Revue RAMReS – Sciences Appliquées et de l'Ingénieur
RAMReS 2023 - *Published Online 2023* - http://publication.lecames.org/
Vol. 5(1), pp. 7-17, Online December 2023

Vol. 5
ISSN 2630-1164
December 2023

Full Length Research Paper

Considérations éthiques dans les systèmes de surveillance des examens en ligne basés sur le Deep Learning.

Konan YAO [1*], Tiémoman KONE [1], Venance Saho ZOH [1], Koffi Fernand KOUAME [1]
[1]Université Virtuelle de Côte d'Ivoire, Unité de Recherche et d'Expertise Numérique (UREN) - Abidjan, Côte d'Ivoire

Received July 2023 – Accepted October 2023

**Corresponding author. Konan9.yao@uvci.edu.ci*

Résumé:
Cet article, explore les préoccupations éthiques liées aux systèmes de surveillance des examens en ligne basés sur le Deep Learning. En effet, Ces systèmes utilisent des données personnelles telles que les empreintes digitales ou les caractéristiques faciales pour identifier et authentifier les utilisateurs, ce qui implique l'accès à des informations liées à leur identité. Toutefois, le fonctionnement de ces systèmes de surveillance, notamment ceux utilisant la technologie de reconnaissance faciale, peut soulever des préoccupations quant à la collecte de données personnelles sans le consentement des utilisateurs, créant ainsi des problèmes potentiels pour la vie privée de ces derniers. En outre, l'identification incorrecte de la fraude en raison de l'utilisation d'algorithmes moins précis peut engendrer des frustrations. Cette étude vise à fournir des directives aux parties prenantes impliquées dans la conception et la mise en place de systèmes de surveillance des examens en ligne. Après une analyse approfondie des considérations éthiques existantes, en nous appuyant principalement sur la littérature et les lois et réglementations en vigueur, nous pouvons identifier quatre principales valeurs éthiques, à savoir : i) la préservation de la vie privée des apprenants, ii) l'équité dans la participation aux examens, iii) la sécurisation et la protection des données des apprenants, iv) et la prévention du biais algorithmique. En conséquence, des lignes directrices ont été élaborées pour garantir que le système respecte les principes d'éthiques et les droits des utilisateurs tout en répondant aux exigences de sécurité et de fiabilité nécessaires pour prévenir la fraude.

Mots clés: Surveillance des examens en ligne ; apprentissage profond ; vie privée ; éthique de l'intelligence artificielle.

Cite this article:
Konan YAO, Tiémoman KONE, Venance Saho ZOH, Koffi Fernand KOUAME. (2023). Considérations éthiques dans les systèmes de surveillance des examens en ligne basés sur le Deep Learning. Revue RAMReS – Sci. Appl. & de l'Ing., Vol. 5(1), pp. 7-17. ISSN 2630-1164.

1. Introduction

L'apprentissage en ligne est en plein essor et connait une évolution continue à travers le monde. Il offre aux étudiants la possibilité de participer à des activités académiques telles que les cours et des conférences, ainsi que d'accéder aux ressources pédagogiques à domicile. Ce mode d'apprentissage leur permet de collaborer avec d'autres étudiants sans avoir à se déplacer. Par ailleurs, l'une des principales composantes de ce type d'apprentissage est l'évaluation qui se déroule généralement en ligne. En effet, l'examen en ligne fait référence à l'utilisation des plateformes et des technologies du numérique pour évaluer les connaissances, les compétences ou les performances des apprenants [1]. Cependant, l'examen en ligne présente des défis en matière de fraude, tels que le plagiat, la collaboration non autorisé, l'utilisation des appareils non autorisée et des logiciels de triche [2]. Afin de lutter contre ces formes de fraude, les établissements et les plateformes d'évaluation en ligne mettent en place diverses mesures de sécurité. Ces mesures comprennent l'utilisation de logiciels de détection de plagiat [3], la surveillance vidéo en direct pendant les examens [4], l'utilisation de questions aléatoires ou adaptatives [5], la limitation du temps alloué pour les évaluations, la surveillance enregistrée [4] ainsi que l'utilisation de technologies de surveillance et d'authentification avancées notamment la reconnaissance faciale avec des algorithmes d'apprentissage profond [6]. Les systèmes de surveillance des examens en ligne basés sur l'apprentissage profond permettent d'identifier une personne à l'aide de ses caractéristiques physiologiques telles que l'empreinte digitales, l'iris, la géométrie de la main et le visage. L'authentification à plusieurs niveaux est utilisée pour authentifier l'individu et pour

effectuer des recoupements tout au long de la période d'examen. Ainsi, de nombreuses institutions éducatives adoptent ces systèmes pour prévenir la fraude [7]. Cependant, l'utilisation de ces systèmes de surveillance dans l'éducation suscite un débat, car elle soulève des questions de confidentialité, d'éthique et de confiance. D'un côté, certains soutiennent que la surveillance des examens en ligne et à distance est nécessaire pour garantir des évaluations justes et crédibles, en identifiant les cas de fraude et en assurant l'équité entre les apprenants [2]. D'un autre côté, d'autres soulignent que la surveillance peut empiéter sur la vie privée des apprenants, créer un environnement stressant et décourager l'apprentissage authentique [8, 9]. Ainsi, il devient primordial de prendre en considération les enjeux éthiques liés aux systèmes de surveillance des examens en ligne et à distance. Il est essentiel de trouver un juste équilibre entre la préservation de la confidentialité des apprenants et la garantie de l'intégrité des évaluations en mettant en œuvre des mesures appropriées et en prenant en compte les préoccupations, les besoins et les attentes des apprenants. Cet article examine les questions éthiques liées aux systèmes de surveillance des examens en ligne basés sur le Deep Learning (SSLDP) telles que l'atteinte à la vie privée des apprenants, la collecte et l'utilisation sans consentement des données personnelles, la discrimination algorithmique et la surveillance excessive. Il se fonde sur une analyse de quelques considérations éthiques principalement issues de la littérature actuelle et les législations en vigueur. Dans ce travail, nous recommandons la mise en place de politiques claires pour encadrer l'utilisation de ces systèmes, ainsi que l'utilisation de techniques de chiffrement pour protéger les données des apprenants. En soulignant l'importance d'établir un équilibre entre la prévention de la fraude et le respect des droits des utilisateurs, cette étude vise à inciter à une réflexion approfondie sur les considérations éthiques liées au développement et à l'utilisation des systèmes de surveillance des examens en ligne basés sur le Deep Learning.

Nous présentons tout d'abord, le matériel et les méthodes utilisées au travers une revue de littérature sur les méthodes et législations existantes et une synthèse. Ensuite nous proposons un cadre éthique adapté aux systèmes de surveillance des examens en ligne.

Enfin, nous concluons notre étude en abordant les étapes nécessaires pour mettre en œuvre nos propositions.

