La lettre innovation et prospective de la CNIL

N°07 / juin 2014

IP INNOVATION & PROSPECTIVE

Retrouvez-nous sur notre site [www.cnil.fr/ip] en flashant le code ou sur :

Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité des données dans l'entreprise numérique

Quelle lecture avoir des évolutions récentes des discussions entre salariés et entreprises ? Aux côtés des sujets classiques (et majeurs en période de crise) tels que les rémunérations, le dialogue social, ou la formation, de nouvelles questions émergent en lien notamment avec la mesure des compétences et des performances. Les responsables des ressources humaines souhaitent mieux comprendre ce qu'ils peuvent faire ou non, par exemple concernant les sources d'informations et de données mobilisables pour connaître candidats ou employés. En un mot, employeurs, employés et autorités de régulation s'interrogent sur le cadre éthique et juridique de la mise en données du monde du travail: comment gérer les besoins de salariés mobiles, aux usages numériques intenses ?

À ces interrogations s'ajoutent des questions concernant l'étendue et la légitimité du contrôle que l'organisation peut exercer sur ses employés pour des raisons de confidentialité ou de performance. Avec le travail collaboratif et nomade, les relations avec l'employeur sont plus diffuses et le contrôle des supérieurs devient moins direct, sans pour autant réduire en intensité. Dans cet environnement, les individus revendiquent de plus en plus une autonomie que les organisations hiérarchiques ont du mal à appréhender. Les modes d'évaluation et les indicateurs de la performance changent et les entreprises tentent de se doter de moyens pour mesurer les nouvelles choses « qui comptent », comme le capital relationnel, le travail cognitif, entrant alors pleinement dans la dimension de l'intime, la personnalité des employés.

La CNIL a souhaité accompagner ses travaux sur la surveillance des salariés d'une réflexion prospective autour de ces mutations des relations de travail. L'objectif de cette lettre IP est de mettre ainsi en perspective des sujets d'actualité tels que le Bring *Your Own Device* (BYOD), car les questions juridiques et éthiques qui se posent dans ce cas concernent à la fois les pratiques des individus au travail et les pratiques de l'organisation vis-à-vis des employés. L'enjeu est de réussir à donner de l'agilité par le biais des nouveaux outils numériques tout en évitant de reproduire dans le monde du travail des situations permanentes de transparence et de traçage qui seraient des décalques malheureux de la situation que les individus vivent comme consommateurs ou internautes. La CNIL reste mobilisée pour placer avec justesse le curseur entre sécurité, performance et respect de la vie privée des travailleurs.

Éric PERES,
Vice-président de la CNIL ■

Recomposition et décomposition de la frontière entre vie personnelle et vie professionnelle : pour le meilleur et pour le pire ?

Le brouillage des frontières entre vie personnelle et vie professionnelle est analysé depuis plusieurs années – notamment depuis que les dispositifs numériques accompagnant les individus au quotidien ont permis de maintenir un lien entre des sphères qui étaient jusque là séparées. Stefana Broadbent, anthropologue et membre du Comité de la Prospective de la CNIL, considère que l'entrée du personnel dans la sphère professionnelle correspond à une « démocratisation de l'intimité », qui vient briser la solitude des individus dans l'entreprise[1]. Les organisations devraient, selon elle, accompagner ce mouvement qui améliore la qualité de vie au travail, plutôt que de chercher à le limiter en restreignant notamment l'accès à certains services de messageries ou de réseaux sociaux. L'éparpillement du temps de travail engendré par l'usage des terminaux mobiles contribue en outre à une intrusion d'une partie de la sphère professionnelle dans la sphère personnelle. La séparation entre données professionnelles et personnelles des individus est donc de moins en moins stricte.

