comportements, par les résultats, ou par socialisation à la gestion des usages des technologies numériques basées sur Internet, à leurs particularités, ainsi qu'à celles de leurs utilisateurs. Après une revue de la littérature, nous introduisons le cadre théorique mobilisé, avant d'exposer nos principaux résultats. Ceux-ci suggèrent que les contrôles par socialisation, reposant sur l'internalisation de normes sociales par les utilisateurs, sont plus adaptés au contrôle de ces usages en ce qu'ils permettent de mieux gérer les tensions inhérentes. Nous concluons en proposant des pistes théoriques et pratiques permettant d'adapter les pratiques de gestion des usages par un

renversement de la hiérarchie des modes de contrôle.

1. REVUE DE LA LITTÉRATURE

Afin d'approcher les problématiques d'usage des technologies numériques basées sur Internet sans toutefois perdre en pertinence contextuelle (Siponen & Vance, 2014), nous nous sommes focalisés sur l'usage de trois de ces technologies couramment répandues, qui constituent des piliers de la transformation numérique des entreprises, et qui ne sont pas restreintes à des utilisateurs particuliers. Nous avons sélectionné l'usage de la navigation Internet et des médias sociaux (Web 2.0), du cloud computing, et des technologies de mobilité (en déplacement ou en télétravail à domicile). Ceux-ci offrent en effet tous trois une forte flexibilité d'usage qui provoque des cas de « riposte technologique » (Luhmann, 1993) où des modes d'utilisation et de contrôle non anticipés apparaissent. Elles constituent ainsi de bons candidats pour explorer les tensions liées à l'usage des technologies numériques basées sur Internet et comprendre comment y adapter les politiques des organisations. Pour ce faire, nous avons pratiqué une double revue de la littérature pour résumer dans un premier temps quelles tensions l'usage de ces technologies génère avant de résumer l'état des connaissances sur le contrôle de ces usages.

1.1. Émergence de tensions liées à l'usage des technologies numériques basées sur Internet

La flexibilité d'usage de ces technologies conduit à l'émergence de tensions variées, liées à la productivité et à la sécurité, mais aussi au bien-être des utilisateurs, à la frontière entre vies personnelles et professionnelles, ainsi qu'à l'autonomie et au contrôle. Bien que les capacités de recherche et d'échange d'information soient améliorées par l'usage des médias sociaux (Teo & Choo, 2001 ; Dong & Wu, 2015), du cloud computing (Marston *et al.*, 2011), et des technologies de mobilité (Loup, 2016 ; Baruch, 2000), ces gains de productivité peuvent toutefois être compensés par le détournement de ces technologies à des fins récréatives (Young & Case, 2004) ou illégales telles que le harcèlement en ligne, des violations du droit d'auteur, la consultation de sites illégaux, ou encore la publication de publicité dissimulée, faux avis et commentaires (Chérigny, 2012 ; Drumwright & Murphy, 2009). Bien que la possibilité d'opérer un arbitrage entre satisfaction des utilisateurs et productivité ait été avancée (Urbaczeswski & Jessup, 2002), celui-ci est d'autant plus complexe que l'usage récréatif des technologies numériques au travail peut également améliorer la productivité (Coker, 2011). Les technologies de mobilité et de cloud computing étendent quant à elles ces bénéfices, quel que soit l'heure ou le lieu, mais également les possibles dérives, qui peuvent être légitimées par le sentiment de possession que les politiques de BYOD génèrent chez les utilisateurs (Hovav & Putri, 2016). Cette tension liée à la productivité est par ailleurs renforcée par le besoin d'assurer la sécurité informatique, travail qui peut perturber les routines de travail (Post & Kagan, 2007), ou enjoindre les utilisateurs à remplir des objectifs contradictoires (Bulgurcu *et al.*, 2010 ; Walsham, 1996). Les objectifs opérationnels demeurent toutefois souvent leur priorité (Li *et al.*, 2010 ; Guo *et al.*, 2011). Cette tension entre sécurité et productivité se manifeste par exemple lorsque les utilisateurs déploient des solutions shadow IT (Walterbusch, *et al.* 2017) qui, bien que problématiques pour la sécurité et l'auditabilité, sont souvent employées pour améliorer

l'efficacité au travail (Haag *et al.*, 2015). La gestion des usages doit alors trouver un équilibre pour par exemple prévenir la divulgation d'informations sur les réseaux sociaux (Chérigny, 2012 ; Teo & Choo, 2001) et les services cloud (Armbrust *et al.*, 2010) ou sécuriser les solutions de mobilité plus vulnérables (Bahli & Benslimane, 2004) sans toutefois trop réduire les bénéfices liés à leur usage.

La continuité entre usages domestiques et professionnels des technologies numériques basées sur Internet génère également des tensions autour du bien-être des employés et de l'équilibre entre vies professionnelles et personnelles. En premier lieu, la navigation récréationnelle au travail (Coker, 2011), l'usage d'outils de mobilité (Chen & Corritore, 2008) et la possibilité de travailler à domicile (Baruch, 2000) peuvent contribuer au bien-être et à la satisfaction liée au travail. Toutefois, de nombreuses recherches mettent en exergue les conséquences sociopsychologiques qui résultent de cette connectivité accrue. Sont par exemple rapportés des phénomènes d'addiction à Internet (Young, 2004) ou aux outils de mobilité (D'Arcy *et al.*, 2014), de surcharge informationnelle (Speier *et al.*, 1999 ; Loup, 2016), une repriorisation continue et un morcellement des tâches (Isaac *et al.*, 2007), ou encore un affaiblissement des relations sociales (Loup, 2016). L'écart parfois important entre liberté et ouverture des usages domestiques et rigidité des politiques d'entreprise peut également se heurter au sens de l'autonomie des utilisateurs (Rodhain & Agarwal, 2001), d'autant plus qu'ils adoptent désormais souvent ces technologies avant leur entreprise, dans des cycles d'adoption inversés (Leclercq-Vandelannoitte, 2015). Cette forme de rupture et de continuité simultanée dans l'usage de ces technologies participe à brouiller la frontière entre vie personnelle et professionnelle, entre lesquelles les utilisateurs transfèrent leurs pratiques. Les pratiques et données personnelles envahissent la vie professionnelle qui parallèlement, se déverse dans la vie familiale et personnelle des employés. Ceux-ci peuvent désormais s'exprimer à propos de leur travail sur des réseaux sociaux personnels et les consulter au travail (McDonald & Thompson, 2016), y amenant ainsi une part de leur intimité (Broadbent, 2016, chap. 3). À l'inverse, l'usage des outils de mobilité peut conduire à un envahissement de la vie personnelle en poussant les employés à se rendre disponibles quel que soit le lieu et hors des heures de travail (Yun *et al.*, 2012 ; Loup, 2016), mais aussi à soustraire des données au contrôle de l'entreprise en les stockant sur des espaces cloud personnels pour y accéder en tout lieu (Walterbusch, *et al.* 2017). Les pratiques de BYOD confondent de surcroît les données personnelles et professionnelles sur un même appareil, donnant aux employés le sentiment que l'entreprise s'introduit dans leur espace personnel en en régulant l'usage (Hovav & Putri, 2016).

La réaction des entreprises peut alors générer une tension supplémentaire entre opportunités de contrôle et d'autonomie. Bien que permettant un accès rapide, flexible et décentralisé à l'information, les réseaux sociaux peuvent ainsi servir de support au profilage des employés, des clients, et des candidats à l'embauche (Chérigny, 2012 ; McDonald & Thompson, 2016). Cette autonomie accrue peut à l'inverse conduire, dans le cas des solutions de cloud computing, à des pertes d'auditabilité (Armbrust *et al.*, 2010), notamment lorsqu'un service grand public ou personnel est utilisé (Walterbusch, *et al.* 2017). Substituant des dépendances technologiques aux dépendances hiérarchiques (Shu *et al.*, 2011), les outils de mobilité peuvent quant à eux générer des phénomènes d'autocontrôle fort (Baruch, 2000) ou permettre la mise en place d'un système de contrôle ubiquitaire (Leclerq-Vandelannoitte & Isaac, 2013).

Tableau 1 : Tensions liées à l'usage de la navigation et des médias sociaux, du cloud computing, et des technologies de mobilité ainsi qu'à sa gestion

Tensions	Usage de la navigation et des médias sociaux	Usage du cloud computing	Usages des technologies de mobilité et télétravail à domicile
Productivité et usage détourné	Productivité accrue, mais usages litigieux ou illégaux (Chérigny, 2012 ; Drumwright & Murphy, 2009) Baisse (e.g. Young & Case, 2004) ou hausse (Coker, 2011) liée aux usages à des fins personnelles. Arbitrage entre satisfaction et productivité (Urbaczeswski & Jessup, 2002)	Productivité accrue par réduction des coûts et flexibilité de l'usage (Zhang *et al.*, 2010 ; Marston *et al.*, 2011), mais aussi par le contournement des règles d'usage (Haag *et al.*, 2015)	Productivité accrue par l'accès rapide et flexible à l'information (Loup, 2016) et par réduction des coûts (Baruch, 2008)
Sécurité	Fuites et divulgation d'informations, risques d'ingénierie sociale, risque d'intelligence économique (Chérigny, 2012 ; Teo & Choo, 2001)	Cyberattaques, fuites de données, propriété et responsabilité (Armbrust *et al.*, 2010) Shadow IT pour remplir les objectifs opérationnels (Haag *et al.*, 2015), mais risques inhérents (Walterbusch, *et al.* 2017)	SI hétérogène et complexe (Forman & Zahorjan, 1994), réseaux et appareils vulnérables (Bahli & Benslimane, 2004) Tensions entre sécurité et objectifs opérationnels (Koch *et al.*, 2014)
	Les mesures destinées à améliorer la sécurité informatique perturbent les routines de travail (Post & Kagan, 2007) et génèrent des objectifs contradictoires (Bulgurcu *et al.*, 2010 ; Walsham, 1996 ; Li *et al.*, 2010 ; Guo *et al.*, 2011)		
Frontière pro / perso	Les utilisateurs apportent vie personnelle et intime au travail (McDonald & Thompson, 2016 ; Broadbent, 2016)	Utilisation de clouds personnels dissimulés (Ahuja & Gallupe, 2015 ; Walterbusch *et al.*, 2017)	Envahissement de la vie personnelle (Yun *et al.*, 2012 ; Loup, 2016) et sentiment d'intrusion dans leur appareil (BYOD) (Hovav & Putri, 2016)
Bien-être	Addiction à Internet (Young, 2004) Usage à des fins récréatives comme source de bien-être au travail (Coker, 2011)	Besoin d'autodétermination comme facteur d'utilisation de cloud personnel et manque d'autodétermination comme facteur de stress et de perte de motivation (Ahuja & Gallupe, 2015).	Addiction (D'Arcy *et al.*, 2014), surcharge informationnelle (Speier *et al.*, 1999 ; Loup, 2016), morcellement et repriorisation continue des tâches (Isaac *et al.*, 2007), amélioration de la qualité de vie au travail, mais dégradation par ailleurs (Kelliher & Anderson, 2008) Télétravail à domicile : moindres opportunités de carrière (Daniels *et al.*, 2001), moins de relations sociales, mais plus de temps libre (Baruch, 2000)
Contrôle & autonomie	Surveillance des employés, profilage des candidats à l'embauche et des clients (Chérigny, 2012 ; McDonald & Thompson, 2016) Écart entre pratiques à domicile et politiques rigides des entreprises (Rodhain & Agarwal, 2001)	Problèmes d'auditabilité et de traçabilité (Armbrust *et al.*, 2010), affranchissement du contrôle de la DSI (Andriole, 2015) et shadow IT (Walterbusch, *et al.* 2017)	Gains d'autonomie (Loup, 2016 ; Shu *et al.*, 2011), mais dépendances technologiques (Shu *et al.*, 2011), autocontrôle fort (Baruch, 2000), contrôle permanent et ubiquitaire (Leclerq-Vandelannoitte & Isaac, 2013)

La gestion de ces tensions est alors essentielle à la gestion des usages, en ce que l'usage que les utilisateurs font de la technologie peut produire des effets importants pour l'organisation, et que les politiques de l'organisation peuvent également produire des effets importants sur les utilisateurs. De cette relation complexe peuvent alors émerger des effets non déterminés à l'avance (Robey & Boudreau, 1999), et potentiellement entraîner utilisateurs et organisations dans des dérives tant dans l'usage des technologies que dans son contrôle. Ces multiples tensions liées aux usages de ces technologies sont résumées dans le tableau 1.

1.2. Contrôle des usages des technologies informatiques

Au-delà de ces multiples tensions, différents courants de recherche ont exploré comment les organisations peuvent contrôler l'usage des technologies par les utilisateurs. En premier lieu, des recherches se sont focalisées sur les chartes informatiques, qui constituent un dispositif central de gestion des usages, et visent à améliorer l'efficience du système d'information, à dissuader les abus et sensibiliser à la sécurité informatique, à codifier le contrôle en précisant droits, devoirs, et responsabilités (Bergeron & Berube, 1990), ainsi qu'à définir des résultats souhaités et les moyens acceptables pour y parvenir (White, 2013). Ces recherches soulignent toutefois la faible efficacité des chartes, auxquelles les utilisateurs n'adhèrent pas forcément (Loch *et al.*, 1998 ; Peacock & Pelfrey, 2016) et qu'ils trouvent rarement utiles (Loch *et al.*, 1998) même lorsqu'elles sont connues, comprises, et largement diffusées (Pierce & Henry, 2000 ; Doherty & Fulford, 2005). Des divergences entre les normes d'usage personnelles et de l'organisation persistent (Pierce & Henry, 2000) et peuvent nourrir une norme collective légitimant des comportements proscrits (Peacock & Pelfrey, 2016), sans que l'on puisse néanmoins établir si ces variations sont le produit ou la cause du manque d'influence des chartes. Peu applicable en contexte d'usage, trop complexe pour l'utilisateur moyen (Loch *et al.*, 1998 ; Doherty & Fulford, 2005) et trop rigide pour l'utilisateur expérimenté (Rodhain & Agarwal, 2001), leur contenu est difficilement appropriable en raison de sa focalisation sur l'efficience opérationnelle du SI et sur des référentiels de sécurité (Doherty & Fulford, 2005). L'efficacité des chartes est d'autant plus faible qu'en l'absence de procédure de mise à jour, les règles sont souvent obsolètes et peu adaptées aux technologies numériques (Berryman, 2008). Ces recherches conduisent donc naturellement à des recommandations sur le contenu des chartes (Whitman *et al.*, 1999 ; Chérigny, 2012 ; Crenn & Vidal, 2010), leurs attributs (e.g. clarté, brièveté, largeur, compréhensibilité – Goel & Chengalur-Smith., 2010 ; Pathari & Sonar, 2012), leur mode de diffusion, ou encore l'implication des utilisateurs (Bergeron & Berube, 1990). En considérant les problématiques de gestion des usages de manière large, ces recherches identifient une grande variété de problèmes liés aux usages et aux politiques mises en place pour les contrôler. Néanmoins souvent peu théorisées (Cram *et al.*, 2017), ces recommandations souffrent de la même obsolescence que les chartes elles-mêmes.

