PIERRE LUBET & SANDRINE CULLAFROZ-JOVER

La souplesse du droit face à l'usage croissant du BYOD : étude sur la gouvernance des données au sein de l'entreprise connectée

PIERRE LUBET, avocat associé, Altana

SANDRINE CULLAFROZ-JOVER, avocate, Altana

INTRODUCTION

« *Une circulation aisée des informations mettra un service meilleur, des décisions plus sûres, une adaptation plus rapide aux incitations et exigences du marché, à ce titre, l'informatique est une condition de croissance de l'entreprise, et, là encore l'enjeu est considérable d'autant plus qu'il se place dans un climat de concurrence plus âpre*. »[1]

Emile ROCHE

Une théorie de l'évolution. Par essence, la mise en œuvre de nouvelles technologies de l'information et de la communication au sein de l'entreprise emporte avec elle bon nombre de bouleversements dans l'organisation et la gestion des relations de travail. Ces mutations internes influencent substantiellement les rapports qu'entretiennent les acteurs de l'entreprise entre eux, mais également vis-à-vis de leur environnement : mieux la technologie est acceptée dans la vie quotidienne, plus elle trouvera à s'intégrer facilement dans le cadre du travail.

Les problèmes juridiques soulevés lors des principales étapes de l'informatisation des entreprises reflètent cette évolution de la perception des ressources informatiques par la société :

- **1ère étape - l'introduction des technologies de l'information (IT)** : l'entreprise

[1] E. ROCHE, Préface, in: P. LHERMITTE, « *Le pari informatique* », Paris, Editions France-Empire, 1968.

organise conventionnellement l'introduction de l'IT, tandis que le salarié fait l'apprentissage de l'utilisation des ressources informatiques au sein de l'entreprise ;

- **2ème étape – la démocratisation de l'IT** : les questionnements juridiques s'orientent vers l'encadrement de l'utilisation, par les salariés, des ressources informatiques de l'entreprise à des fins personnelles ;

- **3ème étape – la consumérisation de l'IT** : les questionnements juridiques s'inversent, et l'entreprise s'interroge sur l'utilisation des ressources informatiques personnelles, par les salariés, à des fins professionnelles ;

- **4ème étape – l'optimisation de l'IT dans le cadre de l'exécution du travail** : l'entreprise développe et optimise des outils informatiques collaboratifs, pour créer des interactions et stimuler l'intelligence collective. L'organisation juridique de cette mutation englobe des problèmes contractuels internes et externes : la question de la propriété intellectuelle des travaux réalisés en commun ainsi que celle des rapports entretenus avec les fournisseurs de solutions informatiques utilisées ne doivent pas être négligées ;

- **5ème étape – la mise en données de la gestion des ressources humaines de l'entreprise** : par l'exploitation des technologies de Big Data[2] l'entreprise cherche à définir des indicateurs de performance et à quantifier l'organisation du travail pour améliorer la gestion des ressources humaines. Une réflexion approfondie est alors menée sur la réglementation et la responsabilité liées au traitement de données personnelles servant de base au processus.

De la gouvernance de l'IT à la gouvernance des données. Au cœur de cette évolution, le rôle de la gouvernance des systèmes d'information s'est accru pour sécuriser les ressources informatiques – matérielles et logicielles – organiser le traitement des données au sein de l'entreprise, et mettre en place une stratégie d'administration.

A cet égard, les questions de propriété et de sécurité des données liées à la consumérisation de l'IT en entreprise favorisent un rapprochement interne entre les acteurs pour définir des règles et bonnes pratiques en vue de contribuer à la productivité du capital humain, et à la valorisation de données de qualité, considérés désormais en tant qu'actifs immatériels.

Le traitement juridique du B.Y.O.D.[3] (*Bring Your Own Device*) en entreprise, analysé sous le prisme de la gouvernance, permet ainsi d'envisager, non seulement les réponses juridiques à l'utilisation d'équipements initialement non répertoriés au sein de l'entreprise, mais également de participer à une réflexion plus générale sur la sécurité des systèmes d'information de l'entreprise (ou cyber stratégie) en vue d'améliorer sa compétitivité.

---

[2] Lucie Lemoine, « *La mise en données de l'organisation du travail comme nouvelle voie de rationalisation managériale* », La lettre innovation et prospective de la CNIL, n°07, juin 2014.

[3] Aussi dénommé A.V.E.C. : « *Apportez votre équipement de communication* », Commission générale de terminologie et de néologie, Vocabulaire de l'informatique et des télécommunications, JORF, 24 mars 2013.

Définitions. Dans le cadre de cette étude, la notion de données doit être entendue sous son acceptation la plus large, et comprend l'ensemble des données techniques, commerciales, financières, et stratégiques susceptibles de créer de la valeur et de constituer le patrimoine informationnel de l'entreprise.

Le phénomène de consumérisation de l'IT repose sur l'utilisation d'un matériel informatique mobile permettant le transport, le stockage, l'échange et la consultation de données de toute nature, personnelles et professionnelles.

Pour une qualification juridique exhaustive, on peut distinguer (i) les équipements nomades non communicants (clés USB, disque dur externe), susceptibles d'être branchés sur du matériel d'entreprise, des (ii) équipements nomades communicants, susceptibles de se connecter à un réseau d'entreprise (smartphone, tablette numérique, ordinateur portable).

La popularité du phénomène est telle que plusieurs modèles économiques se sont développés quasi simultanément :

- le B.Y.O.D. : se dit de l'utilisation, dans un cadre professionnel, d'un matériel personnel, propriété du salarié, tel qu'un téléphone multifonction ou un ordinateur, sur lequel transiteront des données de l'entreprise. Le Code du travail dispose que l'employeur doit fournir au salarié le matériel et l'équipement nécessaires à l'exécution de sa mission[4]. Le recours au modèle du B.Y.O.D. ne peut donc reposer, en France, que sur le volontariat ;

- le C.O.P.E. *(Corporated Owned, Personnaly Enabled) :* se dit de la mise à disposition, dans un cadre privé, d'un matériel professionnel, propriété de l'entreprise et sélectionné par elle ;

- le C.Y.O.D. *(Choose Your Own Device)* : se dit de l'utilisation, dans un cadre privé, d'un matériel professionnel choisi par l'utilisateur au sein d'un catalogue d'équipements nomades ayant reçu l'agrément de l'entreprise.

Rapidement, le B.Y.O.A. (*Bring Your Own Applications*) a fait son apparition dans l'entreprise. L'expression désigne l'utilisation, dans un cadre professionnel, d'applications logicielles, généralement disponibles en mode SaaS[5], permettant notamment le stockage, la synchronisation et le partage d'un nombre infini de données (ex: Dropbox, iCloud, SkyDrive). Plus discrète, moins tangible, l'utilisation de ces solutions applicatives est plus difficile à identifier au sein de l'entreprise.

Dans le cadre d'une gouvernance de l'IT, le B.Y.O.A représente cependant un risque sécuritaire très important, dès lors que les données de l'entreprise côtoient potentiellement les données de plusieurs autres sociétés – voire mêmes celles de concurrents – dans un espace de stockage dont elle ne maîtrise pas l'étanchéité. Ainsi,

[4] Article L. 1222-1 du Code du travail.
[5] SaaS : software as a service (exploitation de logiciels via des serveurs distants).

selon des études statistiques récentes, environ 43% des cadres déclarent utiliser des applications personnelles de ce type à des fins professionnelles[6].

