REVUE
DROIT & SOCIETE
مجلة
القانون و المجتمع
دورية علمية محكمة تعنى با لدراسات و الأبحاث في المجال القانوني و الاجتماعي و الاقتصادي.
PERIODIQUE SCIENTIFIQUE A COMITE DE LECTURE, CONSACRE A LA PUBLICATION D'ETUDES
ET DE RECHERCHES DANS LES DOMAINES JURIDIQUE, ECONOMIQUE ET SOCIAL

DOI : 10.5281/zenodo.10615755 – Vol.4, N° 12- 1ère trimistre 2023

LE SALARIE, L'ORDINATEUR ET LA FAUTE : ETUDE A LA LUMIERE DE LA JURISPRUDENCE SOCIALE

THE EMPLOYEE, THE COMPUTER, AND THE MISCONDUCT: A STUDY IN THE LIGHT OF SOCIAL JURISPRUDENCE

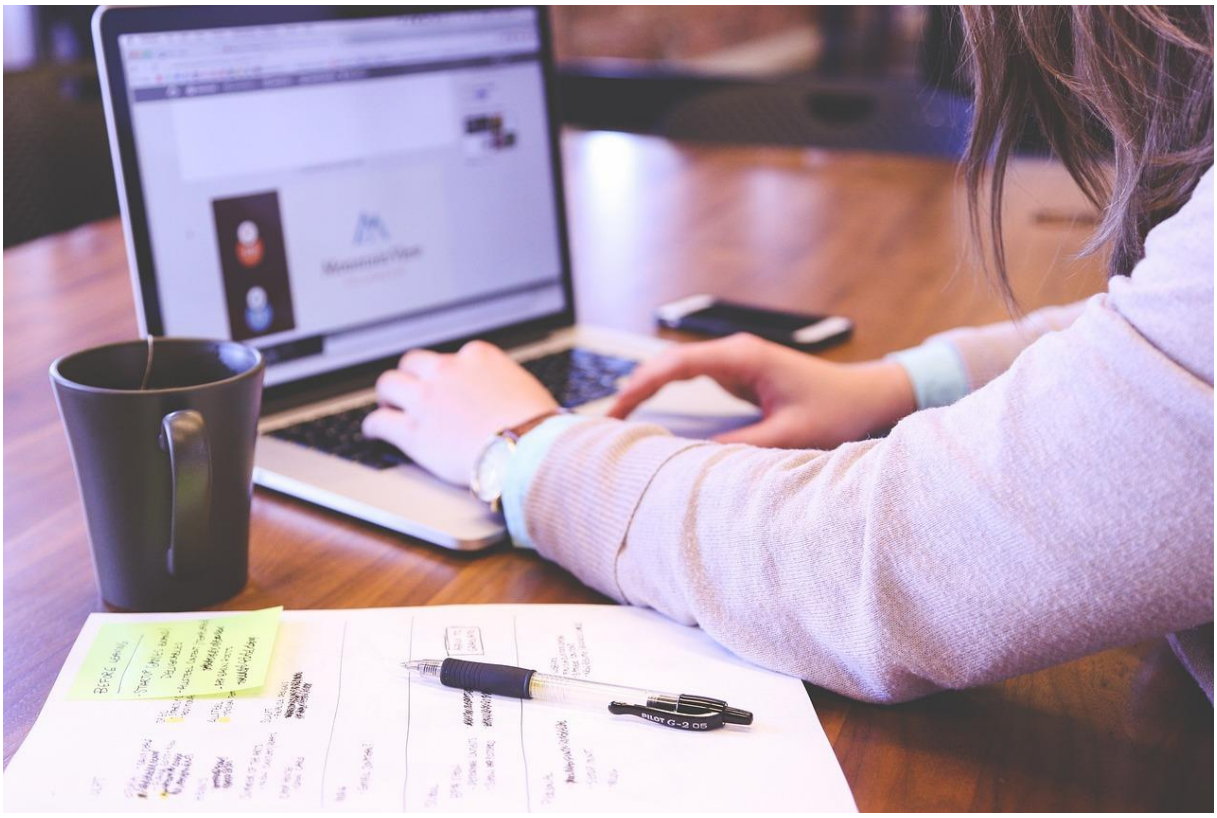
Issam EL KOUITI

Doctorant en sciences juridiques

Université Mohamed V, Rabat, Maroc

Citation:
EL KOUITI, I. (2024). LE SALARIE, L'ORDINATEUR ET LA FAUTE : ETUDE A LA LUMIERE DE LA JURISPRUDENCE SOCIALE. REVUE DROIT ET SOCIETE, 4(12), 7-28. https://doi.org/10.5281/zenodo.10615755

LE SALARIE, L'ORDINATEUR ET LA FAUTE : ETUDE A LA LUMIERE DE LA JURISPRUDENCE SOCIALE



REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

RESUME

La montée en puissance de la digitalisation a considérablement transformé la manière dont les entreprises opèrent, avec une adoption répondue des outils et des solutions informatiques pour faciliter la gestion des données, la communication, et l'efficacité organisationnelle.

Cependant, cette transition a également introduit des défis en matière de sécurité, d'éthique et de discipline, liés notamment au comportement des salariés avec les outils informatiques. Le lien étroit entre le salarié et l'ordinateur peut entraîner des fautes, légères ou graves, pouvant aller de l'utilisation personnelle non autorisée à la diffusion d'informations confidentielles. Les fautes peuvent entraîner des sanctions, allant de l'avertissement au licenciement.

Cette étude vise à explorer les divers aspects des fautes des salariés liées à l'utilisation des outils informatiques, mettant en lumière les implications légales et disciplinaires à la lumière de la jurisprudence. Pour adapter la législation marocaine du travail aux évolutions liées à la digitalisation et à l'utilisation de l'outil et du matériel informatique.

Mots clés : Droit du travail - Droit disciplinaire – Salarié – Ordinateur – Faute – Sanction.

THE EMPLOYEE, THE COMPUTER, AND THE MISCONDUCT

A STUDY IN THE LIGHT OF SOCIAL JURISPRUDENCE

Issam EL KOUITI

PhD student in law

Mohamed V University, Rabat, Morocco

ABSTRACT

The advent of the digitalization has fundamentally reshaped the operational landscape of enterprises, marked by the widespread use of computers, data tools, and technologies to facilitate data management, communication, and organizational efficiency.

However, this transition has also introduced challenges in terms of security, ethics and discipline, notably linked to employees' behavior with IT tools. The close link between the employee and the computer can lead to both minor and serious misconduct, ranging from unauthorized personal use to the dissemination of confidential information. Misconduct can result in sanctions ranging from a warning to dismissal.

This study aims to explore the various aspects of employee misconduct associated with the use of computers and data tools, highlighting the legal and disciplinary implications in the light of case law. To adapt Moroccan labor legislation to developments related to digitization and the use of computer tools and equipment.

Key words: Labor Law - Disciplinary Law - Employee - Computer - Misconduct – Sanction.

INTRODUCTION

L'avènement de l'ère numérique a apporté des changements significatifs à la manière dont les entreprises opèrent et interagissent avec leur environnement. L'utilisation généralisée des outils informatiques dans le milieu professionnel a grandement facilité le traitement des données, la communication et l'efficacité globale des organisations. Cependant, cette transition vers le numérique a également donné naissance à de nouveaux défis et risques en matière de sécurité et d'éthique, mais aussi en matière de la discipline en particulier, en ce qui concerne le comportement des salariés au sein de leur entreprise à travers l'utilisation des outils informatiques mis à leur disposition.

Le salarié et l'ordinateur sont devenus inséparables, l'ordinateur est pour une majorité des salariés plus au moins qualifiés, un outil indispensable au quotidien pour l'exécution de la plupart des tâches professionnelles. Il permet au salarié de stocker des informations, de traiter des données, de communiquer, et de réaliser de nombreuses autres activités.

Cette relation intime entre le salarié et l'ordinateur comporte des risques, En effet,

l'utilisation de l'ordinateur peut donner lieu à la commission de fautes, légères ou graves.

Les fautes légères sont des manquements mineurs aux obligations du salarié, Elles peuvent être commise par inadvertance ou par négligence. Elles peuvent par exemple consister en l'utilisation de l'ordinateur à des fins personnelles entrainant à l'entreprise une perte de temps de travail et impactant la productivité. Elles peuvent aussi consister en la détérioration ou perte involontaire de données informatiques par omission.

Les fautes graves sont de leur côté des manquements graves aux obligations du salarié, Elles peuvent entraîner la rupture du contrat de travail. Elles consistent par exemple en la diffusion d'informations confidentielles sans autorisation de l'entreprise, l'utilisation de l'ordinateur à des fins frauduleuses, la commission d'actes de harcèlement ou de diffamation, via la messagerie ou bien même dans des espaces publics comme les réseaux sociaux pendant le temps du travail et à partir de l'ordinateur de l'entreprise.

