Note sur l’éthique numérique

Actuellement, développer une charte d'éthique numérique est une nécessité puisque les questionnements éthiques posés par la numérisation concernent l’ensemble des fonctions de l’université algérienne.

La charte s’applique à toute personne ayant l’autorisation d’accès, de manière permanente ou temporaire, aux plateformes numériques, sites, comptes réseaux sociaux et/ou ressources matérielles et logicielles informatiques de l’université. Elle devra définir les modalités d’utilisation des ressources informatiques au sein de l’université ainsi que les conditions de sécurité que les utilisateurs doivent impérativement respecter.

Explicitement, la charte devra traiter les points suivants :

- **Gestion de l’accessibilité aux données**

Afin d’assurer la compréhension des données, de faciliter la recherche et de permettre l’accès et l’exploitation des données, les données numériques doivent être documentées, décrites, organisées et formatées selon des méthodes, formats, unités et standards de description qui sont classiques et compréhensibles par la communauté concernée. Il est nécessaire de privilégier les formats usuels et surtout les formats « ouverts » pour faciliter l’accès aux données. Si des logiciels ou outils sont nécessaires pour lire les données, il faut les mentionner.

Dans ce contexte, l’organisme universitaire doit aussi :

- Garantir le bon fonctionnement et la disponibilité des ressources informatiques avec le maintien d’une qualité du service dans la limite des moyens alloués.

- Combler l'écart entre ceux qui ont accès aux technologies numériques et ceux qui ne l'ont pas, en veillant à un accès équitable à l'information et aux ressources.

- **La sécurité des données**

La sécurité des données est relative à la protection des systèmes numériques, l'infrastructure et les utilisateurs contre les accès non autorisés, les violations de données et autres menaces de

cybersécurité. Le respect des règles élémentaires suivantes est nécessaire pour assurer la sécurité des données :

- Définir clairement les moyens d'authentification utilisés et la politique de mots de passe que l'utilisateur doit respecter ;
- Imposer la signature d'un **engagement de confidentialité** pour les utilisateurs.
- Définir les règles de sécurité que les utilisateurs doivent respecter :

  - Ne jamais confier son identifiant/mot de passe à un tiers ;
  - Signaler au service concerné toute violation ou tentative de violation suspectée de son compte informatique,
  - Ne pas utiliser ou tenter d'utiliser les comptes d'autrui ;
  - Signaler toute perte ou vol d'information et, de manière générale, tout fonctionnement suspect ou incident de sécurité ;
  - Ne pas installer, copier, modifier, ou détruire des applications sans autorisation ;

  - Ne pas utiliser les données auxquelles l'utilisateur peut accéder à des fins autres que celles prévues par ces attributions ;
  - Ne divulguer les données qu'aux personnes dûment autorisées, en raison de leurs fonctions, qu'il s'agisse de personnes physiques ou morales ;
  - Ne faire aucune copie des données non autorisées ;

  - S'assurer que seuls des moyens de communication sécurisés seront utilisés pour transférer les données ;
  - Verrouiller son poste de travail informatique dès que la session de travail du concerné est terminée.
  - Il faut restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données en cas de cessation des fonctions d'un des utilisateurs,

Pour renforcer la sécurité des données l'organisme universitaire doit mettre en place une procédure de classification **de l'information** définissant plusieurs niveaux de sécurité (ex: public, interne, confidentiel) et imposant un marquage des documents, des supports et des e-mails contenant des données confidentielles. Il faut aussi sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

- **La validité des données.**

L'organisme universitaire doit assurer un certain niveau de qualité des données produites selon plusieurs dimensions : la pertinence, l'exactitude, l'actualité, clarté et l'intelligibilité.

- La **pertinence** des données correspond à la mesure dans laquelle les besoins réels des utilisateurs sont satisfaits.
- **L'actualité** des données est relative au délai entre le point de référence auquel se rapporte la donnée et la date à laquelle elle disponible.
- L'**exactitude** des données correspond à la mesure à laquelle l'information décrit correctement l'évènement qu'elle doit présenter.
- **La clarté** des données correspond à la facilité avec laquelle les utilisateurs peuvent connaître l'existence de l'information, la localiser et la visualiser.
- L'**intelligibilité** des données est la disponibilité de métadonnées nécessaires à l'interprétation et à l'utilisation appropriée des données.

- **Propriété des ressources informatiques**

Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive de l'université ; ainsi que toutes les données hébergées dans ses équipements ou transitant dans ses réseaux. Tout accès aux ressources et réseaux informatiques de l'université est soumis à une procédure d'authentification préalable. En cas de défaillance de ces moyens ou ressources, il faut informer immédiatement la structure chargée de la maintenance.

