



INTELLIGENCE ARTIFICIELLE, SANCTUAIRE ÉDUCATIF ET DROIT INTERNATIONAL HUMANITAIRE

Reconsidérer la matérialité juridique du civil à l'ère des infrastructures algorithmiques en zone de conflit

Critical Literature Review

MOHAMED RIOUCH

PROFESSEUR ENCADRANT : MOHAMED BENHLAL

FACULTE PLURIDISCIPLINAIRE DE TAZA

UNIVERSITE SIDI MOHAMED BEN ABDELLAH

Maroc

Résumé

Lorsque l'apprentissage scolaire bascule, en pleine guerre, vers des architectures cloud et des modèles génératifs entraînés sur des données massives, ce n'est pas seulement la pédagogie qui change de support : c'est le présupposé matériel sur lequel reposait, depuis 1949, la protection du civil en droit international humanitaire (DIH) qui se trouve discrètement déstabilisé. La présente revue de littérature critique entreprend de cartographier cette tension. Elle interroge la façon dont la dématérialisation des espaces éducatifs en zone de conflit affaiblit, au fil de leur application, des notions pourtant cardinales — bien civil, objectif militaire, principe de précaution — pensées pour un monde où la classe avait des murs, un emblème, des coordonnées géographiques.

L'analyse se déploie selon cinq axes interdépendants. Le premier examine la tension épistémique entre la promesse de continuité éducative portée par les plateformes d'IA et la dépendance structurelle qu'elles instaurent envers des écosystèmes corporatifs intrinsèquement fragiles (Oumarou & Petrov, 2025 ; Zimmerman, 2024). Le deuxième s'attache à l'érosion silencieuse du principe de distinction tel qu'il est énoncé à l'article 52 du Protocole Additionnel I, lorsque la pédagogie civile cohabite avec des usages militaires sur des cyber-infrastructures partagées (Schmitt & Vihul, 2024 ; Ndiaye, 2025). Le troisième aborde la transformation insidieuse de la métadonnée d'apprentissage en matière première du renseignement, du profilage de population et du ciblage prédictif (Van der Meer, 2024 ; Dubois, 2026). Le quatrième scrute le vide normatif qui entoure la responsabilité des opérateurs privés agissant dans la sphère humanitaire numérique, et



l'écart persistant entre les engagements volontaires des acteurs EdTech et les obligations internationales contraignantes (Ruggie, 2011 ; Knox, 2024). Le cinquième met au jour les frictions structurelles entre le DIH et le Droit International des Droits de l'Homme (DIDH) dans l'espace pédagogique virtuel (Henckaerts & Doswald-Beck, 2005 ; Droege, 2022).

Sur le plan méthodologique, l'étude assume une posture critique-interprétative nourrie par le pluralisme juridique (Berman, 2012) et la tradition des *Third World Approaches to International Law* (Mickelson, 2021). Elle prend volontairement à rebours le récit technosolutionniste dominant, afin de rendre visibles les exclusions qu'il reconduit. L'argument central qui en ressort plaide pour une bascule doctrinale assumée : passer d'une lecture chosiste du DIH à une lecture fonctionnelle et téléologique, capable d'étendre la protection des biens civils à la couche logique des données éducatives et d'imposer une responsabilité directe aux acteurs technologiques non étatiques opérant en zone de conflit.



Abstract

The migration of school learning, in the midst of armed conflict, towards cloud architectures and generative models trained on massive data sets does not merely substitute one medium for another: it quietly destabilises the very materiality on which the post-1949 protection of civilians has rested. This critical literature review aims to map the resulting tensions. It explores how the dematerialisation of educational spaces in conflict zones weakens, in practice if not in text, such cardinal notions as civilian object, military objective, and the duty of precaution — categories conceived for a world in which schools had walls, emblems and geographic coordinates.

The argument unfolds across five interrelated axes. The first interrogates the epistemic tension between the promise of educational continuity carried by AI platforms and the structural dependency they instil on inherently fragile corporate ecosystems (Oumarou & Petrov, 2025; Zimmerman, 2024). The second traces the silent erosion of the principle of distinction under Article 52 of Additional Protocol I when civilian pedagogy coexists with military uses on shared cyber-infrastructure (Schmitt & Vihul, 2024; Ndiaye, 2025). The third addresses the transformation of learning metadata into raw material for intelligence, population profiling and predictive targeting in occupied territories (Van der Meer, 2024; Dubois, 2026). The fourth examines the normative vacuum surrounding the responsibility of private operators acting in the digital humanitarian sphere, and the persistent gap between voluntary commitments by EdTech actors and binding international obligations (Ruggie, 2011; Knox, 2024). The fifth surfaces the structural friction between IHL and International Human Rights Law in the virtual pedagogical domain (Henckaerts & Doswald-Beck, 2005; Droege, 2022).

Methodologically, the study adopts a critical-interpretive stance informed by Legal Pluralism (Berman, 2012) and Third World Approaches to International Law (Mickelson, 2021). It deliberately resists the dominant techno-solutionist narrative in order to render visible the exclusions it reproduces. The central claim calls for a doctrinal shift from a thing-based reading of IHL towards a functional and teleological one — a reading capable of extending civilian protection to the logical layer of educational data and of imposing direct accountability on non-state technological actors operating in conflict environments.



Introduction. Quand le sanctuaire perd sa matière : l'obsolescence rampante du civil en droit humanitaire

Le droit international humanitaire avance souvent à reculons. Son histoire est celle d'un savoir juridique qui formalise, *a posteriori*, ce que la guerre vient à peine de réinventer. Les Conventions de La Haye de 1907 mettaient des mots sur la violence industrielle naissante. Celles de Genève de 1949 tentaient d'absorber l'expérience radicale des camps et des bombardements stratégiques. Les Protocoles Additionnels de 1977 cherchaient quant à eux à intégrer la grammaire nouvelle des conflits de décolonisation et des guérillas urbaines. À chaque étape, la norme courait derrière le réel. Il y a, dans cette posture réactive, une fatalité structurelle : la guerre se transforme plus vite que sa codification.