L'entreprise du 21ème siècle est connectée : les risques qui en résultent ne sont donc pas que théoriques et peuvent être répertoriés selon leur nature et leurs impacts.

Panorama des risques et enjeux. En premier lieu, les risques techniques peuvent être divisés en quatre sous-catégories : (i) la violation de la confidentialité des données de l'entreprise (pillage informationnel, divulgation accidentelle ou illicite, etc.), (ii) la violation de l'intégrité des données de l'entreprise (altération, modification accidentelle ou illicite, etc.), (iii) la violation de la disponibilité des données de l'entreprise (perte, destruction accidentelle ou illicite, etc.), et (iv) les atteintes aux systèmes d'information de l'entreprise *per se* (infection virale, destruction physique, bombe logique, déni de service, etc.).

En deuxième lieu, les risques juridiques résultent directement des manquements à des obligations légales et réglementaires de conformité, susceptibles d'engager la responsabilité civile et pénale de l'entreprise[7]. L'entreprise encourt également un risque juridique social du fait de la gestion de l'encadrement de l'usage de l'IT et de la relation employeur-salarié.

En troisième et dernier lieu, les risques économiques doivent s'analyser comme la conséquence de la réalisation des risques techniques et juridiques, et comprennent : les pertes financières dues à une mauvaise gouvernance, la réparation des préjudices causés à des tiers, la détérioration de l'image de l'entreprise sur un marché économique considéré et vis-à-vis de sa cible commerciale, la perte de chiffre d'affaires, etc. Ainsi, la consumérisation de l'IT, facilitant la mobilité des salariés et la portabilité des données, présente une menace interne à l'entreprise, qui doit se prémunir des vulnérabilités d'origine humaine et technologique.

Dans ce contexte, quelles sont les règles juridiques applicables à la sécurité des données au sein de l'entreprise connectée ?

Afin d'accompagner durablement les mutations technologiques au sein de l'entreprise, il apparaît nécessaire de nourrir une réflexion globale sur l'encadrement juridique de la sécurité des données dans un écosystème de mobilité (**I**). La connaissance des principaux instruments juridiques nécessaires à la poursuite des atteintes portées par le salarié à la sécurité des données (**II**) permettra, le cas échéant, ultérieurement de défendre le patrimoine informationnel et les intérêts économiques de l'entreprise.

I. ENCADREMENT JURIDIQUE DE LA SECURITE DES DONNEES DE L'ENTREPRISE CONNECTEE

Une gouvernance raisonnée. L'utilisation de ressources informatiques extérieures – initialement non maîtrisées par l'entreprise – pour stocker des données professionnelles représente une source de risques, à la fois pour la sécurité des systèmes d'information,

[6] Etude IFP-GOOD Technology, 2012.
[7] Voir sur ce point les développements de la Section I de la présente étude.

mais aussi dans le cadre de la gestion du capital humain de l'entreprise. Aussi, une gouvernance raisonnée impose à l'entreprise de respecter une conjonction de règles applicables à la portabilité des données professionnelles (**A**), préalablement à la mise en œuvre d'un contrôle patronal de l'utilisation desdites données par les salariés connectés (**B**).

A. Règles de sécurité applicables à la portabilité des données professionnelles

La technique et le droit. En matière de sécurité informatique, la technique et le droit entretiennent une intime complémentarité, qui tend de plus en plus à s'accentuer par l'adoption de normes légales et sectorielles visant à encadrer le traitement de données stratégiques ou sensibles. Comme le soulignait Bernard Teyssié, « *l'innovation technologique ne pèse plus uniquement sur le travail. Elle exerce aussi une pression sur la norme juridique qui l'organise et l'encadre.*[8] »

Les référentiels et recommandations techniques, émanant d'organisations internationales professionnelles[9] ou de services étatiques spécialement dédiés à la cybersécurité[10], aident donc l'entreprise à proposer et mettre en place des solutions pour gérer et sécuriser ses systèmes d'information ainsi qu'à améliorer ses pratiques managériales (**1**) en vue de répondre au renforcement des obligations légales applicables à la portabilité des données professionnelles (**2**).

1. Panorama des solutions techniques adaptées à la portabilité des données professionnelles

L'hygiène informatique à l'épreuve de la portabilité. En janvier 2013, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié un « Guide d'hygiène informatique » définissant les règles et pratiques nécessaires à maintenir la bonne santé des systèmes d'information des entreprises. Parmi les 40 recommandations de ce guide, certaines trouvent une application directe en matière de portabilité des données professionnelles, que ce soit par l'intermédiaire d'équipements nomades communicants ou non communicants.

Ainsi, l'ANSSI préconise l'adoption des mesures suivantes[11] :

---

[8] B. TEYSSIE, « *Préface* », in M. DEMOULAIN, Nouvelles Technologies et droit des relations de travail, Essai sur une évolution des relations de travail, Editions Panthéons-Assas, 2012.

[9] A titre purement informatif, les méthodologies considérées parmi les meilleures pratiques sont : la norme COBIT (*Control Objectives for Information and Related Technology*), la norme ITIL (*Information Technology Infrastructure Library*), les normes ISO 20000 et 27000 relatives à la sécurité informatique ainsi que la norme ISO/IEC 38500-2008 relative à la gouvernance des technologies de l'information.

[10] En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) publie régulièrement de nombreux guides de bonnes pratiques. Le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques (CERTA), qui dépend de l'ANSSI, publie quant à lui des avis et des alertes sur des vulnérabilités informatiques et tient à jour une série de recommandations visant à protéger les systèmes d'information.

[11] ANSSI, *Guide d'hygiène informatique*, 2013. D'autres règles sont également applicables en matière de gestion de la portabilité des données de l'entreprise, telles que : la règle n°1 (établir une cartographie des ressources technologiques), la règle n°15 (interdire techniquement la connexion des supports amovibles sauf si cela est strictement nécessaire et désactiver l'exécution des *autoruns* (exécution automatique de code) depuis de tels supports (Software Restrictions Policy)), la règle n°21 (mettre en place des réseaux

- interdire la connexion d'équipements personnels aux systèmes d'information (ex : désactiver les ports USB, interdire les transferts de messages professionnels) (Règle n°5) ;

- gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle des postes fixes (Règle n°17) ;

- chiffrer les données sensibles, en particulier sur les postes nomades et les supports amovibles (Règle n°19).

Par une approche sécuritaire maximale, la règle n°5 incite ainsi à bannir, purement et simplement, l'usage du B.Y.O.D., et à privilégier une flotte d'équipements nomades entièrement sélectionnés et maîtrisés par l'entreprise[12]. Ironiquement, la règle n°15 permet, malgré tout, d'envisager la connexion des supports amovibles (ex : USB) « *si cela est strictement nécessaire* ».

La popularité du B.Y.O.D. et du B.Y.O.A. impose toutefois à l'entreprise de tenter de concilier ces règles, qui relèvent d'une prudence drastique, avec une approche plus réaliste, pour sécuriser la portabilité des données professionnelles.

