

**LES ENJEUX ETHIQUES DU NUMERIQUE EDUCATIF,  
POURQUOI FAUT-IL S'INQUIETER A CE SUJET ?**

**THE ETHICAL ISSUES OF DIGITAL EDUCATION,  
WHY SHOULD WE BOTHER?**

**Pr. RAZKAOUI Yassin**

**Faculté des Sciences et des Techniques**

**Université Abdelmalek Essaâdi**

**Tanger – Maroc**

**Résumé**

La crise sanitaire due à la pandémie de COVID-19 a requis l'installation, à l'extérieur des murs des écoles, d'un mode d'enseignement différent et nouveau tout en exploitant lourdement et hâtivement les outils numériques. L'inévitable recours aux outils numériques avec ses usages nouveaux et intenses s'est accompagné d'une augmentation des menaces déjà présentes et mis l'accent sur des enjeux d'éthique qu'il fallait prendre au sérieux. En fait, dans ce contexte d'urgence où des décisions relativement prématurée ont été prises, des déficiences au niveau du recueil des données et de leur utilisation ont émergé. C'est pourquoi une réflexion s'impose pour déterminer les questions éthiques issues de la gestion des données d'éducation entraînées par ces usages accentués du numérique, et ce sur le plan des outils institutionnels, ou bien ceux qui sont moins encadrés. Nous envisageons que le recours massif à des plateformes et aux réseaux sociaux ouverts à tous, a soulevé des difficultés nouvelles en lien avec le respect de la juridiction nationale en matière de protection des données personnelles (partage des données, autorisation parentale, confidentialité, les droits d'auteur, etc.) ce qui enfante un besoin croissant voire imminent de réfléchir sur l'Éthique du numérique éducatif.

**Mots clés:** Distance learning, pandemic, ethics, digital tools, personal data, threats

### ***Abstract***

*The health crisis due to the COVID-19 pandemic has required the installation, outside the walls of schools, of a different and new mode of teaching while making heavy and hasty use of digital tools. The inevitable use of digital tools with their new and intense uses has been accompanied by an increase in the threats already present and has highlighted ethical issues that had to be taken seriously. In fact, in this emergency context where relatively premature decisions were taken, deficiencies in the collection of data and their use emerged. This is why a reflection is necessary to determine the ethical questions arising from the management of educational data resulting from these accentuated uses of digital technology, and this in terms of institutional tools, or those which are less supervised.*

*We consider that the massive use of platforms and social networks open to all has raised new difficulties in connection with respect for national jurisdiction in terms of the protection of personal data (data sharing, parental authorization, confidentiality, rights copyright, etc.) which gives rise to a growing or even imminent need to reflect on the Ethics of digital education. tools or obstacles? Or should we start by extracting them from the heads of our learners to carry out our mission?*

**Key words:** Teacher, learner, pedagogy, foreign language, culture, intercultural, cultural competence.

### **Introduction**

La protection des données personnelles, et son corollaire la préservation des libertés individuelles, est une préoccupation qui a émergé, en particulier avec le développement de l'informatique qui permet la captation, le stockage et le traitement des données. Dans ce cadre, sans compromettre le développement de l'informatique, les responsables ont cherché à créer un dispositif législatif approprié. En effet, le 18 février 2009, le Maroc a créé la commission nationale de contrôle de la protection des données à caractère personnel (CNDP). Elle a comme responsabilité de veiller à ce que les traitements des données personnelles soient licites, légaux et qu'ils ne portent pas atteinte à la vie privée et aux libertés et droits fondamentaux de l'homme<sup>1</sup>. Dans ce cadre, depuis 2011, la protection de la vie privée représente un droit constitutionnel au Maroc. Il dispose d'un régime juridique protecteur des données personnelles, à savoir la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Nous savons tous que certains usages du numérique éducatif impliquent un traitement des données personnelles des élèves. Nous pouvons donner l'exemple des enseignants qui

---

<sup>1</sup> <https://www.cndp.ma/fr/responsabilites/traitement-au-maroc/conditions.html>

s'appuient sur les outils et ressources numériques pour créer des séquences pédagogiques (pour la recherche documentaire, l'illustration des cours, la conception des contenus...). Tous ces aspects évoquent des interrogations d'ordre éthique sur l'emploi logique et sage de ces ressources et données voire la part des données personnelles dans ce système de protection.