Le courant le plus représenté (Cram *et al.*, 2017) est quant à lui focalisé sur les moyens d'influencer le comportement de l'utilisateur pour qu'il soit conforme à celui prescrit par l'organisation. En s'appuyant sur la théorie de la motivation à la protection (Rogers & Maddux, 1983) et la théorie du comportement planifié (Ajzen, 1991), il propose de dissuader les comportements indésirables par des communications censées inspirer la peur. Ces travaux ont ainsi testé l'influence de la sévérité et de la certitude perçue de la menace, de

l'efficacité perçue de la réponse proposée, de la capacité personnelle perçue à mettre en œuvre cette solution (e.g. Johnston & Warkentin, 2010) ou encore des liens d'influence sociale sur cette perception (Herath & Rao, 2009). Les résultats de ces recherches sont toutefois contrastés (Cram *et al.*, 2017), ne validant pas l'influence de l'une de ces variables (e.g. Herath & Rao, 2009), voire n'en validant aucune (Lee *et al.*, 2004) ou seulement pour des abus graves (Harrington, 1996). Des facteurs de contingence individuels ou organisationnels, des problèmes méthodologiques, ou encore théoriques ont été avancés pour expliquer ces divergences (voir Cram *et al.*, 2017 et D'Arcy & Herath, 2011 pour des revues détaillées). L'une des critiques majeures réside dans la possibilité qu'ont les utilisateurs de rationaliser leur comportement par des techniques de « neutralisation », en réduisant leur peur plutôt qu'en ajustant leurs comportements (Siponen & Vance, 2010 ; Haag *et al.*, 2015). De plus et contrairement à d'autres domaines d'application de ces théories tels que la santé publique, la menace informatique pèse sur l'organisation et non sur l'utilisateur (Warkentin & Siponen, 2015). Pour dépasser cette limite, une grande part des approches comportementales s'est donc appuyée sur la théorie de la dissuasion. Théorie la plus citée dans ce courant (Siponen *et al.*, 2008), elle emploie une rhétorique de la sanction afin de faire peser la menace sur l'utilisateur et accroître les coûts de non-conformité du comportement (Herath & Rao, 2009 ; Warkentin & Siponen, 2015). À l'instar des travaux fondateurs (Straub, 1990 ; Straub & Nance, 1990), ces recherches adoptent une perspective disciplinaire et recommandent d'accroître la sévérité des sanctions, la visibilité du processus disciplinaire, ou la surveillance informatique (e.g. Boss *et al.*, 2009). Ces approches étudient toutefois peu les effets secondaires de ces recommandations, tels que des baisses de confiance, de loyauté (Li *et al.*, 2010) ou de la satisfaction au travail (Urbaczewski & Jessup, 2002), qui peuvent entraîner des comportements de réaction (Lowry & Moody, 2015) ou une frustration qui encourage le shadow IT (Haag *et al.*, 2015). De plus, en se focalisant sur la conformité des comportements aux règles dans un objectif de sécurité, ces approches accordent peu d'attention aux raisons de les enfreindre, telle que la poursuite des objectifs opérationnels (Haag *et al.*, 2015 ; Post & Kagan, 2007 ; Li *et al.*, 2010 ; Guo *et al.*, 2011), ignorant ainsi le contexte organisationnel dans lequel se forment les usages.

En revanche, les recherches tenant compte des dynamiques sociales dans la formation des usages ont mis en avant leur influence parfois plus importante que les sanctions formelles (Li *et al.*, 2010) ou que l'efficacité perçue du comportement prescrit (Johnston & Warkentin, 2010) sur l'intention d'adopter des comportements conformes. Bien que les utilisateurs dont les normes personnelles sont faibles soient influencés par les sanctions (Li *et al.*, 2010), ceux qui se perçoivent comme plus compétents avec les outils rejettent les messages basés sur la peur (Johnston & Warkentin, 2010). Par ailleurs, les phénomènes d'apprentissage social favorisent le développement de normes par participation des utilisateurs (Lee *et al.*, 2004), persuasion verbale entre collègues, observation ou aide par des pairs considérés compétents (Warkentin *et al.*, 2011 ; Guo *et al.*, 2011), que ces échanges soient formellement intégrés à leur rôle ou non (Hsu *et al.*, 2015). Enfin, lorsqu'ils considèrent que cela fait d'eux des professionnels compétents, les utilisateurs adaptent plus volontiers leurs comportements (Guo *et al.*, 2011), suggérant que ces dynamiques sociales peuvent constituer un outil pour influencer le milieu de formation des usages des technologies numériques basées sur Internet. L'approche déterministe et principalement basée sur

des perceptions et intentions limite toutefois la capacité de ces travaux à aborder la complexité de ces dynamiques.

Les tensions et enjeux liés à la gestion des usages des technologies numériques basées sur Internet sont donc multiples et dépassent les questions de sécurité, soulevant des problèmes liés à la productivité, au bien-être des employés, à la frontière entre vies personnelles et professionnelles, à l'autonomie et au contrôle. Les chartes informatiques sont néanmoins peu efficaces pour gérer seules les usages, et bien que des approches disciplinaires puissent inciter certains profils d'utilisateurs à changer leurs comportements, elles peinent à capturer les dynamiques organisationnelles et les relations complexes entre organisation, technologies, et utilisateurs, dont émergent les usages. Se focalisant sur la conformité des comportements aux règles de sécurité, elles occultent ainsi les effets négatifs de leurs recommandations, la multiplicité des objectifs de la gestion des usages (y compris lorsque la poursuite de certains d'entre eux conduit à enfreindre les règles), ainsi que l'influence des particularités de la technologie et de la relation que les utilisateurs entretiennent aujourd'hui avec elle.

2. CADRE THÉORIQUE

Pour aborder la gestion des usages des technologies numériques basées sur Internet dans une perspective large qui considère les usages comme émergents d'une relation complexe entre organisation, technologie, et utilisateurs (Markus & Robey, 1988 ; Orlikowski, 1992), nous nous appuyons sur trois éléments théoriques. En premier lieu, la théorie du contrôle d'Ouchi (1979) nous permet de considérer la diversité des contrôles employables, y compris lorsqu'ils reposent sur des phénomènes d'influence sociale, et ainsi de tenir compte d'un élément important du contexte organisationnel de formation des usages. Au moyen d'une théorie des tensions paradoxales liées aux architectures numériques (Tilson *et al.*, 2010), nous considérons les particularités des technologies numériques basées sur Internet ainsi que les tensions qui résultent de leur grande flexibilité d'usage. Enfin, nous considérons les particularités de la relation que les utilisateurs entretiennent avec ces technologies par une théorie de la culture numérique (Deuze, 2006).

Le premier outil théorique que nous avons retenu pour caractériser les politiques de gestion des usages est le mode de contrôle principal sur lequel elles reposent. En effet, les approches centrées sur le contrôle permettent d'analyser l'étendue des choix que peuvent faire les organisations dans la conception de leurs politiques de gestion des usages (Cram *et al.*, 2017). Pour tenir compte des différents mécanismes de contrôle qui peuvent être mis en œuvre, nous nous appuyons sur la typologie des modes de contrôle d'Ouchi (1979). Orientée vers la conception de dispositifs organisationnels et classiquement employée dans l'évaluation des systèmes d'information (SI), cette typologie repose sur trois modes de contrôle distincts (Table 2). Dans les dispositifs basés sur la surveillance, la spécification ou le confinement des comportements, ces derniers constituent le critère essentiel sur lequel porte le contrôle. En contexte informatique, ces contrôles reposent sur des règles ou des procédures spécifiant un comportement attendu, mais également sur l'inscription dans la technologie du confinement de l'action (*control by design*) et dans le recours aux capacités de surveillance informatique. Les dispositifs de contrôle basés sur les résultats reposent quant à eux non pas sur la spécification d'un comportement, mais d'un résultat attendu. Il peut s'agir d'une mesure de productivité, ou de tout autre résultat (e.g. sécurité, intégrité des données

ou préservation de la réputation en ligne). Le choix entre ces deux modes de contrôle dépend dans la typologie d'Ouchi de la capacité à formaliser les processus ou à définir et mesurer les résultats. Lorsque les deux sont impossibles ou trop coûteux, un troisième mode de contrôle par socialisation est plus adapté. Dans ce dernier, le contrôle est exercé au moyen de l'internalisation par les contrôlés des normes et des valeurs de l'organisation. Celle-ci cherche ainsi à orienter le comportement des utilisateurs en réduisant les divergences entre préférences individuelles et organisationnelles à l'aide de dispositifs variés, formels ou informels (e.g. sensibilisation, formation, groupes et forums d'échange, « ambassadeurs » partageant leurs « astuces », pression sociale ou entraide entre pairs, autocontrôle, ou encore rites organisationnels). Ils sont ici considérés dans une perspective instrumentale, comme une tentative de l'organisation d'influencer le cadre de formation des usages plutôt que les comportements. La présence de ce troisième mode de contrôle permet de considérer les dimensions collectives et sociales du contrôle des usages ainsi que d'éventuels effets délétères décrits par Ouchi (1979) tels que des réactions à la perte d'autonomie lorsque les contrôles sont trop stricts.

Pour explorer l'adéquation de ces modes de contrôle à l'usage des technologies numériques basées sur Internet, nous considérons également les particularités de celles-ci. En effet, leur ouverture et leur évolutivité offrent des potentialités d'usage plus importantes et variées que

Tableau 2 : Modes de contrôles (Ouchi, 1979) et exemples liés à la gestion des usages

Mode de ctrl.	Principe	Exemples
Comportements	Évaluation de la conformité du comportement à des règles	– Établissement de règles à respecter, de procédures, formalisation de processus – Surveillance informatique des comportements – Inscription dans la technologie de limites aux comportements (e.g. empêcher l'accès à certains sites ou bloquer les installations)
Résultats	Mesure et évaluation des résultats de l'usage	– Mesure de la productivité ou de toute autre variable pour en rendre l'utilisateur responsable des résultats plutôt que des moyens pour les atteindre (e.g. confidentialité des données, impact des communications sur les réseaux sociaux, compromission de la sécurité…)
Socialisation	Internalisation des normes et valeurs de l'organisation par les utilisateurs	– Dispositifs formels de sensibilisation, d'information, de communication ou de formation destinée à faire connaître et partager ces normes – Dispositifs visant à favoriser le développement de ces normes par échange informel entre pairs (ateliers d'échange, mentorat informel, développement d'un climat de confiance avec les équipes informatiques, forums dédiés à la discussion de ces problèmes…) – Développement d'outils visant à faire internaliser des normes d'usage (e.g. videos, serious games…) – Rites organisationnels destinés à entretenir ou développer ces normes. – Développement de dispositifs visant à accroître la pression sociale ou l'apprentissage social afin que les normes se transmettent et se renforcent entre pairs (e.g. programmes de mentorat) – Autocontrôle et motivation intrinsèque

celles offertes par des technologies précédentes, limitées à l'entreprise, plus rigides et stables. Ce potentiel doit simultanément être exploité par les organisations et maintenu sous contrôle pour en maîtriser les risques. Nous modélisons ce besoin d'équilibre entre exploitation et contrôle des technologies au moyen d'une théorie des besoins paradoxaux fondée sur un double paradoxe (Tilson *et al.*, 2010). Le premier paradoxe provient des logiques opposées entre stabilité et flexibilité, lesquelles sont simultanément nécessaires l'une à l'autre pour assurer la fiabilité de l'organisation. La flexibilité est requise pour que les usages et le contrôle puissent évoluer avec les technologies et l'entreprise. Une certaine stabilité est néanmoins requise pour fournir un cadre à ces variations des usages, les transformer en routines efficientes (Farjoun, 2010) et les répandre dans l'organisation. Le second paradoxe est quant à lui relatif au besoin simultané de contrôle centralisé et d'autonomie individuelle, tous deux potentiellement renforcés par les technologies numériques (Gollac *et al.*, 2000). Le problème qui en résulte réside dans « l'établissement de points de contrôle acceptables par tous » (Tilson *et al.*, 2010). Il s'agit non seulement pour la politique de gestion des usages de répondre au besoin d'autonomie des utilisateurs, mais également de permettre d'adapter les usages aux contextes locaux. Cette politique doit toutefois permettre la fiabilité organisationnelle, la réduction des incertitudes, l'homogénéité des pratiques et des règles qui les régissent. Elle doit pour cela permettre une part de centralisation. Cette approche par les paradoxes organisationnels permet de considérer les particularités des technologies numériques basées sur Internet ainsi que la grande diversité des objectifs qui en naissent sans avoir à tous les spécifier. Nous proposons donc qu'un système de contrôle des usages des technologies numériques doive simultanément répondre à ces demandes paradoxales pour exploiter les technologies numériques efficacement en maîtrisant les tensions issues de leur usage.