Le salarié est responsable des fautes qu'il commet en utilisant l'ordinateur. Il peut être sanctionné par son employeur, qui peut lui infliger une des sanctions prévues par le Code du travail, telle que l'avertissement, le blâme, la mise à pied ou le licenciement.

L'objectif de cette étude est d'explorer en profondeur les diverses facettes de la faute du salarié susceptible d'être commise par le biais de l'utilisation des outils informatiques de l'entreprise avec en tête l'ordinateur mis à sa disposition pour l'exécution exclusive des taches qu'on lui a confié. Nous examinerons de près comment cette utilisation peut impacter la protection des données de l'entreprise, la sécurité informatique et l'utilisation adéquate des ressources informatiques. Ces aspects cruciaux nécessitent une analyse approfondie afin de comprendre pleinement les implications légales et les conséquences disciplinaires de l'utilisation des ordinateurs au sein de l'environnement professionnel.

En explorant les différentes dimensions de la faute du salarié dans le contexte de l'utilisation des outils informatiques de l'entreprise, cette étude aspire à contribuer à une meilleure compréhension des enjeux juridiques et éthiques associés à cette problématique, de l'utilisation des technologies de l'information en général, et l'ordinateur comme matériel, à la connexion internet comme service accessoire, tout en passant par l'utilisation de la messagerie électronique, de périphériques informatiques, et des divers logiciels à installer sur le système d'un ordinateur.

Cela impliquera l'analyse des précédents arrêts de la jurisprudence pertinente, en se basant sur les critères définis dans le cadre de l'étude. En résultat, une synthèse des enseignements tirés de cette analyse sera réalisée pour parvenir à des conclusions éclairées.

Pour dévoiler les enjeux cruciaux de la digitalisation du travail, nous explorerons successivement les domaines sensibles de la protection des données (I), les dangers relatifs à la sécurité informatique (II) et la prévention des abus dans l'utilisation au quotidien des ressources informatiques de l'entreprise (III).

I. La protection des données de l'entreprise

Les manquements du salarié mettant en péril la sécurité des données au sein de l'entreprise peuvent se traduire par le non-respect des réglementations sur la protection des données (A), l'accès ou stockage non autorisé de données confidentielles (B), la manipulation

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

inadéquate des données de l'entreprise (C), ainsi que le partage de données sensibles avec des tiers sans consentement adéquat (D).

A. Non-respect de la législation sur la protection des données

La pratique professionnelle connait un recours massif au traitement des données à caractère personnel. Cette catégorie juridique qui apparait dans les années 80[1], concerne toute information, de quelque nature qu'elle soit, se rattachant à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Le traitement de telles données, doit avoir strictement une finalité loyale, légale et légitime au regard de l'activité professionnelle du salarié, surtout lorsque les données sont informatisées, un seul fichier électronique peut contenir de milliers d'informations, et peut être facilement exploitable pour des fins préjudiciables ou nuisibles à l'intéressé, d'où l'importance de la législation marocaine en la matière qui remonte à 2009.

La loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel est venue pour assurer une protection efficace des particuliers contre toute éventuelle utilisation abusive des données visées par la loi, susceptible de porter atteinte à la vie privée des citoyens en tant que droit fondamental qui passe devant l'intérêt des entreprises, et ce bien que ces données personnelles soient une source importante pour les entreprises afin d'améliorer leur activité commerciale.

Pour se conformer avec les dispositions de la nouvelle loi. Plusieurs entreprises se sont lancé dans la formation de leurs salariés afin de se soumettre aux nouvelles obligations légales et éviter d'être exposées en cas de contravention à des sanctions pénales sévères en plus de l'engagement de la responsabilité civile à l'égard des personnes ayant subi des dommages du fait de la violation de cette obligation légale de protection des données détenues par l'entreprise.

La protection des données fut la préoccupation du législateur depuis si bien longtemps, l'on cite bien plus que la loi relative à la protection des données à caractère personnel et le rôle de la Commission Nationale de contrôle de la protection des Données à caractère Personnel[2], le code de commerce sur les instruments de paiement électronique, la loi 53.05 relative à l'échange électronique de données juridiques, les dispositions de droit pénal relative au système de traitement automatisé de données[3].

[1] Gambardella, S. (2017). La protection des données "sensibles" à l'ère du numérique : Regard sur le droit de l'Union européenne. TALEB-KARLSSON (A.) et BEAUREGARD-BERTHIER (O.) (Dirs), *Protection des données personnelles et sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?*, Bruylant, p.64

[2] La CNDP, a transmis des dossiers à la justice, dont un est fait suite à la réception de plusieurs plaintes contre un site de commerce électronique marocain. La CNDP a mené des investigations, dont notamment un contrôle du site web mis en cause et un contrôle sur place. Les résultats de l'enquête ont révélé des infractions aux dispositions légales en vigueur et ont donné lieu à des soupçons de traitement frauduleux de données personnelles. A la fin, la Commission a décidé de transmettre le dossier au procureur du Roi près le tribunal de première instance. [Voir : « La CNDP transmet pour la première fois des dossiers à la justice », Information publiée au site officiel de la CNDP : cndp-maroc.org]

[3] L'article 607-3 du Code pénal, inséré en vertu de la loi n° 07-03, dispose : « Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un

Toutes ces lois visent essentiellement la protection des données contre toute divulgation, et imposent plutôt « une obligation de moyens appréciable objectivement »[4], afin d'assurer la sécurité des données, et prévenir le salarié à ne pas enfreindre la loi, et respecter aussi son obligation de confidentialité qui lui interdit tout accès ou conservation d'informations sans autorisation préalable.

B. Accès ou conservation non autorisés de données confidentielles

Sur le plan juridique, il convient d'examiner attentivement les implications de l'accès ou de la conservation non autorisés de données confidentielles de l'entreprise par un employé. Cela peut être considéré comme une infraction disciplinaire en vertu du droit du travail. L'accès non autorisé à des informations sensibles peut violer les politiques de l'entreprise et constituer une violation des obligations contractuelles. Les lois sur la confidentialité et la protection des données peuvent également entrer en jeu, imposant des sanctions sévères pour de telles violations.

Les conséquences de l'accès non autorisé ou de la conservation de données confidentielles peuvent être sévères du point de vue disciplinaire. Un employé qui enfreint ces règles peut faire l'objet d'une sanction disciplinaire pouvant aller du simple avertissement à la suspension temporaire, voire au licenciement. Les employeurs ont la responsabilité de protéger les intérêts et les informations privées de leurs entreprises, et ils sont en droit de prendre des mesures disciplinaires lorsque ces règles sont violées, pour garantir la sécurité des données et maintenir l'intégrité de l'entreprise.

Dans un cadre plus large, la légitimité des motifs de licenciement pour accès non autorisé ou conservation de données confidentielles est cruciale. Les tribunaux et les instances juridiques examinent attentivement chaque cas pour s'assurer que le licenciement est justifié. Ils évaluent si l'employeur a énoncé des politiques claires en matière de confidentialité et si les employés étaient bien informés de ces politiques. De plus, ils examinent si l'accès ou la conservation non autorisés étaient intentionnels et s'ils constituaient une violation sérieuse des règles de l'entreprise. Cette démarche garantit une application équitable du droit tout en protégeant les intérêts de toutes les parties impliquées.

La sanction disciplinaire peut être prononcée pour diverses raisons ; En premier lieu, cet acte représente une transgression des obligations de confidentialité et de loyauté envers l'employeur. Le salarié est tenu par un devoir de loyauté envers son employeur, ce qui implique le respect strict de la confidentialité des données et des informations sensibles de l'entreprise. Tout accès ou stockage non autorisé pouvant potentiellement mener à la divulgation de ces renseignements est contraire à cette obligation et peut être perçu comme une violation sérieuse de ce devoir essentiel.

En plus, l'accès ou la conservation non autorisée peut entraîner des risques financiers, légaux et de réputation pour l'entreprise. Ces données peuvent être cruciales pour la compétitivité de l'entreprise et leur conservation non

mois à trois mois d'emprisonnement et de 2.000 à 10.000 dirhams ou de l'une de ces deux peines seulement.

Est passible de la même peine toute personne qui se maintient dans tout ou partie d'un système de traitement automatisé de données auquel elle a accédé par erreur et alors qu'elle n'en a pas le droit ».

[4] Vicente, A. I. (2003). *La convergence de la sécurité informationnelle et la protection des données à caractère personnel : Vers une nouvelle approche juridique*, Thèse de doctorat, Université de Montréal, p. 15

autorisée pourra aboutir à une divulgation ce qui peut causer un préjudice important.

En fin si le salarié doit exécuter son contrat de travail avec bonne foi, l'accès ou conservation est équivalente à une soustraction de données considérées confidentielles pour le salarié hors personnel concerné par la tache en question, la divulgation même interne est fautive.

Si la bonne foi se définit comme « une règle de conduite qui exige des sujets de droit une loyauté et une honnêteté exclusive de toute intention malveillante »[5], cette exigence est « désormais placée en tête des dispositions relatives au contrat »[6], notamment dans les contrats de travail.