Des solutions technologiques. A la recherche d'un équilibre entre sécurité et portabilité des données, l'entreprise est préalablement contrainte de définir un modèle économique correspondant à des besoins réels. Quelque soit le modèle retenu (B.Y.O.D., C.Y.O.D, C.O.P.E), l'entreprise doit donc, à tout le moins, avoir connaissance des usages informatiques de son personnel afin de pouvoir en circonscrire les contours au sein d'une politique de sécurité adaptée et personnalisée.

Des outils logiciels de gestion permettent aujourd'hui de recenser et d'administrer la flotte des équipements nomades de l'entreprise, ainsi que les solutions applicatives utilisées par les salariés (*Mobile Device Management* et *Mobile Application Management*). A ce titre, il peut être recommandé à l'entreprise de fixer en amont des critères objectifs d'éligibilité des équipements – tel que la nature du système d'exploitation – ou de suggérer un paramétrage spécifique des fonctionnalités équipements.

L'entreprise a également la possibilité d'isoler les données professionnelles des contenus privés sur l'équipement du salarié, au sein d'un « silo », qui prend la forme d'une application ou d'un espace dédié, évitant ainsi le stockage anarchique de données professionnelles directement sur les équipements nomades personnels.

Ces méthodes doivent utilement s'articuler avec l'adoption de procédures de réversibilité des données de l'entreprise, notamment en cas de vol ou de perte d'équipement, ou encore dans l'hypothèse d'une rupture du contrat de travail du salarié. En tout état de cause, l'entreprise veillera à sécuriser tous transferts de données en

---

cloisonnés), la règle n°23 (utiliser des applications et des protocoles de transmission sécurisés), la règle n°27 (définir les modalités d'analyse et de contrôle des événements journaliers).

[12] Le C.O.P.E (*Corporated Owned, Personnaly Enabled*) est ici particulièrement visé.

privilégiant des passerelles ou des protocoles sécurisées, tels que VPN / HTTPS, afin d'éviter toute compromission des canaux de communications.

Une responsabilité structurelle. Au cœur de la gestion de la portabilité des données, se trouve, par conséquent, la question du contrôle des accès aux systèmes d'information de l'entreprise[13]. En pratique, celle-ci doit pouvoir justifier de la journalisation des connexions à son réseau et de la gestion des droits numériques des fichiers contenant les données professionnelles. La tenue rigoureuse des historiques participe à la traçabilité des opérations, dans le but de faciliter ultérieurement l'établissement et la conservation d'éléments de preuve des violations de sécurité.

Toutes ces précautions techniques engendrent une responsabilité structurelle qui repose essentiellement sur la direction des systèmes d'information de l'entreprise. Dès lors, l'entreprise doit prévoir en amont une définition claire des responsabilités de chaque intervenant qui participe à la mise en œuvre des mesures de sécurité. La rigueur de la rédaction des éventuelles délégations de pouvoirs au sein de l'entreprise pourront ainsi jouer un rôle essentiel pour définir les responsabilités de chacun dans un schéma plus large de délégation en cascade[14].

2. Renforcement des normes légales applicables à la portabilité des données professionnelles

Une origine sectorielle. La sécurité des systèmes d'information, qui tend à devenir une préoccupation plus juridique que technique, connait son origine et doit une grande part de son développement à des réglementations sectorielles. En matière bancaire et financière[15], par exemple, un corpus important de règles imposent aux entreprises des contrôles internes qui ont contribué à l'émergence d'une véritable gouvernance des systèmes d'information.

La sécurité des traitements de données à caractère personnel. Plus généralement, la loi informatique et libertés n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux Fichiers et aux Libertés (modifiée) impose à tout responsable de traitement de données à caractère personnel de prendre « *toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des*

[13] Voir également la délibération de la CNIL n° 81-094 du 21 juillet 1981, portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques.

[14] A toutes fins utiles, on rappellera que les délégations de pouvoirs permettent un mode de répartition et transfert de pouvoirs et de responsabilités civiles et pénales. Conformément à la jurisprudence de la Chambre criminelle de la Cour de cassation : « *sauf dans les cas où la loi en décide autrement, le chef d'entreprise, qui n'a pas personnellement pris part à la réalisation de l'infraction, peut s'exonérer de sa responsabilité pénale s'il rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la compétence, de l'autorité et des moyens nécessaires* » (Cass. Crim., 11 mars 1993, n° 91-80.598 ; Cass. Crim., 11 mars 1993, n° 92-80.773 ; Cass. Crim., 11 mars 1993, n° 90-84.931 ; Cass. crim., 11 mars 1993, n° 91-83.655).

[15] Doivent être ici mentionnées : la Loi Sarbanes Oxley (SOX) du 30 juillet 2002 pour les entreprises cotées sur le marché américain ; la Loi n° 2003-706 du 1er août 2003 dite loi sur la Sécurité Financière en France ; le Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement (modifié).

tiers non autorisés y aient accès »[16]. Cette obligation de sécurité et de confidentialité est, par ailleurs, pénalement sanctionnée à l'article 226-17 du Code pénal qui condamne par cinq ans d'emprisonnement et 300.000 Euros d'amende, soit 1.500.000 Euros pour une personne morale[17], « *le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée* »[18].

Dans un contexte de portabilité des données, l'entreprise s'expose à voir sa responsabilité pénale engagée dès lors que le salarié peut accéder à des fichiers professionnels de données à caractère personnel (ex : fichiers de gestion des ressources humaines ou de clients et prospects) depuis un environnement informatique non sécurisé ne permettant pas de maîtriser les risques de perte, d'altération, de divulgation, ou de destruction – accidentelle ou illicite. Plusieurs hypothèses sont régulièrement constatées en pratique : accès au réseau de l'entreprise depuis un équipement nomade personnel vulnérable, transfert des fichiers de l'entreprise dans un espace de stockage en ligne ne présentant pas les modalités de protection adéquates (ex : messagerie en ligne, service de stockage et de partage de documents), etc.

La notification des failles de sécurité (*data security breach*) par les fournisseurs de services de communications électroniques. En cas de violation de la sécurité des données à caractère personnel, les opérateurs et fournisseurs de services de communications électroniques ouverts au public sont soumis à des procédures plus formelles et doivent impérativement :

- notifier sans délai :
    - la Commission nationale de l'informatique et des libertés (CNIL) de l'existence d'une violation ;
    - les personnes concernées, lorsqu'il y a un risque d'atteinte à la vie privée ou d'atteinte aux données à caractère personnel [19].
- conserver un registre des failles de sécurité et des mesures prises pour contenir leurs impacts[20].

Le législateur a assorti d'une condamnation pénale tout manquement au dispositif de notification susvisé, aux termes de l'article 226-17-1 du Code pénal[21].

---

[16] Article 34 de la loi « Informatique et Libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004.
[17] Article 131-38 du Code pénal.
[18] Article 226-17 du Code pénal.
[19] Article 34bis de la loi « Informatique et Libertés » du 6 janvier 1978 (modifiée), introduit par l'Ordonnance
n° 2011-1012 du 24 août 2011 relative aux communications électroniques qui a pour objet, dans son titre premier, de transposer les directives 2009/136/CE et 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009.
[20] Idem.
[21] Article 226-17-1 Code pénal : « *Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des*

De plus, il est intéressant de souligner l'ingérence possible du Ministre en charge du secteur des communications électroniques, qui peut désormais imposer des audits de sécurité chez les opérateurs[22].