Enfin, outre les particularités des technologies numériques et de leur usage, nous considérons également les changements dans les pratiques numériques des utilisateurs. En effet, les liens d'influence sociale dont l'effet est mis en avant par les approches comportementales ne se limitent pas à l'organisation. Des éléments de socialisation extérieurs sur lesquels celle-ci a peu de contrôle influencent également les utilisateurs. Nos habitudes numériques se forment désormais pour bonne partie hors de l'organisation, dans un cadre plus flexible et libre, et de nombreux produits et services numériques sont adoptés par les employés avant leur entreprise, dans des cycles d'adoption inversés (Leclercq-Vandelannoitte, 2015). Les utilisateurs maîtrisent de mieux en mieux ces technologies, et peuvent dans leur sphère privée s'adonner librement à l'exploration et à l'apprentissage de nouveaux usages. Cette intimité grandissante avec la technologie fait naître de nouvelles habitudes que les utilisateurs importent avec plus ou moins de frictions dans l'organisation, laquelle doit alors adapter ses politiques ou le comportement des utilisateurs. Pour tenir compte de ce facteur d'influence, nous considérons le bricolage, la participation et la remédiation comme trois dimensions notables de la culture numérique, c'est-à-dire « un système de valeurs et un ensemble d'attentes émergents, tels qu'exprimés dans les activités et pratiques des utilisateurs » (Deuze, 2006, p. 2). Le bricolage consiste en un assemblage, un désassemblage, un réassemblage continu et personnalisé avec les matériaux à disposition (Deuze, 2006). Cette dimension de nos habitudes numériques repose sur des notions d'emprunt (voire de plagiat), d'hybridité, et de mixité. Ces pratiques de bricolage se manifestent dans de nombreuses tâches : des solutions de

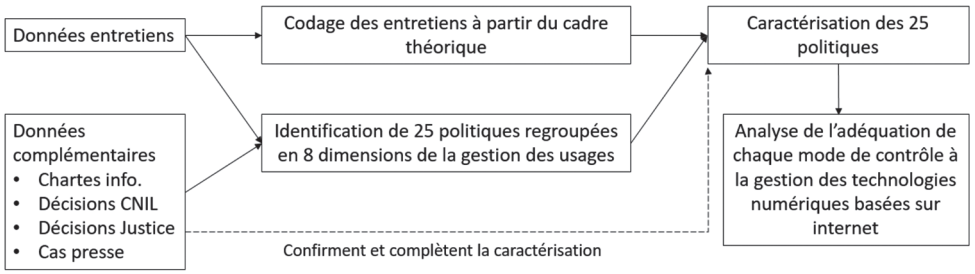
contournement élaborées émergent pour s'accommoder des rigidités des systèmes et la conception de documents s'accélère grâce à l'emprunt de divers paragraphes et images sur Internet. La participation consiste en un individualisme en réseau qui produit des structures bottom-up et redessine les liens entre individus et collectif. Enfin, la remédiation consiste à diverger du média précédent tout en le reproduisant dans une certaine mesure (Bolter & Grusin, 1999). Cette dimension permet de tenir compte de notre habitude de réinstancier nos modes de fonctionnement dans les nouveaux médias sous des formes divergentes, y compris lorsqu'ils sont issus de notre usage personnel. Ces trois dimensions constituent une caractérisation générale de la culture numérique qui ne vise pas à considérer toute sa complexité ou sa variété, mais plutôt ses caractères les plus largement partagés. Nous tenons ainsi compte d'un facteur d'influence des comportements numériques extérieur à l'organisation, avec lequel les politiques d'une organisation sont plus ou moins compatibles.

3. MÉTHODOLOGIE

Nous avons adopté une démarche qualitative pour identifier des inadéquations des différents mécanismes de contrôle aux particularités des technologies numériques, de leurs usages, et de leurs utilisateurs. Afin d'obtenir des données sur les politiques de gestion des usages numériques des organisations, nous avons mené, enregistré, puis retranscrit et codé sept entretiens semi-directifs avec des DSI d'entreprises de taille intermédiaire (8h30 d'entretiens au total). Pour répondre à notre objectif de diversité, nous avons sélectionné des entreprises qui présentaient chacune des particularités intéressantes au regard de la gestion des usages numériques (Annexe A). Pour trianguler les données et accéder aux politiques et aux justifications que les DSI auraient pu préférer ne pas évoquer (parce qu'elles sont très rigides et strictes, ou très peu développées), nous avons analysé trois sources de données complémentaires. Un corpus de 60 chartes informatiques collectées sur Internet nous a servi à concevoir le guide d'entretien, à générer plus de variété dans les politiques, et à représenter des chartes vieillissantes ou très génériques. Pour identifier les dérives possibles (tant de la part des employés que des organisations) et accéder aux arguments de défense des parties, nous avons examiné les décisions de Justice (31) renvoyées par une recherche « charte(s) informatique(s) » sur Legifrance et d'autres bases de données de jurisprudence, ainsi que des décisions prud'homales sélectionnées dans la presse pour leur caractère singulier ou extrême. Enfin, nous avons examiné les 71 sanctions prononcées par la CNIL entre 2011 et 2017, dont 39 ont été rendues publiques (pour les autres, seuls les motifs de sanction et l'organisation sanctionnée étaient accessibles).

Les données ont été analysées en trois étapes (Figure 1). Dans un premier temps, une analyse comparative des données de chaque entreprise a permis d'identifier et de définir 25 politiques au total, regroupées par la suite en 8 dimensions de la gestion des usages (Annexe B). Chacune de ces politiques correspond aux règles mises en place par une entreprise sur l'une de ces dimensions pour gouverner l'usage des technologies par les employés afin de guider leurs perceptions et actions. Les données complémentaires issues des décisions de justice et des chartes collectées sur Internet ont aidé à compléter l'identification de ces politiques et à la confirmer. Constatant par exemple que certaines organisations ne filtrent pas la navigation, filtrent les contenus jugés immoraux ou illégaux, ou encore filtrent tout contenu jugé non professionnel, nous avons positionné ces trois politiques sur une dimension « filtrage de la navigation

Figure 1 : Processus d'analyse des données



et des médias sociaux ». Parallèlement, les entretiens ont été codés en recherchant les mentions relatives aux catégories théoriques présentées ci-dessus. À partir de l'identification des politiques et du codage des entretiens, nous avons ensuite analysé les données par politique pour caractériser chacune d'entre elles et établir sur quel mode de contrôle elles reposent, si elles répondent aux besoins paradoxaux, et présentent une incompatibilité avec les éléments de culture numérique considérés (Résumé général en annexe B ; exemples de caractérisation d'une politique en annexe C). Nous n'avons pour ce faire pas évalué les apports de flexibilité, de stabilité, de centralisation et de décentralisation de manière absolue, mais à partir de verbatims évoquant un apport ou un manque de ces variables (les entretiens suggèrent par exemple que les utilisateurs bénéficient de moins de flexibilité dans l'usage de terminaux mobiles qu'ils ne peuvent pas personnaliser, mais que les appareils et les usages sont ainsi plus stables, facilitant la gestion du parc pour la DSI). Ces apports ont également été évalués relativement aux autres politiques applicables sur la même dimension de la gestion des usages (par exemple, une politique de standardisation des outils permet moins de flexibilité dans les usages, mais plus de stabilité du portefeuille logiciel qu'une politique de standardisation). Le contrôle par socialisation a quant à lui été codé lorsqu'une stratégie ou une intention d'influence, de construction, ou de maintien d'une norme sociale étaient évoquées. Enfin, nous avons analysé ces politiques par mode de contrôle pour en dériver des propositions relatives aux déficiences et apports respectifs de ceux-ci par rapport aux différentes variables.

4. ADÉQUATION DES MODES DE CONTRÔLE À LA GESTION DES USAGES DES TECHNOLOGIES NUMÉRIQUES

Nous ne présentons pas ici en détail les politiques de gestion des usages numériques identifiées pour des raisons de brièveté. Elles sont cependant présentées dans l'annexe B qui résume les politiques identifiées et leur caractérisation. Notre caractérisation de ces différentes politiques suggère une inadéquation des contrôles par les comportements et par les résultats. À l'inverse, les contrôles par socialisation sont les seuls à potentiellement apporter une réponse simultanée aux besoins paradoxaux et correspondent mieux aux éléments de culture numérique ici considérés. Dans la section qui suit, nous montrons comment ces différentes politiques et le mode de contrôle sur lequel elles reposent répondent aux particularités des technologies numériques et des utilisateurs.

4.1. Contrôle par les comportements : risque d'ossification organisationnelle

Les politiques de gestion des usages basées sur un contrôle par les comportements présentent l'avantage de répondre très efficacement au besoin de centralisation des décisions et de stabilité des règles et des comportements. Ces prescriptions comportementales sont généralement établies de manière centrale par la DSI ou la Direction Générale. Celles-ci déterminent par exemple l'étendue des filtres de la navigation, choisissent les matériels et logiciels que la DSI distribue, interdisent l'usage des appareils de l'entreprise à des fins personnelles ou les pratiques de BYOD. Ce mode de contrôle permet une forte stabilité des usages puisque le contrôle est durablement inscrit dans les règles managériales ou dans la technologie. Il permet aussi une forte centralisation en ce que ces règles tolèrent difficilement les exceptions et la singularité des utilisateurs, des groupes, des entités ou des besoins. Les règles strictes de filtrage de la navigation permettent par exemple la centralisation en ce que la DSI (et non les utilisateurs) détermine les usages appropriés, et la stabilité en ce que les filtres ne peuvent être modifiés que sur son intervention. L'interdiction de l'usage des terminaux personnels à des fins professionnelles et la standardisation des appareils de mobilité permettent quant à elles le contrôle central et la stabilité du parc d'équipements. L'un des DSI a par exemple indiqué : *« On a des postes standards et tout le monde a la même chose. Même OS, même explorateur, mêmes outils… On interdit de mettre des logiciels tiers dessus. C'est un choix où l'on finance* [les appareils]*, mais par contre on n'est pas embêtés par 36 000 modèles, 36 000 OS, ou des versions pirates, ce qui facilite le support* […] *et la maintenance. Puisque c'est nous qui fournissons, on en a le contrôle »* (DSI, BS).

En revanche, les contrôles comportementaux n'autorisent que très peu de flexibilité et de distribution du contrôle. Ainsi, l'interdiction de personnaliser les outils de mobilité (sur un plan matériel ou logiciel) empêche l'utilisateur de s'adapter rapidement face à un besoin singulier. Il doit généralement soumettre une demande à la DSI qui l'évalue et en cas d'acceptation, fournit le logiciel dans les jours suivants, parfois trop tard au regard d'un besoin ponctuel. Ces contrôles génèrent des tensions entre DSI et utilisateurs. L'un des DSI explique : « C*'est un peu mal vécu par les salariés. Mais on leur répète* […] *que c'est quelque chose sur lequel on veut garder la main. Dans ces contextes, on explique... C'est vrai que les gens râlent... »* (DSI, IC). L'entreprise CA a identifié les risques qu'induisent cette forte rigidité et cette centralisation et tente de les limiter en répondant au plus vite et favorablement à la majorité des demandes : *« On essaie plutôt d'être agiles et réactifs. Quand les collaborateurs ont besoin d'un outil, on leur fournit pour éviter le shadow IT et qu'ils aillent se servir ailleurs parce qu'on ne peut pas le faire »* (DSI, CA). Dans ce cas, les utilisateurs cherchent à contourner le processus de contrôle pour répondre à leur besoin logiciel rapidement, et c'est le manque de flexibilité et de distribution du contrôle qui induit des comportements indésirables. L'entreprise préfère donc adopter une posture de service plus flexible plutôt que de surveiller et sanctionner les utilisateurs. De manière similaire, un filtrage strict de la navigation et des médias sociaux ne peut que difficilement gérer les besoins particuliers sans complexifier le contrôle des accès. Par exemple, dans l'une des organisations interrogées, un directeur souhaitait consulter un site de presse bloqué par le pare-feu de l'entreprise en raison de son classement « à connotation religieuse ». La DSI dut intervenir pour autoriser le site pour tous les utilisateurs. L'absence de flexibilité

et de décentralisation complique et décourage par ailleurs l'exploration de nouvelles pratiques par les utilisateurs, ainsi que le développement de leurs compétences et de leur culture numérique. L'entreprise LM a par exemple longtemps bloqué l'accès aux réseaux sociaux, ne sachant pas comment les contrôler. Malgré son souhait de développer aujourd'hui leur usage à des fins professionnelles, le manque d'expériences antérieures des employés et de la DSI ralentit fortement l'adoption de ces usages, et la société peine à trouver un moyen de les développer. L'une des chartes collectées sur Internet présente quant à elle des règles dont on se demande comment elles peuvent inciter plutôt que décourager les utilisateurs à publier sur les réseaux sociaux. Après une introduction où l'entreprise vante les capacités de partage et d'échange des réseaux sociaux, et déclare vouloir « *encourager* [leur] *utilisation de manière proactive* », la charte mentionne : « *Vous êtes uniquement autorisés à parler de sujets avalisés* ».

Ces freins à l'exploration de nouveaux usages peuvent conduire des utilisateurs à rediriger leurs efforts d'apprentissage vers la maîtrise des systèmes de contrôle. En effet, en dépit de la présence de stratégies panoptiques dans plusieurs des organisations interrogées (résumées par cette déclaration de l'un des DSI : « *Ils savent que nous savons tout.* »), aucune des organisations interrogées ne dispose de contrôle permettant de limiter ou d'empêcher efficacement l'usage de logiciels en version portable ou de services cloud grand public (y compris des proxys en ligne[1]). Or, ces outils simples suffisent bien souvent à contourner une bonne partie des systèmes de contrôle comportemental, comme nous l'ont indiqué plusieurs DSI : *« Lancer un setup, ils ne peuvent pas. Pas sans compte admin. Mais si c'est du SaaS, etc, ils peuvent… Aujourd'hui, on n'a pas de contrôle. »* (DSI, FI) ; *« Aujourd'hui, on sait qui utilise dropbox par exemple… Par l'URL… Bon, c'est toujours possible de passer à travers. On a aussi une surveillance basée sur la volumétrie… mais sachant qu'on a des tuyaux qui augmentent d'année en année… on a moins de blocages et c'est plus dur de voir les mauvais fonctionnements. »* (DSI, IA). Ces contrôles ne permettent pas non plus de gérer les publications problématiques sur les réseaux sociaux : *« Aujourd'hui, c'est incontrôlable ce genre de choses. Si vous mettez des sondes sur les réseaux sociaux, il y en a qui se créent tous les jours… Là, on fait confiance aux gens… Sur le réseau, on peut* [contrôler techniquement la publication des messages], *mais on ne le fait pas. De toute façon s'il le fait chez lui... je ne vais pas aller contrôler les box de tous les salariés, donc ça ne sert à rien… »* (DSI, BS). L'incapacité des contrôles comportementaux à produire flexibilité et distribution du contrôle conduit donc à une ossification des pratiques numériques, mais également du système de contrôle, qui est dépassé par les usages. Dans certains cas, ces pratiques de surveillance semblent survivre sans que l'on ne sache vraiment quels objectifs elles servent. Interrogé sur son critère de tolérance vis-à-vis de l'utilisation à des fins personnelles d'Internet, l'un des DSI nous explique : « *Je regarde si c'est récurrent. Quelqu'un qui voulait jouer à la Française des jeux, c'était à sa pause, il ne savait pas que c'était interdit, il n'a pas compris sur le moment… Il a essayé deux ou trois fois, bon, on ne dit rien. Maintenant, si la semaine d'après il recommence, je lui dis « écoute ça va quoi ! C'est interdit. »*

[1] Ces sites relaient simplement la connexion par leurs serveurs. L'entreprise peut seulement voir que le site proxy a été consulté. Leur usage est néanmoins indésirable car le service proxy en profite pour capturer les informations de navigation. Certains services malhonnêtes absorbent les mots de passe saisis. Ici, la tentative de surveillance peut entraîner des comportements de dissimulation nuisibles à la sécurité.

