دور الذكاء الاصطناعي في حرب غزة

بين الاستخدامات العسكرية والفضائح التقنية

عبد العزيز عبد الله السعودي

دور الذكاء الاصطناعي في حرب غزة: بين الاستخدامات العسكرية والفضائح التقنية

دراسة حالة فضيحة مايكروسوفت كنموذج

عبد العزيز عبد الله السعودي

الفهرس

مقدمة

شهدت الصراعات العسكرية الحديثة تصاعداً غير مسبوق في دور تقنيات الذكاء الاصطناعي (AI) ضمن العمليات الحربية. خلال العدوان الإسرائيلي الأخير على غزة، برزت هذه التقنيات كـ"عامل تغيير قواعد اللعبة" وفقًا لوصف الجيش "الإسرائيلي"، حيث ساعدت في تتبع واستهداف خصومه بوتيرة أسرع من أي وقت مضى. في المقابل، ارتفعت أعداد الضحايا المدنيين بشكل كبير بالتزامن مع هذا الاعتماد على الخوارزميات، مما أثار مخاوف جدّية من أن تكون الأدوات الرقمية قد ساهمت في وفيات الأبرياء عبر قرارات استهداف خاطئة.

ارتكب جيش الاحتلال "الإسرائيلي" بارتكاب انتهاكات جسيمة للقانون الإنساني الدولي في غزة، ويخشى بعض خبراء التقنية وموظفي الشركات الكبرى أن تكون منتجاتهم قد مكّنت - بشكل غير مباشر - هذه الانتهاكات. في هذه الدراسة التحليلية، نستعرض ***التقنيات المدعومة بالذكاء الاصطناعي المستخدمة عسكريًا***، ودور كبرى شركات التكنولوجيا في تزويد جيش الاحتلال "الإسرائيلي" بتلك الأدوات، مع التركيز على فضيحة مايكروسوفت الأخيرة كمثال كاشف. كما نناقش ***الأبعاد الأخلاقية والقانونية*** لهذا التطور، ونتناول ***ردود أفعال المجتمعات التقنية*** داخليًا وخارجيًا، بالإضافة إلى ***دور الإعلام والتحقيقات الصحفية*** في كشف الحقيقة. سنختتم بتوصيات واقعية لمواجهة عسكرة الذكاء الاصطناعي في حروب غير متكافئة كساحة غزة.

التقنيات العسكرية المدعومة بالذكاء الاصطناعي في حرب غزة

اعتمد جيش الاحتلال "الإسرائيلي" خلال حرب غزة على حزمة واسعة من تقنيات الذكاء الاصطناعي لتعزيز قدراته في جمع المعلومات والاستخبارات والمراقبة والاستهداف. من أبرز تلك التقنيات:

- تحليل البيانات الضخمة والمراقبة الرقمية :قامت خوارزميات متقدمة بتمشيط كميات هائلة من الاتصالات المُعترَضة وبيانات المراقبة، بهدف البحث عن أنماط سلوك أو أقوال مشبوهة والتعرف على تحركات الخصوم. فعلى سبيل

المثال، استخدم جيش الاحتلال الإسرائيلي أنظمة AI لتحليل مكالمات هاتفية ورسائل نصية تم اعتراضها، بحثًا عن كلمات مفتاحية أو حوارات بين أفراد معينين، مما يساعد في تحديد أهداف محتملة بشكل أسرع. وبحسب تحقيق لوكالة أسوشييتد برس، تضاعفت كمية البيانات التي خزّنها جيش الاحتلال الإسرائيلي على خوادم مايكروسوفت بين 1445هـ (أكتوبر 2023م) و1446هـ (يوليو 2024م) لتتجاوز 13.6 بيتابايت، مع ازدياد هائل (بنسبة 200 ضعف) في استخدام خدمات Azure وواجهات OpenAI خلال ذروة الحرب. هذه القفزة الضخمة تعكس مدى اعتماد العمليات العسكرية على المعالجة السريعة للبيانات والاستخبارات عبر السحاب.

- خوارزميات التعرّف والترجمة الآلية :سخّرت "إسرائيل" قدرات الذكاء الاصطناعي في تحويل محتوى الاتصالات العربية إلى نصوص مترجمة يمكن تحليلها فورًا. فقد أكّد ضابط استخبارات "إسرائيلي" أن الجيش يعتمد على منصة Microsoft Azure في تفريغ وترجمة المكالمات الهاتفية والرسائل الصوتية والنصية التي يتم جمعها عبر المراقبة الجماعية. هذه النصوص المترجمة تُدمج بدورها مع أنظمة الاستهداف الداخلية للجيش لتشكيل صورة أوضح للأهداف المحتملة.

على سبيل المثال، يستطيع محللو الاستخبارات استخدام Azure للبحث الفوري ضمن أطنان من الوثائق النصية عن حوار بين شخصين أو إرشادات جغرافية مخفية في الكلام. ورغم أن هذه الأدوات سرعت عملية فرز المعلومات، إلا أنها ليست معصومة من الخطأ: فقد أقرّ الجيش بحدوث أخطاء ترجمة آلية من العربية إلى العبرية أدت إلى تصنيف أهداف بالخطأ. في إحدى الحالات، أساء النظام ترجمة كلمة عربية (بمعنى "قبضة قاذف (RPG" لتصبح "دفعة/دفعة مالية"، وكاد ذلك أن يُدخل أشخاصًا يتحدثون عن دفعات مالية في قوائم الاستهداف لولا اكتشاف الخطأ بشريًا في اللحظة الأخيرة. وفي حالة أخرى، أدى تفسير آلي خاطئ لوثيقة بعنوان "الامتحانات النهائية" إلى تصنيف قائمة تضم ألف طالب مدرسة على أنهم مشتبهون "إرهابيون" لولا أن تدخّل ضابط بشري وفهم أن القائمة لا تعدو كونها أسماء طلاب لامتحان مدرسي. هكذا تُظهِر الأمثلة كيف يمكن للأخطاء الخوارزمية أن تنتهك مبدأ "الدقة."

- الرصد الجوي والطائرات المسيرة :لعبت الطائرات المسيّرة (الـدرونز) دورًا حاسـمًا في حرب غزة، مستفيدةً من تقنيات AI في تمييـز الأهـداف وتتبعهـا تلقائيًـا. نشرت "إسرائيل" مقاطع مصـوّرة تُظهـر عدسـات الـدرون وهـي تـؤطر مركبـاتٍ مشبوهة ضمن دائرة الاستهداف قبل ثوانٍ من تدميرها. وتستخدم بعـض تلـك الدرونز خوارزميات رؤية حاسـوبية للتعـرّف على الأجسـام والوجـوه على الأرض وتصنيفها (مدني، مقاتل، عتاد عسكري) ثم توجيه الضربة أو إرسال الإحداثيات لوحدات المدفعية. ومنظومـة) "The Gospel" الإنجيـل) هـي مثـال على أداة توصية أهداف مدعومة بالذكاء الاصطناعي طوّرها جيش الاحـتلال الإسـرائيلي مـؤخرًا لاختيـار الأهـداف على نحـو شـبه تلقـائي. وذكـرت تقـارير صـحفية أن خوارزمية "Gospel" هذه تعمل كـ«مصنع اغتيالات جماعية» وفـق وصـف أحـد ضباط الاستخبارات السابقين، بحيث تقدّم كميات كبيرة من أسماء الأهداف في وقت قصير على حساب الجودة والدقة. إلى جانبها، طـوّرت إسـرائيل منظومـة أخـرى باسـم) "Lavender" الخُزامـى (تُسـتخدم أيضًـا لاقتـراح وضـبط قـوائم الأهداف للقصف. هـذه الأتمتـة في اختيـار الأهـداف تقلّـص الوقـت بـين جمـع المعلومة وتنفيذ الضربة، لكنها تثير المخاوف بشأن انخفاض مستوى المراجعة الإنسانية لكل هدف على حدة.

- التحلـيلات التنبؤيـة والـذكاء الاصـطناعي التوليـدي :سـعى خبـراء الوحـدة الاسـتخباراتية "الإسـرائيلية" الشـهيرة) 8200 المختصـة بالتجسـس الإلكترونـي والإشارات) إلى الاستفادة من تقنيات الـذكاء التوليـدي أيضًـا. كشـفت تقـارير أن أفرادًا في وحدة 8200 - بعضـهم موظفـون سـابقون في شـركات كبـرى مثـل GoogleوMeta ومايكروسـوفت - قـاموا بتطـوير نظـام ذكـاء اصـطناعي داخلـي مشـابه لـ ChatGPT مـدرَّب على بيانـات فلسـطينية تـم التقاطهـا، بهدف مساعدة المحللين في استخلاص رؤى من البيانات الاعتراضية الضـخمة. هذا الاستخدام يُثير تساؤلات أخلاقية حول خصوصية ملايين المحادثـات التـي جُمعت دون إذن، وحول إمكانية انحياز هذه النماذج ضـد الشـعب الواقـع تحـت الاحتلال.

