ملتقى أسبار

إحدى مبادرات مركز أسبار

تقرير رقم (112)

سبتمبر 2023

ضوابط وقوانين استخدام المعلومات الخاصة في أنظمة الذكاء الاصطناعي

لجنة شؤون التحول الرقمي

بسم الله الرحمن الرحيم

تقرير يصدر عن ملتقى أسبار

- رئيس الملتقى:
  د. فهد العرابي الحارثي
- رئيس الهيئة الإشرافية للملتقى:
  د. محمد المعجل
- **أ. لاحم الناصر:** الأمين العام
  أ. علاء برادة - مساعد الأمين العام
  د. سكينة الشيخ - مساعد الأمين العام
- **التحرير:**
  د. إبراهيم إسماعيل عبده
- **التصميم والإخراج:**
  أ. صفوان يحيى مسعد

- **لجنة شؤون التحول الرقمي**
- د . علي الوهيبي **(رئيس اللجنة)**
- د. حسين الجحدلي **(نائب رئيس اللجنة)**
- **أعضاء اللجنة:**
- د.حامد الشراري
- د. رجا المرزوقي
- د. رياض نجم
- د. عبدالرحمن العريني
- د.عبدالعزيز الباتلي
- د. عبدالعزيز الحرقان
- د. عبدالعزيز السدحان

- ترتيب الأسماء حسب الحروف الأبجدية

تمهيد

يعرض هذا التقرير لقضية مهمة تمَّ طرحها للحوار في ملتقى أسبار خلال شهر سبتمبر 2023م، وناقشها نُخبة متميزة من مفكري المملكة في مختلف المجالات، والذين أثروا الحوار بآرائهم البنَّاءة ومقترحاتهم الهادفة؛ حيث تناولت: ضوابط وقوانين استخدام المعلومات الخاصة في أنظمة الذكاء الاصطناعي، وأعد ورقتها الرئيسة د. عبدالعزيز الحرقان، وعقب عليها كلًا من د. عبدالعزيز الباتلي، د. علي الوهيبي وأدار الحوار حولها د. علي الوهيبي.

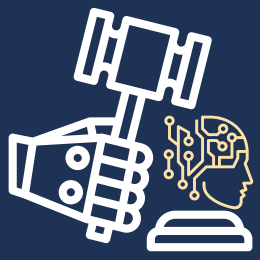
المحتويات

ضوابط وقوانين استخدام المعلومات الخاصة في أنظمة الذكاء الاصطناعي

الملخص التنفيذي:

يتناول هذا التقرير قضية "ضوابط وقوانين استخدام المعلومات الخاصة في أنظمة الذكاء الاصطناعي". وأشار د. عبدالعزيز الحرقان في الورقة الرئيسة إلى أن

الضوابط والقوانين المتعلقة باستخدام المعلومات الحساسة في أنظمة الذكاء الاصطناعي تختلف من بلد إلى آخر ولكن بشكل عام، تتطلب هذه المعلومات مستوى أعلى من الحماية والخصوية وفقاً للقوانين الوطنية والدولية.



ويتم تحديد الضوابط والقوانين المتعلقة باستخدام المعلومات الحساسة في أنظمة الذكاء الاصطناعي بناء على تصنيف هذه المعلومات ومدى حساسيتها، ويتم تحديد مستوى الحماية والخصوصية اللازمة وفقاً لذلك. ويجب أن توفر أنظمة الذكاء الاصطناعي الحماية اللازمة للمعلومات الحساسة، ويجب أن تتبع أفضل الممارسات في مجال الأمن والخصوصية، بما في ذلك تشفير المعلومات وتحديد مستوى الوصول إليها وإدارة الهوية والوصول.

بينما أكَّد د. عبدالعزيز الباتلي في التعقيب الأول على أن الذكاء الاصطناعي يعكس تحولًا ثوريًا في عالم التكنولوجيا، وهو يشكل تحديًا وفرصة لنا جميعًا، سواء كنا مجتمعًا أو دولة، للاستعداد والتكيف مع هذا التطور الرائع. ومن المهم

أن ندرك أن الذكاء الاصطناعي ليس مجرد أداة لتقليل واستبدال الوظائف، بل هو نموذج جديد للتفكير والاقتصاد.

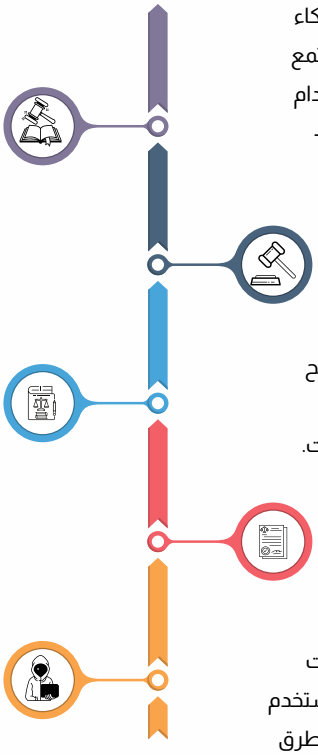
ويمكن للذكاء الاصطناعي أن يؤثر بشكل كبير في الاقتصاد بطرق عديدة ومتنوعة، وذلك من خلال تحسين الإنتاجية، وتوفير الوقت والتكاليف، وخلق فرص جديدة للأعمال، وتحسين تجربة المستخدمين، ودعم اتخاذ القرارات الاستراتيجية والاستشراف.

في حين ذكر د. علي الوهيبي في التعقيب الثاني أن العقد الأخير شهد اقبالًا عالمياً مضطرد على تقنيات الذكاء الاصطناعي من قبل الحكومات وقطاعات الأعمال المتوسطة والصغيرة، وعلى الرغم من ما تقدمه تلك التقنيات من خدمات ومنتجات سهلت حياة الناس، إلا أنها لا تخلو من العديد من السلبيات ومن أبرزها إمكانية انتهاك البيانات الخاصة أو الشخصية. وقد ساعدت جهود المملكة من خلال الهيئة الوطنية للبيانات والذكاء الاصطناعي في وضع البنية التحتية لاستخدام أنظمة الذكاء الاصطناعي وسن التشريعات والقوانين المرتبطة باستخدام البيانات ومشاركتها ومتابعة الامتثال لتلك التشريعات.

وتضمنت المداخلات حول القضية المحاور التالية:

ومن أبرز التوصيات التي انتهى إليها المتحاورون في ملتقى أسبار حول القضية ما يلي:

وضع قيود تنظيمية على تقنية الذكاء الاصطناعي، لحماية الوطن والمجتمع مستقبلا من مخاطر إساءة استخدام أدوات الذكاء الاصطناعي. (سدايا + مجلس الشورى).



دعم المبادرات الدولية لتنظيم وتطوير الذكاء الاصطناعي واستخداماته عالمياً من خلال إنشاء هيئة رقابة دولية للذكاء الاصطناعي على غرار الوكالة الدولية للطاقة الذرية والدعوة لإنشاء منظمة اقليمية لمنطقتنا. (وزارة الخارجية، سدايا).

سن قوانين لمحاسبة شركات الذكاء الاصطناعي وإخضاعها للوائح التنظيمية التي تسنها الجهات الحكومية لضمان خصوصية البيانات. (سدايا + مجلس الشورى).

الاستفادة من بيانات الأفراد الضخمة لأغراض التسويق والتجارة مع الأخذ بعين الاعتبار مخاطر هذه البيانات على السلم الاجتماعي ويمكن أن يكون ذلك من خلال تعهد الجهات بعدم استخدام معلومات العميل الخاصة.

تعزيز "الشفافية" لأنظمة الذكاء الاصطناعي والتأكيد على أن البيانات المخصصة لهذه التقنية تُجمع وتُستخدم ويتم تشاركها وتخزينها وحذفها بطرق تتوافق مع حقوق الأفراد وخصوصيتهم وفرض عقوبات وغرامات على المخالفين كما هو معمول بالاتحاد الأوروبي (مجلس الشورى + المركز الدولي لأبحاث وأخلاقيات الذكاء الصناعي+ سدايا).

تعزيز وسائل تتبع الهاكرز ومرتكبي الجرائم المعلوماتية من خلال المنظمات الدولية المعنية مثل الاتحاد الدولي للاتصالات. ITU

الورقة الرئيسة: د.عبدالعزيز الحرقان

تختلف الضوابط والقوانين المتعلقة باستخدام المعلومات الحساسة في أنظمة الذكاء الاصطناعي من بلد إلى آخر ولكن بشكل عام، تتطلب هذه المعلومات مستوى أعلى من الحماية والخصوية وفقاً للقوانين الوطنية والدولية على سبيل المثال، في الولايات المتحدة، هناك عدد من القوانين واللوائح التي تنظم جمع واستخدام المعلومات الحساسة في أنظمة الذكاء الاصطناعي، مثل قانون حماية الخصوصية الصحية (HIPAA) الذي ينظم جمع واستخدام المعلومات الطبية الحساسة.

يتم تحديد الضوابط والقوانين المتعلقة باستخدام المعلومات الحساسة في أنظمة الذكاء الاصطناعي بناء على تصنيف هذه المعلومات ومدى حساسيتها، ويتم تحديد مستوى الحماية والخصوصية اللازمة وفقاً لذلك

يجب أن يتم جمع المعلومات الحساسة بموافقة صريحة من المواطن، ويجب أن يتم استخدمها فقط للأغراض المحددة والمشروعة، ويجب أن يتم حذفها أو تدميرها بعد انتهاء الأغراض المحدد.

يجب أن توفر أنظمة الذكاء الاصطناعي الحماية اللازمة للمعلومات الحساسة، ويجب أن تتبع أفضل الممارسات في مجال الأمن والخصوصية، بما في ذلك تشفير المعلومات وتحديد مستوى الوصول إليها وإدارة الهوية والوصول. يجب أن يتم الامتثال للقوانين واللوائح المحلية والدولية المتعلقة بجمع واستخدام المعلومات الحساسة في أنظمة الذكاء الاصطناعي الالتزام بمعايير عالية للحماية والخصوصية، ويجب أن يتم تحديد الضوابط والقوانين المناسبة وفقاً للمتطلبات والاحتياجات المحددة في كل بلد.

مصادر بيانات التدريب الخاصة بتطبيقات وأنظمة الذكاء الاصطناعي.

تجمع تطبيقات وأنظمة الذكاء الاصطناعي بيانات التدريب الخاصة بها من مجموعة متنوعة من المصادر تشمل تلك المصادر البيانات المتاحة للجمهور، البيانات التي ينشئها المستخدم، البيانات الاصطناعية، بيانات التعهيد الجماعي، بيانات ملكية الشركة، بيانات الشراكة والتعاون، وسطاء البيانات، البيانات الحكومية والمؤسسية.

