COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

11 février 2020 T-PD(2019)06BISRev2

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES

À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

(Convention 108)

La protection des données personnelles des enfants dans les systèmes éducatifs : enjeux et solutions possibles

Projet de Lignes directrices

par Jen Persson, directrice de defenddigitalme.

Direction générale Droits de l'homme et État de droit

Les opinions exprimées dans ce document sont de la responsabilité des auteurs et ne reflètent pas nécessairement la politique officielle du Conseil de l'Europe.

L’environnement numérique façonne la vie des enfants de multiples manières, ce faisant ouvrant des opportunités et créant des risques pour leur bien être et la jouissance de leurs droits humains (de l’homme ?). Avec ces Lignes directrices, le Comité de la Convention 108 vise à aborder particulièrement la protection des données à caractère personnel dans les systèmes éducatifs, afin de prévenir d’éventuelles conséquences négatives sur les enfants et permettre le respect de leurs droits au respect de la vie privée et à la protection des données (article 8 de la of the Convention européenne des droits de l’homme).

En 2001, [l’observation générale n°1 à] la Convention des Nations Unies relative aux droits de l’enfant stipule :

« Les enfants ne sont pas privés de leurs droits fondamentaux du seul fait qu'ils franchissent les portes de l'école. Ainsi, par exemple, l'éducation doit être dispensée dans le respect de la dignité inhérente de l'enfant et doit permettre à l'enfant d'exprimer ses opinions librement… »

Pour diverses raisons, on observe une croissance rapide des acteurs commerciaux et des technologies émergentes sur le marché mondial des technologies de l'éducation (edTech) dans le monde entier. Il ne faut pas sous-estimer les implications de l'introduction d'outils numériques contrôlés de l'extérieur dans les salles de classe, ni le large éventail et le nombre d'acteurs qui traitent les données personnelles des enfants souvent en dehors de leur pays de résidence.

De nombreux logiciels commerciaux utilisés dans le domaine de l'éducation sont des "logiciels gratuits", c'est-à-dire des logiciels proposés gratuitement aux écoles, souvent dans le cadre d'un échange non explicite de données personnelles. L'expansion rapide de la technologie éducative a fait que des milliers d'entreprises contrôlent des millions de dossiers scolaires d'enfants. Les petites entreprises peuvent être incubées par des investisseurs providentiels et sont ensuite rachetées par des entreprises plus importantes. Leur propriété peut être transférée par des rachats à plusieurs reprises au cours de l'éducation d'un enfant sans que lui ni sa famille ne puissent jamais le savoir. Les entreprises exigent souvent des écoles qu'elles acceptent les modifications apportées aux conditions générales, sous peine de perdre le logiciel de base sans préavis.

Sous la pression économique pour offrir un enseignement public à faible coût et sous l'effet du marketing, l'infrastructure utilisée pour dispenser l'enseignement public peut être détenue par des entreprises commerciales. Cela peut introduire de nouveaux risques et poser de nouvelles questions de sécurité et de durabilité et peut bloquer les pratiques des logiciels propriétaires, avec des conséquences sur l'interopérabilité, l'accès et la réutilisation des données, et les impacts budgétaires et environnementaux de l'obsolescence.

Les enfants ne peuvent pas voir ou comprendre l'ampleur de leur empreinte numérique ni la mesure dans laquelle elle est distribuée à des milliers de tiers dans le paysage éducatif, tout au long de leur vie. Bien que la capacité des enfants à être acteurs soit vitale et qu'ils doivent être mieux informés de la manière dont leurs propres données personnelles sont collectées et traitées, il y a un consensus sur le fait que l'on ne peut pas et ne doit pas s'attendre à ce que les enfants comprennent seuls un environnement en ligne très complexe.

La charge d'investigation dans les écoles peut être trop importante, même pour le personnel enseignant, pour qu'il soit en mesure de comprendre les outils logiciels et leur traitement, de procéder à une évaluation adéquate des risques, de récupérer et d'offrir les informations pertinentes requises à apporter aux personnes concernées, et d'être en mesure de respecter

et de faire respecter les droits des utilisateurs. Le personnel scolaire accepte souvent le traitement de données par des vendeurs sans comprendre toutes les fonctionnalités des produits ou les implications pour les droits des enfants en matière de données. Les établissements d'enseignement ont besoin de cadres législatifs et de codes de pratique solides pour responsabiliser le personnel et pour indiquer clairement aux entreprises ce qui est autorisé et ce qui ne l'est pas lorsqu'elles traitent les données relatives aux enfants dans le cadre de l'enseignement afin de créer des conditions de concurrence équitables pour tous.

La réputation des enfants est protégée en vertu de l'article 16 de la Convention relative aux droits de l'enfant. Il est important de garantir l'intégrité et la capacité d'action des générations futures en offrant aux enfants une enfance où ils peuvent grandir et apprendre sans être touchés par la surveillance, le profilage, l'accoutumance et la manipulation non sollicités pour des finalités à venir d'entreprises commerciales. Il appartient en outre aux adultes d'aujourd'hui de veiller à ce que les protections offertes aux enfants soient non seulement appropriées pour la durée de leur enfance, mais tiennent également compte des intérêts du futur adulte et favorisent leur capacité à atteindre l'âge adulte sans entrave et à se développer pleinement et librement, à réaliser leur plein potentiel et à s'épanouir humainement. De bonnes pratiques, exemptes d'exploitation, permettront de créer un environnement fiable et adapté à l'avenir, de sorte que les familles puissent envoyer leurs enfants à l'école en toute sécurité, sans que cela entraine d'obstacle pour l'avenir.

Les législateurs et les décideurs politiques, les autorités et le personnel de l'éducation, les syndicats, les promoteurs, les fabricants et les vendeurs, les représentants des enfants et la société civile devraient traduire et promouvoir l'utilisation de ces Lignes directrices pour répondre aux obligations en matière de protection des données et de la vie privée dans le cadre de l'article 3 de la Convention 108, ainsi que les mettre à la disposition des enfants et de leurs représentants, d'une manière adaptée et accessible aux enfants.

Les parties prenantes devraient collaborer pour créer un environnement respectueux des droits, pour défendre la dignité humaine, les droits et les libertés fondamentales de chaque personne en ce qui concerne la protection des données et en particulier pour soutenir les droits de l'enfant.

Les décideurs politiques ont l'obligation de respecter, protéger et permettre la jouissance des droits de l'enfant dans l'environnement numérique, conformément aux Lignes directrices du Conseil de l'Europe sur les enfants dans l'environnement numérique, Recommandation CM/Rec(2018)7 .

Aucune disposition de ces Lignes directrices ne doit être interprétée comme excluant ou limitant les dispositions de la Convention européenne des droits de l'homme ni de la Convention 108. Elles tiennent également compte des nouvelles garanties de la Convention 108 modernisée (plus communément appelée "Convention 108+").