باختصار، مثّلـت حـرب غـزة حقـل تجـارب حـي لتطبيقـات عسـكرية متعـددة للـذكاء الاصطناعي: بدءًا من الترجمة الفورية للمكالمات، ومرورًا بـالخوارزميات التـي "تـتعلم"

أنماط العدو من جبال البيانات، وصولًا إلى الطائرات المسيّرة شبه ذاتية القرار في الاشتباك. ويرى مسؤولون "إسرائيليون" أن هذه الأدوات جعلت عملية إنتاج الأهداف أكثر سرعة وفعالية، مع الإشارة إلى استمرار وجود "عدة طبقات من المراجعة البشرية" قبل تنفيذ الضربة. إلا أن الواقع الميداني - مع سقوط أكثر من 50 ألف شهيد -كما نحسبهم- في غزة خلال هذه العمليات - يطرح شكوكًا حول مدى دقة وتمييز تلك الأهداف "السريعة"، لا سيما مع اعتراف بعض الضباط بوقوع أخطاء ترجمة وتصنيف كما أسلفنا. هذا يقودنا للتساؤل: هل كانت وتيرة الاستهداف "الأسرع" على حساب الحياة المدنية؟

دور الشركات التقنية الكبرى في دعم المؤسسة العسكرية "الإسرائيلية"

لم يكن تطور القدرات العسكرية الإسرائيلية القائمة على الذكاء الاصطناعي ليتحقق لولا الدعم الحثيث من عمالقة التكنولوجيا الأمريكية. تشير تحقيقات حديثة إلى أن عددًا من كبرى الشركات - مثل مايكروسوفت وجوجل وأمازون - قدّمت خدمات حوسبة سحابية وأدوات ذكاء اصطناعي لجيش الاحتلال الإسرائيلي بشكل مكثّف خلال حرب غزة. يُضاف إلى ذلك شركات بنية تحتية رقمية مثل Cisco و Dellالتي وفّرت مراكز بيانات وخوادم، وشركة) Red Hat التابعة لـ (IBMالتي قدمت تقنيات للحوسبة السحابية، فضلًا عن شركة Palantir Technologies المتخصصة في تحليل البيانات والتي دخلت في "شراكة استراتيجية" لدعم مجهود "إسرائيل" الحربي بأنظمة ذكاء اصطناعي.

مشروع "نيمبوس" السحابي - تحالف جوجل وأمازون

من أهم معالم هذا التعاون بين وادي السيليكون وإسرائيل كان مشروع "نيمبوس " (Project Nimbus) الذي أُعلن عنه عام 1442هـ (2021م). مشروع نيمبوس هو عقد ضخم بقيمة 1.2 مليار دولار يفترض تزويد الحكومة "الإسرائيلية" - بما فيها وزارة الدفاع - بخدمات حوسبة سحابية متقدمة وقدرات ذكاء اصطناعي، وذلك عبر بناء بنية تحتية سحابية محلية داخل "إسرائيل" بالتعاون مع شركتي Google و Amazon. وبموجب هذا العقد، تؤمّن الشركتان تخزينًا ومعالجة للبيانات على نطاق واسع، وتوفران أدوات ذكاء اصطناعي مثل التعرّف على الوجوه وتصنيف الصور وتتبع الأشياء لصالح الجهات الحكومية "الإسرائيلية". يُتيح "نيمبوس" لـ "إسرائيل" أن تستخدم تقنيات كلاود حديثة "بقدر قليل من الرقابة" من جانب المزود، نظرًا لكون البيانات والتشغيل داخل ما يُسمى "السحابة السيادية" المحصورة جغرافيًا.

الشركات المعنية التزمت الصمت النسبي حول تفاصيل الاستخدامات العسكرية. جوجل مثلاً أكدت علنًا أن عقد نيمبوس مخصص لـ"تشغيل أحمال عمل على منصتنا التجارية من قبل وزارات حكومية كالصحة والمالية والتعليم" ونفت أنه موجه "لمهام حساسة تتعلق بالجيش أو الاستخبارات". كما شددت على أن على جميع زبائن Google Cloud الالتزام بشروط منع استخدام خدماتها فيما ينتهك حقوق الآخرين أو يسبب العنف. أما أمازون فاكتفت بالقول إنها "تركز على إتاحة فوائد التكنولوجيا السحابية لكل زبائنها أينما كانوا"، دون الخوض في التفاصيل.

رغم هذه التطمينات، ظهرت مخاوف جدّية داخل وخارج الشركتين. احتج مئات من موظفي Google و Amazon على العقد ضمن حملة "No Tech for Apartheid" وطالبوا بإلغائه. وقد أشار المحتجون إلى 3 نقاط رئيسية تثير قلقهم:

1. إعلان وزارة المالية "الإسرائيلية" عام 1442هـ (2021م) بصراحة أن وزارة الدفاع ستكون من الجهات المستفيدة من نيمبوس - ما يعني توظيفه عسكريًا منذ البداية.

2. طبيعة الخدمات السحابية المتقدمة التي يحصل عليها "الإسرائيليون" والتي يمكن أن تشمل تطبيقات مراقبة واستهداف تعتمد على – AI في ظل عدم

قـدرة Google على متابعـة كيفيـة اسـتخدام هـذه الأدوات فعليًـا داخـل "السحابة السيادية."

3. بنود التعاقد المقلقة التي تُقيد حق الشركات في إنهاء العقد أو قطع الخدمة استجابةً لضغوط حقوقية. فبحسب التقارير، Google وأمازون ألزمتا نفسيهما بعدم منـع أي جهـة حكوميـة "إسـرائيلية" (بمـا فيهـا الجـيش) مـن اسـتخدام الخدمات، كما تعهّـدتا بعـدم إلغـاء العقـد تحـت أي حملـة مقاطعـة أو ضـغط شعبي. هذا البند الأخير وُقّع استباقيًا تحسّبًا لحملات مناهضة مثل "No Tech for Apartheid"، ويبـدو أنـه نجـح حتـى الآن في إبقـاء الشـركتين ملتـزمتين بالعقد.

مع اندلاع حرب غزة في 1445هـ (أكتـوبر 2023م)، تصـاعدت المخـاوف مـن أن البنيـة التحتية والقدرات التي يوفرها نيمبوس أصبحت جزءًا من آلة الحرب. ورغم عدم ظهـور أدلة علنية مباشرة تربط خدمات Google/Amazon بضربات معينة، فإن التكتم حول تفاصيل المشروع أبقى التساؤلات قائمة. خصوصًا بعد ما كشفته مصادر إعلاميـة عـن اسـتخدام "إسـرائيل" لأنظمـة ذكـاء اصـطناعي جديـدة لاتخـاذ قـرارات القصـف مثـل منظومتي *"Lavender"* و"Gospel" (* المشار إليهما آنفًا).

وقد أبدى موظفو جوجل تخوفًا صريحًا من احتمال مساهمة منصـتهم السـحابية في تشغيل هذه المنظومات "المغموسة بالذكاء الاصطناعي" في المجازر.

الجدير بالذكر أن التعاون التقني بين Amazon/Google و"إسرائيل" ليس وليد الحرب الأخيرة فقط، بل له تـاريخ أطـول في سـياق تعزيـز مشـاريع المراقبـة. فعلـى سـبيل المثال، توفر خدمات Amazon Web Services منذ سنوات حلـول تخـزين ومعالجـة ضخمة للبيانات لوكالات "إسـرائيلية" مختلفـة. كمـا اسـتثمرت Amazon في شـركات "إسرائيلية" ناشئة مرتبطة بـالأمن السـيبراني. لكـن عقـد نيمبـوس مثّـل انتقالًـا إلـى مستوى غير مسبوق بإضفاء طابع رسمي وشامل على شـراكة التكنولوجيـا السـحابية مع المؤسسة العسكرية "الإسرائيلية."

مايكروسوفت - الشريك المفضل للمؤسسة العسكرية "الإسرائيلية"

رغم خسارة مايكروسوفت لصفقة "نيمبوس" أمام منافسيها عام 1442هـ (2021م)، إلا أنها حافظت بقوة على موقعها كشريك أساسي لـ"إسرائيل" في المجال التقني، بل وعززته بعد ذلك. فالشركة تُعتبر مزود الخدمات السحابية الأول لجيش الاحتلال الإسرائيلي عبر منصة Azure ، وقد كشفت وثائق مسرّبة مؤخرًا عن مدى تغلغل تكنولوجيا مايكروسوفت في عمل الوحدات العسكرية والاستخباراتية "الإسرائيلية" أثناء حرب غزة.

وفقًا لتحقيق مشترك أجرته صحيفة *The Guardian* ومجلة +972 وموقع Local Callالعبري، أظهرت السجلات التجارية لوزارة الدفاع "الإسرائيلية" ووثائق من فرع مايكروسوفت في "إسرائيل" أن منتجات وخدمات مايكروسوفت - وعلى رأسها منصة Azureالسحابية - مستخدمة من قبل عشرات الوحدات عبر سلاح الجو والبر والبحر وحتى شعبة الاستخبارات. بعض هذه الاستخدامات إداري (مثل البريد الإلكتروني وإدارة الملفات)، لكن جزءًا كبيرًا منها لدعم أنشطة قتالية واستخباراتية مباشرة. على سبيل المثال:

- وحدة الاستخبارات 8200 الشهيرة، ووحدة التقنية المتقدمة 81 التابعة لها، كانتا من المستفيدين من خدمات Azure لتخزين وتحليل المعطيات التجسسية.
- نظام "Rolling Stone" الإسرائيلي لإدارة تسجيلات السكان الفلسطينيين وحركتهم في الضفة وغزة - وهو نظام رقابي على التنقل - يعتمد في تشغيله على تكنولوجيا مايكروسوفت.
- خلال العدوان على غزة، استخدمت وحدة "أوفِك (Ofek) "التابعة لسلاح الجو - والمكلّفة بإدارة قواعد بيانات هائلة لما يسمى "بنك الأهداف" - حزمة الاتصالات ومنصات التراسل من مايكروسوفت لتنسيق المعلومات حول الأهداف المرشحة للضربات.

أكثر من ذلك، أوفدت مايكروسوفت مهندسيها للعمل جنبًا إلى جنب مع ضباط ووحدات الجيش في الميدان أو عن بُعد لتقديم دعم تقني مكثّف خلال سير العمليات. تفيد الوثائق بأن مهندسي مايكروسوفت تعاونوا مباشرة مع وحدات استخباراتية مثل 8200 ووحدة 9900 (وهي وحدة تجسس مرئي متخصصة بتحليل صور الأقمار الصناعية والاستطلاع) لضبط استخدام البنية السحابية في خدمة المهام الموكلة إليهم أثناء الحرب. وقد أبرمت وزارة الدفاع "الإسرائيلية" عقودًا مع مايكروسوفت لشراء 19 ألف ساعة من الدعم الهندسي والاستشاري بين 1445هـ (أكتوبر 2023م) و 1446هـ (نهاية يونيو 2024م)، مما ضخّ حوالي 10 مليون دولار إلى خزائن الشركة. هذا الاستثمار يعكس مدى "نهم" الجيش لقدرات الحوسبة السحابية الذي تزامن مع نهمه للذخائر، وفق تعبير أحد قادة الوحدات التقنية في الجيش.

