



حماية المعلومات في عصر الذكاء الاصطناعي

بقلم

بختيار أحمد صالح

باحث في مركز حمورابي للبحوث والدراسات الاستراتيجية



تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزاً علمياً بحثياً يهتم بدراسة الموضوعات السياسية والاجتماعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

- لا يجوز إعادة نشر أي من هذه الأوراق البحثية إلا بموافقة المركز، وبالإمكان الاقتباس بشرط ذكر المصدر كاملاً.
- لا تعبر الآراء الواردة في الورقة البحثية عن الاتجاهات التي يتبناها المركز وإنما تعبر عن رأي كاتبها.
- حقوق الطبع والنشر محفوظة لمركز حمورابي للبحوث والدراسات الاستراتيجية.

للتواصل

مركز حمورابي

للبحوث والدراسات الاستراتيجية

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net



مقدمة

أدى ظهور الذكاء الاصطناعي إلى إحداث تحول جوهري في المفهوم التقليدي لحماية المعلومات. ففي النموذج الكلاسيكي لأمن المعلومات، كان التركيز الأساسي ينصب على حماية البيانات والوثائق الحساسة، وضبط الوصول إليها، ومنع تسرب المعلومات، وتقييد وصول الجهات غير المصرح لها إلى مصادر المعلومات. إلا أن انتشار أنظمة الذكاء الاصطناعي والتعلم الآلي وتحليل البيانات الضخمة والمعالجة الآلية، نقل البيئة المعلوماتية إلى مرحلة أصبح فيها حتى البيانات التي تبدو محدودة الأهمية قابلة للتحول، من خلال الربط والتحليل، إلى معلومات ذات قيمة أمنية.

وقد أبرزت حرب الأيام الاثني عشر بين الجمهورية الإسلامية في إيران و"إسرائيل" في حزيران 2025، والحرب التي استمرت أربعين يوماً بين الجمهورية الإسلامية في إيران والولايات المتحدة و"إسرائيل" في شباط - نيسان 2026، أهمية هذا التحول. فقد ظهرت تقارير مختلفة حول الجمع بين العمليات الاستخبارية والاختراق وجمع البيانات واستخدام التقنيات المتقدمة في تحديد الأهداف وترتيب أولوياتها. كما أظهرت التقارير المتعلقة بالحرب الأربعينية أن حجم الأهداف والبيانات العملية التي جرى التعامل معها خلال فترة زمنية قصيرة أصبح كبيراً للغاية.

في مثل هذه البيئة، لم تعد القضية الأساسية في حماية المعلومات تقتصر على السؤال ما البيانات السرية؟ بل أصبح السؤال الأهم هو ما المعلومات التي يمكن استنتاجها من مجموعة البيانات المتاحة؟

تجادل هذه الورقة بأن نظام حماية المعلومات في عصر الذكاء الاصطناعي ينبغي أن يقوم على ثلاثة مستويات مترابطة: حماية البيانات، وحماية العلاقات بين البيانات، وحماية الاستدلال. وفي هذا الإطار تكتسب فكرة الحوكمة الخوارزمية للبيانات أهمية متزايدة، لأن التفوق المعلوماتي لم يعد يعتمد فقط على حجم البيانات المتاحة، وإنما أيضاً على قدرة الفاعل على تحويل البيانات إلى معلومات، والمعلومات إلى معرفة، والمعرفة إلى قرار.

أدت التطورات التكنولوجية خلال العقود الأخيرة إلى تغيير طبيعة المعلومات وأمنها. ففي الماضي، كانت المؤسسات تتعامل بصورة أساسية مع الوثائق والتقارير والرسائل والصور والبيانات التي كانت قيمتها المعلوماتية قابلة للتحديد إلى حد كبير مسبقاً.