1. Synthèse des recommandations à l'intention des responsables de l'élaboration des politiques et des autorités éducatives

1.1 Recommandations sur le traitement légitime en pratique

a. Réexaminer la législation, les politiques et les pratiques pour s'assurer qu'elles sont conformes aux présentes recommandations, principes et autres orientations, promouvoir leur application à tout traitement des données, que ce soit vers, à partir ou au sein du secteur de l'éducation. D'après le paragraphe 1, l'obligation faite au responsable du traitement d'assurer une protection adéquate des données est liée à la responsabilité de vérifier et d'être en mesure de démontrer que le traitement de données est conforme au droit en vigueur. Les principes de protection des données énoncés dans la Convention, qui doivent être appliqués à tous les stades du traitement, y compris lors de la phase de conception, visent à protéger les personnes concernées et sont également un moyen de renforcer leur confiance.

b. Pour respecter l'article 1 et le but de la Convention, les autorités éducatives doivent définir clairement les rôles, les responsabilités et les obligations de rendre compte des membres du personnel éducatif et des autres personnes concernées afin d'établir l'autorité légale et leurs obligations respectives en ce qui concerne le traitement de données et dans le cadre des négociations et relations contractuelles avec des prestataires et des responsables de traitement des données tiers. L'une des mesures qui pourraient être prises par le responsable du traitement pour faciliter la vérification et la démonstration de conformité serait de désigner un « délégué à la protection des données » disposant des moyens nécessaires à l'accomplissement de son mandat. Il pourrait s'agir d'un agent interne ou externe par rapport au responsable du traitement au sein d'une école ou d'une autorité éducative et sa désignation devrait être notifiée à l'autorité de contrôle.

c. Les autorités de contrôle devraient veiller à ce que des normes élevées en matière de respect de la vie privée, une infrastructure de sécurité comprenant le cryptage et les lois sur la protection des données soient appliquées de manière cohérente aux technologies éducatives et que le contrôle de leur mise en œuvre s'effectue dans un cadre de coopération et d'assistance mutuelle.

d. Lors de la définition des exigences techniques des configurations par défaut, les responsables du traitement et les sous-traitants devraient choisir un paramétrage standard respectueux de la vie privée de façon que l'utilisation des applications et logiciels ne porte pas atteinte aux droits des personnes concernées (protection des données par défaut), notamment afin d'éviter de traiter plus de données qu'il n'est nécessaire pour atteindre la finalité légitime.

e. Les données doivent par défaut être limitées au minimum, adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées, non seulement au moment de la collecte mais aussi tout au long de leur cycle de vie. Les responsables du traitement et, le cas échéant, les sous-traitants, doivent procéder, préalablement au début de tout traitement, à l'examen de son impact potentiel sur les

droits et libertés fondamentales de l'enfant et doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales, conformément à l'article 10 de la Convention.

f. Les données personnelles susceptibles de révéler ou de permettre de déduire, dans le contexte des dossiers scolaires, l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres, des informations sur la santé ou la vie sexuelle et des données comportementales concernant des infractions et des procédures et condamnations pénales doivent être considérées comme des catégories de données particulières au sens de l'article 6. Par ailleurs, lorsque le traitement d'une image d'un enfant vise à révéler des informations sur son origine raciale ou ethnique, ou sur sa santé, il sera considéré comme un traitement de données sensibles. Afin d'éviter tout effet préjudiciable pour l'enfant, le traitement doit être assorti de garanties appropriées, adaptées aux risques en jeu et aux intérêts, droits et libertés à protéger.

g. La légitimité du traitement de données effectué par les autorités éducatives à des fins explicites, déterminées et légitimes, conformément à l'article 5 de la Convention, ne devrait pas être compromise par un traitement excessif fait par des tiers avec lesquels ont été conclus des contrats. Les écoles devraient déterminer les finalités du traitement le plus souvent comme nécessaires et proportionnées dans le cadre de leur mission publique et demander à des tiers de les aider à le réaliser. De manière générale, les écoles devraient être considérées comme responsables de traitement et les tiers comme des sous-traitants, le contrôle conjoint des données devant être une exception et non la règle.

h. Les contrats entre des sociétés commerciales et des prestataires publics de services d'éducation devraient empêcher toute modification importante des conditions d'utilisation susceptibles d'affecter les libertés et les droits fondamentaux des personnes concernées sans que les écoles, les enfants et leurs représentants légaux en soient informés. Les autorités devraient donner la possibilité de mettre fin au traitement de données, dans le cadre de l'article 9 de la Convention, dans des délais adéquats.

i. Les enfants ne peuvent conclure de contrats avec des tiers, par exemple avec des prestataires de services d'apprentissage en ligne. Le traitement approprié de données par de tels services doit pouvoir être fait par l'intermédiaire d'une école et reposer sur un fondement légitime prévu par la loi, conformément à ce que peuvent raisonnablement attendre les utilisateurs et sans porter préjudice à ceux qui refusent de tels systèmes.

j. En ce qui concerne le traitement de données relatives à la santé et d'autres catégories particulières de données concernant un enfant, il convient d'obtenir une attestation écrite du consentement explicite, éclairé et librement donné du représentant légal au partage de données, comme garantie appropriée au sens de l'article 6.1, lorsqu'il n'existe pas d'autre fondement légitime du traitement et que des garanties appropriées sont prévues par la loi, conformément à l'intérêt supérieur de l'enfant.

k. La réutilisation de données à des fins autres que l'éducation de l'enfant, en dehors de sa prise en charge ou indépendamment de son intérêt supérieur, telles que la diffusion de données personnelles à un employeur, un organisme caritatif ou aux médias, ou à des fins de recherche, ne devrait se faire qu'avec le consentement exprès et librement donné du représentant légal, de l'enfant, ou de la personne concernée. Des restrictions à l'exercice des présentes dispositions peuvent être prévues par la loi, conformément aux articles 11.2 et 3.

l. En vertu de l'article 5.4.e, les données personnelles qui sortent du cadre éducatif ne devraient pas être conservées plus longtemps que nécessaire sous une forme permettant l'identification des personnes concernées.