تاريخيًّا، بدأت علاقة مايكروسوفت الوثيقة بقطاع الدفاع "الإسرائيلي" تأخذ شكلها الحالي منذ أواخر العقد الماضي. فبعد فشل الشركة في الفوز بعقد نيمبوس، أشارت تقارير إلى أن مسؤولي مايكروسوفت في "إسرائيل" شعروا بالقلق من خسارة موطئ قدمهم لصالح جوجل وأمازون. لكن مسؤولين في وزارة الدفاع "الإسرائيلية" بعثوا إشارات تطمين لمايكروسوفت بأنها ستبقى الشريك الموثوق رغم عدم حصولها على نيمبوس. وقد صدقت هذه التطمينات؛ ففي السنوات التالية، تعمّقت الشراكة لدرجة أن مايكروسوفت أصبحت تُكلف مرارًا بتنفيذ مشاريع شديدة الحساسية ومصنفة سرّية لصالح الجيش. بل إن موظفيها عملوا عن كثب مع وحدة 8200 ذاتها كما ذكرنا. كما استفادت إسرائيل من علاقة مايكروسوفت بشركةOpenAI ، حيث حصلت على وصول واسع لنموذج GPT-4 (محركChatGPT) عبر منصةAzure ، خصوصًا بعد أن عدّلت OpenAI سياساتها ورفعت الحظر عن الاستخدامات العسكرية لمنتجاتها.

وكشفت الوثائق أن استهلاك جيش الاحتلال الإسرائيلي لأدوات) OpenAI مثل-GPT 4(تضاعف عدة مرات في النصف الأول من 1445هـ (2024م)، حتى شكّلت استخدامات الجيش ربع إجمالي استهلاك خدمات Azure-OpenAI في فترة معينة. هذا يعني أن الذكاء الاصطناعي التوليدي قد يكون استُخدم لتلخيص معلومات استخبارية أو للإجابة على استفسارات المحللين بسرعة أو حتى لترجمة محتوى بشكل متقدم.

لم يكن مستغربًا إذًا أن تزداد تبعية جيش الاحتلال الإسرائيلي لشركات التكنولوجيا الكبرى خلال حرب غزة. فقد صرّح عدة مصادر دفاعية "إسرائيلية" للجارديان بأن الجيش بات "يعتمد بشكل متزايد" على شركات كبرى مثل مايكروسوفت وأمازون وجوجل لتخزين وتحليل كميات متزايدة من البيانات الاستخباراتية لفترات أطول. في إحدى المحاضرات خلال مؤتمر تقني في تل أبيب 1445هـ (أواخر 2023م)، شرحت عقيدة في وحدة التكنولوجيا العسكرية (العقيد راحيلي دمبينسكي) كيف أن أنظمة الجيش التقنية انهارت مؤقتًا تحت ضغط البيانات في بدايات الغزو البري لغزة، ما اضطر الوحدة المسؤولة (مامرام Mamram) إلى "شراء قدرة حوسبية من العالم المدني" على الفور. أثنت دمبينسكي في تصريحات كُشف عنها لاحقًا على "الثروة الهائلة من الخدمات" التي وفّرتها شركات السحاب التجارية، بما في ذلك قدراتها المتقدمة في الذكاء الاصطناعي، مؤكدة أن التعاون مع هذه الشركات أعطى الجيش "فعالية عملياتية كبيرة جدًا" في غزة. والمثير أن شعارات Azure و Amazon Web Services وGoogle Cloud ظهرت في الشرائح التي عرضتها دمبينسكي خلال حديثها، مما يؤكد بالصور ذلك التعاون الثلاثي.

باختصار، أصبحت البنى التحتية الرقمية لشركات وادي السيليكون بمثابة" العجلة الخفية "التي تدور في خلفية آلة الحرب "الإسرائيلية". السحابات التجارية تحولت إلى مستودعات بيانات عسكرية، والنماذج اللغوية أضحت محللين استخباريين، ومنصات التعرف صارت أعينًا إضافية في ميدان القتال. هذا "التحالف غير المرئي" بين عمالقة التقنية وصناع القرار العسكريين تجلّى بوضوح في فضيحة مايكروسوفت الأخيرة، التي نناقشها تفصيلًا فيما يلي.

فضيحة مايكروسوفت: نموذج لتحالف التقنية والعسكرة

كشفت التسريبات والتقارير الاستقصائية الأخيرة عن تفاصيل صادمة بشأن مدى تورط مايكروسوفت في الحرب على غزة، مما شكل فضيحة مدوية أعادت تسليط الضوء على دور الشركات التقنية في النزاعات. برز ذلك خصوصًا بعد تحقيق ***أسوشييتد برس*** في 1446هـ (فبراير 2025م)، ومن قبله تحقيق ***الجارديان*** وشركاؤها في 1446هـ (يناير 2025م)، مما أجبر مايكروسوفت نفسها على الاعتراف علنًا ببعض الحقائق.

يمكن تقسيم ملامح هذه القضية إلى ثلاثة محاور: ما كشفته التسريبات، رد فعل الشركة وموظفيها، والتداعيات الأخلاقية.

ما الذي كشفته الوثائق المسربة؟

بحسب وثائق داخلية تسرّبت من وزارة الدفاع "الإسرائيلية" وفرع مايكروسوفت المحلي (حصلت عليها مجموعة *Drop Site* الإخبارية ونُشرت عبر +972 و Local Call والجارديان)، تبيّن أن مايكروسوفت عمّقت تعاونها مع جيش الاحتلال الإسرائيلي إلى مستويات غير مسبوقة بعد ربيع الأول 1445هـ (7 أكتوبر 2023م). من أهم ما ورد في هذه التسريبات:

- قفزة هائلة في استخدام خدمات Azure خلال الحرب :تضاعف متوسط الاستهلاك الشهري للجيش من خدمات التخزين السحابي Azure بنسبة 60% أعلى خلال الأشهر الستة الأولى من الحرب مقارنة بالأشهر الأربعة التي سبقتها. كما ازداد استهلاك خدمات Azure للذكاء الاصطناعي (كأدوات الـ Machine Learning) بمعدل 64 ضعفًا بنهاية مارس 2024 مقارنة بسبتمبر 2023. هذه الزيادة المهولة تؤكد ما كشفته AP أيضًا من أن استخدام "إسرائيل" لخدمات مايكروسوفت و OpenAI ارتفع 200 ضعف مباشرة بعد هجوم 7 أكتوبر – أي أن "إسرائيل" سارعت للاعتماد على الموارد السحابية الأمريكية لتلبية "شهية" الحرب الرقمية.

- خدمات Azure في قلب الوحدات العسكرية :أكدت الوثائق استخدام Azure من قبل وحدات تمسّ صلب العمليات. فقد استُخدمت المنصة في الوحدات الاستخباراتية 8200 و81 (الأخيرة مختصة بابتكار تكنولوجيا التجسس). كما شغّلت Azure نظام الرقابة على السكان الفلسطينيين .("Rolling Stone") واستخدمتها وحدة "أوفك" الجوية لإدارة "بنك الأهداف" أثناء القصف. أي أن Azure لم يكن مجرد مخزن بيانات ثانوي، بل ركيزة للبنى التحتية الحرجة في المجهود الحربي.

- عقود دعم فني بملايين الدولارات :بعد بدء الحرب مباشرة، اتفقت وزارة الدفاع "الإسرائيلية" مع مايكروسوفت على شراء 19 ألف ساعة دعم هندسي سريع

لوحدة الحوسبة المركزية في الجيش (مامرام) ووحدات أخرى بين 1445 و1446هـ (أكتوبر 2023 ويونيو 2024م). بلغت قيمة هذه الساعات حوالي 10 مليون دولار. وشمل الدعم قيام مهندسي مايكروسوفت بالعمل عن قرب مع وحدات استخباراتية مثل 8200 و9900 لضمان استمرارية العمليات الرقمية. أي أن موظفين مدنيين من مايكروسوفت وجدوا أنفسهم فعليًا وسط حرب غزة كمقدمي دعم للمجهود العسكري - وهو مشهد غير مألوف يطمس الحدود بين الدور المدني والتورط العسكري.

- توفير مايكروسوفت نماذج ذكاء اصطناعي متقدمة للجيش :استفاد الجيش عبر Azure من شراكة مايكروسوفت معOpenAI ، فحصل على إمكانية استخدام نموذج) GPT-4 أحد أقوى النماذج اللغوية التوليدية) على نطاق واسع. وتشير الملفات إلى أن جيش الاحتلال الإسرائيلي زاد بشكل حاد اعتماده على أدوات OpenAI في غضون الأشهر الأولى للحرب. نحو ربع استهلاك الجيش من خدمات التعلم الآلي عبر مايكروسوفت كان مخصصًا لنماذج OpenAIفي مرحلة ما. يُذكر أن شركة OpenAI كانت حتى 1445هـ (منتصف 2023م) تمنع استخدام تقنياتها لأغراض "عسكرية أو حربية"، لكنها عدّلت سياساتها بهدوء في 1445هـ (يناير 2024م) لتسمح بحالات "الأمن القومي" المتوافقة مع رسالتها. أعقب ذلك التغيير مباشرة تصاعد في استخدام "إسرائيل" لأدوات .Azure-OpenAI هذا التطور أتاح - نظريًا على الأقل - توظيف نماذج مثل GPT-4 في ترجمة كمّ هائل من النصوص العربية بسرعة أو تحليل محتوى اتصالات أو حتى تحسين برمجيات الاستهداف باستخدام قدرات الذكاء التوليدي.