فالوثيقة السرية، أو التقرير العملي، أو الاتصال المشفر، كان يُنظر إليه باعتباره ذا قيمة معلوماتية بسبب محتواه المباشر. لكن العصر الرقمي غير هذه المعادلة. فالיום يتم إنتاج البيانات على نطاق أوسع بكثير. فالهواتف المحمولة، وأنظمة الاتصالات، وشبكات التواصل الاجتماعي، وصور الأقمار الصناعية، وأنظمة النقل، والمعاملات المالية، والأنظمة الإدارية، وآلاف المصادر الأخرى، تنتج البيانات بصورة مستمرة. وجزء كبير من هذه البيانات لا يكون حساساً بحد ذاته. لكن المشكلة تبدأ عندما يتمكن أحد الفاعلين من ربط هذه البيانات ببعضها. وهنا تبرز أهمية الذكاء الاصطناعي.

فقد يعجز الإنسان عن اكتشاف العلاقة بين آلاف البيانات المتفرقة، بينما يستطيع النظام الخوارزمي تصنيف كميات ضخمة من البيانات ومقارنتها خلال فترة زمنية قصيرة، واكتشاف أنماط متكررة أو علاقات خفية. وبالتالي، لم تعد القيمة الأمنية للبيانات مرتبطة فقط بمحتواها المباشر، وإنما أصبحت مرتبطة أيضاً بقابليتها لإنتاج معلومات جديدة عند دمجها مع بيانات أخرى.

مشكلة البحث

يمكن صياغة المشكلة الأساسية لهذه الورقة في السؤال التالي: هل ما زال نظام حماية المعلومات التقليدي، الذي يركز بصورة أساسية على منع الوصول غير المصرح به إلى البيانات الحساسة، كافياً في مواجهة القدرات الاستدلالية للذكاء الاصطناعي؟

تنطلق الورقة من فرضية أساسية مفادها أن الإجابة هي: لا. فالنظام التقليدي لحماية المعلومات لا يزال ضرورياً، لكنه لم يعد كافياً في بيئة الذكاء الاصطناعي. ذلك أن جهة ما قد تتمكن، من دون الوصول المباشر إلى وثيقة سرية، من استخدام مجموعة من البيانات المتفرقة وإجراء تحليل خوارزمي لها للوصول إلى أجزاء مهمة من تلك المعلومات. وبالتالي أصبحت الحدود بين البيانات العامة والبيانات غير الحساسة والمعلومات الحساسة أكثر مرونة وتعقيداً.

تطور مفهوم المعلومات

لفهم هذا التحول، ينبغي التمييز بين أربعة مفاهيم رئيسية:

1. البيانات: البيانات هي الحقائق الخام قبل معالجتها ومن أمثلتها وقت وقوع حدث معين، موقع جغرافي، صورة، اتصال، معاملة مالية، حركة معينة، أو تغير في سلوك مؤسسة. وقد تكون لكل واحدة من هذه العناصر أهمية محدودة إذا نظر إليها بصورة منفردة.
2. المعلومات: عندما توضع البيانات في سياق محدد وتكتسب معنى، فإنها تتحول إلى معلومات.
3. المعرفة: عندما يتم جمع معلومات متعددة معاً، وتحديد الأنماط والعلاقات بينها، يتشكل مستوى جديد من المعرفة.
4. القرار: يمكن أن تصبح المعرفة في النهاية أساساً لاتخاذ القرار. وبذلك يمكن تمثيل السلسلة على النحو التالي: البيانات، المعلومات، المعرفة، الإدراك، القرار. وتكمن أهمية الذكاء الاصطناعي في هذه السلسلة في قدرته على زيادة سرعة وحجم الانتقال من المرحلة الأولى إلى المراحل اللاحقة.

لماذا يغير الذكاء الاصطناعي معادلة حماية المعلومات؟

يمتلك الذكاء الاصطناعي ثلاث خصائص ذات أهمية خاصة بالنسبة إلى الأنظمة المعلوماتية:

أولاً: الحجم: لا يستطيع الإنسان تحليل كمية غير محدودة من البيانات في الوقت نفسه، في حين تستطيع الأنظمة

الحاسوبية معالجة كميات هائلة من البيانات.

