PROJET SAS

Problématique de l'entreprise AutoConcept

RIQUET ANTIGNY MAXIME
ROBYNS QUENTIN
SICAUD THOMAS
WEBER RAPHAEL

GMSI 2017/2018

SOMMAIRE

1. L'ENTREPRISE THRAQ'MI

1.1 PRESENTATION DE L'ENTREPRISE THRAQ'MI

Depuis plus de 20 ans, l'entreprise Thraq'mi contribue au bien-être des utilisateurs d'outils informatiques. Elle se compose de onze employés dont un commercial et un apprenti.

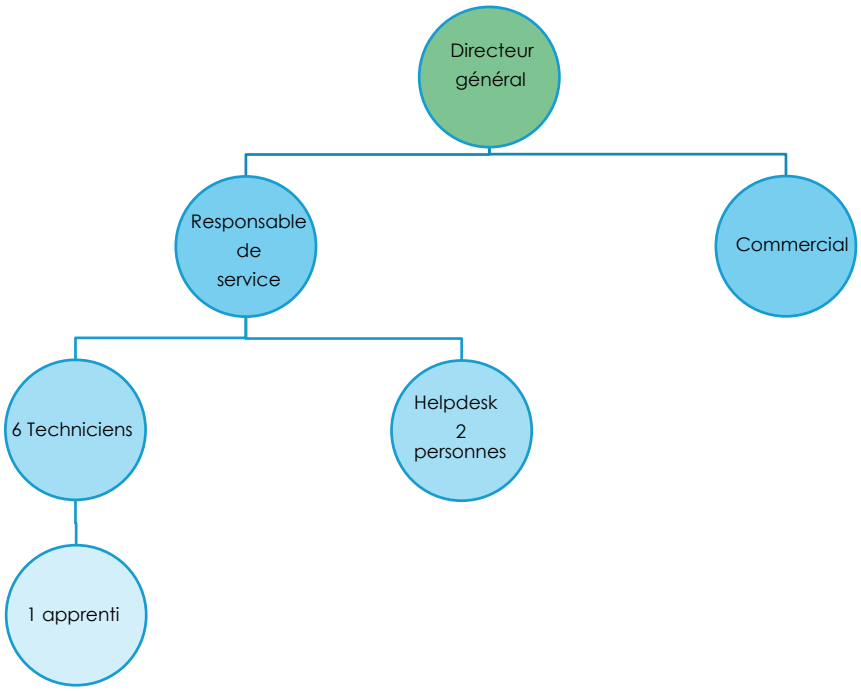
Dans le cadre de la prestation informatique, et au-delà de la maintenance qui est son cœur de métier, notre entreprise a développé un ensemble de garanties et de services pour accompagner ses clients.

Pour répondre à leurs besoins spécifiques, notre entreprise couvre aujourd'hui de nombreux domaines du secteur informatique : Sauvegarde, prévention, vente, maintenance et assistance.

Cette offre globale est adaptée aux différents acteurs qui composent la filière informatique. Elle s'ajuste aux besoins des très petites entreprises comme des grands groupes. Enfin, elle répond également aux attentes des particuliers.

Notre entreprise pense à l'environnement, en effet, nous effectuons un tri de nos DEEE (Déchet d'Equipement Electrique et Electronique).

1.2 ORGANIGRAMME DE L'ENTREPRISE



Notre organisation est la suivante : Un directeur général, qui est le fondateur de l'entreprise, travail sur la gestion des employés, notamment le commercial et le responsable de service.

Il s'occupe également des formalités et de la vie de l'entreprise.

Le responsable de service gère les plannings de chaque technicien ainsi que du recrutement de nouvelles recrues. Les deux employés de l'helpdesk reçoivent les appels, créent des tickets et les transmettent aux techniciens. Les six techniciens réceptionnent les tickets envoyés par l'helpdesk et amènent une résolution à ces derniers. Le commercial s'occupe des devis, de vendre du matériel et de faire connaitre l'entreprise.

L'apprenti assiste les techniciens.

1.3 INFORMATIONS CLE DE L'ENTREPRISE THRAQ'MI :

- Adresse : Route de Bordeaux, 16400 La Couronne.
- Activités principales de l'entreprise : Maintenance, gestion de parc informatique.
- Partenaire : Cisco, Microsoft, HPE, ESET.
- Fournisseur pro : PICATA.
- Capital : 17 500 €.
- Chiffre d'affaire en 2016 : 835 000 €.
- Effectif : 7 employés et 1 stagiaire.
- Statut juridique : SARL (Société à Responsabilité Limitée).
- Horaires : Du lundi au vendredi 8h00 – 12h30 et 14h – 18h.
  Astreinte le Samedi et le dimanche.

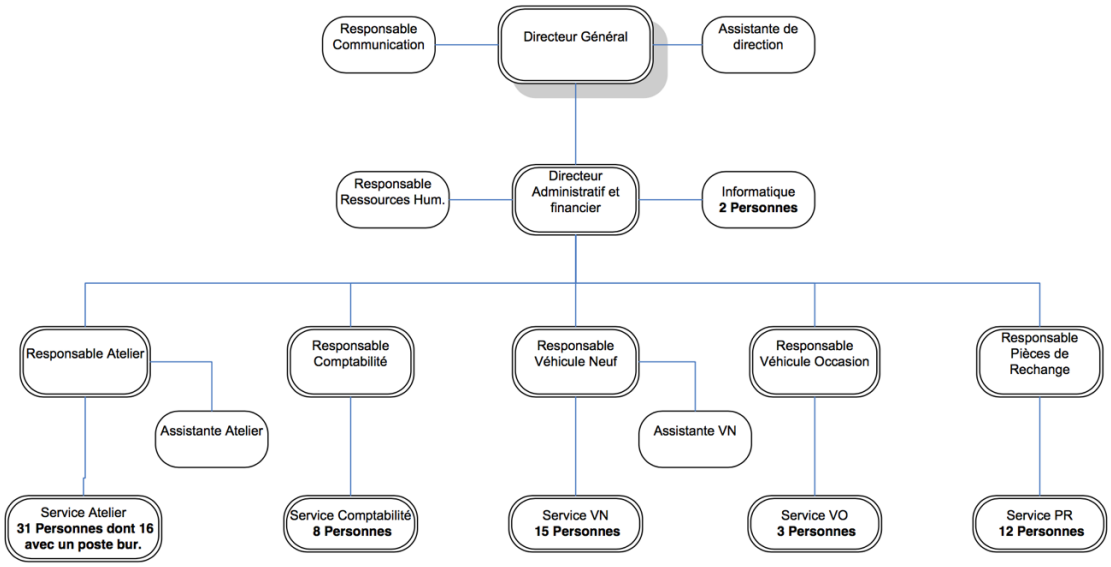
2. LE CLIENT : AUTO CONCEPT

2.1 STATUTS D'AUTO CONCEPT ET INFORMATIONS

Adresse : Route de Bordeaux, 16400 La Couronne.
Activités principales de l'entreprise : Vente, réparation et dépannage de véhicule automobile.

