جامعة عبد الرّحمان ميرة-بجاية
كلية الحقوق والعلوم السياسية
قسم القانون الخاص

الذكاء الاصطناعي وحماية الحياة الخاصة للأفراد

مذكرة تخرج لنيل شهادة الماستر في الحقوق

تخصص: المهن القانونية والقضائية

من إعداد الطالبتين

- دعاشي شيماء
- أوتمزابت نسرين

تحت إشراف الدكتور

- اوسيدهم يوسف

أعضاء لجنة المناقشة:

_ الأستاذ: أوسيدهوم يوسف.....مشرفا و مقرار

_الأستاذة: عشاش حفيظة.....رئيسة

_الأستاذة: إخلف سامية.....ممتحنة

السنة الجامعية:2025/2024

كلمة شكر وعرفان

"من لا يشكر الناس لا يشكر الله"

قال رسول الله صلى الله عليه وسلم:

(صنع إليكم معروفا فكافأوه، فإن لم تجدوا ما تكافئونه فادعوا له حتى ترو أنكم كافأتموه...)

أجمل عبارات الشكر والتقدير تسبق حروفا وتنهي سطورنا معبرة عن صدق المعاني النابعة من قلوبنا أخص بها الدكتور أوسيدهم يوسف على خدماته واستشاراته الطيبة حيث جمع بين الإنسانية والاحترافية في أفضل صورة

أسأل الله أن يبارك لك في علمك ويزيدك من فضله وأن ينعم عليك بالصحة والعافية.

الإهداء:

*إلى **والديّ** العزيزين، اللذين سخروا حياتهم لأجلي، أرفع إليكما أسمى عبارات الشكر والامتنان. بفضل محبتكما ودعمكما الغير محدود، استطعت أن أحقق أحلامي وأصبح أفضل نسخة من نفسي. أنتما النور الذي ينير طريقي، وأتمنى دائما أن أكون مصدر فخر لكما.*

*إلى **إخوتي** الأحباء، أنتم رفاق مغامراتي و ضحكاتي. شكرا لكم على اللحظات الجميلة التي قضيناها معا، وعلى الدعم الذي تقدموه لي في كل مناسبة. في سعادة كل واحد منكم فرحتي، و أتمنى أن تبقى روابطنا قوية دائما.*

*إلى **أخي** العزيز، الذي دائما كان لي الصديق والسند، شكرا لك على كل نصيحة، وكل ضحكة، وكل لحظة تبادلنا فيها الأحاديث. أنت جزء من عالمي، وأتمنى لك كل النجاح والسعادة في حياتك.*

*إلى **صديقاتي** الغاليات، اللاتي لا تقدر صداقتهن بثمن، شكرا لكن على الوفاء والدعم والدردشات الليلية التي لا تنسى. أنتم الأمان في أوقات الضعف و الفرح في أوقات السعادة. أفتخر بكوني جزءا من حياتكن.*

*وأخيرا إلى **خطيبي** الحبيب، الذي ملأ حياتي بالحب والجمال، شكرا لك على وقوفك بجانبي، و على كل لحظة تشاركناها معا. أنت توأم روحي، و أتطلع لمستقبل مشرق نبنيه معا.*

شيماء

الإهداء:

الحمد لله حبا وشكرا وامتنانا على البدء والختام. هنا أنا اليوم أقف على عتبة تخرجي أقطف ثمار تعبي وأرفع قبعتي بكل فخر، فالهم لك الحمد قبل أن ترضى ولك الحمد إذا رضيت ولك الحمد بعد الرضا، لأنك وفقتني على إتمام هذا النجاح وتحقيق حلمي.

و بكل حب أهدي ثمرة نجاحي و تخرجي:

*إلى الذي زين اسمي بأحلى الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل إلى من علمني أن الدنيا كفاح وسلاحها العلموالمعرفة، فخري اعتزازي: "***والدي***".*

*إلى من جعل الجنة تحت أقدامها، واحتضنني قلبها قبل يديها وسهلت لي الشدائد بدعائها، إلى القلب الحنون والشمعة التي كانت لي في الليالي المظلمات، سر قوتي ونجاحي جنتي:"***والدتي***".*

*إلى من ساندوني بكل حب رزقني الله بهم لأعرف من خلالهم طعم الحياة الجميلة، و بوجودهم أكتسب قوة و محبة لا حدود لها:"***أخي***"و"***إخوتي***".*

*إلى من أمدني بالقوة والتوجيه آمن بي ودعمني في الأوقات الصعبة لأصل إلى ما أنا عليه الآن:"***خطيبي***".*

و أخيرا إلى زميلتي التي تشاركنا لحظات التعب و الفرح طيلة هذا العمل.

نسرين

قائمة أهم المختصرات:

أولا: باللغة العربية:

ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية.

د.س.ن: دون سنة النشر.

ص: صفحة.

ص.ص: من الصفحة إلى الصفحة.

ثانيا: باللغة الفرنسية:

IP : InternetProtocol.

AI : Artificiel Intelligence.

CNIL : La Commission National Française et L'informatique et des Libertés.

GDPR: General Data Protection Regulation.

LIL : Loi Informatique et Libertés.

P : page

Op.cit. :opere citato

مقدمة

تعتبر تكنولوجيا الذكاء الاصطناعي intelligence artificielle إحدى الابتكارات الرائدة التي تعكس تفاعل التعاون بين الذكاء الاصطناعي ومختلف التخصصات لتطوير العديد من المجالات والقطاعات، مما يساهم في تحقيق الاجتماعية، العلمية والتكنولوجية. حيث يمك للذكاء الاصطناعي أن يتنافس مع الذكاء البشري، وأحيانا يتفوق عليه.

كما يشير مصطلح الذكاء الاصطناعي إلى قدرة الخوارزميات المتطورة على التعلم من البيانات، مما يمكنها من أداء المهام تلقائيا دون الحاجة لبرمجة كل خطوة على حدة من قبل الإنسان، حيث يهدف علم الذكاء الاصطناعي إلى فهم طبيعة الذكاء الإنساني عن طريق عمل برامج للحاسوب الآلي قادرة على محاكاة السلوك الإنساني المتسم بالذكاء[1] على مدار السنوات الماضية، شهدنا تطورات ملحوظة في مجالات التكنولوجيا و المعلومات، مما اثر بشكل ايجابي على العديد من التخصصات. حيث أصبح عالمنا اليوم يتمتع بتقنيات جديدة وابتكارات تكنولوجية متنوعة، حيث أدرك الإنسان بالفعل أن ذكائه هو قوته الرئيسية، والتي يمكن استغلالها في الذكاء الاصطناعي وبالتالي تمثل أحد الركائز الأساسية للتكنولوجيا العصر الحديث مما تظهر الأنظمة الذكية قدرتها على تحسين جودة الحياة وتقديم الدعم للأفراد في مختلف المجالات.

يعتبر الذكاء الاصطناعي ثمرة تجارب وخبرات البشرية، وهو يمثل تحولا جذريا في تاريخ البشرية، حيث يهدف إلى تلبية احتياجات الأفراد من خلال تقديم المعلومات والبرامج المتطورة. تمكن العلماء من تطوير نماذج أولية للذكاء الاصطناعي، ورغم استمرار تطويرها وتحديثها يوميا، إلا أن هذه التقنية تعد قفزة نوعية نحو المستقبل، حيث تحولنا من الطرق التقليدية إلى استخدام البرامج والتقنيات الحديثة.

[1] آلان بونيه، الذكاء الاصطناعي، دار علم المعرفة، الكويت، 1993،ص11.

من جهة أخرى، أثبت الذكاء المن جهة أخرى، أثبت الذكاء الاصطناعي قدرته على إحداث تغيرات ايجابية في العديد من القطاعات بما في ذلك التعليم، التوظيف، الصحة...الخ. كما يساهم في حل المشكلات وتعزيز الصحة النفسية وبناء علاقات اجتماعية ومهنية ناجحة. ومع ذلك يتطلب الذكاء الاصطناعي وعيا وحذرا، إذ أن له أيضا جوانب سلبية ومخاطر تهدد الخصوصية والأمان الشخصي، مما يستدعي التوازن بين الفوائد والتحديات المحتملة.

ومن جهة يعتمد الذكاء الاصطناعي بشكل أساسي على جمع وتحليل كميات ضخمة من البيانات، غالبا ما تكون بيانات شخصية، يتم استخدامها لتدريب الخوارزميات وتحسين أدائها.