2. Matériels et méthodes

2.1. Revue de la littérature.

Cette section passe en revue et analyse la littérature afin de déterminer les problèmes éthiques que posent les SSLDP et les moyens de les résoudre. Elle sélectionne, analyse et synthétise des recherches menées sur les SSLDP en fonction de leur pertinence et de leur date de publication, en retenant les plus récentes. Les documents analysés proviennent des bases de données comme scopus, web of sciences et google scholar et concernent des articles de journaux, des thèses, des résumés de colloque, des chapitres fournissant des informations pertinentes.

2.1.1. Préoccupations éthiques concernant la vie privée.

L'utilisation des SSLDP pour surveiller les évaluations en ligne exige une véritable analyse de leurs implications en matière d'atteinte à la vie privée car la violation facile de la confidentialité des informations soulève un problème éthique [9]. En effet, le but de la confidentialité est de restreindre l'accès et l'utilisation des informations personnelles, sensibles ou confidentielles aux seules personnes autorisées en donnant la possibilité aux personnes de contrôler la manière dont leurs informations sont utilisées, partagées et protégées. Toutefois, en raison du fonctionnement des systèmes de surveillance utilisant la technologie de la reconnaissance faciale, il est possible de collecter des données personnelles sans obtenir le consentement des utilisateurs [10]. Aussi, le processus de surveillance en ligne à distance oblige parfois les apprenants à montrer avec leur webcam ou la caméra frontale de leur smartphone, leur environnement de travail, des membres de leur famille et cela à tout moment que l'application est utilisée. Cette pratique est perçue par les utilisateurs comme une forme de surveillance excessive [15, 18]. Par exemple les professeurs utilisent les SMS et les réseaux sociaux pour suivre le comportement de leurs étudiants en dehors de la salle d'examen [21, 22]. Selon les auteurs de [13], la surveillance peut compromettre l'autonomie de l'apprenant. Par exemple lors d'un examen surveillé par un logiciel qui exige que l'apprenant soit constamment face à sa caméra, cela peut poser un problème lorsqu'il a besoin de se rendre aux toilettes. En outre, les apprenants peuvent manifester le stress de diverses manières, et des actions telles que s'étirer les bras, se ronger les ongles, détourner le regard, qu'ils utilisent pour se recentrer pourraient être signalées comme des comportements de tricherie [16, 23]. D'autres auteurs [11, 13, 14, 17, 18, 19] vont encore plus loin en indiquant que les systèmes basés sur l'intelligence artificielle, et en particulier les SSLDP, peuvent nous exposer à des décisions injustifiées et discriminatoires supposées à tort exactes parce qu'elles sont prises automatiquement et quantitativement sans une étude empirique nuancée du contexte sociétal entourant l'utilisateur

2.1.2. Equité.

Certaines études suggèrent que les étudiants trichent plus souvent dans les environnements de test en ligne que dans les salles d'examen traditionnelles [2], bien qu'il existe des points de vue contradictoires [8]. Pour toutes ces raisons, les universités et les apprenants ont des intérêts à réaliser des évaluations surveillées pour le maintien de l'intégrité académique et son épanouissement en tant que valeur institutionnelle. Cependant, certains apprenants peuvent être désavantagés par les SSLDP à certains égards. Cela inclut les apprenants qui ne disposent pas d'appareils (ordinateur, smartphone) appropriés, de connexions

Internet fiables. La surveillance électronique requiert souvent des heures d'internet, et un examen en ligne peut être annulé si internet se déconnecte, même momentanément. Les SSLDP peuvent entrainer des discriminations [21]. En effet, le fonctionnement de certains systèmes repose sur le suivi des gestes et des mouvements, ce qui pose problème lorsque certains gestes ne sont pas reconnus ou intégrés. C'est le cas par exemple des handicapés. Une personne atteinte de déficience visuelle qui doit passer un examen surveillé par un système basé sur le clignement des yeux pourrait être mal interprété comme tricheur car son visage pourrait être perçu comme immobile.

2.1.3. Sécurisation et protection des données.

L'utilisation abusive des données et les fuites des données posent un problème éthique important. En général, les SSLDP utilisent les informations personnelles telles que les empreintes digitales ou les caractéristiques faciales pour identifier et authentifier les utilisateurs, ce qui constituent des informations propres à leur identité. Par conséquent, l'utilisation de telles données peut représenter un véritable danger pour l'utilisateur [9]. C'est pourquoi Lan [24], souligne que la protection et la confidentialité des données des apprenants est une question urgente qui doit être traité. Aussi convient-il de souligner que même si des mesures sont prises pour préserver la vie privée, elles ne garantissent pas une non-divulgation des données [56]. Par conséquent, il est important de mettre en place des techniques de sécurité robustes pour protéger les systèmes de gestions des données [25].

2.1.4. Le biais discriminatoire.

Lors de l'utilisation des algorithmes de Deep Learning, il peut se produire des discriminations ou des imprécisions qui est dû au taux d'erreur des algorithmes ou biais [31, 58].

Les biais peuvent avoir des conséquences néfastes, notamment en perpétuant les inégalités et les discriminations existantes dans la société [12, 26, 59, 60]. Par exemple des études faites au Massachusetts Institute of technologie (MIT) Media Lab. ont montré que la technologie de reconnaissance faciale est plus efficace pour détecter les personnes à la peau claire surtout les hommes, que les personnes à la peau foncée et les femmes [27]. En outre, si une fraude est incorrectement identifiée comme étant négative, cela peut causer d'énormes frustrations et même fait perdre une année académique à un apprenant, s'il n'y a pas de procédure de recours suffisamment structurée. Selon les auteurs de [29], les algorithmes mal écrits, l'utilisation d'ensembles de données de formation empoisonnés, incomplets ou biaisés pourraient contribuer à la marginalisation de certains utilisateurs.

2.1.5. Solutions existantes

L'utilisation des technologies numériques pilotées par des algorithmes dans les organisations soulèvent des questions éthiques importantes. Toutefois, des pistes de solutions sont explorées pour favoriser une utilisation éthique de ces technologies

