Charte d'utilisation du Système d'Information du Groupe Darty

Version 2.0
Date : 16 Novembre 2010
Emetteur : RSSI
Diffusion : Généralisée au sein de l'entreprise

Le système d'information de DARTY est aujourd'hui **une ressource indispensable à la réalisation et au développement de nos activités**.

Sa disponibilité est essentielle à la gestion de nos approvisionnements, à la vente des produits en ligne ou en magasins et à la fourniture des services DARTY. L'intégrité et la confidentialité des informations gérées au moyen de ce système doivent être préservées, afin de maintenir nos avantages concurrentiels et de conforter la confiance de nos clients et fournisseurs.

A cet égard, le déploiement de nouvelles applications, l'interconnexion des réseaux, la fourniture de services de mobilité et l'utilisation croissante de l'internet constituent une source nouvelle de progrès mais exposent également notre système d'information à de nombreux risques (intrusion de virus, vol ou divulgation d'information, parasitage de sites internet…).

Dès lors, comment sauvegarder le patrimoine de notre entreprise et assurer la continuité de nos activités ? Comment nous protéger et protéger nos clients et partenaires ?

En réponse à ces questions, des mesures techniques de sécurité sont mises en œuvre par DARTY. En regard, les conditions d'usage du système d'information par ses utilisateurs doivent également respecter certaines pratiques sécuritaires en l'absence desquelles la protection de nos informations ne peut être garantie.

Afin de nous guider dans nos comportements au quotidien, une mise à jour de la **charte d'utilisation du système d'information** a été élaborée. Son application est l'affaire de tous, dans l'intérêt de chacun. La méconnaissance de la législation, l'ignorance des risques encourus ou une mauvaise application des règles de sécurité peuvent être lourds de conséquences, pour notre entreprise comme pour chacun d'entre nous, puisque nous engageons notre propre responsabilité.

Il convient donc d'appréhender tout l'intérêt et le contenu de cette charte et de la valider pour diffusion à l'ensemble des collaborateurs du Groupe et des Filiales.

1. Objet de la charte

Cette charte décrit les **comportements qui doivent être connus et respectés** par tous les collaborateurs de DARTY afin d'**assurer un usage correct et sécurisé du système d'information (SI) de l'Entreprise**.

A cette fin, elle a pour objet de préciser les droits, les devoirs et les responsabilités de chacun s'appliquant lors de l'usage des ressources du SI, en accord avec la législation en vigueur et après information des instances représentatives du personnel.

Les principes énoncés ne sont pas exclusifs des règles normales de courtoisie et de respect d'autrui.

2. Modalités d'application de la charte

Tout collaborateur de DARTY, permanent ou temporaire, quel que soit son statut, ayant accès aux ressources du système d'information de DARTY est tenu de respecter cette charte.

Les manquements sont susceptibles d'engendrer, pour l'utilisateur, la restriction voire la suspension de ses accès aux ressources du SI, sans préjuger d'éventuelles sanctions disciplinaires ou d'actions pénales ou civiles à son encontre.

La présente charte fait l'objet d'une diffusion par voie d'affichage et d'une communication individuelle à chacun des collaborateurs de DARTY par le biais de sa hiérarchie. Elle est portée à la connaissance des prestataires de l'Entreprise dans le cadre de la conclusion des contrats.

3. Respect de la législation

La loi s'appliquant à tous, chaque collaborateur peut être tenu responsable civilement et pénalement dans ses fonctions au quotidien, en cas de manquement aux obligations légales et/ou réglementaires.

Les diverses dispositions du cadre légal français et européen dans le domaine des systèmes d'information doivent être appliquées au sein de DARTY. Elles portent notamment sur la **protection des droits d'auteurs de logiciels**, le **secret des correspondances**, la **protection des données à caractère personnel**, la **lutte contre les accès illicites aux ressources du SI ou leur utilisation frauduleuse** et la **protection de la dignité humaine**. Les sanctions légales potentiellement encourues en cas de non respect de ces dispositions sont précisées en annexe de la présente charte.