وتعد البيانات المتاحة للجمهور أحد أهم مصادر بيانات التدريب الخاصة بتطبيقات وأنظمة الذكاء الاصطناعي ومن أمثلتها: منصة IMAGENET1 لمهام التعرف على الصور وتتضمن قاعدة بيانات للصور منظمة وفقاً لتسلسل WORDNET الهرمي؛ ومستودع البيانات للتعلم الآلي لتنفيذ أنواع مختلفة من المهام مثل مستودع UCI MACHINE LEARNING2والذي يتضمن مجموعة من قواعد البيانات المستخدمة لخوارزميات التعلم الآلي، ومنصات إنتاج مستودعات البيانات المفتوحة التي يمكن الوصول إليها للمساعدة في مزيد من الابتكار في مجالات البحث والأعمال والتعليم مثل منصة THE COMMON CRAWL FOUNDATION3.

كما تتعلم بعض أنظمة الذكاء الاصطناعي من تفاعلات المستخدمين والبيانات التي ينشئها المستخدم ويتضح ذلك في أنماط التوصيات الموجودة في تطبيقات يوتيون وأمازون للتعلم من سلوكيات المشاهدة والشراء لدى المستخدمين. ويتطلب عند الاستفادة من البيانات التي ينشئها المستخدم لتدريب الذكاء الاصطناعي استخدمها وفقاً للوائح وأنظمة الخصوصية ولتوضيح ذلك فإن

منصة جوجل تستعين "بإحصاءات GOOGLE" للتعرف على المدة التي يقضيها أحد الأشخاص في التفاعل على المواقع الإلكترونية المختلفة لقياس متوسط مدة التفاعل.

يمكن أيضاً تدريب أنظمة الذكاء الاصطناعي على البيانات التركيبية الاصطناعية وهي البيانات التي تم إنشاؤها بشكل مصطنع من خلال خوارزميات حاسوبية لمحاكاة بيانات العالم الحقيقي من خلال التعرف على البيانات الأصلية المستمدة من جميع التفاعلات مع الأشخاص الحقيقيين، مثل العملاء والمرضى والموظفين وما إلى ذلك. وتعد تلك النوعية من البيانات مفيدة بشكل خاص عند وضع سيناريوهات يكون فيها بيانات العالم الحقيقي نادرة أو حساسة.

يتم كذلك تدريب بعض أنظمة الذكاء الاصطناعي على البيانات التي يتم جمعها من خلال التعهيد الجماعي CROWDSOURCING وهي العملية يتم من خلالها جمع أكبر عدد من المعلومات أو الآراء أو الخبرات من خلال الإنترنت ووسائل التواصل الاجتماعي وتطبيقات الهواتف الذكية. يعتمد مفهوم التعهيد الجماعي على مشاركة عدد كبير من الأشخاص، نظراً لأنهم على دراية ومهارة وذكاء بشأن الموضوع الذي يتم البحث فيه، مثل تلك البيانات التي تم الحصول عليها لتدريب نموذج لغة GPT-3 والتي أطلقت بواسطة OPEN AI عام 2020م.

تعد بيانات ملكية الشركة مصدر هام لبيانات التدريب لتطبيقات وأنظمة الذكاء الاصطناعي، حيث تمتلك العديد من الشركات كميات كبيرة من بيانات الملكية التي تستخدمها لتدريب أنظمة الذكاء الاصطناعي يمكن أن يشمل ذلك أي شيء من بيانات المبيعات أو بيانات سلوك العملاء أو البيانات التشغيلية.

ومن بين مصادر بيانات تدريب تطبيقات وأنظمة الذكاء الاصطناعي تلك التي يتم الحصول عليها من خلال الشراكات بين الشركات أو المؤسسات أو الباحثين أو من وسطاء البيانات وهي الشركات التي تقوم بجمع البيانات وتهيئتها وبيعها وتستفيد منها أنظمة الذكاء الاصطناعي. كما يتوافر مجموعات كبيرة من البيانات المتاحة من الحكومات والمؤسسات البحثية التي يمكن استخدامها للتدريب الذكاء الاصطناعي مثل تلك البيانات العامة المنشورة بواسطة حكومة الولايات المتحدة 4 وتستعين بها تطبيقات وأنظمة الذكاء الاصطناعي.

وبغض النظر عن مصدر البيانات فمن المهم مراعاة مواءمة استخدام البيانات مع جميع القوانين والقواعد الأخلاقية ذات الصلة بما في ذلك قواعد احترام الخصوصية والإنصاف كذلك من المهم التأكد من أن البيانات غير متحيزة لضمان فاعلية وكفاءة البيانات التي تعتمد عليها أنظمة الذكاء الاصطناعي.

1. HTTP://WWW.IMAGE-NET.ORG
2. . HTTPS://ARCHIVE.ICS.UCI.EDU
3. HTTPS://COMMONCRAWL.ORG

عدم تحيز بيانات التدريب الخاصة بتطبيقات وأنظمة الذكاء الاصطناعي

على الرغم من الطرق المختلفة التي يمكن بواسطتها توفير بيانات التدريب الخاصة بتطبيقات وأنظمة الذكاء الاصطناعي إلا أن ضمان عدم تحيز تلك البيانات من الأمور المعقدة وإن كان يتوافر عدد من الطرق أو الاستراتيجيات لضمان عدم تحيز تلك البيانات، لكن وعلى الرغم من توافر تلك الطرق أو الاستراتيجيات إلا أنه يجب التأكيد على استحالة القضاء على كل أشكال تحيز بيانات تدريب أنظمة الذكاء الاصطناعي، بينما يكون الهدف عادة هو تقليل التحيز بقدر المستطاع وضمان تحقيق الشفافيةبشأن طبيعة وخصائص البيانات وأي تحيزات محتمل تواجدها.

تعد استراتيجية جمع بيانات متنوعة أحد أبز تلك الاستراتيجيات. وتنطوي تلك الاستراتيجية على ضرورة التأكد من أن بيانات التدريب تمثل جميع خصائص المجتمع أو السكان الذي سيخدمه نظام الذكاء الاصطناعي وذلك من حيث العرق والجنس والعمر والوضع الاجتماعي والاقتصادي والموقع الجغرافي وغيرها من الخصائص الديمغرافية، كما ينبغي فهم البيانات بشكل جيد وهو ما يقتضي قضاء بعض الوقت في فهمها والتعرف على حدود استخدامها. وهذا يعني فهم من أين أتت تلك البيانات، ومن ساهم فيها، وأي تحيزات محتملة قد تكون أثرت على طريقة جمعها. ويرتبط بفهم البيانات ضرورة إجراء عمليات تدقيق منتظمة لمواجهة أي تحيزات محتملة في مخرجات نظام الذكاء الاصطناعي، ويساعد في ذلك عدد من أدوات تنفيذ المهام لعدد من التطبيقات الشهيرة مثل 360 AL FAIRNESS G PROPUBLICA وGOOGLE-WHAT-IF في تحديد التحيز وتخفيفه. وتعد شفافية مصادر البيانات أحد طرق ضمان عدم تحيز بيانات التدريب وذلك فيما يتعلق بمعرفة مصادر البيانات وكيفية تجميعها. وتساعد شفافية البيانات أصحاب المصلحة على فهم التحيزات المحتملة وكيف يمكن أن تؤثر على سلوك أنظمة الذكاء الاصطناعي وتتوافر كذلك عدد من تقنيات تقليل تحيز بيانات تدريب أنظمة الذكاء الاصطناعي أثناء مرحلة المعالجة المسبقة للبيانات أو التدريب على نماذج الذكاء الاصطناعي المستخدمة يمكن أن يشمل ذلك تقنيات مثل إعادة توازن البيانات بطرقة آلية ومتزامنة، والوزن المحتمل لدالة الفقد لتقييم الفقد أو "الخسارة" بين النتائج المتوقعة للنموذج والمخرجات الفعلية، والخوارزميات المحققة لعدم التمييز، ويعد التدقيق الخارجي من الاستراتيجيات الهامة لضمان عدم تحيز تلك البيانات ويقصد به الاستعانة بهيئة خارجية تجري عمليات التدقيق لنظام الذكاء الاصطناعي وتساعد تلك الهيئة في ضمان شفافية البيانات وعدم تحيزها ومن بين الطرق المستخدمة في ضمان عدم تحيز البيانات طريقة التعلم المستمر والتحسين فمن المهم تحقيق التعلم المستمر وتحسين أنظمة الذكاء الاصطناعي كلما توافرت بيانات جديدة أو اكتشفت تحيزات غير مرغوبة وأخيراً فمن الضروري التأكد من أن الفرق العاملة على أنظمة الذكاء الاصطناعي مدربة على الأخلاقية وفهم أهمية الحد من التحيز البيانات، وهو ما يمكن أن يساعد على اتخاذ قرارات أفضل خلال عملية التطوير المخطط لها.

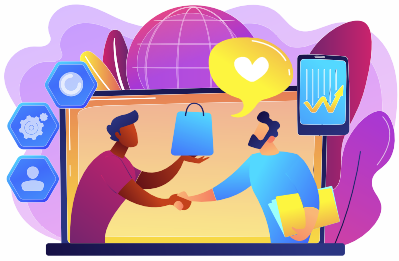
4- HTTPS://WWW.DATA.GOV

الطرق الشائعة المستخدمة لجمع المعلومات بواسطة وسطاء البيانات

يستخدم وسطاء البيانات مجموعة متنوعة من الأساليب لجمع المعلومات وعادة ما يجمعون البيانات من خلال استخدام خوارزميات متطورة تعمل على إنشاء ملفات تعريف مفصلة للأفراد، ومن ثم تحليل هذه البيانات وإجراء استنتاجات حول سلوك المستخدمين وتفضيلاتهم وأنماط حياتهم ويتم بيع تلك الملفات التعريفية إلى شركات أخرى للتسويق أو تقييم المخاطر أو لأغراض أخرى.

تتضمن أهم تلك الطرق طريقة "تجريف الويب" أو "استخلاص المحتوى" وهي الممارسة التي يتم فيها استخدام البرامج الآلية لاستخراج كميات كبيرة من البيانات من مواقع الويب. يمكن أن يشمل ذلك المعلومات العامة من ملفات تعريف الوسائط الاجتماعية والمنتديات والمنصات الأخرى عبر الإنترنت.

ومن بين الطرق الأخرى طريقة "ملفات تعريف الارتباط ووحدات بكسل التتبع" والتي تستخدم على مواقع الويب لتتبع نشاط المستخدم والمساعدة على جمع المعلومات حول الصفحات التي يزورها المستخدم، ومدة بقائهم وما ينقرون عليه، وأنشطة المستخدم الأخرى وتساعد طريقة "شراء أو ترخيص البيانات" والتي يقوم بها وسطاء البيانات عن طريق شراء البيانات أو ترخيصها من شركات جمع بيانات أخرى على سبيل المثال قد يبيع بائع تجزئة بيانات شراء العميل أو قد تبيع خدمة عبر الإنترنت بيانات نشاط المستخدم إضافة لما سبق، فهناك السجلات العامة التي يمكن لوسطاء البيانات استغلالها لجمع معلومات محددة مثل سجلات الناخبين وسجلات الممتلكات وسجلات المحاكم وغيرها من المصادر المتاحة للجمهور من الطرق الشائعة الأخرى طريقة "تكامل التطبيقات"، حيث



تقوم بعض التطبيقات بجمع بيانات المستخدمين وبيعها إلى وسطاء البيانات.