غير أن هذا الاعتماد المكثف على البيانات يثير إشكاليات قانونية وأخلاقية عميقة، تتعلق بمدى احترام الذكاء الاصطناعي لحقوق الأفراد، وعلى رأسها الحق في الخصوصية. إذ يطرح تساءل جدي حول ما إذا كانت هذه التقنيات قادرة على التوفيق بين فعاليتها التقنية من جهة، و حماية الحياة الخاصة للأشخاص من جهة أخرى.

ففي الوقت الذي تستخدم فيه تقنيات الذكاء الاصطناعي لتعزيز الكفاءة و الأمن، تستخدم أيضا لمراقبة الأفراد تتبع تحركاتهم، بل و التنبؤ بسلوكهم، مما قد يؤدي إلى انتهاكات جسيمة للحرية الفردية و الكرامة الإنسانية.

في ضوء ما تقدم نطرح الإشكالية التالية: الإطار القانوني الذي يأطر الأخطار التي تسبب فيها الذكاء الاصطناعي؟

لإجابتنا على هذه الإشكالية، سيتم تقسيم هذا البحث إلى فصلين رئيسيين:

. في الفصل الأول، سنقوم بتحليل كيف يمكن للذكاء الاصطناعي أن يمثل تهديدا فعليا للخصوصية، من خلال تسليط الضوء على آليات جمع البيانات والمراقبة والخوارزميات المعتمدة.

. أما في الفصل الثاني، فسنناقش السبل القانونية والتقنية والأخلاقية الكفيلة بضمان استخدام الذكاء الاصطناعي بطريقة تحترم الخصوصية وتحد من مخاطره.

الفصل الأول

الذكاء الاصطناعي كعامل تهديد متزايد للخصوصية

يعتبر الذكاء الاصطناعي فرعا من العلوم يسعى إلى تمثيل القدرات البشرية في الآلات والحواسيب. فلقد تأسس المجال الحديث للبحث في الذكاء الاصطناعي خلال مؤتمر دارت موث الذي عقد في صيف عام 1956. حيث أصبح العلماء الحاضرون مثل مارفن مينسكي والين نيوويل وهيربرت سايمن، رواد في هذا المجال لعقود قادمة، حيث أسس هؤلاء العلماء مختبرات الذكاء الاصطناعي في معهد ماساتشوستس للتكنولوجيا. [1]

يهدف هذا العلم إلى استكشاف أساليب متقدمة لبرمجة الآلات بحيث تتمكن من أداء مهام واستنتاجات تشابه، حتى و لو بشكل محدود، تلك التي يظهرها الذكاء البشري. وبالتالي يعتبر الذكاء الاصطناعي دراسة تحاول فهم مفهوم الذكاء البشري وتحديد خصائصه،ومن ثم محاولة تقليد بعض جوانبه. يجب التأكيد هنا على أن الهدف ليس مقارنة العقل البشري الذي خلقه الله سبحانه و تعالى بالآلة التي صنعها الإنسان، بل فهم العمليات التي يقوم بها العقل البشري عند ممارسة التفكير، و ترجمة هذه العمليات الذهنية إلى ما يعادلها من عمليات حاسوبية تعزز قدرة الحواسيب على معالجة المشكلات المعقدة.[2]

حيث يقسم الذكاء الاصطناعي إلى نوعين، النوع الأول هو الذكاء الاصطناعي الضعيف الذي يركز على مجموعة من المهام المحددة والضيقة كالطائرة ذاتية القيادة، أي بمعنى آخر أن

---

[1] حيدة سعاد، استخدام الذكاء الاصطناعي في تحسين عملية اتخاذ القرار في المؤسسة الاقتصادية، مذكرة لنيل شهادة الماستر، تخصص إدارة أعمال، كلية العلوم الاقتصادية ، التجارية و علوم التسيير جامعة أحمد دراية، الجزائر، 2020، ص.ص06-09.

1جوزي نور الهدى ،**أثر تطبيق الذكاء الاصطناعي و الذكاء العاطفي على جودة اتخاذ جودة القرار**،مذكرة لنيل شهادة الماستر تخصص : إدارة الأعمال قسم علوم التسيير، كلية العلوم الاقتصادية و التجارية و علوم التسيير، جامعة ابن خلدون، تيارت،2022، ص2.

تكون مبرمجة وفق نظام ثابت من طرف الإنسان. و النوع الآخر هو الذكاء الاصطناعي القوي و الذي يعرف باسم الذكاء العام الاصطناعي و يعد هذا النوع قادرا على أداء معظم الوظائف المعرفية التي قد يمتلكها الإنسان.[3]

بناءا على ما سبق سنحاول إبراز أهم المفاهيم الأساسية للذكاء الاصطناعي وتأثيره على الحياة الخاصة للأفراد، حيث قسمنا هذا الفصل إلى مبحثين وهما:

*المبحث الأول: جمع ومعالجة البيانات الشخصية في عصر الذكاء الاصطناعي.

*المبحث الثاني: نماذج واقعية تظهر التهديد على الخصوصية.

[3] نور محمد عبد الله العزام، **دور الذكاء الاصطناعي في رفع كفاءة النظم الإدارية لإدارة الموارد البشرية**، المجلة التربوية، العدد04، كلية التربية، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية، 2021، ص11.

المبحث الأول

جمع ومعالجة البيانات الشخصية في عصر الذكاء الاصطناعي

تنص المادة الثانية من القانون الفرنسي رقم 78-17، المعدل بموجب القانون رقم 2004-801، المتعلق بحماية البيانات الشخصية، على تعريفات واضحة لمصطلح البيانات الشخصية. وفقا لهذا القانون ذكرت أنه **"يعتبر بيانا شخصيا كل معلومة تتعلق بشخص طبيعي محدد هويته أو من الجائز تحديد هويته بصورة مباشرة أو غير مباشرة ، و سواء تم ذلك من خلال الرجوع إلى الرقم القومي أو بالرجوع لأي شخص يخصه."**[4]

المطلب الأول

مركزية البيانات الشخصية في عمل الذكاء الاصطناعي

تعتبر دراسة موضوع الحماية القانونية من القضايا الهامة والمعقدة التي أثارة جدلا في المجال القانوني. لقد جذبت هذه المسألة اهتمام الفقهاء ورجال القانون نظرا لاتصالها الوثيق بالحقوق والحريات، حيث تعد من الحقوق الأساسية المتعلقة بالإنسان. في السنوات الأخيرة، شاهد هذا الحق العديد من الانتهاكات المتنوعة، سواء من قبل الأفراد أو الجهات الرسمية. مع التقدم السريع والواسع في وسائل الإعلام والاتصال الحديثة، أصبح الحق في حرمة الحياة الخاصة أكثر عرضة للاختراق والانتهاك. مما أدى إلى تحديد أهم العناصر و الطبيعة القانونية للحق في الحياة الخاصة للأفراد.[5]

---

[4] وفاء حلمي السعيد، **تقنية الذكاء الاصطناعي وحماية البيانات الشخصية**، مجلة الشريعة والقانون، العدد43، كلية الشريعة والقانون، جامعة الأزهر، القاهرة، 2024، ص1402.

[5] عثماني رجاء، الحماية القانونية للحق في حرمة الحياة الخاصة، مذكرة لنيل شهادة الماستر، تخصص قانون عام، كلية الحقوق، جامعة بلحاج بوشعيب، عين تيموشنت،2023.

تقدم المادة الأولى من القانون المصري [6]المتعلق بحماية البيانات الشخصية مشيرة إلى أنها تشمل "أي معلومات تتعلق بشخص طبيعي، أو يمكن تحديد هويته بشكل مباشر أو غير مباشر من خلال ربط هذه المعلومات مع بيانات أخرى مثل الاسم، الصوت، الصورة، رقم التعريف، أو محدد الهوية على الانترنت، بالإضافة إلى أي معلومات تتعلق بالهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية."

من المهم أن نلاحظ أن الحماية القانونية الممنوحة للبيانات الشخصية تقتصر على بيانات الأفراد الطبيعيين، بينما تستثنى البيانات المتعلقة بالشخصيات الاعتبارية من هذا الإطار القانوني.[7]

الفرع الأول: تعريف البيانات الشخصية

اعتمد القانون الفرنسي تعريفا للبيانات الشخصية يتضمن معيارا يمكن استخدامه لتحديد ما إذا كانت المعلومات المتعلقة بشخص معين تعتبر بيانات شخصية، وبالتالي هل تستحق الحماية القانونية التي أقرها المشرع الفرنسي.

