Domaine D2 : Être responsable à l'ère du numérique

D2.1 Maîtriser son identité numérique privée, institutionnelle et professionnelle.

D2.2 Veiller à la protection de la vie privée et des données à caractère personnel.

D2.3 Être responsable face aux réglementations concernant l'utilisation de ressources numériques.

D2.4 Adopter les règles de bon usage du numérique.

Chafik Aloulou, Mohamed Koutheir khribi, Walid chaou, Nizar Kayati, Lilia Cheniti, Sonia Guanouchi et Houda Houissa

D2.1 : Maîtriser son identité numérique privée, institutionnelle et professionnelle

1. L'identité numérique

L'ensemble des activités qu'un usager réalise sur Internet contribuent à définir son identité numérique.

L'identité numérique d'un usager se construit donc à partir de plusieurs éléments :

- les données personnelles associées à son ou ses profils ;
- les informations qu'il publie sur le web ;
- les informations que d'autres publient à son sujet ;
- les traces qu'il laisse consciemment ou non.

Selon le contexte, l'usager peut utiliser des identifiants différents :

- les **identifiants professionnels** ou **institutionnels** créés par l'employeur et liés à l'activité professionnelle, permettant souvent d'accéder à un environnement numérique de travail ;
- les **identifiants privés**, qu'ils soient créés à l'initiative de l'usager pour accéder à des services en ligne pour son usage personnel (réseau social, vente en ligne, messagerie, banque en ligne, fournisseur d'accès à internet, etc.) ou qu'ils lui soient donnés dans le cadre des services publics en ligne (déclaration des impôts en ligne, etc.).

Pour maîtriser son identité numérique :

- l'usager choisit judicieusement l'identifiant à utiliser en fonction de son activité ;
- l'usager limite l'accès aux informations qu'il publie ;
- l'usager contrôle régulièrement son image sur le web ou e-réputation.

2. L'authentification

L'authentification est la procédure qui contrôle que les informations de connexion fournies (identifiant et mot de passe, empreintes digitales, etc.) sont correctes. On peut avoir besoin de s'authentifier pour accéder à un service ou une ressource spécifique.

Il est primordial de respecter certaines règles élémentaires :

- garder le **mot de passe secret** (ne pas le donner à une connaissance, ne pas le copier sur un agenda ou sur un post-it à côté de l'ordinateur, etc.) ;
- choisir un **mot de passe complexe** composé d'au moins dix caractères combinant obligatoirement lettres minuscules, lettres majuscules, chiffres et symboles. Le mot qui en résulte ne doit avoir aucune signification évidente (exclure les dates de naissance, prénom, mots du dictionnaire, etc.), de façon à empêcher une personne de le deviner ou un logiciel malveillant de le « craquer » facilement.
- L'**usurpation d'identité** est le fait de prendre délibérément l'identité d'une autre personne.

3. Le paramétrage du profil

Chaque identifiant de connexion peut être associé à un profil contenant des informations diverses : photos, informations personnelles (date de naissance, ville, adresse électronique, téléphone, etc.) et des préférences (musique, film, citation, etc.).

En général, il est possible de paramétrer l'accès à ces informations. On distingue :

- l'**accès public** ou « à tout le monde » : ces informations sont accessibles de tous et peuvent être référencées par les moteurs de recherche ;
- l'**accès restreint** à une communauté : ces informations ne sont accessibles qu'à certaines personnes autorisées et par conséquent, elles ne peuvent pas être référencées par les moteurs de recherche.

Dans le cas particulier du courrier électronique :

Il existe deux façons d'ajouter automatiquement une signature à ses courriels : on peut rédiger un texte qui s'ajoute à la fin du message ou joindre une carte de visite électronique.

4. Les traces numériques

Que peut-on trouver dans les propriétés d'un fichier ?

- S'il s'agit d'un fichier de bureautique : la date, l'heure, le nom du créateur et du dernier contributeur, le nombre de révisions, etc.
- S'il s'agit d'une photo numérique : la date et l'heure du cliché, le modèle de l'appareil photo, etc.

Que peut-on savoir de l'identité d'un internaute ?