L'utilisateur doit :

- Protéger les droits de propriété de DARTY pour l'ensemble de ses savoirs et savoir-faire, notamment pour tous les logiciels que l'Entreprise a fait développer.
- Respecter strictement le secret professionnel et garantir la confidentialité des informations internes à l'Entreprise (relatives notamment aux volumes et chiffres d'affaires, aux conditions d'achat et de vente, aux taux de retour, aux stocks, aux projets de création de services ou de sites, aux personnels, aux systèmes d'information, aux procédures et à l'organisation internes de l'Entreprise…).
- Respecter le secret des correspondances et communications adressées à des tiers et la vie privée des personnes.

L'utilisateur ne doit pas :

- Consulter, télécharger, diffuser, mettre à disposition ou stocker des informations pouvant porter atteinte à la dignité humaine (diffamation, injure…) ou contraires à la législation (pédopornographie, racisme, apologie des stupéfiants…).
- Installer ou distribuer un logiciel commercial sans licence ni déjouer tout dispositif anti-copie, ni dupliquer des installations logicielles au-delà du nombre prévu dans le contrat de licence : il se rendrait alors coupable de délit de contrefaçon.
- Diffuser en dehors de l'Entreprise toute information confidentielle sans l'accord préalable de la Direction de la Communication de DARTY.
- Accéder sans autorisation aux ressources du SI, perturber leur fonctionnement, introduire ou modifier des données de façon frauduleuse ; ni détenir ou fournir tout dispositif conçu pour commettre ce type d'infractions.
- Utiliser ou détourner à son profit ou à celui de tiers tout ou partie du système d'information de DARTY auquel il a accès, que ce soit ou non dans l'exercice de ses fonctions.
- Collecter des informations nominatives (en dehors des données requises par l' utilisation normale des applications métiers délivrées par la DOSI) sans information préalable des personnes concernées ; divulguer ou utiliser ces informations sans leur consentement préalable ou opérer de tels traitements sans avis favorable de la CNIL ; celui-ci étant sollicité uniquement par les services juridiques de DARTY, qui gèrent la conformité légale de toutes les ressources mises à disposition par les services informatiques.
- Collecter des informations personnelles interdites au regard de la loi (origines raciales, opinions politiques, philosophiques, religieuses, appartenance syndicale, mœurs, santé et vie sexuelle).

4. Conditions d'accès aux ressources du SI

Le contrôle des accès aux différentes ressources du SI de DARTY est un dispositif transverse dont l'efficacité est un élément clé pour la sécurité, à la fois pour garantir la disponibilité des ressources de tout dysfonctionnement non accidentel, pour protéger l'intégrité et la confidentialité des informations de malveillances potentielles, et aussi, pour être en mesure de justifier des opérations réalisées à travers le SI.

L'accès aux ressources du système d'information de DARTY n'est autorisé que dans le **cadre de l'activité professionnelle** des collaborateurs, définie par leur fonction et dans les limites de délégations qui leur sont accordées.

Un usage personnel, **ponctuel et raisonnable** dans le cadre des nécessités de la vie courante et familiale est toléré, dès lors qu'il ne porte aucun préjudice à l'activité professionnelle et qu'il n'est pas susceptible d'affecter le bon fonctionnement du SI ou de mettre en cause les intérêts ou la réputation de DARTY.

L'accès aux ressources du système d'information est soumis à l'usage d'un **authentifiant individuel strictement personnel** (mot de passe, carte à puce, …) dont l'utilisation engage la responsabilité du collaborateur. Les exceptions à ce principe dans certains environnements sont recensées par les services informatiques et validées par la Direction de l'Entreprise.

Les droits d'accès peuvent être révoqués à tout moment, et prennent fin en cas de suspension momentanée ou définitive de l'activité professionnelle.

