CHARTE D'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION A DESTINATION DES USAGERS DE L'UNIVERSITE D'ARTOIS

Entre l'Université d'Artois d'une part,

et

l'usager, toute personne susceptible d'utiliser l'internet, les réseaux et les services numériques proposés dans l'établissement, ci-après dénommé l'utilisateur d'autre part,

il est convenu ce qui suit :

Préambule

La fourniture de services liés aux technologies de l'information et de la communication s'inscrit dans la mission de service public de l'université. Cette offre de services vise entre autres à mettre à la disposition des utilisateurs de l'établissement un Environnement Numérique de Travail.

La présente charte définit les conditions générales d'utilisation de l'internet, des réseaux et des services numériques au sein de l'établissement, en rappelant l'application du droit et en précisant le cadre légal afin de sensibiliser et de responsabiliser l'utilisateur. Cette charte précise les droits et obligations que l'université et l'utilisateur s'engagent à respecter et notamment les conditions et les limites d'éventuels contrôles portant sur l'utilisation des services proposés.

Elle vise à promouvoir des comportements de vigilance et de sécurité et à renforcer la prévention d'actes illicites en amenant les utilisateurs à constamment s'interroger sur le caractère licite de leurs actes.

Article 1 - Respect de la législation

Toute utilisation contraire à la loi est interdite et susceptible d'entraîner des sanctions et poursuites pour son auteur. Sont notamment interdits *(cf. annexe I juridique)* :

- l'atteinte à la vie privée d'autrui,
- la diffamation et l'injure,
- l'incitation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur ,
- l'incitation à la consommation de substances interdites,
- la provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination à la haine notamment raciale, ou à la violence,
- l'apologie de tous les crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité, la négation de crimes contre l'humanité,
- la contrefaçon de marque,
- la reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple : extrait musical, photographie, extrait littéraire....) ou d'une prestation de droits voisins (par exemple : interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire de droits voisins et/ou du titulaire des droits de propriété intellectuelle,
- les copies de logiciels commerciaux pour quelque usage que ce soit, à l'exception d'une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.

Article 2 – Droits de l'utilisateur

A) L'utilisateur bénéficie d'un accès aux services proposés par l'Université dans le cadre et les limites définies par celle-ci. L'Université fait bénéficier l'utilisateur d'un accès aux services proposés après acceptation de la présente charte. Cet accès peut être soumis à une identification préalable de l'utilisateur, qui dispose alors d'un compte d'accès personnel aux ressources et services numériques proposés.

B) Le compte d’accès d’un utilisateur est constitué d’un identifiant et d’un mot de passe strictement personnels et confidentiels. Leur usage ne peut en aucun cas être cédé à un tiers à quelque titre que ce soit. L’utilisateur est responsable de leur conservation et s’engage à ne pas les divulguer et à ne pas s’approprier ceux d'un autre utilisateur.

C) Le compte d'accès donne à l'utilisateur un droit d'accès aux services mis à sa disposition. Ce droit d'accès est personnel, incessible et temporaire. Il disparaît dès lors que son titulaire ne répond plus aux critères d'attribution.
Ce droit d'accès peut être suspendu à tout moment, dès lors qu'est supposé un manquement aux dispositions de la présente charte par l'utilisateur.
L'utilisateur donne expressément son consentement pour que les données à caractère personnel le concernant soient collectées dans le cadre de l'ouverture du compte d'accès. Ces données ne seront utilisées que pour les finalités de cette inscription.
L'utilisateur peut demander à l'Université la communication des informations nominatives le concernant et les faires rectifier en application de la loi n°78-17 du 6 juillet 1978 relative à l'informatique aux fichiers et aux libertés.
L'utilisateur est informé qu'en application des dispositions législatives et règlementaires en vigueur, l'Université est tenue de recueillir et conserver des informations sur les utilisateurs de ses services informatiques et peut dans le cadre d'une enquête judiciaire, être dans l'obligation de les donner.
En conséquence, tout refus de l'utilisateur relatif à la collecte des informations à caractère personnel demandées implique le rejet de la demande de compte d'accès.