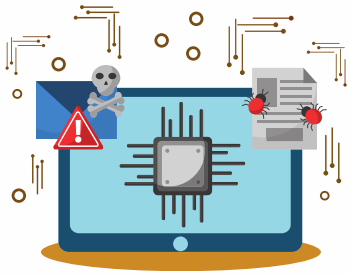
قد تكون هذه التطبيقات ألعاباً أو أدوات مساعدة أو أنواعها أخرى من التطبيقات التي تطلب الوصول إلى معلومات معينة على جهاز المستخدم، وتعد كذلك المسوحات والاستبيانات التي يقوم بجمعها عدد من وسطاء البيانات سواء بشكل مباشر أو غير مباشر من أهم طرق جمع البيانات؛ ويمكن أن تتضمن تفضيلات أو عادات المستخدمين أو تفاصيل شخصية أخرى. كذلك فإن لدى بعض وسطاء البيانات ترتيبات مع مكاتب الائتمان للوصول إلى أنواع معينة من البيانات المالية، وتستخدم هذه المعلومات بشكل عام لتقييم المخاطر وتخضع عادة للوائح صارمة ومن الطرق المتبعة "بطاقات الولاء وبرامج المكافآت" والتي تباع لوسطاء البيانات وغالباً ما تجمع بيانات حول عادات الشراء ويتم استخدامها بعد ذلك لتصميم خطط التسويق والحملات الترويجية.

مخاطر جمع وبيع المعلومات الشخصية بواسطة وسطاء البيانات

بينما يمارس وسطاء البيانات دورهم في مساعدة الشركات على تطوير خدماتهم بما يتناسب مع احتياجات العملاء وتفضيلاتهم فإن جمع البيانات الشخصية وبيعها يتضمن عدد من المخاطر المحتملة، لعل أبرزها انتهاك الخصوصية وتستوجب تلك المخاطر ضرورة وضع قوانين ولوائح قوية لحماية البيانات الشخصية والرقابة على الممارسات المسؤولة لمعالجة البيانات من قبل الشركات إضافة لذلك، فيجب أن تكون هناك توعية من جانب الأفراد بطبيعة تلك المخاطر ومعرفة كافة الطرق الممكنة لحماية بياناتهم الشخصية.

ويعد "انتهاك الخصوصية" أبرز تلك المخاطر، حيث يمكن أن ينتج عن جمع المعلومات الشخصية وبيعها على نطاق واسع انتهاك حقوق الأفراد في ضمان أمن معلوماتهم الشخصية والتعدي على خصوصياتهم فحتى في الحالات التي تكون فيها البيانات مجهولة المصدر، فمن الممكن تحديد هوية الأفراد من خلال تتبع البيانات من مصادرها المختلفة ويمكن لوسطاء البيانات ارتكاب أخطاء نتيجة الاعتماد على معلومات قديمة مما يؤدي إلى استنتاجات غير دقيقة وبالتالي فإن "عدم دقة البيانات" تساهم في حدوث عواقب وخيمة إذا استخدمت البيانات غير الدقيقة في عدد من العمليات، مثل الحصول على الائتمان من المخاطر المحتملة أيضاً مخاطر "سرقة الهوية" وتحدث في الحالات التي يتم فيها اختراق إجراءات الأمان التي وضعها وسيط البيانات، ففي هذه الحالة يمكن استخدام البيانات الشخصية التي يحتفظ بها لسرقة الهوية أو غيرها من أشكال الاحتيال وتعد "الممارسات التمييزية" أحد أشكال المخاطر المحتملة من استخدام المعلومات الشخصية التي يتم جمعها وبيعها من قبل وسطاء البيانات

فعلى سبيل المثال، يمكن للشركات استخدام أو استبعاد مجموعات ديموغرافية معينة بناء على ملفات تعريف البيانات التي يوفرها وسطاء البيانات وقد ينتج عن عمليات جمع البيانات التي تتم من قبل الوسطاء دون معرفة صريحة أو موافقة أصحابها إلى الافتقار إلى مبدأ "الشفافية والتحكم" وهو ما ينتج عنه مشكلة عدم الثقة والقلق بين المستهلكين كذلك يتيح وسطاء البيانات ما يعرف بالتسويق المستهدف، وهو النهج المتبع لزيادة الوعي بمنتج أو خدمة بين مجموعة محددة من المستهلكين وقد يؤدي هذا إلى تلقي المستهلكين إعلانات وطلبات غير مرغوب فيها بناء على بياناتهم الشخصية ويتعرض المستهلكين كذلك لمخاطر "احتمال إساءة الاستخدام" والناتجة عن اساءة استدام البيانات الشخصية بطرق عديدة عندما تقع في الأيدي الخطأ وهو ما قد ينتج عنه ملاحقة أصحاب البيانات أو مضايقتهم أو غيرها من أساليب التحايل.



ويرتبط باحتمال إساءة استخدام البيانات مخاطر "التلاعب السلوكي" من خلال فهم التفضيلات والسلوكيات الشخصية والتي يمكن للشركات التلاعب بسلوك أصحابها لتشجيع الشراء الاندفاعي أو غيرها من السلوكيات الضارة.

تمكين الأفراد من حماية بياناتهم المجمعة من قبل وسطاء البيانات

قد تكون حماية بيانات الأفراد التي تم جمعها من قبل وسطاء البيانات أمراً صعباً نظراً لاتساع نطاق مصادرها والتي جمع منها هؤلاء الوسطاء المعلومات ومع ذلك، فهناك العديد من الخطوات التي يمكن اتباعها للحد من كمية البيانات التي يتم جمعها ومشاركتها إلا أنه يجب ملاحظة أنه يكاد يكون من المستحيل منع جمع بيانات واستخدامها تماماً من قبل وسطاء البيانات وهو ما يتطلب حلول تنظيمية وتشريعية شاملة لمواجهة المشاكل المترتبة عليها.

يمكن من خلال "الحد من المعلومات المتاحة للجمهور" ومتابعة المعلومات التي يتم مشاركتها علنا سواء من خلال وسائل التواصل الاجتماعي أو المنتديات العامة أو غيرها من منصات الويب أن تساهم ولو بشكل جزئي فى حماية البيانات الشخصية وبالتالي فمن المهم استخدام إعداد الخصوصية لتحديد من يمكنه رؤية المنشورات الشخصية وتجنب مشاركة المعلومات الحساسة بشكل عام وكذلك فإن "إلغاء الاشتراك من خدمات جمع البيانات" والتي يتيحها بعض وسطاء البيانات تعد خيار مناسب لحماية البيانات الخاصة، على الرغم من أن تلك الطريقة قد تستغرق وقتاً طويلًا حيث يجب القيام بها لكل وسيط بيانات على حدة وفي هذا الصدد يقدم موقع CLEARINGHOUSE RIGHTS PRICACY قائمة بوسطاء البيانات وتعليمات حول كيفية إلغاء الاشتراك من كل منهم.

ويجب على المستخدمين "استخدام الأدوات التي تركز على الخصوصية" وذلك من خلال استخدام متصفحات الويب التي تركز على الخصوصية (مثل BRAVE أو FIREFOX) ومحركات البحث (مثل DUCKDUCKGO) وأدوات أخرى، حيث تم تصميم هذه الأدوات للحد من التتبع وجمع البيانات تتوافر كذلك عدد من أدوات حظر الإعلانات ومنع التتبع والتي يمكن الاستعانة بها للحد من البيانات التي يمكن لمواقع الويب التابعة لجهات خارجية جمعها عن المستخدمين وفي كل الأحوال فمن الضروري أن يكون جميع المستخدمين حذرين من استخدام الخدمات المجانية، فالعديد من تلك الخدمات تجني الأموال من خلال جمع بيانات المستخدمين وبيعها كذلك فعلى المستخدمين أن يحرصوا على عدم مشاركة معلوماتهم الشخصية ومن الضروري أن يكون المستخدم حذراً بشأن الجهات التي تشارك معها معلوماته الشخصية وأن يكون على دراية بأسباب الحاجة إلى تلك المعلومات وكيف تخطط لحمايتها من الضروري كذلك قيام المستخدمين "بالتحقق من سياسات الخصوصية" قبل الاشتراك في أي من الخدمات التي تقدمها منصات الإنترنت فعلى المستخدم التحقق من كيفية استخدام تلك المنصات البيانات وأخيراً يمكن للمستخدمين الاستعانة "بخوادم VPN أو الاتصالات المشفرة" وهي عبارة عن شبكة افتراضية خاصة (VPN) لإخفاء عنوان IP الخاص بالمستخدم وأنشطة تصفحه كما ينبغي التأكد من أن مواقع الويب المستخدمة والتي تقوم فيه بإدخال معلومات حساسة تستخدم الاتصالات المشفرة (HTTPS).

أهم القوانين ولوائح خصوصية البيانات المتبعة بواسطة الشركات

هناك العديد من قوانين ولوائح خصوصية البيانات الرئيسية حول العالم والتي يجب على الشركات الالتزام بها ومن المهم أن تفهم الشركات هذه القوانين وغيرها من قوانين خصوصية البيانات المعمول بها وتمتثل لها، لأن عدم التزامها قد يعرضها لغرامات كبيرة وإلحاق الضرر بسمعة الشركة من جهة أخرى يساعد الالتزام بقوانين خصوصية البيانات على بناء الثقة مع العملاء والمستخدمين وهو ما يعزز من الميزة التنافسية للشركات ومن أبرز تلك اللوائح والقوانين ما يلي.

يعد القانون العام لحماية البيانات (GDPR) أحد أهم لوائح حماية خصوصية البيانات والتي يفرضها الاتحاد الأوروبي منذ عام 2018 وينطبق القانون على جميع الدول الأعضاء في الاتحاد الأوروبي ويؤثر على الشركات في جميع أنحاء العالم التي تتعامل مع بيانات مواطني الاتحاد الأوروبي ويتضمن القانون مبادئ عامة مثل تقليل استخدام البيانات والحد من أغراض استخدام البيانات ويمنح الأفراد حقوقا مثل الحق في الوصول لبياناتهم وحذفها وإمكانية نقل البيانات ويمكن أن يؤدي عدم الامتثال لذلك القانون إلى غرامات تصل إلى 20 مليون يورو أو 4% من حجم المبيعات السنوي العالمي للشركة غير الممتثلة، أيهما أعلى.

ينطبق قانون خصوصية المستهلك في كاليفورنيا (CCPA) على الشركات العامة في كاليفورنيا بالولايات المتحدة ويقدم حقوقاً مماثلة للمقيمين في كاليفورنيا كما يفعل القانون العام لحماية البيانات (GDPR) لمواطني الاتحاد الأوروبي وتشمل هذه الحقوق في القدرة على تحديد المعلومات الشخصية التي تجمعها الشركات عن المستخدمين والحق في حذف المعلومات الشخصية التي تم جمعها والحق في إلغاء الاشتراك في بيع المعلومات الشخصية.

