C2I Certificat Informatique et Internet

Module A2 – Première partie

Plan de la présentation :

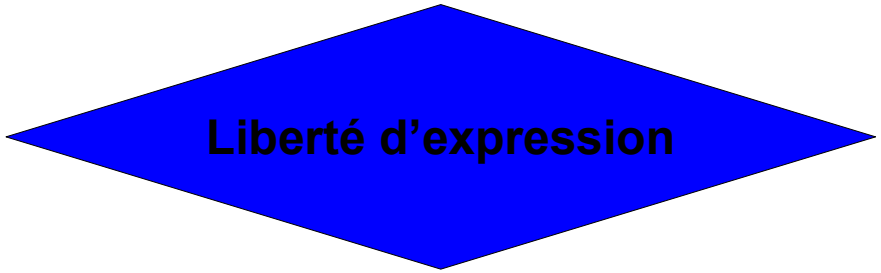
1) Respecter les droits fondamentaux de l'homme, les normes internationales et les lois qui en découlent.
2) Maîtriser son identité numérique.
3) Sécuriser les informations sensibles (personnelles et professionnelles) contre les intrusions frauduleuses, les disparitions, les destructions volontaires ou involontaires.
4) Assurer la protection de la confidentialité. Virus, cheval de Troie, anti-virus, pare feu..

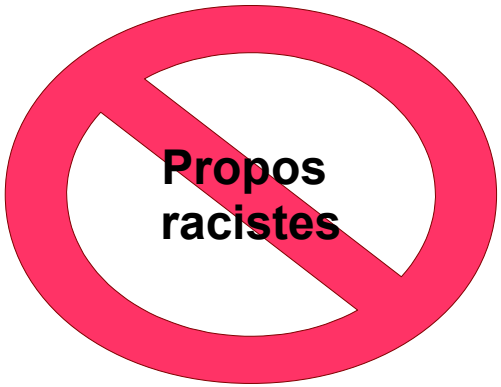
Internet et le Droit

Internet est un moyen de communication. Il n'est donc pas plus extérieur au droit que le téléphone, les journaux ou la télévision.
De plus, certaines lois ont même été votées spécifiquement pour tenir compte ou s'appliquer à Internet.
Internet étant international, le problème essentiel sera de déterminer, cas par cas, quel droit national s'applique. Mais si un litige survient entre un internaute français et un responsable de serveurs basés en France, le droit français s'applique évidemment.

Respecter le Droit : liberté d'expression

Internet étant un outil de communication, on doit y respecter les règles qui sont liées à ces outils... que ce soit dans les forums, les blogs, les sites web, les envois de courriels sur des listes de diffusion...





La liberté de chacun s'arrête où commencent les droits des autres. Le respect dû aux autres est la contrepartie du respect que l'on nous doit.

Respecter le Droit : respect des données personnelles - 1

Les données personnelles sont protégées en France par la loi dite « informatique et libertés » (datant de 1978 et remaniée en août 2005). Des lois similaires existent dans tous les pays européens et, sous une forme ou une autre, les données personnelles sont protégées dans de nombreux autres pays.

Article 1er

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 2

(...) Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, (...)

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Une adresse électronique (courriel ou IP), un code (code client par exemple), un surnom... identifient des personnes

Respecter le Droit : respect des données personnelles - 2

La Loi fixe comme principe le respect des données personnelles. Leur collecte est strictement encadrée et limitée. Les personnes concernées ont un droit d'accès à ce qui les concerne (et de rectification des erreurs).
Si certains traitements de données personnelles peuvent se faire sans formalité (un carnet d'adresses personnel par exemple), le principe reste que tout traitement doit être déclaré auprès de la CNIL (Commission Nationale Informatique et Liberté). La CNIL tient un registre des traitements déclarés, avec un contact auprès duquel s'exerce le droit d'accès et de rectification. Certains traitements particuliers nécessitent une autorisation préalable avant d'être mis en oeuvre (par exemple : si on stocke des données biométriques). Dans tous les cas, la CNIL peut exiger des modifications ou interdire un traitement de données.
Ne pas respecter les procédures, garantes des droits de chacun, est passible de un an de prison et de 15 000 à 150 000 euros d'amende.

CNIL
COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

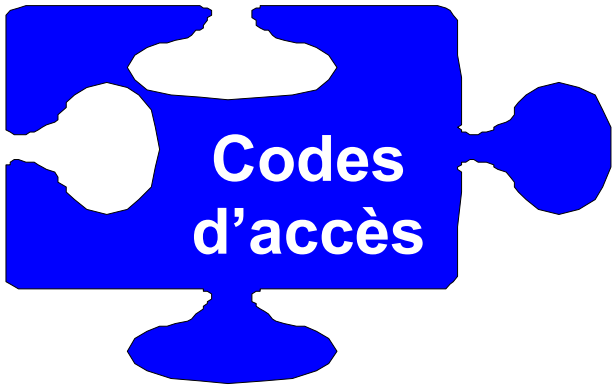
Toutes les informations sur le site web de la CNIL :
http://www.cnil.fr

De nombreuses procédures peuvent être réalisées en ligne en quelques minutes.

