

De la dépendance technologique des États à la responsabilité des entreprises numériques dans les conflits armés : repenser le cadre du droit international humanitaire

KENY M'VOULABOLO

Kenymvoulabolo7@gmail.com

Fès, Maroc

Introduction

La transformation numérique des conflits armés redéfinit les rapports entre puissance publique et acteurs privés. L'intégration de l'intelligence artificielle, du cloud computing, des réseaux satellitaires ou encore des plateformes d'analyse de données dans les capacités militaires a progressivement fait des entreprises technologiques des partenaires indispensables des États [1,2]. Cette évolution dépasse la simple fourniture d'équipements : les infrastructures numériques constituent désormais des éléments essentiels du renseignement, des communications, de la planification opérationnelle et de l'aide à la décision militaire. Cette dépendance technologique s'inscrit dans un contexte de compétition stratégique où les États s'appuient de plus en plus sur les capacités développées par des entreprises privées. Les investissements massifs dans l'intelligence artificielle militaire, les infrastructures cloud souveraines ou les systèmes satellitaires illustrent cette évolution [3,4]. Toutefois, cette intégration croissante soulève une question encore peu explorée par la doctrine : dans quelle mesure la dépendance technologique des États transforme-t-elle la responsabilité des entreprises numériques au regard du droit international humanitaire ? Cet article adopte une démarche qualitative fondée sur une analyse doctrinale et documentaire, complétée par l'étude de cas emblématiques tels que Project Maven, Palantir Technologies et Starlink. L'objectif est d'évaluer les limites du cadre juridique actuel et de proposer une lecture renouvelée de la responsabilité des entreprises numériques dans les conflits armés.

I. De la dépendance technologique à une nouvelle zone grise juridique

Les progrès récents de l'intelligence artificielle, des technologies de traitement des données et du cloud computing ont profondément transformé les capacités militaires contemporaines. Cette évolution crée une dépendance qui ne concerne plus seulement les équipements, mais également les infrastructures numériques sur lesquelles reposent le renseignement, les communications et la conduite des opérations [5-6]. Le Project Maven, lancé par le Département de la Défense des États-Unis, illustre cette évolution. En intégrant les technologies développées par Google afin d'automatiser l'analyse d'images issues des drones militaires, ce programme a démontré que certaines capacités essentielles du renseignement dépendaient désormais d'algorithmes conçus par une entreprise privée [7]. De même, les plateformes développées par Palantir Technologies permettent aujourd'hui la fusion et l'analyse en temps réel de données opérationnelles, renforçant les capacités décisionnelles de plusieurs forces armées [8]. Cette tendance est également visible dans les infrastructures de communication. Depuis le début du conflit en Ukraine, le réseau Starlink est devenu un élément essentiel des communications militaires ukrainiennes, illustrant la place prise par les entreprises privées dans le fonctionnement des capacités stratégiques des États [9]. Les entreprises

numériques ne fournissent plus seulement des technologies ; elles assurent désormais le fonctionnement quotidien de services indispensables aux opérations militaires [10]. Si les entreprises numériques ne participent pas directement aux hostilités au sens classique du droit international humanitaire, leurs infrastructures conditionnent désormais l'efficacité opérationnelle des forces armées. Les catégories juridiques traditionnelles, éappaissent ainsi de plus en plus inadaptées pour appréhender cette nouvelle réalité [11].

II. Les limites du droit international humanitaire face aux entreprises numériques

L'implication croissante des entreprises numériques dans les capacités militaires soulève une difficulté majeure : le droit international humanitaire (DIH) ne fournit pas de cadre pleinement adapté pour qualifier leur rôle. Conçu à une époque où les opérations militaires relevaient essentiellement des États, il distingue les parties au conflit, les combattants, les civils et les personnes participant directement aux hostilités [12,13]. Cette architecture demeure pertinente, mais elle peine à appréhender les acteurs privés qui développent, contrôlent ou exploitent des infrastructures numériques indispensables aux opérations militaires. Selon le Comité international de la Croix-Rouge, la participation directe aux hostilités suppose un lien direct entre l'acte accompli et le préjudice militaire causé à l'adversaire [14]. Or, les entreprises numériques interviennent généralement en amont de l'emploi de la force : elles conçoivent les algorithmes, hébergent les données, assurent les communications ou développent les plateformes d'analyse utilisées par les forces armées. Leur contribution est donc principalement fonctionnelle plutôt qu'opérationnelle. Les exemples de Project Maven, de Palantir ou de Starlink illustrent cette ambiguïté. Pourtant, leur interruption ou leur retrait serait susceptible d'affecter significativement les capacités militaires d'un État. Cette influence stratégique dépasse largement celle d'un simple fournisseur de biens ou de services. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme consacrent certes un devoir de diligence raisonnable (human rights due diligence) imposant aux entreprises de prévenir et d'atténuer les risques d'atteintes aux droits fondamentaux [15]. Toutefois, ce cadre demeure principalement conçu pour les situations de paix et n'apporte qu'une réponse partielle aux enjeux spécifiques des conflits armés [16]. De même, les débats relatifs à la responsabilité internationale des entreprises restent largement centrés sur les violations des droits de l'homme, sans intégrer pleinement leur rôle croissant dans la conduite des opérations militaires [17,18]. Il en résulte une zone grise juridique : les entreprises numériques ne peuvent être assimilées ni à de simples prestataires commerciaux, ni à des parties au conflit. Pourtant, leur contrôle sur des infrastructures devenues essentielles aux capacités militaires leur confère une influence stratégique inédite. Cette évolution invite ainsi à dépasser les catégories classiques du droit international humanitaire afin de mieux appréhender les nouvelles formes d'interdépendance entre États et acteurs privés.