Chiffre d'affaire en 2016 : 5 millions €.
Effectif : 83 personnes.
Statut juridique : SAS (Société par actions simplifiée).

2.2 ORGANIGRAMME DE L'ENTREPRISE



2.3.1PRESENTATION D'AUTO CONCEPT

La société est un concessionnaire automobile équipé d'un parc informatique de 70 à 80 postes.

2.3.2 ORGANISATION DE L'ENTREPRISE

Les 83 salariés de la société sont répartis dans différents services :

- Directoire.
- Service atelier.
- Service comptabilité.
- Service véhicule neuf.
- Service véhicule occasion.
- Service de pièce de rechange.

2.3.3 RAPPEL DES BESOINS D'AUTO CONCEPT

L'entreprise fait le souhait d'externaliser leur maintenance informatique.

L'entreprise a reçu plusieurs plaintes des utilisateurs sur le service informatique :

- Les délais d'intervention des techniciens et le retour de l'équipement du SAV.
- Manque d'explication sur les interventions, ou trop technique.
- L'attitude des informaticiens (tenu vestimentaires négligée, retard, etc…).
- La résolution des problèmes qui reviennent quelque temps après.
- Plusieurs problèmes notifiés aux techniciens sans réponses.
- Ne pas avoir de date de retour des produits envoyé au SAV.
- Message intempestif de « version Windows pirate ».
- Problème de sécurité informatique.
- Non présence d'une charte informatique.
- Manque de matériel de remplacement identique.

« Auto Concept » a également besoin de voir son service continuer même en cas de panne.

Le crash disque d'un poste d'un commercial a causé une perte de 80 000 euros.

La lenteur de certains postes pose également un problème.

3. NOTRE PROPOSITION

Afin de répondre au mieux aux besoins de l'entreprise Auto Concept, nous avons travaillé à l'élaboration des solutions les plus adaptées que nous vous présentons ci-dessous.

Nous proposons d'instaurer une charte informatique, afin de définir les conditions d'utilisation des moyens informatique mis à disposition des salariés par leur employeur. Dans un premier temps, les droits et obligations qu'à l'employeur, et, dans un second temps, la charte informatique que nous avons créée afin d'informer les employés de l'entreprise. Une solution de filtrage de contenu doit également être mise en place, c'est pourquoi nous présentons l'aspect légal de cette solution ainsi que son utilité. Afin de répondre aux besoins de l'entreprise concernant la prévention des pertes de données, nous proposons la mise en place d'un système de sauvegarde des données. Un devis concernant le matériel à changer et à installer est joint, afin que l'entreprise Auto Concept se projette au niveau de son budget. Ce matériel peut être protégé grâce à un contrat de maintenance que nous proposons.

Concernant les prestations de Thraq'mi, nous avons joint une charte de qualité service afin de communiquer nos engagements à l'entreprise Auto Concept.

3.1 LA CHARTE INFORMATIQUE

Quels sont les droits et les obligations ?

La mise en place d'une charte informatique ou charte internet est obligatoire uniquement dans le cas où l'entreprise collecte des données à caractère personnel sur ses salariés (log de connexion, archivage de messagerie, surf internet, etc.)

Ainsi, la CNIL (Commission Nationale Informatique et Libertés) recommande l'adoption d'une charte internet dans l'entreprise si elle a pour objectif de *« sensibiliser les salariés aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de* l'entreprise. ».

Il est important de préciser qu'une charte informatique se doit de ne pas « *porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* ».

Nécessité d'informer les salariés :

Les salariés doivent être informés des dispositifs mis en place et des modalités de contrôle de l'utilisation d'internet :

Le comité d'entreprise doit avoir été consulté et informé (**article L2323-32 du code du travail**).

Les salariés doivent être informés, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées. Une durée de

conservation de l'ordre de six mois est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet.

Comment déclarer ?

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste, le traitement ainsi mis en œuvre doit être déclaré à la CNIL (déclaration normale) sauf si un correspondant informatique et libertés a été désigné, auquel cas aucune déclaration n'est nécessaire.

L'information préalable, condition de transparence :

L'obligation d'information préalable résulte de **l'article L.121-8 du code du travail**. « *Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.* ».

La discussion collective :

L'article L.432-2-1 prescrit que le comité d'entreprise doit être « *informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.* ». Il résulte clairement des textes qu'une information individuelle des salariés ou agents publics ne saurait dispenser les responsables concernés de l'étape de la discussion collective, institutionnellement organisée, avec les représentants élus du personnel.

Première idée fausse : l'ordinateur personnel mis à la disposition des utilisateurs sur leur lieu de travail serait, en tant que tel, protégé par la loi "informatique et libertés" et relèverait de la vie privée du salarié.

Il n'en est rien. Un ordinateur mis à la disposition d'un salarié ou d'un agent public dans le cadre de la relation de travail est la propriété de l'entreprise ou de l'administration et ne peut comporter que subsidiairement des informations relevant de l'intimité de la vie privée.

Deuxième idée fausse : une information préalable des personnels suffirait.

De nombreuses entreprises imaginent qu'une information préalable des salariés suffirait à se prémunir de tout problème et à autoriser l'emploi de tous les modes de surveillance et de contrôle. Une telle manière de procéder n'est pas suffisante dès lors que les finalités seraient mal définies ou mal comprises.

L'avis de la CNIL sur le contrôle de l'employeur :

La CNIL, dans son dernier rapport sur la cyber surveillance, préconise un contrôle transparent. Cette transparence est respectée par, d'une part, une information préalable portée au salarié, et, d'autre part, l'avis du Comité d'entreprise sur la pertinence et la proportionnalité du contrôle face au respect de la vie privée du salarié.

L'information peut être faite par note de service. Toutefois, toute constatation nécessite la présence du salarié et, en son absence, la présence d'institutions représentatives du personnel.

En toute hypothèse, il appartiendra à l'employeur de prouver qui est l'expéditeur du message litigieux.

Enfin, le dispositif de contrôle individuel s'analyse en un traitement automatisé d'informations nominatives qui doit être déclaré à la CNIL.

La CNIL recommande une durée de conservation maximale de ces informations de six mois.

Elle rappelle également que la finalité ne doit pas être détournée à des fins autres que celles liées au bon fonctionnement et à la sécurité.

3.2 LES DISPOSITIONS LEGALES CONCERNANT LA MISE EN PLACE D'UNE SOLUTION DE FILTRAGE DE CONTENUS EN ENTREPRISE.

De nos jours, pour une entreprise, il est courant, voir presque nécessaire, de mettre en place une solution de filtrage de contenus. En effet, les acteurs de l'entreprise, notamment le ou les dirigeants ainsi que le personnel informatique, sont responsables des actions des employés de l'entreprise sur leur porte informatique.