Ces mutations s'accompagnent d'une aspiration des personnes à plus d'autonomie. Éric Pérès, Vice-président de la CNIL et secrétaire général du syndicat FO cadres, considère que le numérique joue un rôle dans l'émergence de nouvelles attentes, les cadres ayant toujours cherché à se distinguer des autres salariés par leur volonté d'être plus autonomes. Pourtant leurs marges de liberté se sont paradoxalement largement amoindries dans le monde très productiviste de l'après-guerre et dans l'entreprise moderne soumise aux nouveaux paradigmes managériaux, en les enfermant dans les processus de rationalisation toujours plus contraignants. Pour lui, « le monde du numérique a fait émerger de nouvelles figures, des personnes qui se sont dotées très rapidement des outils de collaboration et d'échange. Devenues personnes ressources, elles se sont à nouveau émancipées des organigrammes. » Ce phénomène va de pair avec l'essor de la figure de l'entrepreneur, vu comme un travailleur libre et innovant. Certaines organisations s'inspirent d'ailleurs de ce modèle et favorisent l'entreprenariat en interne pour répondre aux mutations de leur environnement et gagner en agilité[2].

Cependant, la tension dans les liens entre travail et numérique vient du fait que le numérique permet à la fois aux individus d'être plus autonomes et flexibles vis-à-vis de leur sphère professionnelle et aux organisations de mieux contrôler leurs employés.

[1] BROADBENT, Stefana. L'intimité au travail : la vie privée et les communications personnelles dans l'entreprise. Paris, FYP éditions, 2011, 192 p.

[2] Le futur du travail dans l'entreprise (1/2) : l'agilité... ou le néant ? , InternetActu, 10/07/2013.

Le BYOD, signal fort de l'imbrication croissante de deux mondes

Les individus à la manœuvre

Les organisations ne sont pas étanches aux évolutions de la société les individus étant eux-mêmes porteurs de changements en interne, ne serait-ce que s'ils adaptent leur environnement à leurs envies d'autonomie. Le BYOD (pour *Bring Your Own Device*, littéralement « apportez vos appareils personnels ») incarne ainsi cette tendance : les propriétaires de smartphones, de tablettes ou même d'ordinateurs portables, apportent et utilisent leurs appareils personnels sur leurs lieux de travail. Des usages clandestins se développent ainsi, autour d'applications ou services mobiles permettant de gagner en confort, en flexibilité et en mobilité. Les fonctionnalités concernées sont souvent basiques : il s'agit de la messagerie, du calendrier, du stockage ou du partage de document dans le cloud. Est-ce à dire qu'il suffit de peu pour améliorer le quotidien des salariés ou bien est-il trop compliqué d'aller *hacker* au-delà ?

L'essor du phénomène est finalement assez simple à expliquer : après l'apparition des premiers smartphones, en 2007, de nombreux usages de facilitation de la vie quotidienne se sont immédiatement imposés. Comme l'a montré en 2011 le sondage *Smartphones et vie privée* réalisé par Médiamétrie pour le compte de la CNIL[3], les utilisateurs adoptent rapidement les usages « avancés » des smartphones : applications, services liés à la géolocalisation, réseaux sociaux... Ainsi, 50 % des possesseurs français de smartphones disent gérer leur agenda grâce à leur smartphone et seuls 44 % des possesseurs disent avoir une utilisation « exclusivement personnelle » de leur smartphone.

Nicolas Colin, entrepreneur et commissaire à la CNIL, pointe la différence de temporalité entre les marchés sur lesquels se fournissent les individus et les processus d'achat au sein des organisations : « c'est sur les marchés de masse que l'innovation va le plus vite. Donc ce sont les individus en tant que particuliers, en tant que consommateurs, qui sont le plus habitués au dernier cri. Dans les organisations, il y a des remparts énormes qui font que l'innovation met beaucoup plus de temps à cheminer : la DSI, la DRH, la direction des achats, et tout ce qui est règlementaire, de l'ordre de la *compliance*. »

[3] « Smartphones et vie privée », novembre 2011

▶▶▶

3 questions à... Jean-François Audenard

Cyber Security Advisor
pour Orange Business Services

Quels sont les usages du BYOD chez Orange ?

