



Lâ??IA au service de la guerre : comment les gÃ©ants de la technologie facilitent les crimes et lâ??occupation dâ??IsraÃ«l

## Description

Lâ??agence MÃ©dia Palestine propose une traduction de cette analyse rÃ©alisÃ©e pour Al-Shabaka de Marwa Fatafta, Ã©crivaine, chercheuse et analyste politique palestinienne basÃ©e Ã Berlin.

Par Marwa Fatafta, le 26 octobre 2025



Les géants États-Uniens de la technologie se présentent comme des innovateurs éthiques qui façonnent un monde meilleur grâce à l'intelligence artificielle (IA) et au cloud computing. Pourtant, à Gaza, ces discours se sont effondrés. Les systèmes d'IA, les infrastructures cloud et les outils de surveillance fournis par des entreprises technologiques telles que Google, Amazon, Microsoft et Palantir sont désormais indissociables de la campagne génocidaire menée par Israël contre les Palestiniens.

## Introduction

Les géants États-Uniens de la technologie se présentent comme les architectes d'un monde meilleur, alimentés par l'intelligence artificielle (IA), le cloud computing et les solutions basées sur les données. Sous des slogans tels que « AI for Good » (l'IA au service du bien), ils s'engagent à agir en tant que gardiens éthiques des technologies qui remodelent nos sociétés. Pourtant, à Gaza, ces discours se sont effondrés, tout comme les normes internationales et ce qui reste du soi-disant État de droit.

La guerre géocidaire menée par le régime israélien à Gaza a attiré l'attention sur le rôle des grandes entreprises technologiques dans la facilitation des opérations militaires et le maintien de l'occupation. Derrière la destruction israélienne se cachent des serveurs, des réseaux neuronaux et des systèmes logiciels construits et déployés par certaines des entreprises les plus puissantes au monde. La militarisation croissante des technologies et des infrastructures numériques est particulièrement visible dans le déploiement par Israël de systèmes basés sur l'IA et l'analyse de données à Gaza, a remodelé les débats sur la responsabilité et mis en évidence des lacunes critiques dans les cadres de gouvernance existants. Cette note d'orientation examine comment la frontière de la responsabilité des entreprises technologiques s'étend désormais à la complicité potentielle dans les crimes de guerre, les crimes contre l'humanité et le génocide, soulignant le besoin urgent de nouvelles approches pour réguler la militarisation de l'IA.

## Un génocide alimentaire par l'IA

Le régime israélien a déployé pour la première fois des systèmes d'IA pour générer et hiérarchiser des cibles ciblées lors du bombardement de Gaza qui a duré 11 jours en mai 2021, une attaque violente et illégale que l'armée israélienne a ensuite qualifiée de première « guerre de l'IA ». Depuis lors, les forces d'occupation ont considérablement accru leur recours aux outils d'IA, utilisant le cloud computing et l'apprentissage automatique pour stocker et traiter de vastes volumes de données de surveillance ( de l'imagerie satellite à l'interception de communications) afin d'automatiser l'identification et le classement des cibles à attaquer.

Au cœur de la guerre IA menée par Israël se trouve le projet Nimbus, un contrat de 1,2 milliard de dollars dans le cadre duquel Google et Amazon ont fourni au gouvernement et à l'armée israéliens une infrastructure cloud avancée et des capacités d'apprentissage automatique. Au début du génocide, les forces israéliennes se seraient appuyées presque exclusivement sur des systèmes de génération de cibles alimentaires par l'IA, tels que Lavender, The Gospel et Where's Daddy, pour accélérer les massacres et les destructions de masse à Gaza. Ces plateformes absorbent des données de surveillance de masse sur l'ensemble de la population de Gaza afin de déterminer de manière algorithmique, à grande échelle : qui doit être tué, quels bâtiments doivent être bombardés et quel niveau de « dommages collatéraux » est jugé acceptable.