Il ne fait pas vraiment courir de risques à l'entreprise… mais ça permet quand même d'être alerté sur un comportement qui pourrait être anormal… » (DSI, FI).

Les contrôles comportementaux sont par ailleurs peu compatibles avec la culture numérique, puisqu'ils empêchent bricolages et ajustements locaux. Ils limitent également la participation en raison du caractère centralisé de la conception et du contrôle des usages. Enfin, ils empêchent la remédiation de nos modes de fonctionnement en entreprise, puisque ces contrôles tolèrent assez mal les habitudes informatiques issues de nos vies privées. Ils cloisonnent par exemple navigation et expression, pourtant libres dans nos habitudes domestiques. Une des chartes collectées tente par exemple de contrôler l'expression de l'image de soi de ses employés en mentionnant : « *n'utilisez jamais ou ne faites jamais référence à votre statut professionnel lorsque vous écrivez dans un cadre non professionnel* ». De nombreux employés de l'entreprise mentionnent néanmoins leur employeur et le poste qu'ils occupent publiquement sur leur page personnelle, signe que leurs habitudes numériques les influencent plus que la charte de leur employeur. Ces contrôles interdisent également la personnalisation des outils, empêchant les utilisateurs d'exploiter les technologies qu'ils ont appris à maîtriser hors de l'organisation et de capitaliser sur ces compétences.

4.2. Contrôle par les résultats : risque d'instabilité et d'hétérogénéité

Nous n'avons identifié que peu de contrôles par les résultats dans les politiques de gestion des usages analysées. Lorsque présents, ils ne portent que sur un objectif et sont complémentés par d'autres contrôles. Par exemple, l'une des entreprises interrogées a mis en place une politique d'incitation à l'usage du stockage cloud de l'entreprise plutôt que du stockage en local. Pour ce faire, elle explique ne garantir aucune sauvegarde dans le cas où l'utilisateur stockerait ses fichiers sur son poste. Le DSI explique sa politique en ces termes : « *Dans la charte informatique, si vous dites" quand vous faites ça, ça nous coûte 500 euros", l'utilisateur s'en moque, ce n'est pas lui qui paie. Alors que si vous dites « là tu vas perdre tous tes contacts, je ne saurai pas les sauvegarder »* » (DSI, BS). Dans ce cas, l'entreprise transfère les risques à ses utilisateurs qui souhaiteraient déroger à la règle, en leur laissant néanmoins la possibilité de le faire lorsqu'ils l'estiment justifié. Cette politique ne traite toutefois que le problème de la disponibilité des données et est donc associée à d'autres mécanismes de contrôle (les données sensibles ne peuvent être techniquement stockées que sur les applications dédiées, et l'effet social de « *la force du groupe* » rappelle aux utilisateurs qu'une partie de leurs fichiers doit être partagée sur l'intranet). Dans le cas des politiques d'autorisation de l'usage à des fins personnelles de la navigation et des outils de mobilité, la même organisation emploie un contrôle par les résultats opérationnels. Elle ne contrôle pas l'usage à des fins personnelles d'Internet, puisque les abus sont limités par l'attention du manager de proximité à la productivité des employés. Les autres objectifs de la gestion des usages sont quant à eux contrôlés par des dispositifs de socialisation accessoires (par exemple, des sensibilisations aux risques liés à la navigation). L'avantage principal de cette politique d'usage libre de la navigation et des médias sociaux est que la DSI joue un rôle de protection de ses utilisateurs et non de surveillance de leurs comportements de navigation. Elle préserve ainsi la confiance qu'ils lui accordent et facilite les échanges informels. Un DSI nous a indiqué : « S*'ils vont sur la Française des jeux, ou sur LeBonCoin, je m'en fiche. Ce n'est pas*

mon problème, c'est le problème de leur manager. S'ils ont le temps de le faire, c'est qu'ils n'ont pas assez de boulot » (DSI, BS). Il explique que son rôle est également de protéger l'utilisateur de demandes abusives de surveillance du management, préservant sa confiance : « *On ne donne jamais l'accès à une messagerie sans que la DRH, le DG et moi soyons en accord. On est trois à avoir la délégation de pouvoir en disant : « on te donne l'autorisation d'aller surveiller » »* (DSI, BS). Un autre DSI présente quant à lui ses doutes sur l'utilité du contrôle de la productivité par les outils informatiques : « *Très concrètement, la personne qui abuse de ces usages, si vous lui enlevez, elle ne sera pas plus productive... On a plutôt considéré qu'on n'a pas de raison de bloquer* » (DSI, IC). Cette politique permet par ailleurs d'éviter le travail complexe de discrimination entre usages professionnels et personnels d'un même site ou de gestion des filtres. Ces politiques fondées sur le contrôle par les résultats permettent décentralisation et flexibilité dans les usages, et ne présentent pas d'incompatibilité avec la culture numérique. Elles ne placent ainsi aucune contrainte sur l'exploration et l'apprentissage de nouveaux usages. Toutefois, ces contrôles répondent mal au besoin de centralisation et de stabilité. Ils conduiraient à l'émergence de publications très hétérogènes sur les médias sociaux, ou de configurations logicielles trop nombreuses qui compliqueraient l'auditabilité et la traçabilité des usages ainsi que la maintenance du parc informatique.

4.3. Contrôle par socialisation : réponses potentiellement simultanées aux besoins paradoxaux

Les politiques fondées sur un contrôle par socialisation sont celles qui sont potentiellement les plus adaptées à la gestion des usages numériques. En effet, elles peuvent permettre une réponse simultanée aux besoins paradoxaux sans contrevenir aux éléments de culture numérique. En s'appuyant sur des normes et valeurs établies de manière centrale, mais en décentralisant leur application et leur diffusion, le contrôle par socialisation peut résoudre le paradoxe du contrôle et permettre la participation. Dans le cas d'une politique d'expression libre sur les médias sociaux, l'organisation établit par exemple un cœur de principes fondamentaux, et peut mettre en avant l'importance de l'attention portée à sa réputation, préciser son rapport aux liens numériques entre vies personnelles et professionnelles, ou se positionner par rapport au risque d'intelligence économique et de divulgation d'informations sensibles. Dans certaines des organisations étudiées, la DSI focalise ainsi ses efforts sur le respect d'un grand principe simple en matière de publication sur les médias sociaux, et limite les contraintes pour encourager à la publication : « *Aujourd'hui, l'expression est totalement libre à partir du moment où l'on respecte ses collègues, ses clients* » *(DSI, CA) ;* « *Aucun* [problème à la publication]. *Au contraire, on est plutôt contents. On y est favorables, et on l'encourage.* […], *ça prouvera qu'on bosse sur des sujets d'innovation* » (DSI, BS).

Néanmoins, ce contrôle social permet décentralisation et participation en ce qu'aucun comportement attendu n'est spécifié et que l'utilisateur en situation peut appliquer ces normes en évaluant lui-même leur pertinence au regard de son besoin. Ainsi, un technicien postant une question sur un forum technique, un acheteur communiquant avec des fournisseurs sur un réseau social professionnel, ou un manager rédigeant un article sur l'un des projets de son entreprise sur des réseaux sociaux grand public peuvent librement mettre ces valeurs en pratique d'une manière adaptée à leur audience et

au média. Ils évitent ainsi de soumettre leur publication à une procédure d'autorisation coûteuse en temps pour les utilisateurs comme pour la DSI (ou le service communication). Celle-ci peut ainsi se concentrer sur la stabilité et la diffusion de ses grands principes plutôt que sur le contrôle du respect d'une déclinaison de règles centrales, nécessairement moins adaptées aux situations locales. Dans le cas par exemple d'une politique de personnalisation des outils de mobilité, l'organisation peut se concentrer sur l'établissement de principes stables dans le temps et à travers l'organisation (par exemple, en stipulant que les applications doivent provenir d'éditeurs fiables et être téléchargées depuis le site de l'éditeur en question). Elle laisse toutefois une certaine flexibilité à ses utilisateurs en ne plaçant pas de contraintes comportementales sur la personnalisation. Les plus avertis d'entre eux peuvent appliquer ce principe en situation, tandis que l'organisation fournit aux autres des conseils pour pratiquer cette sélection par eux-mêmes (par exemple en listant des éditeurs et plateformes de confiance, ou en donnant des exemples d'éléments qui doivent alerter les utilisateurs). L'utilisateur bénéficie ainsi de plus de flexibilité et peut s'équiper rapidement d'un logiciel pour répondre à un besoin ponctuel sans passer par la DSI, qui est ainsi libérée de tâches apportant peu de valeur ajoutée. Décentralisation et flexibilité facilitent de plus l'exploration de nouveaux usages, les échanges et apprentissages. L'un des DSI nous a par exemple expliqué comment le contrôle social permet de mieux développer et transmettre les compétences informatiques : *« On est plutôt partis sur une politique d'* « ambassadeurs », qui sont un peu plus geeks (ou pas, d'*ailleurs), mais qu'on sensibilise d'une façon plus fine à l'usage et qui sont là aussi pour transmettre les bons usages, les bons tuyaux, etc… On est convaincus que c'est le bon mode de fonctionnement…* [ça] *nous semble plus opportun que de la formation, qui est malheureusement aujourd'hui un peu vite oubliée » (DSI, CA).*

L'adéquation à la culture numérique évite par ailleurs les frictions qui compliqueraient l'internalisation des normes et valeurs, comme la DSI du centre d'appel nous l'a expliqué : *« On est aussi convaincus que* c'*est dans le sens de l'histoire. On le voit par rapport aux plus jeunes qui nous rejoignent et qui gardent la page facebook ouverte toute la journée… ça gratouille un peu les plus anciens, qui ne comprennent pas comment ils peuvent travailler… et en même temps, ils sont tout aussi efficaces que leurs collègues… Donc c'est aussi la culture d'entreprise qu'il faut faire évoluer… […] Je pense qu'on pourra difficilement lutter contre ça. Les gens sont tous hyper connectés* » (DSI, CA). L'utilisateur peut ainsi bricoler son propre assemblage d'outils, participer à la conception de son travail en fonction de ses propres capacités et préférences, et pratiquer une remédiation de ses habitudes numériques.

Enfin, ces contrôles sociaux favorisent un climat d'échange et d'implication, permettant de préserver la confiance en la DSI qui est essentielle dans la gestion des pratiques invisibles. Un autre DSI explique ainsi : *« On a souvent des collaborateurs qui viennent nous demander des conseils sur l'achat de téléphones, le volet sécurité, etc. y compris pour leur usage personnel... Parce qu'on est en toute confiance entre nous, c'est plutôt une équipe proche des utilisateurs qu'une équipe répressive. Et on a volontairement internalisé les équipes, on ne les a pas sous-traitées, pour rester très proches des collaborateurs. Ça coûte sans doute un petit peu plus cher, mais il y a une espèce de connivence on va dire… C'est plutôt des collègues que l'*équipe informatique » (DSI, BS). Il ajoute : *« L'objectif, c'est « Pourquoi » on met en place des obligations pour contourner des*

*risques. […] C'est notre rôle d'*être de bon conseil, plutôt que d'*interdire. Et ça passe beaucoup mieux »* (DSI, BS). Plutôt que de tenter de contrôler les publications des employés en ligne, le DSI du centre d'appel, dans lequel les employés réalisent un travail répétitif, a également expliqué travailler sur l'atmosphère de travail plutôt que sur le contrôle de ses conséquences négatives : « *on préfère être sur une politique de la confiance et travailler au bien-être de nos collaborateurs pour qu'ils n'aient pas l'envie de dénigrer l'entreprise* » (DSI, CA). Cette politique contraste avec certaines politiques de contrôle par les comportements et paraît risquée à certains DSI. Celui de la fonderie a par exemple explicitement mentionné un climat social tendu comme cause aux réticences initiales de l'équipe de direction à déverrouiller les réseaux sociaux. Dans le cas du centre d'appel, cette politique n'a néanmoins pas généré de publications problématiques.

4.4. Implications pour les dispositifs de gestion des usages

Ces résultats invitent à réorienter le contrôle des usages vers des dispositifs de socialisation, à la fois dans les chartes informatiques et dans les autres systèmes de contrôles. Des chartes peuvent bien entendu être formalisées à des fins de protection légale, mais seront dans ce cas peu efficaces pour gérer les usages que font les utilisateurs des technologies numériques basées sur Internet. Les règles souvent techniques qui y sont développées ne dissuadent pas les utilisateurs, sont peu adaptées à leurs contraintes locales, mais surtout ne constituent pas un vecteur d'internalisation des principes qui doivent diriger leurs pratiques. Il est donc essentiel de leur présenter les principes, normes et valeurs qu'ils doivent mettre en pratique, en tolérant suffisamment de flexibilité pour qu'ils le fassent d'une manière adaptée à leurs contextes particuliers d'usage. Pour faciliter l'internalisation de ces principes et améliorer leur applicabilité, les principes fondamentaux qui doivent guider la prise de décision par les utilisateurs ainsi que des exemples concrets du raisonnement guidant leur mise en pratique peuvent être présentés pour que l'utilisateur puisse par analogie les adapter à son contexte d'usage de manière flexible (Loch *et al.*, 1998). Cette décentralisation peut se prolonger dans la forme des documents eux-mêmes, qui peuvent être modularisés en présentant les éléments de la charte à l'utilisateur sur le lieu du besoin, au moment du besoin (notifications contextualisées, liens hypertextes) (Wood, 2000). L'utilisateur dispose ainsi des éléments nécessaires à une prise de décision autonome, lui évitant d'interrompre son travail pour se diriger vers un répertoire centralisé au caractère juridique et technique[2]. Plutôt que de pratiquer une simple application d'une règle comportementale, il internalise ces principes en les instanciant lui-même à plusieurs reprises dans sa pratique, développant ainsi des connaissances appliquées qu'il peut alors diffuser dans l'organisation.