تفرض سنغافورة قانون حماية البيانات الشخصية (PDPA) ويلزم القانون الشركات بحماية البيانات الشخصية للأفراد من خلال إتباع ترتيبات أمنية محددة وإلزام الشركات بعدم الاحتفاظ بالبيانات الشخصية لفترة أطول من الإلزام وعدم السماح بنقل البيانات الشخصية خارج سنغافورة ما لم يتم استيفاء متطلبات معينة.

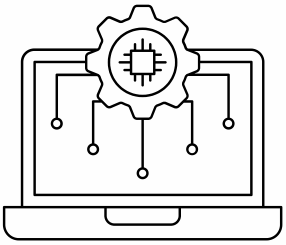
وفي البرازيل فإن القانون العام لحماية البيانات (LGPD) والذي يشبه القانون العام لحماية البيانات (GDPR) بأوروبا يمنح المستخدمين حقوقاً لحماية بياناتهم الشخصية، بما في ذلك الحق في التعرف على آليات تجميع البيانات والوصول للبيانات وتصحيح البيانات غير المكتملة أو غير الدقيقة أو القديمة وإخفاء الهوية وخطر أو حذف البيانات غير الضرورية أو الزائدة أو البيانات التي يتم معالجتها بعيداً عن القانون العام لحماية البيانات (LGPD).

تلتزم الشركات بالمملكة المتحدة بتبني قانون حماية البيانات (DPA 2018) والذي دخل حيز التنفيذ في 25 مايو 2018 بديلًا عن قانون حماية البيانات لعام 1998م ويحدد القانون بجانب القانون العام لحماية البيانات (GDPR) الأوروبي إطار عمل الشركات فيما يخص حماية بيانات المستخدمين.

التعقيبات:

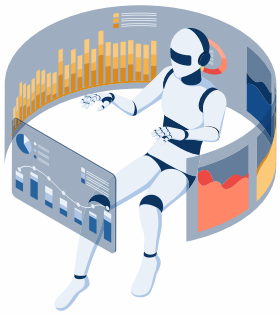
التعقيب الأول: د. عبدالعزيز الباتلي

يعكس الذكاء الاصطناعي تحولًا ثوريًا في عالم التكنولوجيا، وهو يشكل تحديًا وفرصة لنا جميعًا، سواء كنا مجتمعًا أو دولة، للاستعداد والتكيف مع هذا التطور الرائع. تشهد التطورات المذهلة في مجال الذكاء الاصطناعي نموًا سريعًا ولافتًا للنظر. حيث



الأنظمة الذكية والخوارزميات المتقدمة تسهم في تحقيق إنجازات غير مسبوقة في مجموعة متنوعة من المجالات.

على سبيل المثال، في الطب، يُمكن للذكاء الاصطناعي تشخيص الأمراض وتوجيه العلاج بدقة أكبر من البشر. في القطاع الصناعي، يُمكنه زيادة الإنتاجية وتقليل التكاليف من خلال الأتمتة. في التعليم، يُمكنه تخصيص التعليم لكل طالب بناءً على احتياجاته الفردية. واحدة من أهم النقاط التي يجب أن نفهمها هي أن



الذكاء الاصطناعي ليس فقط تقنية متقدمة، بل هو أيضًا محرك للاقتصاد الجديد.

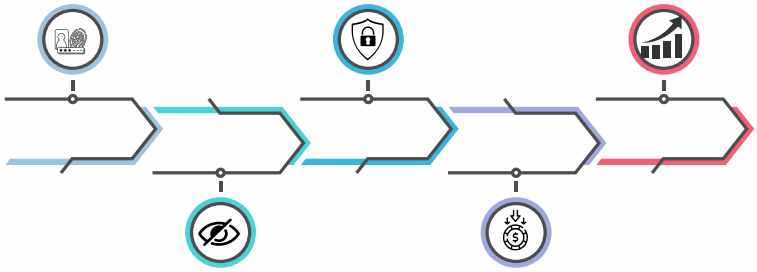
يمكن أن يساهم الذكاء الاصطناعي في خلق وظائف جديدة وزيادة الإنتاجية، مما يعزز النمو الاقتصادي. ولذلك، يجب على الدول والمجتمعات الاستثمار في التعليم والبنية التحتية التكنولوجية للاستفادة القصوى من هذا التطور والاستعداد له قبل وصوله، فهو آت لا محالة. علاوة على ذلك، يجب أن ننظر إلى الجانب الاجتماعي للذكاء الاصطناعي. يمكن أن يسهم في تحسين الخدمات الصحية والتعليمية وزيادة فرص التوظيف. ومع ذلك، يجب أيضًا مراعاة التحديات المحتملة مثل الخصوصية والأمان. يتطلب هذا تطوير تشريعات وسياسات مناسبة لضمان استفادة الجميع من هذا التقدم وحماية حقوقهم.

في الواقع، من المهم أن ندرك أن الذكاء الاصطناعي ليس مجرد أداة لتقليل واستبدال الوظائف، بل هو نموذج جديد للتفكير والاقتصاد. تشمل المخاوف الرئيسية المرتبطة بوصول الذكاء الاصطناعي إلى ما وراء استبدال الوظائف التقليدية ما يلي:

تغيير البنية الاقتصادية: سيؤدي وصول الذكاء الاصطناعي إلى تحول هائل في بنية الاقتصاد، حيث يمكن أن يصبح المعرفة والبيانات هما العملة الرئيسية. هذا يتطلب استعدادًا كبيرًا للمجتمعات لتطوير مهارات جديدة واقتصاد قائم على البيانات.

الخصوصية والأمان: يتطلب استخدام الذكاء الاصطناعي الكثير من البيانات الشخصية، مما يثير مخاوف حول الخصوصية والأمان. يجب وضع قوانين ولوائح صارمة لحماية المعلومات الشخصية والبيانات الحساسة.

التوظيف والتعليم: يمكن أن يؤدي انتشار الذكاء الاصطناعي إلى تغييرات في متطلبات الوظائف والمهارات المطلوبة. يجب أن يكون هناك تركيز على إعادة تدريب القوى العاملة وتطوير مهارات جديدة لمواجهة هذا التحول.



التأثير على الفقراء وغير المحظوظين: هناك مخاوف من أن الذكاء الاصطناعي قد يزيد من الفوارق الاجتماعية إذا لم يتم توجيه الاستفادة منه بشكل عادل للجميع. يجب على الدول والمجتمعات العمل على تحقيق الشمول الاجتماعي والاقتصادي من خلال هذا التقدم.

تحديات أخلاقية: يطرح الذكاء الاصطناعي أيضًا تساؤلات أخلاقية مهمة، مثل القرارات الأخلاقية التي يمكن أن تتخذها الأنظمة الذكية والمسائل المتعلقة بالتحكم البشري في التكنولوجيا.

بناءً على هذه المخاوف، يجب أن يكون هناك خطة استعداد شاملة تشمل التعليم والتشريعات والسياسات الاقتصادية للتأكد من أننا مستعدين لقدوم الذكاء الاصطناعي. يتعين علينا أيضًا الاستفادة من الفرص الكبيرة التي يقدمها الذكاء الاصطناعي لتحقيق أهدافنا الشخصية والاجتماعية والاقتصادية بشكل أفضل.

مشاركة البيانات الشخصية في مستقبل يتسم بانتشار الذكاء الاصطناعي قد يكون لها مقابل مادي أو معنوي، وقد تكون الدافع والقرار راجع للفرد بحد ذاته ورغبة منه، وهذا التطور يفتح الباب أمام تحديات كبيرة تتعلق بالخصوصية والأمان الرقمي. من المهم أن نناقش هذه الجوانب ونضع إطارًا أخلاقيًا وقوانين تنظم هذه الممارسات. في الوقت الحالي، تعتبر البيانات الشخصية من أهم الأصول في العصر الرقمي، وقد تمثل قيمة اقتصادية كبيرة.

مع ازدياد استخدام الذكاء الاصطناعي والتحليلات الضخمة للبيانات، يمكن أن تصبح مشاركة هذه البيانات مصدرًا محتملًا للدخل.

يمكن للأفراد والشركات تبادل بياناتهم مع منصات الذكاء الاصطناعي مقابل مدخول مادي أو خدمات. مع تزايد مشاركة البيانات الشخصية، وكما أشارت الورقة الرئيسة، يجب وضع أنظمة منطقية تضمن الابتكار وبنفس الوقت تضمن حماية الخصوصية. يجب أن تكون الشروط والأحكام لمشاركة البيانات واضحة وشفافة، ويجب أن تكون هناك ضمانات للتحكم في البيانات ومراقبتها. يتطلب ذلك تشديد القوانين المتعلقة بالخصوصية وفرض عقوبات على الانتهاكات. مع البيانات التي تصبح سلعة تجارية، يتوقع أن المجتمع يواجه تحدياتٍ أخلاقيةٍ متنوعة. مثلًا، كيف يمكن التعامل مع بيانات الأفراد الحساسة مثل المعلومات الطبية أو الجينوم؟ هذا يتطلب تطوير أخلاقياتٍ جديدة توجه استخدام البيانات. لضمان استفادة عادلة من مشاركة البيانات، يجب تحقيق التوازن بين المصلحة الشخصية والمصلحة العامة. يجب أن تتوافر فرص متساوية للجميع للمشاركة والاستفادة من البيانات، ويجب أن تكون هناك ضمانات لمنع استغلال البيانات بأي شكل من الأشكال. مع زيادة كميات البيانات المشاركة، يجب تطوير تقنيات تخزين وإدارة البيانات بشكل آمن وفعال. ذلك يشمل تقنيات التشفير وأنظمة الحماية القوية.

فيما يتعلق ببيانات التدريب، فتحديدها هي الخطوة الأولى والأكثر أهمية في بناء نموذج ذكاء اصطناعي. يتعين على المطورين تحديد مصدر البيانات المناسب وجمع مجموعة مناسبة من البيانات لاستخدامها في تدريب النموذج. يمكن أن تكون مصادر البيانات متنوعة، بما في ذلك قواعد البيانات العامة، ومواقع الويب، وبيانات السجلات في المستشفيات، والصور ومقاطع الفيديو، وغيرها. تنظيف البيانات هو الخطوة التالية، حيث يتم تصفية وتهيئة البيانات لاستخدامها في عملية التدريب. هذا يشمل إزالة البيانات المفقودة، ومعالجة القيم المتطرفة، وتحويل البيانات إلى تنسيق مناسب للتدريب. عملية تنظيف البيانات تلعب دورًا حاسمًا في ضمان دقة النموذج النهائي. بعد تنظيف البيانات، يتعين تقسيمها إلى مجموعتين رئيسيتين: مجموعة التدريب ومجموعة الاختبار. مجموعة التدريب تستخدم لتعلم النموذج، بينما تُستخدم مجموعة الاختبار لاختبار أداء النموذج وقياس دقته. من المهم جدًا أن تكون هذه العملية عادلة وتمثل البيانات بشكل جيد للحصول على تقدير دقيق لأداء النموذج.