Dans ce contexte, un arrêt de la cour de Cassation a cassé la décision d'appel qui a refusé la validation du licenciement d'un salarié ayant effectué « un accès non autorisé à des données et informations confidentielles relatives à l'entreprise et à ses salariés en utilisant un logiciel d'espionnage »[7], même en présence d'un rapport technique prouvant l'acte. Explorons à présent un autre aspect qui est la mauvaise manipulation des données de l'entreprise, qui peut être considéré comme une des fautes liées à l'utilisation de l'ordinateur.

C. Mauvaise manipulation des données de l'entreprise

Les salariés ont un devoir implicite de protéger et de manipuler les données de l'entreprise avec soin et intégrité. Le fait pour le salarié de modifier ou supprimer des données du système informatique de l'entreprise, constitue une violation d'une obligation accessoire de son contrat de travail. La destruction volontaire de données informatiques est un comportement fautif susceptible de rompre totalement la confiance dans l'intégrité du salarié, car il appartient à celui-ci dans le cadre de ses obligations contractuelles de rendre possible l'accès à l'ordinateur professionnel et aux fichiers sauvegardés dans ses disques conformément aux consignes de l'employeur.

Un salarié peut faire l'objet de reproches en cas de manipulation inadéquate des données de l'entreprise, englobant une mauvaise gestion des sauvegardes, des modifications non autorisées ou même la destruction inappropriée de ces fichiers enregistrés exclusivement sur son ordinateur, ou par le billet de son compte

[5] Jourdain, P. (1992). La bonne foi. Rapport in *Travaux de l'association H. Capitant*, Litec, p. 121

[6] **Bertier-Lestrade, B. (2019). La bonne foi dans la réforme française des contrats. *Le contrat dans tous ses états*, Cécile Le Gallou (dir), Presses de l'Université Toulouse Capitole, p. 141**

[7] Arrêt n° 588 du 30-06-2020, Dos. Soc. 2362/5/1/2018 : D'après les juges de Cassation : Il est légalement établi que la charge de la preuve de l'existence d'un motif valable de licenciement incombe à l'employeur. La société soutient que les fautes graves commises par le salarié, justifiant son licenciement, principalement constituées par des accès illégaux à des données et informations confidentielles concernant l'entreprise et ses employés, ont été établies de manière irréfutable par le rapport d'expertise technique émis par un cabinet d'experts spécialisés en sécurité informatique et versé au dossier. Cependant, la juridiction en appel, lorsqu'elle a estimé qu'elle avait effectué une enquête approfondie, a relevé que le représentant de l'employeur n'a pas produit d'arguments étayant les violations énoncées dans le rapport de licenciement, ni fait comparaître de témoin renforçant sa position. De plus, les motifs avancés par l'employeur pour justifier le licenciement du salarié n'ont pas été jugés sérieux, sans faire référence au rapport d'expertise ou à sa discussion, et sans justifier l'exclusion de ce dernier ou ordonner toute autre mesure d'enquête, en considérant que les fautes soulevées étaient de nature technique et requéraient l'expertise d'un spécialiste, ce qui a conduit à l'ignorance de l'argument présenté par l'employeur, rendant sa décision insuffisamment motivée, équivalente à son absence.

utilisateur ou depuis son ordinateur professionnel pour les données logées dans un serveur. Ces actions peuvent être considérées comme des atteintes sérieuses à l'intégrité des données de l'entreprise. En conséquence, le salarié s'expose à des sanctions disciplinaires, pouvant aller jusqu'au licenciement pour faute grave.

La responsabilité d'un salarié envers les données de l'entreprise est primordiale. La mauvaise manipulation de ces données peut entraîner des conséquences néfastes, compromettant l'exactitude et l'accessibilité des informations cruciales pour l'activité de l'entreprise. La mauvaise gestion des sauvegardes, des modifications non autorisées ou de la destruction des fichiers peut non seulement mettre en péril la continuité de l'activité de l'entreprise, mais également ébranler la confiance de l'entreprise envers ses salariés.

Ainsi, il est essentiel que les salariés comprennent la gravité de leurs responsabilités concernant la manipulation des données de l'entreprise. Un usage inapproprié peut avoir un impact considérable sur le fonctionnement de l'entreprise et sur sa réputation. Les sanctions disciplinaires, comme le licenciement pour faute grave, visent à dissuader de telles actions et à garantir que les salariés prennent au sérieux leur devoir de protéger et de gérer correctement les données sensibles de l'entreprise.

Cette sanction disciplinaire est généralement prise en réponse à une exécution défaillante du contrat de travail, dans lequel est constatée une violation et un non-respect des directives énoncées dans la charte informatique annexée souvent au règlement intérieur de l'entreprise, ou encore sur un manquement avéré envers l'obligation de loyauté à laquelle le salarié est soumis à l'égard de son employeur.

La sanction peut aussi trouver son fondement dans le comportement fautif incarné dans les dispositions de l'article 22 du Code de travail qui prévoit que « Le salarié doit veiller à la conservation des choses et des moyens qui lui ont été remis pour l'accomplissement du travail dont il a été chargé ; il doit les restituer à la fin de son travail ». Cela signifie que la conservation et la restitution concerne aussi les données informatisées de l'entreprise ainsi que le matériel informatique mis à la disposition du salarié pour l'accomplissement de son travail.

Le licenciement peut être justifié car toute altération non autorisée des données peut perturber l'activité de l'entreprise, induire en erreur les parties prenantes et entraîner des pertes financières substantielles. En même temps l'image et la réputation de l'entreprise peuvent être gravement entachées si des données informatiques de l'entreprise sont compromises, ce qui peut affecter la confiance des clients et des partenaires commerciaux. De ce fait, les salariés ont la responsabilité de manipuler les données avec prudence et intégrité pour éviter des conséquences potentiellement désastreuses pour l'entreprise. De même, la préservation de toutes les données sensibles requiert une autorisation préalable de l'employeur avant tout partage avec un tiers.

D. Partage de données sensibles avec des tiers sans consentement approprié

Il est impératif de maintenir la confidentialité des informations de l'entreprise face à tout risque de divulgation par les salariés. Cette protection peut découler « d'une obligation de loyauté, d'une clause de non-

concurrence, d'une obligation au secret ou d'une obligation de confidentialité »[8].

La divulgation d'un secret professionnel constitue une infraction, l'article 447 du code pénal prévoit une amende allant de 120 à 10 000 DH et une peine d'emprisonnement allant jusqu'à cinq ans à l'encontre de toute personne qui divulgue des secrets de la fabrique ou des secrets de gestion de l'entreprise qui l'emploie.

Le secret professionnel en droit du travail concerne toutes les informations qui sont tenues confidentielles par l'entreprise et qui ne doivent pas être divulguées à des tiers, sauf autorisation expresse de l'employeur. Les informations protégées peuvent inclure les secrets commerciaux, les données confidentielles relatives aux clients, les stratégies de l'entreprise, les informations sur les salariés et les salaires, ainsi que d'autres données sensibles, qu'elles soient partagées par messagerie électroniques ou applications de communication collaborative et services de conférence à distance qui englobent la vidéoconférence, les réunions en ligne, le chat…

Dans un arrêt de la Cour de cassation, le fait pour un salarié de divulguer les informations concernant son employeur à l'un des clients au moyen de la messagerie électronique Google est considéré comme une faute grave, de sorte que la décision des juges d'appel fut bien fondée quant à la validation du licenciement[9].

De même, lorsqu'un salarié a contractuellement souscrit à l'obligation de garantir la protection des données des clients de l'entreprise, l'utilisation de son propre compte de messagerie électronique au détriment de celui fourni par son employeur représente une violation manifeste de cette obligation de confidentialité.

L'obligation de confidentialité est fondamentale dans la relation employeur-salarié. Lorsqu'un salarié néglige délibérément cette obligation en recourant à son compte de messagerie personnel pour envoyer des informations des clients de l'entreprise à un destinataire externe, cela va à l'encontre des clauses contractuelles établies qui concernent l'obligation de confidentialité. De plus, cette action enfreint toutes les réglementations en vigueur qui visent à garantir la sécurité et la confidentialité des données des clients qui sont en possession de l'entreprise.

L'utilisation du compte de messagerie électronique de l'entreprise est généralement régie par des politiques internes clairement définies, allant jusqu'à l'interdiction de l'utilisation formelle de l'usage d'autre messagerie, notamment personnelle. Ces politiques visent à assurer le respect des obligations de confidentialité et de sécurité. En négligeant d'utiliser le compte fourni par l'employeur et en optant pour son compte personnel, le salarié contrevient aux normes établies, ce qui pourrait avoir des répercussions sérieuses, notamment en termes de discipline au sein de l'entreprise et même sur le plan pénal, en fonction de la gravité de la violation.