ثانياً: السرعة: يمكن تنفيذ عمليات تحليل كانت تتطلب في الماضي أعداداً كبيرة من المحللين ووقتاً طويلاً خلال فترات أقصر بكثير.

ثالثاً: اكتشاف الأنماط: وهذه هي الخاصية الأكثر أهمية بالنسبة إلى حماية المعلومات، لأنها تسمح باكتشاف العلاقات والأنماط التي لا تكون ظاهرة بصورة مباشرة.

وقد ركزت وزارة الدفاع الأمريكية منذ سنوات على هذه المسألة. فعلى سبيل المثال، تم تطوير مشروع Project Maven بهدف المساعدة في تحليل كميات كبيرة من البيانات المرئية والفيديوية، وأكدت وزارة الدفاع الأمريكية في وصف المشروع أهمية استخدام الذكاء الاصطناعي والتعلم الآلي في التعامل مع الحجم المتزايد للبيانات. ومن هنا فإن الذكاء الاصطناعي في مجال المعلومات ليس مجرد قضية تقنية، بل أصبح مرتبطاً مباشرة بالقدرة المعرفية للمؤسسات الأمنية.

تجربة حرب الأيام الاثني عشر: أهمية دمج البيانات والعمليات الاستخبارية

تمثل الحرب التي اندلعت بين الجمهورية الإسلامية في إيران و"إسرائيل" في حزيران 2025، والتي عُرفت بحرب الأيام الاثني عشر، حالة مهمة لدراسة هذا التحول. وتشير التقارير المنشورة حول هذه الحرب إلى أن العمليات العسكرية لم تعتمد فقط على القوة النارية، وإنما شملت أيضاً العمليات الاستخبارية والاختراق والطائرات المسيّرة وجمع البيانات والاستطلاع وتحديد الأهداف. كما ظهرت تقارير حول نشاط عناصر "إسرائيلية" داخل الجمهورية الإسلامية في إيران، واستخدام وسائل وتقنيات مختلفة لبناء قدرات أكثر دقة في مجال استهداف الأهداف. وتبرز هنا نقطة مهمة القوة الاستخبارية لا تعني بالضرورة امتلاك سر كبير. فقد تشكل القوة المعلوماتية من خلال تجميع مئات أو آلاف المؤشرات الصغيرة. وفي مثل هذه الظروف، لا يكفي حماية كل معلومة بصورة منفردة. بل ينبغي طرح السؤال التالي: إذا جُمعت جميع البيانات المتفرقة معاً، فما الصورة التي يمكن أن تنتج عنها؟

الحرب الأربعينية ومشكلة حجم معالجة المعلومات

أظهرت الحرب التي استمرت أربعين يوماً في عام 2026، والتي بدأت في 28 شباط وانتهت بهدنة في 8 نيسان، بيئة معلوماتية على نطاق أكبر. وتشير تقارير الرصد المتعلقة بالحرب إلى حجم كبير جداً من الأضرار والأهداف والعمليات العسكرية خلال فترة زمنية قصيرة وبغض النظر عن الاختلاف بين المصادر في تقدير أعداد الأهداف أو تقييم النتائج، فإن هناك حقيقة أساسية يمكن ملاحظتها: لقد أصبح حجم البيانات في الحرب الحديثة كبيراً إلى درجة تجعل المعالجة البشرية وحدها غير قادرة على تلبية جميع الاحتياجات المعلوماتية. وبالتالي أصبحت القدرة على جمع البيانات ومعالجتها وربطها وتحليلها جزءاً من القوة العسكرية والأمنية.

من حماية البيانات إلى حماية الاستدلال

في النظام التقليدي حماية المعلومات تساوي منع تسرب المعلومات الحساسة، أما في عصر الذكاء الاصطناعي، فينبغي تقديم تعريف أوسع، حماية المعلومات تساوي منع الوصول غير المصرح به بالإضافة الى منع إنتاج معلومات حساسة بصورة غير مشروعة من البيانات المتفرقة. وهنا يبرز مفهوم الاستدلال. الاستدلال يعني الوصول إلى نتيجة جديدة اعتماداً على بيانات قد لا تكون حساسة بحد ذاتها. فعلى سبيل المثال:

1. البيانات A ليست حساسة بصورة منفردة.