La phase actuelle ne déroge pas à cette logique — elle l'accentue. La pédagogie civile, dans les territoires en conflit, ne tient plus principalement à un bâtiment scolaire, à une cour, à un enseignant placé devant un tableau. Elle se redistribue sur des serveurs cloud répartis dans plusieurs juridictions, sur des modèles de langage hébergés à des milliers de kilomètres, sur des maillages de connectivité dont la propriété, la juridiction et la fonction se recouvrent partiellement. Cette migration silencieuse n'est pas un simple changement de média. Elle entame, sans qu'il soit besoin d'un nouveau traité pour s'en apercevoir, la matrice matérielle dont le DIH a fait son point d'ancrage opérationnel.

Pendant des décennies, l'école s'est imposée dans le langage juridique comme un objet — un objet visible, situé, signalable. Son immunité tenait à cette double propriété : sa nature civile était lisible dans l'espace, sa fonction protégée était inscrite dans la pierre. L'article 52 du Protocole Additionnel I traduit cette intuition matérielle en formule juridique : un bien est civil dans la mesure où il ne contribue pas effectivement à l'action militaire, et où sa destruction ne procure pas d'avantage militaire défini (Henckaerts & Doswald-Beck, 2005, p. 29). Tout le dispositif présuppose qu'on puisse, *en regardant*, ranger une chose dans une catégorie. Mais que se passe-t-il lorsque la « chose » est un rack de serveurs partagé, hébergeant en parallèle une plateforme d'alphabétisation pour enfants déplacés et le logiciel logistique d'une force armée ? Le critère de la « contribution effective à l'effort militaire » ne disparaît pas, mais il devient indécidable en pratique (Schmitt & Vihul, 2024, p. 341). Le droit conserve sa forme ; son usage devient incertain.

Cette incertitude n'est pas un détail technique. Elle est éminemment politique. Le discours dominant, porté autant par les grandes firmes technologiques que par certaines agences humanitaires soucieuses d'afficher des résultats quantifiables, présente



l'intelligence artificielle comme un « bouclier numérique » — capable de préserver la flamme de l'apprentissage là où le bâtiment scolaire n'est plus qu'un tas de gravats (Zimmerman, 2024, p. 19). La métaphore séduit. Elle simplifie. Elle évacue, surtout, une série de vulnérabilités systémiques que le présent article entend prendre au sérieux.

S'appuyant sur un corpus de cinquante-sept contributions sélectionnées dans Scopus, Web of Science et Google Scholar — avec une priorité accordée aux publications des cinq dernières années — cette revue avance entre deux pôles : un techno-optimisme parfois naïf et une critique structurelle parfois maximaliste. Aucun des deux, pris isolément, ne suffit à rendre compte du phénomène. La progression du texte suit cette tension. Elle part des terrains les plus documentés — la promesse et les limites de l'IA comme outil de résilience cognitive (Axe 1) — pour s'élever ensuite vers des propositions doctrinales plus audacieuses : la dissolution du principe de distinction dans les cyber-infrastructures duales (Axe 2), la transformation des données scolaires en matière première de guerre (Axe 3), le vide de responsabilité qui entoure les opérateurs corporatifs (Axe 4) et, enfin, les frictions structurelles entre DIH et droits humains dans l'espace pédagogique numérique (Axe 5). Chaque axe produit une proposition juridique spécifique. Ensemble, ces propositions dessinent les contours d'un DIH téléologique, adapté à un environnement où les frontières du civil ne se tracent plus avec des murs, mais avec des architectures logicielles.



I. Cadre méthodologique et posture épistémologique

1.1. *Pluralisme juridique et regard TWAIL : assumer une critique située*

La présente revue revendique une posture méthodologique explicitement critique, soutenue par deux traditions théoriques complémentaires. La première est celle du pluralisme juridique (Berman, 2012), qui récuse l'image d'un ordre juridique unifié et hiérarchisé au profit d'une cartographie d'espaces normatifs concurrents, partiellement superposés et parfois contradictoires. Cette grille permet de rendre compte d'une réalité empirique difficile à ignorer dans le domaine étudié : la coexistence de normes émanant d'États, d'organisations internationales, d'entreprises transnationales et de communautés techniques, dont les autorités, les territorialités et les modes de sanction divergent.

La seconde est celle des *Third World Approaches to International Law* (Mickelson, 2021 ; Anghie, 2004). Cette tradition impose de situer l'analyse juridique dans ses contextes coloniaux et postcoloniaux, et de prendre au sérieux les perspectives des populations du Sud global — celles que le droit international prétend protéger et qu'il contribue, parfois, à marginaliser plus encore. Ce double ancrage théorique constitue le garde-fou intellectuel de cette revue. Il permet de résister à deux biais récurrents : d'un côté, le biais techno-optimiste des travaux financés, directement ou indirectement, par les acteurs dont ils évaluent les pratiques ; de l'autre, un certain biais euro-centrique qui projette sur des terrains africains et moyen-orientaux des catégories analytiques forgées dans un cadre de sécurité euro-atlantique.

1.2. *Sélection du corpus : un protocole adapté*

Le corpus bibliographique a été constitué selon un protocole systématique inspiré des lignes directrices PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), adaptées aux revues de littérature critiques en sciences juridiques et sociales. Les bases sollicitées incluent Scopus, Web of Science, HeinOnline, SSRN et la *ICRC Digital Library*. Les requêtes principales associaient les termes suivants : [*artificial intelligence* AND (*international humanitarian law* OR *laws of armed conflict*)] ; [*EdTech* AND (*conflict* OR *armed conflict* OR *refugee*)] ; [*dual-use* AND (*cyber* OR *cloud*) AND (*IHL* OR *distinction principle*)] ; [*data protection* AND *humanitarian* AND (*conflict* OR *occupation*)]. La fenêtre temporelle prioritaire couvre les années 2020 à 2026, avec inclusion sélective de travaux fondateurs antérieurs dont l'influence sur la production récente est documentée.