Ali et al. [18], mentionnent que l'intelligence artificielle est un controversé et que diverses initiatives ont été lancées pour assurer son acceptabilité morale. Ils identifient deux principales stratégies d'atténuation des problèmes éthiques qui sont l'atténuation au niveau des politiques et des entreprises de gouvernance de l'éthique. Les auteurs Aizenberg et Van Den Hoven [9], proposent un cadre de conception de systèmes d'IA basé sur la méthode value design, qui s'appuie sur les méthodologies de conception sensible à la valeur et de conception participative pour engager de manière proactive toutes les parties prenantes. Le cadre proposé vise à traduire les droits humains fondamentaux en exigence de conception dépendant du contexte grâce à un processus structuré, inclusif et transparent. Jordan et al. [29] ont présenté un travail essentiellement basé sur l'intelligence artificielle explicable et l'amélioration de la précision des algorithmes. Après avoir examiné les méthodes de conception existantes, ils recommandent une restructuration des efforts de conception afin de mettre en évidence l'importance de l'humain dans le processus de développement. Dans [10], Isabella propose un code d'éthique et de déontologie afin de garantir la protection de la vie privée et la sécurité des données et de minimiser les biais et les erreurs d'identification dans le cadre de la technologie de la reconnaissance faciale. Coghlan et al. [13], présentent une évaluation critique des systèmes de surveillance des examens en ligne. L'analyse éthique examine de manière critique les concepts clés d'intégrité académique, d'équité, de non-malfaisance, de transparence, de confidentialité, d'autonomie, de liberté et de confiance dans le contexte des technologies SSLDP. Ils en conclu que les institutions devront également faire face à d'éventuelles implications plus vastes découlant du choix d'utiliser ces technologies. Dans la création de cadres de protection et de confidentialité des données des apprenants, Lan [24] propose d'optimiser la réglementation de l'utilisation des données personnelles et de sensibiliser les apprenants à l'autoprotection puisque le cadre juridique de la protection des données fait encore objet de débat. Il souligne l'importance de sensibiliser à l'amélioration des mécanismes d'autorégulation du secteur des technologies de l'information. Une autre mesure proposée consiste à offrir aux apprenants des recours juridiques en cas de violation de la confidentialité de leurs données. En d'autres termes, il s'agit de leur permettre de faire valoir leurs droits légaux si leur confidentialité est compromise, créant ainsi un environnement plus sûr et protégé pour les apprenants lorsqu'ils interagissent avec des technologies éducatives. Des appels continus sont lancés en faveur des lignes directrices éthiques. Après une étude comparative des cadres réglementaires américains, européens et britanniques, Almeida et al. [10] montrent qu'à toutes les étapes du processus des technologies de reconnaissance faciale, dans tous les aspects de la conception et de l'utilisation, y compris des contextes spécifiques, il est nécessaire de documenter et de rendre compte de l'utilisation garantissant des mécanismes de transparence et de remise en question. Zuiderveen Borgesius [31], évalue la protection

juridique actuelle contre les décisions algorithmiques discriminatoires en Europe et montre que le droit de la non-discrimination, notamment à travers le concept de discrimination indirecte, interdit de nombreux types de discrimination algorithmique et suggère comment l'application des textes juridiques actuels peut être améliorée.

2.2. Législations en vigueur

Cette section passe en revue et analyse certaines lois en vigueur afin de déterminer les propositions de textes pour protéger de l'intrusion des SSLDP dans la vie privée. Il est important de souligner que la plupart des textes proposés concernent les systèmes basés sur l'intelligence artificielle en générale et non spécifiquement sur les SSLDP. Aussi, les textes étudiés sont des textes à caractère regional ou continental.

Au cours de ces dernières décennies, les systèmes utilisant l'IA font objet de développements juridiques importants. Les législations sont créées dans le but de protéger les utilisateurs. Ces législations pourraient être liées à divers domaines tels que la protection des utilisateurs, la confidentialité des données, la sécurité en ligne, la non-discrimination etc. Le but de ces lois est d'éviter de nuire aux utilisateurs et de leur donner un sentiment de sécurité lors de l'utilisation des systèmes basés sur l'IA. Par exemple, dans le contexte des plateformes de surveillance des examens en ligne, les législations peuvent exiger des établissements qu'ils aient des politiques strictes de protection des données, fournissent des termes et conditions clairs et veillent à ce que les utilisateurs ne soient pas soumis à des contenus préjudiciables ou au cyber intimidation. La mise en œuvre de ces lois peut impliquer diverses parties prenantes telles que des organismes gouvernementaux, des autorités de réglementation et des acteurs de l'enseignement et de la formation. Des recommandations provenant d'organisations internationales telles que l'Organisation des Nations Unies pour l'Éducation, la Science et la Culture (UNESCO)[30] indiquent que les systèmes utilisés dans l'éducation devraient être soumis à des exigences strictes en matière de suivi, d'évaluation des capacités ou de prédiction du comportement des apprenants. L'utilisation de l'IA doit soutenir le processus d'apprentissage sans réduire les capacités cognitives ni collecter de données sensibles, dans le respect des normes de protection des données en vigueur. Le règlement général sur la protection des données (RGPD) de l'union européenne [32] en vigueur depuis 2016 introduit les données personnelles dans un régime réglementaire [39]. Il vise à protéger les personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données dans l'espace européen. Trois actions de sécurité sont proposées. La première action consiste à sécuriser le traitement des données personnelles. La deuxième action consiste à notifier l'autorité de contrôle en cas de violation de données personnelles. La troisième action consiste à informer la personne concernée en cas de violation de ces données personnelles. Cela signifie qu'en cas de violation de données à caractère personnel, la personne concernée doit en être informée sans retard injustifié. Il établit un cadre juridique pour la collecte, le traitement et la conservation des données personnelles, et confère aux individus un plus grand contrôle sur leurs informations.

Aux États-Unis, la protection des données personnelles est réglementée par un ensemble de lois fédérales et d'États, telles que le California Consumer Privacy Act (CCPA) en Californie, qui peut également s'appliquer à l'utilisation des systèmes d'examens en ligne [33]. Récemment, en Californie, les législateurs ont adopté une loi pour protéger la vie privée des étudiants [43]. Cette loi interdit aux services de surveillance de collecter, utiliser, conserver ou divulguer les informations personnelles des étudiants, à moins qu'ils ne fournissent strictement des services de surveillance ou qu'il s'agisse de cas spécifiques, tels que le respect d'une ordonnance du tribunal. L'objectif principal de cette initiative est de limiter les intrusions dans la vie privée en réduisant au minimum la quantité de données qui peuvent être collectées.

La canada à élaborer un ensemble de textes ayant pour but la protection de la vie privée. Il s'agit d'une loi fédérale : La loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), axée sur la protection des renseignements personnels détenus par le gouvernement fédéral. Ce cadre permet de savoir la façon dont le gouvernement fédéral traite les renseignements personnels et la façon dont les entreprises traitent également ces données. Par ailleurs, la déclaration de Montréal [52] est aussi un cadre pour la protection de la vie privée de l'intrusion de l'IA. L'objectif est de mettre le développement de l'IA au service du bien-être de tout un chacun, et d'orienter le changement social en élaborant des recommandations ayant une forte légitimité démocratique. Cette déclaration de Montréal prend en considération dix principes éthiques incluant le bien-être, le respect de l'autonomie, la protection de l'intimité et de la vie privée, la solidarité, la participation démocratique, l'équité, l'inclusion de la diversité, la prudence, la responsabilité et le développement durable.

En chine et au japon, les textes sont axés sur la reconnaissance faciale.