Le ou les dirigeants de l'entreprise sont responsable pénalement comme le stipule **l'article 121-1 et 121-2 du code pénal**.

121-2 : *« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement […] des infractions commises, pour leur compte, par les organes dirigeants ou représentants »*.

Selon **l'article 121-2** ainsi que **l'article 121-3 du code pénal**, le personnel informatique peut également avoir une part de responsabilité dans la défaillance des systèmes mis en place. La direction informatique peut être poursuivie pour négligence car c'est elle qui doit mettre en place un système de filtrage de contenu afin de ne plus rendre possible certaines actions frauduleuses qui pourraient être faites par un employé. Toutefois, si une action frauduleuse venait à être réalisée, la responsabilité des personnes citées précédemment n'exclut pas la responsabilité de la personne ayant commis la fraude.

121-2 : *« La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits »*.

121-3 *: « les personnes physiques qui n'ont pas causé directement le dommage, mais qui ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter, sont responsables pénalement s'il est établi qu'elles ont, soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'elles ne pouvaient ignorer. »*

La mise en place d'un système de filtrage dans une entreprise est donc presque indispensable. On retrouve dans certains textes de loi, le droit pour une entreprise

d'appliquer ce genre de filtrage afin de se protéger. On peut y retrouver le mot « **filtrage** » à plusieurs reprises.

- Dans la **loi n°2009-669 du 12 juin 2009**, qui est la loi dites Hadopi, qui concerne la diffusion ainsi que la protection de la création sur internet.

Loi n°2009-669 Chapitre 1er, article 5, sous-section 2 : « *Elle évalue, en outre, les expérimentations conduites dans le domaine des technologies de reconnaissance des contenus et de **filtrage** par les concepteurs de ces technologies, les titulaires de droits sur les œuvres et objets protégés et les personnes dont l'activité est d'offrir un service de communication au public en ligne.* »

- Dans un rapport Hadopi paru en février 2013, rapport sur les moyens de lutte contre le streaming et les téléchargements direct illicites. Il est stipulé qu'un paramétrage limitant certains accès peuvent être mis en place.

« *Les logiciels, qui permettent à l'internaute le passage d'un serveur à un autre ou l'accès aux différentes ressources documentaires sur le Web, pourraient également jouer un rôle. D'un point de vue technique, la mesure de **filtrage** pourrait passer ou non par l'installation d'un module chez l'utilisateur (plug-in). L'utilisateur pourrait alors changer de logiciel ou ne pas installer le module, ce qui limiterait l'efficacité de cette solution. L'efficacité d'une mesure de **filtrage** mise en place au niveau du système d'exploitation de l'ordinateur pourrait à cet égard apparaître plus efficace, car inhérente à l'ordinateur. Les acteurs à mobiliser seraient par ailleurs moins nombreux à solliciter mais également étrangers, ce qui pose la question de la contribution volontaire des acteurs industriels aux efforts de régulation française.* »

« *[…] aux modalités de **filtrage** mises en œuvre.* »

- **L'arrêté du 27 juin 1989**, relatif à l'enrichissement du vocabulaire de l'informatique, donne une définition du filtrage. Il définit celui-ci comme étant une « *Mise en correspondance de formes selon un ensemble prédéfinit de règles ou de critères.* »

Egalement au niveau européen, le mot « filtrage » ou la notion de filtrer les données apparait dans de nombreux textes. Dans le texte de la **décision 276/1999/CE du 25 janvier 1999 du Parlement européen et du Conseil**, adoptant un plan d'action communautaire qui s'étend sur plusieurs années, et visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux. Il est notamment évoqué que le filtrage est un moyen de rendre internet plus sûr.

Dans **l'article 6 de la loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique, la notion de filtrage est évoquée dans la phrase : « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.* »

Le filtrage est évoqué dans plusieurs textes français, mais aussi au niveau de l'union européenne, explicitement comme plus implicitement. Il est donc légitime pour une

entreprise de mettre en place une solution de filtrage de contenus puisque la législation le permet.

En effet, la législation permet de mettre en place ce type de dispositif, mais impose également certaines obligations qui induisent à installer un système de filtrage de contenu.

- **L'article L336-3 du code de la propriété intellectuelle** stipule que « *La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.* »
- La **loi n° 2010-476 du 12 mai 2010** relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, impose un contrôle des accès aux plateformes de jeux d'argent en ligne.
- **L'article 227-24 du code pénal**, pour la protection des mineurs, oblige les entreprises à filtrer les informations que peuvent diffuser leurs employés. « *Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.* »

L'entreprise se doit de stocker un historique des évènements passés, ces fichiers sont appelés logs. Ils sont nominatifs et sont consultés en cas de besoin, afin d'identifier l'origine d'un problème. L'entreprise est tenue de conserver les logs pour une durée d'un an comme le stipule différents textes.

- **L'article 1 du décret n° 2006-358 du 24 mars 2006** relatif à la conservation des données des communications électroniques fixe « la durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement. ».
- **L'article R10-13 du Code des postes et des communications électroniques**, qui impose un stockage de ces fichiers afin d'identifier la source d'un problème.
- **La loi 2006-64 du 23 janvier 2006** relative à la lutte contre le terrorisme « *impose aux opérateurs télécoms, aux fournisseurs d'accès (FAI), mais aussi à tout établissement public proposant un accès internet, comme les cybercafés, de conserver les données de connexion (logs) pendant un an.* »

L'entreprise doit être en mesure de fournir ces logs en cas de demande. Si l'entreprise n'a pas respecté ces obligations et n'est pas en mesure de fournir les informations, d'après **l'article L39-3 du Code des postes et des communications électroniques**, la peine est « *d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de*

communications électroniques ou ses agents […] de ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi. »

Un tel dispositif peut nécessiter un enregistrement auprès de la commission nationale de l'informatique et des libertés (CNIL) qui, d'après la **loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 11** : « *veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.* » *Elle sert également « à informer toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations.* »

3.3 UN REGLEMENT QUI DOIT ETRE ACCESSIBLE A TOUS

La charte est un document voué à être diffusé auprès de tous les utilisateurs des outils informatiques, quels qu'ils soient. Il convient de déployer la charte comme un règlement intérieur.

Les salariés doivent être informés, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées. Une durée de conservation de l'ordre de six mois est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet. (La loi fixe une durée maximum d'un an).

Il s'agit donc de soumettre ce document aux instances syndicales ou représentant le personnel, puis de le diffuser auprès des utilisateurs, individuellement ou collectivement.

Dans le cadre d'une petite structure, il peut être intéressant de l'évoquer lors d'une réunion d'entreprise pour échanger autour du sujet.