III. Vers une responsabilité fonctionnelle des entreprises numériques

Face à cette évolution, cet article propose une approche fondée sur la notion de responsabilité fonctionnelle. Celle-ci ne vise pas à reconnaître aux entreprises numériques le statut de belligérant, mais à apprécier leur responsabilité à partir des fonctions qu'elles exercent effectivement dans les conflits armés. Plus une entreprise fournit une capacité indispensable aux opérations militaires, conserve un contrôle sur ses infrastructures et dispose de moyens pour prévenir un usage contraire au droit international humanitaire, plus son implication juridique mérite d'être examinée [19]. Cette approche repose sur quatre critères complémentaires : (i) le degré de dépendance de l'État à l'égard de la technologie fournie ; (ii) le niveau d'intégration de cette technologie aux opérations militaires ; (iii) le contrôle effectif

exercé par l'entreprise sur ses infrastructures numériques ; et (iv) sa capacité à prévenir ou limiter les violations du droit international humanitaire [20]. Pris isolément, aucun de ces critères ne suffit à engager une responsabilité. Leur combinaison permet toutefois d'évaluer le degré d'implication fonctionnelle des entreprises dans la conduite des hostilités, sans remettre en cause les principes fondamentaux du DIH.

Conclusion

La numérisation des conflits armés transforme profondément les relations entre les États et les entreprises technologiques. En devenant des fournisseurs d'infrastructures essentielles au renseignement, aux communications, au traitement des données et à la conduite des opérations militaires, les entreprises numériques occupent désormais une position stratégique qui dépasse le rôle traditionnel de simple prestataire de services. Cette évolution met en évidence les limites du droit international humanitaire, dont les catégories classiques peinent à appréhender l'implication croissante de ces acteurs privés dans les capacités militaires des États. À partir de ce constat, cet article a montré que la dépendance technologique des États conduit à repenser la responsabilité des entreprises numériques au-delà des approches classiques fondées sur la participation directe aux hostilités ou sur les seuls mécanismes de diligence raisonnable. La notion de responsabilité fonctionnelle proposée constitue une grille d'analyse permettant d'évaluer leur implication à partir du degré de dépendance des États, de leur intégration aux opérations militaires, du contrôle exercé sur leurs infrastructures et de leur capacité à prévenir les violations du droit international humanitaire. Si les exemples mobilisés concernent principalement les États-Unis et le conflit en Ukraine, ces enjeux concernent également les États africains, dont les capacités numériques reposent de plus en plus sur des infrastructures développées par des entreprises étrangères. Cette évolution soulève des questions essentielles relatives à la souveraineté technologique, à l'autonomie stratégique et à la responsabilité des acteurs privés dans les conflits contemporains. Dans cette perspective, l'adaptation du droit international humanitaire apparaît comme un enjeu majeur afin de mieux encadrer les nouvelles interactions entre États, entreprises technologiques et infrastructures numériques dans les conflits armés du XXI^e siècle.

Références

- [1] Bousquet A. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York : Columbia University Press; 2009.
- [2] Thibout C. GAFAM et BATX contre les États ? *Politique étrangère*. 2020;85(1):77-89.
- [3] Defense Innovation Board. *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*. Washington DC: U.S. Department of Defense; 2019.
- [4] Kello L. *The Virtual Weapon and International Order*. New Haven: Yale University Press; 2017.
- [5] European Commission. *2030 Digital Compass: the European way for the Digital Decade*. Brussels; 2021.

- [6] Asterès. *La dépendance technologique aux softwares & cloud services américains : une estimation des conséquences économiques en Europe*. Paris; 2025.
- [7] U.S. Department of Defense. *Project Maven Fact Sheet*. Washington, DC; 2017.
- [8] Palantir Technologies. *Defense Solutions*. Denver; 2024.
- [9] European Union Institute for Security Studies (EUISS). *Starlink and the Future of Military Satellite Communications*. Paris; 2023.
- [10] Business & Human Rights Resource Centre. *Amazon, Google & Microsoft fuel Israeli military operations in Gaza, investigation reveals*. London; 2024.
- [11] United Nations. *Guiding Principles on Business and Human Rights*. New York and Geneva: United Nations; 2011.
- [12] Convention (IV) de Genève relative à la protection des personnes civiles en temps de guerre, 12 août 1949.
- [13] Protocoles additionnels aux Conventions de Genève du 12 août 1949, notamment le Protocole additionnel I (1977).
- [14] Clapham A. *Human Rights Obligations of Non-State Actors*. Oxford: Oxford University Press; 2006.
- [15] United Nations. *Guiding Principles on Business and Human Rights*. New York and Geneva: United Nations; 2011.
- [16] Henckaerts JM, Doswald-Beck L. *Customary International Humanitarian Law. Volume I: Rules*. Cambridge: Cambridge University Press; 2005.
- [17] Melzer N. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. Geneva: International Committee of the Red Cross; 2009.
- [18] European Parliament Research Service. *Ukraine, Starlink and the Strategic Role of Commercial Satellite Networks*. Brussels; 2023.
- [19] Schmitt MN, Vihul L, éditeurs. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [Internet]. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press; 2017.
- [20] European Union. Directive (EU) 2024/1760 on Corporate Sustainability Due Diligence (CSDDD). Official Journal of the European Union; 2024.