Chez Orange, des téléphones mobiles sont mis à disposition des salariés par l'entreprise. Le BYOD vient en complément. Les applications les plus utilisées dans ce cadre concernent la messagerie, le calendrier et la gestion des contacts. Les autres applications conçues à des fins professionnelles ne sont pas accessibles sur les terminaux BYOD. C'est le cas des applications « ressources humaines », qui permettent notamment le dépôt et la validation des congés. Certains services sont interdits, comme ceux de stockage « cloud » de documents, fichiers ou dossiers professionnels. L'accès au réseau internet est aussi filtré sur les téléphones professionnels, de même qu'il l'est sur les postes de travail fixes. Mais ce n'est pas le cas sur un terminal BYOD. De ce point de vue, l'usager a donc plus de liberté côté BYOD.

Comment est pensé le déploiement ?

Une assez grande liberté est laissée aux salariés concernant le choix des mobiles BYOD. La condition principale à remplir est que le mobile choisi puisse supporter le MDM (*Mobile Device Management*) utilisé en interne. Si c'est le cas, le salarié doit référencer son appareil en ligne depuis l'intranet et signer une charte informatique. Une fois ces formalités réalisées, il pourra bénéficier d'un accompagnement et contacter le service informatique en cas de problème.
Pour l'entreprise, le challenge réside dans la capacité à maintenir une politique cohérente de sécurité et d'usage entre les différents terminaux. C'est pour cette raison que les mobiles sont soumis au MDM : l'entreprise peut pousser des paramètres de confidentialité, rendre obligatoire la mise en place d'un code PIN ou effacer à distance le contenu du téléphone en cas de perte ou de vol.
Ces mesures permettent de sécuriser les données de l'entreprise, mais peuvent également avoir une résonance positive sur les usages personnels des employés. La mise en place de règles peut engendrer des habitudes ou des « bonnes pratiques » de sécurisation des équipements personnels par exemple.

Dans quel cadre cela s'inscrit-il ?

Le BYOD n'est qu'une partie d'une stratégie plus large centrée sur la mobilité des employés. Faciliter le travail à distance rend possible les pratiques de télétravail et offre la possibilité de se connecter et de recréer un espace de travail personnel quel que soit le site Orange dans lequel se rend l'employé. La sécurité reste omniprésente dans tous les contextes d'usage.

Accompagner et contrôler le BYOD ?

Les organisations se trouvent tiraillées entre d'un côté la pression des employés, devenus prescripteurs, et de l'autre la résistance des responsables des systèmes d'information liée à un sentiment de perte de contrôle. Le BYOD peut certes être vu comme une manière pour les employés d'utiliser des appareils qu'ils connaissent et aiment utiliser. Mais dans le même temps, la circulation de données de l'organisation au sein d'un terminal non contrôlé peut être source de risque. Et pour traiter les risques, les organisations peuvent être tentées une surveillance intrusive des terminaux.
L'une des solutions mobilisées par les organisations pour gérer le BYOD est ainsi le MDM. Il permet à l'employeur de contrôler à distance les terminaux de ses employés – qu'ils auront préalablement déclarés et enrôlés – afin de sécuriser au mieux les données de l'organisation. L'employeur peut par exemple installer des contenus en fonction du profil de l'employé, mais aussi forcer la mise en place de politiques de sécurité. En cas de perte ou de vol de l'appareil, il peut également effacer les données du téléphone. Dès lors que le téléphone est utilisé aussi bien à des fins personnelles que professionnelles, ce contrôle de l'employeur sur les données du téléphone pose question car il est difficile dans ces conditions, pour l'employé, de garder ses données personnelles à l'abri des regards et des actions de l'employeur.
Une piste alternative émerge cependant du côté des dispositifs de « conteneurisation » des données et d'espace sur le téléphone. Un compartiment hermétique est ainsi aménagé sur les appareils personnels des employés afin de recueillir les applications et les usages professionnels. Dans ce cadre, le contrôle par l'organisation ne s'effectue pas sur le terminal dans son ensemble mais seulement au sein du compartiment dédié aux activités professionnelles. Les données personnelles se situent en dehors de cet espace et les employeurs ne peuvent y exercer une quelconque influence. Plusieurs entreprises se sont spécialisées dans ces technologies, par exemple le groupe français Thales qui propose sa solution Teopad ou l'américain Good Technology. C'est également la spécialité de la startup Divide, dont Google a fait l'acquisition en mai 2014.