Si les chartes informatiques peuvent servir de support pour formaliser les principes fondamentaux qui doivent guider la prise de décision des utilisateurs en situation, l'organisation doit toutefois concevoir des dispositifs de contrôle par socialisation pour que les utilisateurs les internalisent. Baser un système de gestion des usages numériques sur des contrôles par socialisation implique alors de reconcevoir le travail de sécurité comme un travail de gestion des usages centré sur l'utilisateur. Il s'agit de considérer ses contraintes opérationnelles, mais aussi les effets négatifs de contrôles trop stricts. Pour cela, reconnaître le rôle

[2] Cette hypothèse est qualifiée d' « hautement improbable » par Wood (2000).

important des utilisateurs les plus avertis dans l'identification d'inadaptations des règles aux contextes d'usage, dans le partage de connaissances ainsi que dans le travail de sensibilisation est essentiel. Certaines des entreprises interrogées ont par exemple mis en place des forums d'échange organisés par ce type d'utilisateurs (avec le soutien des équipes informatiques). Ils y évoquent une problématique particulière durant une demi-heure ou une heure devant des utilisateurs volontairement inscrits, qui eux-mêmes transmettent de manière informelle les connaissances ainsi acquises à leurs collègues pour aider au développement des normes d'usage. Dans une autre, des rites organisationnels informels se sont développés et répandus dans l'organisation pour que les utilisateurs internalisent des principes de base. Lorsque l'un d'entre eux oublie par exemple de verrouiller sa session, un de ses collègues utilise sa messagerie pour offrir en son nom des croissants à l'équipe le lendemain. Le DSI commente : « *lorsque vous en avez marre d'apporter les croissants, vous verrouillez votre session. C'est passé dans les usages et dans tous les services… C'est très drôle, le matin on arrive de temps en temps, il y a des bonbons, des croissants* » (DSI, FI). D'autres misent sur des bases de connaissances alimentées de manière participative, ou sur une courte note de sécurité hebdomadaire par e-mail, rédigée sur un ton informel et présentant un type particulier de menaces aux utilisateurs. De courtes réunions régulières s'appuyant sur un exemple emblématique tel que ceux cités en introduction peuvent ainsi s'avérer plus efficaces que des formations génériques, formelles et « *vite oubliées* ». Bien que l'implication des utilisateurs et le développement d'un climat de confiance avec les équipes informatiques facilitent la détection d'usages problématiques, cela implique toutefois d'aller à l'encontre des recommandations qui préconisent un accroissement des sanctions et de la surveillance des utilisateurs. Adopter une telle approche de la gestion des usages par les valeurs fondamentales de l'organisation plutôt que par la sécurité informatique (laquelle peut toutefois en faire partie) peut cependant représenter une réelle transformation culturelle pour certaines DSI. Celles-ci doivent non seulement accepter que d'autres acteurs participent à l'établissement des principes d'usage de l'organisation, mais également concéder une partie de leur autorité sur les questions de gestion des usages tout en se saisissant de problématiques qui les éloignent de leur rôle traditionnel de sécurisation.

5. DISCUSSION

5.1. Propositions sur l'adéquation des modes de contrôle à la gestion des usages des technologies numériques basées sur Internet

Nos résultats suggèrent donc que les contrôles par les comportements permettent centralisation et stabilité, mais offrent toutefois trop peu de flexibilité et de distribution du contrôle. Celles-ci semblent pourtant nécessaires pour adapter la gestion des usages des technologies numériques aussi bien dans le temps qu'entre divisions fonctionnelles ou profils d'utilisateurs. L'absence de flexibilité et de décentralisation des décisions d'usage génère par ailleurs des tensions entre utilisateurs et DSI, qui s'accusent mutuellement de nuire au travail de sécurité des uns ou à la productivité des autres (Denis, 2012 ; Koch *et al.*, 2014 dans le cas du BYOD). En effet, sous contrôle comportemental chaque demande singulière d'un utilisateur doit faire l'objet d'une évaluation par la DSI, et se heurter à son refus ou attendre son approbation et son intervention. Les

usages ne peuvent alors que difficilement faire preuve de flexibilité et ne peuvent être conçus au plus proches des besoins par les utilisateurs en situation. Cette absence de flexibilité et de décentralisation des décisions d'usage explique la faible applicabilité en contexte des règles comportementales qui constituent les chartes informatiques. Elle conduit par ailleurs les contrôles à une obsolescence rapide face à l'émergence d'usages imprévisibles, notamment par des utilisateurs expérimentés qui maîtrisent mieux le mode de représentation de leur activité dans le dispositif de contrôle et peuvent le contourner plus aisément encore (Leclercq-Vandelannoitte, 2017). En plus de constituer un facteur de défiance envers la DSI, ces stratégies de dissuasion par la surveillance produisent une illusion de sécurité et peuvent générer autant d'usages cachés qu'elles n'en révèlent. Les contrôles basés sur le pistage des comportements sont par ailleurs peu appréciés des utilisateurs (Cecere *et al.*, 2015). Nuisant à leur sens de l'autonomie, ils n'engendrent souvent que de simples réponses de conformité (Ouchi, 1979), et ne suscitent guère d'implication dans les problématiques de sécurité, de confidentialité, ou de préservation de la réputation en ligne. Enfin, leur rigidité empêche participation, remédiation de nos pratiques, et bricolage personnalisé. Certes adaptés au contrôle d'utilisateurs novices dans des systèmes fermés dont l'évolution était fortement planifiée par les DSI, les contrôles comportementaux peuvent aujourd'hui constituer une source de paralysie organisationnelle qui empêche l'organisation de saisir les opportunités numériques. Nous proposons donc :

P1 : Le contrôle par l'observation, la mesure et le confinement technique des comportements est moins adapté à la culture numérique. Il répond au besoin de centralisation et de stabilité, mais ne répond pas simultanément au besoin de flexibilité et de distribution du contrôle.

Hormis en transférant le contrôle de l'usage à des fins personnelles aux managers opérationnels ou pour décourager le stockage des données en local, les organisations interrogées n'ont pas mis en place de politiques basées sur des contrôles par les résultats. Deux explications justifient cette absence. D'une part, ces contrôles sont limités par la présence d'un problème multi-objectifs lié aux divergences entre objectifs de la DSI et des autres entités organisationnelles (Koch *et al.*, 2014). Les utilisateurs risquent ainsi de prioriser leurs objectifs opérationnels plutôt que les résultats liés à la sécurité ou à la confidentialité des données. L'incapacité de mesurer et d'imputer efficacement de mauvais résultats complique d'autant plus le recours à ces contrôles. Une compromission de données sensibles sur un espace cloud personnel peut par exemple n'être exploitée par une personne malveillante que plusieurs années plus tard, sans que l'organisation ne le perçoive ou ne puisse identifier la source de la fuite. D'autre part, la faible capacité de ces contrôles à assurer stabilité et centralisation des décisions d'usage et du contrôle conduirait à l'émergence de pratiques très hétérogènes et difficilement contrôlables. Un contrôle largement basé sur les résultats est donc peu approprié pour gérer tous les risques liés aux usages numériques, mais peut se substituer efficacement au contrôle comportemental pour gérer l'usage des outils à des fins personnelles. Le contrôle de ces usages est ainsi plus flexible et décentralisé, facilitant le développement des compétences et l'acceptabilité du contrôle par les utilisateurs. À partir de nos résultats, nous formulons donc la proposition suivante :

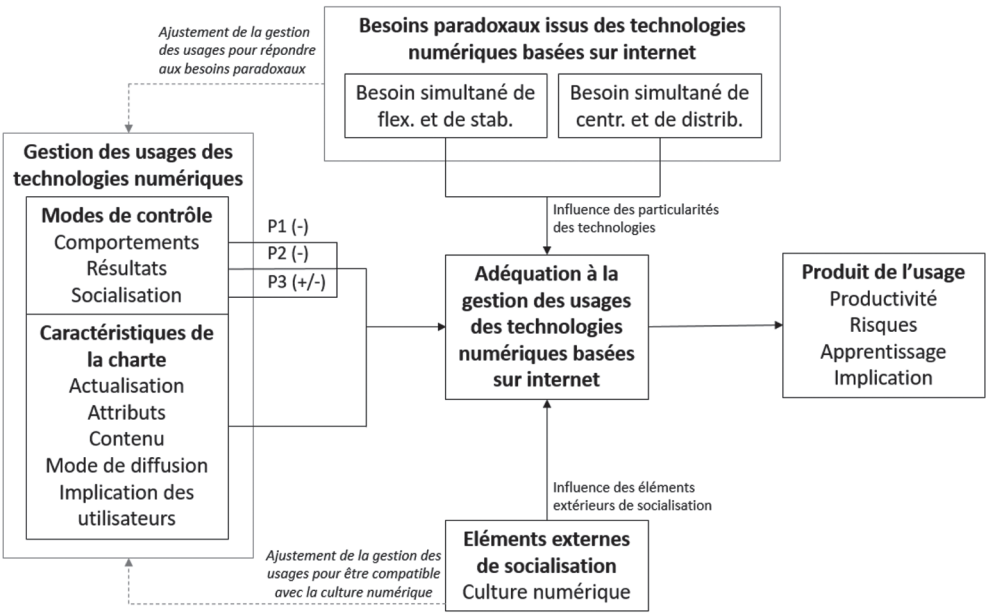
P2 : Le contrôle par la mesure des résultats est adapté à la culture numérique. Il répond au besoin de flexibilité et de distribution du contrôle, mais ne répond pas simultanément au besoin de centralisation et de stabilité.

Enfin, les contrôles par socialisation sont les seuls à pouvoir potentiellement répondre à tous les besoins paradoxaux sans incompatibilité avec les éléments de culture numérique considérés. Centralisation et stabilité permettent d'éviter une trop forte hétérogénéité des usages, de préserver les principes fondamentaux, et de transformer en routines les usages émergents. La conversion de la norme centrale en usage local par l'utilisateur lui permet de mieux l'internaliser puisqu'il doit lui-même l'instancier dans sa pratique de manière régulière, et donc s'engager personnellement dans la problématique d'usage. Cet engagement est par exemple nécessaire pour résoudre en situation un dilemme éthique (Walsham, 1996), mais est limité dans le cas de contrôles comportementaux qui n'appellent qu'une réponse mécanique. Flexibilité et distribution du contrôle permettent par ailleurs de faire face à la variabilité, à l'imprévisibilité, et au caractère émergent des usages à mesure qu'ils ou que les technologies évoluent. Contrairement au corpus monolithique de règles comportementales ou à l'instabilité des usages que génère un contrôle par les résultats, ces contrôles sociaux permettent potentiellement un couplage lâche entre la norme organisationnelle et sa mise en pratique par les utilisateurs. Cette souplesse permet une meilleure flexibilité des usages et rend les contrôles plus tolérables pour les utilisateurs. Ces derniers bénéficient ainsi d'une plus grande autonomie et peuvent s'impliquer dans la gestion des usages, sans toutefois mettre à mal les éléments fondamentaux du système. Le contrôle par socialisation peut ainsi permettre de bénéficier des avantages de deux précédents modes de contrôle sans souffrir de leurs faiblesses. La métaphore numérique de la plateforme illustre cette articulation qui résout les paradoxes du changement et du contrôle au moyen d'un assemblage à la fois stable et flexible et associant un contrôle centralisé et simultanément distribué. Ce modèle de gouvernance articulant un cœur stable de principes fondamentaux et des règles périphériques souples est d'ailleurs à la base du fonctionnement d'organisations entièrement basées sur Internet telles que Wikipédia (Cardon & Levrel, 2009), confirmant sa capacité à préserver la stabilité organisationnelle malgré une forte décentralisation. À partir des éléments précédents, nous proposons :

P3 : Le contrôle par socialisation est adapté à la culture numérique, et permet de répondre simultanément aux besoins paradoxaux.

Les contrôles par socialisation ne sont néanmoins pas *nécessairement* efficaces pour gérer les usages numériques. En effet, bien qu'ils soient plus adaptés au contrôle de l'usage des technologies numériques, nous identifions trois situations qui pourraient conduire à leur échec. En premier lieu, l'internalisation des normes et des valeurs peut être trop forte, au point que le moindre écart à celles-ci entraîne une sanction sociale importante, réduisant toute possibilité de flexibilité. L'un des DSI interrogés nous a par exemple confié sa crainte de voir émerger un système de sanction sociale délétère pour l'ambiance de travail et basé sur la délation (absence de flexibilité). D'autres recherches décrivent des contrôles par les pairs potentiellement intrusifs (Leclercq-Vandelannoitte *et al.*, 2014). Ce risque peut néanmoins être limité en l'absence de sanctions fortes. À l'inverse, ces dispositifs peuvent se révéler instables si les normes collectives sont trop mouvantes, ambiguës, ou trop faiblement partagées entre les utilisateurs (absence de stabilité ou de centralisation). Par exemple, une politique de personnalisation des outils de mobilité n'apporte de stabilité que si elle réduit effectivement les divergences dans les préférences des utilisateurs, sous peine de voir émerger des configurations hétérogènes et difficilement contrôlables. Enfin,

Figure 2 : Modèle d'ajustement de la gestion des usages aux technologies numériques basées sur Internet



des dissonances manifestes entre différents éléments de socialisation ou divers éléments de contrôle peuvent également expliquer selon nous une part de l'inefficacité des dispositifs de socialisation actuels. Nous avons par exemple constaté un décalage presque systématique entre chartes informatiques et politiques effectives des organisations, compliquant pour les utilisateurs la compréhension des normes organisationnelles. De même, la volonté d'implication des utilisateurs semble incompatible avec le registre juridique distant, voire menaçant, des chartes informatiques, qui ne peuvent alors que difficilement constituer un vecteur d'internalisation, d'implication, de confiance en la DSI, et d'apprentissage de nouveaux usages.

Nous présentons nos trois propositions dans le modèle d'ajustement de la gestion des usages aux technologies numériques basées sur Internet dans la figure 2 ci-dessous. Celui-ci met en avant une approche émergente des usages qui tient compte des particularités des technologies numériques basées sur Internet (besoins paradoxaux) ainsi que de celles des utilisateurs (culture numérique) pour y ajuster la gestion des usages (modes de contrôles et chartes informatiques), et ainsi influencer le milieu de formation des comportements par des dispositifs de socialisation.

5.2. Une approche de la gestion des usages priorisant le contrôle par socialisation

En réponse à plusieurs appels à explorer d'autres approches de la gestion des usages (Cram *et al.*, 2017 ; Willison & Warkentin, 2013), cette analyse de l'adéquation de différents modes de contrôle à la gestion des usages des technologies numériques basées sur Internet nous permet de proposer d'en ajuster la gestion en priorisant les contrôles par socialisation. Ceux-ci semblent

en effet plus adaptés lorsque sont considérées les particularités de ces technologies, de leurs utilisateurs et de la relation qu'ils entretiennent avec elles, ainsi que les dynamiques organisationnelles qui entourent la formation des usages et leur contrôle.