Extension de l'obligation de notification à l'ensemble des entreprises. Favorable à une généralisation des obligations de sécurité des systèmes d'information, le projet de règlement européen portant réforme de la réglementation applicable à la protection des données personnelles envisage d'étendre l'obligation de notification des failles de sécurité à l'ensemble des secteurs d'activités[23].

B. Contrôle patronal de l'utilisation des données professionnelles par les salariés connectés

Responsabilisation de l'entreprise connectée. La souplesse offerte par le B.Y.O.D. implique une responsabilisation conjointe du salarié et de l'entreprise, qui doit assurer le contrôle de l'accès aux données et la surveillance de l'activité du salarié connecté (**1**). En particulier, l'entreprise devra prendre des mesures adéquates, y compris technologiques, pour contrôler le temps de travail et vérifier le respect des durées minimales de repos (**2**).

1. Contrôle de l'accès aux données et surveillance de l'activité du salarié connecté

La cybersurveillance à l'ère du B.Y.O.D. Aux termes de l'article L. 1121-1 du Code du travail, « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ». Cet article, qui réaffirme le droit à la protection de la vie privée au travail, impose à l'entreprise des limites dans le contrôle de l'accès aux données et la surveillance de l'activité du salarié connecté.

A l'ère du B.Y.O.D., la cybersurveillance est pourtant rendue d'autant plus nécessaire que l'accès aux données de l'entreprise est facilité à tout moment. Le pillage du patrimoine informationnel de l'entreprise est également favorisé par l'utilisation alternative ou conjointe de supports numériques de forte capacité, et d'espaces illimités de stockage et de partage de documents en ligne.

Dans ce contexte, il est essentiel de définir des bonnes pratiques au sein de l'entreprise ainsi que des modalités du contrôle permettant d'assurer effectivement la recevabilité des éléments de preuves d'un mésusage des ressources informatiques, personnelles ou professionnelles, par le salarié.

De la charte de bonne conduite à la charte informatique. L'autorité des instructions formulées par l'entreprise dépendra de la force contraignante qu'elle entendra leur

---

dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

[22] Article 6 de l'Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques susvisée.

[23] Article 31 du projet de Règlement sur la protection des données personnelles.

donner (ex : note de service, charte de bonne conduite, ou charte informatique annexée au Règlement Intérieur), mais également de la réalité de leur contenu, qui peut :

- soit relever automatiquement du champ du Règlement Intérieur, dès lors que ce contenu présente une nature disciplinaire ;

- soit avoir la portée d'une simple déclaration morale peu contraignante.

Si le document est constitué, même pour partie, de dispositions relevant du champ du Règlement Intérieur, il ne peut être introduit qu'après avoir été soumis au Comité d'entreprise (CE) pour avis, et revu par l'inspection du travail qui peut demander des modifications ou le rejeter. D'une manière générale, il est recommandé de soumettre une telle charte au CE pour une bonne diffusion de son contenu auprès des salariés.

A l'exception des sociétés récemment formées, une charte informatique préexiste souvent à l'intégration de la problématique du B.Y.O.D. au sein de l'entreprise. Dans un tel cas, les mises à jour nécessaires à l'encadrement des usages des équipements nomades sont également soumises à la procédure d'information et de consultation des organes de représentatifs du personnel.

L'information et la consultation des organes représentatifs du personnel. Ainsi, la mise en œuvre de nouvelles technologies et de mesures de contrôle de l'activité des salariés doit nécessairement faire l'objet d'une consultation du CE[24] – et le cas échéant du Comité d'hygiène, de sécurité et des conditions de travail (CHSCT)[25] – ainsi que d'une transmission à l'Inspection du travail[26].
Les dispositions d'un Règlement Intérieur portant sur l'utilisation des systèmes d'informations de l'entreprise ne seront pas opposables faute d'accomplissement des procédures préalables[27].

L'information préalable du salarié. De même, le salarié doit être informé des règles et des mesures de contrôle en vigueur au sein de l'entreprise, ainsi que des sanctions auxquelles il peut être exposé[28]. Les finalités du traitement relatif au contrôle de son activité doivent lui être clairement exposées. Il est fortement recommandé de conserver la matérialisation du consentement du salarié aux obligations de la charte informatique.

Les déclarations CNIL ayant pour finalité la gestion des systèmes d'informations et le contrôle de l'activité du salarié. La mise en œuvre de mesures de contrôle de l'activité du salarié, y compris de son accès aux systèmes d'information de l'entreprise, constituent un traitement de données à caractère personnel. Conformément à la loi « Informatique et Libertés », ce type de traitement doit faire l'objet de formalités préalables devant la CNIL. A défaut, l'entreprise n'est pas fondée à s'en prévaloir[29].

---

[24] Articles L. 2323-13 et L. 2323-32 du Code du travail.
[25] Article L. 4612-9 du Code du travail.
[26] Article L. 2323-13 du Code du travail.
[27] Cass. Soc., 9 mai 2012, n °11-13.687.
[28] Article L.1222-4 du Code du travail.
[29] Cass. Soc., 6 avril 2004, n° 01-45.227 : « *à défaut de déclaration à la Commission nationale de l'informatique et des libertés d'un traitement automatisé d'informations nominatives concernant un*

2. Contrôle du temps de travail du salarié connecté

La problématique du temps de travail du salarié connecté. L'utilisation des équipements nomades personnels communicants – de type smartphone ou ordiphone – permet au salarié de travailler à toute heure, en dehors de son lieu de travail. Dans un tel contexte, l'entreprise peut facilement perdre le contrôle et la maîtrise du temps de travail de son personnel.

Les risques liés au non respect des durées maximales de travail. La durée légale du travail effectif est légalement fixée à 35 heures par semaine civile pour l'ensemble des entreprises[30]. Ainsi, sauf dérogations[31], les durées de travail effectif ne doivent pas dépasser 10 heures par jour, 48 heures par semaine ou 44 heures en moyenne sur une période de 12 semaines consécutives. De plus, le salarié bénéficie d'un repos quotidien minimum de 11 heures par jour[32].

En cas de non-respect de ces durées maximales de travail, l'entreprise encourt une sanction pénale[33] et s'expose à un contentieux prudhommal. En effet, le salarié pourrait notamment formuler des demandes individuelles de rappels d'heures supplémentaires fondés sur des courriels envoyés ou des travaux réalisés en dehors du temps réservé au travail, voire même, prendre acte de la rupture de son contrat de travail au tort de l'employeur.

Les risques liés aux heures supplémentaires étendus à certains cadres au forfait-jour. Les risques liés aux heures supplémentaires concernent tous les salariés soumis aux 35 heures, équipés d'un équipement nomade communiquant, mais également certains cadres au forfait-jour. A ce titre, la Cour de cassation a récemment jugé que pour être valables, les forfaits-jours doivent faire l'objet d'un accord collectif contenant des dispositions de nature à garantir le respect des durées maximales de travail et les repos journaliers et hebdomadaires[34]. Cette interprétation jurisprudentielle stricte peut conduire à la reconnaissance de la nullité des forfaits-jours de l'entreprise et à sa condamnation au paiement de nombreuses heures supplémentaires[35].

---

salarié, son refus de déférer à une exigence de son employeur impliquant la mise en œuvre d'un tel traitement ne peut lui être reproché ».