- استثمارات مبكرة ومشاريع مظلمة :إضافةً لما سبق، يجدر التنويه بأن مايكروسوفت كان لها تاريخ سابق في دعم تكنولوجيات استخباراتية لصالح "إسرائيل". فقد استثمرت عام 1440هـ (2019م) في شركة "إسرائيلية" تدعى AnyVisionمختصة بتقنيات التعرف على الوجوه، أُتهمت بتزويد الاحتلال بأنظمة لمراقبة الفلسطينيين على الحواجز وفي الضفة الغربية. ورغم أن مايكروسوفت انسحبت من الاستثمار في 1441هـ (2020م) تحت ضغط حقوقي، تبقى هذه الحادثة مؤشرًا على انجذاب الشركة لقطاع الأمن "الإسرائيلي".

كذلك أطلقت مايكروسوفت مؤخرًا (يونيو 2023) مركز بيانات Azure جديد في "إسرائيل" لتعزيز خدماتها المحلية، ما يعني استعدادها المسبق لتلبية أية احتياجات حكومية/عسكرية في البنية التحتية السحابية.

مجمل هذه الحقائق يرسّم صورة واضحة: مايكروسوفت لم تكن مجرد مزود خدمات عادي لـ"إسرائيل"، بل شريك تقني موثوق ومنخرط بعمق في عمليات الجيش. الفضيحة هنا تكمن في التضارب الصارخ بين خطاب الشركة العلني عن "الذكاء الاصطناعي المسؤول" والتزامها الأخلاقي، وبين الدور الفعلي الذي لعبته تقنياتها في حرب مدمرة كبّدت المدنيين ثمناً باهظًا.

موقف مايكروسوفت وردود الفعل الداخلية والعالمية

عقب التقارير الإعلامية الكاشفة، وجدت مايكروسوفت نفسها أمام ضغط متصاعد من الرأي العام وداخل صفوفها. بعد حوالي ثلاثة أشهر من نشر تحقيقAP ، اضطرت الشركة في 1446هـ (مايو 2025م) لإصدار بيان رسمي على مدونتها تعترف فيه ببعض الجوانب. أبرز ما جاء في ذلك البيان وما تلاه من ردود:

- إقرار بالدعم التقني وتبرير الاستخدام :أكدت مايكروسوفت أنها خلال حرب غزة قد باعت "خدمات ذكاء اصطناعي وحوسبة سحابية متقدمة" لجيش الاحتلال الإسرائيلي وساعدت في "جهود تحديد مواقع وإنقاذ الرهائن" الذين "اختطفهم" تنظيم حماس. لكنها بنفس الوقت نفت وجود "أي أدلة" على استخدام منصتها Azure أو تقنياتها AI لاستهداف أو إيذاءالمدنيين في غزة. شددت الشركة أن دعمها كان "محدودًا" و"خاضعًا لإشراف صارم" بهدف إنقاذ الرهائن، مشيرة إلى أنها رفضت بعض الطلبات العسكرية ووافقت على البعض "بعد التأكد من احترام الخصوصية وحقوق المدنيين". وأضافت أنها وفّرت برامج وخدمات احترافية وتخزين سحابي وأدوات ترجمة، وكذلك "وصولًا خاصًا لتقنياتنا خارج شروط التعاقد" كجزء من دعم طارئ لـ"إسرائيل". أي أن مايكروسوفت تُقر بأنها تجاوزت ربما عقودها التجارية لتلبية احتياجات "إسرائيل" أثناء الحرب.

- الالتـزام النظـري بالمعـايير الأخلاقيـة :ذكّـرت مايكروسـوفت أن على جـيش الاحتلال الإسرائيلي، كأي زبون آخر، الالتزام بسياسة الاستخدام المقبول ومدونة أخلاقيات الذكاء الاصطناعي للشركة، التي تحظـر اسـتخدام المنتجـات لإلحـاق الأذى بطريقة غير قانونية. وقالت إنها لم تجد دليلًا على انتهاك الجيش لتلـك الشروط. لكن في المقابل أقرت الشركة ضمنيًا بانعـدام الشـفافية بعـد البيـع، حيث أوضحت أنها "لا تملك رؤيـة حـول كيفيـة اسـتخدام العمـلاء لبرمجياتهـا على خـوادمهم الخاصـة أو ضـمن منصـات سـحابية أخـرى". هـذا يعنـي أن مايكروسوفت نفسها ليست متأكدة تمامًا مما يفعله الجـيش بتقنياتهـا بعيـدًا عن أعينها – وهو ما يقوض إلى حد ما تأكيداتها السابقة.

- تحقيـق داخلـي وغسـيل سـمعة :ذكـرت مايكروسـوفت أنهـا وبسـبب قلـق الموظفين وما أثير إعلاميًا بدأت مراجعـة داخليـة واسـتعانت بشـركة خارجيـة للتحقق من الأمر. لكنها لم تفصح عن نتائج تلـك المراجعـة أو تفاصـيلها. هـذا التكتم، إلى جانب لغة البيان التي اعتبرها الموظفون تجميلية وتبريرية، قوبـل بانتقادات حادة. حيـث صـرّح تجمـع) "No Azure for Apartheid" الـذي يضـم موظفين حاليين وسابقين) أن البيان مجرد "حيلة علاقات عامـة لغسـل صـورة الشركة التي تلطخت". وطالب التجمـع بنشـر التقريـر الكامـل لتحقيـق الشـركة المستقل لإثبات الشفافية.

- غضب واحتجاجات الموظفين :على مدار شهور الحـرب، شـهدت مايكروسـوفت حراكًا غير مسـبوق مـن موظفيهـا ضـد تـورط شـركتهم مـع "إسـرائيل". ففـي 1445هـ (أكتوبر 2023م)، شـارك العشـرات في وقفـة احتجاجيـة (صـلاة غائـب) بمقر الشركة حدادًا على ضـحايا غـزة، نظمهـا الموظفـان حُسـام نصـر وعبـدو محمد وآخرون، فقامت الشركة بفصل المنظمين بعد ذلك بوقت قصـير. لاحقًـا، خلال المؤتمر السنوي للمطورين "Microsoft Build" في 1445هـ (مايو 2025م)، لاحظ العاملون أن رسائل البريد الإلكتروني الداخلية التي تتضـمن كلمـات مثـل "فلسطين" أو "غزة" أو "أبارتهايد" لم تعد تصـل للمسـتلمين أو تتـأخر لسـاعات طويلة. وعنـدما تكشّف الأمر، اعترفت مايكروسوفت بأنها حجبت فعليًا الرسـائل ذات المحتوى السياسـي عـن الانتشـار الواسـع داخـل الشـركة، مبـررة ذلـك بـأن "إرسال رسـائل لآلاف المـوظفين بمواضـيع غيـر متعلقـة بالعمـل هـو أمـر غيـر

مناسب". لكن موظفين رأوا في ذلك قمعًا لحرية التعبير ومحاولة لإسكات أي تعاطف مع الفلسطينيين داخل الشركة.

بلغت الاحتجاجات ذروتها في احتفال الشركة بالذكرى الخمسين لتأسيسها في مارس وأبريل 2025. حيث قام موظفون غاضبون بمقاطعة كلمات المسؤولين رفيعي المستوى مرتين خلال شهر واحد. في 20 مارس، هتف موظف حالي وآخر سابق في وجه الرئيس براد سميث والمدير التنفيذي السابق ستيف بالمر بشعارات تندد بدور مايكروسوفت في جرائم الحرب. وفي 4 أبريل، خلال فعالية أخرى، اعتلت المهندستان إبتِهال أبوسعِد وفانيّا أغروال المنصة وقاطعتا كلمة مصطفى سليمان (نائب رئيس قسم الذكاء الاصطناعي بمايكروسوفت) مرددتين "أنتم شركاء في إبادة جماعية، أوقفوا استخدام الذكاء الاصطناعي للإبادة". قامت الشركة بإقالة المهندستين خلال أيام من الحادثة، ما فاقم غضب زملائهما. كما تجمع متظاهرون خارج مقر الحدث رافعين شعار Microsoft" تُشغّل الإبادة" وقد عُرض هذا الشعار ضوئيًا على جدار القاعة في سياتل.

تعكس هذه الأحداث أجواء" اضطراب غير مسبوق "داخل الشركة، وصفها أحد المهندسين السابقين بأن الوضع "يقترب من نقطة الانفجار". كثير من الموظفين بدأوا يرون في سياسات شركاتهم خيانة لقيمهم الأخلاقية والشخصية، حتى أن بعضهم قدّم استقالته علنًا بسبب ذلك. يُذكر أن ما حدث في مايكروسوفت له صدى في شركات أخرى أيضًا: ففي Google مثلًا، احتج المئات (ضمن حملة No Tech for Apartheid) على عقد نيمبوس، مما أدى إلى فصل بعضهم (كالمهندس إدي هاتفيليد) واستقالة آخرين.

- انتقادات حقوقية ودولية :تزامنًا مع الحراك الداخلي، صدرت بيانات عن منظمات حقوقية وتقنية تنتقد اشتراك الشركات في تمكين آلة الحرب. مؤسسة الجبهة الإلكترونية (EFF) رحبت بخطوة مايكروسوفت نحو الشفافية وبيانها العلني، لكنها شددت على أن هناك أسئلة عديدة بلا إجابة حول تفاصيل كيف استُخدمت خدمات الشركة ونماذجها من قبل الجيش. المديرة التنفيذية لـ EFFسيندي كوهن قالت: "من الجيد أن هناك قليلًا من الشفافية هنا، لكنه من الصعب التوفيق بين ذلك وبين ما يحدث فعليًا على الأرض". كما

أثارت منظمات مثل هيومن رايتس ووتش ومنظمة العفو الدولية مسألة المساءلة: هل تُجرى أي تحقيقات مستقلة في دور التكنولوجيا في سقوط هذا العدد الهائل من المدنيين؟ وهل ينبغي تحميل مزودي التقنيات جزءًا من المسؤولية إن ثبت علمهم باستخدامها في جرائم حرب؟ حتى الآن، لا توجد إجابات شافية، لكن مجرد طرح السؤال مؤشر على تغير نظرة المجتمع الدولي لدور الأطراف الخاصة في الحروب.