En somme, la plupart des litiges, liés à la divulgation par un salarié d'informations de l'entreprise stockées sur son ordinateur professionnel, font mention que les employeur sont inévitablement enclins à considérer un tel comportement comme une faute grave[10] constituant un motif valable du licenciement. Cela quel que soit sa manifestation, c'est-à-dire soit par l'appropriation d'une unité centrale, des disques durs ou tout autre support informatique de stockage d'information, ou

[8] Ould-Eba, M. (2013). Le rôle de l'information en droit des entreprises en difficulté, Thèse de doctorat, Université de Toulouse, p. 222

[9] Arrêt n° 674 du 12-07-2017, Dos. Soc. n°2184/5/2/2016

[10] Arrêt n° 430 du 24-06-2020, Dos. Soc. n° 1371/5/2/2018

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

l'accès à des informations secrètes de l'entreprise sans que la position professionnelle et juridique de ce salarié ne lui permette de le faire. Ceci constitue un abus de confiance et une tentative de divulgation d'un secret professionnel notamment lorsque cet acte a causé un préjudice à l'entreprise. Passons à présent à examiner de plus près d'autres fautes liées à la sécurité informatique au sein de l'entreprise.

II. La sécurité informatique

Les transgressions du salarié mettant en danger la sécurité informatique peuvent se matérialiser par le contournement des politiques de sécurité de l'entreprise (A), le téléchargement et l'utilisation de logiciels piratés ou non autorisés (B), une réaction inappropriée face aux menaces de cybersécurité (C), et enfin, l'abstention délibérée de signaler les incidents de sécurité (D).

A. Contournement des politiques de sécurité de l'entreprise

Le salarié vit aujourd'hui dans un environnement de plus en plus numérique, à travers le matériel mis à sa disposition lié le plus souvent à un réseau. En même temps les entreprises ont mis en place des politiques de sécurité informatique et des chartes d'utilisation des ressources informatiques afin de protéger leurs données sensibles et assurer la continuité de l'activité de l'entreprise.

Une politique de sécurité informatique dans une entreprise peut contenir plusieurs éléments, à savoir la définition des responsabilités des différents acteurs, les procédures et les règles pour gérer les accès aux systèmes et aux données, y compris l'utilisation de mots de passe forts, la gestion des comptes d'utilisateurs, la sécurisation du matériel comme les ordinateurs, les appareils mobiles et autres terminaux utilisés par les salariés, la protection des réseaux, l'utilisation de périphériques de stockage amovibles ainsi que les règles de communications électroniques internes et externes.

Les entreprises ont instauré des procédures pour identifier, évaluer et corriger les vulnérabilités potentielles dans le cadre de leurs politiques de sécurité informatique. Cependant, le contournement délibéré de ces politiques peut avoir des conséquences désastreuses sur l'entreprise et sur le salarié. En l'espèce, un employeur a pu établir à travers un bureau d'expertise externe spécialisé dans la sécurité informatique « la responsabilité de son salarié dans des opérations d'accès illégal à des données et informations confidentielles concernant la société et ses salariés, ainsi que l'espionnage du personnel en accédant à leurs boites de courriers électroniques et en falsifiant une application informatique dans le but de pirater des mots de passe et d'usurper l'identité d'un utilisateur/salarié pour envoyer un courrier électronique en son nom »[11].

Ces faits, qui constituent un contournement flagrant des politiques de sécurité, ont causé des dommages matériels considérables à l'entreprise, se manifestant par la nécessité d'utiliser des mécanismes de communication non conventionnels entre les responsables et les salariés. De même, l'entreprise a dû faire appel à des experts spécialisés pour sécuriser son système d'information.

Au-delà de la faute grave à prouver par le rapport de l'expert, des poursuites pénales peuvent être envisagées, ce qui montre que la technologie qui ne cesse d'offrir des opportunités exceptionnelles au travail, crée également de nouveau défis en matière d'éthique et de responsabilité disciplinaire, civile et pénale au sein du monde professionnel.

[11] Arrêt n° 588 du 30-06-2020, Dos. Soc. n° 2362/5/1/2018

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

Aux yeux du droit disciplinaire, le salarié qui enfreint délibérément les règles et politiques de sécurité informatique établies par son employeur, pourra compromettre la confidentialité, l'intégrité et la disponibilité des données et systèmes de l'entreprise, mettant ainsi en danger ses intérêts et sa réputation.

En somme, une politique de sécurité des systèmes d'information vise à établir des normes de conduite pour les salariés dans leur utilisation des moyens et du matériel informatique au sein de l'entreprise. Le contournement des politiques de sécurité informatique peut être considéré comme un manquement grave à ces normes. En conséquence, cela peut entraîner des sanctions disciplinaires sévères pour faute, en fonction de la gravité de la violation et de ses conséquences néfastes. Continuons ainsi notre exploration en abordant désormais le sujet des fautes liées à l'utilisation frauduleuse de logiciels.

B. Téléchargement et utilisation de logiciels piratés ou non autorisés

Au niveau juridique, le Maroc ne s'est, en réalité, jamais attaqué à la commercialisation de produits issus de la contrefaçon, notamment ceux qui relèvent du domaine des technologies de l'information et de la communication. L'on note que le Maroc n'a adhéré à la convention de Berne sur la propriété intellectuelle, adoptée en 1886, qu'en 1987. La loi relative au droit d'auteur et au droit voisin est entrée en vigueur seulement en l'an 2000. On peut noter, par exemple, que le Maroc est considéré comme une plaque tournante du « piratage » au niveau mondial, après la Chine et certains pays de l'Est et de l'Amérique latine[12].

Avec la loi 2-00 portant sur les droit d'auteur et droits voisins, les concepteurs de logiciels sont devenus protégés, après avoir entrée en vigueur le 18 novembre 2000, modifiée et complétée par Dahir portant promulgation de la loi n° 79-12[13] et la loi 34-05[14]. Cette loi interdit entre autres, le piratage des programmes d'ordinateur.

D'après la présente loi, « un "programme d'ordinateur" est un ensemble d'instructions exprimées par des mots, des codes, des schémas ou par toute autre forme pouvant, une fois incorporés dans un support déchiffrable par une machine, faire accomplir ou faire obtenir une tâche ou un résultat particulier par un ordinateur ou par un procédé électronique capable de faire du traitement de l'information »[15]. Désormais, la protection concerne essentiellement en matière de technologie de l'information, entre autres, les téléchargements et utilisation des logiciels sous licence, sans autorisation et de manière illégale.

Si aujourd'hui l'on voit une certaine tolérance vis-à-vis des utilisateurs parmi le public et surtout à des fins personnels, pour absence d'une politique publique efficiente dans le domaine de la protection de la propriété intellectuelle contre les particuliers et les difficultés d'attaquer des clients (personnes physiques) généralement vulnérables, l'on constate que la réaction

[12] **Ledjou, J.-M. et Randrianasolo-Rakotobe (H). (2012). Des réseaux et des hommes. Les suds à l'heure des technologies de l'information et de la communication. Collectif et Bernard Miège. Edition Karthala, p.141**

[13] Bulletin Officiel n° 6266 du 21 chaabane 1435 (19 juin 2014), p. 3588

[14] Bulletin Officiel n° 5400 du 1er safar 1427 (2 mars 2006), p. 325

[15] Définition avancée par l'article premier de la loi n° 2-00 relative aux droits d'auteur et droits voisins telle que modifiée et complétée par la loi n° 34-05.

des éditeurs est totalement différente lorsqu'il s'agit d'un établissement ou d'une entreprise[16]. Cela est dû au fait que les éditeurs de solutions informatiques ont pu gagner plusieurs procès devant la justice et n'hésitent plus à lancer la grande offensive contre le piratage, la commercialisation et l'utilisation sans licence valable de leurs logiciels[17], vue que l'internet leur permet aujourd'hui de détecter toute installation illégale.

Derechef, si un salariés procède au téléchargement et à l'utilisation d'un logiciel piraté, hors licence, de sa propre initiative, et de manière non autorisée au nom de son employeur, il peut s'exposer à des sanctions disciplinaire puisque les sociétés éditrices de logiciels vont engager des poursuites à l'encontre des sociétés privées pour utilisation illégale de leurs produits, ce qui pourraient compromettre l'intégrité de l'entreprise qui emploie le salarié fautif, sans oublier les autres conséquences néfastes sur le plan juridique, financier et réputationnel.

A partir de ce constat, il commet une faute grave le salarié qui télécharge et utilise illégalement un logiciel sur son ordinateur professionnel[18] imposant à son employeur de payer une redevance importante pour régulariser sa situation envers la société éditrice de logiciels. Les dommages potentiels associés à cette faute ne sont pas moins importants que les réponses inadéquates liées aux menaces de la cybercriminalité résultant d'une négligence flagrante de la part du salarié.

C. Réponse inadéquate aux menaces de cybersécurité

Les menaces en matière de cybersécurité peuvent compromettre la confidentialité, l'intégrité et la disponibilité des données sensibles de l'entreprise et de sa capacité d'exercer son activité à cause des perturbations causées par les cybercriminels qui exploitent souvent les failles de sécurité du système informatique de l'entreprise et les fautes des salariés en réponse aux diverses menaces et cyberattaques.