1.2 Recommandations relatives à la représentation des enfants et à la réparation en cas de non-respect de leurs droits

a. Dans toutes les décisions concernant les enfants dans l'environnement numérique, y compris le secteur de l'éducation, l'intérêt supérieur de l'enfant doit être une considération primordiale. Lorsqu'ils évaluent l'intérêt supérieur d'un enfant, les États devraient faire tout leur possible pour équilibrer et, dans la mesure du possible, concilier le droit de l'enfant à la protection avec d'autres droits, notamment le droit à la liberté d'expression et d'information, le droit d'être entendu ainsi que les droits en matière de protection de la vie privée et de participation.

b. Les capacités de l'enfant se développent de sa naissance à l'âge de 18 ans. Comme cela est indiqué dans la recommandation CM/Rec(2018)7 du Comité des Ministres et dans les lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, « *les enfants n'atteignent pas tous le même degré de maturité au même âge. Les États et d'autres parties prenantes concernées devraient reconnaître l'évolution des capacités des enfants, y compris celles des enfants handicapés ou en situation de vulnérabilité, et veiller à ce que des politiques et pratiques soient adoptées pour répondre à leurs besoins respectifs au regard de l'environnement numérique. Cela signifie aussi, par exemple, que les politiques adoptées pour réaliser les droits des adolescents peuvent différer sensiblement de celles adoptées pour les enfants plus jeunes* ».

c. Les enfants ont le droit de s'exprimer librement sur toutes les questions qui les touchent et leur opinion devrait être dûment prise en compte, en fonction de leur âge et de leur degré de maturité. Les États et les autres responsables du traitement devraient veiller à ce que les enfants soient informés, dans le cadre scolaire, des modalités d'exercice de tous leurs droits au respect de la vie privée et à la protection des données, conformément à l'article 9, en tenant compte de leur âge et de leur degré de maturité, et, s'il y a lieu, avec l'orientation et les conseils de leurs représentants légaux ou des autres personnes légalement responsables d'eux, d'une manière adaptée au développement de leurs capacités. Il conviendrait d'apporter un soutien supplémentaire dans les cas de demandes de réparation.

d. Les informations à donner sur ou à une personne concernée en milieu éducatif doivent être adaptées à un enfant de manière proactive. Les procédures de demande d'accès doivent être intelligibles, expliquer comment les enfants et leurs représentants légaux peuvent faire une demande et lire les informations qui en résulteront et expliquer les moyens accessibles d'obtenir réparation ou rectification (par exemple, dans une langue adaptée aux enfants si besoin est). Il ne suffit pas de publier sur un site Web une déclaration de confidentialité pour satisfaire aux obligations en matière de traitement loyal et se conformer à l'article 8 de la Convention et au paragraphe 68 du Rapport explicatif, qui portent sur la transparence du traitement.

e. Pour assurer la cohérence entre différents modèles éducatifs en faveur des droits des représentants légaux et de l'enfant d'accéder aux données ainsi qu'au dossier scolaire, conformément à l'article 9.1.b, les représentants légaux devraient être autorisés à exercer ces droits prévus à l'article 9 au nom de l'enfant en milieu éducatif, lorsque celui-ci, compte tenu du niveau de ses capacités, ne s'y oppose pas.

f. Les écoles doivent fournir des orientations sur l'accès des personnes concernées à leurs données et notamment, s'il y a lieu et dans le respect des lois nationales, des informations sur l'approche recommandée au cas où des enfants compétents refuseraient le partage de leur dossier scolaire avec leurs représentants légaux ainsi qu'en ce qui concerne la communication de données personnelles directement à un enfant plutôt qu'à un représentant légal dans le cadre de l'accès à ses données.

g. La transparence à l'égard d'un enfant et de ses représentants légaux devrait être favorisée par la communication active d'informations. Les études d'impact sur la protection des données (DPIA) témoignent des intentions existantes au début d'un processus de collecte de données. Des rapports sur les données traitées (« rapports sur l'utilisation des données ») doivent ensuite être mis à la disposition de tout enfant concerné, ou de ses représentants légaux lorsque l'enfant ne s'y oppose pas, sur demande et une fois par an. Ces rapports devraient démontrer aux enfants que ce qui a été fait de leurs données en pratique tout au long du cycle de traitement correspond bien à ce qui leur avait été expliqué au préalable dans les déclarations de confidentialité.

h. La notification de la conservation ou de la destruction des données personnelles devrait également devenir une pratique courante dans l'ensemble du secteur de l'éducation afin que des informations nécessaires à la transparence puissent être fournies activement sur le traitement de données lorsqu'un enfant commence, suit et termine chaque cycle de l'instruction obligatoire (à tous les âges de l'enfant, à la maternelle, dans l'enseignement primaire, dans le secondaire et dans l'enseignement supérieur et complémentaire).

i. La représentation par des tiers des enfants concernés auprès des autorités de contrôle (article 18) devrait être facilitée et renforcée. Un État membre peut prévoir, conformément à l'article 13 sur une protection plus étendue, que tout organisme, organisation ou association, indépendamment de tout mandat confié par une personne concernée, a dans l'État membre en question, le droit d'introduire une réclamation

auprès de l'autorité de contrôle compétente et d'exercer les droits visés dans la Convention s'il considère que les droits d'une personne concernée ont été violés du fait du traitement de données.

j. Il faudrait permettre aux enfants d'accéder aisément aux sanctions et recours juridictionnels et non juridictionnels visant les violations des dispositions de la Convention prévus à l'article 12 de la Convention, afin de renforcer le respect des droits des enfants énoncés dans la Convention des Nations Unies relative aux droits de l'enfant (article 12). Les États qui ne prévoient pas encore la possibilité de déposer une plainte collective telle qu'une action de groupe ou une action en justice dans l'intérêt général devraient mettre ces outils en place afin de rendre les tribunaux plus accessibles pour de nombreux enfants touchés par des activités commerciales, dans le cadre de la coopération et de l'entraide des autorités de contrôle (articles 15, 16 et 17.3).

k. Lorsque les voies de recours réglementaires ont été épuisées, les mineurs qui engagent une procédure judiciaire fondée sur la Convention 108 devraient être protégés contre les condamnations aux dépens, afin de bénéficier, quels que soient leur nationalité et leur lieu de résidence, de l'assistance d'une autorité de contrôle, au sens des articles 15 et 18, pour exercer leurs droits énoncés dans la Convention.

2. Recommandations à l'intention du responsable du traitement

2.1 Recommandations sur le traitement en pratique dans un cadre scolaire

a. Les passations de marchés et la législation doivent être conformes à l'observation générale n° 16 (2013) de l'ONU sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant[1]. Les États doivent par exemple prendre les mesures nécessaires pour que les marchés publics soient attribués à des soumissionnaires déterminés à respecter les droits de l'enfant ; de plus, ils ne devraient pas investir de fonds publics ou d'autres ressources dans des activités commerciales qui ne sont pas respectueuses de ces droits.

b. Les autorités et les entreprises doivent assumer la responsabilité commune qui leur incombe de respecter les droits de l'enfant dans l'environnement numérique et de garantir un traitement sûr, loyal et transparent, quelle que soit sa complexité. Si le traitement de données est trop difficile à expliquer pour satisfaire aux obligations en matière de transparence énoncées à l'article 8 de la Convention, il n'est peut-être pas adapté au traitement utilisant les données des enfants pour des interventions qui risquent de porter atteinte à leurs libertés et droits fondamentaux ou qui ont des conséquences non négligeables.

c. Les fournisseurs devraient faciliter l'évaluation de leur aptitude à traiter adéquatement les données des élèves par un code de conduite un certificat approuvé ou, conformément à l'article 14.3.b de la Convention ou à l'article 40 du RGPD.