D'une manière générale, l'Éducation nationale véhicule un très grand nombre de données liées à la vie scolaire, aux évaluations et aux résultats des élèves, aux travaux et aux devoirs qu'ils réalisent. Une panoplie de données numériques propres aux élèves et leurs familles outre le personnel de l'éducation, sont collectées, stockées et font l'objet d'un traitement continu<sup>2</sup> par un bon nombre d'intervenants notamment, les écoles et établissements scolaires, les services académiques, les collectivités territoriales et les collaborateurs privés fournissant des ressources pédagogiques et services numériques. Selon le ministre de l'Éducation nationale, de la Formation professionnelle, de l'Enseignement supérieur et de la Recherche scientifique, Saïd Amzazi<sup>3</sup>, le nombre total des élèves, étudiants et stagiaires marocains inscrits au titre de l'année scolaire 2019-2020 touchait les (9,898) millions, alors que le nombre total d'enseignants atteignait (256.493) <sup>4</sup>. Les données personnelles et éducatives concernent donc plus de 11 millions d'élèves et enseignants, sachant bien que les outils de vie scolaire sous licence privée représentent une faiblesse structurelle dans le système éducatif, plaçant celui-ci non seulement en situation de dépendance, mais également en position de vulnérabilité. Par conséquent, il est possible d'imaginer des « attaques malveillantes » qui pourraient déstabiliser les activités des établissements scolaires<sup>5</sup>. Ces données personnelles doivent être protégées, anonymisées et agrégées sachant bien qu'elles peuvent apporter une connaissance sur les territoires éducatifs, sur les voies et améliorations des apprentissages scolaires, et constituent de ce fait des opportunités pédagogiques très importantes. Elles sont ainsi une mine abondante d'informations mise à la disposition des plateformes et des développeurs.

---

<sup>2</sup> Ce traitement de données personnelles doit se faire, hors cadre domestique, dans le respect du Règlement Général sur la Protection des Données (RGPD)

<sup>3</sup> (<https://Int.ma/10-millions-decoliers-eleves-etudiants-maroc/>)

<sup>4</sup> (<https://www.google.com/search?q=combien+d+enseignant+universitaire+au+maroc&oq=combien+d%27enseignant+universitaire+au+&aqs=chrome.1.69i57j33i22i29i30l4.21754j1j4&sourceid=chrome&ie=UTF-8>)

<sup>5</sup> <https://www.cndp.ma/images/lois/CNDP-Autorisation-Prealable.pdf>

En raison du téléenseignement promu en temps de pandémie, les enseignants et les élèves étaient sollicités pour une utilisation massive et continue des outils numériques de communication, de sorte que leurs données personnelles étaient restées sans défense. La crise sanitaire a imposé le recours à des solutions commerciales (boucles WhatsApp, Google éducation, Padlet, Zoom...) faciles d'accès, non payantes, en l'absence de solutions institutionnelles adaptées. Elles échappent à un usage souverain pour l'éducation nationale. De l'autre côté, à l'instar des géants du numérique, les leaders du marché se constituent en monopole pour exiger aux usagers et aux États des solutions à caractère commercial. Or, la donnée est au cœur des enjeux éducatifs d'un côté et commerciaux de l'autre.