En premier lieu, en considérant les multiples tensions que la gestion des usages doit traiter au-delà des problématiques de productivité et de sécurité informatique, cette approche aide à identifier les effets négatifs de certaines politiques sur d'autres variables. Pour les organisations à tendance disciplinaire, nous soulignons le risque d'enfermement dans une spirale de contrôle comportemental ainsi que ses potentiels effets délétères liés à l'absence de flexibilité, de distribution du contrôle, et d'adéquation à la culture numérique : obsolescence rapide des règles et des dispositifs de contrôle, perte d'implication et d'effets d'apprentissage, comportements de résistance et de dissimulation, méfiance envers la DSI, et illusion de surveillance totale[3]. Ces effets peuvent nuire indirectement à la sécurité (Cram *et al.*, 2017), mais ne peuvent être capturés par les approches comportementales, dont l'approche essentiellement déterministe suggérerait une nouvelle intensification des contrôles. Dans de tels systèmes, les utilisateurs risquent pourtant de limiter leurs initiatives à celles visant à se soustraire à la surveillance. Le recours à une théorie des besoins paradoxaux permet toutefois d'éviter de considérer tous les objectifs de la gestion des usages (qui peuvent par ailleurs évoluer) au moyen d'objectifs plus généraux. De ce point de vue, nous proposons une approche équilibrée entre la spécification fine des objectifs (et donc une focalisation qui implique nécessairement d'en occulter d'autres), et la difficile prise en compte de tous les objectifs que peut poursuivre la gestion des usages et qu'identifient les approches par les chartes informatiques. En effet, la recherche simultanée de centralisation et de distribution du contrôle ainsi que de stabilité et de flexibilité peut constituer un objectif de plus haut niveau et fournir une heuristique qui permette de maîtriser l'évolutivité et la variabilité des usages. La recherche de flexibilité et de distribution du contrôle qui font défaut aux contrôles comportementaux permet alors de considérer les causes de non-conformité des comportements individuels (par exemple, la présence d'objectifs contradictoires, le besoin d'adapter la règle aux contraintes locales, de prendre des décisions d'usage rapides, ou encore de personnaliser outils et pratiques). Cette approche permet également de tenir compte des objectifs organisationnels en proposant que le système de contrôle vise à produire simultanément suffisamment de centralisation et de stabilité dans les usages et leur contrôle. Elle évite ainsi l'un des problèmes majeurs des approches centrées sur les utilisateurs, qui peinent à établir une conciliation entre intérêts individuels et politiques de l'organisation, générant des usages hétérogènes, instables, et peu contrôlables (Siponen, 2000b). L'approche par les besoins paradoxaux peut permettre cette conciliation, aidant ainsi à considérer les usages au sein des dynamiques organisationnelles dans lesquelles ils se forment. En particulier, des contrôles par socialisation peuvent remplir cet objectif puisque l'organisation peut concentrer ses efforts sur la construction du dispositif de socialisation, lui fournir un cadre et influencer son contenu et son évolution tout en décentralisant autant que possible les décisions d'usage à l'utilisateur.

[3] Dans une mesure qui reste à évaluer dans le cadre des usages informatiques, les contrôles comportementaux stricts pourraient également réduire la productivité en raison de contraintes sur les objectifs opérationnels, de leur manque de flexibilité, et d'un possible effet Hawthorne inversé (Bernstein, 2012) où la transparence des comportements conduit les utilisateurs à ne pas améliorer leurs pratiques.

Ils s'approchent ainsi d'un système de gouvernance libérale des TI : ils visent à produire centralisation et stabilité en influençant le « milieu » de formation des usages et non directement les comportements (Leclercq-Vandelannoitte & Bertin, 2018), tandis qu'un contrôle coconstruit et distribué entre pairs (Leclercq-Vandelannoitte *et al.*, 2014) apporte flexibilité, décentralisation, et adéquation à la culture numérique.

En second lieu, cette approche permet de considérer différents modes de contrôle et ce faisant, de tenir compte de la possibilité d'exploiter dans une perspective instrumentale le contrôle clanique (Chua *et al.*, 2012) ou encore les croyances normatives (Bulgurcu *et al.*, 2010) et normes descriptives (Herath & Rao, 2009). Celles-ci sont en effet centrales y compris dans la théorie du comportement planifié (Ajzen, 1991) et sont parfois plus influentes que les sanctions formelles (e.g. Li *et al.*, 2010). Bien que certaines approches comportementales mettent en lumière l'influence des dynamiques sociales et reconnaissent qu'exploiter la culture organisationnelle peut aider à générer une motivation intrinsèque chez l'utilisateur (e.g. Johnston & Warkentin, 2010), cette motivation requiert un sentiment d'autodétermination et de liberté que les approches disciplinaires basées sur la théorie de la dissuasion, la contrainte et la sanction occultent (Siponen, 2000). En évitant la focalisation sur la surveillance et les sanctions, les communications basées sur la peur ou le confinement technique de l'action, nous proposons de considérer l'importance de la légitimité perçue de la politique de gestion des usages (Bijlsma-Frankema & Costa, 2010) ou encore du rôle de la participation des utilisateurs (Spears & Barki, 2010). Nous suggérons ainsi de privilégier des approches sociales du contrôle, par exemple basées sur la confiance organisationnelle (Lee *et al.*, 2004). À l'inverse de certains travaux tenant compte des dynamiques sociales et des politiques disciplinaires (e.g. Herath & Rao, 2009), ces deux approches présentent des incompatibilités fortes qui pourraient causer de fortes différences entre intentions déclarées et comportements. Enfin, notre approche considère également l'adéquation des modes de contrôles à des facteurs de socialisation extérieurs à l'organisation (ici, les dimensions principales de la culture numérique), aidant ainsi à tenir compte de la complexité des dynamiques dont émergent les usages. Nous suggérons sur ce point une incompatibilité grandissante entre culture numérique et contrôle comportementaux, qui ne permettent ni participation, ni bricolage, ni remédiation des habitudes d'usage. Or, ces éléments de culture numérique constituent des normes d'usage personnelles, lesquelles conduisent à rejeter les messages basés sur la peur (Li *et al.*, 2010). Ces derniers sont d'autant moins efficaces qu'ils sont moins tolérables pour les utilisateurs et réduisent leur implication, s'ils n'engendrent pas des comportements de réaction au contrôle (Lowry & Moody, 2015). À l'inverse des perspectives disciplinaires, nous suggérons donc que dans des environnements d'usage instables et hétérogènes où les pratiques émergent de manière non anticipée, flexibilité et autonomie sont non seulement nécessaires, mais représentent une opportunité de faire de l'utilisateur un atout important pour la gestion des usages numériques. Pour cela et à l'inverse de recommandations antérieures (Johnston & Warkentin, 2010), il est néanmoins nécessaire de l'impliquer dans les problèmes de gestion des usages en lui décentralisant autant que possible les décisions inhérentes.

Pour les organisations, ce point semble particulièrement important alors que nombreuses d'entre elles sont à la croisée des chemins entre intensification et relâchement des contrôles informatisés. Notre analyse ne suggère bien entendu pas de supprimer tout contrôle comportemental.

Certains constituent des nécessités légales, d'autres sont utiles à la protection juridique de l'organisation et de ses dirigeants, et d'autres enfin sont nécessaires à la protection d'éléments critiques du SI et au travail d'investigation technique. Il semble par exemple tout à fait acceptable de limiter la personnalisation des logiciels à un catalogue, de proposer des conseils éditoriaux pour la publication sur les médias sociaux, de forcer les utilisateurs à utiliser un mot de passe, ou encore de mettre en place des systèmes de surveillance permettant de détecter des anomalies importantes dans les flux de données. Pour conserver une capacité de changement qui permette de saisir les opportunités apportées par les technologies numériques, nous suggérons néanmoins un renversement de la hiérarchie des modes de contrôles pour concevoir le système de socialisation comme le mode de contrôle dominant, et les contrôles par les comportements et par les résultats comme des contrôles accessoires, des filets de sécurité visant à se prémunir d'éventuels échecs de socialisation. Ils peuvent ainsi être réservés à des points de contrôle centraux et critiques qui permettraient d'assurer une base d'usages stables au SI, tout en permettant la flexibilité et la distribution du contrôle nécessaires à la saisie de nouvelles opportunités numériques et à l'apprentissage de nouveaux usages. À l'aide de données empiriques et en identifiant des politiques particulières, nous appuyons l'intérêt pour les entreprises d'une approche libérale de la gouvernance des TI (Leclercq-Vandelannoitte & Bertin, 2018). Correspondant au passage de la discipline d'une population passive à des dispositifs de régulation visant à influencer le « milieu » où se forment librement les comportements, ce modèle de gouvernance cherche à gouverner moins plutôt qu'à gouverner plus. Toutefois, bien que nous identifiions d'autres effets négatifs de règles restrictives et de la médiation par les DSI de la relation entre utilisateurs et technologies et que nous suggérions de considérer les utilisateurs comme acteurs devant mettre en place leur propre gouvernance par le partage de normes émergentes, nous identifions également certaines limites empiriques à la construction de ce type de gouvernance. En effet, la responsabilité individuelle ou locale, contrepartie à l'autonomie des utilisateurs dans une gouvernance libérale des TI, paraît difficile à mettre en place dans nos données. Non seulement le contrôle par les résultats de l'usage se heurte à des problèmes d'objectifs concurrents et à des difficultés de mesure et d'imputation qui génèrent en pratique une absence de responsabilité, mais ce type de contrôle permet peu de centralisation et de stabilité, pouvant ainsi générer une forte hétérogénéité des usages.

5.3. Limites et voies de recherche

Certaines limites de notre approche doivent néanmoins être soulignées. En raison du caractère qualitatif de nos données, nous nous sommes limités à l'identification de frictions entre modes de contrôles, particularités des environnements d'usage numériques et des utilisateurs qui y agissent, sans les mesurer quantitativement. Nous identifions toutefois des effets négatifs liés au mode de contrôle, que des approches comportementales peuvent intégrer pour considérer leur effet sur d'autres variables que la sécurité. De telles mesures sur un plus grand échantillon d'entreprises pourraient confirmer ces résultats ou les nuancer selon le contexte de l'organisation. En particulier, nous avons ignoré divers facteurs de contingence tels que la taille de l'organisation, la sensibilité de ses données, le dynamisme de son environnement (qui implique des besoins de flexibilité différents), ou encore le niveau de compétence des utilisateurs et la culture organisationnelle. Ce

dernier facteur complexifie la recherche d'un point d'équilibre, qui doit s'accommoder de la culture d'entreprise, de la culture numérique, et des besoins paradoxaux. Pour cette raison, et compte tenu du caractère ubiquitaire des technologies numériques, il pourrait être plus adéquat d'aligner la culture de l'organisation sur la culture numérique (comme le suggère le DSI du centre d'appel). Une autre limite importante tient à la définition de la culture numérique retenue, et qui procède par simplification (Deuze, 2006). Il existe en réalité une myriade de cultures et sous-cultures numériques, qui pourront dans le futur constituer un élément de différenciation pour les organisations, mais aussi donner lieu à des frictions entre différentes sous-cultures (Rowe & Monod, 2000). Enfin, bien que permettant d'identifier un large spectre de conséquences du recours à différents modes de contrôle des usages, cette approche systémique des politiques qui visent à les gérer conduit nécessairement à renoncer à analyser finement chaque cas d'usage.

Bien que nous pensions avoir identifié une inadaptation des contrôles comportementaux à la gestion des usages numériques basés sur Internet et une potentielle adéquation des contrôles par socialisation, notre analyse déplace le problème du contrôle du respect des règles vers la conception d'un dispositif efficace d'internalisation des valeurs. En effet, bien que les approches comportementales disciplinaires aient identifié le rôle des contrôles par socialisation, peu de travaux ont exploré comment les concevoir et les exploiter. Ce déplacement soulève donc deux questions importantes. La première est relative au mécanisme de socialisation. Quels dispositifs de socialisation permettent de résoudre les paradoxes du changement et du contrôle et sont compatibles avec la culture numérique ? Cette question nous semble importante au vu de l'inefficacité de certaines formations ou notes de sensibilisation, dont le caractère générique pourrait expliquer selon nous une bonne partie des difficultés d'internalisation. Décrire d'autres mécanismes de socialisation moins génériques que des formations ainsi que les conditions dans lesquelles ils sont efficaces pourrait inspirer des organisations dans la conception de leurs dispositifs d'internalisation des valeurs. D'autre part, ces discussions soulèvent la question du contenu de la socialisation, car si le mode de contrôle semble plus adapté, son contenu (les valeurs et principes) exerce sans doute une influence importante sur son internalisation, et peut à notre avis se révéler largement aussi incompatible avec par exemple, la flexibilité ou le bricolage. Un contrôle social fondé sur la peur du risque informatique (ou de la sanction) pourrait par exemple paralyser toute initiative, ou se révéler contre-productif si les utilisateurs rejettent la norme et réagissent en réduisant leur peur du risque plutôt que les risques eux-mêmes (Richet & Rowe, 2014). À l'inverse, explorer les approches basées sur la légitimité du contrôle (Bijlsma-Frankema & Costa, 2010) ou sur la justice organisationnelle (Willison & Warkentin, 2013) pourrait par exemple permettre de mieux comprendre quel contenu du dispositif de socialisation est internalisable ou non par les utilisateurs.

CONCLUSION

En basant notre analyse de l'adéquation de différents modes de contrôle à la gestion des usages des technologies numériques basées sur Internet sur une perspective émergente de ces derniers, nous alertons sur les effets contre-productifs des contrôles comportementaux pour la gestion de ces usages et invitons à analyser l'efficacité des contrôles d'une manière plus large que par la seule évaluation de la conformité du comportement à la règle. Bien que réduisant

en apparence les risques liés à l'usage, ces contrôles risquent non seulement de se révéler peu efficaces et d'induire des réponses négatives des utilisateurs, mais par ailleurs de compliquer l'adaptation de l'organisation aux technologies numériques. Nous proposons donc un renversement de la hiérarchie des modes de contrôle des usages des technologies numériques pour prioriser les contrôles par socialisation et réserver les autres modes de contrôles à des éléments du système d'information dont la stabilité et le contrôle central sont critiques. Ce renversement permet de construire une gestion des usages en plateforme, articulant une périphérie flexible et décentralisée d'usages à un cœur stable de principes fondamentaux et internalisés par les utilisateurs. Cette forme de gestion des usages numériques, conçue comme un travail continu et collectif d'implication, de sensibilisation, et de développement des compétences, peut non seulement se révéler efficace dans la gestion des risques, mais permet par ailleurs de mieux préparer l'organisation et ses utilisateurs à agir dans leurs futurs environnements numériques.