من هنا، يصبح من الصعب تحديد أشكال البيانات الشخصية المختلفة بشكل مسبق، حيث من المتوقع أن تظهر في المستقبل أنواع جديدة من المعلومات يمكن اعتبارها بيانات شخصية. على سبيل المثال، يعتبر عنوان بروتوكول ال انترنت(IP) المستخدم في الكمبيوتر الشخصي أحد هذه البيانات الشخصية، وهو ما لم يكن معروفا سابقا ولم يكن يعتبر ضمن فئة البيانات الشخصية.

وبناء على ذلك، لا يمكن حصر أنواع البيانات الشخصية بشكل قاطع، إذ توجد العديد من الأمثلة التي يمكن تبرز هذا التوسع في التعريف. وعليه، فإن الحماية القانونية المقررة للبيانات

[6] القانون رقم 151 مؤرخ في 10 جويلية 2020، يتضمن حماية البيانات الشخصية، ج.ر، عدد28، المؤرخ في 15 يوليو 2020.
[7] وفاء حلمي السعيد، مرجع سابق، ص، ص1403-1404.

الشخصية قد تشمل مجموعة واسعة من المعلومات، ويجب أن تحترم قانونيا، بما في ذلك البيانات التالية التي يجب أن تعتبر بيانات شخصية وتستحق الحماية.

أولا: البيانات التعريفية

1_**الاسم:** يعتبر الاسم وسيلة رئيسية لتميز الأفراد عن بعضهم البعض، ويمكن تصنيفه إلى ثلاثة أنواع: الاسم الأصلي، اسم الشهرة، والاسم المستعار.

فالاسم الأصلي هو الاسم الذي يتم ذكره في شهادة الميلاد وبطاقة الهوية، ويظهر في المعاملات الرسمية. بينما اسم الشهرة هو الاسم الذي يستخدم بشكل شائع بين الناس ويختلف عن الاسم الأصلي، ولا يمكن إدراجه في الوثائق الرسمية مثل شهادة الميلاد أو بطاقة الهوية. أما الاسم المستعار فهو اسم يتبناه الشخص لأغراض مهنية أو فنية أو أدبية، ويستخدم عادة لإخفاء هويته الحقيقية. بالإضافة إلى ذلك، يشير اللقب إلى اسم العائلة الذي ينتمي إليه الشخص. كما اتفق كافة التشريعات المعنية بحماية البيانات الشخصية على أن الاسم و اللقب يعتبران من البيانات الشخصية التي تستوجب الحماية القانونية[8].

2_**العنوان:** يعتبر العنوان، سواء كان عنوان السكن أو عنوان العمل أو عنوان مكان قضاء العطلات، من البيانات الشخصية المحمية بموجب القوانين المعنية بحماية البيانات.

3_**الرقم الشخصي:** يعد الرقم الشخصي الذي يمنح لكل فرد من البيانات الشخصية التي تميزه وتحدد هويته. على سبيل المثال، الرقم القومي هو رقم فردي يعطى لكل شخص ضمن الدولة وينطبق

[8] وفاء حلمي السعيد، مرجع سابق، ص. ص.1404-1406.

ذلك أيضا على الرقم التأميني، والذي يشير إلى رقم التأمين الاجتماعي الخاص بالفرد. بالإضافة إلى ذلك، تشمل هذه المعايير رقم التأمين الصحي ورقم الاشتراك في وسائل المواصلات، طالما أن هذه الأرقام تخص الشخص بشكل حصري وغير قابلة للتكرار.

4_**الصورة والصوت:** تعتمد الحماية القانونية للبيانات المتعلقة بالصورة والصوت على التوجيه الأوروبي بشأن حماية البيانات الشخصية الصادرة في 24 أكتوبر 1990، والذي جاء قبل قانون حماية البيانات الفرنسي ، في حين أن القضاء المدني الفرنسي قد أقر منذ زمن بعيد حق المرء في صورته.[9] يعتبر اعتبار صورة الفرد و صوته كبيانات شخصية مفهوما حديثا[10]، حيث كان نطاق البيانات الشخصية في السابق يقتصر على البيانات الأساسية مثل الاسم و اللقب و العمر و المهنة[11].

ثانيا: البيانات الشخصية

1_**الحالة الصحية:** تعتبر الحالة الصحية من البيانات الشخصية المحمية قانونيا وفقا لما نص عليه في المادة 7[12] من قانون حماية البيانات الشخصية الفرنسي. قبل التعديلات التي أدخلت على هذا القانون، لم يكن يتم تصنيف المعلومات المتعلقة بالحالة الصحية كبيانات شخصية. ولكن، أدى

[9] Levasseur : Protection de la Personne de L'image, p.71

[10] أشرف توفيق شمس الدين، الصحافة والحماية الجنائية للحياة الخاصة (دراسة مقارنة)، دار النهضة العربية، جمهورية مصر العربية،2008، ص. 71.

[11] وفاء حلمي السعيد، مرجع سابق، ص.1405 .

[12]Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.18

تدخل اللجنة الوطنية للحريات الفرنسية إلى اعتبار المعلومات الخاصة بالحالة الصحية بيانات شخصية تستحق الحماية القانونية.

2_**الآراء السياسية والمعتقدات الدينية:** وفقا لما تنص عليه المادة 8 من قانون حماية البيانات الشخصية الفرنسي، تعتبر كافة المعلومات المتعلقة بالآراء السياسية والدينية بيانات شخصية محمية قانونا. كما ينطبق نفس الحكم على البيانات المرتبطة بالانتماءات النقابية للأفراد.

3_**رقم الهاتف:** يعتبر رقم الهاتف الخاص بأي فرد، سواء كان رقم هاتف منزلي أو رقم هاتف محمول، من البيانات الشخصية المحمية بموجب القانون.

4_**عنوان البريد الإلكتروني:** كل فرد لديه بريد إلكتروني على الانترنت، ويعتبر هذا العنوان الالكتروني المستخدم لإرسال و استقبال الرسائل الالكترونية بيانا شخصيا مستوجبا للحماية القانونية[13].

ومن المهم الإشارة إلى أن ما ذكر سابقا يمثل مجرد أمثلة لتوضيح بعض البيانات الشخصية وفقا للتعريف الحديث الذي اعتمده القانون الفرنسي. فهذه المعايير قابلة للتطبيق على أنواع أخرى من البيانات التي لم تذكر سابقا، وقد تظهر بمرور الوقت نتيجة للتغيرات الاجتماعية والاقتصادية.

لذا يعتبر تاريخ ميلاد الفرد، مهنته، وعنوانه البريدي العادي، من البيانات الشخصية المحمية قانونا، وينطبق نفس الأمر على رقم الفاكس ورقم البطاقة الائتمانية. بالإضافة إلى ذلك فإن هوايات

[13]Baffard William, op.cit. p.15

الفرد، و سلوكه، وضعه المالي، و علاقاته الأسرية تعتبر أيضا بيانات شخصية، حتى ولو كانت حماية هذه البيانات تتم بشكل غير مباشر، مماثلة لبيانات تحمل دلالات مباشرة.[14]

الفرع الثاني: مصادر البيانات الشخصية

في عصر الثورة الرقمية والانفجار لمعلوماتي الذي تشهده المجتمعات اليوم، باتت تكنولوجيا المعلومات تلعب دورا محوريا في بنية هذه المجتمعات. مع هذا التطور تغيرت المفاهيم المتعلقة بخصوصية الحياة الفردية، حيث نشأت جوانب جديدة تتعلق بفكرة الخصوصية، مما يجعل من الضروري إدماج البيانات والمعلومات الشخصية ضمن نطاق الحماية الفردية.

يتعين جمع البيانات الشخصية لأغراض معينة وقانونية، مع ضرورة أن تكون هذه الأغراض مرتبطة بمصالح مشروعة. في البداية تأتي عملية جمع البيانات من الأفراد أنفسهم، حيث غالبا ما تطلب العديد من المواقع الإلكترونية معلومات مثل الاسم وعنوان البريد الالكتروني وغيرها. تخزن هذه البيانات في أنظمة رقمية مما يعرضها لخطر الاستغلال وإعادة التسويق من قبل آخرين.