أهمية دقة البيانات تلعب دورًا محوريًا في تحديد جودة المخرجات في خوارزميات الذكاء الاصطناعي. إذا كانت البيانات غير دقيقة أو متلاعب بها، فإن النموذج سيكون غير قادر على التعرف بشكل صحيح على الأنماط والمعلومات في البيانات الجديدة. بينما إذا كانت البيانات دقيقة وتمثل بشكل جيد الظروف المحيطة بالمشكلة، سيكون النموذج أكثر قدرة على تعلم الأنماط الصحيحة وإجراء توقعات دقيقة. هذا ينعكس على جودة النتائج والقدرة على استخدام النموذج في تطبيقات الواقع. من المهم أيضًا أن لا تكون عملية جلب وتحضير البيانات عملية ذات مرة واحدة. يجب على المطورين العمل على استمرارية تحسين البيانات وتحديثها بمرور الوقت. هذا يمكن أن يتضمن إضافة بيانات جديدة، وتحسين تنظيف البيانات الحالية، ومعالجة أي مشكلات أخرى تظهر.

الجدير بالذكر، هناك العديد من الأدوات والمنصات التي تعتمد على الذكاء الاصطناعي وتقدم حلًا مبتكرًا في مجموعة متنوعة من المجالات. من بينها:

- IBM WATSON : فهي واحدة من أشهر منصات الذكاء الاصطناعي التي تقدم مجموعة متنوعة من الخدمات والأدوات لتطبيقات مختلفة، بما في ذلك تحليل البيانات، وتعلم الآلة، ومعالجة اللغة الطبيعية.
- GOOGLE CLOUD AI:تقدم GOOGLE منصة GOOGLE CLOUD AI التي تشمل مجموعة من الخدمات مثل VISION AI للتعرف على الصور وNATURAL LANGUAGE PROCESSING لمعالجة اللغة الطبيعية وAUTOML لبناء نماذج تعلم الآلة دون الحاجة لخبرة متقدمة.
- MICROSOFT AZURE AI: توفر مجموعة متنوعة من الأدوات والخدمات لتطوير تطبيقات الذكاء الاصطناعي، بما في ذلك الخدمات المعرفية COGNITIVE SERVICES التي تمكن من إضافة قدرات مثل التعرف على الصور ومعالجة النصوص إلى التطبيقات.
- AMAZON AWS AI: تقدم مجموعة من الخدمات المتعلقة بالذكاء الاصطناعي بما في ذلك AMAZON SAGE MAKER لبناء نماذج تعلم الآلة وAMAZON LEX لبناء تطبيقات تفاعلية تعتمد على اللغة الطبيعية.
- UIPATH: للروبوتات العملية الآلية والتشغيل الذاتي للعمليات الأعمال.
- SALESFORCE EINSTEIN: تستخدمها الشركات لتحليل البيانات العملية وتوفير توجيهات معنوية لتحسين الأداء.
- H2O.AI:تقدم منصات تعلم الآلة والذكاء الاصطناعي لتطبيقات الأعمال والتحليلات.
- C3.AI: تقدم منصات للذكاء الاصطناعي المخصص لقطاعات مثل الطاقة والخدمات المالية والصناعة.

- SAS AI: توفر أدوات تحليل البيانات وتعلم الآلة.
- وفيما يتعلق بمعالجة الصوت والصورة، فمن بين المنصات والخدمات ما يلي:
- GOOGLE CLOUD VISION: تقدم تحليلًا للصور وتعرف محتوى الصور بما في ذلك الكائنات والنصوص والأماكن والعلامات.
- GOOGLE CLOUD SPEECH-TO-TEXT: تحول الكلام المسجل إلى نص مكتوب باستخدام تقنيات التعرف على الصوت.
- AMAZON REKOGNITION:تيح التعرف على وجوه الأشخاص في الصور والفيديوهات واكتشاف الكائنات والنصوص.
- IBM WATSON VISUAL RECOGNITION: توفر تحليلًا للصور يمكن استخدامه لتصنيف الصور واكتشاف المحتوى.
- IBM WATSON SPEECH TO TEXT: تحول الكلام المسجل إلى نص مكتوب بدقة عالية.
- MICROSOFT AZURE COMPUTER VISION: تتيح تحليل الصور والكشف عن الكائنات والعلامات والنصوص.
- MICROSOFT AZURE SPEECH SERVICE: تحول النص المنطوق إلى نص مكتوب وتقدم أيضًا تحليلًا للصوت.
- CLARIFAI: تعرف الصور وتوفر تحليلًا دقيقًا للمحتوى.
- SHAZAM: تستخدم للكشف عن الموسيقى وتحديد الأغاني من خلال الاستماع إلى الأصوات.
- SOUND HOUND: تعمل على التعرف على الأغاني والموسيقى من خلال الصوت.
- WIT.AI: توفر تحليلًا للنصوص المنطوقة والمكتوبة.
- AZURE FACE API: تتيح التعرف على الوجوه وميزات الوجه والتحقق من الهوية.
- KAIROS: توفر خدمات التعرف على الوجوه وتتبع الوجوه.
- SPEECHMATICS: تحوّل الكلام المنطوق إلى نص مكتوب بلغات متعددة.
- DEEPGRAM: تقدم تحليلًا للصوت باستخدام تعلم الآلة.

فيما يتعلق بتحيز الذكاء الاصطناعي، فمن المهم أولا أن نتفق على تعريف التحيز. تعتبر الخوارزميات في مجال الذكاء الاصطناعي منطقية وبسيطة في أساسها، حيث يتم تدريبها على مجموعة متنوعة من البيانات لاتخاذ القرارات. ومع ذلك، فإن هذه البيانات قد تحتوي على تحيز نحو فئة معينة أو تفضيل لأحد الجوانب على حساب الآخر. على سبيل المثال، إذا كانت بيانات التدريب تحتوي على تمثيلات غير عادلة لفئات معينة من الأشخاص، فإن النموذج الناتج من هذه البيانات قد يكون معرضًا للتحيز نحو هذه الفئات عند اتخاذ القرارات. وهذا يمكن أن يؤدي إلى تباطؤ التقدم نحو المساواة وزيادة العدالة في تكنولوجيا الذكاء الاصطناعي. لمعالجة تحيز الذكاء الاصطناعي، هناك عدة خطوات يجب اتخاذها تبدأ من تنويع مصادر البيانات حيث من المهم جمع مصادر متعددة ومتنوعة من البيانات التي تُستخدم في تدريب النموذج.

يجب ضمان تمثيل جيد لجميع الفئات والمجموعات المستهدفة.، ومن ثم ضمان وجود تحليل للبيانات لاكتشاف التحيز حيث يمكن استخدام تقنيات تحليل البيانات للكشف عن التحيز المحتمل في البيانات. هذا يشمل تحليل التصنيفات وتحليل العلاقات بين المتغيرات. بالإضافة، يمكن تعديل البيانات لتصحيح أو تقليل التحيز. على سبيل المثال، يمكن إضافة بيانات إضافية للفئات المهملة أو تغيير وزن البيانات لتوازن الجداول. ويتضح جليا أهمية تطوير الخوارزميات لتكون أكثر عدالة وقدرة على التعامل مع التحيز. يمكن استخدام التقنيات مثل التفاوت العادل لتحسين أداء النماذج. أيضا، يجب أن تكون عمليات اتخاذ القرارات في الذكاء الاصطناعي شفافة وقابلة للفحص. يجب توثيق الإجراءات المتخذة لمعالجة التحيز والتأكد من مساءلة المسؤولين عن النظام. ولا نغفل أهمية توعية المطورين والمستخدمين بقضية التحيز في الذكاء الاصطناعي وتوجيههم نحو التعرف على التحيز وكيفية التعامل معه.

في عصر يسوده التقدم التكنولوجي واستخدام تزايد مستمر لتقنيات الذكاء الاصطناعي(AI)، أصبحت البيانات هي أحد أهم الموارد. ومن هنا جاء دور وسطاء البيانات في جمعها وتوفيرها للشركات والمؤسسات للاستفادة منها في تطبيقات متعددة. يتيح الذكاء الاصطناعي فهم البيانات واستخدامها بشكل أفضل، ولكن مع ذلك، هناك مخاطر تحيط بدور وسطاء البيانات تتعلق بالخصوصية والأمان. وسطاء البيانات يقومون بدور أساسي في تمكين تطبيقات الذكاء الاصطناعي حيث يقومون بجمع مجموعات ضخمة من البيانات من مصادر متعددة وينظمونها ويجعلونها متاحة للشركات والباحثين. يمكن لهؤلاء الوسطاء توفير بيانات تاريخية وحالية ومتعددة الأبعاد، مما يساهم في تدريب نماذج الذكاء الاصطناعي وتحسين أدائها. على سبيل المثال، يمكن لشركة تطبيقات الذكاء الاصطناعي في مجال الصحة الاستفادة من بيانات المرضى لتطوير نماذج تنبؤية للأمراض وتحسين الرعاية الصحية. لكن مع هذا الدور الحيوي، تأتي مخاطر كبيرة لا يجب تجاهلها. من أبرز هذه المخاطر التهديدات للخصوصية. جمع وتوزيع كميات ضخمة من البيانات يمكن أن يعرض الخصوصية الشخصية للأفراد للتهديد. يمكن أن تتضمن هذه البيانات معلومات حساسة تتعلق بالصحة والمال والسلوك. لا يمكن إغفال مخاطر الاختراقات السيبرانية حيث تعتبر قواعد البيانات الكبيرة التي تمتلكها وسطاء البيانات هدفًا جذابًا للهجمات السيبرانية. إذا تم اختراق هذه القواعد، يمكن أن تتسرب البيانات وتستخدم في الأنشطة غير الأخلاقية.

ختاماً، يمكن للذكاء الاصطناعي (AI)أن يؤثر بشكل كبير في الاقتصاد بطرق عديدة ومتنوعة، وذلك من خلال تحسين الإنتاجية، وتوفير الوقت والتكاليف، وخلق فرص جديدة للأعمال، وتحسين تجربة المستخدمين، ودعم اتخاذ القرارات الاستراتيجية والاستشراف. شهد سوق الذكاء الاصطناعي عالميا نموًا سريعًا، ومن المتوقع أن يستمر هذا النمو في المستقبل بنسبة 18٪ سنويا (CAGR) حيث يتوقع أن يصل حجم السوق في 2030م إلى 740مليار دولار مقارنة بـ 241 مليار دولار في 2023م.

التعقيب الثاني: د. علي الوهيبي

شهد العقد الأخير اقبالًا عالمياً مضطرد على تقنيات الذكاء الاصطناعي من قبل الحكومات وقطاعات الأعمال المتوسطة والصغيرة، وعلى الرغم من ما تقدمه تلك التقنيات من خدمات ومنتجات سهلت حياة الناس، إلا أنها لا تخلو من العديد من السلبيات ومن أبرزها إمكانية انتهاك البيانات الخاصة أو الشخصية.

ساعدت جهود المملكة من خلال الهيئة الوطنية للبيانات والذكاء الاصطناعي في وضع البنية التحتية لاستخدام أنظمة الذكاء الاصطناعي وسن التشريعات والقوانين المرتبطة باستخدام البيانات ومشاركتها ومتابعة الامتثال لتلك التشريعات.