Ces systèmes basés sur l'IA intègrent de manière alarmante la logique géocidaire de leurs opérateurs. Ils sont entraînés à traiter les civils comme des « terroristes », s'appuyant sur la logique géocidaire des responsables israéliens selon laquelle « il n'y a pas de civils innocents à Gaza ». Parmi les efforts visant à automatiser le ciblage meurtrier, les commandants militaires auraient donné pour instruction aux soldats d'identifier et d'introduire autant de cibles que possible dans le système. Cela abaisse efficacement le seuil à partir duquel des individus sont désignés comme « militants du Hamas », jetant un large filet de sujets algorithmiquement signalés. Malgré son taux d'erreur élevé, le seul critère appliqué par les soldats israéliens à la Liste Lavender des personnes à tuer était le sexe de la cible, rendant ainsi tous les hommes palestiniens, enfants et adultes confondus, des cibles légitimes. Dans la pratique, la technologie de l'IA a permis au régime israélien de mettre en œuvre sa logique géocidaire avec une efficacité impitoyable, réduisant les Palestiniens, leurs familles et leurs maisons à ce que l'armée appelle de manière effrayante des « cibles poubelles ».

Si de nombreux détails techniques des systèmes de ciblage IA israéliens restent classifiés, il existe de nombreuses preuves crédibles que leur fonctionnalité dépend de l'infrastructure cloud et des capacités d'apprentissage automatique développées et maintenues par de grandes entreprises technologiques, notamment Google, Amazon, Microsoft et Palantir. Par conséquent, la fourniture directe par les entreprises technologiques de systèmes numériques utilisés dans la guerre menée par Israël soulève des questions urgentes quant à la complicité des entreprises dans de graves violations du droit international, notamment des actes pour lesquels la Cour pénale internationale (CPI) a émis des mandats d'arrêt à l'encontre du Premier ministre israélien Benjamin Netanyahu et de l'ancien ministre de la Défense Yoav Gallant.

## Du code aux listes noires

Alors qu'Israël intensifiait son offensive sur Gaza, sa demande en technologies d'intelligence artificielle et de cloud computing, fournies par les géants états-uniens de la technologie, a rapidement augmenté, intégrant ainsi l'infrastructure des entreprises dans la machine de guerre. En mars 2024, Google a renforcé ses liens avec le ministre israélien de la Défense (IMOD) en signant un nouveau contrat visant à créer une « zone d'atterrissage » spécialisée dans son infrastructure cloud, permettant à plusieurs unités militaires d'accéder à ses technologies d'automatisation. Amazon Web Services (AWS), partenaire de Google dans le cadre du projet Nimbus, aurait fourni à la Direction du renseignement militaire israélien une batterie de serveurs dédiés capable de stocker indéniablement les données de surveillance collectées sur presque tous les habitants de Gaza.

Des rapports récents ont également documenté l'expansion rapide des capacités militaires israéliennes basées sur l'IA, soulignant à quel point les partenariats croissants avec les entreprises technologiques ont accéléré le déploiement de systèmes avancés dans sa guerre contre Gaza. Selon des documents divulgués, Microsoft a hébergé des éléments du programme de surveillance de masse de l'armée israélienne sur ses serveurs cloud, stockant des enregistrements de millions d'appels téléphoniques interceptés provenant de Palestiniens à Gaza et en Cisjordanie. Les forces d'occupation israéliennes auraient utilisé ces fichiers pour identifier des cibles à bombarder, faire chanter des individus, placer des personnes en détention et également pour justifier des meurtres après coup. La dépendance de l'armée israélienne à l'égard de Microsoft Azure a augmenté en conséquence : au cours des six premiers mois de la guerre, son utilisation mensuelle moyenne a augmenté de 60 %, tandis que l'utilisation des outils d'apprentissage automatique d'Azure a été multipliée par 64 par rapport aux niveaux d'avant-guerre. En mars 2024, l'utilisation des outils technologiques de Microsoft et d'OpenAI par les forces israéliennes était près de 200 fois supérieure à celle de la semaine précédant le 7 octobre 2023. En outre, la quantité de données stockées sur les serveurs de Microsoft avait doublé pour atteindre plus de 13 pétaoctets.

