|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Université de Tunis** | **Année Universitaire : 2019/2020** | | | |
| C:\Users\hpg61\AppData\Local\Temp\Rar$DIa0.182\essect-500px.png | **Session : □ PRINCIPALE** | | **□S1 □ Examen Final** | |
| **Filière et niveau : Master DIGITAL-MARKETING** | | | |
| **Épreuve de : Droit de l’Internet Et Sécurité Electronique** | | | |
| **Date Mercredi 08/01/2020**  **(12H-14H)** | **Durée : 2 Heures** | | **Nombre de pages : 02** |
| **Enseignant(es) : Madame Gammara Sarra** | | | |
| **Observations : Documents Non Autorisés** | | | | |

**Correction**

**PARTIE I : (12POINTS)**

#### Melle SALMA est salariée au prés d’une grande entreprise de MODE (création et Haute couture)

**Melle SALMA** pense constituer **une société en ligne** pour vendre ses propres créations (robes de soirée, de mariage et accessoires, etc….)

Elle prépare sérieusement son projet ; elle a fait des recherches actives sur Internet ;à la recherche de fournisseurs, de tissus nobles , des professionnels du domaine  et agents de publicité sur **les Réseaux sociaux .**

SALMA a discuté avec son amie **Sarra,** étudiante en Master Digital -Marketing, cette dernière lui a demandé de faire attention à certains points juridiques .

ELLE l’a prévenue surtout contre d’éventuelles sanctions disciplinaires pour l’usage de l’Internet professionnel pour des besoins privés.

**SALMA**  a répondu qu’elle ne risque rien puisque son employeur autorise l’usage de l’Internet pour des besoins personnels.

ELLE s’inquiète, par contre de **l’installation massive** de caméras de surveillance ; de qualité numérique très sophistiquée.

***Elle veut savoir :***

**1 :** **Quels sont les motifs pour lesquels l’employeur a décidé d’autoriser l’usage de l’internet pour des fins privées ? (04POINTS)**

**Internet représente aujourd’hui, un outil de travail d’une importance capitale et d’une utilité remarquable pour l’entreprise L’employeur et dans un souci :**

**\*\*\*De moderniser les moyens de travail**

**\*\*\* Assurer une meilleure productivité**

**\*\*\*Et surtout des conditions de travail plus avantageuses**

**Met à la disposition de ses salariés l’internet à haut débit pour accomplir leurs tâches professionnelles**

**2 : Le contrôle de l’ordinateur du salarié  est-il un Droit pour l’employeur ; « propriétaire du matériel »; OU constitue-il une atteinte aux droits du salarié ? (04POINTS)**

* *« Le contrat de travail est une convention par laquelle l’une des parties appelée « travailleur » ou salarié s’engage à fournir à l’autre partie appelée « employeur »* *ses services personnels sous la direction et le contrôle de celle-ci moyennant rémunération* » art 06 du code de travail
* Quel que soit le type de [contrat de travail](http://fr.wikipedia.org/wiki/Contrat_de_travail) au sein de l’entreprise, sur un chantier, à domicile, à distance etc….), le lien de subordination existe dès qu'une personne, l'[employeur](http://fr.wikipedia.org/wiki/Employeur), peut exercer son [pouvoir de direction](http://fr.wikipedia.org/w/index.php?title=Pouvoir_de_direction&action=edit&redlink=1) sur une autre personne, le salarié.

Dans la majorité des entreprises qui utilisent l’outil informatique, l’ensemble des postes sont aujourd’hui **connectés en réseau par l’ordinateur.**

**Plusieurs** raisons viennent justifier cette technique :

* - Partager le matériel (imprimante; scanner) et la connexion à Internet ou à l’Intranet.
* -Faciliter les communications des employés qui peuvent ainsi s’échanger des documents sans avoir à se déplacer(envois de mails).
* -Permettre la maintenance à distance des postes de travail

**La consultation par l’employeur EST LEGITIME en vertu du pouvoir de contrôle.** Les fichiers informatiques ou les emails crées par le salarié sont présumés avoir un caractère professionnel .