- Tout ordinateur connecté à Internet est identifié par une **adresse IP**. Cette adresse est attribuée par le fournisseur d'accès à Internet (FAI), qui doit conserver pendant un an le journal des connexions et les informations permettant d'identifier l'internaute.
- Quand on consulte une page web, le navigateur envoie une requête au serveur hébergeant cette page pour récupérer les données (textes, images, etc.) à télécharger. Cette requête contient des **variables d'environnement** décrivant l'ordinateur de l'internaute, notamment l'adresse IP, le système d'exploitation, la version du navigateur et la résolution de l'écran. Le serveur web peut garder ces traces et suivre ainsi la navigation sur le site !
- Dans l'en-tête de chaque courriel est stockée une série d'adresses IP décrivant les serveurs par lesquels transite le courriel ; ces adresses peuvent fournir des indices sur la localisation géographique de l'expéditeur.

5. La e-réputation

La e-réputation ou réputation numérique est l'image que l'on peut se faire d'une personne à travers le web. Il faut être conscient que :

- **tout le monde peut publier sur le web sans aucun contrôle** : sur un blog ou un réseau social, en participant à un forum de discussion, en publiant un site chez un hébergeur, etc.
- **on perd la maîtrise d'une information publiée avec un « accès public » :** à partir du moment où une information est publique, elle peut être indexée par les moteurs de recherche et recopiée dans leur cache. Elle peut mettre plusieurs mois à disparaître.

D2.2 : Veiller à la protection de la vie privée et des données à caractère personnel

1. Les atteintes à la vie privée

Il faut être conscient que l'évolution des nouvelles technologies de l'information et de la communication, issues du développement de l'informatique, d'Internet et des télécommunications, peut porter atteinte à la vie privée.

Quelles sont les dérives possibles ?

- La collecte et le traitement automatique de l'information : beaucoup d'informations personnelles sont stockées sous forme numérique dans des fichiers. L'**interconnexion de ces fichiers** peut être préjudiciable à la vie privée et aux libertés individuelles.
- L'usage des NTIC se démocratise et **tout le monde peut publier sur le web** sans difficulté à travers les réseaux sociaux, les blogs, les forums, etc. Ces informations sont publiées sans aucun contrôle et peuvent contenir des informations personnelles.
- Le courrier électronique est devenu un mode de communication utilisé au quotidien : il existe des règles à respecter concernant le **secret de la correspondance privée**.

2. Le traitement automatique de l'information

L'**interconnexion des fichiers** peut porter atteinte aux libertés individuelles.

3. La CNIL

La **Commission Nationale de l'Informatique et des Libertés** (CNIL) est une autorité administrative indépendante française dont la mission essentielle est de protéger la vie privée et les libertés dans un monde interconnecté. Elle a été instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite loi « Informatique et Libertés »)

Les missions de la CNIL :

« La CNIL est l'autorité en charge de veiller à la protection des données personnelles. A ce titre, elle dispose notamment d'un pouvoir de contrôle et de sanction. Jouant aussi un rôle d'alerte et de conseil, elle a pour mission de veiller à ce que le développement des nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. ». Extrait du site de la CNIL (consulté le 10 août 2011).

4. La collecte d'informations

Quelques obligations des personnes responsables de la collecte des données :

- **finalité des traitements** : un fichier doit avoir un objectif précis ; les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées ;
- **durée de conservation des informations** : les données personnelles ont une date de péremption ; le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier.

- En France, tout fichier (sauf exception) contenant des données personnelles doit faire l'objet d'une déclaration à la CNIL. Le citoyen a le **droit d'accès**, de **rectification** et d'**opposition** sur les informations de ces fichiers.

5. La publication sur le web

Toute personne qui publie des informations sur le web (blog, mur, page personnelle, site web, etc.) doit être consciente de ses obligations.

- Elle doit **respecter le droit à l'image** des personnes en leur demandant l'autorisation de publier leur photo exception faite des personnages publics dans l'exercice de leur fonction et des personnes non identifiables (de dos ou dans une foule).
- Elle doit vérifier qu'**aucun commentaire délictueux** (injure, diffamation, incitation à la haine raciale, etc.) n'ait été déposé sur le site car sa responsabilité peut être engagée.
- Elle doit s'assurer des **droits d'exploitation des ressources** publiées et que les sites qu'elle référence ne soient pas illicites.
- Elle doit suivre les **directives de la CNIL** en ce qui concerne le recueil et la diffusion de données à caractère personnel.

6. La correspondance privée

Le courrier électronique relève du régime du **secret de la correspondance privée**.

Quelques précautions à prendre

- Pour rendre public le contenu d'un courriel, on doit demander l'autorisation préalable à l'expéditeur.
- Quand on transfère un courriel à un tiers, on doit s'assurer que l'expéditeur n'y verra pas d'inconvénient.
- Quand on répond à un courriel en citant le message initial dans la réponse, il faut être conscient que si on ajoute des destinataires, ceux-ci auront accès aux échanges précédents.