Enfin, dans le cadre des entreprises et des administrations employant des agents de droit privé dépendant du code du travail, il convient d'effectuer des démarches complémentaires prévues par les **articles R1321-2 et R1321-4 du code du travail** :

- Déposer la charte au Greffe du Conseil des prud'hommes.
- Transmettre la charte à l'Inspection du Travail en double exemplaire.
- Communiquer la charte à la CNIL.

CHARTE INFORMATIQUE

PREAMBULE :

L'entreprise met en œuvre un système d'informations et de communication nécessaire à son activité, comprenant notamment un réseau informatique.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.

1. RESPECT DE LA DEONTOLOGIE INFORMATIQUE :

Tout utilisateur est responsable de l'usage qu'il fait des ressources informatiques. Il doit particulièrement veiller à user raisonnablement de toutes les ressources partagées auxquelles il accède (puissance de calcul, espace disque, bande passante du réseau...). Tout utilisateur s'engage à respecter les règles de la charte informatique et notamment à ne pas effectuer des opérations ayant pour but :

- De masquer sa véritable identité.
- D'usurper l'identité d'autrui.
- De s'approprier le mot de passe d'un autre utilisateur.
- D'utiliser ou de développer des programmes mettant sciemment en cause l'intégrité des systèmes informatique.
- De mettre en place un programme pour contourner les procédures établies dans le but d'augmenter le niveau de sécurité des systèmes.
- D'installer et d'utiliser un logiciel à des fins non conformes aux missions de l'entreprise.
- De ne pas respecter les règles d'accès aux salles contenant le matériel informatique.
- D'utiliser des comptes autres que ceux auxquels il a légitimement accès.
- D'utiliser un poste de travail ou toute autre ressource informatique sans une autorisation explicite de la personne à qui elle est attribuée.
- D'accéder aux données d'autrui sans l'accord exprès des détenteurs, même lorsque ces données ne sont pas explicitement protégées.

2. LE RESPECT DE L'INTEGRITE D'UN SYSTEME INFORMATIQUE :

L'utilisateur s'engage à ne pas effectuer des opérations pouvant nuire au bon fonctionnement du réseau, à l'intégrité de l'outil informatique et aux relations internes et externes de l'établissement. La simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement du dit système. Si de telles altérations sont constatées, les sanctions prévues sont doublées (**article 323-1 du nouveau code pénal)**. Les actes consistant à empêcher un système de fonctionner, par exemple par l'introduction de « *virus* », sont visés par **l'article 323-2 du nouveau code pénal**. L'introduction ou la modification frauduleuse de données font l'objet des **articles 323-3 et 323-4 du nouveau code pénal**. Il est important de noter que la simple tentative ainsi que la participation à une entente établie en vue de la préparation d'une infraction est punie des peines prévues pour l'infraction elle-même.

3. ATTEINTES AUX DROITS DE LA PERSONNE :

La **loi 92-684 du 22 juillet 1992** protège tout individu contre tout usage abusif ou malveillant, d'informations le concernant et figurant dans un fichier quelconque. Elle prévoit en particulier que :

- L'entreprise doit déclarer aux préalables auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), tout fichier contenant des informations personnelles.
- Toute personne figurant dans un tel fichier doit être informée de l'existence de ce fichier, sa finalité, l'existence d'un droit d'accès et de rectifications, et des modalités d'utilisations de celui-ci, dès la collecte des informations la concernant.

4. ACCES AU COMPTE ET SECURITE :

En cas d'oubli d'une mise en veille d'un poste, un système de veille automatique est programmé sur les postes, pour éviter un oubli de déconnexion.

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur. Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Un login et un mot de passe sont confiés à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit pas les communiquer.

Chaque mot de passe doit impérativement être modifié tous les 90 jours. Un mot de passe doit, pour être efficace, être composé d'au moins 8 caractères alphanumériques. Il ne doit pas contenir le nom et/ou prénom de l'utilisateur ou son numéro de téléphone. Ne doit pas être écrit sur un document et communiqué à un tiers.

Chaque utilisateur est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisées.

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte. Chaque personne de l'entreprise doit avoir un compte avec un login et un mot de passe qu'ils choisissent, où ils ont uniquement accès à leurs infos.

4. PROTECTION DES DONNEES A CARACTERE PERSONNEL :

La **loi n°78-17 du 6 janvier 1978 modifiée en 2004** relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel, le fait de collecter des données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

5. LES REGLES DE SECURITE :

- Signaler au service informatique interne de toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propres à la société.
- Verrouiller son ordinateur dès que l'employé quitte son poste de travail.

- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.

- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par l'entreprise. En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information sans l'accord préalable du service informatique interne.

5. INTERNET :

- Pas de transmission d'information professionnelles non autorisées sur le web.

- A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information afin d'assurer la sécurité des données. Il s'agit du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles.

- Une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

- Interdiction de télécharger et d'installer des applications non autorisées (MSN, Ccleaner, etc)

6. MESSAGERIE ELECTRONIQUE :

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de l'entreprise.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Thraq'mi s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'agent.

7. DISPOSITIONS LEGALES CONCERNANT LA SOLUTION DE FILTRAGE DE CONTENUS EN ENTREPRISE :

Selon les **articles 121-2 et 121-3 du code pénal**, le personnel informatique peut avoir une part de responsabilité dans la défaillance des systèmes mis en place.

La **loi n°2009-669 du 12 juin 2009** (loi Hadopi) concerne la diffusion ainsi que la protection de la création sur internet. Des paramétrages limitant certains accès peuvent être mis en place.

Obligations d'installation de filtrage des jeux d'argent et de hasard en ligne, impose un contrôle des accès aux plateformes de jeux d'argent en ligne. Pour la protection des mineurs, oblige les entreprises à filtrer les informations que peuvent diffuser leurs employés.

L'entreprise se doit de stocker un historique des évènements passés, ils sont nominatifs et sont consultés en cas de besoin, afin d'identifier l'origine d'un problème.

L'entreprise doit être en mesure de fournir ces logs en cas de demande.

5. SYSTEME DE SAUVEGARDE :

5.1 LA METHODE QUE NOUS SOUHAITONS UTILISER : LE 3-2-1.

Cela consiste à conserver 3 copies de vos fichiers. (NAS, serveur de stockage, bande magnétique).

Ensuite stocker les sauvegardes sur au moins deux types de stockages différents. Dans notre cas nous vous proposons sur un support magnétique et un support sur disque.

Enfin gardez une copie des données hors site grâce au serveur de stockage que nous vous proposons.

5.2 POURQUOI NOUS UTILISONS LA TECHNIQUE DU 3-2-1 ?

Pour éviter tout risque de perte de données en cas d'incident (destruction, vol, inondation, incendie…) il est recommandé d'utiliser la règle du 3-2-1 cela consiste à avoir 3 copies sur au moins deux types de support distincts dont une à distance.

Nous vous proposons 3 méthodes de sauvegarde :

Il est évident que plus vous faites de copies de vos données, moins vous avez de risques de tout perdre.