Article 3 - Obligations de l'utilisateur

L’utilisateur s’engage à informer immédiatement le gestionnaire de toute perte, de toute tentative de violation ou anomalie relative à une utilisation de son compte d’accès.
L’utilisateur s’engage à effectuer une utilisation rationnelle et loyale des services et, notamment du réseau, de la messagerie et des ressources informatiques afin d’en éviter la saturation et le détournement à des fins personnelles.
L’utilisateur accepte que l’Université puisse avoir connaissance des informations nécessaires à l’administration du réseau (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper la perturbation de ses services. L’Université se réserve, notamment, la possibilité de stopper l’accès aux services en cas d’utilisation excessive ou non conforme à ses missions spécifiques telles que définies dans la présente convention.
L’utilisateur est responsable de l’usage qu’il fait du réseau. Il assure notamment, à son niveau, la sécurité de ce réseau et s’engage à ne pas apporter volontairement de perturbations à son fonctionnement et à mettre en péril l’intégrité des ressources informatiques.

Il s’engage, notamment, à :

- ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;
- ne pas introduire des programmes virus, ou contournant la protection des logiciels ;
- ne pas installer de logiciels susceptibles de modifier la configuration des machines sans accord préalable du gestionnaire;
- ne pas s’attaquer aux systèmes d’information de l’Université ou de tout autre organisme public ou privé, européen ou étranger, en modifier ou altérer le contenu ;
- ne pas collecter ou tenter de collecter des informations susceptibles d’être utilisées lors de tentatives d’attaques contre des systèmes d’information externes ou internes ;
- ne pas utiliser les ressources informatiques afin de dupliquer, diffuser ou distribuer des logiciels, images, sons et vidéos aux contenus visés par le code pénal ou collectés par des moyens contraires au droit de la propriété intellectuelle, sous quelque forme que ce soit.

Article 4 - Disponibilité des services

L’Université s’efforce, dans la mesure du possible de maintenir accessible les services qu’elle propose de manière permanente, sans être tenue à une obligation de résultat. Elle peut interrompre l’accès, notamment pour des raisons de maintenance, de mise à niveau et de sécurité, sans pouvoir être tenue pour responsable des conséquences de ces interruptions tant à l’égard des utilisateurs que des tiers.

Article 5 - Contrôle et maintenance par le gestionnaire

L’utilisateur est averti que le gestionnaire peut avoir accès à l’ensemble des composants du système d’information, à l’exclusion de la messagerie et des espaces personnels, à n’importe quel moment et ce afin d’effectuer tout acte de protection du système d’information concernant :

- la conservation et la sauvegarde, le contrôle de l'absence de diffusion non autorisée d'informations sur les sites web,
- la preuve de la date de création ou de diffusion des dites informations,
- la recherche et le rejet d'intrusions dans le système d'informations ou de matériels violant les règles relatives au droit d'auteur,
- la mise à jour, maintenance, correction et réparation des matériels et logiciels.

Tout utilisateur peut obtenir auprès du gestionnaire les informations sur les moyens de contrôle mis en oeuvre.
Les contrôles techniques qui peuvent être effectués sont justifiés par un souci de sécurité du réseau et/ou des ressources informatiques :
Les services techniques peuvent être amenés à effectuer des sauvegardes, y compris sur les contenus personnels, dans le but exclusif d'empêcher des pertes d'informations. Ces contenus ne sont pas accessibles aux tiers sauf procédure juridictionnelle.

Article 6 - Antivirus

L'Université dispose d'antivirus sur l'ensemble de ses postes. Chaque utilisateur doit se conformer aux instructions de l'Administrateur en ce qui concerne la mise à jour de l'antivirus.

L'accès au réseau WIFI de l'université depuis un ordinateur personnel n'est autorisé que si celui-ci est à jour au niveau système et antivirus.