Lucie Le Moine,
Chargée d'études prospectives, CNIL ■

Comment assurer l'équilibre entre protection des données des salariés et de l'entreprise dans le BYOD ? Quelques pistes...

Appréhender le BYOD

Une approche pertinente pour mettre en balance les exigences de sécurité de l'entreprise et la protection des données des salariés dans le cadre du BYOD consiste à apprécier au cas par cas l'effectivité des droits des personnes et les risques sur la vie privée des personnes concernées en cas d'atteinte à la disponibilité, à l'intégrité et à la confidentialité de leurs données. Cette logique est par exemple au cœur des travaux du Club EBIOS[4] sur le BYOD, qui se sont traduits par la publication d'éléments de réflexion[5]. Les questions qui se posent sont d'ordre juridique (notamment en termes de droit du travail) et technologiques, les équipements concernés étant moins connus et moins maîtrisés par les organisations. Le BYOD peut être source de risque et de vulnérabilité, car il induit une exposition accrue des équipements. L'enjeu de cette approche est de favoriser un traitement des risques proportionné et adapté au contexte et à la culture de l'organisme et de ses salariés. En réalité, beaucoup de risques existant dans le cadre du BYOD ne sont pas nouveaux, et devaient déjà être appréhendés dans le cadre du télétravail, notamment dans le cas où les salariés souhaitent se transférer des documents de travail par email pour pouvoir travailler depuis leur domicile.
Les solutions pour répondre à ces questions sont diverses et ont des portées très différentes : classification des données, liste de matériels supportés, limitation et contrôle des usages via MDM ou MAM (*Mobile Application Management*), fourniture de services spécifiques, accès par un environnement sécurisé et cloisonné, chiffrement de données stockées, chiffrement de flux, usage d'un VPN, etc.

[4] Le Club EBIOS est une association composée d'experts individuels et d'organismes qui supporte et enrichit le référentiel de gestion des risques français depuis 2003 en particulier par la promotion et le développement de la méthode EBIOS.
[5] Club EBIOS. BYOD : Éléments de réflexion pour gérer les risques

L'occasion de faire autrement

La recherche de solutions techniques ne doit pas conduire à mésestimer l'inventivité des modes de contournement par les usagers (envoi d'un document sur la messagerie personnelle, photographie de l'écran,...). Cette inventivité, si elle est source de risques et de vulnérabilités nouveaux, peut également être source de souplesse et d'innovation dans les pratiques professionnelles. Finalement, que l'on laisse tout faire ou qu'au contraire l'espace de liberté soit très restreint pour l'employé, établir une zone grise à laquelle les employés peuvent connecter leurs équipements mais qui n'est pas directement liés au réseau de l'entreprise est souvent une nécessité.

Les pratiques de BYOD poussent en fait à faire évoluer la sécurité comme elle aurait sans doute dû évoluer depuis longtemps : d'une défense périmétrique sur le modèle des châteaux-forts à une défense centrée sur les données, et éventuellement sur les personnes concernées. Pour les responsables des systèmes d'information et de la sécurité, c'est un changement fondamental : passer d'une gestion des matériels durant tout leur cycle de vie à, peut-être, une fourniture de services informatiques (interfaces, applications spécifiques, etc.). De ce point de vue, la recherche d'un point d'équilibre efficient entre protection des données des employés et protection de l'entreprise dans le cadre du BYOD permettra peut-être de prototyper des solutions répondant aux besoins futurs des systèmes d'information professionnels plus souples, plus ouverts et plus agiles.