Désormais, la question de la circulation et de la captation des données numériques se pose en termes de souveraineté numérique et de protection des données personnelles. En fait, les données souveraines permettent à un pays de rester maître de ses choix et de ses valeurs. Dans ce contexte, le développement du numérique et en particulier de l'intelligence artificielle pose le problème éthique de l'attribution de la décision ou de l'orientation des réponses à des algorithmes qui ne sont guère neutres. Les algorithmes, source de progrès, introduisent des échappatoires. Toutefois, ils peuvent aboutir, s'ils ne sont pas maîtrisés, à des finalités incompatibles avec les valeurs et les missions de l'école. La CNDP pointe ce risque surtout que l'usage du numérique devient exponentiel à l'école ainsi que dans la vie de tous les jours. Cette double prise de conscience est donc essentielle à l'heure où l'État doit prendre des décisions politiques stratégiques dans le domaine de l'éducation, pour garantir les droits fondamentaux de ces acteurs.

### **1. Les données scolaires exportent des informations sensibles sur les élèves**

Les données propres à l'enseignement révèlent beaucoup d'informations sur ces acteurs. D'une part, le travail effectué par un élève renseigne sur son niveau scolaire et sa maîtrise des matières étudiées. De l'autre, le contenu des cours présentés par un enseignant explicite sa manière d'enseigner et ses choix pédagogiques. Par ailleurs, les moments ou lieux de connexion d'un élève ou d'un enseignant sur une plateforme numérique informent sur leurs modes de vie. Ces informations mobilisées par les données éducatives s'enrichissent en fonction de l'évolution des méthodes de traitement. Par exemple, la cadence de frappe d'une

personne sur un clavier peut fournir des informations sur son état émotionnel<sup>6</sup>. Les données portant sur le comportement des élèves et des enseignants sur une plateforme numérique peuvent également être exploitées de façon algorithmique pour les catégoriser et ipso facto, par association, les orienter vers des contenus précis tout en personnalisant le service qui leur est proposé sur la plateforme. Cette catégorisation algorithmique poussée à l'extrême induit le phénomène bien connu de « bulle » qui enferme les individus, devenant une source de discrimination et de perte d'objectivité. D'ailleurs, les données personnelles sensibles sont celles qui sont particulièrement risquées, à savoir les libertés et droits fondamentaux dont le système juridique de protection est renforcé. Il s'agit « d'informations qui révèlent une origine raciale ou ethnique présumée, des opinions politiques, des convictions religieuses ou philosophiques ou une appartenance syndicale. Il s'agit aussi de données génétiques, de données biométriques permettant d'identifier de manière unique une personne physique, de données relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle d'une personne physique. Il est interdit de collecter et d'utiliser ces données, sauf dans certains cas particuliers<sup>7</sup> ». Nous déduisons alors que le traitement des données personnelles sensibles est strictement encadré par la loi. Par rapport aux données d'éducation, il y en a celles qui sont clairement nommées (sensibles), car elles concernent par exemple la santé (allergies alimentaires ou handicaps) et sont traitées uniquement dans le cadre scolaire (alimentation à la cantine), tandis que d'autres sont qualifiées délicates sur le niveau social, puisqu'elles peuvent entraîner un préjudice aux apprenants. Dans le même cadre, les données relatives aux résultats scolaires peuvent être discriminantes pour les élèves voire nuisibles pour leurs carrières futures dans le cas où elles quittent les murs de l'école et soient dévoilées aux futurs employeurs. En effet, en les liant à d'autres données, les renseignements du contexte scolaire peuvent également révéler des informations (sensibles). Par exemple, s'il existe une corrélation entre les absences répétées d'un élève et les vacances religieuses ; il serait possible de définir sa croyance religieuse. En outre, les difficultés scolaires qui se lisent dans les évaluations ainsi que les dossiers administratifs sont susceptibles d'être reliées à d'autres données portant sur la santé telles que les troubles d'apprentissage, notamment la dyslexie ou la dyspraxie. Nous devons rappeler aussi que la connaissance des données relatives aux

<sup>6</sup> (Identifying Emotional States using Keystroke Dynamics. CHI 2011, May 7–12, 2011, Vancouver, BC, Canada)

<sup>7</sup> <https://www.cnil.fr/fr/cnil-direct/question/une-donnee-sensible-cest-quoi> et RGPD, art. 9. 10 »

élèves permet de les connaître profondément et offre la possibilité de guider leurs choix avec un risque de manipulation.