Faire une seule sauvegarde est viable mais tout simplement pas assez. C'est pour cela que nous proposons plusieurs supports de sauvegarde :

- Une sauvegarde sur bande magnétique.
- Une sauvegarde sur le NAS.
- Une sauvegarde sur nos serveurs de stockage.

Il ne sert à rien de faire plusieurs copies sur le même support car en cas de crash du système, toutes les sauvegardes seront perdues (même les systèmes RAID peuvent s'avérer délicats à remonter).

5.3 POURQUOI FAIRE UNE SAUVEGARDE A DISTANCE ?

Le risque de perte de données peut aussi être physique (incendie, dégât des eaux, vol). Conserver une copie externalisée permet de se prémunir contre ce type de dommage. Entreposer un disque USB à l'extérieur, le ramener par exemple à la maison est une solution, mais le facteur humain (oubli, vacances…) introduit le risque de perte de ce disque et de fuite de données si quelqu'un de mal intentionné le trouve. Il vaut mieux se baser sur des solutions de backup automatisées via internet (Cloud). Pour cette copie, le cryptage des données est nécessaire.

5.4 POURQUOI FAIRE UNE SAUVEGARDE SUR BANDE MAGNETIQUE ?

La bande magnétique va surtout servir pour l'archivage des fichiers. C'est un support externalisé qui se retrouvera en banque, assurant la conservation des documents ainsi que leur restitution en cas de contrôle ou lors d'un litige.

5.5 POURQUOI FAIRE UNE SAUVEGARDE SUR NAS ?

Ils sont une solution simple et adaptée au stockage, à la sauvegarde et au partage de données entre plusieurs ordinateurs. Il vous est même possible d'accéder à vos données depuis l'extérieur.

CHARTE QUALITE SERVICE

LA CONTINUITE DE SERVICE EN CAS DE PANNE :

- Un « Helpdesk » disponible de 8h à 18h du lundi au vendredi ou 7j/7 selon le contrat.
- Dépannage sur site en fonction du type d'intervention à effectuer.

LA RELATION CLIENTELE :

- Nous sommes toujours à votre disposition et à votre écoute pour vos problèmes.
- Respect de vos données confidentielles.
- Suivi constant de votre problème grâce à des tickets pour le SAV.
- Communication préalable de chaque durée d'intervention.
- Explication systématique sur toutes les interventions réalisées.

QUALITE DE LA PRESTATION :

- Une équipe de technicien compétant.
- Sécurité et productivité.
- Respect des délais annoncés au préalable.
- Mettre en place une solution adaptée pour que le problème n'apparaisse plus.
- Procédure de suivi de la qualité des interventions, par un système de fiche remplie par le client.

GARANTIE :

- Toute ré-intervention est gratuite 30 jours pour une panne identique à la première.
- Notre technicien vérifiera avec vous que la panne pour laquelle il est intervenu soit bien résolue.
- Proposition de formation pour améliorer vos différents services.
- Respects des réglementations en vigueur et du code du travail.
- Un contrôle qualité est effectué tous les trimestres chez nos clients.

7. DEVIS MATERIEL A REMPLACER

HP 280 G2 (V7Q80EA)

- Design compact et élégant
- Processeur Intel Core i3-6100 (Dual-Core 3.7 GHz - Cache 3 Mo)
- 4 Go de mémoire vive DDR4 2133 MHz (1x 4 Go - 2 slots au total - maximum 32 Go)
- Disque dur de 500 Go avec 7200 RPM (rotations par minute)
- Graveur DVD multiformats ultra-plat
- 2 ports USB 3.0 à l'arrière, pour des vitesses de transfert haut débit
- Connexion réseau Gigabit Ethernet
- Clavier + souris USB fournis
- Windows 10 Professionnel 64 bits
- Garantie constructeur : 1 an

FUJITSU PRIMERGY TX1330 M2 (VFY:T1332SC040IN)

- Processeur Intel Xeon E3-1220 v5 (Quad-Core 3 GHz / 3.5 GHz Turbo - cache 8 Mo)
- 8 Go de mémoire DDR4 ECC (1x 8 Go - 4 slots - maximum 64 Go au total)
- 2 disques durs de 1 To (3.5" SATA 7200 RPM)
- 4 baies pour disques durs 3.5 pouces SATA (2 occupées)
- Graveur DVD intégré
- 2 slots PCIe 3.0 x8 (max 240 mm) + 1 slot PCIe 3.0 x4 (max 167 mm)
- Alimentation hot-plug de 450 Watts certifiée 80PLUS Platinum (câble secteur non fourni)
- Système d'exploitation : non-fourni
- Garantie constructeur : 1 an (intervention sur site)
- Windows serveur 2016

TANDBERG LTO-6 HH - LECTEUR DE BANDES MAGNETIQUES - LTO ULTRIUM - SAS-2

- Type de périphérique : Lecteur de bandes magnétiques
- Data Transfer Rate: LTO Ultrium 6
- Type de châssis : Externe
- Type d'interface : SAS-2
- Fonctions clés : Chiffrement
- Stockage amovible : LTO Ultrium
- Capacité de l'unité de stockage amovible : 2.5 To (natif) / 6.25 To (compressé)
- Cartouches de bande prises en charge (lecture et écriture) : Ultrium 6, Ultrium 5
- Licence Type : 160 Mo/s (576 Gbph)
- Débit de transfert de données (compressé) : 400 Mo/s (1.44 Toph)
- Alimentation : CA 120/230 V (50/60 Hz)
- Garantie du fabricant : 3 ans de garantie

TANDBERG - LTO ULTRIUM X 1 - 1.5 TO - SUPPORT DE STOCKAGE

- Type Support de stockage : LTO Ultrium
- Cartouche de bande : Ultrium 5
- Optical Storage : 1
- Display 1.5 To
- Capacité compressée: 3 To
- Garantie du fabricant : Garantie à vie

QNAP TS-453A - SERVEUR NAS - 3 TO

- Type de périphérique : Serveur NAS
- Connectivité hôte : Gigabit Ethernet
- Capacité totale de stockage : 3 To
- Périphériques installés / Nbre de modules : 4
- Dimensions (LxPxH) : 17.5 cm
- Processeur : Intel N3150 1.6 GHz (Quadri cœur)
- Contrôleur de stockage : RAID SATA 6Gb/s - RAID 5
- Disque dur : 4
- Réseaux : GigE
- Alimentation : CA 120/230 V
- Alimentation redondante : Oui

Thraq'mi

Devis

Thraq'mi

Date : 10/31/2017
N° FACTURE [100]
Date d'expiration : 11/29/2017

À

SAS Auto Concept
Route de Bordeaux
16400 La Couronne
05.46.25.50.16
Réf client [ABC12345]

Qté	N°article	Description	Prix unitaire HT	TVA	Total de la ligne HT
50	3215	Poste HP 280 G2	408.29	20 %	20414.50
1	4587	Serveur Fujitsu PRIMERGY TX1330 M2	1166.63	20 %	1166.63
1	6845	Licence windows SRV 2016	182.03	20 %	182.03
1	1524	Tandberg LTO-6 HH - lecteur de bandes magnétiques	1 585.99	20 %	1585.99
3	6558	Tandberg bande magnétique 1.5 To	70.89	20 %	23.63
1	3214	NAS QNAP TS-453A	782.98	20 %	782.98
50	0013	Prestation horaire d'installation et paramétrage	75.00	20 %	3750.00

Sous-total	27953.02
TVA	5590.60
Total	33543.62

Devis préparé par : _____

Ceci est un devis des biens nommés, soumis aux conditions indiquées ci-dessous : (Décrivez toutes les conditions liées à ces prix et toutes les conditions supplémentaires de l'accord. Il est conseillé d'inclure les dépenses imprévues qui affecteront le devis.)