التحالف الخفي بين الذكاء الاصطناعي والسياسات العسكرية

فضيحة مايكروسوفت – بما ظهر فيها من تكتم ثم انكشاف – عرّت التحالف غير المرئي الذي طالما جمع بين شركات التقنية الكبرى والمؤسسات العسكرية لكن من وراء الستار. لقد كشفت الوثائق كيف تم دمج أنظمة رقمية مدنية داخل التكتيكات العسكرية بأعقد تفاصيلها، وكيف أصبحت شركة مثل مايكروسوفت جزءًا لا يتجزأ من البنية التحتية للحرب. هذا الواقع الجديد يثير أسئلة جوهرية حول مفهوم "حيادية التكنولوجيا". فلطالما ادّعت الشركات أن منتجاتها "أدوات محايدة" يمكن استخدامها للخير أو الشر بحسب نوايا المستخدم. غير أن حالة غزة تظهر أن توفير تلك الأدوات المتقدمة لطرف يمارس الاحتلال وهجمات عسكرية واسعة النطاق يمنحه تفوقًا غير عادل وقد يكرس سياسات عدوانية. كما أن سرّية الاتفاقيات (مثل عقد نيمبوس، أو عقود Azure) حجبت عن الجمهور أي نقاش ديمقراطي حول جدوى تورط شركات أميركية في صراع معقّد ذي أبعاد حقوقية وإنسانية. وبالتالي، عندما ظهرت الحقيقة، شعر كثيرون بالخيانة: الموظفون أيقنوا أنهم ربما ساهموا دون قصد في إراقة دماء، والجمهور صُدم بأن أدوات الذكاء الاصطناعي المستخدمة لإمتاعهم أو زيادة إنتاجيتهم ذات صباح، استُخدمت في قتل عائلات بأكملها في غزة ذات مساء.

من زاوية أخرى، أظهرت هذه الفضيحة أيضًا مدى تغلغل التفكير العسكري في رؤية الشركات التقنية للمستقبل. فخلال الحرب، غيّرت كبرى شركات AI سياساتها الأخلاقية لتفتح الباب أمام الاستخدام العسكري :OpenAI أزالت حظرًا صريحًا كان موجودًا على استخدام خدماتها في أغراض حربية، و Googleبدورها حذفت من ميثاق أخلاقياتها في 1445هـ (فبراير 2025م) عبارة تمنع استخدام الذكاء الاصطناعي في المراقبة أو تطوير الأسلحة. أي أننا أمام حالة تطبيع متزايد لفكرة أن تقنيات

الذكاء الاصطناعي ستكون أدوات في أيدي الجيوش وأجهزة الأمن. ولعل تعليقًا ورد في كتاب جديد لرئيس شركة Palantir ألكسندر كارب يلخص هذا التوجه، حيث دعا صراحةً لتعاون أعمق بين وادي السيليكون والجيوش لتطوير "أسراب الدرونز والروبوتات غير المأهولة التي ستسيطر على ساحات المعارك القادمة". إذا أخذنا هذا التصريح في سياق فضيحة مايكروسوفت، ندرك أننا نقف أمام تحول paradigmatic: من عهد كانت التقنية فيه "مدنية أولًا" مع استثناءات عسكرية، إلى عهد تصبح فيه العسكرة جزءًا مدمجًا في صلب استراتيجية شركات التقنية.

الأبعاد الأخلاقية والقانونية لاستخدام الذكاء الاصطناعي عسكريًا

يثير استخدام الذكاء الاصطناعي في ساحات القتال – لا سيما في نزاع غير متكافئ كالحرب على غزة – أسئلة أخلاقية وقانونية معقدة. فالتكنولوجيا التي يُروّج لها بأنها تساهم في "جعل الاستهداف أكثر دقة وفعالية"، قد تتحول إلى سلاح ذو حدين: إما أن تقلل الأضرار الجانبية بفضل الدقة المحسّنة، أو تفاقمها إذا ما اعتمد عليها عميانًا رغم ما يشوبها من قصور. نناقش هنا ثلاثة محاور أساسية: انتهاكات القانون الدولي الإنساني، مسألة المسؤولية عن القرارات الخوارزمية القاتلة، وجدلية حياد التكنولوجيا.

انتهاكات القانون الدولي الإنساني(IHL)

يُلزم القانون الدولي الإنساني (وخاصة اتفاقيات جنيف) الأطراف المتحاربة بقاعدة التمييز بين المقاتلين والمدنيين وقاعدة التناسب في الهجمات (أي عدم شن هجوم تُعلم أنه سيسبب خسائر مفرطة بالمدنيين قياسًا بالميزة العسكرية المرجوة). عندما تدخل الخوارزميات على خط اتخاذ القرار، تبرز مخاطر جديدة على هاتين القاعدتين:

- خطر الخطأ في التمييز :إذا كانت خوارزميات التعرف على الصور أو الترجمة الآلية تُخطيء أحيانًا في تفسير مشهد أو عبارة – كما رأينا في مثال ترجمة "قبضة – RPG" فإن قرار استهداف مبني على تلك المعلومات المغلوطة قد يعني ضرب هدف مدني ظنًا أنه عسكري. إحدى الوثائق المسرّبة أشارت إلى أن نظام الاستهداف الإسرائيلي كاد يضم طلاب مدارس أبرياء إلى قائمته بسبب

خطأ تقني. مثل هذا الإجراء (استهداف مدنيين بناءً على معلومات خاطئة) يخرق مباشرة مبدأ التمييز ويُعرّض منفذيه للمساءلة عن هجوم غير مشروع حتى لو كانت النية الأصلية استهداف مقاتلين.

- خطر القرارات الآلية السريعة على مبدأ التناسب :يعتمد مبدأ التناسب على تقييم بشري واجتهادي إلى حد كبير (ما "ميزة" ضرب هدف مقابل "الأضرار الجانبية" المتوقعة). إذا تُركت خوارزمية توصية الأهداف تقرر دون إشراف كافٍ، فقد ترشّح أهدافًا ذات أهمية تكتيكية ضئيلة لكن في مناطق مزدحمة بالمدنيين. وقد أشار خبراء أن أنظمة الذكاء الاصطناعي تفتقر للإحساس البشري بالحكم الأخلاقي. فآلة قد ترى تجمعًا لشخصين قرب موقع إطلاق صواريخ فتعتبرهم هدفًا مشروعًا، بينما قائدٌ بشري ربما يدرك أن الضربة ستدمر حيًا بأكمله مقابل فائدة محدودة. وإذا نفذت الضربة عشوائيًا تحت تأثير سرعة التوصيات الآلية، فقد تقع مجزرة لا تتناسب مع أي مكسب عسكري – مما يشكّل انتهاكًا صارخًا للقانون الدولي. جدير بالذكر أن عدد الضحايا المدنيين ارتفع بشكل هائل خلال الحرب على غزة (أكثر من 50 ألف قتيل في غزة ولبنان، كثير منهم نساء وأطفال)، ما دفع خبراء وقانونيين للتساؤل إن كان الاستخدام الموسّع لـ AIقد ساهم في "تطبيع" قتل المدنيين عبر جعل الدمار الواسع يبدو كأنه نتيجة "أخطاء تقنية" أو قرارات معقمة. بمعنى آخر: هل هناك جرائم حرب ارتُكبت بواسطة قرارات خوارزمية أو بمساعدتها؟

هيئة مثل اللجنة الدولية للصليب الأحمر عبّرت سابقًا عن قلقها من أن الأسلحة ذاتية التشغيل أو الأنظمة المؤتمتة قد لا تستطيع الامتثال لقواعد القانون الدولي الإنساني. ومع أن إسرائيل تدّعي وجود "إنسان في الحلقة" بكل قرار، إلا أن السرعة الهائلة التي وفرتها أنظمة الذكاء ربما قلّصت فعليًا ذلك الهامش للمراجعة الإنسانية المتأنية. في المحصلة، يظل الجيش المستخدم للتقنية مسؤولًا قانونيًا عن نتائج الضربات. ولا يُقبل قانونًا الدفع بأن "الخوارزمية أخطأت" لتجنب المسؤولية – فالمسؤولية الجنائية عن جرائم الحرب شخصية وتقع على عاتق القادة والمنفذين.

هل تسهم هذه التقنيات في جرائم حرب؟

انطلاقًا مما سبق، يمكن القول إن التقنية نفسها لا تُرتكب جرائم، إنما البشر الذين يستخدمونها بطرق مخالفة للقانون هم من يُحاسبون. لكن المساهمة في الجريمة قد تأتي بشكل غير مباشر عبر توفير الأدوات مع العلم باحتمال إساءة استخدامها. هنا تبرز مسألة مسؤولية الشركات التقنية: هل يمكن اعتبار شركات مثل مايكروسوفت وجوجل وأمازون متواطئة أو متورطة في جرائم حرب "إسرائيل" ضد المدنيين في غزة؟ بعض خبراء القانون الدولي يرون أنه إذا كانت الشركة تعلم أو يفترض بها أن تعلم بأن خدماتها ستستخدم في أنشطة غير مشروعة (مثل هجمات عشوائية)، واستمرت رغم ذلك في التزويد والدعم الفني، فقد تقترب من عتبة "المشاركة في الجريمة". هذا المبدأ شبيه بمسؤولية الشركات التي زودت نظام الفصل العنصري في جنوب أفريقيا بتكنولوجيا القمع – حيث لاحقها ناشطون قانونيًا بدعوى التواطؤ في انتهاكات حقوق الإنسان.