D2.3 : Être responsable face aux réglementations concernant l'utilisation de ressources numériques

1. La protection des œuvres

Concernant la protection des œuvres, il faut être conscient que les réglementations et les usages diffèrent d'un pays à l'autre.

En France, c'est le **droit d'auteur** qui protège les œuvres de l'esprit (texte, musique, photographie, schéma, programme informatique, etc.). Il se compose du droit moral et des droits patrimoniaux.

Le **droit moral** reconnaît la paternité de l'auteur et protège l'intégrité de l'œuvre. Ce droit est perpétuel.

Les **droits patrimoniaux** permettent à l'auteur (ou à ses héritiers) d'être rémunéré pour chaque utilisation de l'œuvre.

Une œuvre tombe dans le **domaine public** à l'expiration des droits patrimoniaux. L'œuvre peut alors être utilisée librement à condition de respecter le droit moral de l'auteur (citation et intégrité).

2. Les licences des ressources

Tout élément publié sur le web est soumis au droit d'auteur. Pour pouvoir exploiter une ressource du web, il est nécessaire de respecter la licence associée.

Une **licence** est un contrat qui régit les conditions d'utilisation et de distribution d'une œuvre.

On distingue deux types de licence : les licences libres et les licences propriétaires.

Les **licences libres** offrent :

- la possibilité d'utiliser l'œuvre pour tous les usages ;
- la possibilité d'étudier l'œuvre ;
- la possibilité de redistribuer des copies de l'œuvre ;
- la possibilité de modifier l'œuvre et de publier ces modifications.

Dans certains cas, cette licence peut imposer que toute copie ou œuvre dérivée soit diffusée avec la même licence. C'est ce qu'on appelle le copyleft, ou partage à l'identique des conditions initiales.

Les licences propriétaires définissent les conditions d'exploitation des ressources.

Voici quelques exceptions qui permettent d'utiliser une ressource sans être contraint par les termes du contrat :

- la copie privée et la représentation dans un cercle de famille ;
- les courtes citations ;
- l'exploitation à des fins pédagogiques.

3. Le téléchargement de musique et de films

On appelle communément **téléchargement,** le procédé qui consiste à rapatrier un fichier situé sur un ordinateur distant vers son propre ordinateur via Internet.

Il existe deux méthodes pour mettre à disposition des fichiers en téléchargement :

- ils peuvent se trouver **sur un serveur** c'est-à-dire un ordinateur connecté à Internet centralisant les fichiers que les internautes viennent télécharger
- ils peuvent se trouver **dans un réseau d'échange poste à poste** ou P2P ou *peer to peer* : les fichiers que les internautes vont télécharger se trouvent sur les ordinateurs des autres internautes.

Peut-on télécharger des films ou des musiques à partir d'un site web ?

- Il existe de nombreux sites de vente en ligne de musique ou de films : ils permettent de télécharger légalement des films moyennant le plus souvent une contribution financière.
- Il existe d'autres sites qui proposent de télécharger gratuitement de la musique ou des films. Le téléchargement est illégal si l'on ne respecte pas les recommandations que l'on peut trouver dans leurs conditions d'utilisation.

Peut-on télécharger des films ou des musiques à partir d'un réseau d'échange poste à poste ?

- S'il s'agit de ressources libres (domaine public ou diffusées avec l'accord de l'auteur), il n'y a aucun problème.
- Dans le cas contraire, c'est illégal (loi Hapodi).

4. L'exploitation des ressources du web

Une personne trouve sur le web un support de cours complet sur le C2i. Qu'a-t-il le droit de faire ?

S'il s'agit d'une licence libre :

- si sa licence autorise la **reproduction**, elle a le droit de le télécharger et de l'utiliser pour réviser ;
- si sa licence autorise la **distribution**, elle a le droit de l'envoyer à des amis et de le proposer en téléchargement sur son blog à condition de citer l'auteur ;
- si sa licence autorise la **modification**, elle peut l'adapter à ses besoins pour une utilisation personnelle.
- si sa licence autorise à **distribuer le support modifié** : elle doit obligatoirement citer l'auteur du support initial et respecter le copyleft s'il est imposé (c'est à dire que la distribution de ce nouveau support doit se faire avec des conditions identiques) ;
- si sa licence interdit d'en faire une **exploitation commerciale**, elle ne pourra pas le vendre directement, ni même le mettre en téléchargement sur un site rémunéré par de la publicité.