Article 7 – Utilisation des services internet

A) **Services mis à disposition et capacité technique**

L'Université offre à l'utilisateur, dans la mesure de ses capacités techniques, un bouquet de services ainsi que l'accès Internet avec possibilité de navigation sur ce réseau.
L'accès aux services offerts peut avoir lieu :

- soit depuis les sites de l'Université (serveurs, micro-ordinateurs en libre service)
- soit par un accès individuel à partir de toute machine connectée à Internet.

L'Université s'est dotée des moyens lui permettant d'être un fournisseur d'accès.
L'Université s'est dotée des moyens lui permettant d'être un fournisseur d'hébergement Internet.

B) **Contrôles techniques**

Des contrôles techniques peuvent être effectués :

- soit dans un souci de sécurité du réseau et / ou des ressources informatiques.

Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées. L'Université se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système.

- soit dans un souci de protection des utilisateurs et notamment des mineurs. L'établissement se réserve la possibilité de procéder à un contrôle des sites visités par les utilisateurs afin de limiter l'accès par ces derniers à des sites illicites ou requérant l'âge de la majorité.

C) **Contrôle des pages Web hébergées sur les serveurs de l'université**

L'université peut contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente charte. L'Université est autorisée à suspendre l'usage pour un utilisateur du service d'hébergement des pages Web en cas de non-respect de la charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages un contenu manifestement illicite.

Une procédure spécifique régit les règles d'hébergement des sites web satellites.

Article 8 - Utilisation de la messagerie

Dans le cadre de ses services Intranet/Internet, l'Université met à la disposition de l'utilisateur un service de messagerie électronique. L'université ne garantit pas que le service de messagerie soit exempt de toute interruption, retard, incident de sécurité ou erreur. L'Université ne garantit pas les résultats pouvant être obtenus à l'aide de ce service, ni la précision ou la fiabilité des informations acquises par son intermédiaire. Elle n'exerce aucune surveillance ni aucun contrôle éditorial sur les messages envoyés et reçus dans le cadre de la messagerie électronique. L'utilisateur le reconnaît et l'accepte. L'Université ne pourra, de ce fait, être tenue pour responsable des messages échangés.

Article 9 - Sanctions

Suspension de l'accès aux services

En cas de non respect des règles définies dans la présente charte, le Président de l'Université peut sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre de l'utilisateur, limiter ou interdire les usages par mesure conservatoire.

Sanctions disciplinaires

Le non respect des règles établies ou rappelées par la présente charte peut donner lieu à sanctions disciplinaires. Indépendamment de l'engagement d'éventuelles actions en justice, notamment au plan pénal.

Les sanctions encourues par l'utilisateur sont déterminées par chacune les dispositions règlementaires relatives à son statut.

Article 10 - Responsabilité et devoirs de l'Université

L'établissement ne pourra être tenu pour responsable de détérioration d'informations du fait d'un utilisateur ne s'étant pas conformé à l'engagement qu'il a accepté par validation de la présente charte. L'établissement ne fournit aucune garantie, implicite ou explicite, quant à l'exactitude des résultats obtenus par l'utilisation de ses moyens informatiques.

Article 11. Entrée en vigueur de la charte

La présente charte est adoptée par le Conseil d'Administration et prend effet immédiatement.

Elle est accessible sur le site institutionnel de l'Université.

Aucun accès aux ressources numériques ne sera autorisé sans approbation préalable de la présente charte par l'utilisateur.

UNIVERSITÉ D'ARTOIS

CHARTE REGISSANT L'USAGE
DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
PAR LES USAGERS DE L'UNIVERSITE D'ARTOIS

Annexe I

ANNEXE JURIDIQUE

1. Préambule

La présente annexe juridique a pour objet d'exposer à l'«utilisateur» les principales règles légales applicables, de manière non exhaustive. Ces règles en particulier ne sont pas exclusives de celles qui s'imposent à tout agent public notamment en ce qui concerne l'obligation de neutralité (religieuse, politique et commerciale), de réserve, de discrétion professionnelle et de respect des secrets protégés par la loi.