En 2019, la Chine a eu son premier procès concernant l'utilisation de la technologie de reconnaissance faciale, déclenchant un débat sur la collecte des caractéristiques individuelles des utilisateurs [45]. En octobre 2020, rentre en vigueur la réglementation chinoise sur la protection des données, appelée Personal Information Security Specification [44]. Elle vise à réglementer le traitement et la protection des informations personnelles tout en préservant les droits des individus et les intérêts publics. La Chine a également publié un projet de norme sur les exigences de sécurité des données de reconnaissance faciale, qui définit des lignes directrices pour la collecte, le traitement, le partage et le transfert des données de reconnaissance faciale [44]. Les exigences énoncées dans la norme sont les suivantes : l'utilisation de ces données ne doit être faite qu'à des fins d'identification et aucune prédiction ne doit être faite sur leur base, la technologie de reconnaissance faciale ne doit être utilisé que

lorsqu'aucune technologie alternative n'est disponible pour remplir l'objectif de sécurité ou de commodité, les personnes de moins de 14 ans ne doivent pas être identifiées sur la base de la reconnaissance faciale, les données de la reconnaissance faciale ne doivent pas être stockées sans avoir obtenu le consentement du propriétaire et les données de reconnaissance faciale générées ou collectées en Chine doivent être stockées localement.

Au Japon [46, 47], les membres de la Société Japonaise d'intelligence artificielle (JSAI) formalisent des lignes directrices éthiques. Ces directives servent de fondement moral et visent à sensibiliser aux responsabilités sociales et morales envers la société. Les principes éthiques découlant de ces lignes directrices sont les suivants : contribuer à l'humanité, respecter les lois et règlements, préserver la vie privée d'autrui, promouvoir l'équité, garantir la sécurité, préserver l'intégrité, assumer la responsabilité de rendre compte et agir avec une conscience sociale

L'union africaine (UA) a élaboré une loi type sur la protection des données personnelles, qui fournit des orientations aux pays africains pour l'adoption de lois nationales sur la protection des données [47]. Ainsi, plusieurs pays africains ont mis des réglementations spécifiques concernant la protection des données personnelles. Nous analyserons quelques pays en exemple. Il faut noter que la majorité des textes se ressemblent.

La Protection of Personal Information Act (POPIA) [48], une loi sud-africaine qui régit la protection des données personnelles. Au Nigeria [34], le Nigeria Data Protection Regulation (NDPR) adopté en 2019 a pour but de réglementer la protection des données personnelles notamment la non divulgation de données, la suppression de contenu. Au Sénégal [49], la loi n° 2008-12 du 25 janvier 2008 sur la protection des données personnelles prévoit la protection des individus contre la violation de leur vie privée par le traitement des données personnelles. En Mars 2012, les autorités Ivoiriennes ont instauré l'autorité de régulation de la télécommunication de côte d'Ivoire (ARTCI) [50] qui a pour mission, entre autres, de veiller à la protection des données à caractère personnel. Suite à cela, la loi n°2013-450 relative à la protection des données personnelles a été adoptée. Cette loi établit un cadre éthique pour la collecte, le traitement, le partage et l'utilisation des données personnelles.

2.3. Synthèse d'étude

A travers l'étude exploratoire de la littérature et des législations en vigueur les principes éthiques peuvent se regrouper en quatre principaux principes relatifs aux systèmes de surveillances des examens en ligne qui sont considérés comme des valeurs [41]. Ces principes sont : la préservation de la vie privée des apprenants, l'équité dans la participation des examens, la sécurisation et la protection des données des apprenants et la prévention du biais algorithmique. D'autres écrits tels que [41, 43] regroupent la notion de biais et d'équité car tous deux font référence aux notions d'impartialité, d'égalité et d'injustice. Cependant, dans le contexte des Systèmes de Surveillance des examens en ligne basés sur le Deep Learning (SSLDP), ces deux notions présentent des problèmes qui méritent d'être examinés de manière distincte. La notion d'équité aborde des problèmes logistiques, tandis que le biais algorithmique constitue un élément essentiel à analyser dans la prise de décision d'un algorithme. Malgré l'utilisation répandue des SSLDP dans nos établissements, il est alarmant de constater que la plupart des études ne tiennent pas compte d'une analyse éthique spécifique de leur utilisation. De plus, la lacune concernant des textes régissant l'usage de l'intelligence artificielle dans de nombreux pays souligne davantage l'urgence de considérer les implications éthiques dans ces domaines.

Dans notre travail, nous avons structuré ces principes éthiques en tenant compte des éléments significatifs pour chaque principe (tableau 1), ce qui nous permet de formuler des recommandations adaptées pour un déploiement responsable des SSLDP tout en respectant les droits et le bien-être des utilisateurs.

2.4. Analyse statistique

Une analyse des correspondances a été réalisée dans le but de déterminer quels mots (tableau 1) décrivent mieux les principes éthiques retenus. Les mots du tableau 1 ont été relevés dans chaque définition présente dans nos références bibliographiques. Cela a permis de compter, de façon manuelle, le nombre de fois où le mot a été utilisé pour définir ou décrire le principe dans les textes choisis.

3. Résultats

3.1. Résultats de l'analyse des correspondances

χ^2 = 1200.811
p-value = 1.259992e-188

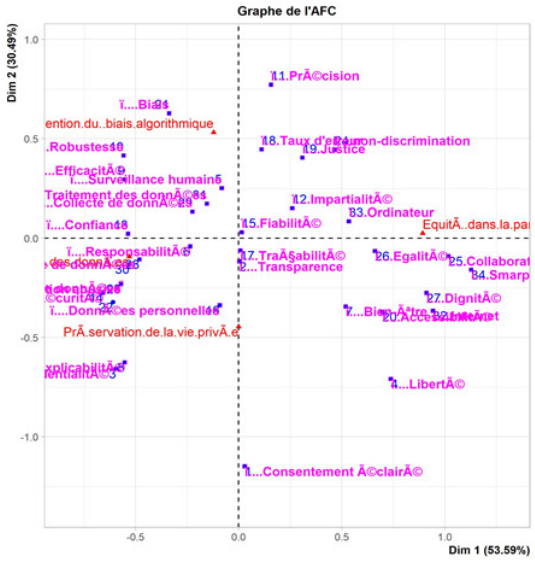

Fig.1: Représentation des Principes éthiques et des mots

Le chi-carré χ^2 et le p-value extrêmement faible montrent que la liaison entre les principes éthiques et les mots qui les descrivent est significative.

D'après la figure (fig 1.), nous observons que les mots comme "données personnelles", "Confidentialité", "responsabilité", "explicabilité "etc. sont proches du principe éthique "préservation de la vie privée". Cela signifie que ces mots sont fréquemment utilisés pour décrire ou définir ce principe éthique.
Quant aux mots tels que "Ordinateur", "égalité", "Impartialité", etc. sont proches du principe éthique "Equité dans la participation des examens". Cela signifie que ces mots sont suremployés pour décrire ou définir ce principe éthique.
Pour le principe éthique "Sécurisation et protection des données", les mots les plus utilisés dans la description sont "Sécurité", "confiance", "responsabilité", Collecte de données etc.
Dans le cadre de l'étude du principe éthique "préservation du biais algorithmiquee", les mots qui semble le décrire le mieux sont "précision", "Taux d'erreur", "robustesse", "non-discrimination", "justice", etc.