Les résultats de l'enquête interne menée par Microsoft, annoncés en septembre 2025, ont finalement confirmé qu'une unité du ministre israélien de la Défense avait effectivement utilisé certains de ses services à des fins de surveillance interdites. En conséquence, l'entreprise a suspendu certains services cloud et d'IA, admettant que sa technologie était complice de pratiques contraires à ses conditions d'utilisation. Pourtant, la suspension des services de Microsoft à l'armée israélienne a été minimale : de nombreux contrats et fonctions avec l'armée israélienne et d'autres organismes gouvernementaux responsables de violations

flagrantes des droits humains et de crimes atroces restent intacts. Bien que l'examen lui-même soit toujours en cours, cet aveu partiel met à nu la complicité de l'entreprise dans la machine militaire israélienne.

De plus, l'implication des grandes entreprises technologiques dans la guerre d'Israël semble aller au-delà de la simple fourniture de services. Les ingénieurs de Microsoft auraient fourni une assistance technique à distance et sur place aux forces israéliennes, notamment à l'unité 8200 (cyberopérations et surveillance) et à l'unité 9900 (renseignement géospatial et ciblage). En fait, le ministre israélien de la Défense a acheté environ 19 000 heures de services d'ingénierie et de conseil à Microsoft, pour une valeur d'environ 10 millions de dollars. Amazon serait également impliquée, fournissant non seulement une infrastructure cloud, mais aussi une assistance directe pour la vérification des cibles des frappes aériennes. Le rôle de Google soulève des inquiétudes supplémentaires : selon des documents internes, l'entreprise aurait créé une équipe classifiée composée de ressortissants israéliens disposant d'habilitations de sécurité, chargée explicitement de recevoir des informations sensibles du gouvernement israélien qui ne pouvaient être partagées avec l'ensemble de l'entreprise. Cette équipe est chargée de dispenser une formation spécialisée avec les agences de sécurité gouvernementales et de participer à des exercices conjoints et des scénarios adaptés des menaces spécifiques. Aucun accord comparable ne semble exister entre Google et un autre État, ce qui souligne la portée exceptionnelle de sa collaboration avec le régime israélien.

Le profit n'est pas le seul moteur de l'implication croissante des grandes entreprises technologiques auprès de l'armée israélienne ; l'affinité politique joue également un rôle. Palantir Technologies, une société américaine d'analyse de données et de surveillance connue pour ses liens étroits avec les agences de renseignement et de défense, a ouvertement exprimé son soutien à Israël tout au long du génocide de Gaza. Palantir est associée à AWS pour fournir des outils conçus pour aider ses clients, tels que l'armée israélienne, à gagner dans le contexte de la guerre. La société a signé un partenariat stratégique avec le ministre israélien de la Défense afin de fournir des technologies soutenant directement la campagne génocidaire. Microsoft entretient également des liens de longue date avec l'armée et l'appareil sécuritaire israéliens, des liens si étroits que Netanyahu a un jour décrit cette relation comme un mariage fait au paradis mais reconnu ici sur terre.

En apportant un soutien direct aux opérations militaires israéliennes, les entreprises technologiques ne se contentent pas de fournir des infrastructures ; elles facilitent et contribuent activement à la surveillance, au ciblage et à l'exécution d'actions qui violent le droit international. Dans une évolution sinistre, le déploiement de l'IA commerciale à Gaza marque une frontière effrayante : des systèmes autrefois conçus pour optimiser la logistique et la prise de décision à grande échelle ont entraîné des listes d'élimination, effacent des familles et rasant des quartiers entiers. Les technologies développées et maintenues par les géants de la tech soutiennent désormais la guerre, le nettoyage ethnique et le génocide en Palestine, servant de prototype pour l'avenir de la guerre automatisée.

L'avenir de la guerre

Le régime israélien a officialisé son engagement en faveur de la guerre automatisée en créant une division de recherche dédiée à l'IA au sein du ministère de la Défense, chargée de faire progresser les capacités militaires vers un avenir où « les champs de bataille compteront des équipes de soldats et des systèmes autonomes travaillant de concert ». Cette initiative marque un tournant important vers la normalisation des combats basés sur l'IA. Les gouvernements occidentaux, notamment ceux de la France, de l'Allemagne et des États-Unis, suivent une trajectoire similaire, se précipitant pour intégrer l'intelligence artificielle dans leurs systèmes d'armement et leurs forces armées. Ensemble, ces développements positionnent Israël non seulement comme un précurseur, mais aussi comme un modèle pour la prochaine ère de la guerre algorithmique.