[1] Comité des droits de l'enfant, observation générale n° 16 (2013) sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant (https://www.unicef.org/csr/css/crc.c.gc.16._french.pdf).

d. Une attention particulière devant être accordée aux droits des enfants et d'autres personnes vulnérables en matière de protection des données, les autorités éducatives doivent veiller à ce que les membres du personnel scolaire soient formés à leurs droits et responsabilités relatifs au traitement des données dans le cadre de leur emploi. Ils devraient être en mesure, grâce au renforcement continu de leurs compétences professionnelles, de comprendre le rôle qui leur revient aux fins de la réalisation de l'objet et du but de la Convention et des activités visées à l'article 2.

e. Avant l'introduction de nouvelles politiques ou technologies entraînant le traitement de données relatives à des enfants dans le cadre éducatif, chaque partie veillera à ce que le personnel concerné dispose du niveau de formation, des ressources et des capacités nécessaires pour s'acquitter d'une obligation de vigilance conforme aux dispositions de l'article 10, requise dans toute procédure de passation de marchés, notamment pour comprendre les mesures techniques et organisationnelles appropriées et pour réaliser des études d'impact relatives à l'éthique et au respect de la vie privée.

f. Étant donné que les établissements d'enseignement ne sont pas tous des écoles, toutes les parties doivent considérer le rôle des enseignants ou du personnel équivalent en ce qui concerne l'obligation de vigilance dans l'acquisition d'outils qui traitent les données d'enfants afin d'assurer le respect des droits d'un enfant ou de son représentant légal lors de la prise de décisions sur l'introduction éventuelle de nouveaux outils, qu'ils soient achetés ou mis à disposition gratuitement.

g. Les responsables du traitement doivent reconnaître que les enfants ne peuvent consentir librement à l'utilisation de services proposés par des tiers, en particulier lorsque le déséquilibre des pouvoirs est tel, dans un cadre éducatif ou dans le secteur public, que cela ne peut être librement refusé sans préjudice.

h. Le droit de s'opposer au traitement de données doit être accordé aux enfants et aux représentants conformément à l'article 9.1.d.

i. Une opposition au traitement de données à des fins de marketing devrait entraîner l'effacement ou le retrait sans condition des données personnelles visées.

j. Conformément à l'article 9.d sur le droit d'une personne de s'opposer à tout moment à ce que des données personnelles la concernant fassent l'objet d'un traitement, la publicité ne devrait pas être considérée comme un motif légitime justifiant un traitement qui prévaudrait sur les intérêts ou les droits et libertés fondamentales de l'élève. L'éducation des enfants devrait être protégée de toute exploitation commerciale afin de permettre leur développement libre et entier, dans le respect de leurs droits et libertés fondamentales tels qu'ils sont inscrits dans la Convention des Nations Unies relative aux droits de l'enfant[2].

[2] Article 29.1 : Les États parties conviennent que l'éducation de l'enfant doit viser à : a) favoriser l'épanouissement de la personnalité de l'enfant et le développement de ses dons et de ses aptitudes mentales et physiques, dans toute la mesure de leurs potentialités ; b) inculquer à l'enfant le respect des droits de l'homme et des libertés fondamentales, et des principes consacrés dans la Charte des Nations Unies.

k. Lorsque les familles ou l'enfant exercent leur droit d'opposition, les écoles sont tenues d'offrir, comme recours au sens de l'article 9.1.d, un niveau adéquat d'enseignement dispensé selon d'autres modalités, sans préjudice pour l'enfant.

l. Conformément à l'article 9.d sur le droit d'une personne de s'opposer à tout moment à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, la conservation d'un dossier permanent, sous quelque forme que ce soit, à des fins d'analyse de données et de mise au point de produits ne devrait pas être considérée comme un motif légitime justifiant un traitement qui prévaudrait sur les intérêts ou les droits et libertés fondamentales de l'enfant.

m. Conformément aux principes de limitation des finalités et de conservation minimale des données, les accords signés par les écoles devraient interdire tout traitement des données personnelles par des tiers qui viserait à désidentifier ou anonymiser les données pour les conserver et les réutiliser à des fins dépassant la mission de l'école et ce que le représentant légal ou l'enfant peuvent raisonnablement attendre.

n. Les accords sur le traitement de données assortis de conditions d'utilisation que les écoles ne peuvent pas modifier peuvent priver ces dernières de la capacité de limiter les données qu'une entreprise peut extraire, ses méthodes et ses finalités de traitement. De telles conditions d'utilisation augmentent le risque que les sous-traitants assument le rôle de responsables du traitement. Les sociétés commerciales qui vendent à des prestataires publics de services d'éducation devraient permettre aux écoles de modifier les conditions d'utilisation des contrats types et de pouvoir indiquer leur opposition sans pénalité en cas de nouvelle politique commerciale ou de changements tels que le rachat d'une entreprise. Les entreprises doivent avertir les écoles des modifications des conditions d'utilisation en respectant une période de préavis qui permette d'assurer une transition commerciale adéquate et en permettant de mettre fin au traitement de données.

o. Les établissements d'enseignement devraient établir et publier un rapport d'audit sur la protection des données à leur niveau afin de montrer qu'ils s'acquittent de leur responsabilité et de prouver la transparence du traitement de données faisant intervenir des tiers, ainsi qu'un registre des destinataires auxquelles ils ont transmis des données personnelles (par exemple pour des outils administratifs et d'apprentissage en ligne). En outre, la transparence devrait être renforcée par la publication de manière proactive, d'études d'impact sur la protection des données, de déclarations de confidentialité et de toute modification ultérieure de conditions d'utilisation, en rendant compte de toute violation, et en partageant tout rapport d'audit sur les fournisseurs ou les sous-traitants.

p. Selon les principes énoncés dans la Convention qui visent à protéger les personnes concernées et également à renforcer leur confiance, les responsables du traitement et les sous-traitants ne doivent pas vendre des données personnelles d'enfants collectées au cours de leur scolarité, ni les soumettre à un nouveau traitement en vue de vendre des données anonymisées ou désidentifiées.

q. Conformément au droit interne des États membres, il convient de mettre en œuvre des codes de pratique clairs à l'intention des personnes lorsque les membres du personnel ou les enfants sont susceptibles d'accéder aux logiciels de l'école au moyen d'appareils électronique personnels. Ces codes devraient définir clairement les usages appropriés, les limitations et les conséquences de l'usage d'un appareil personnel – en particulier lorsque des logiciels ou des applications mobiles sont installés.

r. Afin de réduire les risques qu'un dossier permanent unique présente pour les droits et libertés des enfants, il convient de faire « table rase » du passé en supprimant, à leur entrée dans l'âge adulte, les données les concernant qui étaient conservées par un organisme commercial ou tiers. Il existe des exceptions pour un usage compatible, lorsque la conservation licite et des garanties appropriées sont prévues par la loi, conformément à l'article 5, et lorsque cela est directement dans l'intérêt supérieur de la personne concernée.