2. البيانات B ليست حساسة أيضاً.

3. البيانات C كذلك.

لكن الجمع بين $A+B+C$ يمكن أن ينتج نمطاً ذا أهمية كبيرة.

ومن هنا: الحساسية ليست بالضرورة صفة للبيانات وحدها؛ بل قد تكون أيضاً صفة للعلاقة بين البيانات. وهذه إحدى أهم تحديات حماية المعلومات في عصر الذكاء الاصطناعي.

مفهوم حماية الاستدلال

يمكن تعريف حماية الاستدلال بأنها مجموعة السياسات والإجراءات والآليات الأمنية الهادفة إلى تحديد وتقليل إمكانية استخراج معلومات حساسة من خلال دمج البيانات المتفرقة، حتى عندما لا تكون كل واحدة من تلك البيانات حساسة بصورة منفردة. ويتضمن هذا المفهوم عدة مراحل:

المرحلة الأولى تحديد البيانات: يجب على المؤسسة أن تعرف ما البيانات التي تنتجها.

المرحلة الثانية تحديد العلاقات: يجب تحديد البيانات التي يمكن ربطها ببعضها.

المرحلة الثالثة تحديد الأنماط القابلة للاستخراج: ينبغي دراسة الأنماط التي يمكن إنتاجها من خلال دمج البيانات.

المرحلة الرابعة تقييم التهديد: ينبغي طرح السؤال: ماذا يمكن لفاعل يمتلك أدوات تحليل متقدمة أن يستنتج من هذه الأنماط؟

المرحلة الخامسة تقليل قابلية الاستدلال: عند وجود خطر، ينبغي إدارة مستوى الوصول إلى البيانات أو نشرها أو تجميعها.

الحوكمة الخوارزمية للبيانات

في الماضي كان السؤال الرئيسي من يستطيع الوصول إلى البيانات؟ أما اليوم فينبغي طرح سؤال ثانٍ من يمتلك قدرة أكبر على تحليل البيانات؟ قد يمتلك فاعلان اثنان إمكانية الوصول إلى مجموعة البيانات نفسها، ولكنهما قد يتوصلان إلى نتائج مختلفة تماماً. فقد يرى الفاعل الأول مجموعة من الجداول والتقارير فقط. بينما يستطيع الفاعل الثاني دمج البيانات نفسها مع صور الأقمار الصناعية والمعلومات المكانية والزمنية وبيانات الاتصالات والمصادر المفتوحة، ثم إنتاج صورة أكثر شمولاً. وبالتالي فإن القوة المعلوماتية لا تعتمد فقط على الوصول

إلى البيانات، وإنما تعتمد أيضاً على القدرة على المعالجة والاستدلال. ومن هذا المنظور، فإن الحوكمة الخوارزمية للبيانات تعني الاهتمام بثلاثة عناصر بصورة متزامنة: البيانات، الخوارزمية، والقدرة على الاستدلال.

أمن المعلومات في مواجهة البيانات التي تبدو غير مهمة

من المخاطر المهمة في عصر الذكاء الاصطناعي التقليل من أهمية البيانات الصغيرة. في ثقافة حماية المعلومات التقليدية، قد يتركز الاهتمام على الوثيقة السرية. لكن في البيئة الجديدة، يمكن لصورة عامة، أو توقيت معين، أو تغير صغير في نشاط مؤسسة، أو معلومة مكانية، أن تكتسب قيمة كبيرة عند دمجها مع بيانات أخرى. وبالتالي ينبغي التعامل بحذر مع مفهوم البيانات غير المهمة. فقد تبدو بيانات معينة غير مهمة اليوم، لكنها قد تكتسب قيمة معلوماتية غداً عندما ترتبط ببيانات جديدة. ويمكن تسمية هذه الخاصية القيمة الزمنية للبيانات. وعليه، لا ينبغي أن تكون عملية تصنيف البيانات ثابتة بصورة مطلقة.