## **2. Protection des données d'éducation et consentement**

Selon le RGPD, du point de vue des libertés et droits fondamentaux, on ne peut pas considérer toutes les données liées à la scolarité des étudiants comme données personnelles qui nécessitent une protection particulière<sup>8</sup>. Nonobstant, il existe des informations qui méritent d'avoir un statut particulier. Dans ce sens, le RGPD s'occupe de la protection des données personnelles sollicitant une attention particulière, particulièrement les données éducatives jugées sensibles telles celles qui portent sur la santé. Le principe est que le droit d'accès et de traitement des données personnelles éducatives est singulièrement autorisé pour l'exécution d'une mission d'intérêt public. Dans le cas où l'extraction et l'utilisation de ces données ne respectent pas ce fondement, le désireux de ces données pourra recourir aux privilèges accordés à l'autorité publique dans le cadre d'une obligation légale ou un intérêt légitime. Nous devons signaler que les activités de traitement des données effectuées par l'école ou tout autre acteur dans le cadre éducatif doivent être basées sur le consentement voir l'acceptation du concerné, sin qua non, l'élève ne doit être ni influencé ni contraint car c'est illégal. Parmi les situations dans lesquelles le consentement d'un tuteur légal (ou de l'élève s'il est majeur) peut être requis, c'est celle où l'école a besoin d'utiliser la photo d'un élève sur son site internet pour enregistrer ses activités scolaires ou bien parascolaires. L'assentiment doit être le résultat d'un choix sincère, de sorte que l'élève/tuteur légal ne sera privé d'aucun enseignement ou bien service et pourra refuser sans condition toute atteinte et tout préjudice<sup>9</sup>. Il convient de souligner ici que même si l'accord est obtenu, l'élève doit pouvoir revenir sur sa décision et refuser, faute de quoi ce refus entraînera une violation de l'égalité avec ses pairs. De l'autre pôle, étant donné que le Ministère est bien conscient que de nombreuses activités pédagogiques reposent aujourd'hui sur l'utilisation des données personnelles des élèves, il est demandé, en collaboration avec la (CNDP), de publier un opusculé à l'intention

---

<sup>8</sup> RGPD articles 9 et 10, et considérant 51.

<sup>9</sup> Considérants 38, 58, 65, 71 et 75 du RGPD. Concernant les droits des mineurs, le RGPD considère les enfants comme vulnérables, et ce critère doit donner lieu, combiné à un autre critère issu des lignes directrices du G29, à la réalisation d'une analyse d'impact (AIPD), pour construire des traitements respectueux de la vie privée (<https://www.cnil.fr/fr/ce-quit-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>)

des enseignants pour leur conseiller d'adopter certaines attitudes et réflexes quand ils utilisent le numérique. Il doit y figurer des principes clés concernant la protection des données des élèves lors de toute activité pédagogique. À titre d'exemple, il faut surveiller toute collecte de données personnelles ou informations nécessaires au bon fonctionnement des activités scolaires tout en s'assurant que ces données sont supprimées ou stockées conformément à la réglementation. Il devrait y avoir également des instructions recommandant aux enseignants de « sensibiliser les élèves aux enjeux de la protection des données personnelles ». Pour que ces conseils soient compris et suivis, les enseignants eux-mêmes doivent reconnaître l'importance de ces préceptes et craindre les conséquences de leur non-respect. En réalité, la tâche est colossale, il est nécessaire d'encourager non seulement les élèves, mais aussi leurs familles et bien sûr les enseignants à être sérieux au niveau du respect de ces droits fondamentaux.