S'il s'agit d'une licence non libre (propriétaire), il faut se reporter aux termes de celle-ci.

S'il s'agit d'une ressource du domaine public : elle peut être utilisée librement à condition de respecter le droit moral de l'auteur.

5. Les licences des logiciels

Lorsqu'un ordinateur accomplit une tâche, il le fait à partir d'une liste d'instructions élémentaires codées en langage binaire. Les informaticiens ne peuvent pas écrire dans ce langage trop basique ; ils utilisent un langage intermédiaire appelé langage de programmation pour décrire les traitements à exécuter : c'est le **code source** ou programme source.

Le fait d'avoir respecté les règles du langage de programmation va permettre de générer automatiquement le programme correspondant en langage machine ou binaire : c'est le code exécutable ou **programme exécutable**.

Un **logiciel** est un ensemble de fichiers permettant d'exécuter un programme informatique.

Un **logiciel libre** est un logiciel pour lequel on dispose de 4 libertés fondamentales :

- on est libre de l'utiliser ;
- on est libre d'étudier son code source et de l'adapter à ses besoins ;
- on est libre de le redistribuer ;
- on est libre de le modifier et de le diffuser.

Un logiciel libre est souvent gratuit mais ce n'est pas une obligation. Il peut aussi être associé à des services payants.

Un **logiciel propriétaire** est un logiciel non libre.

En général, un logiciel propriétaire est diffusé sans son code source et son contrat de licence limite ses droits d'utilisation (nombre limité d'utilisateurs simultanés, reproduction interdite, …).

Un **gratuiciel** ou *freeware* est un logiciel mis gratuitement à disposition. Il peut être libre ou propriétaire.

Un **partagiciel** ou *shareware* est un logiciel propriétaire qui peut être utilisé gratuitement, en version complète ou partielle (version de démonstration), pendant une durée déterminée. Après cette période de gratuité, l'utilisateur doit payer une contribution s'il veut continuer à l'utiliser.

D2.4 : Adopter les règles en vigueur et se conformer au bon usage du numérique

1. Le bon usage du numérique

Il existe des règles de bon usage à respecter :

- en utilisant les ressources numériques d'un établissement (université, etc.) ou d'un service en ligne (forum, réseau social, chat, etc.), l'usager est soumis à une **charte d'utilisation** qui indique ce qu'il peut faire ou ne pas faire.
- en communiquant sur Internet (messagerie, forum, etc.), l'usager doit respecter des règles de bonne conduite et de politesse : c'est la **netiquette**.
- en construisant un document numérique, l'usager doit connaître et appliquer les règles de base qui le rendra **accessible à tous**, notamment aux personnes en situation de handicap.

2. Les chartes

Une **charte** est un règlement intérieur à une organisation. Il existe plusieurs types de chartes :

- **Les chartes d'établissement** spécifient ce que l'on peut faire (et surtout ne pas faire) lors de l'utilisation des ressources informatiques et des réseaux de l'établissement.
- **Les chartes de service** décrivent les règles à respecter pour utiliser un service d'internet (forum, réseau social, chat, etc.). L'usager est implicitement soumis à sa charte d'utilisation (même s'il ne l'a pas signée).
- **Les chartes de confidentialité** précisent la façon dont les informations (coordonnées personnelles, correspondances, documents, géolocalisation, etc.) pourraient être utilisées par ce service.

3. La Netiquette

Il existe une charte définissant les règles de conduite et de politesse à respecter quand on utilise les services d'Internet. C'est la **Netiquette** (l'étiquette des réseaux). Voici quelques **règles de bonne conduite** concernant l'usage du courriel électronique :

- Chaque courriel devrait avoir un sujet dans l'en-tête qui reflète le contenu du message.
- Si une information est à transmettre à plusieurs personnes qui ne se connaissent pas, il est préférable de placer leurs adresses en copie cachée (Bcc ou Cci).
- Il faut apprendre à reconnaître les canulars et à ne pas les propager.

Un **canular informatique** ou *hoax* est un courriel demandant de relayer une rumeur à tous ses contacts.

4. L'accessibilité

L'**accessibilité numérique** est le fait que les contenus numériques sont accessibles à tous.

La question de l'accessibilité concerne tous les individus, et en particulier :

- les personnes en situation de handicap (handicap visuel, moteur, cognitif, etc.) ;
- les novices dans l'utilisation des nouvelles technologies du numérique ;
- les personnes utilisant une connexion bas débit ou un terminal mobile.