L'utilisateur doit :

- Choisir des mots de passe robustes, c'est-à-dire difficile à découvrir par un tiers (composés de 8 caractères associant des chiffres, des majuscules et minuscules) et en préserver la confidentialité (mémorisation, saisie à l'abri des regards) et la validité sur la période prévue.
- Changer régulièrement ses mots de passe (au moins tous les 3 mois) et les modifier immédiatement en cas de suspicion de divulgation du secret.
- Limiter son usage du SI dans un contexte non professionnel, et clairement identifier comme telles les informations à caractère privé (intitulé « privé » dans l'objet d'un message électronique ou le nom d'un support de stockage) et assurer la sécurité de ces informations qui est de sa seule responsabilité.

L'utilisateur ne doit pas :

- Communiquer ou céder en aucune manière, même temporairement, son authentifiant à un tiers.
- Ecrire son mot de passe ou l'enregistrer sur le système en vue d'automatiser la procédure d'authentification, en dehors des applications de SSO fournies par la DOSI.
- Usurper l'identité d'un autre collaborateur ou tenter de s'approprier son authentifiant, ni contourner les restrictions d'accès aux ressources mises à disposition par DARTY.
- Introduire des failles de sécurité dans l'architecture du système d'information, ou exploiter ou tenter d'exploiter une éventuelle faille de sécurité constatée ou en faire la publicité.

5. Conditions d'utilisation des postes de travail

Le poste de travail est le principal point d'accès au SI mis à disposition des collaborateurs de DARTY. C'est par conséquent un composant particulièrement sensible quant à la sécurité et potentiellement vulnérable si de bonnes pratiques d'utilisation ne sont pas adoptées par tous.

Les postes de travail sont configurés selon des standards définis par les services informatiques de DARTY qui intègrent les mesures de sécurité nécessaires à la protection du système d'information de l'Entreprise. Leurs **conditions d'usage** au quotidien ne doivent par remettre en cause l'efficacité de ces dispositifs de sécurité.

L'utilisateur doit :

- Connecter au réseau de l'Entreprise uniquement des postes de travail fournis par les services informatiques de DARTY.
- Afin que les mises à jour des dispositifs de sécurité puissent s'opérer, ne pas éteindre le poste de travail fixe en fin de journée, mais fermer la session ; connecter au moins une fois par mois son ordinateur portable au réseau de DARTY ; et redémarrer les postes de travail au moins une fois par semaine.
- Verrouiller son poste de travail en cas d'absence, même temporaire.
- Sauvegarder ses données bureautiques dont la perte serait préjudiciable sur le réseau ou, à défaut, sur un support de stockage mis à disposition par les services informatiques et stocké de façon sécurisée (mise sous clé et conservation d'un double dans un lieu différent).
- Veiller, en toutes circonstances, à mettre en sécurité le matériel, notamment les ordinateurs portables et les supports de stockage externe.
- Etre vigilant et signaler tout constat d'anomalie (dysfonctionnement ou comportement anormal, tentative d'accès illicite ou de vol, perte de données…) à sa hiérarchie et au service support (SVP).

L'utilisateur ne doit pas :

- Modifier la configuration d'un poste de travail ni le paramétrage des logiciels mis à sa disposition.
- Installer sur un poste de travail, ni connecter au réseau, des composants matériels ou logiciels sans accord préalable des services informatiques de DARTY (par exemple : postes de travail, ordinateurs portables, téléphones mobiles, assistants personnels, imprimantes, postes de prestataires, modems…).
- Désactiver l'antivirus ou entraver la mise à jour des dispositifs de sécurité.
- Surcharger les supports de stockage par des données inutiles à l'activité de l'Entreprise.
- Stocker sur des supports externes (ex : disque dur amovible, clé usb, cd ou dvd, …) des informations confidentielles non protégées par les dispositifs de sécurité mis à disposition par les services informatiques de DARTY (ex : outils de chiffrement de données).
- Permettre à des personnes situées en dehors du réseau de l'entreprise, de prendre le contrôle du poste de travail à distance, en dehors des procédures référencées par la DOSI. Les actions sont toujours réalisées sous l'entière responsabilité de l'utilisateur qui a autorisé la connexion à distance, et sa présence physique devant le poste est impérative pour un contrôle effectif.