### **3. Les risques éventuels pour les données d'éducation**

Les données éducatives liées aux libertés essentielles sont exposées à plusieurs risques. D'un côté, les données peuvent être récupérées par divers organismes publics ou privés, fournissant des informations confidentielles sur les étudiants, ce qui pourrait mettre leur intimité en danger. En fait, la connaissance des données comportementales des élèves et des enseignants sur les plateformes numériques peut créer des incitations à se référer à des contenus ciblés, ce qui peut entraîner des manipulations et des restrictions, sachant bien que l'espace physique clos et confidentiel de la salle de classe n'existe plus lors de l'enseignement à distance. Chose qui conduit à des interférences des membres extérieurs à la classe dans l'espace virtuel. De l'autre, les données scolaires collectées et stockées par l'État peuvent faire l'objet d'attaques si le système de cybersécurité est fragile. La contrainte est même si les données personnelles des étudiants puissent être divulguées, nous ne souhaitons pas anonymiser toutes les données éducatives des étudiants, et ce, pour pouvoir les suivre d'une manière personnalisée, sachant que la pseudonymisation n'exclut pas la possibilité de ré-identification.

### **4. Les données d'éducation : une richesse stratégique nationale**

Comme nous l'avons vu précédemment, par le biais des données, on peut extraire des statistiques sur le système éducatif d'une ville, d'une région, voire d'un pays. En effet, les



données agrégées permettent d'évaluer la situation d'un pays en matière d'éducation nationale et son évolution dans le temps, devenant ainsi un enjeu de stratégie nationale. L'accès donc à ces données par d'autres pays, capables de les utiliser à mauvais escient, est susceptible de créer d'amples problèmes. Ainsi, les États doivent pouvoir sauvegarder ces informations et contrôler leur diffusion. Il faut rappeler que ces données pédagogiques représentent, tant pour les institutions publiques que privées, qu'elles soient nationales ou internationales, un véritable champ de mines pour la recherche et l'innovation pédagogiques permettant la création et le développement des dispositifs didactiques et les contenus éducatifs. Les données scolaires agrégées sont en conséquence un atout national et, à ce titre, l'éducation est une souveraineté stratégique nationale à l'instar de l'eau potable, des transports, des médias numériques ou la santé publique. Alors, il revient à l'état de les prémunir contre toute attaque et utilisation malsaines.

Dans ce sens, nous pouvons avancer certaines recommandations. Premièrement, les responsables sont demandés de définir une stratégie nationale qui veille à ce que le développement des produits éducatifs numériques respecte les valeurs fondamentales de la liberté individuelle, et ce, en donnant un statut juridique plus protecteur aux données éducatives. En effet, dans le but de protéger la vie privée des étudiants et des enseignants, il faut commencer à réfléchir sur la capacité d'inclure dans la (CNDP) le statut des « données sensibles » pour les données d'éducation. Par ailleurs, il faut minutieusement étudier et analyser les principaux outils de communication et de partage utilisés dans le cadre de l'éducation scolaire pour cerner la collaboration avec ceux qui respectent les libertés individuelles impératives. Ensuite, il faut sensibiliser les différents acteurs (enseignants, étudiants, familles, entreprises, universitaires, politiques) aux enjeux de la souveraineté numérique surtout celle qui concerne les données numériques scolaires. Et ce, en attirant leur attention sur le caractère « spécifique » des données éducatives et en incitant ces acteurs à être responsables voire méfiants dans l'utilisation de ces données. Dans le même sens, il faut renforcer les formations sur les droits à la protection des données. Ces initiatives de sensibilisation et formations doivent aller au-delà de l'éducation pour englober l'utilisation des médias sociaux par les élèves.