Parallèlement, les grandes entreprises technologiques abandonnent les barrières éthiques qu'elles s'étaient elles-mêmes imposées afin de décrocher des contrats militaires. Au début de l'année, Google et OpenAI ont discrètement renoncé à leur engagement volontaire de ne pas développer d'IA à des fins militaires, signalant ainsi un réalignement plus large avec les secteurs de la sécurité et de la défense. Quelques semaines après avoir modifié ses principes en matière d'IA, Google a signé un partenariat officiel avec Lockheed Martin, le plus grand fabricant d'armes au monde et l'un des principaux fournisseurs d'armes de l'armée israélienne. En novembre 2024, Meta a annoncé mettre ses grands modèles linguistiques, appelés Llama, à la disposition des agences gouvernementales américaines et des sous-traitants travaillant dans le domaine de la sécurité nationale. Lockheed Martin a depuis intégré Llama à ses opérations.

Dans la course à l'IA pour la guerre, Meta s'est également associé à Anduril, une start-up de technologie de défense, afin de développer des dispositifs de réalité virtuelle et augmentée pour l'armée américaine. Malgré son statut d'organisation à but non lucratif, OpenAI a collaboré avec Anduril pour déployer sa technologie sur le champ de bataille. En outre, Palantir et Anthropic, une société de recherche et développement en IA soutenue par Google, ont annoncé un partenariat avec AWS afin de « fournir aux agences de renseignement et de défense américaines un accès à ses systèmes d'IA ».

La décision de l'armée américaine d'accorder le grade de lieutenant-colonel à des cadres supérieurs de Palantir, Meta, OpenAI et Thinking Machines Labs et de les intégrer comme conseillers au sein des forces armées est un indicateur révélateur de la convergence croissante entre les grandes entreprises technologiques et les ministères de la guerre. Présentée comme un effort visant à « orienter des solutions technologiques rapides et évolutives vers des problèmes complexes », cette initiative vise à rendre l'armée américaine « plus intelligente, plus meurtrière ». Le symbolisme est difficile à ignorer : les dirigeants de la Silicon Valley ne se contentent plus de créer des outils pour le champ de bataille, ils sont désormais officiellement intégrés à sa structure de commandement.

La militarisation de l'IA dans un vide réglementaire

La militarisation de l'IA se développe rapidement en l'absence de cadres réglementaires en vigueur. Alors que les États continuent de débattre des normes relatives aux armes autonomes à l'ONU, aucun traité international contraignant ne régit spécifiquement leur développement ou leur déploiement. Les technologies à double usage, telles que les LLM et l'infrastructure

cloud, qui sont désormais intégrées dans les opérations militaires, sont encore moins réglementées. Les récentes discussions nationales et mondiales et les propositions réglementaires concernant la gouvernance de l'IA, qui se concentrent souvent sur la protection de la vie privée et des droits humains, évaluent largement l'impact dévastateur des systèmes d'IA dans les zones de conflit. L'exemple le plus éloquent de ce décalage est la signature par Israël du traité du Conseil de l'Europe sur l'IA, qui traite des droits de l'homme, de la démocratie et de l'état de droit, alors que des informations crédibles faisaient état de son utilisation de l'IA pour cibler des objectifs à Gaza. Si le traité contient de nombreuses réserves qui limitent son efficacité, la signature d'Israël dans le contexte d'une campagne génocidaire en cours souligne le profond décalage entre les normes juridiques en cours d'élaboration et le déploiement sur le champ de bataille des technologies qu'elles cherchent à réglementer.