Les textes de références sont disponibles sur les sites institutionnels, notamment sur le site Legifrance : **http://www.legifrance.gouv.fr/**

2. La protection des données nominatives

Les données nominatives font l'objet d'une protection légale particulière dont la violation expose son auteur à des sanctions pénales

Les textes applicables en la matière sont les suivants :

- la loi n° 78-17 du 6 janvier 1978, modifiée par la loi n° 2004-801 du 6 août 2004, relative à l'informatique, aux fichiers et aux libertés ;
- la convention n° 108 du Conseil de l'Europe du 28 janvier 1980 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel ;
- la directive n° 95/46 des communautés européennes du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Ces règles s'appliquent à l'ensemble des systèmes de traitement de l'information dès lors que cette information permet d'identifier un ou plusieurs individus.

La loi du 6 janvier 1978, modifiée par la loi n°2004-801 du 6 août 2004, a créé un dispositif juridique pour encadrer la mise en œuvre des «traitements automatisés d'informations nominatives» et ouvrir aux individus un droit d'accès et de rectification sur les données les concernant détenues et gérées par des tiers.

Cette loi impose de procéder à une déclaration et / ou une demande d'avis auprès de la CNIL préalablement à la mise en œuvre d'un traitement automatisé d'informations nominatives.

Toute personne auprès de laquelle sont collectées (oralement ou par écrit) des informations mises en œuvre dans un système automatisé de traitement doit être informée :

- du caractère obligatoire ou facultatif des réponses,
- des conséquences d'un défaut de réponse,
- de l'identité des destinataires des informations,
- de l'existence d'un droit d'accès et de rectification,
- de l'identité du responsable du traitement,
- des finalités du traitement auquel les données sont destinées,
- si les données sont destinées à être communiquées à des pays tiers à l'union européenne,
- si les données sont destinées à être utilisées à des fins de prospection, ou à être communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection, et d'avoir la possibilité de s'y opposer.

3. La protection des personnes

Ainsi qu'il l'a été précédemment évoqué, les traitements automatisés d'informations nominatives sont strictement réglementés par la loi du 6 janvier 1978, modifiée par loi n°2004-801 du 06 août 2004. Les dispositions relatives aux personnes sont identiques à celles décrite pour les données nominatives dans le point précédent.

La violation de la loi précitée entraîne des sanctions pénales.

4. La protection des droits de propriété intellectuelle

4-1. Les règles de protection du droit d'auteur

En vertu des règles du code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création «d'un droit de propriété incorporel et exclusif opposable à tous».

Cette disposition s'applique à toutes les œuvres de l'esprit quel qu'en soit le genre, la forme d'expression, le mérité ou la destination.

Sont notamment considérées comme des œuvres de l'esprit, au sens du code de la propriété intellectuelle et en particulier de l'article L112-2 les œuvres suivantes :

- les livres, brochures et autres écrits littéraires, artistiques et scientifiques,
- les conférences, allocutions et autres œuvres de même nature,
- les œuvres dramatiques ou dramatico-musicales,
- les œuvres chorégraphiques,
- les œuvres musicales avec ou sans paroles,
- les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensembles œuvres audiovisuelles,
- les œuvres de dessins, de peintures, d'architectures, de sculptures, de gravures, de lithographies,
- les œuvres graphiques et typographiques ,
- les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie,
- les œuvres d'art appliqué,
- les illustrations, les cartes géographiques,
- les logiciels, y compris le matériel de conception préparatoire.

Les actes de reproduction en tout ou partie, par tout moyen et sous toute forme sont ainsi soumis à l'autorisation du /ou des titulaires des droits sur les œuvres.

L'utilisation de ces œuvres suppose donc une acceptation préalable du / ou des titulaire(s) des droits.

L'«utilisateur» est donc informé qu'à défaut d'une autorisation express du / ou des titulaire(s) respectant les dispositions du code de la propriété intellectuelle, il lui est interdit d'utiliser une telle œuvre. A défaut, sa responsabilité civile et / ou pénale peut être engagée.

4-2. les règles de protection des logiciels

Les logiciels son protégés par le droit d'auteur.