Pour accepter ce devis, signez ici et renvoyez-le : _____

Merci de votre commande !

8. CONTRAT DE MAINTENANCE

Un technicien reste sur site le temps du contrat, il vérifie le bon fonctionnement du parc informatique.

Si vous rencontrez un problème de virus ou que vous avez simplement besoin d'aide pour installer un logiciel ou un périphérique avant la date du prochain contrôle, ou pour tout autre problème, vous pouvez le contacter chaque fois que vous en avez besoin.

8.1 DESCRIPTIF DU CONTRAT DE MAINTENANCE

Merci de bien lire ces conditions avant de vous engager. Vous devrez les accepter avant de vous abonner à notre contrat de maintenance pour professionnel.

1. DELAIS D'INTERVENTION :

Nous intervenons dans les 4 heures maximum après la réservation de l'intervention ou l'ouverture d'un ticket. Les horaires de dépannage sont du lundi au samedi de 8 heures à 18 heures (les interventions réservées après 17 heures pourront être reportées au lendemain).

2. PAIEMENT ET TARIFS DU CONTRAT DE MAINTENANCE INFORMATIQUE :

Le contrat de maintenance informatique est payable au comptant ou par mois.

Le tarif de ce contrat de maintenance informatique est de 28 000€ si vous réglez au comptant ou 2399€ si vous réglez mensuellement pendant douze mois. Le paiement comptant permet de bénéficier de 788€ d'économie.

Quand le client choisit de régler par mois, le prélèvement de chaque mensualité s'effectue de mois en mois à date fixe, automatiquement (si vous achetez un abonnement le 05/01/2018, le prélèvement s'effectuera le 05 de chaque mois suivant jusqu'à la fin de votre contrat de maintenance informatique).

3. DEVOIR DE SAUVEGARDE ET RESPONSABILITE :

Le client choisit lui-même et sous sa seule responsabilité, les données à sauvegarder et dont la liste établie contradictoirement entre les parties figure en annexe au présent contrat. La sauvegarde individualisée permet une restitution ou une restauration sélective d'une ou plusieurs données sauvegardées sans avoir besoin de procéder à une restauration complète du serveur. Le client est informé qu'en cas d'incident, seules les données figurant sur cette liste pourront être restaurées ou restituées. Si le client souhaite modifier la liste des données sauvegardées, cela fera l'objet d'une annexe complémentaire au présent contrat dûment signé par les deux parties. Il appartient au client de veiller scrupuleusement à ce que la liste des données sauvegardées soit parfaitement conforme aux données sensibles qu'il souhaite sécuriser et donc sauvegarder.

4. DUREE DU CONTRAT DE MAINTENANCE INFORMATIQUE A DISTANCE :

Le présent contrat est conclu pour une durée d'un an.

L'abonnement prendra fin automatiquement à la fin de cette durée.

Vous pourrez vous réabonner d'année en année si vous le souhaitez.

Le contrat de maintenance ne pourra pas être arrêté pendant toute la durée de l'abonnement.

Le non-paiement d'une échéance de la part du client entrainera une suspension de nos services, définitives ou temporaires ainsi que la réclamation de la totalité des échéances restantes jusqu'à la fin de l'abonnement du client.

En cas de résiliation anticipée aux torts du client, toutes les échéances payées par le client resteront définitivement acquises pour la société et les redevances restantes jusqu'à la fin du contrat seront immédiatement exigibles et devront être réglées par le client dans les 30 jours suivant la résiliation.

5. CONFIDENTIALITE :

Toutes les informations et données personnelles concernant le client ou son entreprise et dont la société Thraq'mi pourrait avoir connaissance au moment de ses interventions de dépannage informatique seront et resteront strictement confidentielles sauf si cette divulgation ou communication est imposée par la loi, conformément aux articles **434-1 et 434-3 du code pénal**.

6. CE CONTRAT INCLUT LES PRESTATIONS INFORMATIQUES SUIVANTES :

Une vérification mensuelle des ordinateurs (vérification des navigateurs, suppression des programmes superflus ou malveillants, vérification des pilotes et mises à jour, vérification de l'antivirus).

- Réinstallation du système si besoin.
- La désinfection occasionnelle si vous avez été infecté. Avant la date de la vérification de l'ordinateur.
- Installation de logiciels, programmes, périphériques à volonté.
- Conseils informatiques à volonté.
- Sauvegarde à chaud (protection continue des données) ou à froid. Encryptage des données avant l'envoi vers la sauvegarde distante.
- Gestion complète par le client de sa politique de sauvegarde : horaires différenciés par jour de sauvegarde, quotidien, hebdomadaire, mensuel, annuel…
- Déduplication pour un gain d'espace de sauvegarde, optimisation des flux pour l'envoi des blocs (sauvegarde incrémentielle).

Signature client : Signature prestataire :

9. ANNEXES

9.1 POURQUOI GERER LES DEEE ?

Les DEEE contiennent des matériaux polluants et des matériaux valorisables. La collecte et le traitement des DEEE, permet d'une part de limiter le gaspillage des ressources naturelles nécessaires à leur conception et d'autre part, d'éviter la dissémination de certains polluants.

- Les polluants : les gaz CFC, le plomb, le mercure…
- Les matériaux valorisables : Les métaux ferreux et non-ferreux, les plastiques, le verre, les terres rares…

Se préoccuper de ses DEEE, c'est donc une obligation réglementaire qui permet de réduire sensiblement son empreinte environnementale.

9.2 MEMO INTERNE

MEMO

À : Techniciens DSI

DE : La direction

DATE : Le 15 octobre 2017

OBJET : Conduite à tenir chez un client

Au sein de la Direction des Systèmes d'Information, chaque technicien est tenu d'adopter des règles de conduite lors de ses interventions. Dans ce mémo, vous trouverez toutes les règles et recommandations sur l'attitude à observer.

LA TENUE

Une tenue vestimentaire correcte est exigée. Les techniciens représentent l'entreprise, un aspect visuel décent est donc de mise.