التحديات الرئيسية لحماية المعلومات في عصر الذكاء الاصطناعي

1. تجميع البيانات: يمكن جمع البيانات المتفرقة من مصادر متعددة في بيئة تحليل واحدة.
2. التحليل المتقاطع: يمكن دمج البيانات القادمة من مجالات مختلفة.
3. التحليل الزمني: يمكن أن يؤدي تكرار سلوك معين على مدى فترة زمنية إلى الكشف عن نمط قابل للتحديد.
4. التحليل المكاني: يمكن أن يكشف دمج البيانات المكانية عن علاقات لا تظهر في البيانات الفردية.
5. تحليل الشبكات: يمكن إعادة بناء العلاقات بين الأفراد والمؤسسات والأحداث من خلال تحليل الشبكات.
6. التحليل السلوكي: يمكن للخوارزميات تحديد التغيرات في السلوك.
7. البيانات العامة: يمكن للمعلومات العامة نفسها أن تكتسب قيمة استخباراتية عندما يتم تجميعها وتحليلها.

المعلومات مفتوحة المصدر ونهاية الحدود التقليدية بين السري والعام

من أهم التحولات في العصر الرقمي ازدياد قيمة المعلومات مفتوحة المصدر، فالمعلومات المنشورة على الإنترنت أو شبكات التواصل الاجتماعي أو صور الأقمار الصناعية أو المصادر العامة قد تكون محدودة الأهمية إذا نُظر إليها بصورة منفردة. لكن دمجها يمكن أن يؤدي إلى إنتاج معلومات جديدة. ولهذا السبب، لم يعد بإمكان حماية المعلومات أن تقتصر على البيانات المصنفة. ينبغي للمؤسسة أن تعرف ما الصورة التي يمكن إعادة بنائها عن نشاطاتها باستخدام المصادر العامة فقط؟ وينبغي أن يصبح هذا السؤال جزءاً ثابتاً من عمليات التقييم الأمني.

الذكاء الاصطناعي وخفض تكلفة التحليل

من أهم التحولات التي أحدثها الذكاء الاصطناعي خفض تكلفة التحليل. في الماضي، كان تحليل آلاف الوثائق أو الصور أو الاتصالات يحتاج إلى عدد كبير من المحللين. أما اليوم، فيمكن للخوارزميات تنفيذ جزء كبير من مراحل المعالجة الأولية. وقد أكد المعهد الوطني للمعايير والتكنولوجيا الأمريكي (NIST) في إطار إدارة مخاطر الذكاء الاصطناعي ضرورة الإدارة المستمرة للمخاطر طوال دورة حياة أنظمة الذكاء الاصطناعي، واقترح أربعة وظائف رئيسية هي الحوكمة، التحديد، القياس، والإدارة.

النموذج المقترح لحماية المعلومات في عصر الذكاء الاصطناعي

استناداً إلى ما سبق، يمكن اقتراح نموذج مكون من خمس طبقات:

الطبقة الأولى حماية البيانات: وتشمل التحكم في الوصول، التشفير، التصنيف، المصادقة، الحماية المادية والرقمية.

الطبقة الثانية حماية العلاقات بين البيانات: دراسة البيانات التي يمكن ربطها ببعضها.

الطبقة الثالثة حماية الأنماط: تحديد الأنماط التي يمكن استخراجها من مجموعات البيانات.

الطبقة الرابعة حماية الاستدلال: تقييم ما يمكن لفاعل خارجي أن يستنتجه من البيانات المتاحة.

الطبقة الخامسة حماية القرار: دراسة كيفية تأثير المعلومات المستخرجة في عملية اتخاذ القرار.