Parallèlement, les lignes directrices ou les mécanismes de droit souple sont systématiquement ignorés. Les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme (UNGPs), qui définissent à la fois les obligations des États et les responsabilités des entreprises en matière d'identification et d'atténuation des risques liés aux droits humains, sont souvent ignorés par les entreprises technologiques. Alors que ces principes stipulent clairement que les entreprises opérant dans des zones de conflit doivent traiter le risque de contribuer à des violations flagrantes des droits humains et du droit international humanitaire comme une question de conformité juridique, les entreprises technologiques continuent de s'y conformer de manière sélective. L'aveu tardif de Microsoft selon lequel le régime israélien a utilisé son infrastructure cloud pour surveiller massivement la population de Gaza en est un exemple typique. En mai 2025, Microsoft a nié avoir permis au régime israélien de nuire aux Palestiniens par le biais d'une surveillance massive, avant de faire marche arrière quelques mois plus tard en admettant à demi mot l'utilisation impropre de sa technologie. Comme mentionné précédemment, cet aveu révèle à quel point les entreprises manquent leur responsabilité, en vertu des Principes directeurs, d'identifier et d'atténuer ces pratiques.

Dans ce contexte, le droit pénal international reste insuffisant pour traiter la complicité des entreprises dans les crimes de guerre. Le droit coutumier et le Statut de Rome limitent la responsabilité pénale aux personnes physiques, excluant les entreprises en tant que personnes morales. Par conséquent, la responsabilisation des entreprises vis-à-vis de leur implication dans la commission et la perpétration de crimes atroces, notamment le génocide, les crimes de guerre et les crimes contre l'humanité, constitue un combat juridique à part entière.

Alors que la perspective de voir un dirigeant du secteur technologique comparaître devant un tribunal pour avoir aidé et encouragé des crimes internationaux peut sembler lointaine, même les appels modestes en faveur d'une réglementation et d'une responsabilisation sont de plus en plus contestés. L'administration Trump a intégré les grandes entreprises technologiques dans sa quête plus large de domination mondiale, rendant ainsi les géants de l'industrie intouchables. En accord avec les lobbyistes du secteur, Trump s'est engagé à s'opposer à toute réglementation du secteur technologique au niveau national et a déjà commencé à démanteler les mécanismes de contrôle. Les sanctions infligées à la rapporteuse spéciale des Nations unies pour la Palestine, Francesca Albanese, à la suite de la publication de son rapport sur la complicité des entreprises dans l'occupation illégale et le génocide perpétrés par Israël, illustrent encore davantage le climat actuel dans lequel le gouvernement américain et les entreprises

se serrent les coudes pour se protéger de toute poursuite en justice et de toute obligation de rendre des comptes. Aggravée par un préjugé anti-palestinien profondément ancré et le double standard persistant entourant les crimes et l'occupation d'Israël, cette dynamique a créé un environnement juridique et politique permissif qui protège le secteur technologique des regards. En conséquence, les entreprises technologiques peuvent continuer à concevoir, déployer et soutenir des systèmes de ciblage basés sur l'IA et des technologies de surveillance de masse en collaboration directe avec l'occupation militaire israélienne, sans contrôle ni responsabilité.

Dans ce contexte de crise de la responsabilité, les travailleurs du secteur technologique jouent un rôle de plus en plus important dans la dénonciation de la complicité des entreprises. Alors que les dirigeants renforcent leurs liens commerciaux avec le régime israélien, la dissidence au sein de l'industrie technologique continue de croître, car de plus en plus d'employés refusent de développer des outils qui permettent le génocide, la colonisation et l'apartheid. Le licenciement récent de travailleurs de Microsoft qui protestaient contre le rôle de l'entreprise dans le génocide perpétré par Israël à Gaza a trouvé un écho chez Google, où des employés ont subi des représailles pour s'être opposés à la collaboration avec l'armée et les agences de sécurité israéliennes. Les organisateurs de groupes tels que No Tech for Apartheid et la Tech Workers Coalition ont joué un rôle central dans la dénonciation de l'implication profonde de l'industrie dans la violence étatique, souvent mise en œuvre par le biais de contrats militaires opaques et non divulgués.

## Recommandations

Alors que la résistance au sein de l'industrie technologique continue de croître, la société civile palestinienne et les mouvements de solidarité mondiale doivent intensifier leurs efforts pour démanteler les structures qui déshumanisent les Palestiniens et les traitent comme des cobayes pour de nouvelles technologies de guerre.