[30] Article L. 3121-10 du Code du travail.

[31] Les dérogations à la durée du travail sont accordées (i) par l'inspecteur du travail pour les demandes de dérogation relatives à la durée maximale journalière et (ii) par le directeur régional des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (Direccte) ou, par délégation, le responsable de l'unité territoriale, ou par subdélégation, l'inspecteur du travail, pour les demandes de dérogation relatives à la durée maximale hebdomadaire. L'autorité administrative compétente est celle dont relève l'établissement qui emploie les salariés concernés par la dérogation (Instruction DGT n° 2010/06 du 29 juillet 2010).

[32] Article L. 3131-1 du Code du travail.

[33] Article R. 3135-1 et suivants du Code du travail : les pénalités relatives à la durée du travail sont de nature contraventionnelle (4ème et 5ème classe).

[34] Cass. Soc., 29 juin 2011, n° 09-71.107.

[35] Il convient de relever que certains secteurs d'activité se révèlent plus à risques que d'autres : Industries chimiques, Communications Electroniques. A contrario, des secteurs d'activité sont aujourd'hui couverts par un accord collectif valide en matière de forfaits-jours : Métallurgie, Syntec (depuis 2014).

Par conséquent, il est recommandé de consulter la convention collective et les accords d'entreprise applicables, afin de vérifier la présence de dispositions relatives aux forfaits-jours. A défaut de telles dispositions, la mise en place d'un accord collectif d'entreprise semble incontournable.

Les risques psycho-sociaux liés à l'hyperconnectivité du salarié. La consumérisation de l'IT est à l'origine de profonds bouleversements dans les conditions d'exécution du contrat de travail et fait peser une nouvelle responsabilité sur l'entreprise.

Notamment, l'usage du B.Y.O.D. et le déferlement des données professionnelles à toute heure confrontent le salarié à la réception massive d'informations et l'incite à être toujours plus disponible et plus réactif. Dans ces conditions, les temps de repos et de travail sont fongibles, constituant une source potentielle de déséquilibre[36], parfois qualifiée de « *stress électronique* »[37] en considération de la suractivité du salarié connecté.

L'entreprise doit alors veiller à encadrer l'utilisation des équipements personnels, afin de prendre les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale de son personnel[38]. Dans un avis du 14 mai 2013 sur les risques psychosociaux au travail, le Conseil Economique, Social et Environnemental a d'ailleurs expressément cité les TIC (Technologies de l'information et de la communication) comme « *cause interne à l'entreprise* ». A cet égard, la formation des responsables de services et chefs d'équipes aux problématiques liées à l'utilisation des équipements nomades et aux risques pesant sur l'entreprise est également cruciale.

Certaines entreprises ont déjà pris des mesures techniques pour limiter les connexions de leurs salariés à leur réseau en dehors des heures ouvrables. En interrompant ainsi la transmission des flux de données professionnelles sur les équipements nomades personnels de leurs salariés, ces entreprises ont instauré au sein de leur charte informatique un véritable « *droit à la déconnexion* »[39].

Plus récemment, un avenant de révision à l'accord national SYNTEC, étendu par arrêté le 26 juin 2014[40], a consacré une « *obligation de déconnexion des outils de communication à distance* ». Afin que le salarié respecte les durées minimales de repos, il est prévu que « *l'employeur veillera à mettre en place un outil de suivi pour assurer le respect des temps de repos quotidien et hebdomadaires du salarié* ». Il relève alors de la responsabilité de l'entreprise de s'assurer que le salarié peut techniquement se

---

[36] Le 2 juillet 2008, un accord interprofessionnel, étendu depuis 2009 (ANI du 2 juillet 2008 étendu par arrêté 23 avril 2009 (JO 6 mai 2009), définit le stress comme une situation de « *déséquilibre entre la perception qu'une personne a des contraintes que lui impose son environnement et la perception qu'elle a de ses propres ressources pour y faire face* » (art. 3, alinéa 1).

[37] Aurélia Dejean de La Bâtie, « *Gare au stress électronique !* », Les Cahiers Lamy du CE, 2009.

[38] Article L. 4121-14 Code du travail.

[39] Sophie Fantoni-Quinton, Céline Leborgne-Ingelaere, L'impact des TIC sur la santé au travail, La Semaine Juridique Social n° 48, 26 Novembre 2013, 1452 ; Jean-Emmanuel Ray, *Droit du Travail Droit Vivant*, Wolters Klumer, 23ème éd. 2014-2015, n°214.

[40] Avenant de révision de l'article 4 du Chapitre 2 de l'Accord National du 22 juin 1999 sur la durée du travail de la branche des bureaux d'études techniques, cabinets d'ingénieurs, conseils, sociétés de conseils (IDCC 1486), étendu par arrêté du 26 juin 2014 (JORF du 4 juillet 2014).

déconnecter des outils de communication mis à sa disposition et de surveiller que cette déconnexion est effective en pratique.

II. POURSUITE DES ATTEINTES A LA SECURITE DES DONNEES DE L'ENTREPRISE CONNECTEE

Une stratégie de défense protéiforme. Malgré la mise en place de mesures de protection adéquates, l'entreprise peut demeurer vulnérable aux atteintes internes (méprise, maladresse ou malveillance d'un salarié) et/ou externes (malveillance d'un tiers). Un arsenal juridique de protection varié permet alors à l'entreprise d'assurer la défense de ses intérêts en justice, dans un contexte de portabilité des données. Les mesures conservatoires et probatoires (A), précédant toutes actions à l'encontre du salarié fautif (B), permettent de réunir des moyens de preuve utiles. Parallèlement, des voies de recours répressives permettent à l'entreprise de poursuivre pénalement les atteintes à son patrimoine informationnel.

A. Mesures conservatoires et probatoires

Pour être en mesure de fonder ultérieurement ses prétentions et afin de garantir le respect de la protection de la vie privée du salarié (**1**), dans le cadre particulier de l'accès aux données professionnelles stockées sur des équipements nomades (**2**), l'entreprise peut faire établir des constats en matière informatique (**3**).

1. Le respect de la protection de la vie privée du salarié

L'admissibilité de la preuve en droit du travail. L'irrecevabilité de la preuve déloyale en droit du travail résulte de l'application de l'article 9 du Code de procédure civile, de l'article L. 1121-1 du Code du travail protégeant la liberté individuelle au travail, et de l'article 9 du Code civil, dernier rempart de protection de la vie privée de droit commun. Ainsi, les moyens de preuve obtenus à l'encontre d'un salarié fautif doivent répondre à un examen de proportionnalité et de finalité pour être admissibles devant des juridictions prudhommales, ce qui exclut la mise en œuvre de tout procédé clandestin. Cette exigence a donné lieu à une jurisprudence foisonnante sur le caractère privé des contenus stockés sur l'outil informatique mis à la disposition du salarié par l'entreprise. Compte tenu de la supériorité des intérêts protégés[41], les moyens de preuves illicitement obtenus pourront, en revanche, être librement invoqués dans le cadre d'une procédure pénale.

Les développements jurisprudentiels sur le caractère privé des contenus du salarié. Traditionnellement, la jurisprudence s'est attachée à limiter le pouvoir inquisiteur de l'entreprise dans la recherche de moyens de preuves en définissant les contours du caractère privé de la correspondance électronique et des fichiers informatiques du salarié.