LA COMMUNICATION

La communication avec le client est une chose primordiale.

- Un échange respectueux et cordial est demandé.
- Les explications doivent être vulgarisées, claires et précises. Le technicien doit savoir s'adapter à son interlocuteur.
- Être à l'écoute et calme dans toutes les situations.

LA GESTION DU TEMPS ET DES TACHES A EFFECTUER

Lors d'interventions extérieures, les techniciens doivent être ponctuels. Le respect des dates et horaires défini avec le client est indispensable. Il est donc impératif d'estimer et de communiquer au client le plus précisément possible le temps nécessaire à l'intervention. Une bonne gestion des priorités est également importante sans pour autant négliger les problèmes moins graves.

LE RESPECT DE LA CONFIDENTIALITE ET DES DONNEES PERSONNELLES

Pendant les interventions, les techniciens peuvent avoir accès à des documents confidentiels ou personnels. Il est strictement interdit de consulter et/ou recueillir sciemment ces données. D'après l'article 226-22 du code pénal, la peine pour avoir recueilli et diffusé des informations personnelles peut aller jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende.

LA QUALITE DU TRAVAIL EFFECTUE

Les techniciens doivent être consciencieux dans leur travail. D'un point de vue matériel comme logiciel.

- Lorsqu'une intervention est terminée, il faut s'assurer du bon fonctionnement du travail effectué avant la restitution du matériel au client. Il faut également veiller à restituer le bon matériel au client.
- Utiliser des versions officielles des logiciels.
- Ne pas installer tous les logiciels que le client demande, bien vérifier que le logiciel demandé est autorisé dans son entreprise, et informer la personne des réglementations.

LA GESTION DU MATERIEL

La gestion du matériel est importante. Chez un client, si un matériel doit être envoyé en réparation, il convient de fournir un matériel temporaire le temps de la réparation afin que le client puisse continuer à travailler. Il est également important de prendre un rendez-vous avec le client afin de ne pas prendre le client au dépourvu.

9.3 TEXTES DE LOI

Article 323-1

- Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises 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 cinq ans d'emprisonnement et à 150 000 € d'amende.

Article 323-2

- Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3

- Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € 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 300 000 € d'amende.

Article 323-4

- Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 121-2 du code pénal

- Modifié par Loi n°2004-204 du 9 mars 2004 - art. 54 JORF 10 mars 2004 en vigueur le 31 décembre 2005

Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.

Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.

La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3.

Article 121-3 du code pénal

- Modifié par Loi n°2000-647 du 10 juillet 2000 - art. 1 JORF 11 juillet 2000

Il n'y a point de crime ou de délit sans intention de le commettre.

Toutefois, lorsque la loi le prévoit, il y a délit en cas de mise en danger délibérée de la personne d'autrui.

Il y a également délit, lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, s'il est établi que l'auteur des faits n'a pas accompli les diligences normales compte tenu, le cas échéant, de la nature de ses missions ou de ses fonctions, de ses compétences ainsi que du pouvoir et des moyens dont il disposait.

Dans le cas prévu par l'alinéa qui précède, les personnes physiques qui n'ont pas causé directement le dommage, mais qui ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter, sont responsables pénalement s'il est établi qu'elles ont, soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'elles ne pouvaient ignorer.

Il n'y a point de contravention en cas de force majeure.

LOI n° 2009-669 du 12 juin 2009

Article 5

Sous-section 2

Mission d'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite d'œuvres et d'objets protégés par un droit d'auteur ou par un droit voisin sur les réseaux de communications électroniques.
Art.L. 331-23.-Au titre de sa mission d'encouragement au développement de l'offre légale, qu'elle soit ou non commerciale, et d'observation de l'utilisation, qu'elle soit licite ou illicite, des œuvres et des objets protégés par un droit d'auteur ou par un droit voisin sur les réseaux de communications électroniques, la Haute Autorité publie chaque année des indicateurs dont la liste est fixée par décret. Elle rend compte du développement de l'offre légale dans le rapport mentionné à l'article L. 331-14.
Dans des conditions fixées par décret en Conseil d'Etat, la Haute Autorité attribue aux offres proposées par des personnes dont l'activité est d'offrir un service de communication au public en ligne un label permettant aux usagers de ce service d'identifier clairement le caractère légal de ces offres. Cette labellisation est revue périodiquement.
« La Haute Autorité veille à la mise en place, à la mise en valeur et à l'actualisation d'un portail de référencement de ces mêmes offres.
Elle évalue, en outre, les expérimentations conduites dans le domaine des technologies de reconnaissance des contenus et de filtrage par les concepteurs de ces technologies, les titulaires de droits sur les œuvres et objets protégés et les personnes dont l'activité est d'offrir un service de communication au public en ligne. Elle rend compte des principales évolutions constatées en la matière, notamment pour ce qui regarde l'efficacité de telles technologies, dans son rapport annuel prévu à l'article L. 331-14.
Elle identifie et étudie les modalités techniques permettant l'usage illicite des œuvres et des objets protégés par un droit d'auteur ou par un droit voisin sur les réseaux de communications électroniques. Dans le cadre du rapport prévu à l'article L. 331-14, elle propose, le cas échéant, des solutions visant à y remédier.

Rapport sur les moyens de lutte contre le streaming et le téléchargement direct illicites

2-1-4 LES AUTRES INTERMEDIAIRES TECHNIQUES

La liste des intermédiaires dont l'implication peut être sollicitée ou envisagée à des fins de lutte contre la contrefaçon n'est pas exhaustive, elle est au contraire évolutive en fonction des usages et des technologies. Ainsi, le blocage des noms de domaine (les adresses des sites sur Internet) peut être demandé au registre qui gère les noms de domaine, pour empêcher l'accès à un site. Dans l'affaire MegaUpload par exemple, les autorités américaines ont demandé à l'opérateur VeriSign, qui gère les noms de domaine utilisés aux Etats Unis, le 88 Ce service propose aux internautes des termes de recherche