RÉFÉRENCES

Ahuja S. & Gallupe B. (2015), "A Foundation for the Study of Personal Cloud Computing in Organizations", *21st Americas Conference on Information Systems*, Puerto Rico.

Ajzen I. (1991), "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes*, vol. 50, n°2, p. 179-211.

Andriole S.J. (2015), "Who Owns IT?", *Communications of the ACM*, vol. 58, n°3, p. 50–57.

Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., Zaharia M. (2010), "A view of cloud computing", *Communications of the ACM*, vol. 53, n°4, p. 50-58.

Bahli B. & Benslimane Y. (2004), "An Exploration of Wireless Computing Risks: Development of a Risk Taxonomy", *Information Management & Computer Security*, vol. 12, n°3, p. 245-254.

Baruch Y. (2000), "Teleworking: Benefits and Pitfalls as Perceived by Professionals and Managers", *New Technology, Work and Employment*, vol. 15, n°1, p. 34-49.

Bergeron F. & Berube C. (1990), "End Users Talk Computer Policy", *Journal of Systems Management*, vol. 41, n°12, p. 14-32.

Bernstein E.S. (2012), "The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control", *Administrative Science Quarterly*, vol. 57, n°12, p. 181-216.

Berryman M. (2008), "IT policy: Setting Sensible Internet Policies. a Rapidly Evolving Web Environment Requires Employers to Develop Smarter Internet-Use Policies", *New Zealand Management*, vol. 55, n°1, p. 43.

Bijlsma-Frankema K.M. & Costa A.C. (2010), "Consequences and Antecedents of Managerial and Employee Legitimacy Interpretations of Control: a Natural, Open System Approach", dans Organizational Control, S.B. Sitkin, L.B Cardinal, K.M. Bijlsma-Frankema (eds), Cambridge University Press, Cambridge, UK, p. 396-434.

Bolter J.D. & Grusin R. (1999), "*Remediation: Understanding new media*", MIT Press, Cambridge, USA.

Boss S.R., Kirsch L.J., Angermeier I., Shingler R.A., Boss R.W. (2009), "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security", *European Journal of Information Systems*, vol. 18, n°2, p. 151-164.

Broadbent S. (2016), "Intimacy at work: How digital media bring private life to the workplace", Routledge, Walnut Creek, CA, USA.

Bulgurcu B., Cavusoglu H., Benbasat I. (2010), "Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly*, vol. 34, n°3, p. 523-548.

CA Versailles, 17e chambre, 4 février 2015, Monsieur Q K contre SAS MESSER, n° 12/02764

Cardon D. & Levrel J. (2009), "La vigilance participative. Une interprétation de la gouvernance de Wikipédia", *Réseaux*, vol. 154, n°2, p. 51-89.

Cass., Civ., Com. 10 fév 2015, n°13/14779.

Cass., Civ., Soc., 19 déc 2018, n°17/14631.

Cbsnews (2013), "Applebee's Waitress Fired for Posting Customer Comment Online", accessible le 24/04/2020 depuis https://www.cbsnews.com/news/applebees-waitress-fired-for-posting-customer-comment-online/

Cecere G., Le Guel F., Rochelandet F. (2015), "Les modèles d'affaires numériques sont-ils trop indiscrets ?", *Réseaux*, vol. 189, n°1, p. 77-101.

Chérigny F. (2012), "La charte des bons usages des services de réseautage social, outil juridique au service d'une stratégie-réseau", *Revue Internationale d'Intelligence Economique*, vol. 4, n°1, p. 71-85.

Chua C.E.H., Lim W.K., Soh C., Sia S.K. (2012), "Enacting clan control in complex IT projects: A social capital perspective", *MIS Quarterly*, vol. 36, n°2, p. 577-600.

Coker B. L. (2011). "Freedom to surf: the positive effects of workplace Internet leisure browsing", *New Technology, Work and Employment*, vol. 26, n°3, p. 238-247.

CPH Boulogne-Billancourt 19 nov. 2010, Madame S. contre Société Alten Sir, n° 09/00343 et 09/00316.

Cram W.A., Proudfoot J.G., D'Arcy J. (2017), "Organizational Information Security Policies: a Review and Research Framework", *European Journal of Information Systems*, vol. 26, n°6, p. 605-641.

Crenn G. & Vidal G. (2010), "Les musées et le Web 2.0 : approches méthodologiques pour l'analyse des usages", dans *Web social : mutation de la communication*, F. Millerand, S. Proulx, J. Rueff (Eds), Presses de l'Université du Québec, Le Delta, Canada.

Daniels K., Lamond D., Standen P. (2001), "Teleworking: Frameworks for Organizational Research", *Journal of Management Studies*, vol. 38, n°8, p. 1151-1185.

D'Arcy J., Gupta A., Tarafdar M., Turel O. (2014), "Reflecting on the 'Dark Side' of Information Technology Use", *Communications of the Association for Information Systems*, vol. 35, n°5, p. 109-118.

D'arcy J. & Herath T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, vol. 20, n°6, p. 643-658.

Denis J. (2012), "L'informatique et sa sécurité", *Réseaux*, vol. 171, n°1, 161-187.

Deuze M. (2006), "Participation, Remediation, Bricolage: Considering Principal Components of a Digital Culture", *The Information Society*, vol. 22, n°2, p. 63-75.

Doherty N.F. & Fulford H. (2005), "Do Information Security Policies Reduce the Incidence of Security Breaches: an Exploratory Analysis", *Information Resources Management Journal*, vol. 18, n°4, p. 21-39.

Dong J.Q. & Wu W. (2015), "Business Value of Social Media Technologies: Evidence from Online User Innovation Communities", *The Journal of Strategic Information Systems*, vol. 24, n°2, p. 113-127.

Drumwright M.E. & Murphy P.E. (2009), "The Current State of Advertising Ethics: Industry and Academic Perspectives", *Journal of Advertising*, vol. 38, n°1, p. 83-108.

Farjoun M. (2010), "Beyond Dualism: Stability and Change as a Duality", *Academy of Management Review*, vol. 35, n°2, p. 202-225.

Forman G.H. & Zahorjan J. (1994), "The Challenges of Mobile Computing", *Computer*, vol. 27, n°4, p. 38-47.

Goel S. & Chengalur-Smith I.N. (2010), "Metrics for Characterizing the Form of Security Policies", *The Journal of Strategic Information Systems*, vol. 19, n°4, p. 281-295.

Gollac M., Greenan N., Hamon-Cholet S. (2000), "L'informatisation de l' « ancienne » économie: nouvelles machines, nouvelles organisations et nouveaux travailleurs", *Économie et Statistique*, vol. 339, n°1, p. 171-201.

Guo K.H., Yuan Y., Archer N.P., Connelly C.E. (2011), "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", *Journal of Management Information Systems*, vol. 28, n°2, p. 203-236.

Haag S., Eckhardt A., Bozoyan C. (2015), "Are Shadow System Users the Better IS Users?–Insights of a Lab Experiment", 36th

International Conference On Information Systems, Fort Worth, Texas, USA.

Harrington S.J. (1996), "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions", *MIS Quarterly*, vol. 20, n°3, p. 257-278.

Healy M. & Iles J. (2002), "The Establishment and Enforcement of Codes", *Journal of Business Ethics*, vol. 39, n°1/2, p. 117-124.

Herath T. & Rao H.R. (2009), "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations", *European Journal of Information Systems*, vol. 18, n°2, p. 106-125.

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*, vol. 32, p. 35-49.

Hsu J.S.C., Shih S.P., Hung Y.W., Lowry P.B. (2015), "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness", *Information Systems Research*, vol. 26, n°2, p. 282-300.

Isaac H., Campoy E., Kalika M. (2007), "Surcharge informationnelle, urgence et TIC. L'effet temporel des technologies de l'information", *Management & Avenir*, vol. 3, p. 149-168.

Johnston A.C. & Warkentin M. (2010), "Fear Appeals and Information Security Behaviors: an Empirical Study", *MIS Quarterly*, vol. 34, n°3, p. 549-566.

Kelliher C. & Anderson, D. (2008), "For better or for worse? An analysis of how flexible working practices influence employees' perceptions of job quality", *The International Journal of Human Resource Management,* vol. 19, n°3, p. 419-431.

Koch H., Zhang S., Giddens L., Milic N., Yan K., Curry P. (2014), "Consumerization and IT Department Conflict", *35th International Conference on Information Systems (ICIS)*, Auckland, New Zealand.

Leclercq-Vandelannoitte A. (2015), "Managing BYOD: how do organizations incorporate user-driven IT innovations?", *Information Technology & People*, vol. 28, n°1, p. 2-33.

Leclercq-Vandelannoitte A. (2017), "Victime ou coupable? Repenser le rôle du contrôlé dans la relation entre contrôle, information et technologies de l'information", *Systèmes d'Information et Management*, vol. 22, n°2, p. 49-80.

Leclercq-Vandelannoitte A. & Bertin, E. (2018), "From sovereign IT governance to liberal IT governmentality? A Foucauldian analogy", *European Journal of Information Systems*, vol. 27, n°3, p. 326-346.

Leclercq-Vandelannoitte A. & Isaac H. (2013), "Technologies de l'information, contrôle et panoptique: Pour une approche deleuzienne", *Systèmes d'Information et Management*, vol. 18, n°2, p. 9-36.

Leclercq-Vandelannoitte A., Isaac H., & Kalika M. (2014), "Mobile information systems and organisational control: beyond the panopticon metaphor?", *European Journal of Information Systems*, vol. 23, n°5, p. 543-557.

Lee S.M., Lee S.G., Yoo S. (2004), "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories", *Information & Management*, vol. 41, n°6, p. 707-718.

Li H., Zhang J., Sarathy R. (2010), "Understanding Compliance with Internet Use Policy From the Perspective of Rational Choice Theory", *Decision Support Systems*, vol. 48, n°4, p. 635-645.

Loch K.D., Conger S., Oz E. (1998), "Ownership, Privacy and Monitoring in the Workplace: a Debate on Technology and Ethics", *Journal of Business Ethics*, vol. 17, n°6, p. 653-663.

Loup P. (2016), "Influence des Technologies Nomades sur le bien-être au travail: une lecture par la théorie de la conservation des ressources", Thèse de Doctorat, Economies et finances, Université Montpellier, France.

Lowry P.B. & Moody G.D. (2015), "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies", *Information Systems Journal*, vol. 25, n°5, p. 433-463.

Luhmann N. (1993), "*The sociology of risk",* Walter der Gruyter, Berlin.

Maddux J.E. & Rogers R.W. (1983), "Protection Motivation and Self-Efficacy: A Revised Theory

of Fear Appeals and Attitude Change", *Journal of Experimental Social Psychology*, vol. 19, n°5, p. 469-479.

Markus M. L. (1994), "Electronic mail as the medium of managerial choice", *Organization Science*, vol. 5, n°4, p. 502-527.

Markus M. L. & Robey D. (1988), "Information technology and organizational change: causal structure in theory and research". *Management science*, vol. 34, n°5, p. 583-598.

Marston S., Li Z., Bandyopadhyay S., Zhang J., Ghalsasi A. (2011), "Cloud Computing—The Business Perspective", *Decision Support Systems*, vol. 51, n°1, p. 176-189.

McDonald P. & Thompson P. (2016), "Social media (tion) and the reshaping of public/private boundaries in employment relations", *International Journal of Management Reviews*, vol. 18, n°1, p. 69-84.

Orlikowski W. J. (1992), "The duality of technology: Rethinking the concept of technology in organizations", *Organization Science*, vol. 3, n°3, p. 398-427.

Ouchi W.G. (1979), "A Conceptual Framework for the Design of Organizational Control Mechanisms", *Management Science*, vol. 25, n°9, p. 833-848.

Pathari V. & Sonar R. (2012), "Identifying Linkages between Statements in Information Security Policy, Procedures and Controls", *Information Management & Computer Security*, vol. 20, n°4, p. 264-280.

Peacock E. & Pelfrey S.H. (1991), "Internal Auditors and the Code of Conduct", *Internal Auditor*, vol. 48, n°1, p. 45-51.

Pierce M.A. & Henry J.W. (2000), "Judgements about Computer Ethics: Do Individual, Co-Worker, and Company Judgements Differ? Do Company Codes Make a Difference", *Journal of Business Ethics*, vol. 28, n°4, p. 307-322.

Post G.V. & Kagan A. (2007), "Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks", *Computers & Security*, vol. 26, n°3, p. 229-237.

Richet J.L. & Rowe F. (2014), "Cornerstone of Terror: the Double-Edged Impact of Fear Appeals in a Transformational Information System Security Project", *35th International Conference on Information Systems,* Auckland, New Zealand.

Robey D., & Boudreau M. C. (1999), "Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications", *Information Systems Research*, vol. 10, n°2, p. 167-185.

Rodhain F. & Agarwal R. (2001), "Le message électronique : une propriété privée ? Perception des salariés quant à la propriété de leurs courriels et au respect de leur vie privée sur le lieu de travail", *Systèmes d'Information et Management*, vol. 6, n°4, p. 49-72.

Rowe F. & Monod E. (2000), "Limites structurelles et culturelles à l'usage de la messagerie dans les banques à réseau", *Réseaux,* vol. 104, n°6, p. 139-158.

Shu Q., Tu Q., Wang K. (2011), "The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective", *International Journal of Human-Computer Interaction*, Vol. 27, n°10, p. 923-939.

Siponen M.T. (2000), "A Conceptual Foundation for Organizational Information Security Awareness", *Information Management & Computer Security*, Vol. 8, n°1, p. 31-41.

Siponen M.T. (2000b), "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice", *Information Management & Computer Security*, Vol. 8, n°5, p. 197-209.

Siponen M. & Vance A. (2010), "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations", *MIS Quarterly*, Vol. 34, n°3, p. 487-502.

Siponen M. & Vance A. (2014), "Guidelines for Improving the Contextual Relevance of Field Surveys: the Case of Information Security Policy Violations", *European Journal of Information Systems*, Vol. 23, n°3, p. 289-305.

Siponen M., Willison R., Baskerville R. (2008), "Power and Practice in Information Systems Security Research", *29th International Conference on Information Systems,* Paris, France.

Southern District of Texas (2014), *Saman Rajaee, Plaintiff, V. Design Tech Homes, Ltd And Design Tech Homes Of Texas, Llc, Defendants*, United States District Court, S. D. Texas, Houston Division, November 11, 2014.