Une cyberattaque peut être définie comme un « ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité »[19]. Ces attaques revêtent diverses formes, dont l'utilisation de logiciels malveillants pour verrouiller les données de l'entreprise, entraînant ainsi une impossibilité d'accès au système et parfois demandant une rançon en échange. D'autres types sont sous forme de programmes indésirables également injectés dans le système informatique pour voler les données, perturber son fonctionnement ou détruire des fichiers.

Selon l'Indice de la cybersécurité dans le monde (GCI-2018) de l'UIT, le Maroc occupe la 93ème place parmi les 197 pays couverts en 2018. Cette performance relativement moyenne du Maroc nécessite une attention particulière qui doit être portée au critère de renforcement des capacités des entreprises, et de bâtir une

[16] Décision n° 5288/2013 du 05-12-2013, Dos. n° 3182/2012/17 : Procès Sage Software contre une société qui installe le fameux logiciel de comptabilité sans licence. (Cour d'appel de commerce de Casablanca).

[17] Décision n° 859 du 18-02-2005, Dos. n° 1275/12/02 de la Cour d'appel de commerce de Marrakech. Décision n° 1326/2011 du 05-04-2011, Dos. 3888/2010/17 de la Cour d'appel de commerce de Casablanca: Procès *Microsoft Corp* contre des sociétés qui offrent des logiciels piratés comme Microsoft Office et Windows.

[18] Cass. soc., 16 juin 2015, n°13-26.913, Inédit

[19] France, Ministère des armés, « Lexique des termes utilisés dans la Loi de programmation militaire 2019-2025 ». www.defense.gouv.fr

infrastructure sécuritaire à la hauteur du défi[20].

Du côté des entreprises, la CGEM a élaboré un guide[21] en matière de « cybersécurité en entreprise », la confédération a proposé aux employeurs marocains certaines mesures indispensables et a mis l'accent sur la question de sensibilisation. D'après le « guide », la réponse adéquate aux menaces de cybersécurité passe avant tout par le top management, et la sensibilisation de chacun des salariés dans leur quotidien professionnel, en leur précisant les conditions d'utilisation du matériel informatique, de la messagerie ou encore l'utilisation mixte d'un matériel informatique de l'entreprise comme l'insertion des clés USB personnelles ou un disque de stockage de données externe.

Si le renforcement de l'équipe technique par des professionnels hautement qualifiés est un moyen de prévention, la mise en place de réglementations du travail peut également optimiser cette prévention. Plusieurs pratiques, encadrées par le droit du travail, peuvent être instaurées au sein de l'entreprise afin de réduire les risques liés à la cybercriminalité et inciter les salariés à ne pas ignorer les mesures de prévention nécessaires en cas d'attaque. Cela passe par une sensibilisation et une formation régulières des salariés, ainsi que l'élaboration d'un plan d'actions comme norme impérative en cas de cyberattaque, cela peut garantir une réponse appropriée face aux diverses menaces informatiques.

En cas d'accès libre à internet, le salarié doit impérativement ignorer tout message reçu d'un émetteur douteux. Le fait de cliquer sur un lien malveillant ou accéder à un site web non sécurisé peut menacer la cybersécurité de l'entreprise et constituer une réponse inadéquate à une menace cybernétique susceptible d'exposer l'entreprise à des risques majeurs entravant son activité et son image.

Toute réponse inadéquate par un salarié aux menaces de cybersécurité et essentiellement lorsqu'elle est volontaire peut constituer une faute grave et un motif de licenciement pour plusieurs raisons ; d'abord il s'agit clairement d'une violation de la politique de sécurité informatique. En plus, l'accès à des sites malveillants ou l'utilisation de périphériques infectés peut introduire des logiciels malicieux, des virus ou d'autres formes de programmes nuisibles dans le réseau de l'entreprise. Cela peut entraîner la compromission des données sensibles, la fuite d'informations confidentielles ou même des attaques plus larges contre l'infrastructure informatique de l'entreprise, avec des répercutions financières couteuses pour l'employeur. Ce dernier peut considérer de tels actes comme des fautes graves pouvant justifier un licenciement immédiat. Passons en suite à la faute liée à la détection et la non déclaration d'incidents de sécurité.

D. Défaut de signaler les incidents de sécurité

L'agence nationale de la sécurité des systèmes d'information française (ANSSI) définit l'incident de sécurité comme étant « un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc. »[22].

Il s'agit d'un événement, potentiel ou avéré, indésirable et/ou inattendu,

[20] AUSIM Association des utilisateurs des systèmes d'information au Maroc (2018). Les enjeux de la sybersécurité au Maroc, DATAPROTECT/AUSIM, (6), p. 9

[21] CGEM. (2022). Cybersécurité en entreprise : Guide de bonnes pratiques », p. 22, URL : www.cgem.ma

[22] Agence nationale de la sécurité des systèmes d'information, définition du Glossaire, URL : https://www.ssi.gouv.fr/entreprise/glossaire/i/

impactant ou présentant une probabilité forte d'impacter la sécurité des systèmes d'information, ce qui pourra perturber le bon fonctionnement de l'entreprise. L'incident de sécurité se différencie généralement des autres incidents par son degré de gravité ainsi que son risque pour l'organisation.

En cas de détection d'un incident de sécurité, le salarié doit passer par les circuits appropriés, afin de remonter l'information. Le Service Desk ou l'équipe intermédiaire concernée peut être le point d'entrée pour le signalement des incidents liés à la sécurité du système d'information dans les meilleurs délais.

C'est ainsi que le fait de ne pas signaler un incident de sécurité est susceptible d'être évalué comme une faute d'omission et une violation de la part du salarié des consignes de sécurité en sein de l'entreprise, ce qui constitue un manquement passible d'une sanction disciplinaire, allant de l'avertissement au licenciement.

Le signalement des incidents peut aider à repérer les évènements et failles sécuritaires et faire face aux risques liés aux cyberattaque menaçant les systèmes d'information et faciliter leur résilience au cas où l'incident s'est produit.

Les incidents de sécurité informatique qui nécessitent une attention particulière peuvent varier, il y a notamment le Phishing (hameçonnage), « qui consiste, pour un individu à répondre à un message qu'il croit émaner d'un de ses contacts[23] », il s'agit d'une méthode courante de vol de données, tels que les identifiants d'utilisateurs et leurs mots de passe. Il y a aussi incident de sécurité informatique qui n'est pas forcément lié au système d'information mais plutôt au matériel d'exploitation lui-même de nature informatique. C'est lorsqu'un appareil informatique est perdu ou volé (PC portable, unité centrale, disque de stockage de donnée, téléphone portable professionnel…), ce genre d'incident doit être rapidement remonté afin de lancer une riposte.

Cependant, dès lors qu'un salarié identifie une fuite de données accidentelle, comme par exemple un mauvais routage d'un e-mail ou l'ajout par erreur d'une pièce jointe inappropriée, il est impératif de le notifier immédiatement. Omettre de signaler ce type d'incident pourrait compromettre la nature involontaire de l'acte, ce qui pourrait ultérieurement être considéré comme une faute grave de la part du salarié. Ceci, à son tour, pourrait conduire à des sanctions disciplinaires sévères à l'encontre de l'employé.

Dans un environnement professionnel de plus en plus axé sur la protection des données, la réactivité et la diligence dans la gestion des incidents liés à la sécurité informatique sont cruciales. Si un salarié observe un incident tel qu'une fuite de données causée par une erreur dans le processus de communication électronique, il est non seulement de sa responsabilité mais également de son intérêt de signaler rapidement cette situation à sa hiérarchie ou au service compétent.

En ne rapportant pas cette situation, le salarié prend le risque que l'incident, qui aurait pu être considéré comme accidentel et involontaire, soit interprété autrement. Le fait de ne pas signaler l'incident peut être interprété comme un manquement à l'obligation de diligence et de responsabilité inhérente à la gestion des données et de la sécurité informatique au sein de l'entreprise. Cette interprétation peut avoir des conséquences graves sur la carrière et la réputation professionnelle du salarié.

[23] Julien, M. (2022). La confiance numérique dans le domaine bancaire. Thèse de doctorat. Université La Rochelle, p. 221

Par conséquent, il est essentiel que les employés soient pleinement conscients de leur rôle dans la préservation de la sécurité des données et de l'importance cruciale de signaler promptement toute fuite ou incident, même s'il s'agit d'une erreur accidentelle. Une communication proactive et efficace des incidents est fondamentale pour maintenir un environnement professionnel sûr et sécurisé, et cela se reflète positivement sur l'intégrité et la fiabilité de l'ensemble de l'entreprise.

Après avoir conclu l'existence de fautes dans la violation des obligations liées à la protection des données de l'entreprise et dans les menaces à la sécurité informatique, il est également crucial de souligner une autre faute, à savoir l'utilisation abusive des ressources informatiques de l'entreprise.