إضافة إلى ما سبق، يمكن أن تجمع المعلومات تلقائيا أثناء تصفح الانترنت، مثل عنوان بروتوكول الانترنت(ip) الخاص بالمستخدم. كل كمبيوتر يتصل بالشبكة يحصل على عنوان يتكون من 32 رقما، و يسجل كذلك معلومات تتعلق بالمتصفح المستخدم، ووقت و تاريخ زيارة المواقع، فإن تخزينها على الخوادم يمثل تهديدا واضحا لخصوصية الأفراد في الفضاء الافتراضي.[15]

[14] وفاء حلمي السعيد، الرجع السابق، ص1409.

[15] باسم محمد فاضل، **حماية الخصوصية عبر البيئة الرقمية**، (دراسة تحليلية مقارنة في ضوء القانون المصري والفرنسي والشريعة الإسلامية)، دار الفكر الجامعي، الإسكندرية، 2021، ص. ص177.176.

المطلب الثاني

أدوات وتقنيات المراقبة وانعكاساتها على الخصوصية

يمكن للذكاء الاصطناعي أن يلعب دورا مهما في استخدام تقنيات التقييم الذكي للمحتوى التعليمي، حيث يمكن تحديد نقاط القوة و الضعف لدى تحسين تجربة التعليم، حيث يمكن تعزيز التفاعل و التخصيص و الكفاءة في العملية التعليمية.[16]

أما بالنسبة إلى تزايد قدرة الذكاء الاصطناعي على إحداث تغيرات جذرية في العديد من مجالات التوظيف فلقد تزايد مخاوف بشأن الآلية و مستقبل العمل فإنه يتواصل النقاش حول السياسة العامة و الخاصة المتعلقة بالذكاء الاصطناعي و علاقاته بالعمل و الوظائف.[17]

يزداد استخدام تقنيات الذكاء الاصطناعي في تحليل السلوك البشري ورصد الحركات بشكل ملحوظ، سواء من قبل الشركات التجارية أو الجهات الحكومية. ورغم أن هذه التقنيات قد تسهم في تحسين الخدمات وتعزيز الأمن، إلا أنها تثير قلقا مشروعا بشأن حماية الخصوصية.

الفرع الأول: الأنظمة الذكية المتقدمة في المراقبة والتحليل

تعتبر الكاميرات الرقمية، وأنظمة المراقبة عن بعد، وأجهزة الاستشعار من أبرز أدوات الذكاء الاصطناعي المستخدمة في هذا السياق، كما تساهم هذه الأدوات في تكاملها مع الأنظمة الأمنية التقليدية لزيادة فعالية الأداء.

---

[16] عابد جميل السفياني، **ايجابيات وسلبيات الذكاء الاصطناعي على المنظومة التعليمية**، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص إدارة أعمال، جامعة ستار دوم، اسطنبول، تركيا،2024، ص05.

[17] مرزوق فاطمة، **الحماية القانونية للحق في الحياة الخاصة عبر الانترنت**، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، ص.13، تيارت، 2015.

لقد شهدت تكنولوجيا المراقبة الحديثة تطورا سريعا في العقود الأخيرة، حيث تعتمد بشكل متزايد على تقنيات متقدمة كالذكاء الاصطناعي، والتحليل الضوئي، وأنظمة التعرف على الوجوه. هذه التقنيات تعزز من كفاءة عمليات المراقبة في مجالات متعددة مثل الأمن العام، وإدارة المرور، وحماية المنشآت التجارية والحكومية.

لنلاحظ نقطتين تقنيتين يمكن لهما أن تأثرا على برمجة وسائل الحماية، يمكن وضع الحماية في مجموعة المنظومة أو أن يكون لها مقرا خاصا للإقامة في المجموعة، و يمكن للمقر أن ينفذ مختلف الوظائف كعرقلة كشف نظام الحماية، حماية المصورات، حماية أقسام الديسك.[18]

و بالتالي تستخدم الأنظمة الحديثة لالتقاط تفاصيل دقيقة و رصد الأنشطة في الوقت الحقيقي مما يعزز من سرعة الاستجابة و التدخل في الحالات الطارئة.[19]

الفرع الثاني: مخاطر الاستخدام في القطاعين العام والخاص

يعتبر الذكاء الاصطناعي في العصر الحديث الأداة الأكثر استخداما في الشبكات الالكترونية للبحث عن معلومات محددة، فقد أصبح جزءا أساسيا في جميع المجالات لتمتعه بعدد هائل من المزايا التي لا تحصى.[20]

[18] فايز البرشة، **حماية ونزع حماية البرامج (منظومة MS DOS)**، دار الطليعة الجديدة، سوريا،1997، ص61.

[19] محمد عدنان محمد عبد الحميد، "**أثر تكنولوجيا المراقبة الحديثة على تحسين أداء حراس البلدية**"، **مجلة المجتمع العربي لنشر الدراسات العلمية**، العدد74، الجزائر ،2024، **ص112**.

[20] نرمين مجدي، "**الذكاء الاصطناعي وتعلم الآلة**"، **مجلة صندوق النقد العربي**، العدد03، الإمارات العربية المتحدة، ابوظبي،2020، ص. ص12_16.

ففي ظل التحول الرقمي المتسارع الذي أدى إلى تزايد الرقابة واستغلال البيانات الشخصية إلكترونيا، ظهرت مخاطر كبيرة مذ أواخر الستينات وحتى الثمانينات من القرن الماضي. استجابة لهذه المخاطر، بدأت بعض الدول الأوروبية في اتخاذ خطوات قانونية تهدف إلى تنظيم استخدام البيانات الشخصية من قبل الإدارات الحكومية والشركات الكبرى. ولقد أقرت دول مثل النمسا، والدنمارك، وفرنسا، ألمانيا، قوانين تهدف إلى حماية البيانات، حيث ضمنت إسبانيا والبرتغال الحق في حماية البيانات الشخصية كجزء من الحقوق الأساسية المحكمة في الدستور.

يعود هذا التركيز الأوروبي على حماية البيانات ومعالجتها بشكل يضر بالمواطنين، مما قد يؤدي إلى تدخل غير مبرر من الدولة في حياتهم الشخصية وتصنيفهم ضمن قوائم كتلك التي شهدتها الفترات الزمنية للأنظمة النازية والفاشية.

إضافة إلى ذلك، يأتي القلق من دخول القطاع الخاص في هذا النطاق، حيث بات بالإمكان الوصول إلى ملايين المعلومات الشخصية عبر الانترنت مقابل دفع مبالغ مالية. يستخدم العديد من هذه المعلومات ليس فقط لاستهداف الأشخاص بالإعلانات الترويجية، ولكن أيضا في عمليات الاحتيال المالي والمصرفي والاعتداءات على ممتلكات الأشخاص.

و من الواضح أن هذه الممارسات تمثل نوعا من الاتجار غير المشروع و غير المسبوق بالبيانات الشخصية، مثل أسماء الأفراد، و عناوينهم، و أرقام حساباتهم المصرفية، أو معلوماتهم

الصحية، التي تجمع بشكل غير قانوني من مواقع الانترنت، مما يشكل تهديدا مباشرا للأمن الاجتماعي و الشخصي للأفراد[21].

[21] منى الأشقر جبور، "**البيانات الشخصية والقوانين العربية**"، **المركز العربي للبحوث القانونية والقضائية**، تم الاطلاع عليه بتاريخ 2025/05/25، على الساعة 11:50 سا، في الموقع: https://www.carjj.org

المبحث الثاني

نماذج واقعية مهددة للخصوصية

على الرغم من التقدم الملحوظ الذي أحرزته حقوق الإنسان في العقود الأخيرة من أجل تعزيز كرامة الإنسان وضمان حقوقه، إلا أن ظهور وسائل التواصل الاجتماعي قد أسفر عن تحديات جديدة في هذا المجال. حيث يشارك الأفراد بياناتهم الشخصية، مثل الاسم الوظيفي والصور، على هذه المنصات بثقة كبيرة، مما يعرض تلك البيانات لانتهاكات متعلقة بالخصوصية.