6. Conditions d'usage de la messagerie électronique

Le courrier électronique est aujourd'hui un mode de communication privilégié dans l'Entreprise en raison de sa flexibilité et de sa rapidité. Cependant, le mode de fonctionnement de la messagerie électronique et sa facilité d'utilisation induisent de nombreux risques dont les plus préjudiciables concernent la divulgation d'informations confidentielles, la diffusion d'informations à caractère illégal, la propagation de virus et autres codes malveillants ou l'abus d'usage entrainant une dégradation du service.

La réduction de ces risques repose essentiellement sur le comportement des usagers de la messagerie électronique au sein de l'Entreprise, qui doivent par conséquent **respecter un code de bonne conduite et de sécurité rigoureux** en la matière.

L'utilisateur doit :

- Utiliser exclusivement le client de messagerie fourni et installé par DARTY, tout autre ne bénéficiant pas des dispositifs de sécurité mis en place par l'Entreprise.
- Vérifier l'adresse du destinataire avant l'envoi d'un mail afin d'éviter tout adressage erroné et la communication d'informations à des destinataires non habilités à en prendre connaissance.
- Utiliser avec discernement les listes de diffusion pour maîtriser l'envoi de copies à un nombre injustifié de destinataires.
- S'efforcer de limiter le volume des messages (notamment la taille des pièces jointes) afin d'éviter de surcharger les réseaux de l'Entreprise (utiliser si besoin les outils de compression mis à disposition par les services informatiques).
- Protéger la confidentialité des informations sensibles échangées en interne au moyen des dispositifs de chiffrement fournis par la messagerie, ou solliciter les services informatiques de DARTY en cas d'autres besoins spécifiques.
- En cas d'absence, mettre en place un message de réponse automatique informant l'expéditeur de sa date de retour et de la personne à contacter si besoin.

L'utilisateur ne doit pas :

- Utiliser de procédure de renvoi automatique des messages professionnels vers une messagerie externe à celle de DARTY, la sécurité de ces flux ne pouvant être maîtrisée.
- Ouvrir un message, ou une pièce jointe associée, qui présentent un doute quant à leur provenance ou leur contenu.
- Donner suite ou rediffuser les messages en chaîne ou alarmistes (*hoax*) qui utilisent inutilement les ressources du système d'information.
- Répondre aux messages électroniques commerciaux non sollicités (*spam*), ou cliquer sur les liens qu'ils proposent (même dans l'intension de se désabonner d'une liste de diffusion).
- Cliquer, en aucun cas, sur les liens hypertextes contenus dans un message non sollicité et demandant de fournir des données confidentielles (*phishing*).

7. Conditions de navigation sur l'Internet

L'Internet étant un média public de portée mondiale constitue à la fois un vecteur de développement fort pour les activités de l'Entreprise mais aussi une zone à risques multiformes (détournement d'informations, fraude, sabotage ou intrusions logiques, comportement illégaux…) dont les impacts, à la fois juridiques et techniques, peuvent atteindre à l'image de marque de DARTY ou remettre en cause la continuité de certaines de ses activités (vente en ligne, services au client …).

DARTY met en œuvre des dispositifs de sécurité (cloisonnement des réseaux et contrôle des flux) permettant de **protéger le système d'information de l'Entreprise des actions malveillantes susceptibles d'être conduites depuis l'Internet** tout en fournissant l'accès aux services Internet devenus indispensables à ses activités.

DARTY se réserve la possibilité de mettre en place des mesures techniques visant à interdire aux utilisateurs l'accès à certains sites à caractère manifestement non professionnel.

L'utilisateur doit :

- Utiliser exclusivement la connexion et le navigateur Internet officiels fournis et sécurisés par DARTY.
- Observer un devoir de réserve et se garder d'émettre toute opinion ou d'exercer toute activité susceptible de porter atteinte à l'image de l'Entreprise, notamment lors de la participation à des forums ou sur les différents réseaux sociaux (ex : Facebook, LinkedIn, Viadeo, etc.) dont il est membre à titre personnel.
- Eviter de laisser son adresse de messagerie professionnelle sur les sites, forums et autres lieux de l'Internet, afin de prémunir DARTY contre la réception de mails indésirables (*spam*).