## 5. Former au numérique et à la citoyenneté numérique

Il faut faire un usage responsable du numérique. Dans cette perspective, les compétences numériques de base doivent être maîtrisées par tous les citoyens, en particulier les élèves, leurs familles et les enseignants. Autrement dit, il faut s'assurer que tous les citoyens disposent des compétences numériques de base, leur permettant de comprendre et d'appliquer les conseils de sécurité fournis pour protéger les données personnelles. Mais cela implique aussi de leur faire comprendre le modèle économique sous-jacent de l'offre dite gratuite des prestataires privés qui ne l'est pas en réalité. Ainsi, en connaissance de cause, ils peuvent choisir les outils gratuits de leur choix. D'ailleurs, c'est grâce à ces compétences numériques fondamentales que la citoyenneté numérique est possible. C'est-à-dire « la capacité de participer activement, de manière critique et compétente à l'environnement numérique, en s'appuyant sur la communication efficace et la créativité, pour pratiquer des formes de participation sociale respectueuses des droits de l'homme et la dignité par une utilisation responsable des technologies <sup>10</sup>». Il y a donc un enjeu éthique majeur dans la formation de tous les citoyens au numérique et à la citoyenneté numérique.

## Conclusion

On parlait de « netiquette<sup>11</sup> », un amas de normes à révéler dans nos attitudes sur Internet. Il s'agit d'une liste donnée de règles à respecter dans notre façon d'écrire un mail, de contribuer à un forum ou de publier des dépêches sur un blogue. Il y figure, par exemple, la règle qui exige de ne pas écrire en majuscules, car cela signifie du non-respect pour le lecteur. L'écriture en majuscules se lit comme une agression visuelle pour le lecteur, assimilée aux hurlements dans une communication orale.

De fil en aiguille, une bonne partie de notre vie a immigré vers le Web. Le numérique, et précisément le Web, se présente comme notre principale sphère de vie et d'action. La plupart de nos activités se réalise à l'aide d'Internet, nous contactons nos familles et amis sur le Web,

---

<sup>10</sup> Lignes directrices sur le consentement au sens du règlement 2016/679A :

[https://www.cnil.fr/sites/default/files/atoms/files/Idconsentement\\_wp259\\_rev\\_0.1\\_fr.pdf](https://www.cnil.fr/sites/default/files/atoms/files/Idconsentement_wp259_rev_0.1_fr.pdf)

<sup>11</sup> <https://primabord.eduscol.education.fr/qu-est-ce-que-la-netiquette>

nous nous y instruisons et nous y distrayons, nous y bouquinons, planifions nos voyages, faisons nos achats, administrons notre argent. Une partie sérieuse de notre vie quotidienne se vit dans l'espace numérique. Et dans le futur, cet espace va accaparer notre vie, ce qui pose la question de l'état aussi que du destin de nos informations personnelles dispersées dans le Web. Autrement dit, la protection des données personnelles véhiculées est un besoin imminent<sup>12</sup>.

Dans ce contexte, l'Éducation nationale, entrée dans l'époque du numérique, engendre un grand nombre de données amarrées à la vie scolaire, aux évaluations et aux résultats des élèves. Ces données personnelles assemblées et sauvegardées représentent les pivots de création (individualisation des enseignements, recherche, aide au travail personnel...), à condition qu'elles soient prémunies contre toute attaque malveillante tout en respectant l'éthique numérique<sup>13</sup>. D'ailleurs, les mesures du respect des éthiques inséparables des technologies numériques en éducation n'ont cessé d'intriguer plusieurs auteurs (Choi, 2016<sup>14</sup> ; Downes, 2017<sup>15</sup>; Jandrić et al<sup>16</sup>. 2018) vu que le numérique effectue un grand changement sur les activités humaines communes, et ce, en prolongeant l'action humaine dans le cadre spatiotemporel, ainsi qu'en formalisant leurs activités dans des espaces structurés. De ce fait, la présence des technologies dans le secteur d'enseignement doit être permise sous condition du respect d'une charte morale stricte et d'un ensemble de règles éthiques rigoureusement formulées.