Tableau 1. - Tableau de champs lexical

Principes éthiques	Eléments significatifs
Préservation de la vie privée de des apprenants	Transparence, Surveillance humaine, consentement éclairé, Liberté et conviction personnelle, sureté Confidentialité, bien être Collecte et stockage de données
Equité dans la participation des examens	Impartialité, explicabilité Accessibilité, justice, non-discrimination Surveillance humaine, dignité
Sécurisation et protection des données	Collecte et stockage de données, Fuite ou utilisation abusive de données, traçabilité Sécurité, confiance
Prévention du biais algorithmiquee	Collecte et stockage de données, efficacité Traitement de données, Précision, robustesse Impartialité, sureté, traçabilité Taux d'erreur, confiance, fiabilité -

3.2. Cadre éthique proposé

Dans cette partie, nous présentons un cadre éthique conçu à partir des résultats de notre analyse. L'objet de ce cadre est de garantir une utilisation éthique des systèmes de surveillance des examens en ligne basés sur le Deep Learning. L'automatisation de la surveillance des examens est de plus en plus courante en raison de la prolifération des établissements et des plateformes de formation en ligne. Par conséquent, Il est important de proposer des directives éthiques afin de s'assurer de l'utilisation appropriée des SSLDP. Pour l'auteur de [41], il est important de noter qu'un objet, un programme ou une technique ne peut pas être intrinsèquement qualifié d'éthique. En effet, l'adjectif éthique (selon la définition 1 : relatif à la morale) ne peut être associé qu'à une démarche, une délibération, une réflexion, une question, un principe, une valeur, etc.
Dans notre approche, nous considérons les principes éthiques comme des valeurs à atteindre et nous analysons les normes pour parvenir à ces valeurs. Cela signifie que l'éthique réside dans le processus de réflexion et de conception pour déterminer les principes à suivre.
La méthode proposée utilise la technique value design de [14]. Cette approche prend en compte les principes de valeurs ainsi que les normes à suivre pour atteindre ces valeurs. Quatre valeurs essentielles sont identifiées. Ce sont la préservation de la vie privée et la gestion des données des apprenants, l'équité dans la participation des examens, la sécurisation et la protection des données et la prévention du biais algorithmiques. Les normes sont libellées en action dont chaque établissement doit prendre en compte avant d'instaurer un système de surveillance des examens à distance.
Notre approche suggère que, du processus de conception à l'utilisation effective, les systèmes doivent suivre des procédures spécifiques. Tout établissement qui déploie une telle technologie doit s'assurer de respecter rigoureusement ces étapes pour garantir une utilisation éthique des systèmes de surveillance des examens en ligne basés sur le Deep Learning. En adoptant ce cadre éthique, nous visons à promouvoir des pratiques responsables et respectueuses des droits des utilisateurs tout au long du processus de surveillance des examens en ligne.
Afin de faciliter la compréhension de cette étude, nous adopterons un cadre de travail spécifique, celui de l'université Virtuelle de Côte d'Ivoire (UVCI). Cette université est un établissement public de formation en ligne, avec des étudiants répartis géographiquement sur tout le territoire ivoirien et à l'international. Le défi auquel l'UVCI est confrontée est de pouvoir surveiller tous les étudiants en même temps, alors que chaque étudiant doit rester chez lui pour passer les examens. Cette situation soulève des questions cruciales concernant l'intégrité des examens et les considérations éthiques liées au système de surveillance.

3.3. Cadre éthique pour la préservation de la vie privée des apprenants

- **Etablir une contrainte technique**

Lors de la conception d'un système de surveillance des examens en ligne, l'établissement se doit de définir les lignes directrices spécifiques ou des règles à suivre pour atteindre certains objectifs ou résoudre des problèmes spécifiques. Le dispositif technique est conçu pour être déployé dans un certain cadre où il serait éthique par nature, et pour transmettre avec fidélité les objectifs fixés afin de s'assurer que le produit final réponde à certaines normes spécifiques. Les fonctionnalités de protection de la vie privée peuvent être intégrées dès le début du processus de conception et non pas en seconde intention.

- **Garantir la transparence et la responsabilité.**

La transparence dans les SSLDP fait référence à la capacité de comprendre et d'expliquer le fonctionnement et les décisions du système ou des algorithmes aux utilisateurs et aux parties prenantes concernées. Cela implique de rendre le processus de prise de décision du système explicite, de manière à ce que les raisons pour lesquelles une action ou une prédiction spécifique a été effectuée soient claires et compréhensibles. La transparence est cruciale pour établir la confiance des utilisateurs. Quant à la responsabilité, elle se rapporte à la prise en compte des conséquences de l'utilisation du système sur les individus, la société et l'environnement et les mesures mise en place pour résoudre les éventuels problèmes. Cela implique d'assumer la responsabilité des erreurs et des conséquences indésirables liées à l'utilisation du système.

- **Obtenir le consentement éclairé et explicite de l'apprenant.**

L'apprenant doit être correctement informé de l'utilisation du système de surveillance automatisée dans le processus de l'examen. Cela implique de fournir des informations claires et compréhensibles sur la manière dont le système sera utilisé, les types de données qui seront collectées et les objectifs de cette collecte de données. Les apprenants doivent être conscients de la manière dont le système peut influencer leur examen. Le système doit permettre à l'apprenant de prendre une action claire qui matérialise son consentement par exemple prévoir un bouton l'accueil qui permet à l'étudiant de donner son accord pour l'utilisation de la reconnaissance faciale.

- **Règlementer l'utilisation des données personnelles.**

Les données personnelles sont des informations qui peuvent identifier une personne spécifique. Les règlements de l'examen doivent informer et garantir que les données sont traitées avec soin et que les droits des apprenants sont respectés

- **Offrir aux apprenants un cadre de recours en cas de collecte de données compromettant ou mauvaise identification du système.**

Mettre en place un mécanisme qui permet aux apprenants de signaler les problèmes liés à l'utilisation des données personnelles ou la décision du système. Par exemple dans le cas où un apprenant est faussement identifié en tant que tricheur, il doit avoir la possibilité de faire une réclamation, et le processus de réclamation doit être clairement définie et connue.

- **Assurer une adoption durable des systèmes de surveillance des examens.**

Pour garantir l'efficacité et l'acceptation des SSLDP, il est important d'assurer une communication claire et transparente sur la mise en œuvre de ces systèmes. Expliquer les raisons de leur utilisation, les avantages qu'ils apportent et les mesures prises pour protéger la vie privée des apprenants. Impliquer les parties prenantes, y compris les apprenants et les enseignants dans le processus décisionnel et recueillir leurs commentaires pour d'éventuelles améliorations.

3.4. Cadre éthique pour l'équité dans la participation aux examens.

- **S'assurer que les apprenants ont ou peuvent avoir des appareils adéquats.**

Chaque apprenant qui participe à un examen en ligne, et qui doit subir un système de surveillance en ligne a besoin d'outils adéquat lui donnant les mêmes chances que ses condisciples. ¨Par conséquent, il est nécessaire de s'assurer que la majorité des apprenants a accès à des dispositifs appropriés pour participer pleinement à un examen en ligne utilisant des technologies de Deep Learning. Cela vise à réduire les inégalités d'accès aux ressources technologiques et à permettre à tous les apprenants d'avoir des conditions équitables pour participer pleinement à leur education.