وعلى الرغم من الفوائد الكبيرة التي تقدمها وسائل التواصل الاجتماعي في تعزيز التفاعل الاجتماعي والتسويق، فإن هناك جانبا مظلما لها يتمثل في استغلال المجرمين للثغرات في نظم المعلومات. إذ يمكنهم اختراق هذه الأنظمة بهدف سرقة البيانات الشخصية للمستخدمين أو الاطلاع على المعلومات الموجودة فيها واستغلالها بطرق غير قانونية.

المطلب الأول

قضية كامبريدج أنال تكيا

في عام 2018، اندلعت فضيحة عالمية عندما تم الكشف عن أن شركة "كامبريدج أنال تكيا " قامت بجمع بيانات عشرات الملايين من مستخدمي فيسبوك دون علمهم، واستغلال هذه البيانات لتوجيه الحملات الانتخابية، و أبرزها استفتاء "بريكسيت" والانتخابات الرئاسية الأمريكية في عام

2016.اعتمدت الشركة على تقنيات الذكاء الاصطناعي لإنشاء ملفات شخصية دقيقة جدا عن الناخبين، مما مكنها من التأثير في قراراتهم التصويتية[22].

الفرع الأول: استغلال بيانات المستخدمين

يمثل خطر جمع البيانات الشخصية للمستخدمين التحدي الأكبر في الزمن الحالي. حيث يقوم المستخدمون بتقديم بياناتهم بأنفسهم عند التسجيل في شبكات التواصل الاجتماعي مثل "فيس بوك" و" ماي سيبس". تدعو هذه المنصات المستخدمين للإدلاء بمعلومات شخصية كثيرة وواضحة من أجل تعزيز تجربتهم على الموقع.

لكن للأسف، فإن الأفراد غالبا ما يقدمون معلوماتهم دون وعي كامل بالعواقب المترتبة على إعادة استخدام هذه البيانات. بالإضافة إلى ذلك، يتم فهرستها ونشرها واستثمارها دون أن يتمكن أصحابها من ممارسة حقوقهم المتعلقة بها.

تتمثل الخطورة في أن البيانات الشخصية أصبحت موضوعا للتجارة من قبل المواقع والشبكات، الأمر الذي أدى إلى بروز اقتصاد جديد قائم على جمع وبيع البيانات الشخصية. و يعود ذلك إلى سهولة جمع هذه المعلومات و انخفاض تكاليفها، مما شجع العديد من الشركات على الدخول في هذا المجال[23].

[22] مقال منشور بموقع سكاي نيوز عربية تحت عنوان فضيحة تسريب البيانات لا تزال تؤرق "فيسبوك"، 30 يوليو 2023، تم الاطلاع عليه بتاريخ 2025/05/25، على الساعة 14:00 سا في الموقع: https://www.skynewsarabia.com

[23] باسم محمد الفاضل، **حماية الخصوصية عبر البيئة الرقمية**، مرجع سابق، ص. ص182،183.

الفرع الثاني: شركة Clearview AI

قامت الشركة الأمريكية الناشئة المتخصصة في تقنيات التعرف على الوجه بجمع مليارات الصور من الانترنت دون الحصول على إذن من أصحابها. تستخدم هذه الصور في تطوير نظام للتعرف على الوجه يستعمله جهاز الشرطة في عدة دول. كما يعتبر هذا الاستخدام انتهاكا خطيرا للحق في الخصوصية، خاصة في ظل غياب إطار قانوني واضح أو رقابة قضائية مناسبة.[24]

المطلب الثاني

التطبيقات اليومية وتأثيرها على الخصوصية

لقد أحدثت التكنولوجيا الحديثة تحولا جذريا في الطريقة التي نتعامل بها مع الخصوصية الشخصية. بفضل التطور السريع في مجالات الحوسبة الحسابية، والذكاء الاصطناعي، وانترنت الأشياء، أصبحت الشركات قادرة على جمع وتحليل كميات ضخمة من البيانات الشخصية بكل سهولة، وبدون الحاجة إلى التفاعل المباشر مع المستخدمين. التطبيقات التي نستخدمها يوميا، سواء كانت خاصة بالتواصل الاجتماعي أو التسوق أو حتى الصحية، تقوم بتجميع المعلومات عن سلوكنا واهتماماتنا. تستخدم هذه البيانات لتحليل سلوك المستخدمين و استهدافهم بإعلانات مخصصة، أو لتحسين الخدمات التي تقدمها الشركات.[25]

[24] مقال منشور بموقع سانجو للأتمتة المحدودة تحت عنوان هولندا تغرم شركة Clearview AI بمبلغ 30.5 مليون يورو بسبب جمع بيانات الوجه بشكل غير قانوني، سبتمبر 2024، تم الاطلاع عليه بتاريخ 2025/05/30، على الساعة 06:00 سا في الموقع:https://ar.sango-robot.com

[25] حسام الدين كامل الاهواني، **الحق في احترام الحياة الخاصة الحق في الخصوصية**، (دراسة مقارنة) دار النهضة العربية، القاهرة، 1978، ص8.

الفرع الأول: وسائل التواصل الاجتماعي

على الرغم من أن ظهور وسائل التواصل الاجتماعي الحديثة قد أحدث ثورة نوعية في أساليب التواصل بين الأفراد، إلا أنه أسفر عن آثار سلبية وممارسات غير محمودة كان لها تأثير على المجتمع بشكل عام، وعلى الأسرة بشكل خاص. من بين هذه الممارسات، نجد جمع البيانات الرقمية دون موافقة أصحابها.

البيانات الشخصية الرقمية لا تختلف كثيرا عن البيانات الشخصية التقليدية، حيث يتمثل الفرق في طريقة استخدامها ضمن الوسائط الالكترونية. فلكل النوعين من البيانات الخصائص الشخصية لكل فرد، و التي تشمل الاسم، اللقب، رقم الهاتف، الرمز البريدي، العمر، الجنس، تاريخ الميلاد، الجنسية، و غيرها من المعلومات التي تتيح التعرف على صاحبها أو تكون قابلة للتحديد.[26]

الفرع الثاني: التجسس والمراقبة الالكترونية

لقد ساهمت التكنولوجيا الحديثة بشكل كبير في تسهيل عمليات التجسس والمراقبة بطرق كانت غير ممكنة سابقا. من خلال انتشار الكاميرات الرقمية والميكروفونات المدمجة في الأجهزة الذكية، أصبح بالإمكان مراقبة الأفراد بشكل مباشر أو غير مباشر.

إضافة على ذلك، تستفيد الحكومات والشركات الكبرى من البرامج المتطورة التي تمكنها من جمع وتحليل البيانات الصوتية والمرئية بشكل مباشر. يشكل ذلك تهديدا كبيرا لخصوصية الأفراد، حيث يمكن استغلال المعلومات الشخصية لأغراض متعددة، مثل التجسس على الأنشطة اليومية

[26] باسم محمد فاضل، **حماية الخصوصية عبر البيئة الرقمية**، مرجع سابق، ص.176.

من خلال مساعدات مثل Google Assistant et Alexa،أو حتى السيطرة على الأجهزة الذكية.[27]

[27] مقال منشور بموقع المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات تحت عنوان: التجسس الالكتروني، أكتوبر 2020، تم الاطلاع عليه بتاريخ 2025/06/01، على الساعة 08:30 سا، في الموقع:
https://www.europarabct.com

الفصل الثاني

الإطار القانوني لحماية الخصوصية في عصر الذكاء الاصطناعي

بعد استعراض المخاطر والتحديات التي يطرحها الذكاء الاصطناعي على خصوصية الأفراد في الفصل الأول، يصبح من الضروري البحث عن آليات الحماية والضمانات اللازمة للحفاظ على الخصوصية في ظل هذا التطور التكنولوجي السريع.

يهدف هذا الفصل إلى دراسة الأطر القانونية الموجودة، بالإضافة إلى استكشاف التقنيات الحديثة والحلول التكنولوجية المتاحة لحماية الخصوصية في سياق الذكاء الاصطناعي. كما سيتم التطرق إلى التحديات المستقبلية التي قد تواجه الحماية والبحث عن حلول مبتكرة للتصدي لها.

المبحث الأول

القوانين والتشريعات الدولية والوطنية لحماية الخصوصية في ظل الذكاء الاصطناعي

لقد قامت العديد من التشريعات الدولية بتكييف أنظمتها القانونية لتتواكب مع التطورات التكنولوجية والرقمية، خاصة في مجالات الاتصال والمعلوماتية. وفي هذا السياق، تم التركيز على حماية الخصوصية من خلال حماية البيانات الشخصية، وتحديد طرق معالجتها، بالإضافة إلى توضيح العقوبات المترتبة على أي انتهاك لهذه الحقوق.