s. Les écoles ne devraient garder que les dossiers des élèves sortants qui sont nécessaires et proportionnés, conformément à l'article 5 et aux fins de l'application de l'article 7.1, et veiller à ce que des tiers, sans fonction statutaires, ne conservent pas de dossier permanent sur l'enfant ou sur son comportement.

t. Les dossiers ne devraient pas être conservés sous une forme permettant l'identification des personnes concernées pendant une durée plus longue que nécessaire, en particulier au-delà de la scolarisation, conformément aux dispositions de l'article 5.4, de l'article 7.2, de l'article 8.1 et de l'article 9, lorsqu'une telle exception est prévue par la loi, qu'elle respecte l'essence des droits et libertés fondamentales, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique aux fins de l'article 11.

u. Le couplage de données du dossier de l'élève avec d'autres données personnelles ne devrait pas constituer une pratique régulière et les personnes concernées doivent en être informées avant tout nouveau traitement effectué à des fins qui doivent être conformes aux dispositions de l'article 5.3.b de la Convention. Les données avec lesquelles les données scolaires seront couplées doivent également être accessibles à la personne concernée ou à ses représentants légaux. Le traitement de données visant des objectifs similaires devrait faire l'objet d'une étude d'impact sur la vie privée et d'un contrôle éthique s'il est effectué à des fins de recherche.

v. Pour garantir la transparence et l'application du principe de responsabilité à tous les stades du traitement de données, les autorités éducatives devraient, à leur niveau, tenir et publier de manière proactive un registre de leurs partenaires en matière de traitement de données, tels que les fournisseurs et les sous-traitants, ainsi que, par souci de transparence, un registre des destinataires, que ceux-ci reçoivent des données par l'octroi d'un accès ou dans le cadre de leur diffusion.

w. Chaque responsable du traitement garantira la transparence[3] de ses politiques relatives au traitement de données, en rédigeant, en tenant à jour et en publiant ses politiques sur le traitement de données – y compris le fondement juridique et les finalités escomptées du traitement –, sur la conservation et le partage des dossiers des élèves, sur les droits des personnes concernées conformément à l'article 9 et sur les responsabilités du responsable du traitement. Les politiques concernant la confidentialité professionnelle devraient également être rendues publiques.

x. Les responsables du traitement doivent garantir la transparence des mesures techniques et organisationnelles prises en ce qui concerne le traitement des données des enfants après qu'elles ont été transférées aux sous-traitants ou destinataires, en tenant compte des obligations relatives à la protection des données à caractère personnel à tous les stades du traitement prévues à l'article 10.3. Afin de s'acquitter de cette obligation, les institutions éducatives devraient publier régulièrement , pour le traitement des données à caractère personnel dont elles sont responsables, des informations sur les sous-traitants et les coresponsables avec lesquels elles collaborent et publier également des études d'impact relatives à la protection des données, des évaluations sur les droits de l'enfant et les risques afférents, les accords de partage des données, les conditions d'utilisation énoncées dans les contrats et des déclarations de confidentialité. Le traitement par chaque partie devrait être défini dans des dispositions contractuelles et rendu public, en étant par exemple mis en ligne.

y. Les responsables du traitement doivent, à titre proactif, informer du traitement les personnes concernées au moment de la collecte, pendant le traitement et tout au long du cycle de traitement des données personnelles, afin de satisfaire aux obligations en matière de transparence énoncées à l'article 8 de la Convention.

2.2 Recommandations sur la participation des enfants et de leurs représentants légaux

a. Pour que les enfants et leurs représentants légaux comprennent les droits que leur confère l'article 8.1.e, les communications sur le traitement de données doivent se faire sous forme intelligible et correspondre au niveau de compétence de l'enfant. Toute chaîne de diffusion de données doit pouvoir être expliquée dans une langue adaptée aux enfants et être conforme au principe de responsabilité au moment de la collecte[4].

b. Au moins une fois par an, les autorités éducatives devraient informer de manière proactive, les élèves et leurs représentants légaux du traitement de données fait par

[3] Comme le Groupe de travail « Article 29 » l'a recommandé dans ses lignes directrices sur la transparence, si les responsables du traitement ont des incertitudes sur le niveau de compréhensibilité et de transparence, en particulier auprès des enfants, des informations et de l'efficacité des interfaces utilisateur, avis, politiques, etc., ils ont la possibilité de tester ces derniers au moyen, par exemple, de différents mécanismes tels que des panels d'utilisateurs, des tests de lisibilité, des interactions formelles et informelles ou en dialoguant, entre autres, avec des groupes d'entreprises, des organisations représentatives des intérêts des consommateurs ou des organes réglementaires, le cas échéant (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

[4] Paragraphe 68 (Transparence du traitement) du Rapport explicatif sur le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91b).

l'institution, l'État ou des entreprises privées, en publiant une déclaration annuelle ou en la fournissant sur demande dans un délai raisonnable et en énumérant tous les sous-traitants et responsables du traitement des données personnelles des enfants qui sont traitées par l'intermédiaire de l'école et par des tiers avec lesquels celle-ci a passé contrat, afin de permettre la compréhension nécessaire à l'exercice des droits des personnes concernées énoncés à l'article 9.1. Ces informations devraient être fournies par l'intermédiaire de l'école.

c. Lorsque l'enfant quitte le système éducatif, seule la quantité minimale nécessaire de données permettant de l'identifier devrait être conservée, et ce dans son intérêt supérieur, par exemple pour attester de ses résultats, préserver ses futurs droits d'accès et satisfaire aux obligations légales. Une copie complète du dossier devrait être mise à la disposition de l'enfant compétent ou de son représentant légal, accompagnée d'informations sur les obligations en cours en matière de traitement et de conservation des données, même après la fin de la scolarité de l'enfant.

d. Lorsqu'un enfant quitte un établissement scolaire, l'autorité éducative, dans son rôle de responsable du traitement, doit être en mesure de lui fournir sur demande, un état indiquant les tiers auxquels ses données personnelles ont été communiquées, toutes les politiques de conservation et la date de destruction prévue. Ces informations devraient continuer d'être mises à la disposition de la personne concernée de manière proactive et à intervalle raisonnable, tout au long du cycle de traitement.

e. Afin que les données à caractère personnel soient traitées loyalement et de manière transparente conformément à l'article 5.4.a, les pouvoirs publics devraient adopter une position par défaut consistant à associer les représentants légaux aux décisions avant de partager les données personnelles des enfants concernés, sauf dans les cas où un enfant compétent refuse cette participation ou lorsque ce partage menace l'intérêt supérieur de l'enfant.