- **Améliorer l'accessibilité aux outils.**

Lors des examens, les apprenants ont besoin d'accéder à divers outils technologiques. Il est donc essentiel de rendre ces outils, applications et technologies faciles à utiliser et accessibles à un large éventail de personnes, y compris celles ayant des capacités différentes ou des besoins spécifiques. L'objectif est de créer un environnement inclusif où tous les individus, quels que soient leurs handicaps ou leurs différences, peuvent bénéficier pleinement des ressources numériques et des services disponibles. Il peut s'agir de prendre en compte les besoins des personnes handicapées visuelles, auditives, motrices ou cognitives en proposant des options alternatives.

3.5. Cadre éthique pour la sécurisation et la protection des données.

- **Réduire les fuites et l'utilisation abusive des données.**

Les fuites de données se produisent lorsqu'une information confidentielle est divulguée de manière non autorisée, tandis que l'utilisation abusive des données se réfère à l'utilisation inappropriée ou non éthique des informations collectées. Il est donc important, de mettre en place des mesures de sécurité robustes, telles que le cryptage, les pares-feux et les contrôles d'accès, pour protéger les données contre les accès non autorisés. Limiter l'accès aux données uniquement aux personnes autorisées.

- **Prévenir les vulnérabilités**

Cette action invite les concepteurs à mettre en place des mesures proactives pour identifier, atténuer ou éliminer les faiblesses potentielles dans les systèmes, qui pourraient être exploitées par les acteurs malveillants pour causer des dommages. Il s'agit notamment d'intégrer la sécurité dans le processus de développement du système dès le début de la conception, d'appliquer les bonnes pratiques de codages, d'exécuter des actions de configurations rigoureuses, de maintenir les logiciels du système à jour etc.

- **Adopter des méthodes de chiffrement robuste empêchant la divulgation des données.**

L'objectif du chiffrement vise à empêcher la divulgation non autorisée ou la divulgation accidentelle pendant l'entrainement du modèle, en les transformant sous une forme illisible. Pour atteindre cet objectif, il est primordial d'utiliser des méthodes de chiffrement largement reconnues et considérées comme étant sécurisées. Le chiffrement est appliqué à différentes étapes, tant lors du stockage des données que pendant l'entraînement du modèle, avec des techniques telles que la cryptographie homomorphe qui permettent d'effectuer des calculs sur des données chiffrées sans les déchiffrer préalablement.

La cryptographie homomorphe [53] est une méthode de chiffrement qui permet de réaliser les calculs (par exemple un entrainement de modèle de machine learning) directement sur les données chiffrées sans les déchiffrer. Traditionnellement, les données chiffrées doivent être déchiffrées avant de pouvoir être traitées, ce qui les rend vulnérables si l'entité ou l'appareil qui les traite n'est pas entièrement fiable. Pour résoudre ce problème le théoricien, informaticien Craig Gentry [54] a montré comment crypter des informations à l'aide de structures mathématiques qui préservent la capacité de les traiter directement sous forme cryptée. Ainsi, une tierce personne peut manipuler les données sans y accéder directement.

Le fonctionnement du chiffrement homomorphe est le suivant : soit x et y deux entiers et E un opérateur de chiffrement. Si x et y sont chiffrés (E(x) , E(y)), alors pour obtenir x+y il suffit de calculer

$E(x+y)= E(x)+E(y)$ car E est homomorphe.

3.6. Cadre éthique pour la prévention du biais algorithmique.

- **Préparation des données**

Cette étape est un aspect crucial pour le développement de tout système utilisant des données. Une grande partie du travail de conception réside dans la préparation de l'ensemble des données qui serviront à entraîner puis valider le modèle. Une première étape essentielle est la collette des données. Il faut s'assurer que les données collectées et utilisées pour entrainer les algorithmes sont représentatives de la population cible. Les ensembles de données doivent être diversifiés et équilibrés pour éviter d'introduire des biais systématiques.

- **Contextualiser les données.**

Lorsqu'on traite des données, il est essentiel de comprendre le contexte dans lequel elles ont été recueillies, car cela peut avoir une influence significative sur leur signification, leur pertinence et leur interprétation. Comprendre d'où proviennent les données est important pour évaluer leur qualité et leur fiabilité. Les données peuvent provenir de différentes sources, telles que des enquêtes, des capteurs, des transactions, des réseaux sociaux, etc. Chaque source peut avoir ses propres biais et limitations. Par conséquent, Il est essentiel de comprendre pour qui les données ont été collectées ou à qui elles sont destinées afin de bien interpréter leur signification. Les données qui ont été spécifiquement recueillies pour un public particulier peuvent ne pas être généralisables à d'autres contextes.

- **Construire des algorithmes précis et impartial.**

Durant la phase d'entraînement, les paramètres du modèle sont optimisés par des successions d'opérations mettant en jeu une fraction des données d'entraînement. Ce modèle est mis à l'épreuve sur la base de performances définies par des métriques choisies à l'avance. Un point d'attention concerne le choix de la métrique de performance. La manière dont est mesurée la performance d'un système doit être en accord avec l'usage qui sera fait de celui-ci.

Des données non utilisées dans la phase d'entraînement servent à tester le modèle pour vérifier s'il est performant sur de nouvelles données, évaluant ainsi son pouvoir de généralisation. L'étape de test du modèle sert à éviter le surapprentissage, c'est-à-dire que le modèle n'apprenne à résoudre le problème déterminé que sur le jeu de données qui l'a entraîné.

- **Adopter une démarche d'équité active autorisant l'usage de variables sensibles pour évaluer les algorithmes.**

Dans ce contexte, il s'agit d'autoriser l'utilisation de variables sensibles, telles que la race, le genre, l'origine ethnique, ou d'autres caractéristiques délicates, dans le but de mesurer les biais et d'évaluer les performances des algorithmes. L'idée derrière cette approche est de reconnaître que les variables sensibles peuvent être

liées à des biais et des discriminations potentielles dans les résultats des algorithmes. Plutôt que d'ignorer complètement ces variables, l'équité active consiste à les inclure de manière transparente dans le processus de mesure et d'évaluation pour mieux comprendre l'impact qu'elles peuvent avoir sur les décisions prises par l'algorithme.

4. Conclusion

Cette étude sur les considérations éthiques dans les systèmes de surveillance des examens en ligne basés sur le Deep Learning revêt d'une importance capitale pour prévenir la fraude et respecter les droits des apprenants.

Dans ce sens, nous avons pu identifier les questions éthiques dans les SSLDP et les solutions existantes en analysant la littérature actuelle et les lois en vigueur.

Les résultats de l'analyse ont permis d'identifier quatre valeurs éthiques centrales qui doivent être prises en compte dans la conception et l'utilisation des SSLDP, notamment la préservation de la vie privée des apprenants, l'équité dans la participation aux examens, la sécurisation et la protection des données des apprenants et la prévention du biais algorithmique.