في حالتنا، أعلنت مايكروسوفت أنها لم تجد دليلًا على أن الجيش انتهك بنود الاستخدام أو القانون. ولكن منظمات حقوقية أشارت إلى أن انعدام الشفافية يجعل هذا الادعاء فارغًا. تقرير لوكالة الأناضول نقل عن خبيرة الذكاء الاصطناعي الدكتورة هايدي خلاّف (من معهد AI Now قولها" :***إسرائيل تستخدم أنظمة ذكاء اصطناعي في كل مرحلة تقريبًا من عملياتها العسكرية، رغم علمها بمخاطر عدم الدقة الكامنة فيها، وهذا قد يجعل شركات التكنولوجيا الأمريكية شريكة في إزهاق أرواح المدنيين بصورة اعتيادية***." بعبارة أخرى، يشير البعض إلى أن تطبيع مخرجات قاتلة للمدنيين عبر أدوات AI يجعل اللوم موزعًا على مطوري التقنية وبائعيها، وليس فقط المستخدم المباشر لها.

حتى اللحظة، لا توجد سوابق قانونية واضحة تحمل شركات التقنية مسؤولية قانونية مباشرة عن جرائم حرب ارتكبها عملاؤها. لكن الضغط المعنوي والأخلاقي يتصاعد. ونظرًا لجسامة أحداث غزة، قد نشهد دعوات لتطوير أطر دولية جديدة تشرف على صادرات التقنيات الحساسة كما تشرف على صادرات الأسلحة التقليدية. إن سوء الاستخدام الخوارزمي الذي يؤدي لقتل المدنيين عمداً أو بلا تمييز، قد يُجادَل بأنه يرقى إلى سلاح محظور إذا لم يمكن تدارك مخاطره. في الحد الأدنى، طالبت

جماعات حقوقية بأن تقوم الشركات بواجب العناية الواجبة (Due Diligence) قبل إبرام عقود عسكرية – أي أن تقيم مخاطر حقوق الإنسان وأن تمتنع عن المشاركة إن وُجد خطر كبير بالمساهمة في الانتهاكات.

جدلية "حياد التكنولوجيا" في سياق الاحتلال

كثيرًا ما تتحجج الشركات التقنية بأن دورها محايد، فهي تبيع أدوات للعميل ولا تتدخل في كيفية الاستخدام. لكن سياق الاحتلال الإسرائيلي يضع هذا الادعاء على المحك. فحين توفر شركة ما بنية تحتية بياناتية وأدوات تحليل لمنظومة هدفها المعلن السيطرة على شعبٍ محتل – كما هو حال أنظمة إدارة السكان والحواجز البيومترية في فلسطين – فإن المنتج التقني يصبح جزءًا من هيكل القمع. تقول الباحثة القانونية مروة فطافطة: ***"التكنولوجيا ليست محايدة عندما تُستخدم لاستدامة مشروع استعماري"***. وفي حالة مشروع نيمبوس، ادعى متحدثو جوجل أن العقد لا يستهدف تطبيقات عسكرية مباشرة، لكن وجود بند يمنعهم من تقييد استخدام الجيش يجعل هذا الادعاء نظريًا. فعليًا، لا قيود تحول دون استخدام قدرات Nimbusفي مجالات التجسس أو الاستهداف إذا قررت الحكومة الإسرائيلية ذلك.

يجدر أيضًا النظر للموضوع من جهة الاحتلال الطويل الأمد: "إسرائيل" كقوة محتلة تخضع لقوانين دولية تمنعها من ممارسة عقوبات جماعية أو مراقبة شاملة جائرة ضد السكان الواقعين تحت احتلالها. وبالتالي، أي تقنية تساعدها في خرق تلك الواجبات (كالمراقبة الشاملة عبر كاميرات وتعرف وجوهAI ، أو الاستهداف القاتل السريع) لا يمكن اعتبارها "محايدة". هنا يأتي مفهوم "الاستعمار الرقمي" الذي أشار إليه بعض الباحثين – أي استخدام التكنولوجيا الحديثة لتعميق السيطرة الاستعمارية. شركات وادي السيليكون من هذا المنظور ليست جهات محايدة، بل هي امتداد غير رسمي لنفوذ القوى الكبرى (في هذه الحالة الولايات المتحدة) لدعم حليفها الاستراتيجي. هذا ما عبّر عنه مقال رأي في الجزيرة بأن الشركات الأمريكية "امتداد للإمبريالية الأمريكية eager لدعم فظائع إسرائيل."

في المقابل، يجادل آخرون بأنه لا ينبغي تحميل الأداة ذنب المستخدم؛ فالحاسوب السحابي نفسه يمكن استخدامه لإنقاذ أرواح (مثلاً بتحليل بيانات إنذار مبكر للصواريخ

لحماية المدنيين)، مثلما يمكن استخدامه لأذية أرواح. المنظور الأكثر واقعية ربما يكون المطالبة بشفافية ومسؤولية مشتركة: أي إلزام هذه الشركات بالتقصّي والمتابعة لكيفية استغلال تقنياتها في مناطق نزاع، ووضع شروط صارمة أو "فواصل آمنة" برمجية تمنع الاستخدامات غير القانونية (على غرار منع برمجيات التعرف على الوجه في انتهاك الخصوصية الجماعية أو منع استخدام خدمات الترجمة في الاستهداف دون تدقيق بشري إلزامي). حاليًا، هذه الأمور طوعية وتُركت لكل شركة على حدة - ومما رأيناه فإن اعتبارات الأرباح والمنافسة قد طغت على الاعتبارات الأخلاقية الذاتية.

خلاصة القول، مع دخول الذكاء الاصطناعي ميدان الحرب، تزحزحت معايير المسؤولية بشكل ينذر بفراغ خطير إن لم يُعالج. التقنية قد لا تكون جيدة أو شريرة في ذاتها، لكنها ليست منفصلة عن سياق استخدامها. وفي حالة غزة، كان السياق هو حصار طويل لشعب مُحتل وحرب طاحنة على منطقة كثيفة السكان - ما يعني أن أي مساهمة تقنية ***بدون ضوابط*** كانت على الأرجح تعين المعتدي أكثر مما تحمي الضحية. وهذا في جوهره موقف لا يمكن وصفه بالحياد.

ردود الأفعال ومقاومة المجتمعات التقنية

أفرز الدور العسكري للذكاء الاصطناعي في حرب غزة ردود أفعال قوية ومتعددة المستويات. ظهرت مقاومة من داخل شركات التكنولوجيا نفسها، ومن تحالفات العاملين، كما تحركت منظمات حقوقية دولية لفضح التعاون المشين بين وادي السيليكون والآلة العسكرية الإسرائيلية. فيما يلي نستعرض أهم مظاهر هذه المقاومة والنقد:

حركات موظفي التكنولوجيا المناهضة للحرب

شكّلت احتجاجات الموظفين داخل كبرى الشركات التقنية إحدى أبرز المفاجآت خلال الصراع. فللمرة الأولى ربما منذ حرب فيتنام، نشهد حراكًا ملموسًا لمهنيي التكنولوجيا ضد استخدام منتجاتهم في العنف:

- في Google وأمازون (حملة :(No Tech for Apartheid منذ الكشف عن مشروع Nimbus في 1442هـ (2021م)، انخرط مئات العاملين في الشركتين في حملة رافضة للتعاون مع نظام الفصل العنصري الإسرائيلي. تجددت هذه الحملة بزخم أكبر بعد حرب 1445هـ (2023م) على غزة، حيث وقع أكثر من 800 موظف من جوجل وأمازون على رسالة مفتوحة تطالب بإلغاء عقد نيمبوس ووقف أي دعم تكنولوجي ل"إسرائيل". قام الموظفون بنشاطات جريئة: من ضمنها احتجاجات صاخبة خلال اجتماعات المساهمين والمؤتمرات، ووقفات أمام مقار الشركة (مثل الوقفة أمام مكتب جوجل في سان فرانسيسكو في 1445هـ (ديسمبر 2023م)). وكشفت *TIME* أن أكثر من 200 موظف في جوجل انخرطوا بعمق في تنظيم هذه الجهود، وبعضهم قدم استقالته احتجاجًا. أحد مهندسي جوجل الشباب (إدي هاتفيليد) انتفض خلال مؤتمر تقني بهتاف" ***:أرفض بناء تقنية تُشغّل الإبادة الجماعية أو الأبارتهايد أو المراقبة*** "مرتديًا قميصًا كتب عليه شعار جوجل، فقوبل بصيحات استهجان من الحضور وتم طرده ولاحقًا فُصل من عمله. هذه الحوادث سلطت الضوء عالميًا على رفض شريحة من التقنيين الشباب تحويل مهاراتهم إلى أداة حرب.

- في) Microsoft مجموعة :(No Azure for Apartheid كما أوردنا آنفًا، تشكلت في مايكروسوفت نواة صلبة من الموظفين (حاليين وسابقين) رفعت شعار "لا لأزور للأبارتهايد"، قامت بنقاشات داخلية حامية على منتديات الشركة، ونظمت فعاليات احتجاجية (رالي 1446هـ (24 فبراير 2025م)، وفعلات الذكرى الخمسين في مارس-أبريل). هؤلاء العاملون - ومنهم مهندسون ومسؤولون تقنيون - خاطروا بوظائفهم في سبيل إيصال رسالة أخلاقية :***لا نريد أن نصبح موظفي حرب"، وشركتنا يجب أن تتوقف عن تمكين الجرائم بحق المدنيين*** " . وبالفعل فقد عدة منهم وظائفهم (إبتهاج أبوسعد، فانيا أغروال، حسام نصر، عبدو محمد وغيرهم) ولكنهم كسبوا تعاطفًا وتضامنًا واسعًا في مجتمع التقنية الأوسع.