f. Les parties devraient reconnaître que le consentement libre, spécifique, éclairé et non-équivoque de la personne concernée au traitement des données est impossible à obtenir dans le cas d'un enfant, compte tenu du déséquilibre en matière de pouvoir entre une autorité publique et un mineur, sauf lorsqu'il s'agit d'une opposition exprimant le retrait du consentement.

g. Les représentants légaux devraient être autorisés à exercer les droits énoncés à l'article 9 au nom de l'enfant scolarisé dès lors que celui-ci, compte tenu de son niveau de capacité, ne s'y oppose pas. Pour protéger les droits dès la conception et par défaut, lorsque la possibilité est donnée à l'enfant ou à son représentant légal de s'opposer au traitement, l'obligation d'obtenir le consentement explicite (*opt-in)* est plus appropriée que *l'opt-out.*

h. Les écoles ne peuvent partir du principe qu'elles ont le consentement des représentants légaux ou des enfants pour transmettre des données à des prestataires tiers mais doivent plutôt obtenir, avant le traitement, une autre base légale pour leur propre rôle dans le traitement de données et s'assurer de la validité de la base licite

du traitement effectué par tout destinataire des données collectées par une école ou une autorité éducative ou en son nom.

i. Les parties veillent à ce que le traitement de données soit effectué sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi avant que les données d'un enfant relevant des catégories particulières définies à l'article 6 puissent être partagées à des fins autres que sa prise en charge directe et son éducation par l'institution qu'il fréquente. Si un représentant légal ou l'enfant compétent s'y oppose, les données ne peuvent être partagées.

j. Les parties veillent à ce que le traitement de données soit effectué sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi avant que les flux transfrontières de données à caractère personnel puissent avoir lieu, et sous réserve de niveaux de protection appropriés, conformément aux articles 14.3 et 4. Si un représentant légal ou l'enfant compétent s'y oppose, les données ne peuvent être partagées.

k. Lorsque le traitement de données s'est effectué sur la base du consentement libre, spécifique, éclairé et non-équivoque du représentant légal de la personne concernée et que celle-ci est un enfant, l'aptitude du représentant à exercer au nom de l'enfant les droits prévus par la loi expirera lorsque l'enfant compétent atteindra l'âge de la maturité prévu par la loi de l'État membre. Le processus d'obtention du consentement doit alors être transféré à la personne concernée, à savoir l'enfant du représentant légal, et son consentement doit être demandé pour qu'il puisse exercer ses droits en tant qu'adulte.

l. Le consentement libre, spécifique, éclairé et non-équivoque des représentants légaux devrait être requis avant que leurs propres données personnelles soient transférées à des établissements d'enseignement commerciaux par l'intermédiaire du système scolaire dans le cadre du dossier scolaire de l'enfant, et ils doivent pouvoir le refuser sans aucun préjudice.

m. Lorsque l'enfant achève le cycle d'enseignement obligatoire, quitte une école pour une autre ou passe du primaire au secondaire, puis à l'enseignement supérieur ou complémentaire, les autorités concernées devraient avoir conscience du fait que la base légale du consentement peut ne plus s'appliquer lorsque l'enfant n'est plus scolarisé ou directement pris en charge par leurs soins et devraient chercher à obtenir régulièrement un nouveau consentement au traitement de données ou disposer d'un autre fondement légitime pour conserver les données tout au long de leur cycle de traitement.

n. Le contenu diffusé sur les réseaux sociaux provenant des comptes personnels et des forums publics constitue des données personnelles qui sortent du domaine de compétence de l'école. De telles données provenant des représentants légaux, des enfants ou du personnel ne peuvent faire l'objet d'un traitement par les écoles qu'avec le consentement des personnes concernées car elles ne relèvent pas de la fonction

statutaire et du cadre éducatif de l'école. Les pages des associations de parents d'élèves diffusées sur les réseaux sociaux peuvent faire l'objet d'un tel traitement. Le traitement de telles informations provenant de l'accès d'un enfant à des services pendant les heures passées à l'école ne devrait pas faire partie de son dossier permanent ni être conservé s'il n'existe pas de finalités explicites prévues par la loi conformément à l'article 11.

2.3 Recommandations sur l'utilisation de données dans le cadre de décisions automatisées et de profilage

a. En vertu du principe énoncé à l'article 9.1.a de la Convention, tout traitement de données, par quelque moyen technologique que ce soit, doit pouvoir être expliqué d'une façon intelligible à un l'enfant.

b. Toute personne a le droit de ne pas être soumise à une décision l'affectant de manière significative qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte. Conformément aux articles 9.a et 9.c, elle devrait pouvoir prendre aisément connaissance du raisonnement qui sous-tend le traitement de données lorsque les résultats de ce traitement lui sont appliqués.

c. Il est recommandé, dans le principe 3.5 de la recommandation CM/Rec(2010)13 du Conseil de l'Europe et de son exposé des motifs[5], d'interdire en principe le profilage de personnes ne pouvant librement exprimer leur consentement, en particulier par exemple, les personnes atteintes d'incapacité ainsi que les enfants, au sens de la Convention des Nations Unies relative aux droits de l'enfant. Il est considéré qu'une telle interdiction de principe est nécessaire au vu des risques de manipulation et de discrimination négative que représente le profilage eu égard à ces catégories de personnes. L'interdiction peut être levée par les États membres lorsque l'utilisation du profilage se fait dans l'intérêt légitime des personnes concernées (ainsi, pour la prévention d'un danger particulier dont elles doivent être averties, ou pour le bénéfice d'une aide dont elles ont spécifiquement besoin) ou dans le cadre d'un intérêt public supérieur consacré par la loi et prévoyant des garanties appropriées. Les résultats scolaires des enfants ne devraient pas faire l'objet d'un profilage régulier visant à évaluer les systèmes, par exemple les écoles ou la gestion des performances des enseignants.

d. En cas de recours à l'intelligence artificielle, le développement et l'utilisation des outils concernés doivent être évalués pour veiller à ce qu'ils ne soient pas discriminatoires, n'aggravent pas la fracture numérique et ne comportent ou ne renforcent pas de préjugés. Tout outil qui utilise des données provenant d'enfants nécessite que soit réalisées des études d'impact sur la protection des données et la vie privée et des études d'impact sur les droits de l'enfant[6].

[5] Recommandation CM/Rec(2010)13 et exposé des motifs du Conseil de l'Europe (2011) (https://rm.coe.int/16807096c4).