[41] Article 427 du Code de procédure pénale ; voir également la thèse de Matthieu Démoulain, « *Nouvelles technologies et droit des relations de travail – Essai sur une évolution des relations de travail* », Editions Panthéon-Assas, 2012, n°680 et suivants.

Dans le désormais célèbre arrêt Nikon, la Cour de cassation pose le principe selon lequel « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances ; l'employeur ne peut dès lors prendre connaissance des messages émis par le salarié ou reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnel de l'ordinateur* »[42].

Depuis lors, la Cour de cassation a régulièrement pu affirmer le principe selon lequel les contenus des salariés, créés à partir de l'outil de travail mis à disposition par l'employeur, sont présumés professionnels, et peuvent être consultés par l'employeur, hors la présence du salarié et sans restrictions particulières[43]. Cette prérogative procède du pouvoir de direction de l'employeur qui est en droit de contrôler l'activité de ses salariés pendant leur temps de travail.

Il en résulte donc une obligation à la charge du salarié d'identifier expressément et d'intituler sans ambigüités comme « *personnel* » les contenus qui relèvent de sa vie privée. En revanche, un fichier informatique intitulé *« mes documents »* ne lui confère pas un caractère personnel[44]. La mention de son nom ou de ses initiales par le salarié ne suffit pas à renverser la présomption[45].

L'accès aux contenus privés du salarié à partir de l'outil informatique de l'entreprise. La Cour de cassation maintient une jurisprudence constante et uniformisée, que ce soit en matière d'accès aux messages électroniques personnels ou en matière d'accès aux fichiers informatiques personnels : l'entreprise ne peut accéder aux contenus privés du salarié qu'en présence de celui-ci ou après l'avoir dûment appelé, sauf lorsqu'un risque ou un évènement particulier le justifie[46].

2. L'accès aux données professionnelles stockées sur des équipements nomades

Portée de la problématique. La question de l'accès aux données professionnelles stockées sur des équipements nomades se pose essentiellement pour le matériel dont le salarié est propriétaire (B.Y.O.D.). En effet, « *l'employeur ne peut porter atteinte à la propriété d'autrui, que ce soit en termes de contrôle du contenu, mais aussi lors du départ du salarié* »[47]. Toutefois, dans l'hypothèse d'une mise à disposition d'équipements nomades par l'entreprise (par exemple, dans le cas du C.O.P.E.), la difficulté d'assurer la protection des données professionnelles conserve tout son sens dès lors que le matériel considéré est en possession du salarié qui en détient la maîtrise effective jusqu'à sa restitution.

---

[42] Cass. Soc., 2 octobre 2001, n° 99-42.942.
[43] Cass. Soc., 18 octobre 2006, n°04-48.025 ; Cass. Soc., 19 juin 2013, n° 12-12.138 ; Cass. Soc., 26 juin 2012, n° 11-15.310; Cass. Soc., 8 décembre 2009, n° 08-44.840.
[44] Cass. Soc., 10 mai 2012, n° 11-13.884.
[45] Cass. Soc., 21 octobre 2009, n° 07-43.877.
[46] Pour les fichiers informatiques personnelles : Cass. Soc., 17 mai 2005, n° 03-40017 ; pour les messages électroniques personnels : Cass. Soc., 10 juin 2008, n° 06-19.229 ; Cass. Soc., 23 mai 2007, n° 06-43.209.
[47] Jean-Emmanuel Ray, « *A propos de la révolution numérique* » (seconde partie), Revue de droit social, n°11-12, nov.-déc. 2012, p.1029.

Dès lors, comment l'entreprise peut-elle accéder aux données professionnelles stockées sur de tels équipements ? **La position de la jurisprudence** est exprimé dans deux arrêts récents, rendus à l'occasion de contentieux impliquant l'usage par un salarié de son matériel personnel sur le lieu de travail, permettent d'envisager des éléments de réponse.

Dans un premier arrêt du 23 mai 2012[48], qui concernait l'accès par l'employeur au dictaphone personnel d'un salarié, la Cour de cassation a précisé que *« l'employeur ne pouvait procéder à l'écoute des enregistrements réalisés par la salariée sur son dictaphone personnel en son absence ou sans qu'elle ait été dûment appelée ».* Ainsi, l'entreprise ne peut accéder aux éléments contenus dans un équipement personnel qu'en présence du salarié ou celui-ci dûment appelé. Il est intéressant de souligner l'absence de mention de la possibilité d'accéder à l'équipement en cas de « *risques ou événement particulier* ». Cette mention, habituellement reprise par la jurisprudence pour justifier d'un risque d'atteinte aux systèmes d'information de l'entreprise, n'aurait effectivement que de rares causes de légitimité alors que l'équipement considéré n'est ni connecté au réseau, ni partie intégrante des ressources informatiques de l'entreprise.

Dans un second arrêt du 12 février 2013[49], qui concernait une clé USB personnelle connectée à l'ordinateur professionnel du salarié, la Cour de cassation a estimé que *« la clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, étant présumée utilisée à des fins professionnelles, l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient hors la présence du salarié ».* Dans l'hypothèse où l'équipement considéré est connecté au réseau ou relié aux systèmes d'information de l'entreprise, l'entreprise peut donc, même hors la présence du salarié, accéder aux contenus stockés non expressément identifiés comme « *personnel* ». Par un mécanisme d'association, le rattachement de l'équipement aux ressources informatiques de l'entreprise lui confère ainsi une finalité professionnelle.

Par extrapolation, il ne pourrait être exclu que la jurisprudence reconnaisse à terme, pour l'administrateur réseaux de l'entreprise, le pouvoir d'accéder aux contenus privés en cas de « *risques ou événement particulier* », dès lors qu'il peut justifier que le rattachement de l'équipement considéré aux ressources informatiques de l'entreprise fait courir un risque de sécurité aux systèmes d'information de l'entreprise.

3. Les constats en matière informatiques

Le constat d'huissier. De sa propre initiative, l'entreprise peut recourir à un huissier pour « *effectuer des constations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter* »[50]. Ainsi, le procès-verbal permettra d'établir la matérialité de faits objectifs, à l'exclusion de toute appréciation.

Le procès verbal de constat constitue un élément de preuve valablement admissible devant les juridictions. Les mentions intrinsèques du constat propres aux actes

[48] Cass. Soc., 23 mai 2012, n° 10-23.521.
[49] Cass. Soc., 12 février 2013, n° 11-28.649.
[50] Article 1er de l'ordonnance n°45-2592 du 2 novembre 1945 relative au statut des huissiers.

d'huissiers de justice font foi jusqu'à inscription de faux, tandis que les autres mentions relatives aux pures constations font foi jusqu'à preuve du contraire depuis la loi dite « Béteille »[51] du 22 décembre 2010[52].

En matière informatique, le procès-verbal de constat doit également contenir un ensemble de pré-requis techniques permettant de vérifier le mode opératoire utilisé[53] par l'huissier. Toute impression des copies d'écran descriptives dudit mode opératoire doit être personnellement réalisée par l'huissier. Le cas échéant, le procès-verbal pourra se voir dénier toute force probante par les juridictions[54].