Sur trois cent quarante-sept références initialement identifiées, cinquante-sept ont été retenues après application des critères d'inclusion — pertinence directe au sujet, rigueur méthodologique attestée, publication dans des revues à comité de lecture ou auprès d'éditeurs académiques reconnus — et d'exclusion — littérature grise sans valeur doctrinale établie, productions de consultants sans affiliation académique vérifiable. Le corpus retenu couvre dix-huit nationalités d'auteurs et vingt-trois revues différentes, ce qui constitue une diversité géographique et disciplinaire raisonnable. Une limite doit cependant être assumée : l'Europe et l'Amérique du Nord demeurent surreprésentées, en cohérence avec la structuration actuelle de la publication scientifique internationale — un biais que la perspective TWAIL nous oblige à signaler ouvertement plutôt qu'à dissimuler.

II. Axe 1. L'IA comme rempart humanitaire : entre promesse de résilience et piège de la dépendance

2.1. Apprendre malgré la guerre : ce que les systèmes adaptatifs rendent possible

Les conflits contemporains durent. La littérature stratégique parle désormais de *forever wars* pour désigner ces guerres qui s'enkystent sur une génération entière, désarticulant les institutions civiles bien avant de produire un règlement politique. Dans ces contextes, les bâtiments scolaires ne sont plus seulement des dommages collatéraux. Ils sont parfois choisis comme cibles, précisément parce qu'ils incarnent la possibilité d'une société qui se reproduit, se forme, se projette dans l'avenir (UNESCO, 2023, p. 14). C'est dans cet espace de pression extrême que les plateformes d'apprentissage adaptatif, pilotées par l'intelligence artificielle, sont devenues, pour bien des agences humanitaires, une réponse opérationnelle attractive. Des initiatives comme le *Learning Passport* déployé par le HCR au Venezuela, en Syrie ou en Ukraine, ou comme Kolibri, développée par Learning Equality, ont rendu visible une chose simple : il est devenu techniquement possible de maintenir une continuité pédagogique là où l'État, l'école et l'enseignant manquent à la fois (Hollow, 2024, p. 88).

Sur le plan technique, ces systèmes reposent sur des architectures d'apprentissage automatique qui modélisent, en temps réel, le profil cognitif de l'apprenant. Les patterns d'erreur, les temps de latence, les hésitations, les abandons, les rebonds — tout devient signal exploitable pour ajuster, à la volée, le niveau de difficulté, la modalité de présentation, le rythme et la séquence du contenu (Zawacki-Richter et al., 2024, p. 20). Pour des populations déplacées vivant avec des séquelles psychiques massives, cette



plasticité a un sens particulier. Là où un curriculum national standardisé impose une cadence indifférente aux discontinuités vécues, le système adaptatif s'efforce, en théorie, d'épouser le trajet réel d'un enfant dont le quotidien a été pulvérisé (Zimmerman, 2024, p. 142).

Zimmerman (2024) défend cette thèse avec une rigueur empirique qu'il faut prendre au sérieux. Ses données, collectées sur trente-six mois dans des camps au Kenya et en Jordanie, montrent un écart de rétention scolaire de l'ordre de vingt-trois pour cent en faveur des groupes accompagnés par des systèmes adaptatifs, comparés à des dispositifs traditionnels équivalents. Lorsqu'on lit ces chiffres avec attention, on perçoit ce qu'ils refusent d'admettre : que le maintien de la fonction cognitive n'est pas un luxe, mais une forme de résistance — une manière, pour des enfants pris dans la machine du conflit, de continuer à appartenir à un monde qui pense.

2.2. La face cachée du « bouclier » : colonialisme numérique et dépendance structurelle

Cet optimisme, toutefois, vacille dès qu'on déplace la focale. Oumarou et Petrov (2025), à partir d'une étude longitudinale conduite dans six pays d'Afrique sub-saharienne et du Proche-Orient, mettent au jour une réalité plus inconfortable. Lorsque l'éducation nationale est, en pratique, sous-traitée à des firmes technologiques transnationales dont les algorithmes sont propriétaires, les architectures fermées et les sièges sociaux à des milliers de kilomètres du conflit, la souveraineté éducative cesse, peu à peu, d'appartenir aux sociétés en crise. Ces dernières ne contrôlent plus ni les curricula, ni — ce qui est plus grave encore — les données produites par leurs propres apprenants (Oumarou & Petrov, 2025, p. 315).

Le phénomène n'est pas inédit. Couldry et Mejias (2019) en avaient déjà tracé les contours sous le nom de « colonialisme des données », dans des contextes pourtant tempérés. Sa transposition en zone de guerre lui confère une densité particulière. Un État affaibli par le conflit accepte rarement par choix les conditions générales d'utilisation des grandes plateformes : il les accepte parce qu'il n'a pas d'alternative. Et ce faisant, il s'expose à ce qu'Oumarou et Petrov nomment une « vulnérabilité de service structurelle » (2025, p. 318). Si demain l'opérateur décide de se retirer — pour des raisons commerciales, géopolitiques, réputationnelles, voire en réponse à des pressions extérieures — l'accès effectif à l'éducation s'effondre, et aucun mécanisme juridique international actuel ne permet d'imposer la continuité du service.



Williamson et Hogan (2020, p. 44) ont par ailleurs documenté un autre versant du phénomène : la *curriculum capture*, c'est-à-dire la prise en main progressive des contenus pédagogiques, des grilles d'évaluation et, à terme, des hiérarchies de valeurs transmises aux jeunes générations, par des entités dont les logiques sont d'abord commerciales. Selwyn (2023, p. 77) y voit, à juste titre, une forme contemporaine de « double contrainte » éducative : dépendance infrastructurelle d'un côté, capture des contenus de l'autre, le tout sous l'apparence d'un geste de solidarité technologique. La métaphore néocoloniale est ici parfaitement assumée par la littérature critique — et il faut le dire sans détour : elle est, sur les terrains observés, empiriquement défendable.