[6] Comité des droits de l'enfant, observation générale nº 16 (2013) sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant (https://www.unicef.org/csr/css/crc.c.gc.16._french.pdf).

e. Quand des données sont utilisées à des fins d'évaluation, de prévision ou de prise de décision automatisée, les enseignants et autres membres du personnel, les apprenants, les représentants légaux et les enfants devraient avoir accès dans des conditions de transparence au processus et aux informations relatifs au raisonnement qui sous-tend le traitement de données lorsque les résultats de ce traitement leur sont appliqués. Le droit de faire part de son opposition, de contester les évaluations et les mesures qui en résultent et de demander qu'une décision soit plutôt prise par des êtres humains devrait être proposé de manière proactive. Les personnes concernées doivent avoir la possibilité de prouver l'inexactitude éventuelle des données à caractère personnel avant leur utilisation, la non-pertinence du profil qu'il est prévu d'appliquer à leur situation particulière ou d'autres facteurs qui auront un impact sur le résultat de la décision automatisée, impact qui pourrait être particulièrement durable dans le cas d'un enfant.

f. La personnalisation du contenu peut constituer (parfois) un élément intrinsèque et attendu de certains services en ligne et peut donc être considérée comme nécessaire, dans certains cas, à l'exécution du contrat avec l'acquéreur de services tel que l'école, mais pas avec l'enfant car ce dernier n'est pas en mesure de conclure un contrat[7].

2.4 Recommandations sur la biométrie

a. Parmi les bonnes pratiques relatives au traitement des données biométriques des enfants, il peut être fait obligation aux responsables du traitement de déclarer expressément ce traitement aux autorités de contrôle afin que celles-ci puissent le suivre dans la limite de leurs compétences territoriales en reconnaissant le caractère sensible des données et en reconnaissant qu'une attention particulière doit être portée au droit à la protection des données des enfants et des autres personnes vulnérables afin d'aider les personnes concernées à exercer les droits prévus à l'article 18 de la Convention.

b. L'utilisation de la biométrie dans les écoles à des fins telles que la vérification de l'identité et la surveillance à distance n'est autorisée qu'à condition que des garanties appropriées, venant compléter celles de la Convention, soient prévues par la loi conformément à l'article 6.1, compte tenu des risques, notamment de discrimination toute la vie durant, que le traitement de données sensibles peut présenter pour les droits et les libertés fondamentales de l'enfant.

c. Les données biométriques collectées auprès d'enfants à des fins éducatives ne devraient pas sortir du cadre scolaire et ne devraient pas être mises à la disposition de tiers, aux fins, internes ou externes, d'application des lois, de prévention de la criminalité, de l'immigration ou d'autres raisons ne relevant pas de l'éducation. Lorsqu'il existe des techniques moins invasives de traitement de données, les données biométriques d'enfants ne devraient pas faire l'objet d'un traitement routinier. Les applications de la biométrie qui visent à aider les personnes ayant des besoins en matière d'accessibilité, pour leur bénéfice direct, par exemple grâce à l'oculométrie,

[7] La personnalisation du contenu peut constituer (mais ne constitue pas toujours) un élément intrinsèque et attendu de certains services en ligne et peut donc être considérée comme nécessaire à l'exécution du contrat avec l'acquéreur de services dans certains cas (Lignes directrices 2/2019 du Comité européen de la protection des données).

constituent des exceptions pour lesquelles un traitement de données peut être effectué à condition que des garanties appropriées soient prévues par la loi.

d. Compte tenu du fait que les données biométriques visées à l'article 6 de la Convention identifient un individu de façon unique, les autorités devraient également avoir conscience du caractère sensible du traitement de données comportementales d'un enfant qui peuvent ne pas être utilisées aux seules fins de la vérification d'identité mais peuvent être traitées pour influencer un état physique ou mental, comme dans la réalité virtuelle immersive. Les caractéristiques de la voix, du mouvement des yeux, de la démarche, des émotions et de l'humeur et les réactions à la neurostimulation peuvent faire l'objet d'un traitement visant à influencer ou surveiller le comportement et le développement physique ou affectif d'un enfant. De telles données devraient être traitées avec autant de précautions et de prudence que les données biométriques mentionnées dans la Convention.

2.5 Recommandations relatives au traitement des données provenant du contenu et des communications en ligne

a. Le filtrage et le blocage de contenus diffusés sur Internet peut s'effectuer sans contrôle ni profilage d'individus. Si des données à caractère personnel sont traitées dans le but de protéger les enfants de dangers en ligne, toutes les obligations habituelles en matière de protection des données doivent être satisfaites avant que le traitement commence. Il s'agit par exemple d'établir un fondement juste et légal au traitement, de veiller à ce que le traitement soit nécessaire et proportionné aux dangers que l'on cherche à éviter et de fournir les informations nécessaires à la transparence.

b. Une mesure « nécessaire dans une société démocratique » doit poursuivre un but légitime et donc répondre à un besoin social impérieux qui ne peut être atteint par des moyens moins intrusifs. De plus, elle doit être proportionnée au but légitime poursuivi et les motifs avancés par les autorités nationales pour la justifier doivent être pertinents et adéquats. Enfin, elle doit être établie par une loi accessible et prévisible qui doit être suffisamment détaillée.

c. Pour que le personnel scolaire prenne des décisions éclairées lors du contrôle des données des contenu et communications en ligne des enfants et du personnel des écoles, la connaissance de la législation sur la protection des données n'est pas suffisante. Il est par exemple indiqué à l'article 5 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 consacrée à la confidentialité des communications que « *Les États membres garantissent la confidentialité des communications et des données relatives au trafic y afférentes […] interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés …* » et que la « loi » doit effectivement être « *suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu – en s'entourant au besoin de conseils éclairés – de régler sa conduite* »,

d'en « *prévoir les conséquences pour lui*[8] » et « *de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences pouvant résulter d'un acte déterminé*[9] ».

d. Il est recommandé, dans le principe 3.8 de la Recommandation CM/Rec(2010)13 du Conseil de l'Europe et son exposé des motifs[10], que « *ne soient pas autorisées la diffusion et l'utilisation de logiciels visant l'observation ou la surveillance de l'usage d'un terminal ou de réseaux de communication et qui permettraient ainsi la collecte de données et le recours à des méthodes de profilage, et ce à l'insu des personnes concernées, à moins que le droit interne ne le stipule expressément et ne prévoie des garanties appropriées. Ainsi, on peut difficilement accepter que, grâce à des trous de sécurité des logiciels proposés sur le marché, certains puissent s'introduire dans l'ordinateur d'un individu ou simplement surveiller toutes ou certaines utilisations du terminal ou du réseau, de manière à constituer des profils d'internaute* ».

e. Le traitement des données à caractère personnel doit, pour être conforme aux dispositions de l'article 3 de la Convention, être licite et doit s'effectuer de façon loyale et de manière transparente conformément à l'article 5.2.a.

f. Les systèmes ne peuvent à la fois répondre aux obligations de transparence en matière de traitement des données prévues par la Convention et également contrôler le contenu ou les communications en ligne des enfants dans le but de les prendre en défaut ou d'exercer une surveillance secrète. Une telle fonctionnalité devrait être encadrée par la législation en raison des possibilités d'ingérence massive dans la vie privée et familiale, des risques qui en résultent pour la liberté d'expression et des risques qu'elle présente de porter atteinte, par son effet dissuasif, au libre et plein épanouissement de l'enfant. Les activités de traitement menées à des fins de sécurité et de défense nationales doivent être soumises aux conditions applicables relatives au caractère effectif des mécanismes de contrôle et de supervision indépendants.