Toute reproduction, adaptation et /ou distribution du logiciel n'est autorisée que sous réserve du consentement du titulaire des droits sur ledit logiciel.

L'étendue et les caractéristiques des droits conférés sont définies en général par des contrats de licence d'utilisation des logiciels visés.

L'utilisation du logiciel, même à des fins d'essais, de démonstration de courte durée ou à des fins pédagogiques et à défaut d'autorisation expresse et écrite du titulaire des droits est en principe interdite.

L'«utilisateur» d'un logiciel s'expose à des sanctions civiles et pénales prévues et réprimées par le code de la propriété intellectuelle lorsqu'il utilise un logiciel sans autorisation.

Afin de prévenir les risques liés à la contrefaçon de logiciel, une vigilance particulière de l'«utilisateur» comme de leur autorité hiérarchique est indispensable.

Est un délit de contrefaçon puni par le code de propriété intellectuelle, (articles L.335-3 du code de la propriété intellectuelle) toute reproduction, représentation ou diffusion, par quelque moyen que ce soit,

d'une œuvre de l'esprit en violation des droits de l'auteur ainsi que la violation de l'un des droits de l'auteur d'un logiciel.

4-3. Les règles de protection des données

De la même façon, les données telles que les textes et, dès lors que ceux-ci présentent une certaine originalité, les images et les sons sont protégés par le droit d'auteur.

L'autorisation écrite du titulaire des droits est ainsi nécessaire pour leur utilisation.

Le non-respect des dispositions relatives à la protection des droits de l'auteur sur ces données est constitutif de contrefaçon et donc soumis aux sanctions pénales prévues par la loi.

D'une manière générale, la difficulté à connaître précisément l'origine des données transmises et donc les droits y afférents, en particulier avec le développement des moyens d'échanges d'informations en réseau ouvert comme internet, oblige l' «utilisateur» à la plus grande prudence.

4-4. Les règles de protection des bases de données

On entend par bases de données un recueil d'œuvres de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données sont protégées par le code de la propriété intellectuelle indépendamment de la protection dont peuvent bénéficier les données au titre du droit d'auteur contenu dans la dite base.

Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, bénéficient des dispositions du code de la propriété intellectuelle.

L'«utilisateur» est susceptible de se rendre coupable de contrefaçon dans plusieurs cas :

lorsqu'il procède à toute extraction par transfert permanent ou temporaire de la totalité ou en partie, qualitativement ou quantitativement substantielle, du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;

d'autre part, par la réutilisation ou par la mise à disposition de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base quelle que soit sa forme.

A ce titre, un «utilisateur» des bases de données de l'Université ne saurait s'autoriser à utiliser à des fins privées par exemple un fichier d'adresses, dont l'Université est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au code de la propriété intellectuelle.

5. La protection des marques

Le code de la propriété intellectuelle protège toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale (article L711-1).

Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblage de mots, nom patronymique, nom géographique pseudonyme, lettre, chiffre, sigle, emblème, photographie, dessin, empreinte, logo ou la combinaison de certains d'entre eux.

Ces droits et leur protection sur une marque confèrent à son titulaire par un enregistrement un droit de propriété sur cette marque. L'«'utilisateur» ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque, ainsi qu'utiliser une marque protégée ainsi que de supprimer ou modifier une marque régulièrement déposée.

L'«utilisateur» s'interdit donc, sauf autorisation express du propriétaire, toute reproduction ou usage ou apposition d'une marque ainsi que l'usage d'une marque reproduite pour des produits ou services identiques à ceux désignés dans l'enregistrement, la suppression ou la modification d'une marque.

L'utilisateur ne saurait utiliser une marque sur laquelle l'Université ne détient pas l'autorisation expresse d'utilisation dans le cadre de ses fonctions.

Il lui sera outre interdit d'utiliser à des fins privée toutes marque dont l'Université est titulaire.

6. la protection des systèmes d'information.

(articles 323-1 à 323-3-1 du code pénal)

Les atteintes aux systèmes d'information en tant que systèmes de traitements automatisés de données sont sanctionnées au titre de la réglementation sur la fraude informatique contenue aux articles 323-1 et suivants du code pénal.