L'utilisateur ne doit pas :

- Modifier la configuration de son navigateur Internet, notamment les paramètres de connexion et de sécurité.
- Tenter d'accéder à l'Internet par des moyens autres que ceux mis à disposition par les services informatiques de DARTY ; la connexion d'un poste de travail DARTY à l'Internet par le biais d'un modem local pouvant notamment remettre en cause la sécurité de l'ensemble du réseau de l'Entreprise.
- Transmettre ou publier sur Internet des informations non publiques ou confidentielles à propos de DARTY, de ses clients, partenaires ou fournisseurs, ou de son personnel (sauf autorisation spécifique validée par la hiérarchie).
- Créer ou administrer des services Internet ou de communication électronique étrangers aux besoins de l'activité professionnelle ou n'ayant pas fait l'objet d'une autorisation des services informatiques de DARTY.
- Utiliser à des fins professionnelles des messageries Internet grand public (ex : Yahoo, Hotmail, Voilà, Gmail…) ou des messageries instantanées (ex : MSN Messenger, ICQ, Yahoo Messenger …) dont la sécurité ne peut être assurée.
- Consulter des sites, télécharger ou échanger des informations dont le contenu est contraire à la loi *(cf. § 3 : Respect de la législation)*.
- Consulter à titre personnel des sites Internet nécessitant des ressources importantes en bande passante – à titre d'exemple non exhaustif des sites de streaming vidéo (Youtube, Dailymotion, Wat, etc.), des sites de streaming audio (Deezer, goom-radio,

etc.) – afin de ne pas pénaliser les performances en bande passante nécessaires aux usages professionnels ;

- Tenter de contourner les restrictions d'accès à certains sites Internet mises en œuvre par DARTY.

8. Contrôle de l'utilisation des ressources du SI

L'enregistrement des accès ou tentatives d'accès aux ressources du système d'information de DARTY constitue une mesure de sécurité dont la finalité première est d'en garantir l'utilisation normale. L'employeur doit pouvoir, le cas échéant, identifier et sanctionner les usages contraires à la loi et à ses règles internes, répondre aux requêtes émanant des tribunaux ou des organismes de police relatives au comportement de ses collaborateurs, y compris lors de l'usage de son système d'information.

A ces fins, DARTY met en œuvre des **moyens d'enregistrement et d'analyse** dans le respect de l'information des personnels concernés, ainsi que de la législation applicable à l'information, aux fichiers et aux libertés, relative à la protection de la vie privée, de sorte que les informations enregistrées jouissent d'une protection particulière contre tout risque de divulgation.

Les moyens et techniques de contrôle qui sont mis en œuvre au niveau du système d'information évolueront à mesure que la technologie se perfectionnera. Ils sont précisés dans une annexe de la présente charte, qui sera remise à jour régulièrement.

Lorsque les circonstances l'exigeront (événements menaçant l'intégrité et la sécurité du système d'information), que la responsabilité ou les intérêts de DARTY seront en jeu, les **moyens d'investigation** nécessaires seront mis en œuvre, à l'initiative d'un des Membres du Comité de Direction du Groupe Darty ou du Comité d'Audit Groupe et, le cas échéant, l'accès aux ressources du système d'information pourra être restreint, voire fermé, sans préavis.

9. Annexe 1 : informations relatives aux conditions de mise en œuvre du contrôle

9.1. Messagerie

Contrôle global :

Dans le cadre des services de messagerie électronique, les éléments collectés visent à contrôler globalement :

- le nombre de messages reçus de l'Internet ;
- le volume occupé par l'ensemble des boîtes aux lettres sur tout le système et par serveur de messagerie ;
- le format de certaines pièces jointes ;
- la présence de certains mots clés indésirables dans le contenu des messages ;

ces informations pouvant être comptabilisées, sur une base journalière, à des fins statistiques.