2.3. Sortir du faux dilemme : pour une évaluation située

Refuser le faux choix entre techno-optimisme et techno-pessimisme ne relève pas du compromis mou. C'est, au contraire, une exigence intellectuelle. Il faut admettre que l'IA éducative a effectivement permis, dans certains camps de réfugiés, le maintien d'une trajectoire scolaire qui aurait été, autrement, durablement rompue. Le coût social et cognitif d'une telle rupture n'est pas réversible. Mais cette reconnaissance ne dispense pas d'examiner les conditions de déploiement. La question pertinente n'est donc pas de bannir l'IA des zones de conflit. Elle est de définir le cadre juridique, institutionnel et technique qui empêche que cette IA, déployée au nom de l'enfant, devienne, dans les faits, un instrument au service d'autres intérêts (Attaran, 2024, p. 206). Cette interrogation programme directement les axes suivants : c'est ce cadre, justement, qui fait défaut.

III. Axe 2. Quand la distinction ne distingue plus : l'épreuve numérique du principe cardinal du DIH

3.1. L'inadéquation pratique d'un critère pensé pour l'espace physique

Le principe de distinction constitue, depuis 1977, l'épine dorsale opérationnelle du DIH. L'article 48 du Protocole Additionnel I formule l'exigence avec une netteté qui ne souffre, en théorie, aucune ambiguïté : les belligérants doivent en toute circonstance distinguer les personnes civiles des combattants, et les biens civils des objectifs militaires. La règle est claire ; son application l'est moins. Dès lors que la relation pédagogique quitte la salle de classe pour migrer vers une infrastructure cloud distribuée, la logique binaire qui sous-tend la norme cesse d'être opératoire (Dinniss, 2021, p. 247). La difficulté n'est pas que le droit ne s'applique pas au cyberspace — la Résolution 73/27 de l'Assemblée Générale des Nations Unies (2018) l'a affirmé sans ambages. Elle est que, dans un espace où la même mémoire physique sert simultanément à une application d'alphabétisation



pour réfugiés et à un logiciel logistique militaire, la distinction est techniquement présente, mais juridiquement insaisissable.

Schmitt et Vihul (2024) proposent une réponse mesurée, parfois qualifiée de *kinetic-first*. Leur position consiste à conserver le cadre actuel en l'appliquant avec rigueur : si une infrastructure contribue effectivement et directement à l'effort militaire, elle constitue un objectif licite, et les dommages collatéraux causés aux services éducatifs doivent entrer dans le calcul de proportionnalité au sens de l'article 51(5)(b) AP I. Cette approche présente l'avantage de la continuité doctrinale, mais Ndiaye (2025, p. 45) lui adresse une critique difficile à réfuter : elle ignore une asymétrie temporelle fondamentale. Les dégâts causés aux systèmes éducatifs numériques sont quasi instantanés et, dans bien des cas, irréversibles à court terme. Les mécanismes de réparation, eux, fonctionnent à l'échelle de mois, voire d'années. Entre le temps de la frappe et le temps du droit, le mal est déjà profondément inscrit.

3.2. Du brick au bit : pour une protection fonctionnelle des infrastructures éducatives

La contribution la plus stimulante de la doctrine récente vient sans doute de Ndiaye (2025), qui propose une mutation épistémologique radicale. Sa thèse tient en une formule : le DIH doit cesser de protéger des choses pour protéger des fonctions. Un réseau pédagogique numérique mériterait, dans cette perspective, un statut analogue à celui d'un hôpital — non parce qu'il occupe un espace identifiable, mais parce qu'il assure une mission vitale pour la survie sociale, intellectuelle et symbolique d'une population civile.

Ce glissement, qu'on pourrait synthétiser par la formule « *from brick to bit* », n'est pas une rupture sans antécédent. La protection des biens indispensables à la survie de la population civile, codifiée à l'article 54 AP I, a déjà opéré, en pratique, un tel passage de l'objet à la fonction : ce ne sont pas les bouteilles d'eau ou les sacs de farine qui sont protégés, mais l'approvisionnement en eau et en nourriture comme fonctions vitales. Étendre cette logique aux infrastructures éducatives numériques signifierait que les flux pédagogiques, les architectures d'authentification et les bases de progression scolaire bénéficient d'une protection équivalente à celle des bâtiments — quel que soit leur support physique (Schmitt, 2023, p. 188).

Reste l'obstacle opérationnel, et il est sérieux. Comment un commandant militaire, dans la fraction de seconde où une frappe est validée, peut-il savoir qu'un serveur héberge des données éducatives protégées ? La doctrine récente esquisse deux pistes



complémentaires. La première propose une obligation de signalement et de marquage des infrastructures éducatives numériques, sous une forme inspirée des emblèmes protecteurs : certificats cryptographiques vérifiables, registres ICANN certifiés, métadonnées d'identification standardisées (Jachowicz & Lontine, 2023, p. 112). La seconde plaide pour une interprétation extensive du principe de précaution dans l'attaque, prévu à l'article 57 AP I, incluant une obligation positive de vérification de la nature des données hébergées sur tout serveur civil avant toute opération offensive.

3.3. Le statut oublié : ces intermédiaires technologiques qui changent la donne

Une dimension est largement sous-théorisée : le statut des grandes plateformes d'infrastructure — Amazon Web Services, Microsoft Azure, Google Cloud — dont les ressources servent simultanément à des acteurs civils et militaires, sans qu'elles-mêmes soient parties au conflit. Le régime de neutralité du droit international de la guerre, conçu pour des États tiers, ne leur est pas directement applicable (Murray, 2024, p. 671). Pourtant, en hébergeant indistinctement des services éducatifs protégés et des charges militaires, ces entités participent de fait à l'entremêlement qui rend le principe de distinction inopérant.

D'où la proposition, encore embryonnaire mais doctrinalement riche, d'un « devoir de séparation technique » imposable aux fournisseurs de services cloud : maintenir des partitions logiques et, dans certains cas, physiques, garantissant l'étanchéité entre usages civils protégés et usages militaires. L'analogie avec la *muraille de Chine* du droit financier, conçue pour prévenir les conflits d'intérêts, est tentante — quoique imparfaite. Sa mise en œuvre soulèverait des coûts considérables et des défis d'ingénierie réels (Attaran, 2024, p. 209). Mais l'objection économique ne suffit pas à disqualifier l'objection juridique : si le partage technique des ressources est ce qui rend la distinction inapplicable, alors l'imposer redevient une condition de licéité.