Le recours à l'article 145 du Code de procédure civile. L'entreprise a également la possibilité, pour contourner la protection accrue des contenus privés du salarié, de solliciter – par voie de requête ou de référé – une mesure d'instruction *in futurum* sur le fondement de l'article 145 du Code de procédure civile[55]. Le texte présente principalement l'avantage de permettre à l'entreprise de procéder par voie de requête, c'est-à-dire suivant une procédure non contradictoire, pour autant que les circonstances de l'espèce le justifie.

Dans un arrêt Datacep du 23 mai 2007, la Chambre sociale de la Cour de cassation a jugé que le respect dû à la vie personnelle du salarié ne faisait pas obstacle à l'application de l'article 145 du Code de procédure civile.

L'application de l'article 145 du Code de procédure civile[56] suppose néanmoins la réunion des 3 critères de recevabilité suivants :

- que le requérant initial détermine spécifiquement la **nature des mesures d'investigations** sollicitées ;

- que le requérant initial vise le **texte légal ou réglementaire** permettant de fonder les mesures sollicitées ;

- que le requérant initial précise le **caractère nécessaire et proportionnel** des mesures sollicitées.

---

[51] Loi n° 2010-1609 du 22 décembre 2010 relative à l'exécution des décisions de justice, aux conditions d'exercice de certaines professions réglementées et aux experts judiciaires.

[52] Sur ce point, voir Joël Mazure, « *Constat d'huissier de justice : quelle force probante ?* », Revue de l'Habitat, Avril 2012.

[53] La norme AFNOR NF Z67-147 relative au « *mode opératoire de procès-verbal de constat sur Internet effectué par huissier de justice* » définit le mode opératoire que devrait suivre l'huissier afin de garantir que son constat soit le plus fiable possible. Cette norme n'a cependant pas un caractère obligatoire et ne saurait être invoquée seule pour contester la validité d'un procès-verbal (CA Paris, Pôle 5, Ch. 1, 27 février 2013).

[54] TGI Paris, 16 octobre 2009, Keepschool / KP média accessible sur LEGALIS à l'adresse url suivante : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2850.

[55] Cass. Soc., 23 mai 2007, n° 05-17.818 ; dans le même sens : Cass. Soc., 10 juin 2008, n° 06-19.229.

[56] Article 145 du Code de procédure civile : « *S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ».

Sous réserves de caractériser un motif légitime, une stratégie processuelle peut, de ce fait, être mise en place pour permettre à l'entreprise d'appréhender le contenu de l'équipement personnel d'un salarié (de type B.Y.O.D.), sans s'exposer au risque de destruction d'éléments de preuves compromettants par ce dernier.

Toutefois, le caractère non contradictoire de cette procédure n'exclut pas la présence du salarié au moment de l'exécution de l'ordonnance obtenue. Dans un telle hypothèse, la Cour de cassation a déjà jugé que « *l'employeur avait des raisons légitimes et sérieuses de craindre que l'ordinateur mis à la disposition de la salariée avait été utilisé pour favoriser des actes de concurrence déloyale, a pu confier à un huissier de justice la mission de prendre copie, en présence de la salariée ou celle-ci dûment appelée et aux conditions définies par le jugement confirmé, des messages échangés avec des personnes identifiées comme étant susceptibles d'être concernées par les faits de concurrence soupçonnés* »[57].

B. Actions à l'encontre du salarié fautif

Types d'actions envisagées. L'atteinte portée à la sécurité et à la confidentialité des données de l'entreprise peut naturellement trouver son origine dans la maladresse ou la malveillance d'un salarié, mais également par la malveillance d'un tiers, qui aura malicieusement exploité les failles de sécurité des systèmes d'information de l'entreprise, y compris les vulnérabilités liées à l'intégration des B.Y.O.D. Cependant, dans le cadre de cette étude des rapports internes à l'entreprise sur l'usage des B.Y.O.D, seules les actions à l'encontre du salarié fautif feront l'objet d'une analyse. Ainsi, en cas de malveillance dans l'accès aux données de l'entreprise, l'entreprise pourra sanctionner le salarié (**1**), et/ou exercer une action devant les juridictions pénales (**2**).

1. Sanction à l'encontre du salarié fautif

Le licenciement pour faute grave. Le salarié fautif qui aura volontairement ou par une négligence impardonnable porté atteinte aux données de l'entreprise pourra être licencié pour faute grave. Le licenciement pour faute nécessite l'application de la procédure disciplinaire.

Selon la jurisprudence, la « *faute grave* » est caractérisée lorsque le salarié commet une faute d'une importance telle qu'elle peut seule justifier une mise à pied conservatoire, et rend impossible son maintien dans l'entreprise[58], y compris pendant la durée du préavis[59]. Par conséquent, le salarié ne bénéficie plus de son droit à l'indemnité de licenciement ni à l'indemnité de préavis[60] mais conserve son droit aux congés payés (par opposition au salarié licencié pour faute lourde).

---

[57] Cass. Soc., 10 juin 2008, n° 06-19.229.
[58] « *La faute grave résulte d'un fait ou d'un ensemble de faits imputables au salarié qui constitue une violation des obligations résultant du contrat de travail ou des relations de travail d'une importance telle qu'elle rend impossible le maintien du salarié dans l'entreprise pendant la durée du préavis* » (Cass. Soc., 26 févr. 1991, n° 88-44.908).
[59] Cass. Soc., 27 septembre 2007, n° 06-43.867.
[60] Articles L. 1234-1 et L. 1234-9 du Code du travail.

L'entreprise est obligée de suivre une procédure stricte pour que le licenciement opéré soit régulier. A ce titre, la mesure de mise à pied conservatoire[61] est, en principe, prononcée dans le cadre d'une procédure de licenciement pour faute grave[62] : le salarié de l'entreprise concernée ne peut plus se rendre sur son lieu de travail, le contrat de travail étant suspendu dans le but de préserver la sécurité des systèmes d'information de l'entreprise.

Applications jurisprudentielles. Les juridictions ont d'ores et déjà estimé que constituait une faute grave toute entrave aux limitations et gestion des droits d'accès établies par l'entreprise. Par exemple, le fait d'emprunter un mot de passe pour se connecter au poste informatique d'un tiers[63] ou de divulguer des codes à des salariés non habilités ou à des tiers constitue une faute grave[64].

De même, en matière d'utilisation de périphériques, la Cour d'appel de Riom a jugé que le licenciement du salarié, à qui il était reproché d'avoir consulté des données de nature confidentielle et de les avoir transférés sur une clé USB, reposait sur une faute grave[65].

Par conséquent, peut être caractérisée de faute grave et faire l'objet d'un licenciement, toute atteinte au patrimoine informationnel de l'entreprise, résultant de l'utilisation d'un équipement personnel nomade, ou résultant de l'accès aux systèmes d'information de l'entreprise en violation de l'habilitation expressément donnée par l'administrateur des systèmes de l'entreprise.

2. Action répressive à l'encontre du salarié fautif

La pluralité des fondements. La divulgation intentionnelle d'éléments confidentiels du patrimoine informationnel de l'entreprise peut être sanctionnée sur la base de plusieurs fondements[66]. Il n'est pas question ici d'en dresser un catalogue exhaustif, mais de mettre l'accent sur des infractions particulièrement propices à la poursuite des atteintes à la sécurité des données de l'entreprise connectée.