اتجه بعض من الفقه والقضاء الحديث إلى اعتبار الحق في حماية الحياة الخاصة من قبيل الحقوق الملازمة لصفة الإنسان والحقوق الشخصية هي التي يكون موضوعها العناصر المكونة للشخصية أو هي الحقوق التي تنصب على عناصر الشخصية في مختلف مظاهرها الطبيعية والمعنوية والاجتماعية.

كما اعترف المشرع الفرنسي صراحة بأن للشخص الحق في احترام حياته الخاصة، فالحماية تقررت للحق و ليس للحرية فأساس الحماية القانونية ليس أحكام المسؤولية المدنية، إنما وجود حق شخصي في حرمة الحياة الخاصة.[1]

وعلى غرار ذلك، أدرك المشرع الجزائري أهمية هذا الموضوع الحساس، حيث أكد على حماية المعطيات الشخصية من خلال التعديل الدستوري لسنة 2016. تل ذلك إصدار القانون رقم 18-

[1] عبد الرحمان خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري (دراسة تأصيلية تحليلية مقارنة)، **مجلة البحوث والدراسات**، العدد12، كلية الحقوق، جامعة بجاية، الجزائر،2011، ص. ص159-161.

07[2]، الذي يتناول حماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي. مما ساهم في سد جزء من الفراغ القانوني الذي كان موجودا في هذا المجال[3].

المطلب الأول

القوانين والتشريعات الدولية

في ظل التحول الرقمي المتسارع والانتشار الواسع لتقنيات الذكاء الاصطناعي ومع تقدم تكنولوجيا تطور أسلوب الاعتداء على الحياة الشخصية مما أدى إلى انتشار الابتزاز والأخبار الكاذبة والمعلومات السرية وتداولها بشكل واسع. [4]

تفطنت العديد من الجهات إلى ضرورة وجود إطار قانوني فعال لحماية الخصوصية من الانتهاكات التي قد تنجم عن جمع البيانات الشخصية وتحليلها بشكل آلي. وبالفعل عملت العديد من المنظمات الدولية والهيئات التشريعية الإقليمية على وضع هذا الإطار التنظيمي.

كما أنه من الجدير بالذكر أن الكثير من القوانين المقارنة أنشأت هيئات مشابهة، مثل اللجنة الوطنية المغربية لمراقبة حماية المعطيات ذات الطابع الشخصي، والهيئة الفرنسية لحماية المعلومات والحريات(CNIL).

---

[2] القانون رقم 18_07 مؤرخ في 10 جوان 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال المعالجة للبيانات ذات الطابع الشخصي، ج.ر، العدد 34، صادر بتاريخ 10 جوان 2018.

[3] كحلاوي عبد الهادي، بن زيطة عبد الهادي، **آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 18_07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي** مجلة القانون والعلوم السياسية، العدد1، كلية الحقوق و العلوم السياسية، جامعة أدرار، 2019، ص115.

[4] نصر الله خيرة، جرائم تطبيقات التواصل الاجتماعي في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي و علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة د.مولاي الطاهر، سعيدة،2022 ص.ص74-75.

و على الرغم من وجود الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال و مكافحتها، التي أنشأت بموجب القانون رقم 09-04[5]، إلا أنه لا يمكن القول إنها تقوم بمهمة مراقبة حماية المعطيات الشخصية. ورغم أنها هيئة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تحت إشراف الوزير المكلف بالعدل (طبقا للمادة 2 من المرسوم الرئاسي 15-261)، فإن المهام التي حددتها المادة14 من قانون 09-04 تركز على الوقاية و مكافحة الجريمة الالكترونية بشكل عام، دون تضمين مهمة مراقبة مدى احترام حماية المعطيات الشخصية من المعالجة الآلية.

كما أدرج في القانون نفسه إنشاء سجل وطني لحماية البيانات الشخصية، و ذلك بموجب المادة 28، حيث تسجل فيه البيانات المذكورة وفقا للطبيعة المحددة في المادة[6].

الفرع الأول: اللائحة العامة لحماية البيانات (GDPR)

تعتبر اللائحة العامة لحماية البيانات، التي تم تطبيقها في الاتحاد الأوربي ابتداء من عام 2018، واحدة من أهم التشريعات العالمية في مجال حماية البيانات. حيث تحدد هذه اللائحة القواعد المتعلقة بجمع ومعالجة البيانات الشخصية وتمنح الأفراد مجموعة من الحقوق الأساسية، ومن أبرزها:

1_**الحق في المحو**: يحق للأفراد المعنيين طلب حذف بياناتهم الشخصية.

[5] القانون رقم 09_04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر.ج.ج، عدد47، صادر في 16 أوت 2009.

[6] الطيب فرجان، عبد الحليم عزوز، أسس حماية الحق في الخصوصية بين القانون الدولي والقانون الوطني، **مجلة الدراسات القانونية والاقتصادية**، المجلد05، العدد03، جامعة المسيلة، الجزائر،2023، ص.ص.1143، 1159.

2_**الحق في تقييد المعالجة:** يمكن للأفراد المعنيين تحديد كيفية استخدام بياناتهم إذا كان لديهم شك في دقة هذه البيانات أو إذا كانت لم تعد ضرورية أو تستخدم بشكل غير صحيح.

3_**الحق في الاعتراض:** يوجد لدى الأفراد المعنيين الحق في الاعتراض على معالجة بياناتهم، كما أن الأفراد الذين قدموا موافقتهم سابقا يجب أن يتمكنوا من سحبها بسهولة في أي وقت.

4_**الحق في إمكانية نقل البيانات:** يحق للأفراد المعنيين نقل بياناتهم، ويجب على جهات التحكم والمعالجة تسهيل هذه العملية.

عدة تحديات عند التعامل مع الذكاء الاصطناعي، خاصة بسبب GDPRو مع ذلك، يواجه الغموض الذي يحيط بعمل الخوارزميات و صعوبة تفسيرها من قبل المستخدمين أو المراقبين القانونيين[7].

الفرع الثاني: المبادئ والتوصيات الدولية

أبدت عدة هيئات دولية أهمية تنظيم الذكاء الاصطناعي بما يتماشى مع احترام الحقوق الأساسية مما قد نصت المادة 12 من الإعلان العالمي لحقوق الإنسان و المادة 17 من العهد الدولي الخاص بالحقوق المدنية و السياسية على أنه لا يجوز التدخل التعسفي في خصوصية الفرد أو أسرته أو منزله أو مراسلته، كما أن لكل شخص الحق في حماية القانون من مثل هذه التدخلات[8].

ومن بين هذه الهيئات:

[7] مقال منشور على الموقع IBM تحت عنوان قائمة التحقق في الامتثال للائحة العامة لحماية البيانات GDPR، يناير2024، تم الاطلاع عليه بتاريخ 2025/05/03 على الساعة 15:45 سا، في الموقع:
https://www.ibm.com

[8] نزيه محمد علي، دور التشريعات و القوانين الوطنية و الدولية الحاكمة لحماية أمن المعلومات، **المجلة المصرية لبحوث الإعلام** ، المجلد25، العدد91، جامعة القاهرة، مصر ص.1287.

أولا: توصية اليونسكو حول أخلاقيات الذكاء الاصطناعي

في عام 2021، حثت منظمة اليونسكو دول العالم على تطبيق توصيتها بشأن تنظيم الذكاء الاصطناعي. جاء ذلك بعدما دعا أيلون ماسك ومئات من الخبراء إلى وقف تطوير هذه الأنظمة لمدة ستة أشهر، محذرين من "المخاطر الكبيرة على البشرية".

في نوفمبر 2021، اتفقت الدول 193الأعضاء في هذه المنظمة التابعة للأمم المتحدة بالإجماع على "إطار العمل المعياري العالمي الأول للاستخدام الأخلاقي للذكاء الاصطناعي". ووصفت هذه الوثيقة بأنها "خريطة طريق للدول تهدف إلى تحقيق أقصى استفادة من تكنولوجيا الذكاء الاصطناعي مع تقليل المخاطر المرتبطة بها".