ويقودنا ذلك إلى مفهوم تصنيف البيانات وهو تنظيم البيانات في فئات بناءً على المحتوى بحيث يمكن تعيين حقوق الوصول بشكل مناسب مع مراعاة أمن وحماية تلك البيانات. يعتبر تصنيف البيانات حجر الزاوية لتنظيم عملية نشر البيانات المفتوحة، وإتاحة المعلومات العامة وتبادل البيانات المحمية بما في ذلك البيانات الشخصية، وهذا بدوره يساعد على رفع مستوى معايير الرقابة المجتمعية على أداء الجهات العامة وزيادة مستوى الشفافية وتعزيز النزاهة وإزالة السرية غير الضرورية عن أنشطة الجهات العامة عن طريق تنظيم ممارسة حق الاطلاع على المعلومات العامة أو الحصول عليها. وحسب حساسية البيانات فيمكن تصنيفها إلى أحد الفئات التالية:

1. **البيانات العامة:** اعتمادا على مبدأ الأصل بالبيانات الاتاحة، تشمل البيانات العامة أي معلومات يمكن الكشف عنها للجميع دون أن تشكل تهديدًا على المنظمة، مثل الأسماء أو الأوصاف الوظيفية أو النشرات الإخبارية. نظرًا لأن البيانات العامة غير مقيدة بشكل أساسي، فهي الأقل صلة بمستويات التصنيف الأربعة.
2. **البيانات الداخلية:** يتضمن هذا النوع من البيانات أي معلومات مقصورة على الموظفين الداخليين وأصحاب المصلحة المعنيين فقط. قد تتضمن أمثلة البيانات الداخلية المذكرات والخطط والمخططات والعروض التقديمية وما إلى ذلك. في حالة الكشف عن هذا النوع من البيانات للجمهور، فمن غير المرجح أن تخضع المؤسسة لأي غرامات تنظيمية أو دعاوى قضائية؛ ومع ذلك، يمكن أن تكون مشكلة إذا احتوت البيانات المسربة على أسرار عمل يمكن أن يستخدمها منافسوهم.
3. **البيانات السرية:** يتضمن هذا النوع من البيانات أي معلومات يمكن أن تؤدي، في حالة تسريبها إلى الجمهور، إلى دعاوى قضائية وغرامات وإضرار بالسمعة. تتضمن أمثلة البيانات السرية: أرقام الضمان الاجتماعي، وتفاصيل البنوك، والمعلومات الصحية المحمية، وأي بيانات تغطيها قوانين خصوصية البيانات ذات الصلة بالمؤسسة.

4.البيانات المقيدة: يتضمن هذا النوع من البيانات أي معلومات، إذا تم اختراقها بطريقة ما، يمكن أن تلحق ضررًا كبيرًا بالمؤسسة وموضوع البيانات المعنية. بالإضافة إلى الدعاوى القضائية باهظة التكلفة والغرامات والأضرار التي تلحق بسمعة المؤسسة، فإن الخرق الذي يتضمن بيانات مقيدة يمكن أن يعرض حياة الأشخاص للخطر. فلو تعرضت مثلًا إحدى مؤسسات الرعاية الصحية لخرق حيث تمكن المهاجم من الوصول إلى بيانات اعتماد الحساب المميزة، فيمكنه تثبيت برنامج فدية وتشغيله والذي سيضع الممارسين الداخليين خارج الأنظمة الهامة.

يعتمد تحديد الفئة من التصنيفات السابقة للبيانات على التشريعات والقيود على البيانات، كما يوضع معيار أحياناً لتقسيم كل فئة من الفئات السابقة إلى درجات مثل عالي أو منخفض ونحو ذلك، حسب التأثير الذي سينتج في حال نشر تلك البيانات.

وفي المملكة، يتولى مكتب إدارة البيانات وضع السياسات المتعلقة بالبيانات ومتابعة امتثال الجهات بتلك السياسات. وحدد المكتب تصنيفات البيانات إلى سري للغاية، سري، مقيّد وعام.

المداخلات حول القضية

الخصوصية والتعامل مع البيانات في الذكاء الاصطناعي.

يمكن تصنيف أهم المعلومات الشخصية المطلوبة في خوارزميات الذكاء الاصطناعي فيما يلي:

-الموقع الجغرافي: يمكن التحكم فيها وصلاحياتها بشكل دائم من خلال اعدادات الأجهزة المحمولة.

-الجنس: معلومات عامه لأخطر منها.

-العمر: معلومات عامة لأخطر منها.

-معلومات تاريخية: في محركات البحث، أو التصفح.

-معلومات الحيوية: مثل معلومات الساعة الذكية كعدد الخطوات وعدد ساعات التصفح ونبض القلب ونحوه معلومات يمكن الحصول منها على بيانات استدلالية.

-الصور ومحتوى تطبيقات التواصل الاجتماعي: معلومات عامة لا يمكن بالغالب التحكم فيها وانما يتحكم فيها أرباب هذه التطبيقات ويتم استغلالها لأغراض عدة.

هنا تصبح بيانات التواصل الاجتماعي والتاريخية أو أي بيانات استدلالية أو توليدة هي الوحيدة التي لم تخضع بعد لأحكام خاصة للتحكم فيها. ولم يتم معالجه الخصوصية فيها وتبقى خيار شخصي إلى هذه اللحظة.

-أما بيانات رقم الهاتف، البريد الالكتروني وغيرها لا تحتاجهم خوارزميات الذكاء وانما تستخدم كأدوات للتحقق من هويه الأشخاص.

-المعلومات البنكية في حال احتاجت التطبيقات إلى عمليات الدفع.

ويمكن أن تخضع لرقابة جهات موثوقة لضمان ذلك داخل كل دولة وإلزام مطورين البرامج على إتباعها مثل خدمات نفاذ وبالتالي الاستغناء عن التعريفات المستخدمة من قوقل أو محفظة أبل. وهنا يبرز التساؤل: لماذا نقوم بدفع مبلغ شهري للتخزين السحابي ونحن على يقين بأن الصور والبيانات يمكن استغلالها للأغراض تجاريه ويمكن تحليلها والاستفادة منها؟

وفي هذا السياق يلاحظ أن اغلب البيانات المستخدمة في الوقت الحاضر هي استدلالات من بيانات عامة فمن المناسب إضافة نوع جديد من البيانات ممكن تسميته بيانات استدلاله أو استشرافية يمكن مثلا من خلال تغريدات الشخص معرفة ما إذا كان يعاني من حالة نفسية أو عنده ميول انتحارية على سبيل المثال. هذه الاستدلالات قد تكون صحيحة بنسب عالية وقد تكون مسيئة، وقد تؤثر على الشخص بشكل مباشر أو غير مباشر، وقد تعرضه لمسائلات قانونية. هذه البيانات أو التنبؤات يتم الوصول لها من خلال بيانات عامة غير سرية إذا ما تم استخدام تقنيات الذكاء الاصطناعي.

بقية البيانات يمكن أن تخضع بوسائل التعاملات الأخلاقية والتشفير لها دون أي مشكله خصوصا إذا ما تمت تحت مظلة حكومية. ومن ثم فإن من المهم الوعي بأن البيانات الداخلة للنماذج لا يتم استخدامها بحالتها الأصلية وإنما يتم استخدام دلالات رقميه منها بطريقة ما لفهم هذه البيانات والاستدلال بها. ما يتم بعد ذلك للبيانات هو الخطر الأعظم.

في حين تذهب بعض الآراء إلى أن مفهوم توظيف الذكاء الاصطناعي في حوكمة استخدام المعلومات الخاصة يجعل من الصعب تطبيق أي ضوابط وقوانين تتعلق باستخدام المعلومات الخاصة في أنظمة الذكاء الاصطناعي، لا سيما وأن التقنية منذ فترة وهي تتسارع في توظيف كل ما هو متاح من المعلومات المتعلقة بالأشخاص للإفادة منها عبر خوارزميات معينة في الوصول لطبيعة المحتوى الذي يمكن تقديمه وفي نمط الاعلانات التي تتسق وطبيعة اهتمام كل شخص .اليوم غالب الناس يوافقون على توظيف معلوماتهم الشخصية بحيث يمكن أن تفيد منها تطبيقات وجهات ومؤسسات لصالحها. إن تطبيقات الذكاء الاصطناعي في مختلف المجالات من خلال قدرتها على تحليل بيانات ضخمة جدا ستعطي تلك الجهات صلاحيات واسعة في استثمار ما نحسبه بيانات شخصية وهو لم يعد كذلك.

وتعتمد طرق جمع المعلومات على عدة وسائل مباشرة وغير مباشرة. غير المباشرة تعتمد على بناء "شخصية نموذجية إلكترونية" وتقوم الشركات بتحديث اهتماماتها باستمرار من خلال أفعال أصدقاء ومعارف حقيقين وكذلك الشخصيات النموذجية الإلكترونية الأخرى المشابهة وهي شخصيات قد لا نعرفها ولكن نتشارك معهم في نفس الاهتمامات والسلوك في الإنترنت. تبني المواقع نماذج احصائية دقيقة تتوقع الاشياء التي يريدها الشخص من مشتريات وكلمات بحث وغيرها.

أما ملفات تعريف الارتباط (الكوكيز) هي ملفات نصية صغيرة تقوم المواقع الإلكترونية بتخزينها على جهاز المستخدم لتذكر بعض المعلومات أو تتبع أنشطته. تحفظها المواقع في أجهزة المستخدمين بهدف واضح مثل سلة المشتريات ومعلومات الدخول ونماذج التفاعل هي محصورة للموقع فقط الذي نتعامل معها. ولكن توجد ملفات كوكيز للتعرف على سلوك زوار المواقع.

ويمكن لأطراف ثالثة الوصول إلى المعلومات المخزنة في ملفات تعريف الارتباط (الكوكيز) حسب الظروف والتكوينات المحددة. بينما تضع ملفات تعريف الارتباط من قبل نطاقات أخرى غير الموقع الذي تزوره حاليًا تحت مسمى "ملفات تعريف الارتباط الثالثة".

غالبًا ما تستخدم ملفات تعريف الارتباط الثالثة لأغراض الإعلان والتتبع. يمكن للمعلنين وخدمات التحليل وضع ملفات تعريف الارتباط على عدة مواقع لجمع معلومات حول اهتمامات المستخدمين وأنشطتهم عبر مواقع مختلفة. يمكن استخدام هذه البيانات لتقديم إعلانات مستهدفة أو تحليل سلوك المستخدم.

ومع ذلك، تخضع ملفات تعريف الارتباط الثالثة لعديد من عمليات التنظيم والتشريع. يقوم العديد من متصفحات الويب ولوائح الخصوصية باتخاذ خطوات لتقييد التتبع من قِبَل الأطراف الثالثة وتعزيز خصوصية المستخدم. قامت بعض المتصفحات بتنفيذ ميزات مثل منع التتبع الذكي، وتحسين مراقبة ملفات تعريف الارتباط، أو حتى حظر ملفات تعريف الارتباط الثالثة افتراضيًا.

بالإضافة إلى ذلك، فإن لوائح الخصوصية مثل التوجيه العام لحماية البيانات (GDPR) في الاتحاد الأوروبي وقانون حماية المستهلك في ولاية كاليفورنيا (CCPA) فرضت قيودًا على جمع واستخدام البيانات الشخصية، بما في ذلك ملف تعريف الارتباط.