Maîtriser son identité numérique

Qui aurait l'idée de se promener avec des liasses de billets dépassant de ses poches ? Qui distribuerait la clé de son appartement (avec son adresse) à tous les passants dans la rue ?
Pourtant, de nombreuses personnes agissent comme cela sur Internet...

Son identité numérique est constituée de tous les éléments pouvant identifier un individu sur Internet ou dans des traitements informatiques.
Ces éléments sont précieux. Il ne faut pas les diffuser sans précaution.



Préserver son identité numérique : Bonnes pratiques

1) **Avant de transmettre une information personnelle, il faut s'assurer de l'identité de son interlocuteur.** Avant de remplir un formulaire sur un site web, suis-je bien sur que je peux avoir confiance dans ce site ? Ce site est-il bien ce qu'il prétend être ou une imitation (comme une imitation de site de banque) ?

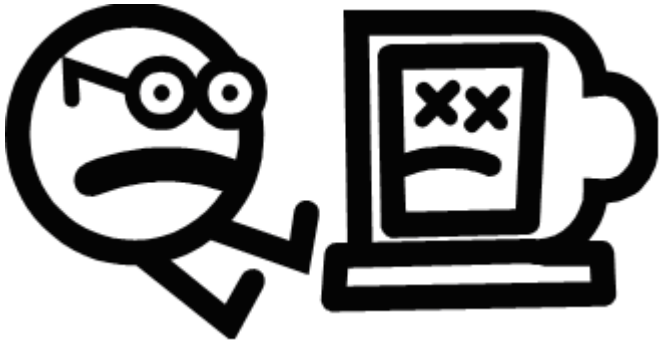
2) **L'information requise est-elle logique ?** Donner un numéro de carte bancaire est nécessaire pour payer. Mais pas donner son code secret !

3) **L'interlocuteur qui me demande une information est-il crédible ?** Si mon banquier, qui ne dispose pas de mon adresse de courrier électronique, m'envoie un courriel pour me demander mon numéro de compte, est-ce normal ? Il y a plutôt de fortes chances que celui qui se fait passer pour mon banquier soit un escroc...

4) **Mon interlocuteur prend-il lui-même des précautions avec les informations que je vais lui confier ?** L'affaire Tati contre Kitetoa a démontré que ce n'était pas toujours le cas... Le site web Kitetoa avait ainsi révélé que les numéros de cartes bancaires des clients de la boutique en ligne de Tati étaient stockés sur le site web de manière accessible.

5) **Internet a de la mémoire...** Avant de noter quelque chose sur un blog ou dans un forum, il faut s'assurer que ce quelque chose ne peut pas me nuire ultérieurement. A tout moment, un moteur de recherche peut retrouver (même accidentellement) un commentaire gênant que j'aurais posté quelques années auparavant...

Préserver ses données personnelles : les sauvegardes



Un ordinateur peut tomber en panne.
Il peut être cassé.
Il peut être volé.

Tout ce qu'il contient peut être détruit à tout moment.

On peut aussi détruire accidentellement des données.

Tout ce qui a de l'importance ou de la valeur doit donc être sauvegardé sur des supports amovibles (par exemple : un CD-Rom). Le niveau de sauvegarde doit être en rapport avec l'importance des données.

Ainsi, sauvegarder en dix exemplaires un document que l'on va détruire deux jours plus tard n'a pas de sens.
Ne pas sauvegarder en au moins deux exemplaires situés dans deux endroits différents une thèse ou un rapport de stage est de l'inconscience.

Préserver ses données personnelles : la sécurité

Etes-vous seul à accéder à cet ordinateur sur lequel vous stockez des données personnelles ?

Les personnes pouvant accéder à cet ordinateur ont-elles bien le droit de prendre connaissance de tout ce qui s'y trouve ?

Pour préserver le secret de documents, le plus simple est de ne jamais les rendre accessibles. Si un ordinateur est personnel, il est en général simple de le protéger par un mot de passe. Mais de telles méthodes ont des limites face à des personnes ayant des connaissances techniques.

Un document lui-même peut être protégé. Certains programmes proposent ainsi de ne permettre l'ouverture des documents qu'après avoir tapé un mot de passe. Le niveau de protection offert et sa résistance face à une personne mal intentionnée est variable selon le type de document.
Il est aussi possible de crypter un document (voir ci-après).

Le cryptage

Qu'est-ce que le cryptage ? A quoi sert-il ? Comment ça marche ?

Le cryptage sert à protéger des fichiers contre une appropriation non désirée. Même récupéré, un fichier crypté est normalement inutilisable par son possesseur s'il ne possède pas le moyen de décrypter. Seul le fichier crypté doit être échangé. Le fichier initial "en clair" doit rester sur votre disque dur ou, mieux, être détruit ou sauvegardé uniquement sur un support amovible.