- **Utilisation d'internet**

Les utilisateurs ayant accès à internet s'engagent impérativement à :

- Ne pas fournir des informations professionnelles ou liées à l'université sur les réseaux sociaux non-professionnels ;
- Ne pas utiliser l'internet à des fins malveillantes, frauduleuses, haineuses, diffamatoires, pornographiques ou illégales ;
- Ne pas utiliser l'internet et la numérisation comme moyens d'influence trompeuse ou négative, en particulier sur les mineurs ou les personnes à protection limitée ;
- Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus

- **Le respect de la vie privée**

L'organisme universitaire s'engage à protéger la confidentialité et l'intégrité des données à caractère personnel fournies par l'utilisation de moyens de sécurisation physiques et logiques. Aucun tiers ne peut accéder ou utiliser des données à caractère personnel à d'autres fins que l'inscription et/ou autre fonctionnalité avec consentement de l'utilisateur concerné. D'une manière générale, il faut aborder les pratiques de collecte de données, le consentement, le stockage, l'utilisation et le partage des données.

- **Protection des droits de propriété**

Les droits de propriété recouvrent un droit de l'auteur physique ou moral vis-à-vis à l'utilisation de son produit. En effet, il lui revient de décider de la manière dont ce produit va être communiqué et exploité par les utilisateurs.

Les utilisateurs ne peuvent pas prendre le produit, le modifier, le partager sans l'accord de l'auteur et doivent en indiquer toujours la source.

Il faut promouvoir l'utilisation des logiciels anti plagiats dans les différents domaines de recherche et les standardiser.

Biais et Discrimination

Aborder les biais et la discrimination pouvant survenir dans les technologies numériques, tels que les algorithmes biaisés ou les ensembles de données biaisés. Cela implique d'identifier, d'atténuer et de prévenir les résultats discriminatoires, ainsi que de promouvoir la diversité et l'inclusion dans le développement technologique et les processus de prise de décision.

- **La signature électronique**

L'autorité de certification des échanges électroniques. (Intégrité du contenu du message, identification de l'expéditeur et du destinataire, date d'émission, etc.).

- **Veille technologique**

L'ensemble de la composante universitaire (gestionnaire, enseignant, étudiant, travailleur) doit assurer une veille technologique en matière de numérisation sur les points relatifs :

- A l'utilisation et l'actualisation des connaissances et des nouveautés ;
- A la sécurité des intérêts du personnel, de l'université et du pays ;

- A la sauvegarde des droits et à la promotion des obligations.

Conception éthique et l'intelligence artificielle

L'introduction de l'intelligence artificielle dans le secteur universitaire est une étape essentielle pour favoriser l'optimisation des processus avec une productivité et une efficacité accrue des d'activités et une amélioration conséquente du service aux différents utilisateurs. D'autre part, il est nécessaire de considérer tous les défis éthiques, moraux et sociaux que l'intelligence artificielle peut présenter, et il est donc nécessaire de :

- Établir des cadres et des mécanismes pour la gouvernance éthique de l'IA, comprenant des principes, des lignes directrices et des réglementations régissant le développement, le déploiement et l'utilisation des technologies d'IA. Cela implique de traiter des questions telles que la responsabilité, la transparence et la surveillance pour garantir des pratiques d'IA responsables.

- Prendre en compte les implications éthiques des technologies émergentes telles que la réalité virtuelle, la blockchain, l'Internet des objets (IoT) et des comportements, certains logiciels tel que le chat GPT et leur impact potentiel sur les individus et la société.

Références :

https://unesdoc.unesco.org/ark:/48223/pf0000378426_fre Projet de Recommandation sur l'éthique de l'intelligence artificielle 2021.

https://www150.statcan.gc.ca/n1/pub/12-539-x/2019001/ensuring-assurer-fra.htm Lignes directrices pour assurer la qualité des données.

https://www.ibm.com/fr-fr/topics/cybersecurity Qu'est-ce que la cybersécurité ?

https://www.ifemdr.fr/charte-de-protection-des-donnees/ .

https://www.cairn.info/revue-cites-2001-4-page-103.htm : Création, droits d'auteur et propriété intellectuelle sur Internet

https://www.oecd.org/science/we-need-to-talk-about-digital-ethics.htm

https://www.gartner.com/smarterwithgartner/getting-digital-ethics-right Digital Ethics by Design: A Framework for Better Digital Business.

https://baliz.ca/etude-et-rapport/charte-des-donnees-numeriques-de-montreal-pour-les-droits-de-la-personne-le-bien-commun-et-avenir-octobre-2020.

Armony Altinier, L'accessibilité web. Normes et bonnes pratiques pour des sites plus accessibles, Eyrolles, 2012, 332 p. (ISBN 9-782212-128895).