نتيجة لذلك، يصبح قدرة الأطراف الثالثة على الوصول إلى المعلومات المخزنة في ملفات تعريف الارتباط أكثر تقييدًا. ومع ذلك، من المهم الاطلاع على إعدادات الخصوصية والخيارات المقدمة من متصفح الويب، ومراجعة سياسات الخصوصية للمواقع لفهم كيفية التعامل مع ملفات تعريف الارتباط والتتبع من قِبَل أطراف ثالثة.

إيجابيات وسلبيات تقنيات الذكاء الاصطناعي.

يرتبط مصطلح "الذكاء الاصطناعي بالآلات ككل، ولكن برامج الحاسوب التي يتم تثبيتها على هذه الأجهزة، والتي تتسم بسلوك وخاصيات تقنية تجعلها تحاكي القدرات الذهنية البشرية، وأنماط عملها وهذا الأمر منطقي حيث أن الآلة أو الجهاز نفسه يشابه جسم الإنسان في الوقت الذي يقوم به العقل البشري بكافة الوظائف المتعلقة بالتفكير، اتخاذ القرار وحل المسائل".

ويشهد العالم ثورة جديدة يقودها الذكاء الاصطناعي الذي اتفقت جميع الأبحاث المتخصصة حول تأثيراته على الإنسان ومختلف مجالات الحياة التي تحيط به. ورغم أن البدايات الأولى للذكاء الاصطناعي انطلقت مع منتصف خمسينيات القرن الماضي، إلا أنه وصل إلى مراحل متقدمة في الوقت الحاضر، ويظهر بطرق متعددة وأكثر انتشارا مما نتخيله، وسيستمر في التطور مستقبلا، هذا التطور الذي لا شك ستكون له تأثيرات كبيرة ومختلفة وطنياً ودولياً.

ولا شك أن الكثير من الاختراعات لها جوانب ايجابية وسلبية مثل الجوال والذكاء الاصطناعي وغيرهما.

الكثير من الأفراد لا يدركون سلبيات الذكاء الاصطناعي بكافة مجالاته المستخدمة ومنها انتهاكات الخصوصية

فالواقع أن البيانات في عصرنا الحالي أصبحت ثروة تتسابق لجمعها المؤسسات. ويمكن الاستدلال هنا بتجربة الصين كمثال؛ حيث أن محرك البحث قوقل وبعض وسائل التواصل كالفيسبوك وتويتر محجوبة لديهم، ولديهم حلول ومنصات بديلة صينية لها. ولعل من أهم أسباب الحجب حصول الحكومة على حق الوصول الكامل للبيانات وفرض الشروط والأحكام التي يريدونها.

والمتوقع أن تطبيقات الذكاء الاصطناعي ستستطيع الوصول لأدق المعلومات الشخصية وغير الشخصية وستوظفها على نحو قد يسهم في تقديم معلومات وآراء وأفكار ثرية للفرد نفسه وللمؤسسة وللجهات المهتمة مما يوازي جهودا كبيرة ووقتا طويلا ومالا كثيرا كان يتطلب القيام به للوصول لذلك.

وذلك من الجوانب الايجابية التي ينبغي أن نُغَلبها حتى نتوقع من الذكاء الاصطناعي أن يقدم للإنسان حين يتعامل مع بياناته الشخصية الكثير من المنجزات الايجابية الجيدة والمفيدة. حتى وإن تزامن معها بعض السلبيات.

وللأسف أن كثير من المنصات المعروفة تستخدم ما يسميه القانونيين عقود الاذعان مستغلة شهرتها وارتباط الشعوب بها فتجد نفسك توافق بمضض على شروطهم.

والملاحظ أن انتهاك الخصوصية بدأ يتسع بشكل كبير بعد انتشار تقنية الذكاء الاصطناعي خاصة تقنية بصمة الوجه التي تستخدمها الصين وإيران وغيرها من الانظمة التسلطية. في الصين مثلًا لديهم قواعد معلومات تضم عشرات الملايين من بصمات الوجه لمتابعة أفراد المجتمع والتعرف على ادق تفاصيلهم. وتستخدم بكثرة في إقليم شينجيانغ الأويغوري في الصين لمتابعة المسلمين ومساجدهم وتحركاتهم. وفي إيران (باستخدام التقنية الصينية) تستخدم الكاميرات الذكية بصمة الوجه عن بعد للتعرف على من لا ترتدي الحجاب لإنذارها ومعاقبتها. وعادة تستخدم بيانات صور الوجه في الهوية الوطنية المخزنة لدى الحكومات لبناء ملفات لبصمات الوجه ليسهل التعرف على المُستهدف. وهناك أبعاد اخرى لبصمة الوجه من خلالها يتم تصنيف المستهدفين عرقيا وجندريا... الخ؛ مما دفع ببعض الجمعيات الحقوقية الدولية للاعتراض على استخدامها حيث يرون أنها تشجع على إثارة العنصرية ضد الأقليات والملونين. وذكرت دراسة سرية أمريكية تسربت معلوماتها أن الاستخبارات الأمريكية خزنت ٩٢ مليون رقم جوال باكستاني وجمعت معلومات عنهم ووجدت من خلال تحليل بياناتهم أن حوالي 15 ألف باكستاني منهم يحملون أفكار متطرفة وذلك من خلال مؤشرات وضعوها للتعرف على من هو المتطرف من غير المتطرف.

آليات التعامل القانونية مع تقنيات الذكاء الاصطناعي.

وصلت المملكة في ظل توجهات قيادتنا الحكيمة والرؤية المباركة إلى تحقيق طفرات في التقدم التقني والنضوج المعلوماتي، رغم تأخر العديد من دول الجوار في هذا الجانب. كما أن وجود اتفاق إقليمي على مستوى منطقتنا العربية أو الخليجية سيسهم ايجابا بلا شك في عمل التنظيمات والتشريعات في مجال البيانات والذكاء الاصطناعي.

إلا أنه وفي ظل التسارع في استخدامات تقنيات الذكاء الاصطناعي في مختلف المجالات لا مناص من رؤية تضع بعين الاعتبار سن قوانين وأنظمة تضبط عملية الاستفادة من المعلومات الخاصة في سبيل التقليل من المخاطر والتحديات المصاحبة لتبادل البيانات واستخدامها بالاستعانة بتقنيات الذكاء الاصطناعي وذلك لضمان كفاءة استغلال الجهود المبذولة في هذا المجال وتعزيز مخرجاته بمستوى يوازي تسارع الدول المتقدمة.

ويلاحظ أن كثير من فقرات ومواد نظام جرائم المعلوماتية وما شابهها تحتوي على عقوبات مغلظة بهدف الردع وتترك للقاضي تقدير ما يوقعه من عقوبة حسب ملابسات الجريمة ... فمثلا (سجن سنتين وغرامة ٥ مليون ريال) قد لا تطبق الا في حالات نادرة لكن وجودها في يد القاضي تجعل المقدم على الجريمة يفكر كثيرا قبل ارتكابها ... والمشكلة أن مثل هذه الجرائم عابرة للحدود فالمطلوب تعزيز وسائل متابعة مجرمي المعلوماتية من خلال الاتحاد الدولي للاتصالات مثلًا.

ومن ناحية أخرى فإنه مهما كانت القيود على البيانات واستخدامها سننجح في السيطرة على آلية استخدامها، الدور الرئيسي يعتمد على خلفية الفرد ومدى قدرته على حماية بياناته وطريقة تمييز المعلومات الحقيقية من المزيفة. كذلك فإن الشفافية ممن يجمع البيانات قد تساعد بطريقة غير مباشرة في رفع وعي الأفراد في الحفاظ على بياناتهم ومدى مشاركتها مع من يطلبها.

ومن ثم فهناك حاجة لتثقيف الأفراد والجهات على حد سواء فيما يخص تعريف "ماهية البيانات الشخصية"؛ فمثلا وظيفة الشخص أو مدينة العيش هل يعتبر ذلك بيانات شخصية وهل تلك البيانات مساوية لحساسية رقم الهاتف وتاريخ الميلاد الخ. بجانب تفعيل الحوكمة خاصة في المنصات والمواقع التي تتعامل مع البيانات الشخصية.

لكن ما يزيد من صعوبة تطبيق القوانين الحاكمة لبرامج الذكاء الاصطناعي هو عدم أهمية المعلومة الفردية. فمعلومات الشخص وما انتجه من محتوى ليست مهمة بحد ذاتها ويمكن شطبها من الأنظمة التي تستخدمها بدون أن تتأثر جودتها ودقة نتائجها. فأنظمة الذكاء الاصطناعي تبحث عن المعلومات الجماعية الضخمة؛ لذا فبعض بنود قوانين وضوابط أنظمة الذكاء الاصطناعي لا تعالج الضرر الفردي وانما تعاقب الشركة على السلوك الخاطئ لجمع واستخدام المعلومات.

وتجدر الإشارة إلى أنه في عام 2018، بدأ الاتحاد الاوربي بتطبيق القانون العام لحماية البيانات للاتحاد الأوروبي، ما أدى إلى تغيير جذري في الطريقة التي تتعامل بها الشركات مع بيانات المستخدمين، مع فرض غرامات ضخمة جداً على الشركات التي تنتهك القواعد. اضافة إلى تنظيم جديد يلزم كبريات الشركات بمراقبة المحتوى بجدية وعدم التهاون مع مثيري الكراهية وناشري المعلومات الزائفة وغيرهم، وإلا تعرضوا لعقوبات شديدة. وكذلك يعملون الآن على تطوير بعض القوانين بحيث تكون أكثر شمولية بشأن تنظيم عملية الذكاء الاصطناعي. ولعل الجهات المختصة في المملكة تستفيد بشكل كبير من هذه التنظيمات حول المعلومات الرقمية. والمأمول كذلك أن تقوم جامعة الدول العربية بعمل مماثل لما يقوم به الاتحاد الاوربي. خاصة وأن المؤشرات تؤكد أن هناك اهتمام متزايد بالذكاء الاصطناعي من معظم اجهزة الدولة في المملكة.

وبالفعل فإن محاولة وضع قوانين وأنظمة تضبط عملية استغلال المعلومات الخاصة قد يقلل من كثير من السلبيات والمخاطر

لكن ما ينبغي إدراكه أننا اليوم نعيش في وسط تقنيات نستخدمها مجانا وهي تقوم على فكرة توظيف هذه المعلومات والبيانات لأغراض ومصالح ونحن نوافق على ذلك من حيث ندري ومن حيث لا ندري؛ بل إن الصراع القائم اليوم بين مُصنعي أجهزة الهواتف والألواح الذكية وبين مختلف التطبيقات هو صراع من أجل الاستحواذ على طبيعة محتوى كعكة هذه المعلومات. ولعل التحديات ستكون أشد بالنسبة لمختلف تقنيات الذكاء الاصطناعي الذي يبدو أن كثيرا من معطياته تذهب باتجاه استغلال كل البيانات والمعلومات واستثمارها وبيعها وتوزيعها.