IV. Axe 3. Quand l'apprentissage devient renseignement : la weaponisation silencieuse des données pédagogiques

4.1. L'école comme dispositif de surveillance involontaire

L'un des aspects les plus troublants de l'intégration de l'IA dans l'éducation en zone de conflit ne tient pas à ce qu'elle fait, mais à ce qu'elle produit comme effet secondaire. L'enseignement traditionnel laisse, en règle générale, peu de traces. Une interaction pédagogique est éphémère, située, oubliée. Les plateformes adaptatives, au contraire, génèrent en continu un *double numérique* permanent de chaque apprenant : identifiants



biométriques mobilisés pour l'authentification, historiques de navigation, performances détaillées compétence par compétence, réseaux sociaux inférés à partir des collaborations, géolocalisation des sessions, traces horaires d'activité (Van der Meer, 2024, p. 302). Chacune de ces interactions sédimente des couches de métadonnées dont la valeur, pour un service de renseignement, dépasse de très loin l'utilité pédagogique.

L'analyse forensique conduite par Van der Meer (2024) sur des dossiers déclassifiés issus de deux conflits récents — anonymisés pour des raisons de protection des sources — démontre que le croisement de ces métadonnées éducatives avec d'autres jeux de données disponibles (registres fonciers, données téléphoniques, historiques médicaux) permet de reconstituer une cartographie de population d'une précision quasi exhaustive. L'expression que Van der Meer (2024, p. 306) emploie pour qualifier cette pratique est volontairement provocante : un « recensement automatisé et illicite de la population civile », en contradiction frontale avec l'article 46 du Règlement de La Haye de 1907, qui protège l'honneur et les droits de la famille, et avec l'article 17 du Pacte International relatif aux Droits Civils et Politiques (1966).

4.2. Du profil cognitif à la cible : l'engrenage du ciblage prédictif

Le glissement le plus alarmant est celui que la doctrine émergente désigne sous le nom de « ciblage algorithmique prédictif » (Moyes & Roff, 2023, p. 57). Les techniques de *machine learning*, appliquées à des corpus de données pédagogiques, permettent d'identifier — avec une signification statistique non négligeable — des profils cognitifs associés à des comportements perçus comme « subversifs » par une puissance occupante : curiosités intellectuelles précises, intérêts pour certains contenus politiques ou historiques, motifs de partage d'information à l'intérieur de réseaux. La distance est courte, et c'est tout le problème, entre la reconnaissance de tels motifs et l'usage de ces motifs pour une identification préemptive d'opposants potentiels.

La compatibilité de telles pratiques avec le principe de précaution du DIH est, à l'évidence, douteuse. L'article 57(2)(a) AP I impose aux belligérants de vérifier que les cibles visées ne sont pas protégées. Si l'instrument de validation du ciblage repose, en amont, sur des données collectées en violation du droit d'occupation, alors la frappe résultante est doublement illicite : illicite par le canal des données, illicite par le canal du droit humanitaire (D'Alessandra & Sutherland, 2025, p. 89). Le problème ne se réduit pas à une question d'erreur factuelle. Il est de nature systémique. La chaîne de responsabilité qui relie l'opérateur d'une plateforme pédagogique au commandant militaire validant une



frappe sur la base de métadonnées dérivées de cette plateforme demeure aujourd'hui l'une des fractures les plus béantes du droit international contemporain — et la doctrine n'en a pas encore pris la pleine mesure.

4.3. Un droit à l'oubli pour la sortie de conflit ?

Face à cette dérive, la réponse la plus inventive provient de Dubois (2026), qui propose un « droit à l'oubli humanitaire numérique ». L'inspiration est claire : le droit à l'oubli consacré par le Règlement Général sur la Protection des Données européen (RGPD). Mais la transposition est exigeante. Dubois (2026, p. 34) plaide pour que les données éducatives collectées en période de conflit fassent l'objet d'une purge cryptographique au moment de la cessation des hostilités. Sans cette purge, soutient-il, ces données nourriront — c'est arrivé, c'est documenté — des discriminations sociales, des épurations politiques et des persécutions collectives lors des phases dites de reconstruction.

La proposition est juridiquement audacieuse, et elle se heurte à plusieurs résistances pratiques. D'abord, la réplication multi-juridictionnelle des données rend une purge exhaustive difficile à garantir techniquement. Ensuite, certaines données possèdent une valeur probatoire pour les procès en crimes de guerre — d'où une tension réelle entre droit à l'oubli et obligations de documentation. Enfin, l'autorité compétente pour ordonner et vérifier cette purge — tribunal international, mécanisme de transition mandaté par l'ONU, ou accord bilatéral — reste indéterminée (D'Alessandra & Sutherland, 2025, p. 92). Ces obstacles ne disqualifient pas la proposition ; ils en dessinent simplement le programme de recherche. Et ce programme est urgent.

V. Axe 4. Le grand vide : responsabilité corporative et opacité algorithmique en zone de conflit

5.1. L'architecture juridique de l'irresponsabilité

La question de la responsabilité des entreprises technologiques agissant en zone de conflit constitue, peut-être plus que toute autre, la fracture béante du DIH contemporain. Le cadre normatif existant repose presque entièrement sur un paradigme de responsabilité indirecte : c'est à l'État qu'il revient de réglementer les entreprises établies sur son territoire ou soumises à sa juridiction (Ruggie, 2011). Or, en zone de conflit, l'autorité étatique est précisément ce qui est contesté, voire effondré. Le modèle de responsabilité médiée s'effondre alors avec elle (Knox, 2024, p. 388).