---

<sup>12</sup> Une éthique appliquée ? (openedition.org)

<sup>13</sup> Défis et enjeux d'une éducation numérique éthique et responsable. (educavox.fr)

<sup>14</sup> Choi, M. (2016). A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. *Theory & Research in Social Education*, 44, 565-607. DOI: 10.1080/00933104.2016.1210549

<sup>15</sup> Downes, S. (2017). *Toward Personal Learning Reclaiming a role for humanity in a world of commercialism and automation*

<sup>16</sup> Jandrić, P., Knox, J., Besley, T., Ryberg, T., Suoranta, J., & Hayes, S. (2018). Postdigital science and education. *Educational Philosophy and Theory*, 50(10), 893-899. DOI: 10.1080/00131857.2018.1454000

## Bibliographie

### 1. Ouvrages généraux et spécialisés

. Choi, M. (2016). A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. *Therory & Research in Social Education*, 44, 565-607. DOI: 10.1080/00933104.2016.1210549

. Jandrić, P., Knox, J., Besley, T., Ryberg, T., Suoranta, J., & Hayes, S. (2018). Postdigital science and education. *Educational Philosophy and Theory*, 50(10), 893-899. DOI: 10.1080/00131857.2018.1454000

. (Identifying Emotional States using Keystroke Dynamics. CHI 2011, May 7–12, 2011, Vancouver, BC, Canada)

### 2. Sitographie

. (<https://www.cndp.ma/fr/cndp/qui-sommes-nous/commision.html>)

. Ce traitement de données personnelles doit se faire, hors cadre domestique, dans le respect du Règlement Général sur la Protection des Données (RGPD)

. (<https://lnt.ma/10-millions-decoliers-eleves-etudiants-maroc/>)

. (<https://www.google.com/search?q=combien+d+enseignant+universitaire+au+maroc&oq=combien+d%27enseignant+universitaire+au+&aqs=chrome.1.69i57j33i22i29i30l4.21754j1j4&sourceid=chrome&ie=UTF-8>).

. A cet effet, Index Éducation, leader français des logiciels dédiés à l'enseignement secondaire (Emploi du temps, vie scolaire...) avec 80% du marché français des logiciels de vie scolaire, a été racheté en décembre 2020, par 2 acteurs publics - Docaposte et la Banque des territoires/ Caisse des dépôts- permettant ainsi de répondre aux attentes de la communauté éducative quant à la garantie de confidentialité et d'intégrité des données collectées par les solutions d'Index Éducation, et dans une perspective de souveraineté numérique souhaitée par le ministère de l'Éducation

. <https://www.cnil.fr/fr/cnil-direct/question/une-donnee-sensible-cest-quoi> et RGPD, art. 9. 10 »

. RGPD articles 9 et 10, et considérant 51.

. Considérants 38, 58, 65, 71 et 75 du RGPD. Concernant les droits des mineurs, le RGPD considère les enfants comme vulnérables, et ce critère doit donner lieu, combiné à un autre critère issu des lignes directrices du G29, à la réalisation d'une analyse d'impact (AIPD), pour construire des traitements respectueux de la vie privée (<https://www.cnil.fr/fr/ce-quit-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>)

. Lignes directrices sur le consentement au sens du règlement 2016/679A :  
[https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement\\_wp259\\_rev\\_0.1\\_fr.pdf](https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf)

. <https://primabord.eduscol.education.fr/qu-est-ce-que-la-netiquette>

. Une éthique appliquée ? ([openedition.org](https://openedition.org))

. Défis et enjeux d'une éducation numérique éthique et responsable. ([educavox.fr](https://educavox.fr))

. Downes, S. (2017). Toward Personal Learning Reclaiming a role for humanity in a world of commercialism and automation  
<https://www.downes.ca/files/books/Toward%20Personal%20Learning%20v09.pdf>