III. L'utilisation abusive des ressources informatiques

Les fautes du salarié concernant l'utilisation abusive des ressources informatiques peuvent se manifester par l'utilisation démesurée de l'ordinateur à des fins personnelles pendant les heures de travail (A), le téléchargement et l'accès au contenu inapproprié sur internet (B), l'usage des outils informatiques de l'entreprise pour tirer un profit personnel (C), et enfin, le cyberharcèlement et la diffamation via les canaux de messagerie professionnelle (D).

A. Utilisation excessive pendant le temps de travail à des fins personnelles

L'utilisation excessive majeure de l'outil informatique consiste dans le fait de surfer sur internet pendant les heures de travail. Si l'usage personnel d'internet par le salarié dans l'entreprise s'avère parfois tolérée par l'employeur, ce dernier possède aujourd'hui d'autres alternatives pour limiter l'accès à certaines adresses web jugées par lui et par la nature de l'activité de l'entreprise comme source de fuite et de perte majeure du temps de travail, comme les réseaux sociaux ou les sites de divertissement entre autres.

Cependant toute interdiction de l'usage personnel d'internet doit être disproportionnée, le salarié ne peut être coupé totalement du monde extérieur sauf si la nature et la tâche à accomplir au sein de l'entreprise l'en exige. A défaut, l'interdiction serait une atteinte au droit d'avoir une vie privée et à la liberté individuelle du salarié.

Toutefois, l'employeur peut interdire l'usage abusive par le salarié de l'outil informatique, notamment l'ordinateur, dans la navigation sur internet pour des fins loin du but recherché et des taches inhérentes à la fiche de poste du salarié, et ce même en l'absence d'un préjudice. L'employeur peut même informer l'ensemble des membres de l'entreprise de cette interdiction d'usage abusive en insérant un tel comportement dans la liste des fautes qui figurent dans le règlement intérieur ou la charte d'utilisation des moyens et ressources informatiques.

D'ailleurs, ce formalisme n'est pas obligatoire, c'est une obligation inhérente au contrat de travail, et aux pouvoirs de l'employeur, qui dispose d'un certain nombre de prérogatives, qui se traduisent par des ordres, des directives, et des sanctions qu'il peut prononcer à l'encontre du salarié. Traditionnellement, on distingue le pouvoir de direction, le pouvoir réglementaire et le pouvoir disciplinaire[24].

Cependant, au sujet du matériel et périphériques informatiques mis à

[24] Bocquillon J-F. (2022). Les pouvoirs de l'employeur et les libertés des salariés. *DCG 3. Droit social.* Paris, Dunod, « Expert Sup », p. 170-189

disposition du salarié dans le cadre de l'exécution des tâches qui lui sont confiées, c'est plutôt la diversité qui caractérise la jurisprudence, à cause « du caractère duel de l'outil. Evidemment professionnel, celui-ci se voit nécessairement détourné à des fins personnelles, ne serait-ce que de manière minime et raisonnablement »[25].

Dans une décision de la Cour d'appel de Paris, constitue une faute professionnelle le fait d'utiliser de façon abusive son ordinateur durant le temps de travail, de passer plusieurs heures par jour sur des sites internet de rencontre, d'immobilier, de musique et de jeux, et de participer également à des conversation en ligne et que les connexions étaient fréquentes, même si le salarié pouvait se prévaloir de bons résultats dans le cadre de ses missions[26].

Un tel usage abusif de la navigation internet en se servant des ressources informatiques de l'entreprise pendant la durée du travail pourra apporter une perturbation à la bonne marche de l'entreprise ; il peut même constituer un bien-fondé d'une sanction disciplinaire en raison d'un abus de confiance.

D'ailleurs, l'abus de confiance est le fait pour une personne, à qui a été remis de l'argent ou un bien, de détourner l'usage de ce bien à son profit ou pour un usage frauduleux. Cela pourra concerner notamment le détournement de l'usage du temps de travail, et les moyens de travail, à son profit ou pour un usage abusif non profitable à l'entreprise. En l'espèce l'abus a été reconnu par une décision de la Cour d'appel de Paris qui a confirmé le fait fautif de consacrer plus de 20 % de son temps de travail et de présence dans l'entreprise à visiter Facebook et d'autres sites web sans rapport avec le travail[27]. La conclusion est que l'usage de l'internet pendant le temps du travail et avec les moyens de l'entreprise ne doit pas dépasser « un minimum vital », par contre l'usage excessif est digne de la qualification de « faute grave ».

Afin d'explorer de manière approfondie les ramifications de comportements en ligne inappropriés, nous orientons maintenant notre attention vers la question des fautes disciplinaires liées au téléchargement et à l'accès à du contenu inapproprié sur Internet.

B. Téléchargement et accès à du contenu inapproprié sur Internet

Toute utilisation inappropriée de l'ordinateur mis à la disposition du salarié dans des activités non professionnelles constitue une violation sérieuse des règles de travail et de la politique de l'entreprise. C'est une faute qui peut avoir des conséquences graves pour le salarié.

En l'espèce, un employeur n'a pas hésité à considérer que son salarié « avait commis une faute grave consistant à utiliser l'ordinateur de l'entreprise à des fins contraires aux bonnes mœurs »[28]. De même, un employeur a pris la décision de licencier l'un de ses salariés pour « l'envoi des insultes et des injures accompagnées d'images pornographiques aux responsables de l'entreprise »[29] après avoir téléchargé un contenu de nature sexuelle via l'ordinateur et le réseau de la société et s'est servi enfin de la messagerie professionnelle pour un tel acte. Le salarié

[25] Amic, L. (2014). La loyauté dans les rapports de travail. Thèse de doctorat. Université d'Avignon, p. 501

[26] Cour d'appel de Paris, pôle 6 - ch. 7, 12 septembre 2019, n°17/09980

[27] Cour d'Appel de Rennes, 20 novembre 2013, n°12/03567

[28] Arrêt n° 783 du 12-06-2014, Dos. Soc. 2013-1-5-1366

[29] Arrêt n° 725 du 30-06-2021, Dos. Soc. 2019-2-5-2643

s'est retrouvé confronté à une poursuite judiciaire pour avoir commis une faute grave, que seul un vice dans le respect de la procédure de licenciement a pu lui permettre d'échapper de la validation de la sanction la plus sévère.

En France, la jurisprudence a établi des précédents significatifs en matière de faute grave liée à des comportements inappropriés sur le lieu de travail en ce qui concerne l'utilisation inadéquate des outils informatiques. Un cas marquant a été celui où la Cour du Quai de l'Horloge a validé le licenciement pour faute grave d'un salarié ayant été découvert avec pas moins de 500 Go de fichiers pornographiques stockés sur son ordinateur professionnel, équivalant à la capacité totale d'un disque dur. Cette affaire souligne l'importance cruciale de l'utilisation responsable des ressources numériques mises à disposition par l'employeur, mettant en lumière le fait que de tels comportements peuvent être considérés comme des fautes graves, entraînant des conséquences disciplinaires substantielles[30].

D'ailleurs, seule la constatations d'une visite de sites pornographiques peut coûter un licenciement, sinon une sanction lourde pour le salarié, sous prétexte que la navigation dans un tel site et le clic sur ses différents liens peut mettre en péril la sécurité informatique[31] sans nier l'incidence de ces pratiques sur l'image de l'entreprise[32].

Quant au Dark web, qui n'est accessible que par des navigateurs Web spécialement conçus à cet effet ou via des logiciels, des configurations ou des protocoles spécifiques. Celui-ci attire un grand public notamment à cause de plusieurs plateformes de ventes de stupéfiants et autres produits illicites, ainsi que certains processus liés à l'extorsion de fonds, de même que les sites de vente de données piratées.

Sur le Dark web, il est possible de trouver des offres incluant la cybercriminalité ainsi que les services de piratage de données provenant d'institutions financières ou de banques, et la commercialisation d'armes à feu. Naviguer dans le Dark web n'est pas illicite par nature, cela dépond de l'utilisation de son contenu à des fins illicites. Le salarié qui accède à un tel contenu et participe à des activités non conformes à la loi et aux règles imposées par l'employeur est généralement considéré comme fautif pour violation des politiques de sécurité informatique et cela peut constituer un motif de licenciement.

Afin d'explorer une facette supplémentaire des fautes disciplinaires liées à l'utilisation inappropriée des outils informatiques en milieu professionnel, nous nous penchons maintenant sur le cas spécifique de ceux qui cherchent à tirer un profit personnel en exploitant l'ordinateur de l'entreprise et ses accessoires de manière détournée.