. Les employeurs utilisent **des logiciels de contrôle.   
-**Ces logiciels permettent **un suivi en temps réel de l’activité sur chaque poste informatique connecté.**

* -Ces logiciels peuvent être utilisés pour surveiller l’activité des employés (En effet l’employeur peut avoir intérêt à identifier les employés qui négligent leur travail.)
* **Le régime juridique applicable aux logiciels de contrôle** :   
  Les principes de base doivent être respectés, à savoir : **information du personnel , information des représentants syndicaux, respect du principe de proportionnalité.**
* **MAIS L’employeur doit s’abstenir de consulter les FICHIERS PERSONNELS** ; les mails OU de faire des investigations dans la vie privée du salarié.
* Le cas échéant l’employeur engagerait sa responsabilité pénale sur la base de l’article 253 du code pénal qui sanctionne et **réprime de 03 mois d’emprisonnement** **« Toute divulgation du « contenu d’une lettre, d’un télégramme ou de tout autre document »appartenant à autrui »**
* La jurisprudence a considéré comme «  licenciement abusif » **celui d’une salariée, pour avoir envoyé des messages électroniques outrageant à son employeur à une de ses collaboratrices sur le lieu de travail. Les messages ne comportant aucun élément professionnel laissant ainsi penser à une correspondance privée et il n’appartiendrait pas l’employeur de prendre connaissance de ces messages personnels émis ou reçus par l’outil informatique mis à la disposition du salarié pour son travail.** TB de 1 ère Instance de Sousse du 12/05 /2013
* **En contrepartie le salarié est tenu de :**

**Respecter le contenu de la CHARTE**

|  |
| --- |
| * L’employé ne doit pas se servir de l’adresse mail de l’entreprise pour son courrier personnel. * -          L’employé ne doit pas envoyer de mails dans lesquels il pourrait y avoir de la violence, du racisme, de l’intolérance à partir de la boite mail professionnelle. * -          L’employé ne doit pas envoyer de mails dans lesquels il mettrait en cause la réputation de l’entreprise . |

-      **3 : Quelles sont les conditions juridiques que l’employeur doit respecter lors de la mise en place d’un système de Vidéosurveillance dans l’entreprise ?** **(04POINTS**)

* Le salarié a t-il une vie privée concomitante à sa vie professionnelle, ou doit –il mettre sa vie privée à l’écart du moment où il a franchi la porte de son entreprise ?
* L’autorité de l’employeur comprend : le pouvoir de donner des directives, le pouvoir **d'en contrôler** l'exécution et le pouvoir **d'en sanctionner** la mauvaise exécution.
* Cependant, le lien de subordination n’a pas pour effet **de nier au salarié** son droit à **la vie privée tout comme l’ensemble** de ses droits fondamentaux.
* Une affirmation contraire serait de nature à **déshumaniser le salarié** et de le robotiser et serait donc contraire à la constitution consacrant le droit au respect de la vie privée **et le droit à la dignité**
* **L’employeur a le Droit d’utiliser les nouvelles technologies ; entre autre l’installation de caméras de surveillance SANS POUR AUTANT PORTER ATTEINTE aux droits de l’employé .**
* **POUR REALISER cet équilibre ; il faut que l’employeur respecte certaines conditions :**