L'algorithme de cryptage peut reposer soit sur une paire de clés privée/publique (la clé privée pouvant être protégée par un mot de passe), soit sur une clé avec mot de passe.

Clé privée/clé publique ou mot de passe ?

Un programme de cryptage comme PGP utilise le principe de la paire de clés publique/privée ou PKI (Public Key Infrastructure), également appelée Architecture à Clés Asymétriques. Les système à mot de passe sont plutôt internes à des programmes (comme Word ou OpenOffice).
Clés publiques et clés privées sont de petits fichiers informatiques servant à sécuriser d'autres fichiers lors d'un échange ou d'un stockage par du cryptage. Elles contiennent des paramètres utilisées par l'algorithme de cryptage. Dans ce cas, pour crypter un fichier, il faut posséder la clé publique du destinataire. Pour décrypter un fichier, il faut posséder la clé privée de celui-ci. Normalement, seul le propriétaire légitime d'une clé privée la possède... et ne l'a pas perdue.
Dans le cas d'un algorithme reposant sur un simple mot de passe, aucune "clé" n'est à échanger entre celui qui a crypté un fichier et son destinataire. Le cryptage ne repose en effet que sur les caractères composant le mot de passe.

La signature électronique

L'article 1316-4 du Code Civil donne la même force probante à une signature qu'elle ait été réalisée électroniquement ou grâce à un stylo. L'objectif d'une signature est de prouver que l'individu ayant signé est d'accord avec le contenu du document signé, dont l'intégrité doit donc être garantie. L'identité du signataire doit également être démontrée.
La signature électronique repose sur les certificats. Un certificat est une clé publique (voir ci-avant) dont le titulaire a son identité certifiée par un tiers de confiance, l'autorité de certification (comme une préfecture certifie une carte d'identité ou un passeport). Le certificat est utilisé, combiné à une empreinte numérique du document, pour signer celui-ci. L'empreinte garantit l'intégrité du document, le certificat l'identité du signataire. La norme la plus courante de certificats, recommandée par les organismes de normalisation, est la X509. Cette norme garantit que la plupart des logiciels pourront utiliser le certificat : messagerie, cryptographie,…
Le certificat peut être révoqué s'il a été perdu par son titulaire (ou volé) ou automatiquement au bout d'un certain temps (à la fin d'un contrat, d'une mission). La reconnaissance d'un certificat suppose donc d'interroger l'autorité qui l'a délivré pour vérifier sa validité. Les logiciels lisant les certificats font cette interrogation auprès du serveur de l'Autorité automatiquement ou manuellement.
La création et la gestion d'un certificat se réalise grâce à trois intervenants qui peuvent être regroupés en une ou deux entités. L'autorité de certification (AC) décide des règles de délivrance et de gestion des certificats réalisés sous son autorité. L'autorité d'enregistrement (AE) exécute ces règles en délivrant effectivement les certificats aux titulaires. L'opérateur de certification (OC) fournit l'infrastructure matérielle et logicielle requise.
La seule signature peut être insuffisante pour donner une valeur juridique à un document. La date et l'heure de celle-ci peut être essentielle, d'où la notion d'horodatage, également réalisée par des tiers de confiance.

Les menaces contre la sécurité de son ordinateur : les virus

Le terme de *virus* est devenu très général et englobe aujourd'hui pratiquement tous les types de programmes malicieux pouvant infecter un ordinateur.

Certains virus visent à détruire des données. D'autres sont des Chevaux de Troie et visent à permettre à un pirate de prendre le contrôle de la machine d'un utilisateur pour voler son contenu (notamment des données personnelles ou professionnelles confidentielles) ou l'utiliser pour commettre des délits (par exemple : utiliser sa connexion Internet pour attaquer un autre ordinateur en se faisant passer pour l'utilisateur infecté).

Il faut avoir un logiciel anti-virus sur tout ordinateur : il détecte et détruit les virus

Les virus sont des programmes. Ils se transmettent comme tous les autres programmes (par un envoie sur Internet, par un CD...). Ils ne peuvent se reproduire que grâce à un ordinateur infecté (qui peut alors propager le virus vers d'autres ordinateurs, notamment en s'envoyant par courrier électronique à tout le carnet d'adresse présent sur la machine).

Les menaces contre la sécurité de son ordinateur : les intrusions et les communications non autorisées

Un pirate peut chercher à prendre possession de votre machine en s'y connectant comme on peut se connecter à n'importe quel ordinateur. Il peut y avoir des failles dans votre système informatique qui lui permettront de se rendre maître de celui-ci.

A l'inverse, des programmes peuvent tenter de communiquer avec l'extérieur, y compris pour transférer des données personnelles, sans que vous le souhaitiez.

Le rôle d'un logiciel pare-feu est d'analyser ce qui entre ou qui sort de votre ordinateur par les réseaux informatiques et de bloquer les flux de données qui ne sont pas conformes à vos désirs.

Il faut avoir un logiciel pare-feu sur tout ordinateur : il détecte et bloque les intrusions