مذكرة حول الأخلاقيات الرقمية

تطوير ميثاق للأخلاقيات الرقمية صار، حاليا، أمرًا ضروريًا لأن التساؤلات الأخلاقية التي تطرحها الرقمنة تتعلق بمجموع وظائف الجامعة الجزائرية.

يسري الميثاق على أي شخص لديه إذن وصول دائم أو مؤقت إلى منصات الجامعة الرقمية والمواقع وحسابات الشبكات الاجتماعية و / أو الموارد المادية والبرامج الإعلامية للجامعة. يجب أن يحدد الميثاق كيفيات استخدام الموارد الإعلامية داخل الجامعة وكذا الشروط الأمنية التي يجب على المستخدمين احترامها بشكل إلزامي.

وعلى وجه التحديد، يجب أن يتناول الميثاق النقاط التالية:

إدارة الوصول إلى البيانات من أجل ضمان فهم البيانات وتسهيل البحث والتمكين من الوصول إلى البيانات واستغلالها؛ يجب توثيق البيانات الرقمية ووصفها وتنظيمها وتنسيقها وفقًا للطرق والأشكال والوحدات ومعايير الوصف الكلاسيكية المتعارف عليها من قبل المجتمع المعني؛ من الضروري تفضيل الأشكال المعتادة لا سيما الأشكال "المفتوحة" لتسهيل الوصول إلى البيانات. وفي حالة ما إذا كانت هناك ضرورة إلى برامج أو أدوات لقراءة البيانات فيجب ذكرها.

وفي هذا السياق، يجب على الهيئة الجامعية، إضافة لما سبق:

- أن تضمن حسن سير وتوافر موارد إعلامية مع الحفاظ على جودة الخدمة في حدود الموارد المخصصة.

- سد الفجوة بين أولئك الذين لديهم إمكانية الوصول إلى التقنيات الرقمية وأولئك الذين هم محرومون منها، وذلك من خلال السهر على ضمان الوصول العادل إلى المعلومات والموارد.

- أمن البيانات

يتعلق أمن البيانات بحماية الأنظمة الرقمية والبنية التحتية والمستخدمين ضد الوصول غير المصرح به وانتهاكات البيانات وغيرها من تهديدات الأمن السيبراني. يعد الامتثال للقواعد الأساسية التالية ضروريًا لضمان أمن البيانات:

- التحديد الواضح لوسائل المصادقة المستخدمة وسياسة كلمات المرور التي يجب على المستخدم احترامها؛

• فرض توقيع التزام سرية للمستخدمين.

• تحديد قواعد الأمن التي يجب على المستخدمين اتباعها:
• عدم تمكين طرف ثالث من اسم المستخدم / كلمة المرور؛
• إبلاغ المصلحة المعنية بأي انتهاك أو محاولة انتهاك مشتبه به أو محاولة انتهاك حساب الكمبيوتر الخاص به؛
• عدم استخدام أو محاولة استخدام حسابات الآخرين؛
• الإبلاغ عن أي فقدان أو سرقة للمعلومات، وبشكل عام، الإبلاغ عن أي عملية مشبوهة أو حادث أمني؛
• عدم القيام بتثبيت التطبيقات أو نسخها أو تعديلها أو إتلافها بدون إذن؛
• عدم استخدام البيانات التي يمكن للمستخدم الوصول إليها لأغراض أخرى غير تلك المنصوص عليها في هذه الصلاحيات؛
• عدم الكشف عن البيانات إلّا للأشخاص المصرح لهم حسب الأصول، بحكم وظائفهم، سواء أكانوا أشخاصًا طبيعيين أم اعتباريين؛
• عدم القيام بأي نسخ، غير مرخص به، للبيانات؛

• التأكد من استخدام وسائل الاتصال الآمنة، حصريا ودون غيرها، لنقل البيانات؛

• قفل الحاسوب عند مجرد الانتهاء من العمل؛

• يجب استرجاع البيانات والملفات المعلوماتية وأي دعامة معلومات متعلقة بهذه البيانات بالكامل في حالة إنهاء مهام أحد المستخدمين، لتعزيز أمن البيانات ، يجب على الهيئة الجامعية أن تضع إجراءً لتصنيف المعلومات يحدد عدة مستويات للأمن (على سبيل المثال ، عامة ، داخلية ، سرية) وفرض علامات على الوثائق والمستندات ورسائل البريد الإلكتروني التي تحتوي على بيانات سرية. يجب أيضًا توعية المستخدمين بالمخاطر المرتبطة بالأمن المعلوماتي.

- **صحة البيانات.**

يجب أن تضمن المؤسسة الجامعية مستوى معينًا من جودة البيانات المنتجة وفق عدة أبعاد: الملاءمة والدقة والتحيين والوضوح وإمكانية الفهم.

• ملاءمة البيانات تتمثل في مدى تلبية احتياجات المستخدم الحقيقية.
• يرتبط تحيين البيانات بالمدة بين النقطة المرجعية التي تتعلق بها البيانات وتاريخ توفرها.
• دقة البيانات تتمثل في المدى الذي تصل إليه المعلومات في وصف الحدث المقصود تقديمه بشكل صحيح.