g. La possibilité de recourir à la vidéosurveillance ou à des webcams pour filmer ou photographier un enfant secrètement et à son insu devrait être considérée comme interdite à l'école, même à titre exceptionnel, à moins que l'on puisse s'assurer de satisfaire aux obligations relatives à la légitimité du traitement (article 5), à la sécurité (article 7) et à la protection des droits et libertés de l'enfant, notamment la liberté d'expression (article 11.1.b).

h. Les responsables du traitement devraient rendre compte au moins une fois par an, de façon transparente, aux enfants et aux représentants légaux, de la façon dont ils se sont acquittés de l'obligation relative à la transparence du traitement des données des personnes concernées et, conformément à l'article 8.1.e, des moyens d'exercer les droits énoncés à l'article 9. Ils pourraient par exemple rendre compte des taux de filtrage et du blocage de contenu. Au niveau de l'enfant, toute surveillance devrait être

[8] Arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *Leander c. Suède* (1987), nº 9248/81, série A nº 116, § 50,

[9] Arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *Margareta et Roger Andersson c. Suède* (1992) nº 12963/87, série A nº 226-A, p. 25, § 75.

[10] Recommandation CM/Rec(2010)13 du Conseil de l'Europe et son exposé des motifs (2011) (https://rm.coe.int/16807096c4).

assortie d'une obligation de rapport sur la classification des enfants, la conservation des données, leur accès et leur diffusion, le volume et le contenu des fichiers journaux, les taux d'erreur et de rectification et les réparations. Au niveau de l'école, un rapport devrait être fourni chaque année aux responsables légaux et aux élèves, être disponible sur demande et faire l'objet d'un suivi pour s'assurer que les principes de nécessité et de proportionnalité sont respectés en pratique, pour contrôler les capacités et éviter toute dérive des objectifs, et pour accroître la transparence en ce qui concerne toute discrimination éventuelle à l'égard de certaines communautés afin de permettre l'exercice du droit individuel de mettre fin à des pratiques inéquitables et de faciliter l'obtention d'une réparation.

i. Toute surveillance en ligne ciblée des données provenant du contenu et des communications en ligne des enfants exercée aux fins de la lutte d'un État contre des programmes d'extrémisme violent mis en évidence en milieu éducatif devrait faire l'objet d'un contrôle judiciaire indépendant.

3. Recommandations à l'intention des développeurs, des fabricants et des fournisseurs

3.1 Recommandations relatives aux outils technologiques éducatifs

a. Le traitement des données portant sur des enfants dans le secteur éducatif devrait être soumis à un degré d'exigence élevé dès sa conception afin d'atteindre des niveaux de qualité acceptables et de respecter le droit et les principes de protection des données dès la conception et par défaut. Cela doit s'appuyer à la fois sur des lignes directrices sectorielles, des codes de pratiques statutaires et un contrôle plus spécifique au secteur exercé par les instances de réglementation.

b. De telles normes peuvent être définies dans des codes de pratique et il est impératif que leur élaboration s'inscrive dans le cadre d'une vaste coopération avec les développeurs et le secteur privé, les praticiens du secteur de l'éducation, les milieux universitaires, les organisations représentant les enseignants et les familles, ainsi que la société civile.

c. Les développeurs doivent veiller à ce que leur propre compréhension de toutes les fonctionnalités des produits destinés au secteur éducatif qu'ils conçoivent puisse être suffisamment expliquée pour répondre aux exigences réglementaires et légales du secteur et éviter dès la conception d'entraîner une lourde charge d'investigation qui est inappropriée pour les écoles et les enfants.

d. La géolocalisation visant à identifier le lieu de l'utilisation et l'utilisateur, à cibler des fonctions intégrées aux applications ou à procéder à un profilage devrait comprendre un indicateur qui signale quand elle est active. Ces profils et historiques devraient être faciles à effacer à la fin d'une session. Il ne devrait pas être nécessaire de transmettre ces informations à un nombre indéfini de personnes.

e. Aux fins du respect escompté des principes de la protection des données dès la conception et par défaut, il conviendrait notamment, lors de la conception des outils, de ne pas inciter les enfants, par diverses fonctions, à fournir des données à caractère personnel non nécessaires ou à affaiblir leurs paramètres de confidentialité.

f. Les informations sur la confidentialité et les autres conditions d'utilisation, politiques et normes communautaires publiées doivent être concises et rédigées dans une langue claire et adaptée aux enfants. Les méthodes de communication adaptées aux enfants ne devraient pas délayer les explications nécessaires à un traitement loyal, sans être toutefois excessives, et devraient être distinctes des conditions légales et contractuelles destinées aux représentants légaux et aux enseignants.

g. Le traitement de données aux fins d'amélioration du service doit être restreint et s'effectuer dans les limites de la fourniture du service principal ainsi que des attentes raisonnables et de la fourniture du service faisant l'objet du contrat avec les utilisateurs, aux fins par exemple du perfectionnement de la sécurité. L'analyse de données et le suivi de l'utilisateur ne devraient pas être considérés comme une forme d'amélioration du service ou de perfectionnement de la sécurité et ne sont pas nécessaires à l'exécution d'un contrat. Les perfectionnements apportés à un produit, par exemple pour ajouter de nouvelles fonctions à une application ou améliorer son fonctionnement, devraient nécessiter une nouvelle acceptation ou un nouveau consentement ainsi qu' une adhésion explicite avant leur installation *(opt-in*).

h. Puisque les enfants méritent une protection particulière, une plus grande importance devrait être accordée à l'article 12 de la Convention, afin de limiter les flux transfrontières de données personnelles aux fins de l'éducation et de veiller à ce que de tels flux s'effectuent dans un cadre établi et adéquat de protection des données.

i. Le traitement de données dans des outils logiciels éducatifs (EdTech) ne devrait pas être autorisé pour diffuser ou cibler des publicités comportementales, pour des technologies publicitaires RTB (enchères d'espace en ligne en temps réel), des publicités intégrées aux applications ou la diffusion auprès des enfants ou des familles de messages de marketing sur la mise à niveau de produits ou d'autres produits proposés par le fournisseur.

j. L'obligation d'assurer une conception conforme aux lois et des contrats licites de traitement des données au moment de la passation de marché devrait continuer de s'appliquer après l'achat, la fusion ou toute autre acquisition d'un opérateur par une autre entité, ou être assortie d'une période suffisamment équitable au cours de laquelle doivent être communiqués les modifications des conditions d'utilisation et le droit de modifier de nouvelles conditions ou de s'y opposer, ou faire de telles modifications un motif de résiliation automatique du contrat et le retrait sur demande de toutes les données relatives aux clients.