La préservation de la vie privée des apprenants concerne la gestion, la protection et l'utilisation des données personnelles. L'équité dans la participation aux examens en ligne est essentielle pour assurer que tous les étudiants aient les ressources nécessaires pour participer pleinement aux évaluations. La sécurisation et la protection des données des apprenants impliquent l'exploration de techniques de sécurisation et de stockage pour garantir la sécurité des informations collectées et stockées. Enfin, la prévention du biais algorithmique nécessite une prise de conscience éthique de la part des concepteurs et l'application de bonnes pratiques de codage.

L'évolution rapide de l'intelligence artificielle offre de nouvelles opportunités pour renforcer la sécurité des examens en ligne, mais soulève également des questions éthiques cruciales. Il est essentiel d'examiner de manière critique l'existence et l'utilisation des logiciels de surveillance en évaluant leur pertinence, leur valeur ajoutée pour les établissements d'enseignement et de formation, et leur impact sur les droits des apprenants.

Dans nos travaux futurs, nous prévoyons d'approfondir l'étude de la méthode de la cryptographie homomorphe, tant d'un point de vue théorique que technique, afin de mieux comprendre son potentiel pour concilier les notions d'éthique et d'intégrité académique dans les systèmes de surveillance des examens en ligne.

Remerciements

Nos remerciements s'adressent à l'Université Virtuelle de Côte d'Ivoire pour l'opportunité offerte pour ma participation à ce colloque

REFERENCES

[1] L. Audet. Les pratiques et défis de l'évaluation en ligne », 2011.

[2] T. H. Reisenwitz. Examining the necessity of proctoring online exams. Journal of Higher Education Theory and Practice, vol. 20, no 1, p. 118-124, 2020.

[3] G. Burel, K. B. Gaied, R. B. Abdelkader, et R. Gautier. Aide à la détection de l'échange d'information entre étudiants dans les contrôles à distance. J3eA, vol. 22, p. 0001, 2023.

[4] A. Nigam, R. Pasricha, T. Singh, et P. Churi. A systematic review on ai-based proctoring systems : Past, present and future. Education and Information Technologies, vol. 26, no 5, p. 6421-6445, 2021.

[5] Y. Zhenming, Z. Liang, et Z. Guohua. A novel web-based online examination system for computer science education. in 33rd ASEE/IEEE Frontiers in Education Conference, 2003, p. 5-8.

[6] P. Wang, W.-H. Lin, K.-M. Chao, et C.-C. Lo. A face-recognition approach using deep reinforcement learning approach for user authentication. in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), IEEE, 2017, p. 183-188.

[7] S. G. Rabiha, I. H. Kartowisastro, R. Setiawan, et W. Budiharto. Survey of Online Exam Proctoring Model to Detect Cheating Behavior based on Face Recognition. In 2022 8th International Conference on Systems and Informatics (ICSAI), IEEE, 2022, p. 1-7.

[8] G. N. Uunona et L. Goosen. Leveraging Ethical Standards in Artificial Intelligence Technologies : A Guideline for Responsible Teaching and Learning Applications. In Handbook of Research on Instructional Technologies in Health Education and Allied Disciplines, IGI Global, 2023, p. 310-330.

[9] C. Fontes, E. Hohma, C. C. Corrigan, C. Lütge. AI-powered public surveillance systems : why we (might) need them and how we want them », Technology in Society, vol. 71, p. 102137, nov. 2022, doi : 10.1016/j.techsoc.2022.102137

[10] I. T. Ketley. Case Study : Code of Ethics for Facial Recognition Technology », WFEESS, juill. 2022, doi : 10.26686/wfeess.vi.7664.

[11] D. Almeida, K. Shmarko, et E. Lomas. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence : a comparative analysis of US, EU, and UK regulatory frameworks. AI Ethics, vol. 2, no 3, p. 377-387, août 2022, doi : 10.1007/s43681-021-00077-w.

[12] T. Y. Zhuo, Y. Huang, C. Chen, et Z. Xing. Exploring ai ethics of chatgpt : A diagnostic analysis. ArXiv preprint arXiv :2301.12867, 2023.

[13] S. Coghlan, T. Miller, et J. Paterson. Good proctor or "big brother" ? Ethics of online exam supervision technologies. Philosophy & Technology, vol. 34, no 4, p. 1581-1606, 2021.

[14] E. Aizenberg et J. Van Den Hoven. Designing for human rights in AI. Big Data & Society, vol. 7, no 2, p. 2053951720949566, 2020.

[15] H. Beetham et al. Surveillance practices, risks and responses in the post pandemic university. Digital Culture and Education, vol. 14, no 1, p. 16-37, 2022.

[16] D. Harwell. Cheating-detection companies made millions during the pandemic. Now students are fighting back. », Washington Post, 12 novembre 2020. https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/ (consulté le 18 juillet 2023).

[17] M. Smith et S. Miller. The ethical application of biometric facial recognition technology. Ai & Society, p. 1-9, 2022.