Les notions de « *vol de données* » et d' « *abus de confiance* ». Le vol est traditionnellement caractérisé par « *la soustraction frauduleuse de la chose d'autrui* »[67]et est puni de trois ans d'emprisonnement et de 45 000 euros d'amende[68]. Le « *vol d'informations* » ou « *vol de données informatiques* » a longtemps été ignoré du Code pénal et ne constituait pas en tant que telle une infraction. Au contraire, l'élément matériel de la qualification traditionnel du vol renvoyait expressément à la soustraction d'« *une chose* » corporelle et tangible.

---

[61] Article L. 1332-3 du Code du travail.
[62] Cass. Soc., 6 nov. 2001, n° 99-43.012.
[63] Cass. Soc., 21 décembre 2006, n° 05-41.165.
[64] Cass. Soc., 5 juillet 2011, n° 10-14.685.
[65] CA Riom, chambre civile 4, 12 Février 2013, n° 11-01.747.
[66] Par exemple : Violation du secret professionnel (article 226-13 du Code pénal) ; Violation du secret de fabrique (article 621-1 du Code de la propriété intellectuelle) ; Violation des secrets de fabrication (article L. 1227-1 du Code du travail) et bientôt Violation du secret des affaires (Projet de loi portant sur la protection du secret des affaires n°2139, Assemblée nationale, 16 juillet 2014).
[67] Article 311-1 du Code pénal.
[68] Article 311-3 du Code pénal.

Néanmoins, les juridictions ont pu juger que l'information pouvait faire l'objet d'un vol[69], pour autant que celle-ci soit reproduite sur un support, dont la soustraction serait l'objet du délit[70]. Ainsi, bien que classiquement perçue par les juristes comme le parent pauvre de la répression des infractions via les nouvelles technologies, la qualification de « vol » semblait pouvoir retrouver une nouvelle source d'interprétation sur le terrain du B.Y.O.D. En effet, la copie de données confidentielles sur un équipement périphérique personnel devait permettre de caractériser le support nécessaire à l'application du texte pénal.

En modifiant la rédaction de l'article L. 323-3 du Code Pénal, la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a mis fin à ce débat pour consacrer la qualification de vol de données immatérielles.

Le nouveau texte, entré en vigueur depuis le 15 novembre, permet désormais de poursuivre l'extraction, la détention, la reproduction, ou la transmission frauduleuse de données contenues dans un système de traitement automatisé (et non plus uniquement l'introduction, la modification et la suppression frauduleuse de telles données).

Cette nouvelle rédaction permettra sans aucun doute une répression plus efficace et plus coercitive[71].

La qualification d' « *abus de confiance* »[72] sanctionne quant à elle « *le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé* ». L'abus de confiance est puni de trois ans d'emprisonnement et de 375.000 euros d'amende. La référence à la notion peu précise de « *bien quelconque* » permet, en effet, de couvrir a priori l'ensemble des données informatiques pouvant représenter une valeur économique pour l'entreprise. Ainsi, la Cour de cassation a jugé que « *les informations relatives à la clientèle constituent un bien susceptible d'être détourné par un salarié et caractériser un abus de confiance* »[73].

En tout état de cause, il faut considérer ces infractions comme complémentaires, dans le cadre du traitement juridique des B.Y.O.D. : dans un jugement du 26 septembre 2011, le Tribunal correctionnel de Clermont-Ferrand a condamné, pour vol et abus de confiance, une salariée ayant transféré des fichiers confidentiels sur une clé USB, le jour de son départ de l'entreprise, afin de les utiliser à des fins personnelles[74].

---

[69] Cass. Crim., 4 mars 2008, n° 07-84.002 et plus récemment Cour d'appel de Paris Pôle 4, chambre 10 Arrêt du 5 février 2014

[70] Relevons qu'ici la soustraction de l'information, duplicable par nature, n'emportera pas nécessairement dépossession de son propriétaire initial.

[71] L'infraction visée à l'article L. 323-3 du Code Pénal est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

[72] Article 314-1 du Code pénal.

[73] Cass. Crim., 16 novembre 2011, n° 10-87.866.

[74] TGI Clermont-Ferrand, Ch. Corr., 26 septembre 2011, voir commentaire de É. A. CAPRIOLI, « *Condamnation pour vol et abus de confiance d'une ex-salariée ayant transféré des fichiers sur une clé USB* », Communication Commerce électronique n° 3, Mars 2012, comm. 36.

La notion d' « atteinte à un système de traitement automatisé de données ». Une liste d'infractions sanctionne les atteintes à un système de traitement automatisé de données (STAD) aux articles 323-1 et suivants du Code pénal, parmi lesquelles :

- l'intrusion frauduleuse et le maintien dans un STAD ;
- l'entrave au fonctionnement d'un STAD ;
- l'introduction, la modification, ou la suppression frauduleuse de données dans un STAD.

Comme indiqué précédemment, la loi appréhende désormais également l'extraction, la détention, la reproduction, ou la transmission frauduleuse de données[75].

Les condamnations applicables aux infractions susvisées ont été successivement renforcées par les lois n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, et n° 2012-410 du 27 mars 2012, relative à la protection de l'identité. Les peines oscillent ainsi entre 2 à 7 ans d'emprisonnement et entre 30.000 euros et 100.000 euros d'amende.

Dans le cadre de la gestion du B.Y.O.D, le risque résulte principalement de l'intrusion frauduleuse au sein des systèmes d'information de l'entreprise comme préalable à l'extraction frauduleuse de données. A ce titre, la jurisprudence a déjà jugé que « *l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un STAD, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication* »[76].

La notion d'«atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques». Les articles 226-16 à 226-24 du Code pénal visent l'ensemble des infractions relatives à la violation des obligations prescrites par la loi Informatiques et Libertés n° 78-17 du 6 janvier 1978. La plupart d'entre elles sont sanctionnées de 5 ans d'emprisonnement et de 300.000 euros d'amende pour les personnes physiques.

L'utilisation d'équipements personnels par le salarié accroît d'une part, le risque de divulgation des données à caractère personnel à des tiers non autorisés (article 226-22 du Code pénal), et, d'autre part, le risque de manquement à l'obligation de sécuriser un traitement informatique comportant des données personnelles (article 226-17 du Code pénal).

En tout état de cause, la recherche de la responsabilité pénale de l'auteur du délit, de quelque nature que ce soit, n'exclut pas la présentation de demandes d'indemnisation en dommages et intérêts pour réparer le préjudice subi par l'entreprise.

---

[75] Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

[76] CA Paris, 5 avril 1994 ; CA Paris, 14 janvier 1997.

CONCLUSION

Les risques encourus par le phénomène du B.Y.O.D. rappellent aux entreprises la nécessité d'organiser efficacement – en interne – la bonne gouvernance de leurs systèmes d'information, et en particulier des données traitées dans le cadre de leurs activités.

Des outils juridiques de protection, permettant d'encadrer l'accès et l'utilisation, par les salariés, du patrimoine informationnel de l'entreprise, doivent impérativement être mis en place en complément des mesures techniques. En cas de réalisation du risque, la sanction et la répression des comportements malveillants devra être organisée de façon stratégique au regard (i) de la nature des faits reprochés et (ii) du préjudice subi. La connaissance des aspects juridiques de la cybersécurité permettra à l'entreprise de sécuriser ses données stratégiques, de valoriser son capital, et d'accroître sa compétitivité.