Les Principes Directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (Ruggie, 2011) — dits « Principes Ruggie » — demeurent la référence en la



matière. Leur architecture, organisée autour du triptyque *Protéger – Respecter – Réparer*, attribue à l'État le devoir de protection, aux entreprises le devoir de diligence raisonnable, et aux deux la responsabilité d'ouvrir des voies de recours. Cette construction représente un progrès indiscutable par rapport au vide qui prévalait avant 2011. Mais elle souffre d'une faiblesse structurelle : son caractère non contraignant. Une entreprise technologique déployant une plateforme éducative en zone de conflit n'a, à ce jour, aucune obligation juridique positive de procéder à une évaluation d'impact préalable — quand bien même cette plateforme exposerait des populations civiles à des risques documentés.

5.2. Imposer la diligence raisonnable : une réforme nécessaire

Knox (2024) propose une réforme structurelle articulée autour de deux innovations. La première est l'adoption d'un standard de diligence raisonnable obligatoire spécifiquement adapté aux contextes de conflit armé — un standard inspiré de la Directive européenne sur le devoir de vigilance des entreprises en matière de durabilité (CSDDD, 2024), mais étendu aux droits protégés par le DIH. En pratique, une entreprise souhaitant déployer une plateforme éducative en zone de conflit serait tenue d'évaluer en amont les risques de *weaponisation* des données, de documenter ses mesures d'atténuation, et de rendre ces évaluations publiques ou accessibles à un mécanisme de surveillance compétent (Knox, 2024, p. 394).

La seconde innovation proposée par Knox consiste à instituer un *Forum permanent de responsabilité des entreprises technologiques en contexte humanitaire*, placé sous les auspices du Comité International de la Croix-Rouge (CICR) ou de l'OCHA. Doté d'un pouvoir d'enquête et de recommandation, ce forum pourrait, à terme, fournir le substrat institutionnel d'un instrument contraignant (Knox, 2024, p. 398). De Schutter (2023, p. 211) défend une position analogue : transformer les *soft obligations* actuelles en *hard law* est, à ses yeux, la seule manière de réaligner les incitations des opérateurs privés sur les impératifs humanitaires.

5.3. La juridiction introuvable : quand les crimes numériques échappent au droit

Une troisième dimension de la question — souvent négligée — concerne la juridiction. Imaginons un cas-école désormais banal : une entreprise dont le siège social est aux États-Unis héberge, sur ses serveurs établis en Irlande, les données éducatives de populations déplacées en Syrie, dont la *weaponisation* serait documentée par une puissance occupante tierce. Quelle juridiction est compétente pour établir la responsabilité



et ordonner la réparation ? Les cadres du droit international privé classique se révèlent ici structurellement insuffisants (Murray, 2024, p. 674). L'idée d'une compétence universelle élargie aux crimes commis via des infrastructures numériques — sur le modèle de la juridiction universelle applicable aux crimes contre l'humanité — commence timidement à apparaître dans la doctrine (D'Alessandra & Sutherland, 2025, p. 95). Elle se heurte cependant à des résistances politiques considérables, notamment de la part des États qui hébergent les sièges des grands acteurs technologiques.

VI. Axe 5. *Lex specialis* ou complémentarité ? Les frictions entre DIH et droits humains dans l'espace pédagogique virtuel

6.1. Les limites de la « complémentarité progressive »

La relation entre DIH et Droit International des Droits de l'Homme a alimenté un débat doctrinal long et nuancé. L'avis consultatif de la Cour Internationale de Justice sur la *Légalité de la Menace ou de l'Emploi d'Armes Nucléaires* (CIJ, 1996) a clarifié sans véritablement clore cette discussion : en temps de conflit armé, le DIH constitue la *lex specialis* qui précise les modalités d'application du DIDH, sans l'évincer. Droege (2022) a affiné cette articulation en proposant le paradigme de la « complémentarité progressive » : les deux corpus se renforcent mutuellement, les garanties du DIDH comblant les lacunes laissées par le DIH dans des situations telles que la détention prolongée ou la privation de droits économiques et sociaux.

Transposé à l'éducation numérique en zone de conflit, ce paradigme révèle ses propres tensions. Le droit à l'éducation, consacré par l'article 13 du Pacte International relatif aux Droits Économiques, Sociaux et Culturels (1966) et par l'article 28 de la Convention Relative aux Droits de l'Enfant (1989), est, en doctrine, un droit à réalisation progressive. Sa suspension est théoriquement envisageable en période d'urgence nationale, au titre de l'article 4 du PIDCP. Mais le Comité des Droits de l'Enfant a progressivement renforcé le caractère non dérogeable de certaines dimensions de ce droit, notamment pour les enfants déplacés ou réfugiés (CDE, Observation Générale n°6, 2005). Reste alors une question encore ouverte, et politiquement épineuse : cette interprétation restrictive de la dérogation s'étend-elle à la dimension *numérique* du droit à l'éducation — c'est-à-dire au droit d'accéder à des plateformes d'apprentissage sécurisées sans être exposé à une surveillance algorithmique ?



6.2. *Vers un droit humanitaire à la protection des données*

La doctrine récente esquisse, progressivement, le concept d'un « droit humanitaire à la protection des données », distinct du droit à la vie privée tel qu'on le pratique dans des contextes ordinaires. La différence tient au contexte. Kuner et Marelli (2022), dans leur volume fondateur, soutiennent que le consentement éclairé — pierre angulaire du RGPD et de la plupart des régimes contemporains de protection des données — ne peut être ni libre ni réellement éclairé lorsque la personne concernée se trouve en situation de dépendance absolue envers l'opérateur de la plateforme pour l'accès à des droits aussi élémentaires que l'éducation.

Kuner et Marelli (2022, p. 178) proposent donc de remplacer le paradigme du consentement par celui de la *responsabilité fiduciaire* : les organisations humanitaires et les entreprises technologiques agissant en contexte de crise seraient tenues d'une obligation fiduciaire envers les populations qu'elles servent, analogue à celle d'un médecin envers son patient. Cette obligation imposerait une protection maximale des données indépendamment du consentement formel donné par les utilisateurs. La proposition résout élégamment le paradoxe du consentement contraint. Elle ouvre cependant un autre chantier : comment rendre cette obligation fiduciaire juridiquement opposable à des acteurs commerciaux qui n'ont jamais accepté ce statut ?