[18] K. Ali, M. Alzaidi, D. Al-Fraihat, et A. M. Elamir. Artificial Intelligence : Benefits, Application, Ethical Issues, and Organizational Responses », in Intelligent Sustainable Systems, Springer, Singapore, 2023, p. 685-702. doi : 10.1007/978-981-19-7660-5_62.
[19] G. Kostka, L. Steinacker, M. Meckel. Under big brother's watchful eye : Cross-country attitudes toward facial recognition technology », Government Information Quarterly, vol. 40, no 1, p. 101761, janv. 2023, doi : 10.1016/j.giq.2022.101761.
[20] K. Lee et M. Fanguy. Online exam proctoring technologies : Educational innovation or deterioration ? British Journal of Educational Technology, vol. 53, no 3, p. 475-490, 2022.
[21] S. Swauger, « Our bodies encoded : Algorithmic test proctoring in higher education », Cluster Learning, 2021.
[22] R. K. Sandhu, J. Vasconcelos-Gomes, Manoj A. Thomas, T. Oliveira. Unfolding the popularity of video conferencing apps – A privacy calculus perspective », International Journal of Information Management, vol. 68, p. 102569, févr. 2023, doi: 10.1016/j.ijinfomgt.2022.102569.
[23] E. Archer, « Technology-driven proctoring: Validity, social justice and ethics in higher education », pie, vol. 41, no 1, Art. no 1, mars 2023, doi: 10.38140/pie.v41i1.6666.
[24] L. Huang, « Ethics of artificial intelligence in education : Student privacy and data protection », Science Insights Education Frontiers, vol. 16, no 2, p. 2577-2587, 2023.
[25] Md R. I. Sattar, Md. T. B. H. Efty, T. S. Rafa, T. Das, Md S. Samad, A. Pathak, M. U. Khandaker, Md. H. Ullah. An advanced and secure framework for conducting online examination using blockchain method. Cyber Security and Applications, vol. 1, p. 100005, déc. 2023, doi : 10.1016/j.csa.2022.100005.
[26] P. P. Ray. ChatGPT : A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope », Internet of Things and Cyber-Physical Systems, vol. 3, p. 121-154, janv. 2023, doi : 10.1016/j.iotcps.2023.04.003.
[27] J. Buolamwini et T. Gebru. Gender shades : Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency, PMLR, 2018, p. 77-91.
[28] UNESCO. Managing high-stakes assessments and exams during crisis - UNESCO Bibliothèque Numérique ». https://unesdoc.unesco.org/ark:/48223/pf0000373387 (consulté le 19 juillet 2023).
[29] J. R. Schoenherr ; R. Abbas ; K. Michael ; P. Rivas ; T. D. Anderson. Designing AI Using a Human-Centered Approach : Explainability and Accuracy Toward Trustworthiness. https://ieeexplore.ieee.org/abstract/document/10086944/ (consulté le 19 juillet 2023).
[30] UNESCO. Éthique de l'intelligence artificielle | UNESCO. https://www.unesco.org/fr/artificial-intelligence/recommendation-ethics (consulté le 20 juillet 2023).
[31] F. J. Zuiderveen Borgesius. Strengthening legal protection against discrimination by algorithms and artificial intelligence », The International Journal of Human Rights, vol. 24, no 10, p. 1572-1593, 2020.
[32] Union Européenne, « EUR-Lex - 32016R0679 - EN - EUR-Lex ». https://eur-lex.europa.eu/eli/reg/2016/679/oj (consulté le 20 juillet 2023).
[33] « California Consumer Privacy Act (CCPA) », State of California - Department of Justice - Office of the Attorney General, 15 octobre 2018. https://oag.ca.gov/privacy/ccpa (consulté le 20 juillet 2023).
[34] NITDA. National Information Technology Development Agency ». https://nitda.gov.ng/ (consulté le 20 juillet 2023).
[35] « Home - Information Regulator ». https://inforegulator.org.za/ (consulté le 20 juillet 2023).
[36] M. Gornet et W. Maxwell, « Normes techniques et éthique de l'IA », in Conférence Nationale en Intelligence Artificielle (CNIA), 2023.
[37] T. Ménissier, « Quelle éthique pour l'IA ? », in Naissance et développements de l'intelligence artificielle à Grenoble, 2019.
[38] E. Pardoux et L. Devillaine, « Vers une éthique processuelle de l'IA », in Conférence Nationale en Intelligence Artificielle 2022 (CNIA 2022), 2022.
[39] H. Brahmi, S. Belouali, Y. Demazeau, T. Bouchentouf, et N. H. Alaoui, « Vers un référentiel universel pour un usage éthique de l'intelligence artificielle », East African Journal of Information Technology, vol. 6, no 1, p. 91-106, 2023.
[40] S. Nzobonimpa. Algorithmes et intelligence artificielle : une note sur l'état de la réglementation des technologies utilisant la reconnaissance faciale automatique au Canada et aux États-Unis », gouvernance, vol. 19, no 2, p. 99-114, 2022, doi: 10.7202/1094078ar.
[41] C. Tessier. Éthique et IA: analyse et discussion », in CNIA 2021: Conférence Nationale en Intelligence Artificielle, 2021, p. pp-22.
[42] « Algorithmes discriminatoires - Comprendre le numérique - UNIGE », 3 mai 2021. https://www.unige.ch/comprendre-le-numerique/archives/cas-pratiques/algorithmes-discriminatoires/ (consulté le 22 juillet 2023).
[43] « Loi modifiée d'aujourd'hui - SB-1172 Loi sur la protection de la vie privée des étudiants candidats. » https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220SB1172&showamends=false (consulté le 22 juillet 2023).
[44] « Facial Recognition Laws in China #ProjectPanoptic », Internet Freedom Foundation, 3 juin 2021. https://internetfreedom.in/facial-recognition-laws-in-china/ (consulté le 22 juillet 2023).
[45] « Coming into Focus : China's Facial Recognition Regulations | Trustee China Hand | CSIS ». https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations (consulté le 22 juillet 2023).
[46] D. générale du Trésor. La stratégie japonaise sur l'intelligence artificielle : augmentation des investissements, enjeux éthiques, sociétaux et réglementaires, et opportunités de coopérations avec la France. Direction générale du Trésor, 9 juillet 2018. https://www.tresor.economie.gouv.fr/Articles/2018/07/03/la-strategie-japonaise-sur-l-intelligence-artificielle-augmentation-des-investissements-enjeux-ethiques-societaux-et-reglementaires-et-opportunites-de-cooperations-avec-la-france (consulté le 22 juillet 2023).
[47] P. par thinkoneadmin. 【Summary Report】Open Discussion: The Japanese Society for Artificial Intelligence (2017/5/24). https://www.ai-gakkai.or.jp/ai-elsi/archives/615 (consulté le 22 juillet 2023).
[48] « Formulaires POPIA - Régulateur d'information », 4 mars 2022. https://inforegulator.org.za/popia-forms/ (consulté le 22 juillet 2023).
[49] « WIPO Lex, Sénégal, Loi n° 2008-12 sur la Protection des données à caractère personnel ». https://www.wipo.int/wipolex/fr/legislation/details/6229 (consulté le 22 juillet 2023).
[50] « Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire - L'Autorité ». https://www.artci.ci/ (consulté le 22 juillet 2023).
[51] C. à la protection de la vie privée du Canada, « Aperçu des lois sur la protection des renseignements personnels au Canada », 15 mai 2014. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-

renseignements-personnels-au-canada/02_05_d_15/ (consulté le 26 juillet 2023).
[52] Montréal. Déclaration de Montréal IA responsable », Déclaration de Montréal IA responsable. https://declarationmontreal-iaresponsable.com/ (consulté le 26 juillet 2023).
[53] D. Nokam Kuaté. Cryptographie homomorphe et transcodage d'image/video dans le domaine chiffré. PhD Thesis, Université Paris-Saclay (ComUE), 2018.
[54] C. Gentry et S. Halevi. Implementing gentry's fully-homomorphic encryption scheme. In Annual international conference on the theory and applications of cryptographic techniques, Springer, 2011, p. 129-148.
[55] P. Bertail, D. Bounie, S. Clémençon, et P. Waelbroeck. Algorithmes : biais, discrimination et équité. 2019.
[56] C. D. Biais. Comment limiter les biais des algorithmes ?
[57] S. Michel, S. Gerbaix, et M. Bidan, « Questionnement éthique des systèmes algorithmiques. RIMHE : Revue Interdisciplinaire Management, Homme (s) & Entreprise, no 1, p. 105-116, 2023.
[58] M. Verger, F. Bouchet, S. Lallé, et V. Luengo. Caractérisation et mesure des discriminations algorithmiques dans la prédiction de la réussite à des cours en ligne. In EIAH2023 : 11ème Conférence sur les Environnements Informatiques pour l'Apprentissage Humain, 2023.
[59] T. Kirat, O. Tambou, V. Do, et A. Tsoukias. Equité et explicabilité des algorithmes d'apprentissage automatique : un défi technique et juridique. 2022.
[60] G. Saporta. Équité, explicabilité, paradoxes et biais. Statistique et Société, vol. 10, no 3, 2023.