|  |
| --- |
| 1/- L’obligation d’information :  L’information se fait par affichage, circulaire interne ou autre moyen. L’information doit se faire de manière claire et permanente de la mise en place d’un dispositif de contrôle et de surveillance , le cas échéant , cette surveillance serait clandestine et attentatoire aux droits des salariés   * Les représentants des salariés sont amenés à être informés et consultés préalablement à tout projet d’introduction de nouvelles technologies..   PB / SALARIES DE MAISON |
| 2/- Le respect de la vie privée du salarié  Le salarié a droit à la protection de l’intimité de sa vie privée sur son lieu de travail:   * Les démarches à effectuer avant d’installer un système de vidéo surveillance : L’employeur ; personne physique ou morale doit:   **\*\*\*\*\***Obtenir **une autorisation préalable de l'Instance Nationale de Protection des Données à Caractère Personnel**  **\*\*\*\*\*** Les moyens de surveillance**, ne peuvent être utilisés que** dans les lieux suivants :   * 1. les lieux ouverts au public et leurs entrées ; * 2. les parkings, les moyens de transport public, les stations, les ports maritimes et les aéroports ; * 3. les lieux de travail collectifs. **Art 70 de la loi.** * **\*\*\*\*\* L**es enregistrements vidéo ne peuvent PAS être **accompagnés d'enregistrements sonores.ART 71 de la loi.** * **\*\*\*\*\*\*** L’employeur doit remplir des formulaires fournis par l’INPDCP ET INDIQUER LE type de matériel, le fournisseur, le descriptif technique,les modalités de stockage des informations...) * **Il est interdit** de donner, à autrui, les enregistrements et vidéo collectés **sauf** dans les cas suivants * 1**. ACCORD d**e la personne concernée , son tuteur ou ses héritiers * 2 . AUTORISATION DE L’INPDCP en cas de salarié Enfant ( ART 28 de la loi) * 3. COMMUNICATION AUX AUTORITES PUBLIQUES * (La communication EST nécessaire pour la constatation, la découverte ou la poursuite d'infractions pénales.) * **\*\*\*\*\*\*L**es enregistrements vidéo **doivent être détruits** lorsqu'ils ne sont plus nécessaires à la réalisation des finalités pour lesquelles ils ont été effectués |
| **3/- L’exigence de proportionnalité**   * Le procédé de surveillance doit être proportionné avec le but recherché. * LE respect du principe de proportionnalité EST souvent mis en avant par l’ INPDCP lorsqu'il s'agit de mettre en œuvre des dispositifs utilisant de la biométrie.   (Systèmes de vidéo surveillance installés en vue de **prévenir le vol** dans les banques ou dans les espaces commerciaux.  Toute installation **clandestine** de cyber surveillance est interdite quand elle permet de :   * - capter, enregistrer ou transmettre, **sans le consentement du salarié ,** des paroles prononcées à titre privé ou confidentiel ;  - Fixer, enregistrer ou transmettre, **sans son consentement** , son image. * -En cas d’utilisation de vidéosurveillance IP (par exemple l'alimentation d'un fichier informatique), un dossier de déclaration préalable est à déposer auprès de L’INPDCP. * L’employeur doit remplir des formulaires fournis par l’INPDCP , relatifs au dispositif d'enregistrement numérique qui sera mis en œuvre (type de matériel et fournisseur, descriptif technique, modalités de stockage des informations...) |

**PARTIE II : (08POINTS)**

**Répondre à la question suivante**:

« L’usage des technologies de l’information et de la communication essentiellement Internet, a **entraîné l’abolition des limites** **entre la sphère publique et la sphère privée dans le monde numérique et a multiplié** les atteintes à la vie privée des individus leur causant des **dommages matériaux et moraux. »**

**1 :** Qu’est ce qu’un Internaut**e** **?** La communication sur Internet présente-elle des risques quand à la vie privée de l’internaute ?

Surfer sur la toile est devenu an acte banal **( se renseigner, communiquer, acheter ou vendre , faire des recherches etc….. )**