- دور تحالفات أوسع :برزت كذلك منظمات مثل "Coalition Tech Workers" (تحالف عمال التقنية)، وإن كانت ظهرت أساسًا لمطالب عمالية عامة، فقد تبنت الكثير من مبادئ مناهضة التورط العسكري. كما ساعدت

مجموعات حقوق رقمية (مثل Access Now وحملة codepink التقنيـة (في تنظيم فعاليات دعم وإطلاق هاشتاغات تضامن مع الموظفين الشجعان الـذين جاهروا بموقفهم. هنا تجـدر الإشـارة إلـى أن هـذه الحركـات اسـتلهمت تجـارب سابقة ناجحة: في 1439هـ (2018م)، نجـح موظفـو جوجـل في دفـع الشـركة لإلغاء مشروع "مافن" مع البنتـاغون الخـاص باسـتخدام AI لتحليـل فيـديوهات الدرونز. تلك السابقة أعطـت العـاملين أملًـا بأنـه يمكـنهم التـأثير علـى قـرارات شركاتهم الأخلاقية. لكـن الفـارق في 1444-1445هـ (2023-2024م) أن الحـرب دائرة ومشاهد المجازر اليومية في غزة شحذت الضمائر سريعًا.

الدور الرقابي للمنظمات الحقوقية والدولية

لم تقف منظمات حقوق الإنسان مكتوفة الأيدي. عدد من المبـادرات والبيانـات سـعت لمساءلة التعاون التقني العسكري:

- تقارير الخبراء والمقررين الخاصين :دعـا مقـرر الأمـم المتحـدة المعنـي بحقـوق الإنسان في الأراضي المحتلة (وفرق أمميـة أخـرى) إلـى وقـف فـوري للهجمـات العشوائية على المدنيين في غزة وعبّروا عـن قلقهـم مـن الـدور الـذي تلعبـه التقنيات الحديثة في تضخيم قدرة إسرائيل التدميرية. ورغم أنهـم لـم يسـمّوا شركات بعينها، فإن إيحاءاتهم واضـحة بـأن أي طـرف يمـد المعتـدي بالقـدرات التقنية المتقدمة يجب أن يعيد النظر في ذلك فورًا.
- رسائل احتجاج من منظمات دولية :وجهت منظمة العفو الدوليـة (Amnesty) رسالة إلى شركات التقنيـة المعنيـة تـدعوها إلـى الإفصـاح الكامـل عـن نطـاق تعاونها مع جيش الاحـتلال الإسـرائيلي واتخـاذ خطـوات عاجلـة لضـمان عـدم مساهمة تقنياتها في جرائم حرب أو جرائم ضـد الإنسـانية. وأطلقـت منظمـة هيومن رايتس ووتش حملة موازيـة للضـغط مـن أجـل حظـر صـادرات تقنيـات المراقبـة لــ"إسـرائيل" بسـبب سـجلها في انتهـاك خصوصـية الفلسـطينيين واستخدام تلك الأدوات لتكريس الفصل العنصري.
- تحقيقات رقمية مستقلة :قام مختبر التحقيقات في منظمة 7) amlehحملـة الحقوق الرقمية الفلسطينية) بتوثيق سلسـلة انتهاكـات رقميـة أثنـاء الحـرب،

منها استخدام تقنية التعرف على الوجه لمسح وجوه جثامين الشهداء -كما نحسبهم- والمصابين على المعابر، الأمر الذي يطرح تساؤلات حول مصدر هذه التقنيات (حيث أن جوجل لديها خدمة Face Recognition عبر Google Photosمثلاً). مثل هذه التحقيقات حاولت وصل النقاط بين الضحية والأداة والشركة، لتكوين أدلة يمكن البناء عليها لمساءلة أخلاقية وربما قانونية مستقبلًا.

- حملات المقاطعة وسحب الاستثمارات (BDS) رقمية :على غرار حركة المقاطعة الاقتصادية، برزت دعوات لـ"مقاطعة رقمية" تستهدف خدمات سحابية معينة. فمثلاً اقترح نشطاء التوقف عن استخدام خدمات Amazon Web Servicesأو Azure وإلغاء الاشتراكات فيها كورقة ضغط تجارية. كما تم التواصل مع مستثمرين أخلاقيين لحثهم على إعادة النظر في حيازاتهم بأسهم تلك الشركات إذا لم تغير سياساتها. هذه الجهود لا تزال رمزية إلى حد كبير، لكنها مؤشر إلى أن سمعة الشركات باتت على المحك بما يكفي لتهديد مصالحها إن استمرت بالتجاهل.

فضح التعاون عبر الإعلام والتحقيقات الصحفية

كان للإعلام - الاستقصائي خاصة - دور محوري في كشف المستور وإجبار الشركات والحكومات على التبرير أو التصحيح:

- تقارير أسوشييتد برس الرائدة :حقق فريق صحفي من AP سبقًا صحفيًا بنشره في 1446هـ (مطلع 2025م) تحقيقًا شاملاً كشف لأول مرة أن نماذج ذكاء اصطناعي تجارية أمريكية OpenAI) عبر مايكروسوفت) استُخدمت فعليًا في ساحة الحرب. واستند التحقيق إلى مصادر داخل جيش الاحتلال الإسرائيلي ومايكروسوفت وغيرها، كاشفًا تفاصيل مذهلة عن الزيادة الهائلة في استخدام الخدمات التقنية بعد 7 أكتوبر، وعن كيفية اختيار الأهداف بواسطة AI واحتمالات الخطأ. وقد أجبر هذا الكشف غير المسبوق شركة مايكروسوفت على الرد - وإنكار الاستخدام المباشر في الاستهداف - لكنه شكل مرجعًا لكل النقاشات اللاحقة حول المسألة. أيضًا، قدمت AP منصة لخبراء مستقلين مثل

الدكتورة هايدي خلاّف للتعليق والتحذير من التداعيات، مما أعطى المصداقية العلمية للطرح الإعلامي.

- تحقيق Guardian/ +972 المسرب :بالاستفادة من وثائق سربتها منصة DropSite، نشرت Guardian بالتعاون مع +٩٧٢ Magazine تحقيقًا مدويًا بعنوان" ***مايكروسوفت عمّقت روابطها مع جيش الاحتلال الإسرائيلي خلال حرب غزة*** ." هذا التقرير فصّل الكثير مما ناقشناه بشأن ساعات الدعم ووجود Azureفي مختلف الوحدات، وأورد مسميات البرامج كـ "Rolling Stone" و "Ofek"وغيرها. كما عرض السياق التاريخي (خسارة مايكروسوفت لعقد نيمبوس ثم تعويضه بتعميق الشراكة). مثل هذه التفاصيل لم تكن معروفة قبلًا وفضحت كيف أن شركات التقنية مستعدة للتكيف سريعًا مع الطلب العسكري لضمان حصتها - أي منطق "لا مشكلة أني لم أربح العقد الرسمي، سأعوضه بتفاهمات خلفية."

- مجلة *Time* وواجهة التيار الرئيسي :دخول مجلة رصينة كـ TIMEعلى الخط عبر تقريرها الحصري عن تمرد موظفي جوجل أعطى المسألة زخمًا كبيرًا في الأوساط العامة. التقرير الذي صدر في 1446هـ (أبريل 2024م) كشف وجود أكثر من 200 موظف نشط في الاحتجاج داخل جوجل، وتحدث عن فصل الموظف المحتج وإقدام آخرين على الاستقالة، كما حصل على تعليق من جوجل وأمازون وإن كان تبريريًا. الأهمية هنا أن *Time* أوصلت القصة إلى جمهور أوسع خارج الفقاعة التقنية والحقوقية، مما زاد الضغط الشعبي على الشركتين. لاحقًا، استكملت *Time* والمتابعة الإعلامية سرد قصص الموظفين المفصولين في مقالات أخرى، مما شكل تعاطفًا عامًا مع قضيتهم ووضع الشركات في زاوية حرجة.

- دور *The Intercept* والجناح الإعلامي الناقد :مؤسسة مثل Intercept تبنّت نهجًا فضحيًا مباشرًا، فكشفت مثلًا سياسة مايكروسوفت لكتم أصوات موظفيها المؤيدين لفلسطين، ونشرت في 1445هـ (يناير 2024م) خبر تعديل OpenAI لقواعدها لصالح الاستخدام العسكري. كما سلطت الضوء على حالات مشابهة (مثل دعم شركة Meta عبر خبراء بيانات إسرائيليين لبرامج تجسس). هذه

المنصات وإن كانت ذات توجهات واضحة ناقدة للمؤسسة الأمريكية، إلا أنها دعمت الحجة بأن ما يجري ليس مجرد صدفة فردية، بل جزء من نمط ممنهج في صناعة التقنية الأمريكية لوضع الأرباح والجيوسياسة قبل حقوق الإنسان.

- الفارق بين الإعلام الغربي والتيار العربي الإسلامي :من المفيد هنا عقد مقارنة. الإعلام الغربي السائد (كبريات الشبكات التلفزيونية والصحف اليومية) تأخر نسبيًا في تناول هذا الموضوع وكان حذرًا في أحكامه، ربما تجنبًا لمواجهة مباشرة مع شركات ضخمة أو تفاديًا للظهور بمظهر "المتعاطف مع العدو" وسط أجواء اصطفاف مع "إسرائيل" في بعض الدول. في المقابل، الإعلام العربي والإسلامي – لا سيما المستقل – لم يتردد في الوصف الصريح. على سبيل المثال، نشرت ***الجزيرة*** مقالات رأي تصف ما يحدث بأنه "إبادة جماعية مدعومة بالذكاء الاصطناعي"، واتهمت شركات وادي السيليكون بدعم نظام الفصل العنصري رقميًا .***ميدل إيست آي*** البريطانية (ذات الصوت الموالي للقضايا العربية) وصفت استخدام إسرائيل للذكاء الاصطناعي في غزة بأنه "نموذج مرعب قد يتكرر عالمياً"، مشيرة إلى أن تل أبيب تستغل غزة كساحة لاختبار أحدث وسائل القتل والمراقبة بينما يراقب اليمين المتطرف العالمي ليتعلم. مثل هذا الطرح يندر ظهوره بتلك الصراحة في الإعلام الغربي السائد.