تم اعتماد هذا النص بعد ثلاث سنوات من الجهود المتواصلة، حيث يحدد الإجراءات اللازم اتخاذها، بما في ذلك إنشاء تشريعات لتنظيم و مراقبة الذكاء الاصطناعي، و ضمان حماية البيانات الشخصية و الحساسة و تعزيز التوعية حول هذا الموضوع.[9]

ثانيا: إعلان الحقوق الرقمية للأمم المتحدة

يهدف الميثاق الرقمي العالمي إلى إنشاء إطار شامل يتطلب تعاون مختلف الأطراف لمواجهة الفجوات الرقمية والابتكارية. من المتوقع أن يحدد هذا التعهد المبادئ والأهداف والإجراءات اللازمة لبناء مستقبل رقمي مفتوح وآمن للجميع، يرتكز على حقوق الإنسان العالمية ويدعم تحقيق أهداف التنمية المستدامة.

[9] أحمد المسلماني، الهيئة الوطنية للإعلام، مارس2023، تم الاطلاع عليه بتاريخ 2025/06/03، على الساعة 12:30 سا، في الموقع:
https://www.masgpero.eg

لذا، يجب أن يستمر التركيز على تطوير رؤية مشتركة للتعاون في العالم الرقمي، مع استثمار كامل الإمكانيات الإيجابية للتكنولوجيا ومعالجة قضايا الثقة والأمان في الفضاء الرقمي. فقد أصبح الاعتماد على الأدوات الرقمية أكثر أهمية من أي وقت مضى لتحقيق التواصل وضمان الازدهار الاجتماعي والاقتصادي.

كما يمكن أن تساهم التقنيات الرقمية في تسريع تنفيذ خطة عام2030، وبذلك يجب ضمان الوصول الآمن والميسور للجميع إلى الفضاء الرقمي. و يمكن للأمم المتحدة أن توفر منصة لجميع المعنيين للمشاركة في هذه النقاشات[10].

ثالثا: مبادرات مجلس أوروبا ولجنة حماية البيانات الأوربية

نصت المادة 12 من الاعلان العالمي لحقوق الإنسان لسنة 1948 على وجوب احترام حرمة الحياة الخاصة، كما نصت المادة 08 من الاتفاقية الأوروبية لحقوق الإنسان لسنة 1908 على احترام الحياة الخاصة. و نصت المادة 16 من اتفاقية نيو يورك لحقوق الطفل لسنة 1990 على عدم جواز التدخل التعسفي في الحياة الخاصة.[11]

[10] مقال منشور على موقع: welcome to the united nations تحت عنوان التعاهد الرقمي العالمي،أفريل 2024، تم الاطلاع غليه بتاريخ 2025/06/03 على الساعة 18:40 سا، في الموقع:https://www.un.org

[11] ANCEL (Jean-Pierre) : protection de la personne : Image et vie privée, Gazette du palais, no.254, 1994, p.13_14.

فإنه تم اعتماد الإعلان العالمي لحقوق الإنسان والاتفاقيات الأوربية لحقوق الإنسان قبل وقت طويل من تطور الحواسيب والانترنت وظهور مجتمع المعلومات. وقد جلبت هذه التطورات فوائد كبيرة للأفراد والمجتمعات وساهمت في تحسين جودة الحياة والكفاءة والإنتاجية. [12]

ومع ذلك نشأت عن هذه التطورات مخاطر جديدة تهدد حق الأفراد في احترام حياتهم الخاصة. استجابة لهذه الحاجة إلى قواعد واضحة تنظم جمع واستخدام المعلومات الشخصية، ظهر مفهوم جديد للخصوصية، الذي يعرف في بعض الولايات القضائية ب "خصوصية البيانات «أو "الحق في تقرير المصير لمعلوماتي". و قد أدت هذه المفاهيم إلى تطوير لوائح قانونية خاصة تعنى بحماية البيانات الشخصية[13].

المطلب الثاني

التشريعات الوطنية

صدر القانون رقم 18-07 بعد موافقة مجلس الوزراء عليه في 8 مارس 2018، ومن ثم تم التصديق عليه من قبل نواب المجلس الشعبي الوطني في 28 مارس 2018، وأقره مجلس الأمة بالإجماع في 13 مايو 2018. كما يهدف هذا القانون، وفقا للمادة الثانية منه، إلى تنظيم ومعالجة المعطيات ذات الطابع الشخصي بغض النظر عن مصدرها أو شكلها، مع التأكيد على ضرورة

[12] أشرف توفيق شمس الدين، الصحافة و الحماية الجنائية للحياة الخاصة، مرجع سابق، ص11.

[13] مقال منشور على موقع European union agency for fundamtalrighys تحت عنوان دليل قانون حماية البيانات الأوروبية، أبريل2018، تم الاطلاع عليه ب تاريخ2025/06/03، على الساعة،19:07 سا، في الموقع:

احترام الكرامة الإنسانية وحقوق الأفراد، وعدم المساس بشرفهم أو سمعتهم. يتكون القانون من 76 مادة موزعة على 7 أبواب.

على الرغم من التطورات الكبيرة والمزايا العديدة التي أفرزتها الثورة التكنولوجية، خصوصا في مجال الاتصالات، والتي جعلت العالم يبدو كقرية صغيرة وسهلت عمليات نقل المعلومات والبيانات والأخبار، فإن هناك العديد من العيوب المرتبطة باستخدام وسائل الاتصال الحديثة. من أبرز هذه العيوب سهولة الوصول إلى المعلومات والبيانات الشخصية، وكذلك أي معلومات يتم تخزينها على أجهزة الكمبيوتر أو الأجهزة الذكية، مثل الهواتف المحمولة. لقد أصبح الاطلاع على هذه المعلومات أسهل بكثير باستخدام برامج مخصصة تعرف ببرامج "الهكر".

نتيجة لذلك، ظهر في الفكر القانوني الحديث مصطلح الجريمة المعلوماتية، الذي يشمل الاعتداء على بيانات ومعلومات خاصة وسرية تهم الأفراد أو المؤسسات. ومن المهم التأكيد على قيمة البيانات والمعلومات السرية، حيث يعد الاعتداء عليها انتهاكا لحقوق الإنسان.

الفرع الأول: قانون حماية البيانات في فرنسا(Loi informatique libertes)

قانون حماية البيانات في فرنسا، المعروف أيضا بقانون "المعلوماتية والحريات" أو "LIL"، يعتبر التشريع الأساسي الذي ينظم معالجة البيانات الشخصية في البلاد. هذا التشريع التاريخي يضبط كيفية جمع وتخزين واستخدام المعلومات الشخصية في فرنسا ويعزز حقوق الأفراد فيما يتعلق ببياناتهم.[14]

[14] La loi 78-17 du 6 janvier 1978 , relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés, est une loi française qui réglemente le traitement des données personnelles, sur le site : WWW.legifrance.fr.

ينشئ القانون اللجنة الوطنية للتكنولوجيا المعلومات والحريات (CNIL) كسلطة مستقلة مسؤولة عن حماية البيانات. كما يحدد القانون مجموعة من الحقوق للأفراد، مثل حق الوصول إلى بياناتهم وحق تصحيح المعلومات المضللة وما إلى ذلك.

رغم كون قانون LIL جزءا أساسيا من الإطار القانوني لحماية البيانات، إلا أنه لم يعد ساري المفعول بعد دخول اللائحة العامة لحماية البيانات (GDPR) حيز التنفيذ في عام 2016، ومع ذلك، يستمر هذا التشريع في تغطية أي كيان يقوم بمعالجة البيانات الشخصية للأفراد المقيمين في فرنسا، بغض النظر عن مكان وجود ذلك الكيان.

تواجه المؤسسات التي لا تلزم بالقانون عقوبات مالية صارمة، قد تصل إلى 3 ملايين يورو أو 5 بالمئة من إجمالي المبيعات السنوية، أيهما أعلى، يتم تحديد قيمة الغرامة بناء على شدة المخالفة وحجم المؤسسة وحجم مبيعاتها.