C. Utilisation inappropriée des outils informatiques de l'entreprise pour un profit personnel

L'utilisation des ressources informatiques de l'entreprise à des fins lucratives personnelles, en dehors des tâches spécifiquement définies par l'employeur, peut facilement être classée parmi les fautes graves liées à la concurrence déloyale. En effet, le contrat de travail qui lie le salarié à son employeur comprend généralement une clause d'exclusivité pendant la relation de travail, interdisant au salarié l'exercice de toute activité similaire à celle de l'entreprise ou non, telle que la vente du même produit ou la fourniture de la même prestation ou service aux clients en échange d'une rémunération versée

[30] France, Cass. soc., 16 mai 2007, n°05-43.455
[31] Cour d'appel de Rennes, 19 avril 2007, n°06/03156
[32] Conseil de prud'hommes de Lyon, 28 février 2007, R.G. n°04/03949

directement au compte du salarié, ou bien l'exercice de toute autre activité commerciale génératrice de profit personnel.

En effet, « le motif qui constitue une concurrence pour l'employeur justifie le licenciement du salarié, lorsqu'il exécute des actions qui affectent effectivement l'activité de l'employeur sur le marché du travail, telles que l'utilisation par le salarié de son expérience ou de ses services pour le compte d'une entité autre que l'employeur d'une manière qui affecte son rendement au travail auprès de son employeur, ou divulgue des secrets de l'entreprise dans laquelle il travaille »[33].

D'après la jurisprudence de la cour de Cassation, cela concerne non seulement les activités concurrentes par rapport à celles de l'entreprise, mais également toute autre activité menée en dehors des missions qui ont été spécifiquement confiées au salarié dans l'entreprise, pour lesquelles il perçoit un salaire régulier. Si le salarié entreprend une activité commerciale en utilisant les ressources informatiques de l'entreprise, son expérience dans les activités de la branche informatique, et on se servant notamment des ordinateurs, de la connexion internet, et autres outils informatique de l'entreprise, et sans autorisation préalable de l'employeur, cela peut constituer une faute grave aux yeux du juge social.

En général, l'employeur conserve la prérogative de refuser une telle autorisation, renforçant ainsi l'importance des clauses d'exclusivité présentes dans les contrats de travail. Ces clauses énoncent clairement que le salarié s'engage à consacrer son temps et ses compétences à l'accomplissement des tâches spécifiques déterminées par et pour l'employeur exclusivement. Cette règle fondamentale repose sur la notion que l'emploi au sein de l'entreprise est basé sur un accord mutuel où le salarié met à disposition ses compétences pour atteindre les objectifs définis par l'employeur. Ainsi, l'utilisation des ressources informatiques de l'entreprise à des fins lucratives personnelles peut être considérée comme une violation de cette relation professionnelle. Le salarié est donc dans l'obligation de maintenir l'intégrité de son engagement envers l'entreprise et doit éviter toute utilisation inappropriée des outils informatiques mis à sa disposition.

La même situation s'applique au salarié qui procède à la création d'une entreprise en son nom et utilise les outils de travail, y compris son ordinateur professionnel. Cela est considéré comme une violation de son engagement envers son employeur. « Dans la mesure où l'employé n'a pas nié avoir fondé une entreprise concurrente de l'employeur, et sachant qu'une clause du contrat de travail qui le lie à l'employeur l'empêche d'exercer toute activité similaire à son travail, quelle que soit sa nature, sans une autorisation spéciale délivrée par l'entreprise employeuse, et n'a pas contredit cela lors de l'audition, la faute grave qui lui est imputée demeure établie à son encontre »[34].

Dans le cas où le contrat de travail ne comporte pas de stipulations spécifiques ou de clauses d'exclusivité, le salarié n'est pas contraint, au cours de la période du contrat, de se consacrer exclusivement à un seul employeur. Cette disposition vise à éviter toute injustice en empêchant le salarié de cumuler divers emplois, particulièrement s'il s'agit d'emplois à temps partiel, tant que cela ne présente aucun risque de préjudice. Ici, ce n'est que la question de l'exploitation des outils informatiques ou des équipements mis à la disposition du salarié à des fins lucratives personnelles, loin des tâches qui lui ont été confiées par

[33] Arrêt n° 180 du 23/02/2005. Dos. Soc. n° 772/5/1/2004

[34] Arrêt n° 349 du 31/03/2021. Dos. Soc. n° 531/5/2/2019

son employeur, qui permet à ce dernier de considérer cet acte comme une faute grave de la part du salarié.

En explorant les aspects cruciaux des fautes disciplinaires liées à l'utilisation des outils informatiques en milieu professionnel, nous nous tournons en fin vers un sujet particulièrement délicat : le cyberharcèlement et la diffamation par le biais de la messagerie professionnelle. Cela souligne l'importance croissante de la communication numérique dans le monde du travail et les implications sérieuses que de tels comportements peuvent avoir sur le bien-être des salariés et l'environnement professionnel.

D. D. Le cyberharcèlement et la diffamation par messagerie professionnelle

Le développement d'internet a permis un large recours à la correspondance par messagerie électronique entre entreprises et entre salariés au sein d'une même entreprise, mais ce rôle s'est ainsi retrouvé disséminé permettant par conséquent l'apparition du cybercrime et de harcèlement. Le cyberharcèlement, à l'instar des autres infractions en ligne, est facilité par de nombreux éléments : « du côté de la victime, la non-protection de ses données et les fragilités des systèmes ; du point de vue de l'auteur, la perception de la distance entre la cybervictime et lui, et l'immatérialité de l'action qui peuvent créer une forme de déresponsabilisation »[35].

Selon Bocij et McFarlane (2002), le cyberharcèlement est le fait pour un individu « d'utiliser les technologies de l'information et de la communication dans le but de harceler une ou plusieurs personnes. Les comportements de l'individu peuvent inclure (…) des menaces et des allégations mensongères, le vol d'identité et de données, des atteintes aux équipements ou aux données, la surveillance des équipements (…). Le harcèlement est un ensemble de conduites et de moyens d'action qu'une personne raisonnable, en possession de telles informations sur une tierce personne, sait qu'elle lui causerait une grande détresse émotionnelle »[36].

Le cyberharcèlement est une forme de violence numérique qui peut s'exercer à travers l'ordinateur et via les canaux de communication mis à la disposition du salarié comme la messagerie professionnelle. Les messages électroniques objets du cyberharcèlement peuvent contenir des menaces, des insultes ou du chantage.

Lorsque l'on considère que le harcèlement sexuel est une faute grave lorsqu'il est commis par l'employeur, il est étonnant que le législateur n'ait pas pris en compte la nécessité de le qualifier également en tant que faute grave pour le salarié qui peut le commettre à l'encontre d'un autre salarié. Cela est particulièrement pertinent étant donné que le harcèlement, tel que compris par le législateur, peut se produire en raison du pouvoir conféré à l'employeur au sein de l'entreprise et de sa capacité à en abuser, étant la partie la plus puissante.

Le code du travail marocain semblait être en plus, limité dans sa configuration lorsqu'il ne considère plus qu'un harcèlement pourra être entre salariés sans implication de l'employeur notamment en l'absence de toute alerte lancée, c'est le cas où un salarié de catégorie socioprofessionnelle supérieur pourrait harceler un salarié de rang inférieur, ou un salarié plus expérimenté pourrait harceler

[35] Estano, N. (2019). Les nouvelles technologie et cyberharcèlement : l'exemple du swatting. *Criminologie*, Vol. 52, No. 2, *La criminologie de l'information : état des lieux et perspectives*, p. 18

[36] Bocij, P. et McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, n° 139, p. 38.

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

une nouvelle recrue. En réalité, le Code du Travail n'a pas pris en compte le harcèlement sexuel entre les salariés jusqu'à ce que le droit pénal intervienne avec des sanctions sévères contre les auteurs du harcèlement sexuel.

Cependant, à moins que le législateur ne considère que le harcèlement sexuel entre salarié puisse constituer une incitation à la débauche, ce qui ne semble pas être le cas, étant donné que le Code du Travail aborde conjointement les fautes graves de l'employeur, il est difficile de comprendre pourquoi le législateur n'a pas inclus le harcèlement sexuel commis par les salariés.

Afin de faciliter notre compréhension de la question du harcèlement sexuel, et compte tenu de la révolution numérique qui a eu lieu dans les entreprises, il est impératif que le législateur examine également le harcèlement numérique, qu'il soit de nature sexuelle ou morale.

Le harcèlement moral, malheureusement, a été omis par le législateur marocain, puisqu'aucune définition de ce terme n'apparaît dans la législation du travail. Bien que ce concept soit relativement nouveau, la jurisprudence a réussi à en définir certaines caractéristiques. Peut-on alors envisager le harcèlement moral numérique ?

Le dénigrement de la personne du salarié est une des formes du harcèlement, elle se traduit par l'humiliation, l'insulte, la moquerie et le reproche. Aussi le salarié qui suit et traque sans relâche les moindres faits et gestes de sa victime à travers ses courriers électroniques est un harceleur. « Ce type de violence se met en place par l'envoi répété de messages injurieux ; le but étant de faire savoir à la proie que celle-ci est épiée, [alors que] l'objectif premier est de nuire à la personne. L'agression est réitérée et le harcelé est plongé dans une détresse profonde car il ne peut répliquer à l'affront. Cette situation est due notamment à la disproportion de pouvoir dans la relation entre le harcelé et le harceleur »[37], et c'est le cas notamment des rapports entre salariés dans leur relation hiérarchique.