|  |  |
| --- | --- |
| **1 :** Qu’est ce qu’un Internaut**e** | Un **internaute** est un [utilisateur](https://fr.wikipedia.org/wiki/Utilisateur_(informatique)) du réseau [Internet](https://fr.wikipedia.org/wiki/Internet).  Il désigne donc une personne PHYSIQUE OU MORALE ; qui utilise un [navigateur Web](https://fr.wikipedia.org/wiki/Navigateur_Web) pour visiter des [sites web](https://fr.wikipedia.org/wiki/Site_web) et, par extension, toute personne employant une application informatique permettant d'obtenir sur [Internet](https://fr.wikipedia.org/wiki/Internet) des informations, ou de l'interactivité avec d'autres personnes : [courrier électronique](https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique), [chat](https://fr.wikipedia.org/wiki/Chat_(informatique)), transfert de fichiers par [FTP](https://fr.wikipedia.org/wiki/File_Transfer_Protocol) ou [peer to peer](https://fr.wikipedia.org/wiki/Peer_to_peer), forums de discussions sur [Usenet](https://fr.wikipedia.org/wiki/Usenet), etc.  Un [**mobinaute**](https://fr.wikipedia.org/wiki/Mobinaute) est un utilisateur d’Internet sur [téléphone mobile](https://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9phone_mobile). |
| La communication sur internet et les risques quand à la vie privée de l’internaute **?** | **INTERNAUTE MAJEUR :**  **Usurpation d’identité :**  1/ Tous les actes de communication laissent des traces personnelles.  Ces traces sont utilisées **avec ou sans le consentement** des personnes et servent à élaborer des statistiques ciblées par les géants d’internet appelés aujourd’hui les **« GAFA », (Consentement extorqué par le téléchargement d’application OFFERT SOIT DISANT GRATUITEMENT)** Ces données **sont traitées; et « volées » pour être vendues par paquet.**  2/ Les données PERSONNELLES **peuvent simplement être piratées.**  \* Soit par le vol d’identifiants (nom d’utilisateur et mot de passe)  \* Soit par la création **d’un faux profil**  Le coupable est peut être condamné à payer une amende au trésor public et **risquer jusqu’à** un an de prison.  Les dispositions juridiques relatives à la protection de la correspondance classique ;sont applicables à la **correspondance numérique** .  \*La divulgation **non autorisée** par l’émetteur du contenu d’un courriel est une violation au secret de correspondance.  \*Le piratage de la boite mail (Envoi de virus et l’appareil informatique devient sous le contrôle exclusif du hacker).   * **Le portage des données par le PIRATAGE DES comptes mails** S ’opère par l’usage De :   **1.Logiciels espions** dont le téléchargement est gratuit  **2.Des cookies**  **3.Le black box** connecté au router d’un espace public pour scanner le contenu intégral des appareils ou ordinateurs connectés) **cybercafés**  **La géolocalisation**:Elle **R**epresente une menace constante à la vie privée des invidus.  **EN FAIT Les cameras et micros des appareils informatiques sont la porte d’entrée des pirates!!!! (tel ; empreintes digitales; commande de la voiture avec application téléchargée)**  **INTERNAUTE MINEUR :**  UN MINEUR Est « Toute personne humaine âgée au moins de dix-huit ans ».  La loi 2004\_63 du 27/07/2004, relative à la protection des données à caractère personnel : prévoit des incriminations spécifiques destinées à protéger « le mineur »lorsqu’il est **sujet** ou **destinataire de l’information.**  **LES FACTEURS DE RISQUES :**  Expansion de l’usage de l’internet dans le secteur de l’enseignement et de la recherche  « **portails éducatifs** »  -Création de sites par les élèves eux-mêmes à titre expérimental ou éducatif ( comptes : Facebook; youtube; instagram, et autres)   * \_ -Le mineur voit Internet comme un MIRACLE de la technologie , il a tout à sa disposition ( jeux, recherche, voyage, shopping, forums, chat,…) * Le mineur est exposé, chaque jour à des sites à contenu violent, agressif (crash d’avions, catastrophes, assassinats, terrorisme, sites sexuels, apologie du suicide \_\_ Cyber intimidation , cyber chantage : * \_ Jeux vidéos dangereux, provoquant chez les jeunes des crises d’épilepsie et les repoussent à commettre des tragédies .   Le « MASSACRE LITTLETON( en USA) »   * Le risque venant de **l’internaute caché** : le mineur est une proie largement facile pour, les pédophiles et les intégristes) En effet et d’après « **le Congrès des praticiens de la justice des mineurs »** tenu à Athènes, le 03/03/2003 ,   INTERNET est le **paradis de la pédopornographie**, et de l’exploitation sexuelle des mineurs à des fins commerciales ; de nouvelles formes de promotion du tourisme sexuel caché, **informel** donc plus difficile à faire disparaître.  \_ Le mineur est aussi confronté à de fausses informations , rumeurs propagées à une vitesse vertigineuse,à un nombre indéfini d’internautes |