• يشير مصطلح "وضوح البيانات" إلى السهولة التي يمكن للمستخدمين من خلالها معرفة وجود المعلومات وتحديد موقعها ومشاهدتها.

• قابلية فهم البيانات هي توافر البيانات الوصفية اللازمة لتفسير البيانات واستخدامها بشكل مناسب.

- ملكية الموارد المعلوماتية

جميع الموارد المعلوماتية المتاحة للمستخدمين هي ملكية حصرية للجامعة؛ وكذلك جميع البيانات التي تستضيفها أجهزتها أو تمر عبر شبكاتها. يخضع كل وصول إلى موارد والشبكات المعلوماتية بالجامعة لإجراءات مصادقة مسبقة. في حالة عجز هذه الوسائل أو الموارد، يجب إبلاغ الهيكل المسؤول عن الصيانة فورا.

- استخدام الانترنت

يتعهد المستخدمون الذين لديهم إمكانية الوصول إلى الإنترنت بما يلي:

• عدم تقديم معلومات مهنية أو متعلقة بالجامعة على الشبكات الاجتماعية غير المهنية؛

• عدم استخدام الإنترنت لأغراض خبيثة أو احتيالية أو بغيضة أو تشهيرية أو إباحية أو لأغراض غير قانونية؛

• عدم استخدام الإنترنت والرقمنة كوسيلة للتأثير الخادع أو السلبي، لا سيما على القصّر أو الأشخاص ذوي الحماية المحدودة؛

• توخي الحذر عند تنزيل الملفات، والتأكد من فحصها باستخدام أحد برامج مكافحة الفيروسات.

- احترام الخصوصية

تتعهد الهيئة الجامعية بحماية سرية وسلامة البيانات الشخصية المتاحة من خلال استخدام وسائل الأمن المادية والمنطقية. لا يجوز لأي طرف ثالث الوصول إلى البيانات الشخصية أو استخدامها لأي غرض ما عدا التسجيل و / أو عمل آخر بموافقة المستخدم المعني. بشكل عام، يجب أن يتناول ذلك ممارسات جمع البيانات والموافقة والتخزين واستخدام البيانات ومشاركتها.

- حماية حقوق الملكية

تشمل حقوق الملكية حق المؤلف المادي أو المعنوي في استخدام منتجه. في الواقع، الأمر متروك له لتقرير كيف سيتم توصيل هذا المنتج واستغلاله من قبل المستخدمين.

لا يمكن للمستخدمين أخذ المنتج وتعديله ومشاركته دون موافقة المؤلف ويجب دائمًا الإشارة إلى المصدر.

من الضروري ترقية استخدام برامج مكافحة الانتحال في مختلف مجالات البحث وتقنينها.

- **التحيز والتمييز**

معالجة التحيزات والتمييز التي يمكن أن تحدث في التقنيات الرقمية، مثل الخوارزميات المتحيزة أو مجموعات البيانات المتحيزة. يتضمن ذلك تحديد النتائج التمييزية وتخفيفها وتجنب حدوثها، فضلاً عن ترقية التنوع والإدماج في تطوير التكنولوجيا وعمليات أخذ القرار.

- **التوقيع الالكتروني**

سلطة ضمان التبادلات الإلكترونية. (سلامة محتوى الرسالة، وتحديد المرسل والمتلقي، وتاريخ الإصدار، وما إلى ذلك).

- **اليقظة التكنولوجية**

يجب أن يضمن مكون الجامعة بأكمله (مدير، مدرس، طالب، عامل) يقظة تكنولوجية من حيث الرقمنة بخصوص النقاط ذات العلاقة:

- باستخدام وتحديث المعرفة والمستجدات؛
- بالحفاظ على مصالح الموظفين والجامعة والوطن؛
- بحماية الحقوق وترقية الالتزامات.

- **التصميم الأخلاقي والذكاء الاصطناعي**

إدخال الذكاء الاصطناعي في القطاع الجامعي خطوة أساسية لتعزيز تحسين العمليات من خلال إنتاجية وفعالية متميزة للنشاطات وكذا تحسين مشهود في الخدمة لمختلف المستخدمين. من ناحية أخرى، من الضروري النظر في جميع التحديات الأخلاقية والمعنوية والاجتماعية التي قد يطرحها الذكاء الاصطناعي، وبالتالي فمن الضروري:

- **وضع أطر وآليات للحوكمة الأخلاقية للذكاء الاصطناعي،** تتضّمن المبادئ والتوجيهات واللوائح التي تحكم تطوير ونشر واستخدام تقنيات الذكاء الاصطناعي. يتطلب ذلك معالجة قضايا مثل المسؤولية والشفافية والرقابة لضمان ممارسات الذكاء الاصطناعي المسؤولة.

- الأخذ بالاعتبار الآثار الأخلاقية للتقنيات الناشئة من مثل الواقع الافتراضي، وسلسلة الكتل (blockchain)، وإنترنت الأشياء (IoT) والسلوكات وكذا بعض البرامج مثل دردشة GPT وتأثيرها المحتمل على الأفراد والمجتمع.

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).