Matthieu Grall,
Chef du service de l'expertise technologique, CNIL ■

Vincent Toubiana,
Expert au service de l'expertise technologique, CNIL ■

La mise en données de l'organisation du travail comme nouvelle voie de rationalisation managériale

Le numérique ne s'invite pas dans le monde du travail seulement par le biais des outils que les individus utilisent (ordinateur, smartphone, tablette), il participe également à l'émergence de nouveaux indicateurs de performance.

À nouveaux métiers, nouveaux indicateurs

De nouveaux indicateurs émergent afin d'appréhender les emplois de l'économie de la connaissance. La startup Peak propose par exemple de mesurer automatiquement une multitude d'activités : envois de mails, ajout de contacts, modifications de documents, moment privilégié pour travailler (suivant l'hypothèse de la flexibilité des journées de travail), etc. Regroupées au sein d'une même plateforme, ces données sont censées favoriser une meilleure circulation de l'information. Les données concernant les activités physiques des employés, mesurées à l'aide d'un bracelet ou d'un podomètre connecté, pourraient à l'avenir également y avoir leur place. Le « bien être » des employés est en effet présenté comme une source de productivité par les acteurs du marché des objets connectés.

Analyser les comportements en temps réel

Au-delà du bien-être des employés, la traçabilité des habitudes de travail recèle peut-être d'autres sources de gains de productivité, qu'il faudra concilier avec les exigences de protection des données et de la vie privée. Des entreprises proposent aujourd'hui d'utiliser des capteurs et des logiques de big data pour optimiser l'efficience au travail. Le Wall Street Journal (Rachel Emma Silverman « *Tracking Sensors Invade the Workplace* », *Wall Street Journal*, 7 mars 2013) explique ainsi que l'entreprise *Sociometrics Solutions*, créée par des chercheurs du MIT, veut faire porter à des employés « volontaires » des capteurs qui enregistrent leurs déplacements, mais aussi leurs interactions sociales (notamment les intonations) afin de recommander des réorganisations des espaces de travail ou de pause qui favorisent les échanges ... Ben Waber, PDG de *sociometrics solutions* a lui-même théorisé cette nouvelle approche dans un ouvrage judicieusement appelé « *People Analytics* » (FT press, 2013). En résumé : les employés seront soumis aux techniques de profilage comportemental déjà appliquées sur les consommateurs, mais cette fois il s'agira d'un contexte où le recueil du consentement libre et éclairé d'un individu est bien plus difficile à garantir. Comme le reconnaissait d'ailleurs Ben Waber dans l'article du *Wall Street Journal*, la frontière avec la surveillance des salariés et leur performance individuelle est étroite du fait de la soumission du salarié à sa hiérarchie : selon ses dires ; « une poignée de managers » a déjà cherché à accéder à des données individuelles... ce que le contrat signé entre *Sociometrics solutions* et son client interdit bien sûr...

Après le consommateur, voilà le salarié placé potentiellement sous le microscope d'algorithmes ou de chercheurs chargés d'assurer le bien-être, la productivité et la réussite de tous. Reste à savoir comment les organisations pourront s'approprier cette multiplication des sources de données concernant les activités de leurs employés. Qui doit s'en charger ? Qui possède suffisamment de compétences en analyse de données pour transformer ces dernières en atout pour l'organisation ? Enfin, quelle est la place laissée à l'individu dans la quantification de ses activités au travail et comment les libertés individuelles et la vie privée seront effectivement protégées ?

Lucie Le Moine,
Chargée d'études prospectives, CNIL ■

CNIL.
Commission Nationale de l'Informatique et des Libertés

Commission Nationale de l'Informatique et des Libertés

8, rue Vivienne - CS 30223 - 75083 Paris CEDEX 02
Tél. : 01 53 73 22 22 - **Fax** : 01 53 73 22 00
publications@cnil.fr
Édition trimestrielle
Directeur de la publication : Édouard Geffray
Rédacteur en chef : Gwendal Le Grand
Conception graphique : EFIL Communication 02 47 47 03 20 - www.efil.fr
Impression : Champagnac
Crédit photos : CNIL, Istock
ISSN : 2118-9102
Dépôt légal : à publication