ومع ذلك، من الإنصاف القول إن صحافة التحقيق الغربية لعبت الدور الأبرز في الكشف التقني، بينما الإعلام العربي ركز على وضع هذه المعلومات في إطارها الإنساني والأخلاقي الأوسع. الاثنان معًا ساهما في تكوين صورة شبه متكاملة: صورة جيش الاحتلال الإسرائيلي الذي تحول إلى جيش عالي التقنية لا يتورع عن استخدامها بلا رحمة، وصورة الشركات الأمريكية التي إما تجاهلت أو بررت أو أخفت مشاركتها حتى انفضحت بالأدلة.

خاتمة وتوصيات

تكشف حالة حرب غزة وتحالف الذكاء الاصطناعي مع الآلة العسكرية "الإسرائيلية" عن مفترق طرق تاريخي. فنحن أمام اختبار حقيقي: هل ستصبح الحروب المقبلة أكثر فتكًا بسبب التقنية غير المنضبطة، أم أكثر إنسانية بضبط أخلاقيات استخدامها؟

في ضوء ما استعرضناه من حقائق وفضائح، تتضح الحاجة الملحة لخطوات وتوصيات على عدة مستويات لمجابهة عسكرة الذكاء الاصطناعي خاصة في الصراعات غير المتكافئة. فيما يلي بعض التوصيات الواقعية:

1. إطار دولي تنظيمي لتقنيات الذكاء الاصطناعي العسكرية :يجب على الأمم المتحدة والدول الأعضاء بدء العمل على معاهدة أو بروتوكول دولي يضع ضوابط لاستخدام الذكاء الاصطناعي في العمليات العسكرية، مشابهة للاتفاقيات الخاصة بالأسلحة التقليدية. ينبغي أن تشمل هذه الضوابط حظر أي استخدام ذاتي بالكامل قاتل للذكاء الاصطناعي (LAWs) بدون تحكم بشري، وإلزام الجيوش بضمان مراجعة بشرية واعية لأي هدف يرشحه .AI كما يجب أن تتضمن آليات تحقيق دولية في حال الاشتباه بأن قرارات خوارزمية أدت لجرائم حرب، مع إمكانية مساءلة القادة الذين اعتمدوا عليها دون حرص. لقد دعت اللجنة الدولية للصليب الأحمر بالفعل إلى مثل هذه التدابير، وحان الوقت لتحويل الدعوات إلى اتفاقيات ملزمة.

2. مدوّنات سلوك وتحفظات من قبل الشركات التقنية :تقع على عاتق شركات التكنولوجيا مسؤولية أخلاقية تجاه عدم التحول إلى مقاول حروب. لذا ينبغي أن تتبنى هذه الشركات مواثيق داخلية تمنع المشاركة في مشاريع من شأنها انتهاك حقوق الإنسان. يمكن الاسترشاد بالسابقة التي وضعتها جوجل عام 1439هـ (2018م) حين انسحبت من مشروع Maven العسكري تحت ضغط موظفيها. وعلى غرار ذلك، يمكن لمايكروسوفت وأمازون وغيرها إعلان سياسة "عدم تسليح الذكاء الاصطناعي"، بحيث ترفض عقودًا معينة أو تضيف شروطًا واضحة في العقود تمنع الاستخدامات العدوانية. وفي حالة الارتباط بعقود حكومية (كما في(Nimbus ، يمكنها فرض نطاق استخدام محدد تقنيًا – مثلاً تعطيل خدمات التصنيف أو التعرف البصري في بيئة السحابة المقدمة إذا كان ذلك ممكنًا، أو على الأقل توفير إشراف تقني لمنع إساءة الاستخدام. هذه الخطوات قد تبدو صعبة في ظل منافسة السوق، لكن الشركات التي تبادر إليها ستكسب ثقة الجمهور وتجنب نفسها ضرر السمعة (كما حدث لمايكروسوفت في فضيحتها.(

3. تعزيز شفافية التعاون بين شركات التقنية والجيوش :لا بد من كشف النقاب عن العقود العسكرية التقنية. يمكن للمشرّعين في الدول الديمقراطية الضغط لسنّ قوانين تُلزم شركات التقنية بالكشف الدوري عما تقدمه من خدمات أو منتجات للجيوش والجهات الأمنية (مع مراعاة الأمن القومي في تفاصيل حساسة محدودة). مثلًا، أن يُطلب من مايكروسوفت أو جوجل تقديم تقرير سنوي علني يحدد الدول والجهات الحكومية الأجنبية التي تستخدم منصاتها السحابية وأدواتAI ، ونوع الاستخدامات العامة المسموحة في تلك العقود. الشفافية هي الخطوة الأولى نحو المحاسبة. فلو لم تُسرّب وثائق Azureولم تحقق AP في الأمر، لبقيت مشاركة مايكروسوفت الخفية طي الكتمان. يجب ألا يتكرر ذلك.

4. تمكين ودعم حركات موظفي التقنية المناهضين للعسكرة :إحدى أقوى خطوط الدفاع ضد عسكرة AI هم المهندسون والعاملون أنفسهم. لذا، على الشركات أن تنشئ آليات استماع داخلية لمخاوف الموظفين بشأن أخلاقيات استخدام التقنية. بدلاً من فصل المحتجين أو إسكاتهم، ينبغي إشراكهم في حوارات وصياغة سياسات الشركة. يمكن مثلاً تشكيل لجنة أخلاقيات داخلية مستقلة تضم موظفين منتخبين وخبراء خارجيين، تراجع عقود الشركة المثيرة للجدل وتقدم توصيات. كما على المجتمع المدني والمنظمات دعم هؤلاء الموظفين – قانونيًا (في حالات الفصل التعسفي) ومعنويًا وإعلاميًا – لضمان استمرار قدرتهم على التأثير. إن حراك "No Tech for Apartheid" وأمثاله بحاجة إلى التضامن الدولي وربط شبكاته بين مختلف الشركات، ليشكلوا معًا جبهة عمال تقنية عالمية لأخلاقيات التكنولوجيا.

5. مراقبة دولية وحقوقية مستمرة للوضع في فلسطين :فيما يخص الاحتلال الإسرائيلي، ينبغي للمنظمات الدولية مواصلة تسليط الضوء على الدور التقني في إدامته. مثلاً، متابعة مشاريع مثل منظومة "الذئب الأزرق (Blue Wolf) " للتعرف على وجوه الفلسطينيين في الضفة الغربية، والتي طُورت بشراكة مع شركات خاصة. أو مشروع "بطاقة الهوية البيومترية" الذي تنفذه شركات مثل IBMالتتبع تحركات الفلسطينيين. كل هذه الممارسات يجب توثيقها وفضحها

وجعل التعاون التجاري فيها مكلفًا للشركات من منظور السمعة وربما المقاضاة مستقبلاً.

6. تعزيز قدرات الإعلام والتحقيقات في مجال التقنية العسكرية :كشفت هذه القضية أن الصحافة الاستقصائية التقنية بالغة الأهمية. لذا، يُوصى بدعم المؤسسات الإعلامية والمبادرات البحثية التي تركز على تقاطع التقنية وحقوق الإنسان (مثل مشروع *Citizen Lab* في كندا أو *Forensic Architecture*في بريطانيا)، فهذه الجهات قادرة على تتبع البرمجيات وتحليل الأدوات المستخدمة حتى لو حاولت الأطراف إخفاءها. كذلك تشجيع الشهود من الداخل (whistleblowers) على التقدم بمعلوماتهم تحت حماية القوانين، كما حصل مع مسرّبي وثائق مايكروسوفت. الشفافية تبدأ أحيانًا بفرد شجاع يكشف المستور.

7. إعمال مبدأ المحاسبة وعدم الإفلات من العقاب :في نهاية المطاف، لن يستقيم الأمر ما لم يشعر كل طرف – عسكري أو مدني – بأن قراراته تحمل عواقب. على مستوى الدول، يجب الدفع نحو مساءلة دولية للكيان المحتل على انتهاكاته بغزة، وإذا ثبت أن قرارات اعتماد أنظمة AI المغلوطة تسببت في قتل المدنيين، ينبغي أن يؤخذ ذلك في الحسبان كعامل مشدد. وعلى مستوى الشركات، يمكن للمساهمين ممارسة دورهم: رفع قضايا ضد مجالس الإدارة إن أخلّت بواجباتها الأخلاقية وتسببت في فضائح أضرت بقيمة الشركة. كما يمكن للمستهلكين تعديل سلوكهم الاستهلاكي (مثلاً البعض انتقل من خدمات جوجل السحابية إلى بدائل احتجاجًا على .(Nimbus هذه الممارسات تزيد تكلفة الانخراط غير الأخلاقي.

في الخلاصة، تعتبر حرب غزة 1445–1446هـ (2023–2024م) جرس إنذار عالمي حول خطورة المزج غير المنضبط بين الذكاء الاصطناعي والحرب. لقد رأينا كيف يمكن لتقنيات مصممة ظاهريًا لخدمة البشرية أن تُستخدم لإيقاع دمار هائل إذا وقعت في الأيدي الخطأ وبدون قيود. التوصيات أعلاه، إذا ما تم تبنيها، قد تشكل خطوة أولى لحماية المستقبل – مستقبل تُستخدم فيه قدرات الذكاء الاصطناعي لتعزيز السلام وحماية الأرواح، لا لتسريع القتل وإخفاء الجناة. إن مواجهة عسكرة الذكاء الاصطناعي

ليست مهمة التقنيين أو القانونيين وحدهم، بل هي واجب إنساني جماعي لضمان أن تظل التكنولوجيا أداة لرفع راية الإنسانية، لا لابتكار طرق جديدة لإبادة بعضها البعض.

المصادر:

تمت كتابة هذه الدراسة بالاستناد إلى تقارير صحفية موثوقة وتحقيقات استقصائية وأوراق بحثية. للاطلاع التفصيلي، يمكن مراجعة تقرير أسوشييتد برس، وتحقيق الجارديان، ومقال تايم، وغيرها من المراجع المثبتة في متن النص أعلاه. جميع الاقتباسات موثقة لضمان المصداقية