supplémentaires associés automatiquement à ceux de la requête initiale en fonction du nombre de saisies. 89 Cass. civ. 1ère, 12 juillet 2012, n°11-20.358., SNEP c/ Google France et autres, précité. 28 reroutage des requêtes vers un site du FBI. Cette mesure a été rendue possible parce que MegaUpload opérait sous un nom de domaine en « .com ». En France, ce type de blocage est également possible mais il ne concerne que les noms de domaine en « .fr », qui apparaissent peu utilisés pour commettre les actes illicites à grande échelle. Les logiciels, qui permettent à l'internaute le passage d'un serveur à un autre ou l'accès aux différentes ressources documentaires sur le Web, pourraient également jouer un rôle. D'un point de vue technique, la mesure de filtrage pourrait passer ou non par l'installation d'un module chez l'utilisateur (plug-in). L'utilisateur pourrait alors changer de logiciel ou ne pas installer le module, ce qui limiterait l'efficacité de cette solution. L'efficacité d'une mesure de filtrage mise en place au niveau du système d'exploitation de l'ordinateur pourrait à cet égard apparaître plus efficace, car inhérente à l'ordinateur. Les acteurs à mobiliser seraient par ailleurs moins nombreux à solliciter mais également étrangers, ce qui pose la question de la contribution volontaire des acteurs industriels aux efforts de régulation française. Ainsi, la décision d'impliquer tel ou tel intermédiaire doit prendre en compte une série de facteurs tels que la facilité de contournement de la mesure envisagée, le nombre d'acteurs concernés, les effets et conséquences sur le réseau Internet et, de façon plus générale, un souci de proportionnalité et d'efficacité. La réflexion ne se limite d'ailleurs pas aux intermédiaires techniques mais touche aussi les fournisseurs d'instruments de paiement et les acteurs de la publicité en ligne, au centre du modèle économique du streaming et du téléchargement direct illicites, et sur lesquels l'attention des pouvoirs publics est de plus en plus soutenue.

2-2 A l'égard des sites de référencement ou des moteurs de recherche

3 | Accompagner les décisions de blocage des sites Si la question du blocage par les FAI de l'accès à un site en cas d'atteinte à un droit d'auteur a pu faire partie des questions les plus débattues au cours des dernières années tant dans son principe que dans ses modalités, la faculté conférée au juge par la loi d'ordonner une telle mesure parait aujourd'hui acquise tant en France que dans bon nombre de pays européens. La question ne relève plus aujourd'hui du principe mais de son application à chaque cas particulier, c'est-à-dire de la proportionnalité de la mesure concernée par rapport à la gravité de l'atteinte et aux modalités de filtrage mises en œuvre. Comme rappelé par la CJUE dans sa décision Sabam, la proportionnalité est d'abord une question d'équilibre entre le droit de propriété intellectuelle et la liberté d'entreprendre du FAI, la protection des données à caractère personnel des clients et leur liberté de recevoir et de communiquer des informations111.

Arrêté du 27 juin 1989 relatif à l'enrichissement du vocabulaire de l'informatique

ANNEXE II

Termes d'intelligence artificielle

appariement de formes,n.m.

Domaine : Informatique-Intelligence artificielle.

Synonyme : filtrage, n.m.

Définition : Mise en correspondance de formes selon un ensemble prédéfini de règles ou de critères.

Anglais : pattern matching.

base de connaissances,n.f.

Domaine : Informatique-Intelligence artificielle.

Définition : Partie d'un système expert contenant l'ensemble des informations, en particulier des règles et des faits, qui constituent le domaine de compétence du système.

Anglais : knowledge base.

cadre,n.m.

Domaine : Informatique-Intelligence artificielle.

Synonyme : schéma, n.m.

Définition : Structure de données permettant de décrire les connaissances relatives à une entité, sous forme d'un ensemble d'attributs et de procédures liées à ces attributs.

Anglais : frame.

filtrage, n.m.

Voir : appariement de formes.

[…]

DÉCISION No 276/1999/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 25 janvier 1999 adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux

-(5) considérant que la promotion de l'autoréglementation de l'industrie et des systèmes de suivi du contenu, le développement des outils de filtrage et des systèmes de classement fournis par l'industrie et une sensibilisation accrue portant sur les services offerts par l'industrie, de même que l'encouragement de la coopération internationale entre toutes les parties concernées, joueront un rôle crucial dans la consolidation de cet environnement sûr et contribueront à lever les obstacles au développement et à la compétitivité de l'industrie concernée.

-(15) considérant qu'il convient d'encourager, au niveau européen, la mise à disposition des consommateurs d'outils de filtrage et la création de systèmes de classement […]

-Les lignes d'action, en conjonction avec la recommandation du Conseil sur la protection des mineurs et de la dignité humaine, sont un moyen de mise en œuvre de l'approche européenne relative à une utilisation plus sûre d'Internet, fondée sur une autoréglementation de l'industrie, le filtrage

-2. Ligne d'action no 2. Développer les systèmes de filtrage et de classement Afin de promouvoir une utilisation plus sûre d'Internet, il est important de rendre plus facile l'identification du contenu.

Article 227-24 du code pénal

- Modifié par LOI n°2014-1353 du 13 novembre 2014 - art. 7

Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques

Article 1

La section 3 du chapitre II du titre Ier du livre II de la partie réglementaire (Décrets en Conseil d'Etat) du code des postes et des communications électroniques intitulée : « Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques » comprend les articles R. 10-12, R. 10-13 et R. 10-14 ainsi rédigés :

Art. R. 10-12. - Pour l'application des II et III de l'article L. 34-1, les données relatives au trafic s'entendent des informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi.

Art. R. 10-13. - I. - En application du II de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ;

b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

e) Les données permettant d'identifier le ou les destinataires de la communication.

II. - Pour les activités de téléphonie l'opérateur conserve les données mentionnées au I et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

III. - La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

IV. - Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

Art. R. 10-14. - I. - En application du III de l'article L. 34-1 les opérateurs de communications électroniques sont autorisés à conserver pour les besoins de leurs opérations de facturation et de paiement les données à caractère technique permettant d'identifier l'utilisateur ainsi que celles mentionnées aux b, c et d du I de l'article R. 10-13.

II. - Pour les activités de téléphonie, les opérateurs peuvent conserver, outre les données mentionnées au I, les données à caractère technique relatives à la localisation de la

communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.

III. - Les données mentionnées aux I et II du présent article ne peuvent être conservées que si elles sont nécessaires à la facturation et au paiement des services rendus. Leur conservation devra se limiter au temps strictement nécessaire à cette finalité sans excéder un an.

IV. - Pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver pour une durée n'excédant pas trois mois :

a) Les données permettant d'identifier l'origine de la communication ;

b) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

c) Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs. »

Code des postes et des communications électroniques

Article R10-13

- Créé par Décret n°2006-358 du 24 mars 2006 - art. 1 JORF 26 mars 2006

I. - En application du II de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ;

b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

e) Les données permettant d'identifier le ou les destinataires de la communication.

II. - Pour les activités de téléphonie l'opérateur conserve les données mentionnées au I et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

III. - La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

IV. - Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

Code des postes et des communications électroniques

Article L39-3

- Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 19 JORF 10 juillet 2004

I. - Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents :

1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;

2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

Les personnes physiques coupables de ces infractions encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise.

II. - Paragraphe abrogé.

Article 226-22

- Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

11. SOURCES

olfeo.com

legifrance.gouv.fr

cnil.fr

s2b-net.fr

ecologique-solidaire.gouv

nasexpert.fr

net.iris.fr

Livre blanc juridique OLFEO, Volume I : "Droit de filtrer, droit de loguer"

LDLC PRO

Picata

Inmac