Contrôle individuel :

La taille des boîtes aux lettres est limitée ; des dépassements de seuil sont autorisés de manière dérogatoire et sont suivis de manière statistique.

Des contrôles sur le nombre de messages reçus d'un même émetteur depuis Internet sont effectués, afin de détecter les courriers indésirables.

Chaque message fait l'objet d'un traitement automatique visant à détecter la présence de virus et à l'éradiquer chaque fois que c'est possible. En cas de présence de virus, les adresses de l'émetteur et du destinataire, l'objet du message et le type de virus détecté sont enregistrés à des fins d'analyse et de statistiques. Le message infecté n'est pas délivré.

Conservation :

Des sauvegardes sont effectuées de façon à pouvoir restaurer la base de messagerie en cas d'incident. Les sauvegardes effectuées quotidiennement sont conservées 15 jours, les sauvegardes mensuelles sont conservées pendant 1 an.

Contrôle du contenu :

Afin de pouvoir procéder à des investigations visant à déterminer la cause de certains dysfonctionnements, ou en cas de violation délibérée des règles d'usage de la messagerie, il pourra être procédé à la lecture de l'enveloppe (contenant la date et l'heure d'émission, l'émetteur, le(s) destinataires, l'objet, le nom et le type des pièces jointes) de certains messages.

Le contenu d'un message pourra être consulté, selon les modalités suivantes :

- accord préalable explicite de l'intéressé ;
- ou en cas de nécessité de service sérieuse et de présomption à la lecture de l'enveloppe que le message n'a manifestement pas un caractère privé.

Cette lecture ne pourra être effectuée que sur demande du Directeur de l'Audit Groupe ou d'un des Membres du Comité de Direction du Groupe en présence autant qu'il est possible de l'intéressé. Dans le cas où la présence de l'intéressé n'est pas possible, cette lecture sera effectuée en présence d'un huissier, mandaté par l'Entreprise.

Dans tous les cas, après lecture du contenu du message, l'intéressé en sera informé par écrit, le motif lui étant également signalé.

Non utilisation ou cessation d'activité :

En cas de suspension momentanée ou définitive de l'activité professionnelle, la boîte aux lettres est archivée pour 13 mois puis détruite si le propriétaire n'a pas demandé sa réactivation.

9.2. Usage de l'Internet

Contrôle global :

La liste des sites visités est collectée, à des fins statistiques et pour adapter les caractéristiques techniques de l'accès Internet.

Contrôle individuel :

La liste des sites visités et le volume des consommations sont collectés. Ces informations sont utilisées :

- à des fins statistiques et/ou de refacturation ;
- pour vérifier que le trafic reste dans des limites raisonnables (dans le cas contraire, les utilisateurs sont alertés ; il en sera de même de leur responsable hiérarchique en cas de récidive non justifiée professionnellement) ;
- en cas de dysfonctionnement du réseau, pour permettre de rechercher les éventuelles consommations atypiques qui en perturberaient le fonctionnement, puis prendre contact avec les utilisateurs concernés ou leur hiérarchie pour rechercher avec eux une solution correctrice ;
- pour assurer une traçabilité en cas de problème grave (comme par exemple l'utilisation d'Internet pour commettre des infractions, des délits ou des crimes). Dans ce cas, l'information collectée n'est accessible, selon des procédures particulières, que sur demande explicite d'un Membre du Comité de Direction du Groupe ou du Directeur de l'Audit Groupe, en présence de l'intéressé et à défaut d'un représentant de personnel.

La durée de conservation de ces informations individuelles est de 6 mois.

9.3. Utilisation de l'espace bureautique : accès aux espaces communs et individuels

Contrôle global :

Des contrôles peuvent être effectués sur la taille des espaces bureautiques, afin de convenir avec le responsable de l'environnement bureautique du service de mesures de réduction si besoin est.

Contrôle individuel :

Peuvent être l'objet de contrôles périodiques : la taille globale de l'espace bureautique, le nombre de fichiers, leurs tailles et leurs types. Ces informations sont utilisées pour veiller au respect des règles d'utilisation des espaces bureautiques.