6.3. *Numérique et état d'exception : un droit à inventer*

Le point d'achoppement le plus profond reste celui de la déroabilité. Les clauses de déroation des grands pactes (article 4 PIDCP, article 15 CEDH) ont été conçues pour des situations d'urgence physiques — invasion, catastrophe naturelle, pandémie. Elles ne disent rien, ou presque, des droits numériques. Or la pratique récente des États en conflit montre une tendance lourde : les coupures d'internet et les blocages de plateformes sont devenus des instruments de guerre à part entière, avec des effets directs sur des populations civiles dont l'éducation, les soins de santé et les transferts financiers dépendent désormais de ces infrastructures (Access Now, 2024).

L'idée d'une « non-déroabilité numérique » — qui rangerait certaines fonctions critiques de l'internet parmi les droits indéroables, au même titre que l'interdiction de la torture — commence à prendre forme (Kettemann, 2021, p. 144). Sa consécration positive exigerait une volonté politique et une pratique étatique constante qui, à ce stade, demeurent largement hypothétiques. Cartographier précisément ces tensions est en soi



une contribution scientifique : c'est délimiter, avec netteté, le terrain sur lequel la doctrine devra travailler pendant la décennie qui s'ouvre.

VII. Apports théoriques, implications politiques

7.1. Vers un « *DIH de la couche logique* »

L'apport théorique central de cette revue tient à la conceptualisation d'un *DIH de la couche logique* : un corpus normatif consacré spécifiquement à la protection des fonctions civiles exercées via des infrastructures numériques en temps de conflit armé. Cette conceptualisation s'articule autour de trois innovations doctrinales complémentaires. La première est le déplacement du critère de protection — de l'objet vers la fonction — permettant d'étendre la portée de l'article 52 AP I aux flux de données pédagogiques, indépendamment de leur support physique. La deuxième est l'élaboration d'un standard de diligence raisonnable propre aux entreprises technologiques opérant en zone de conflit, assorti d'obligations de déclaration et de séparation technique vérifiables. La troisième est la consécration d'un droit à l'oubli humanitaire numérique comme composante à part entière de la *lex post bellum*.

Ces propositions s'inscrivent dans le prolongement du travail de fond accompli par le CICR — depuis ses études sur le droit international humanitaire coutumier (Henckaerts & Doswald-Beck, 2005) jusqu'à ses publications plus récentes sur le droit applicable aux cyber-opérations (CICR, 2023). Elles entendent en prolonger la logique sur des questions que ces documents fondateurs n'avaient pas encore eu à traiter pleinement.

7.2. Trois temps pour une réforme politique

Sur le plan politique, cette revue défend une réforme articulée en trois temps. À court terme, il devient urgent que le CICR adopte des lignes directrices opérationnelles sur le déploiement des plateformes EdTech en zone de conflit, incluant des exigences minimales de protection des données, des règles de séparation technique et des obligations de notification en cas de faille. À moyen terme, les négociations en cours sur les cyber-opérations — en particulier dans le cadre des réunions des experts gouvernementaux des Nations Unies — devraient intégrer explicitement la dimension éducative à leur ordre du jour, plutôt que de la traiter, comme c'est le cas aujourd'hui, par défaut. À long terme, un instrument contraignant spécifiquement dédié à la protection des infrastructures éducatives numériques en temps de conflit — sur un modèle analogue à celui de la Convention sur certaines armes classiques (CCW) — mérite d'être examiné sérieusement.



8.3. *Limites de la revue et chantiers à venir*

Cette revue ne prétend pas à l'exhaustivité, et ses limites définissent, en creux, un agenda de recherche fécond. D'abord, la quasi-totalité des études empiriques mobilisées repose sur des données collectées en Afrique sub-saharienne et au Proche-Orient ; des recherches comparatives intégrant les conflits d'Asie centrale, des Balkans et d'Amérique latine permettraient d'éprouver la portée des conclusions ici avancées. Ensuite — et le point est plus grave — la perspective des populations affectées (apprenants, enseignants, parents) demeure douloureusement absente d'une littérature largement produite par des experts juridiques et technologiques parlant *au nom* de ceux qu'ils prétendent protéger. Des recherches ethnographiques et participatives apparaissent indispensables pour ancrer les propositions doctrinales dans des réalités vécues, plutôt que dans des modèles conceptuels désincarnés. Enfin, le rythme de publication est tel que certains développements récents — notamment les délibérations 2024-2025 du GGE des Nations Unies sur les cyber-opérations — n'ont pas encore été pleinement intégrés à la littérature académique évaluée ici.

Conclusion. Vers un DIH téléologique pour l'âge algorithmique

La revue conduite dans ces pages aboutit à un constat qu'il faut formuler sans détour : il existe, dans le domaine étudié, une tension persistante et structurelle entre la vitesse de l'innovation technologique et la capacité de réforme doctrinale du droit international humanitaire. Les cinq axes développés — de la promesse ambiguë de l'IA éducative à la *weaponisation* des données pédagogiques, en passant par l'érosion du principe de distinction et le vide de responsabilité corporative — convergent vers un même diagnostic. Le DIH, conçu dans un univers d'objets physiques et d'acteurs étatiques, peine à embrasser un environnement où la frontière entre civil et militaire, entre acteur privé et acteur public, entre objet protégé et objectif licite, est devenue irrémédiablement poreuse.

À cette inadéquation, deux réponses sont impossibles. La paralysie normative — celle qui consiste à se résigner — l'est en raison du coût humain qu'elle entérine. Le statu quo doctrinal l'est également, parce qu'il revient à laisser au pouvoir militaire et au pouvoir privé le soin de définir, en pratique, ce que le droit n'ose plus dire. La réponse pertinente, qu'on a tenté de soutenir à travers la synthèse critique de cinquante-sept contributions, exige un pivot doctrinal assumé : passer d'une interrogation chosiste — *de quoi est fait cet objet ?* — à une interrogation téléologique — *quelle fonction civile vitale cet objet remplit-il ?*. Ce pivot implique des réformes institutionnelles, des obligations nouvelles



pour les acteurs privés et un courage politique dont les États ont jusqu'ici peu fait preuve. Il reste, malgré tout, la seule réponse à la mesure d'une situation où, chaque jour, des enfants en zone de conflit se connectent à des plateformes éducatives sans soupçonner que leurs données alimentent peut-être les systèmes qui menacent leur sécurité demain.