Ce dernier interdit notamment :

- L'accès illicite, c'est-à-dire toute introduction dans un système informatique par une personne non autorisée (articles 323-1 du code pénal). La notion d'accès s'entend de tout système de pénétration tel que la connexion pirate tant physique que logique, l'appel d'un programme alors que l'on ne dispose pas d'habilitation, l'interrogation d'un fichier sans autorisation.
- Le maintien frauduleux, c'est à dire le maintien sur le système informatique après un accès illicite et après avoir pris conscience du caractère «anormal» de ce maintien (article 323-3 du code pénal). Le maintien frauduleux est notamment caractérisé par des connexions, visualisation ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est «anormal».
- Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 susvisés .
- L'entrave du système, c'est à dire toute perturbation volontaire du fonctionnement d'un système informatique (article 323-2 du code pénal).
- L'entrave au système est appréhendée de manière extrêmement large car il suffit d'une influence «négative» sur le fonctionnement du système pour que le concept d'entrave soit retenu.
- L'altération des données, c'est à dire toute suppression, modification ou introduction de données «pirates», avec la volonté de modifier l'état du système informatique les exploitant et ce, quelle qu'en soit l'influence (article 323 code pénal).

Il en est ainsi pour les bombes logiques, l'occupation de capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal.

Par ailleurs, la création de faux et leur usage constitue un délit autonome sanctionné au titre de faux en écriture privée, publique ou de commerce.

L'utilisateur doit impérativement adopter un comportement exempt de toute fraude car à défaut, il s'expose à de sévères sanctions pénales et disciplinaires.

7. le secret des correspondances

L'«utilisateur» est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende « le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination adressées à des tiers, ou d'en prendre frauduleusement connaissance, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises ou transmises par la voie de télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ». (article 226-15 du code pénal).

Il est également informé qu'est puni de trois ans d'emprisonnement et de 45 000 euros d'amende, «le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances... » (article 432-9 du code pénal).

8. La responsabilité en matière de transmission des informations

Les moyens informatiques mis à la disposition de l'«utilisateur» permettent l'accès à une communication et à une information importante et mutualisée.

Or, de tels moyens de communication ne doivent pas permettre de véhiculer n'importe quelle information ou donnée. Ainsi, le code pénal dans ses articles 227-23 et 227-24, sanctionne le fait de fabriquer, de

transporter, de diffuser, par quelque moyen que ce soit et quel que soit le support, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message de trois ans d'emprisonnement et de 75 000 euros d'amende.

Est également puni de trois ans d'emprisonnement et de 45 000 euros d'amende, le fait de fixer, d'enregistrer ou de transmettre en vue de sa diffusion l'image d'un mineur lorsque cette dernière présente un caractère pornographique et de diffuser une telle image, par quelque moyen que ce soit.

Est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende, «le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit».

9. Le respect de la vie privée

9-1. Le droit à la vie privée

Le principe est posé par l'article 9 du code civil qui prévoit que «chacun a droit au respect de sa vie privée».

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestres ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée.

9-2. Droit à l'image

L'«utilisateur» est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende, le fait au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui :

1. - En captant, enregistrant ou transmettant, sans le consentement de leur auteur des paroles prononcées à titre privé ou confidentiel ;
2. - En fixant, enregistrant ou transmettant, sans le consentement de celle-ci l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés ci-dessus ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de faire, le consentement de ceux-ci est présumé » (article 226-1 du code pénal).

9-3. Le droit de représentation

L'«utilisateur» est informé qu'est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (article 226-8 du code pénal).

10. Les règles de preuve

Le principe est celui de la liberté de preuve qui peut donc être rapportée par tout moyen.

A ce titre, l'«utilisateur» est informé qu'un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'Université ainsi que la sienne.

Il est nécessaire que chaque « utilisateur» respecte scrupuleusement la législation en vigueur car le non-respect de cette obligation est passible de sanctions pénales.