Certes le harcèlement moral n'est pas explicitement traité dans la législation de travail ni dans le code pénal, alors qu'il est très répondu dans les entreprises. De plus, il est souvent utilisé comme moyen redoutable pour inciter les salariés à déposer leur démission. Il est impératif de mettre fin définitivement à de telles pratiques en adoptant une législation qui pénalise ou interdit de tels comportements, tels que le harcèlement moral sur le lieu de travail, tout en imposant des sanctions disciplinaires à l'encontre du salarié harceleur, quel que soit ses canaux, directement ou via messagerie, tout en garantissant une protection complète pour les victimes de harcèlement.

CONCLUSION

L'évolution rapide des technologies de l'information dans le milieu de travail a entraîné de nouveaux défis en matière de droit du travail, notamment en ce qui concerne l'utilisation des ordinateurs et des outils informatiques par les salariés. Bien que le Code du Travail traite déjà de certaines questions liées à l'utilisation du matériel de l'entreprise au travail, il est possible que des ajustements soient nécessaires pour tenir compte des aspects spécifiques liés aux nouvelles technologies.

Actuellement, plusieurs principes du Code de Travail peuvent être appliqués pour réglementer l'utilisation des ordinateurs au travail. Par exemple, l'employeur a le droit de mettre en place un règlement intérieur

[37] Julie Alev Dilmaç et Özker Kocadal, « Prévenir le cyberharcèlement en France et au Royaume-Uni : une tâche impossible ? », *Déviance et Société*, Vol. 43, (mars), 2019, p. 396

dans l'entreprise, définissant les modalités d'utilisation des outils informatiques par les salariés. Ces règles doivent être claires, communiquées aux employés et doivent respecter les droits fondamentaux, tels que la vie privée.

Cependant, si des ajustements sont jugés nécessaires pour traiter spécifiquement des fautes graves potentielles liées à l'utilisation des ordinateurs, une évolution du Code de Travail pourrait être envisagée. Cela pourrait inclure des dispositions spécifiques sur les sanctions en cas de comportement inapproprié ou de fautes graves commises par les salariés par le biais des outils informatiques de l'entreprise.

Il est important de noter que les entreprises ont également un rôle à jouer en définissant des politiques internes claires et en sensibilisant les salariés aux risques liés à l'utilisation des technologies. Cela peut inclure des formations sur la sécurité informatique, la confidentialité des données, et des rappels réguliers des règles internes de l'entreprise.

L'utilisation de l'ordinateur en entreprise comportera toujours des risques. Le salarié doit être conscient de ces risques et prendre les mesures nécessaires pour les éviter. Il doit notamment respecter les règles et les consignes fixées par son employeur.

Toute modification du Code de Travail devrait être élaborée en concertation avec les partenaires sociaux afin de trouver un équilibre entre la protection des droits des salariés, la prévention des abus, et la nécessité pour les entreprises de protéger leurs intérêts légitimes en sanctionnant les fautes graves susceptibles d'être commises par les salariés à l'occasion de l'utilisation de l'ordinateur et tout autre matériel informatique de l'entreprise.

En fin, voici quelques points pertinents destinés aux réformistes, qui peuvent être intégrés et liés à l'utilisation des ordinateurs au travail, afin de favoriser un environnement professionnel sain et éthique.

Droit à la déconnexion : Certaines entreprises doivent fixer des modalités d'exercice du droit à la déconnexion. Cela vise à garantir le respect des temps de repos et de congé, notamment en limitant l'utilisation des outils numériques, comme l'ordinateur portable professionnel ou autre en dehors des heures de travail. Cela évite une appréciation arbitraire de la faute dite : « refus délibéré et injustifié du salarié d'exécuter un travail de sa compétence ».

Protection des données personnelles : La législation marocaine, notamment la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel impose une lourde responsabilité quant à la divulgation de ces données. La législation du travail de son côté, doit inviter les entreprises à assurer un verrouillage strict et rigoureux quant à la collecte et au traitement des données personnelles, y compris celles des salariés, car toute indulgence de la part des entreprises est susceptible d'impliquer le salarié dans la faute.

Contrôle de l'activité des salariés : Les employeurs ont le droit de contrôler l'activité de leurs salariés, mais cela doit être fait dans le respect de certaines limites. Tout système de surveillance des salariés, y compris l'utilisation des ordinateurs, doit respecter la vie privée des salariés. Cela pourra éviter tout abus de la part de l'employeur, en facilitant aux juges leur tâche d'apprécier la gravité de la faute, ou l'existence même des motifs invoqués par l'employeur.

Obligation d'établir une charte informatique : Les entreprises doivent mettre en place des chartes informatiques ou intégrer au minimum des dispositions dans les règlements intérieurs qui

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

 ISSN: 2737-8101

définissent les règles d'utilisation des outils informatiques au sein de l'entreprise. Cette pratique devrait non seulement être promue, mais également encadrée par des dispositifs légaux en matière de travail.

Bibliographie

Amic, L. (2014). *La loyauté dans les rapports de travail*. Thèse de doctorat, Université d'Avignon.

AUSIM (Association des utilisateurs des systèmes d'information au Maroc). (2018). Les enjeux de la sybersécurité au Maroc. DATAPROTECT/AUSIM, (6).

Bertier-Lestrade, B. (2019). La bonne foi dans la réforme française des contrats. *Le contrat dans tous ses états*, Cécile Le Gallou (dir), Presses de l'Université Toulouse Capitole.

Bocij, P. et McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, 139.

Bocquillon, J. F. et al. (2022). Les pouvoirs de l'employeur et les libertés des salariés. *DCG 3. Droit social.* J. F. Bocquillon, C. Alglave, M. Mariage (dir) , Expert Sup, Paris, Dunod

Dilmaç, J. A. et Kocadal, O. (2019). Prévenir le cyberharcèlement en France et au Royaume-Uni : une tâche impossible ?. *Déviance et Société*, Vol. 43, (3)

Estano, N. (2019). Les nouvelles technologie et cyberharcèlement : l'exemple du swatting. *Criminologie*, Vol. 52, No. 2, *La criminologie de l'information : état des lieux et perspectives.*

Gambardella, S. (2017). La protection des données "sensibles" à l'ère du numérique : Regard sur le droit de l'Union européenne. TALEB-KARLSSON (A.) et BEAUREGARD-BERTHIER (O.) (Dirs), *Protection des données personnelles et sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?*, Bruylant.

Jourdain, P. (1992). La bonne foi. Rapport in *Travaux de l'association H. Capitant*, Litec.

Ledjou, J.-M. (2012). et Randrianasolo-Rakotobe (H). Des réseaux et des hommes. Les suds à l'heure des technologies de l'information et de la communication. Collectif et Bernard Miège. Edition Karthala.

Vicente, A. I. (2003). *La convergence de la sécurité informationnelle et la protection des données à caractère personnel : Vers une nouvelle approche juridique*, Thèse de doctorat, Université de Montréal.

Rapports et guides:

Confédération Générale des Entreprises du Maroc, (2022). Cybersécurité en entreprise : Guide de bonnes pratiques.

Ministère française des armés. Lexique des termes utilisés dans la Loi de programmation militaire 2019-2025. www.defense.gouv.fr

Jurisprudence marocaine :

Cour de cassation (https://juriscassation.cspj.ma/) :

Arrêt n° 180 du 23/02/2005. Dos. Soc. n° 772/5/1/2004

Arrêt n° 783 du 12-06-2014, Dos. Soc. 2013-1-5-1366

Arrêt n° 674 du 12-07-2017, Dos. Soc. n°2184/5/2/2016

Arrêt n° 588 du 30-06-2020, Dos. Soc. 2362/5/1/2018

Arrêt n° 430 du 24-06-2020, Dos. Soc. n° 1371/5/2/2018

Arrêt n° 349 du 31/03/2021. Dos. Soc. n° 531/5/2/2019

Arrêt n° 725 du 30-06-2021, Dos. Soc. 2019-2-5-2643

Cour d'appel de commerce de Casablanca :

Décision n° 1326/2011 du 05-04-2011, Dos. 3888/2010/17

Décision n° 5288/2013 du 05-12-2013, Dos. n° 3182/2012/17

Cour d'appel de commerce de Marrakech :

Décision n° 859 du 18-02-2005, Dos. n° 1275/12/02

Jurisprudence française *(https://legifrance.gouv.fr/) :*

Conseil prud'hommes de Lyon, 28 février 2007, R.G. n°04/03949

Cour d'appel de Rennes, 19 avril 2007, n°06/03156

Cass. soc., 16 mai 2007, n°05-43.455

Cour d'appel de Rennes, 20 novembre 2013, n°12/03567

Cass. soc., 16 juin 2015, n°13-26.913

Cour d'appel Paris, pôle 6 - ch. 7, 12 septembre 2019, n°17/09980

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023