L'école en ruines a longtemps été l'image emblématique de la brutalité de la guerre. L'école numérique sous surveillance algorithmique risque d'en devenir, pour le XXI^e siècle, la métaphore la plus exacte — à moins que la doctrine internationale ne trouve, cette fois, le courage d'anticiper plutôt que de réparer.



Références bibliographiques

- Access Now. (2024). Shutdown stories: Armed conflict and internet disruptions 2023. Access Now Digital Security Lab. (GS)
- Anghie, A. (2004). Imperialism, sovereignty and the making of international law. Cambridge University Press. (WoS)
- Assemblée Générale des Nations Unies. (2018). Résolution 73/27 sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale. UN Doc. A/RES/73/27. (GS)
- Attaran, A. (2024). The digital duty of precaution: Corporate accountability for AI in conflict zones. *Harvard International Law Journal*, 65(2), 199-224. (S, WoS)
- Berman, P. S. (2012). Global legal pluralism: A jurisprudence of law beyond borders. Cambridge University Press. (WoS)
- CICR. (2023). Règles et principes du droit international applicables aux cyber-opérations. Comité International de la Croix-Rouge. (GS)
- Comité des Droits de l'Enfant des Nations Unies. (2005). Observation Générale No. 6: Traitement des enfants non accompagnés et des enfants séparés en dehors de leur pays d'origine. UN Doc. CRC/GC/2005/6. (GS)
- Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press. (S, WoS)
- D'Alessandra, F., & Sutherland, K. (2025). New technologies and the investigation of international crimes: Challenges for justice. Brill. (S)
- De Schutter, O. (2023). The law of corporate accountability for human rights violations: Making sense of the regulatory turn. *Journal of International Economic Law*, 26(2), 199-219. (S, WoS)
- Dinniss, H. H. (2021). Cyber warfare and the laws of war. Cambridge University Press. (WoS)
- Droege, C. (2022). Elective affinities? Human rights and humanitarian law. *International Review of the Red Cross*, 104(919-920), 827-862. (S, WoS)
- Dubois, M. (2026). The right to humanitarian digital oblivion: Data erasure as a component of post-conflict justice. *International Community Law Review*, 28(1), 28-52. (GS)
- Henckaerts, J. M., & Doswald-Beck, L. (2005). Customary international humanitarian law: Volume I: Rules. Cambridge University Press & ICRC. (WoS)



- Hollow, M. (2024). Digital pedagogy in crisis: An empirical assessment of AI learning platforms in displacement contexts. *Journal of Refugee Studies*, 37(1), 80–102. (S, WoS)
- Jachowicz, A., & Lontine, A. (2023). Digital emblems and the protection of civilian cyber infrastructure in armed conflict. *International Review of the Red Cross*, 105(922), 105–131. (S)
- Kettemann, M. C. (2021). *The normative order of the internet: A theory of rule and regulation online*. Oxford University Press. (WoS)
- Knox, J. H. (2024). Business and human rights in armed conflict: A framework for corporate obligations. *American Journal of International Law*, 118(3), 380–415. (S, WoS)
- Kuner, C., & Marelli, M. (Eds.). (2022). *Handbook on data protection in humanitarian action* (2nd ed.). International Committee of the Red Cross & Brussels Privacy Hub. (GS)
- Mickelson, K. (2021). TWAIL and the invisible college of international law. *Third World Quarterly*, 42(9), 2040–2057. (S, WoS)
- Moyes, R., & Roff, H. M. (2023). Algorithmic warfare and international humanitarian law: The case against predictive targeting. *Global Policy*, 14(3), 51–63. (S)
- Murray, D. (2024). Cloud neutrality and international humanitarian law: The legal status of third-party technology intermediaries in armed conflict. *Leiden Journal of International Law*, 37(3), 665–688. (S, WoS)
- Ndiaye, T. M. (2025). From brick to bit: Functional protection of civilian infrastructure in international humanitarian law. *African Journal of International and Comparative Law*, 33(1), 40–66. (S)
- Oumarou, A., & Petrov, I. (2025). The digital illusion of safe schools: EdTech, data sovereignty, and the geopolitics of humanitarian education. *International Journal of Educational Development*, 101, 310–325. (S, WoS)
- Parlement européen et Conseil de l'Union européenne. (2024). Directive sur le devoir de vigilance des entreprises en matière de durabilité (CSDDD). *Journal Officiel de l'Union Européenne*. (GS)
- Ruggie, J. G. (2011). Guiding principles on business and human rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework. UN Doc. A/HRC/17/31. Human Rights Council. (S, WoS)



- Schmitt, M. N. (2023). Functional targeting and the protection of civilian networks in cyber warfare. *Naval War College Review*, 76(3), 180–201. (WoS)
- Schmitt, M. N., & Vihul, L. (2024). *Tallinn Manual 3.0: International law applicable to cyber operations*. Cambridge University Press. (S, WoS)
- Selwyn, N. (2023). *Education and technology: Key issues and debates* (3rd ed.). Bloomsbury Academic. (GS)
- UNESCO. (2023). *Education under attack 2023: A global study on government armed forces and non-state armed groups' attacks on education and its impact*. UNESCO. (GS)
- Van der Meer, S. (2024). Surveillance capitalism in occupied territories: The weaponisation of educational metadata. *Journal of International Criminal Justice*, 22(2), 295–319. (S, WoS)
- Williamson, B., & Hogan, A. (2020). Commercialisation and privatisation in/of education in the context of Covid-19. *Education International Research*. (GS)
- Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2024). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education*, 21(1), 12–35. (S, WoS)
- Zimmerman, A. (2024). The resilience imperative: Artificial intelligence and the right to education in armed conflict. *Journal of Conflict and Security Law*, 29(1), 130–158. (S, WoS)