ضرورة التدقيق الاستدلالي من المقترحات الرئيسية لهذه الورقة إنشاء عملية يمكن تسميتها التدقيق الاستدلالي. في التدقيق التقليدي يكون السؤال هل تم تسريب معلومات سرية؟ أما في التدقيق الاستدلالي فيصبح السؤال إذا تمكن فاعل خارجي من الوصول إلى جميع البيانات المتاحة، فما المعلومات التي يستطيع استخراجها منها؟ وينبغي أن تتم هذه العملية بصورة دورية. ويمكن أن تشمل تحديد البيانات المتاحة، تصنيف المصادر، دراسة العلاقات بين البيانات، تحديد الأنماط القابلة للاستخراج، تقييم القيمة الأمنية للأنماط، تحديد نقاط الضعف، تعديل سياسات النشر والوصول.

ضرورة تغيير ثقافة أمن المعلومات

في الماضي، كان من الممكن أن يتركز تدريب العاملين في مجال حماية المعلومات حول قاعدة بسيطة لا تفش المعلومات السرية. لكن في عصر الذكاء الاصطناعي ينبغي أن يتجاوز التدريب هذه القاعدة اعلم أن المعلومات غير السرية نفسها قد تنتج معلومات حساسة عند دمجها مع معلومات أخرى. وهذا التحول الثقافي مهم للغاية. فالموظف والمدير والمحلل ومستخدم النظام المعلوماتي يجب أن يفهموا مفهوم البصمة الرقمية للبيانات. فالمشكلة لم تعد تقتصر على نشر وثيقة، بل يمكن أيضاً أن يكون إنتاج نمط قابل للتحليل بصورة غير مقصودة ذا أهمية أمنية.

التداعيات التنظيمية

يتطلب هذا التحول تغييراً في البنية التنظيمية أيضاً. ففي المؤسسة الحديثة، لا ينبغي أن تكون مسؤولية حماية المعلومات محصورة في إدارة الأمن أو تكنولوجيا المعلومات. بل ينبغي أن يكون هناك تنسيق بين أمن المعلومات، الأمن السيبراني، تحليل البيانات، إدارة المخاطر، الذكاء الاصطناعي، الموارد البشرية، إدارة الاتصالات، والإدارة العليا. كما يؤكد NIST أن إدارة مخاطر الذكاء الاصطناعي ينبغي أن تكون جزءاً من الحوكمة التنظيمية ودورة حياة الأنظمة، وليس مجرد إجراء تقني محدود.

الخوارزمية بوصفها مكوناً من مكونات الأمن القومي

في الماضي كان الأمن القومي يركز بصورة رئيسية على ثلاثة مصادر للقوة الإنسان، والمعدات، والمعلومات. أما اليوم فينبغي إضافة عنصر رابع، الخوارزمية. فالخوارزمية يمكن أن تحدد، من بين ملايين البيانات، أيها أكثر أهمية، وما العلاقات القائمة بينها، وما الأنماط التي ينبغي أن تحظى باهتمام المحلل. وبالتالي فإن المنافسة المستقبلية لن تكون فقط على جمع المعلومات، وإنما أيضاً على القدرة على تحويل البيانات إلى معرفة. وهنا ينتقل الذكاء الاصطناعي من كونه أداة تقنية إلى كونه مكوناً من مكونات الأمن القومي.

حدود ومخاطر الاعتماد المفرط على الذكاء الاصطناعي

على الرغم من أهمية الذكاء الاصطناعي، فإنه لا ينبغي اعتباره بديلاً كاملاً عن التحليل البشري. فأنظمة الذكاء الاصطناعي يمكن أن تخطئ، تعمل على بيانات ناقصة، تنتج علاقات زائفة، تتضمن تحيزات، أو تحدد أنماطاً لا تحمل معنى حقيقياً من الناحية الإنسانية أو العملية. كما يشدد NIST على مجموعة من المخاطر المتعلقة بالأمن والخصوصية والموثوقية وقابلية التفسير وغيرها من خصائص الثقة في أنظمة الذكاء الاصطناعي. لذلك فإن الحل لا يكمن في الإنسان من دون الذكاء الاصطناعي ولا في الذكاء الاصطناعي من دون الإنسان. بل في الإنسان، الخوارزمية، وآلية تقييم مستقلة بوصفها أساساً لنظام التحليل المعلوماتي الحديث.