Tout d'abord, pour lutter contre la complicité des entreprises, il faut attaquer aux partenariats de recherche impliquant des entités privées, notamment des entreprises commerciales et des institutions universitaires, qui collaborent au développement et à la mise à l'échelle de technologies militaires. Il faut également examiner les flux financiers, les flux commerciaux et les liens économiques plus larges qui soutiennent et légitiment le secteur technologique militarisé d'Israël. Souvent décrite comme le « moteur de la croissance », l'industrie high-tech israélienne dépend structurellement des capitaux privés et étrangers. Environ 91 % de son financement provient du secteur privé, et environ 80 % des investissements en capital-risque proviennent de l'étranger. Ces chiffres soulignent à quel point les investisseurs internationaux, les universités et les entreprises sont directement impliqués dans le financement et la légitimation de l'appareil technologique militaire israélien. Les gouvernements, les régulateurs et la société civile devraient faire pression pour obtenir la transparence des flux financiers, subordonner les partenariats au respect du droit international et poursuivre le désinvestissement ou les sanctions contre les entreprises complices de crimes atroces et de violations systématiques des droits humains.

Deuxièmement, les efforts de la société civile et les initiatives juridiques axées sur la responsabilité doivent mettre davantage l'accent sur les infrastructures numériques qui sous-tendent les crimes d'Israël, non seulement à Gaza, mais aussi en Cisjordanie. Le Bureau du

---

Procureur de la CPI a récemment publié son premier plan d'action sur les enquêtes et les poursuites relatives aux crimes commis par voie électronique, reconnaissant enfin la dimension numérique des crimes atroces commis aujourd'hui. Si la poursuite des dirigeants du secteur technologique pour complicité dans ces crimes est une entreprise complexe et de longue haleine, semée d'embûches en matière de preuve, d'intention et de complicité, elle offre néanmoins une voie qui mérite d'être explorée.

L'avis consultatif de la Cour internationale de justice de 2024 sur l'illégalité de l'occupation israélienne indique clairement que les États ont l'obligation de s'abstenir de soutenir ou de maintenir cette présence illégale. Cet avis ouvre la voie à des poursuites judiciaires non seulement contre les gouvernements qui entretiennent des liens économiques ou militaires avec Israël, mais aussi contre les entreprises domiciliées dans ces États dont les technologies facilitent concrètement le nettoyage ethnique et l'occupation. Les acteurs de la société civile devraient utiliser cet avis pour faire pression sur les États afin qu'ils révoquent l'implication de ces entreprises, engager des poursuites judiciaires lorsque celles-ci ne se conforment pas à la loi et plaider en faveur du désinvestissement des entreprises qui continuent à fournir des infrastructures numériques au régime israélien.

Troisièmement, il est essentiel de renforcer les alliances entre les défenseurs juridiques et les travailleurs du secteur technologique. Ces collaborations peuvent mettre au jour des contrats militaires opaques, renforcer la collecte de preuves et amplifier la dissidence interne au sein de l'industrie. En reliant les stratégies juridiques à la résistance menée par les travailleurs, ces alliances peuvent à la fois remettre en cause la complicité inhérente aux infrastructures numériques de la guerre et de l'apartheid et jeter les bases de futurs mécanismes de responsabilisation.

Enfin, la mise en place de mécanismes clairs de responsabilisation pour l'IA militaire nécessite que les gouvernements, les régulateurs et la société civile collaborent pour combler les lacunes juridiques et remodeler le paysage technologique mondial dans le respect du droit international. La responsabilisation des grandes entreprises technologiques est particulièrement urgente compte tenu de l'utilisation croissante de l'IA dans la guerre et, par conséquent, de l'ampleur, de la rapidité et de l'opacité accrues de la force meurtrière générée par l'IA. Dans le cas de la Palestine, les technologies d'IA fournies par les grandes entreprises technologiques ont joué un rôle central en permettant au régime israélien de mener une campagne génocidaire à Gaza avec une ampleur et une cruauté sans précédent. La responsabilisation de ces entreprises est donc un élément central de la recherche plus large de justice et de responsabilité pour les crimes de guerre commis par Israël.

Traduction : JB pour l'Agence Média Palestine

Source : [Al-Shabaka](#)

**date créée**

2025/10/28