وتوجد في المملكة جهات تتولى التصدي لهجمات المخترقين لأجهزة وأنظمة الدولة والبنية التحتية لتقنية المعلومات. وقد يكون من المناسب أن تعمل هذه الجهات على تنظيم جمع البيانات من المملكة بحيث تحقق التوازن بين الاستفادة من أنظمة تقنية المعلومات الدولية مع الحفاظ على خصوصية بيانات المواطن السعودي.

نظام حماية البيانات الشخصية السعودي وتقنيات الذكاء الاصطناعي.

صدر نظام حماية البيانات الشخصية في المملكة العربية السعودية، بموجب بالمرسوم الملكي رقم (م/19) وتاريخ 9/2/1443هـ، ومن أبرز ما تضمنه النظام : (نطاق تطبيق النظام، عدم إخلال أحكام النظام مع أحكام أنظمة أخرى، حقوق صاحب البيانات الشخصية، معالجة البيانات الشخصية أو تغيير الغرض من معالجتها، اختيار جهة المعالجة، تحديد مدد لممارسة حق الوصول إلى البيانات، جمع البيانات، محتوى البيانات، إتلاف البيانات، اعتماد سياسة لخصوصية البيانات، وسائل وعناصر جمع البيانات، الإفصاح عن البيانات، تعديل وتحديث البيانات، الاحتفاظ بالبيانات، المحافظة على البيانات، تسرب أو تلف البيانات، تقويم آثار معالجة البيانات، معالجة البيانات الصحية والائتمانية، وسائل الاتصال الشخصية، تصوير الوثائق الرسمية، نقل البيانات، جهة إشراف تطبيق النظام، سجلات البيانات، إنشاء بوابة إلكترونية، الشكاوى، المخالفات والعقوبات، لجنة نظر المخالفات، ضبط المخالفات، المحافظة على أسرار البيانات، إصدار اللوائح، النشر والنفاذ).

وقد أوضحت المادة الثانية من نظام حماية البيانات الشخصية السعودي أن النظام "يُطبق على أي عملية مُعالجة لبيانات شخصية تتعلق بالأفراد تتم في المملكة بأي وسيلة كانت، بما في ذلك معالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة بأي وسيلة كانت من أي جهة خارج المملكة. ويشمل ذلك بيانات المتوفى إذا كانت ستؤدي إلى معرفته أو معرفة أحد أفراد أُسرته على وجه التحديد. كما يُستثنى من نطاق تطبيق النظام، قيام الفرد بمعالجة البيانات الشخصية لأغراض لا تتجاوز الاستخدام الشخصي أو العائلي، ما دام أنه لم ينشرها أو يفصح عنها للغير. وتحدد اللوائح المقصود بالاستخدام الشخصي والعائلي المنصوص عليهما". ووفقاً للمادة الرابعة "يكون لصاحب البيانات الشخصية - وفقاً للأحكام الواردة في النظام - الحقوق الآتية:

- الحق في العلم، ويشمل ذلك إحاطته علماً بالمسوغ النظامي أو العملي المعتبر لجمع بياناته الشخصية، والغرض من ذلك، وألَّا تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها أو في غير الأحوال المنصوص عليها في المادة (العاشرة) من النظام.
- الحق في وصوله إلى بياناته الشخصية المتوافرة لدى جهة التحكم، ويشمل ذلك الاطلاع عليها، والحصول على نسخة منها بصيغة واضحة ومطابقة لمضمون السجلات وبلا مقابل مادي -وفقاً لما تحدده اللوائح- وذلك دون إخلال بما يقضي به نظام المعلومات الائتمانية فيما يخص المقابل المالي، ودون إخلال بما تقضي به المادة (التاسعة) من النظام.
- الحق في طلب تصحيح بياناته الشخصية المتوافرة لدى جهة التحكم، أو إتمامها، أو تحديثها.
- الحق في طلب إتلاف بياناته الشخصية المتوافرة لدى جهة التحكم مما انتهت الحاجة إليه منها، وذلك دون إخلال بما تقضي به المادة (الثامنة عشرة) من النظام.
- الحقوق الأخرى المنصوص عليها في النظام، التي تُبينها اللوائح".

بينما أشارت المادة السابعة والعشرون من نظام حماية البيانات الشخصية إلى أنه "يجوز جمع البيانات الشخصية أو مُعالجتها لأغراض علمية أو بحثية أو إحصائية دون موافقة صاحبها، في الأحوال الآتية:

1-إذا لم تتضمن البيانات الشخصية ما يدل على هوية صاحبها على وجه التحديد.

2-إذا كان سَيُجرى إتلاف ما يدل على هوية صاحب البيانات الشخصية على وجه التحديد خلال عملية مُعالجتها وقبل الإفصاح عنها لأي جهة أُخرى ولم تكن تلك البيانات بيانات حساسة.

3-إذا كان جمع البيانات الشخصية أو معالجتها لهذه الأغراض يقتضيها نظام آخر أو تنفيذاً لاتفاق سابق يكون صاحبها طرفاً فيه".

والواقع أن استخدام المعلومات الشخصية مسألة أخلاقية حساسة سواءً كانت في الذكاء الاصطناعي أو غيره. وضابط هذه المسألة هو رادع الخُلُق أو رادع السلطان (الخوف من إيقاع عقوبة النظام). ويجب على الأفراد أو المنظمات المعنية بجمع واستخدام معلومات الأشخاص في الذكاء الاصطناعي أن تكون شفافة بشأن الأغراض التي تستخدم فيها هذه المعلومات وطرق جمعها ومعالجتها. ويفترض أن يكون هناك أيضًا إعلان مسبق للمستخدمين قبل جمع معلوماتهم الشخصية.

وتجدر الإشارة إلى أن نظام حماية البيانات الشخصية السعودي لا يعالج كثير من المعلومات التي يتطوع الشخص لنشرها في الإنترنت مثل المقالات والتغريدات والتي تستخدم في تدريب أنظمة الذكاء الاصطناعي، ومثل عادات الشراء التي يمارسها الشخص في مواقع التجارة الإلكترونية. ومؤخرًا ظهرت قضية جديدة وهي من يملك نبرة الصوت؟ فقد ظهرت مقاطع صوتيه تم عملها من خلال برامج ذكاء اصطناعي لشخصيات مشهورة منها الشيخ ابن باز رحمه الله ومحمد عبده وغيرهم.

التوصيات

1-وضع قيود تنظيمية على تقنية الذكاء الاصطناعي، لحماية الوطن والمجتمع مستقبلا من مخاطر إساءة استخدام أدوات الذكاء الاصطناعي. (سدايا + مجلس الشورى).

2-تعزيز "الشفافية" لأنظمة الذكاء الاصطناعي والتأكيد على أن البيانات المخصصة لهذه التقنية تُجمع وتُستخدم ويتم تشاركها وتخزينها وحذفها بطرق تتوافق مع حقوق الأفراد وخصوصيتهم وفرض عقوبات وغرامات على المخالفين كما هو معمول بالاتحاد الأوروبي (مجلس الشورى + المركز الدولي لأبحاث وأخلاقيات الذكاء الصناعي+ سدايا).

3-سن قوانين لمحاسبة شركات الذكاء الاصطناعي وإخضاعها للوائح التنظيمية التي تسنها الجهات الحكومية لضمان خصوصية البيانات. (سدايا + مجلس الشورى).

4-دعم المبادرات الدولية لتنظيم وتطوير الذكاء الاصطناعي واستخداماته عالمياً من خلال إنشاء هيئة رقابة دولية للذكاء الاصطناعي على غرار الوكالة الدولية للطاقة الذرية والدعوة لإنشاء منظمة اقليمية لمنطقتنا. (وزارة الخارجية، سدايا).

5- الاستفادة من بيانات الأفراد الضخمة لأغراض التسويق والتجارة مع الأخذ بعين الاعتبار مخاطر هذه البيانات على السلم الاجتماعي ويمكن أن يكون ذلك من خلال تعهد الجهات بعدم استخدام معلومات العميل الخاصة.

6-تعزيز وسائل تتبع الهاكرز ومرتكبي الجرائم المعلوماتية من خلال المنظمات الدولية المعنية مثل الاتحاد الدولي للاتصالات. ITU

المصادر والمراجع

1. HTTPS://WWW.TECHTARGET.COM/SEARCHDATAMANAGEMENT/TIP/5-BENEFITS-OF-BUILDING-A-STRONG-DATA-GOVERNANCE-STRATEGY
2. HTTPS://WWW.TECHTARGET.COM/SEARCHDATAMANAGEMENT/TIP/DEVELOPING-AN-ENTERPRISE-DATA-STRATEGY-10-STEPS-TO-TAKE
3. HTTPS://WWW.TECHTARGET.COM/SEARCHDATAMANAGEMENT/TIP/6-KEY-COMPONENTS-OF-A-SUCCESSFUL-DATA-STRATEGY
4. HTTPS://DISCOVERY.UCL.AC.UK/ID/EPRINT/1471258/1/ACCESS%20TO%20INFORMATION-RT-SHEPHERD42015-FINAL%20(2).PDF
5. HTTPS://WWW.STATISTA.COM/OUTLOOK/TMO/ARTIFICIAL-INTELLIGENCE/WORLDWIDE#MARKET-SIZE

6-نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 9/2/1443هـ.

7-عبدالحميد، عائشة. (2023). الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي. مجلة الباحث للدراسات القانونية والقضائية، ع 50، 21 - 42 .

8-العلوي، سكينة الأمراني، والتوزاني، محمد. (2023). مستقبل الذكاء الاصطناعي: الميتافيرس نموذجا. مجلة القانون والأعمال، ع 88، 256 - 278 .

9-أحمد، كريمة محمود محمد وآخرون. (2023). الذكاء الاصطناعي وتطبيقاته المعاصرة. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، مج 3، ع 2، 297 - 301 .

10-الطيبي، محمود. (2023). الذكاء الاصطناعي وتحديات الأسس المفاهيمية للقانون: رؤى استشرافية لإعادة النظر في النظام القانوني. مسارات في الأبحاث والدراسات القانونية، ع 29، 112 - 129 .

المشاركون.

- **الورقة الرئيسة**: د. عبدالعزيز الحرقان
- **التعقيب الأول**: د. عبدالعزيز الباتلي
- **التعقيب الثاني**: د. علي الوهيبي
- **إدارة الحوار**:د. علي الوهيبي
- **المشاركون بالحوار والمناقشة**:

-أ. أحمد المحيميد
-د. أماني البريكان
-د. خالد المنصور
-معالي د. عبدالإله الصالح
-د. عبدالرحمن العريني
-د. عبدالرحمن الهدلق
-د. عبدالعزيز العثمان
-أ. فائزة العجروش
-أ. فهد الأحمري
-م. محمد المعجل
-د. مساعد المحيا

*ترتيب الأسماء حسب الحروف الأبجدية

ملتقى أسبار

إحدى مبادرات مركز أسبار

تأسس الملتقى في 28 يونيو 2015م

@MultaqaAsbar

@Multaqa_Asbar

https://cutt.us/U0nnC

00966114624229

www.asbar.com