التوصيات والسياسات المقترحة

استناداً إلى الإطار السابق، يمكن تقديم عدد من التوصيات العامة:

1. إعادة تعريف مفهوم المعلومات الحساسة: ينبغي ألا تكون الحساسية خاصة للبيانات الفردية فقط، بل يجب تقييم إمكانية إنتاج معلومات حساسة من خلال دمج البيانات.
2. إنشاء وحدة لتقييم الاستدلال: يمكن للمؤسسات الحساسة إنشاء قدرة تخصصية لدراسة قابلية البيانات للاستدلال.
3. تنفيذ عمليات تدقيق استدلال: ينبغي إجراء تقييم دوري لما يمكن استخراجه من البيانات المتاحة.
4. إنشاء قاعدة للأنماط الأمنية: ينبغي تحديد الأنماط الحساسة للمؤسسة ووضع آليات لحمايتها.

5. دمج أمن البيانات والذكاء الاصطناعي: ينبغي أن تعمل إدارات أمن المعلومات بصورة وثيقة مع متخصصي البيانات والذكاء الاصطناعي.
6. إعادة النظر في تدريب العاملين: ينبغي أن ينتقل التدريب من مفهوم عدم إفشاء المعلومات السرية إلى فهم قابلية البيانات للاستدلال.
7. التقييم المستمر للمصادر العامة: ينبغي أن تعرف المؤسسة ما الصورة التي يمكن إعادة بنائها عن نشاطاتها من خلال المصادر العامة.
8. إنشاء آلية للرقابة البشرية: ينبغي ألا تدخل النتائج الخوارزمية في القرارات الحساسة دون تقييم بشري.

خاتمة

لقد غير الذكاء الاصطناعي المفهوم التقليدي لحماية المعلومات. ففي الماضي كانت حماية المعلومات تعني بصورة أساسية منع الخصم من الوصول إلى المعلومات الحساسة. أما اليوم فلم يعد هذا التعريف كافياً. فقد يتمكن أحد الفاعلين، من دون الوصول المباشر إلى وثيقة سرية، من خلال جمع البيانات المتفرقة وتحليلها خوارزمية، من إعادة بناء جزء مهم من تلك المعلومات. وعليه ينبغي النظر إلى مستقبل حماية المعلومات من خلال ثلاثة مستويات: أولاً: حماية البيانات.

ثانياً: حماية العلاقات والأنماط بين البيانات.

ثالثاً: حماية الاستدلال.

ويمثل هذا التحول أيضاً تغييراً في فلسفة الأمن المعلوماتي. فالسؤال التقليدي كان ما الذي ينبغي أن نخفيه؟ أما السؤال الجديد فهو ماذا يستطيع الآخرون أن يفهموا مما يرونه؟ وهذا الاختلاف، رغم بساطته الظاهرية، يمثل تحولاً عميقاً في مفهوم حماية المعلومات. ففي عصر الذكاء الاصطناعي، لم تعد المعلومات مجرد شيء تنتجه المؤسسة وتخزنه، بل يمكن أن تكون شيئاً ينتجه الآخرون من الآثار والبيانات التي تتركها المؤسسة وراءها. ومن هنا، ينبغي أن يتضمن نظام حماية المعلومات في المستقبل، إلى جانب التحكم في البيانات، القدرة على تحديد الأنماط القابلة للاستخراج، وتقييم القدرات الخوارزمية للجهات المقابلة، وإدارة مخاطر الاستدلال.

وبصياغة مختصرة: في عصر الذكاء الاصطناعي، لم تعد حماية المعلومات تعني فقط حماية ما تعرفه المؤسسة؛ بل حماية ما يستطيع الآخرون معرفته من بيانات المؤسسة. وربما يمثل هذا التحول أهم تغيير في فلسفة حماية المعلومات في البيئة الأمنية الجديدة.