Spears J. L. & Barki, H. (2010), "User participation in information systems security risk management", *MIS quarterly*, vol. 34, n°3, p. 503-522.

Speier C., Valacich J.S., Vessey I. (1999), "The Influence of Task Interruption on Individual Decision Making: An Information Overload Perspective", *Decision Sciences*, vol. 30, n°2, p. 337-360.

Straub D.W. (1990), "Effective IS Security: An Empirical Study", *Information Systems Research*, vol. 1, n°3, p. 255-276.

Straub D.W. & Nance W.D. (1990), "Discovering and Disciplining Computer Abuse in Organizations: a Field Study", *MIS Quarterly*, vol. 14, n°1, p. 45-60.

Teo T.S. & Choo W.Y. (2001), "Assessing the Impact of Using the Internet for Competitive Intelligence", *Information & Management*, vol. 39, n°1, p. 67-83.

Tilson D., Lyytinen K., Sørensen C. (2010), "Research Commentary—Digital Infrastructures: The Missing IS Research Agenda", *Information Systems Research*, vol. 21, n°4, p. 748-759.

Upguard (2018, 1er mai), "*The RNC Files: Inside the Largest US Voter Data Leak*", accessible le 24/04/2020 depuis https://www.upguard.com/breaches/the-rnc-files

Urbaczewski A. & Jessup L.M. (2002), "Does Electronic Monitoring of Employee Internet Usage Work?", *Communications of the ACM*, vol. 45, n°1, p. 80-83.

Walsham G. (1996), "Ethical Theory, Codes of Ethics and IS Practice", *Information Systems Journal*, vol. 6, n°1, p. 69-81.

Walterbusch M., Fietz A., Teuteberg, F. (2017), "Missing cloud security awareness: investigating risk exposure in shadow IT", *Journal of Enterprise Information Management*, vol. 30, n°4, p. 644-665.

Warkentin M., Johnston A.C., Shropshire J. (2011), "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention", *European Journal of Information Systems*, vol. 20, n°3, p. 267-284.

Warkentin M. & Siponen M. (2015), "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric", *MIS Quarterly*, vol. 39, n°1, p. 113-134.

Willison R. & Warkentin M. (2013), "Beyond Deterrence: An Expanded View of Employee Computer Abuse", *MIS Quarterly*, vol. 37, n°1, p. 1-20.

White G.L. (2013), "A New Value for Information Security Policy Education". *Proceedings of the Information Systems Educators Conference*, San Antonio, Texas, USA.

Whitman M.E., Townsend A.M., Aalberts R.J. (1999), "Considerations for an Effective Telecommunication-Use Policy", *Communications of the ACM*, vol. 42, n°6, p. 101-108.

Wood C.C. (2000), "An Unappreciated Reason Why Information Security Policies Fail", *Computer Fraud & Security*, vol. 2000, n°10, p. 13-14.

Young K.S. (2004), "Internet Addiction: A New Clinical Phenomenon and its Consequences", *American Behavioral Scientist*, vol. 48, n°4, p. 402-415.

Young K.S. & Case C.J. (2004), "Internet Abuse in the Workplace: New Trends in Risk Management", *CyberPsychology & Behavior*, vol. 7, n°1, p. 105-111.

Yun H., Kettinger J.W., Lee C.C. (2012), "A New Open Door: The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance", *International Journal of Electronic Commerce*, Vol, 16, n°4, p. 121-152.

Zhang Q., Cheng L., Boutaba R. (2010), "Cloud Computing: State-of-the-Art and Research Challenges", *Journal of Internet Services and Applications*, vol. 1, n°1, p. 7-18.

ANNEXES

Annexe A : Organisations interrogées

ID	Organisation	Particularités notables
BS	Bailleur Social	Administration publique Données sensibles (de santé, fiscales, familiales…)
FI	Fonderie Industrielle	Industrie historiquement peu orientée vers les SI
CA	Centre d'Appel	SI central à l'activité Démarche de « libération d'entreprise »
LM	Entreprise de Levage et de Manutention	Déplacements importants de chargements de valeur, géolocalisation des véhicules, et travail à distance
FC	Fabricant de Câbles	Statut coopératif
IA	Industrie Agroalimentaire	Problématiques liées à la réputation en ligne
CE	Fabricant de Composants Electroniques et d'objets connectés	Sous-traitant de grands donneurs d'ordres SI très hétérogène en raison d'une croissance historique par acquisition

Annexe B : Caractérisation des politiques de gestion des usages par mode de contrôle, réponse aux besoins paradoxaux et adéquation à la culture numérique

Modes de contrôle	(C)omportements ; (R)ésultats ; (S)ocialisation ; Le mode de contrôle dominant, sur lequel les politiques reposent principalement, est indiqué en gras
Centralisation du contrôle	(C)entralisé ; (D)istribué
Stabilité – Flexibilité	(S)tabilité ; (F)lexibilité ; Une mention entre parenthèses indique que la politique peut potentiellement répondre au besoin et qu'aucune incompatibilité n'a été identifiée, mais que l'élément est trop peu présent dans nos données pour que l'apport soit codé.
Culture numérique	(p)articipation ; (b)ricolage ; (r)emédiation ; Une mention entre parenthèses indique que la politique peut potentiellement répondre au besoin et qu'aucune incompatibilité n'a été identifiée, mais que l'élément est trop peu présent dans nos données pour être codé.
Cas	Une croix indique que la politique a été codée pour cette entreprise. Lorsque la colonne est grisée et barrée, l'organisation n'a pas établi de politique. La colonne « Autres chartes » indique qu'une politique a été établie à partir des chartes annexes uniquement.

Gestion des usages d'Internet et des médias sociaux		Modes de contrôle	Centralisation - Distrib.	Stab - Flex	Culture num.	Cas							Autres chartes
						BS	FI	CA	LM	FC	IA	CE	
Filtrage	Aucun	S	D	F	p, b, r	x							
	Moral/légal	S, C	D - C	F - S	p, b, r			x		x	x	x	
	Professionnel	**C**, S	C	S			x		x			x	
Usage à des fins personnelles	Autorisé	**R**, S	D	F	r, b	x							
	Toléré sous condition de productivité	R, C, S	D - C	F - S	r, b			x		x	x	x	
	Interdit	**C**, S	C	S			x		x				
Expression sur les médias sociaux	Libre et encouragée	S	D	F	p, b, r	x		x				x	
	Conseils éditoriaux	S, C	D – C	F - S	p, (b), (r)							x	
	Restriction dynamique (limitée au cas par cas)	**C**, S	C	S – (F)							x		
	Restriction statique (limitée selon fonction)	C	C	S					x				

Gestion des usages du cloud computing		Modes de contrôle	Locus	Stab - Flex	Culture num.	Cas							Autres chartes
						BS	FI	CA	LM	FC	IA	CE	
Stockage en local	Autorisé (avec garantie des données)	**S,** C	D – C	F – S	(b, r)							x	
	Autorisé/toléré sans garantie sur les données	**R**, C, S	D	F	(b, r)	x		x	x	x			
	Interdit	**C**, S	C	S							x		

Annexe B (suite) : Caractérisation des politiques de gestion des usages par mode de contrôle, réponse aux besoins paradoxaux et adéquation à la culture numérique

Gestion des usages de mobilité		Modes de contrôle	Locus	Stab - Flex	Culture num.	Cas							Autres chartes
						BS	FI	CA	LM	FC	IA	CE	
Personnalisation	Personnalisation	**S**, C	D - (C)	F – (S)	p, b, r			x	x				
	Mixte	**C, S**	D – C	F – S	p, b, r					x	x		
	Standardisation	**C**, S	C	S		x	x					x	
Usage à des fins perso.	Autorisation	**S, R**	D	F – (S)	p, b, r			x		x			
	Tolérance	**R, S, C**	D - C	F - S	b, r	x					x	x	
	Interdiction	**C**	C	S			x		x				
Usage pro. des terminaux perso.	Autorisation	**S**	D	F	p, b, r	aucune organisation étudiée							x
	Autorisation restreinte (à certains profils)	**S, C**	D - C	F - S	b, r			x		x		x	
	Interdiction	**C**	C	S		x	x		x		x		
Télétravail à domicile	Institutionnalisation	**S, C,** R	C - D	F – (S)	b, r			x					
	Adaptation aux cas particuliers	**S, C**, R	C - D	S - F	b, r		x		x	x	x	x	
	Interdiction	**C**	C	S		x							

Annexe C : Exemple de caractérisation d'une politique à partir du codage des données (Expression libre et encouragée sur les réseaux sociaux)

Code	Exemples de verbatims
Contrôle par socialisation	*C'est comme la presse nationale. Aujourd'hui si vous répondez à un journaliste « Bailleur Social ne paie pas bien, on va se mettre en grève. » et qu'il publie ça, c'est exactement pareil que sur les réseaux sociaux. C'est un canal de communication comme un autre, ce n'est qu'un outil. Par contre, c'est un outil hyperactif, hyper-puissant… ça va beaucoup plus vite. C'est surtout à ça qu'il faut les acculturer.* (BS) *Il s'agit surtout de leur dire « voilà à quoi ça peut servir, voilà ce que tu peux en tirer de bien, et attention, ça c'est public, plutôt que de mettre des interdictions.* (BS) *On préfère être sur une politique de la confiance et travailler au bien-être de nos collaborateurs pour qu'ils n'aient pas envie de dénigrer l'entreprise.* (CA). *On éduque les collaborateurs, en disant « voilà les risques que tu encours… »* […] *On a souvent des collaborateurs (pas tous les jours, mais pas loin), qui viennent nous demander des conseils sur l'achat de téléphone, le volet sécurité, etc. Parce qu'on est en toute confiance entre nous, c'est plutôt une équipe proche des utilisateurs qu'une équipe répressive. Et on a volontairement internalisé les équipes, on ne les a pas sous-traité (pourtant c'est très facile), parce que comme ça, on est très proches des collaborateurs. Ça coûte sans doute un petit peu plus cher, mais il y a une espèce de connivence on va dire… C'est plutôt des collègues, que l'*équipe informatique. (BS) *On fait avant tout de la pédagogie, et on croise surtout les doigts, parce que l'objectif, ce n'est pas tellement de sanctionner les gens. Ce n'est pas ça l'objectif. L'objectif, c'est surtout de les sensibiliser et leur rappeler (et on le fait régulièrement à travers l'intranet), de leur donner des règles d'usage pour les protéger eux, pour protéger l'entreprise. Parce que ce qui est vrai pour l'entreprise est aussi vrai pour eux, chez eux. C'est vrai avec les ransomwares, les cryptolockers…* (FI) *Vu qu'on n'est pas en mode répressif, ils sont plutôt bienveillants et les collaborateurs demandent plutôt des conseils externes : « voilà, à la maison comment je fais pour que mon fils n'aille pas sur ces trucs-là ?, etc. »* (DSI, BS) **[A propos du mode de contrôle de la publication]** *Aujourd'hui, ce sont les valeurs qu'on prône dans notre mode de management de l'entreprise, donc c'est basé sur la règle de la tolérance.* (CA)
Flexibilité	**[A propos du mode de contrôle de la publication]** *L'expression est totalement libre à partir du moment où l'on respecte ses collègues, ses clients…* (CA) **[A propos des limites de ce qu'il est acceptable d'**évoquer librement, et **de ce qui pourrait requérir une autorisation préalable]** C'est open bar. Il peut citer [notre entreprise] sur le volet technique… C'est comme en interne sur les zones de commentaires, ils savent très bien que le nom de l'entreprise est protégé, que les données de l'entreprise sont protégées… Ils ont le droit de dire « Je suis Machin, je bosse à telle entreprise, voilà mon problème technique. » Moi ça ne me cause aucun problème, bien au contraire, je les incite à le faire. (BS) *On a fait un choix ouvert de dire : « On ne limite pas. »* (CA)

Code	Exemples de verbatims
Décentralisation	*Le management est basé sur la confiance, et donc on part du principe que les utilisateurs sauront faire la part des choses entre la part personnelle et professionnelle des outils. (CA)* *On a des forums (des gens qui animent des petits forums d'une heure) en disant « voilà, aujourd'hui je vais vous parler de ça ». Les gens viennent sur inscription, mais ils peuvent venir librement. Et on a créé un serious game sur Internet.* (BS). *On est plutôt partis sur une politique d'ambassadeurs, qui sont un peu plus geeks (ou pas d'ailleurs), mais qu'on sensibilise d'une façon plus fine à l'usage, et qui sont là aussi pour transmettre les bons usages, les bons tuyaux, etc… On est convaincus que c'est le bon mode de fonctionnement… […] C'est ce mode qui nous semble le plus opportun, plus que de la formation, qui est malheureusement aujourd'hui un peu vite oubliée.* (CA).
Participation	**Pas d'incompatibilité notable, à l'inverse des autres politiques applicables sur cette dimension** Aucun **[problème à la publication]**. *Au contraire, on est plutôt content. On y est favorable et on l'encourage.* (CA) *Je les incite même à le faire. Au contraire, ça prouvera qu'on bosse sur des sujets d'innovation, etc.* (BS) **[A propos de la participation des utilisateurs à l'**établissement des règles] *J'appelle ça un « forum » de l'entreprise, mais vous pouvez l'appeler « blog interne » à l'entreprise, qui permet justement de libérer l'expression orale. Avant il fallait passer par les syndicats pour faire une réclamation au patron, etc, aujourd'hui je connais beaucoup d'entreprise où l'accès au DG est direct.* (BS)
Bricolage	**Pas d'incompatibilité notable, à l'inverse des autres politiques applicables sur cette dimension** *Je pense que l'usage est raisonnable, même si on se rend compte qu'il y a quand même un usage des réseaux sociaux qui est important… Aujourd'hui, c'est plutôt une interrogation au niveau individuel, mais les collaborateurs qui abusent en général n'abusent pas que dans ce sens-là…* (CA)
Remédiation	**Pas d'incompatibilité notable, à l'inverse des autres politiques applicables sur cette dimension** *On est aussi convaincus que c'est dans le sens de l'histoire. On le voit par rapport aux plus jeunes qui nous rejoignent, et qui gardent la page facebook ouverte toute la journée… ça gratouille un peu les plus anciens, qui ne comprennent pas comment ils peuvent être efficaces et travailler… et en même temps, ils sont tout aussi efficaces que leurs collègues… Donc c'est aussi la culture d'entreprise qu'il faut faire évoluer…* […] *Je pense qu'on pourra difficilement lutter contre ça. Les gens sont tous hyper connectés.* (CA)