Le contenu d'un fichier d'un répertoire individuel pourra être consulté, après accord préalable explicite écrit de l'intéressé ou nécessité de service sérieuse. Cette lecture ne pourra être effectuée que sur demande de l'Audit Groupe, en présence du salarié et à défaut d'un représentant du personnel.

Non utilisation ou cessation d'activité :

En cas de suspension momentanée ou définitive de l'activité professionnelle, les espaces individuels sont archivés pour 13 mois puis détruits si le propriétaire n'a pas demandé leur réactivation.

9.4. 4 – Accès distants sécurisés

Il s'agit des accès au système d'information réalisés depuis l'extérieur de DARTY au moyen du réseau téléphonique commuté ou du réseau Internet.

Pour chaque connexion individuelle, les dates et heures de début et de fin de connexion ainsi que les volumes transmis sont enregistrés.

Ces informations sont conservées 3 mois et sont utilisées :

- pour diagnostiquer un dysfonctionnement dans le service rendu à l'utilisateur ;
- pour procéder à des investigations en cas de tentatives d'accès ou d'utilisation frauduleuse.

10. Annexe 2 : informations relatives au cadre légal et aux sanctions encourues

Le contenu de cette annexe mentionne, en regard du *§ 3* de la *Charte d'utilisation du système d'information de DARTY*, les principales **sanctions** potentiellement encourues (peines de prison et amendes) **en cas de non respect des dispositions du cadre légal** français applicable au domaine des systèmes d'information.

Violation des droits d'auteurs de logiciel et contrefaçon (respect de la propriété intellectuelle) :

- 3 ans de prison
- 300 000 euros d'amende (+ dommages et intérêts éventuels)

Violation des droits d'auteurs de logiciel (complément apporté par la loi HADOPI) :

- Suspension de l'accès Internet de l'entreprise
- 3 ans de prison applicables au chef d'entreprise
- 300 000 euros d'amende

Atteinte au secret des correspondances :

- 1 an de prison
- 45 000 euros d'amende

Atteinte à la protection des données à caractère personnel :

- 5 ans de prison
- 300 000 euros d'amende

Accès illicite aux ressources du système d'information ou utilisation frauduleuse :

- 2 à 5 ans de prison
- 30 000 euros à 75 000 euros d'amende

Pédopornographie :

- Mise à disposition, diffusion, transmission, importation d'une image ou représentation pornographique d'un mineur, ainsi que leur tentative :
  - 5 ans de prison
  - 75 000 euros d'amende
- Consultation ou détention d'une telle image ou représentation :
  - 2 ans de prison
  - 30 000 euros d'amende

Provocation à l'usage de stupéfiants :

- 5 ans de prison
- 75 000 euros d'amende

« Délits de presse » (provocation à la haine raciale ou au terrorisme, apologie ou contestation de crimes contre l'humanité, …) :

- 1 an de prison
- 45 000 euros d'amende

11. Annexe 3 : définitions

Système d'information :

Il s'agit de l'organisation de l'ensemble des moyens humains et techniques destinés à élaborer, traiter, stocker, acheminer, présenter ou détruire des informations, quelle que soit leur forme (électronique, imprimée, manuscrite, vocale, imagée, …).

Ressource du système d'information :

Il s'agit à la fois de l'information, des différents composants informatiques et télécoms (postes de travail, systèmes et réseaux, applications, bases de données, services de messagerie, supports de stockage, …) permettant de la gérer et des procédures associées, ainsi que de leurs environnements d'exploitation (bâtiments et locaux hébergeant ces ressources).

Utilisateur du système d'information :

Il s'agit de toute personne (interne ou externe à l'Entreprise) autorisée à accéder, utiliser ou traiter des ressources du système d'information de DARTY dans le cadre de son activité professionnelle.

Informations confidentielles :

Il s'agit de toutes les informations qui concernent et/ou mesurent les activités de DARTY, l'efficacité des moyens mis en œuvre et les coûts associés, les principes d'organisation de l'Entreprise et ses projets de développement.