تتولى اللجة الوطنية لمعلوماتية و الحريات (CNIL) مسؤولية التأكد من الامتثال لقانون LIL تقوم اللجنة بإجراء عمليات تدقيق، وتقديم الإرشادات، وفرض العقوبات للحفاظ على معايير خصوصية البيانات. كما تتمتعCNILبسلطة التحقيق في أي انتهاكات لقانونLIL و ملاحقة الأفراد أو الكيانات قضائيا، إضافة إلى إمكانية إصدار أوامر للجهات المعنية بضرورة الامتثال للقانون.[15]

في سبتمبر الماضي، قام حاكم ولاية كاليفورنيا، جافين نيوسوم، بالتوقيع على أكثر من عشرة قوانين تتعلق بمجال الذكاء الاصطناعي، تغطي هذه القوانين مجموعة واسعة من الموضوعات، بدءا من ضرورة الكشف عن تفاصيل بيانات التدريب وصولا إلى معاجلة قضايا التزييف العميق.

[15] مقال منشور على الموقع:solixtrchnologies ,inc.Arabic تحت عنوان ما هو قانون ? LIL، يونيو2025، تم الاطلاع عليه بتاريخ2025/06/07 على الساعة 20:46 سا، على الموقع:https://www.solix.com

من بين هذه التشريعات، تم إقرار ثلاث مشاريع قوانين رئيسية تهدف إلى تعزيز أمان وثقة تطوير الذكاء الاصطناعي، مع التركيز بشكل خاص على تحسين ثقة الجمهور في كيفية تعامل أنظمة الذكاء الاصطناعي مع المعلومات الشخصية.

أظهرت دراسة استقصائية أن أكثر من 81بالمئة من المستهلكين يشعرون بالقلق حيال إمكانية استخدام شركات الذكاء الاصطناعي لمعلوماتهم بطرق غير مقصودة. ولتخفيف هذه المخاوف، وضعت القوانين قيودا واضحة على كيفية استخدام الشركات للمعلومات الشخصية، مثل الأسماء والعناوين والبيانات البيومترية. هذا يساعد شركات الذكاء الاصطناعي على طمأنة المستخدمين بأن بياناتهم ستعامل بطريقة مسؤولة، حتى في حالة تعرضها للكشف بواسطة أنظمة الذكاء الاصطناعي.[16]

الفرع الثاني: التشريعات العربية

على الصعيد العربي شهد استخدام تقنيات المعلومات والاتصالات انتشارا واسعا، حيث تعددت استخدامات أجهزة الاتصال ودخلت التكنولوجيا الرقمية إلى العديد من القطاعات، خاصة في مجالات الخدمات المالية والمصرفية. ومن أبرز التطورات الملحوظة هنا هو توجه العديد من الحكومة العربية نحو تفعيل الاقتصاد من خلال تعزيز الاقتصاد الرقمي.

[16] أبرامي فينا، لوائح الذكاء الاصطناعي الجديدة في كاليفورنيا، التركيز على الذكاء الاصطناعي الأخلاقي، أكتوبر 2024، تم الاطلاع عليه بتاريخ2025/06/07، على الساعة 21:00 سا، على الموقع:https://www.ultralytics.com

وفقا لتقرير دوري تصدره الأمم المتحدة، تحقق الدول العربية تقدما ملحوظا في الاعتماد على الحكومة الالكترونية، وخاصة في دول مجلس التعاون الخليجي. حيث تصدرت الإمارات العربية المتحدة وقطر والسعودية والكويت والبحرين المراكز الأولى على مستوى العالم في هذا المجال.

كما نجحت دول مثل المغرب و الإمارات و السعودية و تونس في بذل جهود كبيرة لتحسين التواصل مع المواطنين، و توفير المعلومات المتاحة للجمهور حول مجالات مثل الصحة و الرعاية الاجتماعية و العمل و غيرها.[17]

الفرع الثالث: الحماية الجنائية والمدنية للبيانات الشخصية في القانون الجزائري

أولا: الحماية الجنائية للبيانات الشخصية

رغم الضمانات التي أسراها الإطار الإجرائي والمؤسساتي لحماية البيانات الشخصية، تبقى فعالية هذه الآليات نسبية مقارنة بالتدابير الجنائية التي تمثل واحدة من أنجح الوسائل لحماية هذه البيانات.

العقوبات المنصوص عليها في قانون العقوبات، والتي أقر المشرع الجزائري جانبا من الحماية الشخصية، خاصة من خلال تعديل قانون العقوبات في سنة 2004 بموجب القانون 04-15، حيث تم إدراج قسم جديد بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وتم استحداث مواد جديدة من المادة 394مكرر حتى المادة 394مكرر7. كما تم تضمين التعديل الصادر في سنة 2006 بموجب القانون 06-23، الذي يؤرخ في 20 ديسمبر 2006، لنصوص تتعلق بالاعتداء على الخصوصية باستخدام تقنيات رقمية، وذلك من خلال نص المواد من 303إلى 303مكرر2.

[17] منى الأشقر محمود جبور، المرجع السابق، ص15.

في هذا السياق، تنص المادة 394مكرر على عقوبة السجن من ثلاثة أشهر إلى سنة، بالإضافة إلى غرامة مالية تتراوح بين100.000 دج و 500.000دج، بسبب الدخول أو البقاء بصورة غي قانونية ضمن نظام معالجة المعلومات. وفي حال حدوث حذف أو تغيير للمعطيات، تتضاعف العقوبة. أما في حال إدخال أو إزالة أو تعديل المعطيات بصورة غير قانونية في نظام المعالجة الآلية، فإن العقوبة تتصاعد لتصبح بين ستة أشهر و ثلاث سنوات، مع غرامة تتراوح بين.5000.000دج و1.000.000دج .[18]

كما أقر المشرع الجزائري في المادة 394 مكرر 2 عقوبة الحبس من شهرين إلى ثلاث سنوات، وغرامة مالية تتراوح ب ين5.000.000دج و1.000.000دج، لكل من يقوم عمدا أو بصورة غير قانونية بتصميم أو بحث أو تجميع أو توفير أو نشر أو مرسلة من خلال نظام معلوماتي يمكن أن ترتكب به الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

كما اعتبر المشرع مجرد الشروع في ارتكاب المخالفات المنصوص عليها في هذا القسم بعقوبته نفسها كعقوبة الشروع في ارتكاب الجريمة الكاملة، بالإضافة إلى التأكيد على مصادرة الأجهزة و البرامج و وسائل التنفيذ المستخدمة و تغلق المواقع التي تستخدم كوسيلة لتنفيذ الجرائم المنصوص عليها.[19]

[18] كحلاوي عبد الهادي، الحماية القانونية للبيانات الشخصية في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في الحقوق تخصص: حقوق وحريات كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار،2022، ص211.

[19] راجع المواد 394 مكرر، إلى 394مكرر7، من الأمر156/66 المؤرخ في 18 صفر 1386 الموافق08يونيو 1996المتضمن قانون العقوبات، المعدل و المتمم، لاسيما ما تضمنه القانون رقم15/04 المؤرخ في 2004/11/10، الجريدة الرسمية عدد71 المؤرخة في 10نوفمبر2004.

ثانيا: المسؤولية المدنية عن انتهاك الخصوصية

وفقا للقواعد الأساسية في المسؤولية التقصيرية، يلزم كل شخص يحدث ضرر للآخرين نتيجة لخطأ ارتكبه بتعويض المتضرر، تعتبر المسؤولية التقصيرية قائمة متى ما خالف شخص ما الالتزام القانوني بعدم التعرض للآخرين، وذلك من خلال ارتكابه لفعل ضار يسبب الضرر للغير.

تتمثل إحدى الصعوبات في إثبات وجود الخطأ في حالات معينة تتعلق بانتهاكات تتكرر ظهورها على صفحات الانترنت. في هذه الحالات يكون الانتهاك الأساسي واحدا، إلا أنه يتم نسخه عبر عدة صفحات، وهو ما يعرف في الفقه الانجليزي بمصطلح "Mirror sites".

يلجأ بعض الأفراد إلى هذه الحيلة للتهرب من المسؤولية المحتملة الناتجة عن الفعل المسؤول، حيث يحاجون أنهم لم يقوموا بارتكاب الفعل الأصلي الذي أدى إلى الانتهاك. وفقا لمبدأ حرية التعبير، يدعون أيضا أن لديهم الحق في نسخ أو نشر أي معلومات متاحة على صفحات الانترنت. بالرغم من تواجد وسائل الحماية على الشبك، إلا أن ذلك لا يمنع انتهاك الحقوق من خلال استخدام « Mirror sites ».[20]

[20] باسم محمد فاضل، حماية الخصوصية عبر البيئة الرقمية، المرجع السابق، ص185.

المبحث الثاني

الحلول التقنية لحماية الخصوصية في عصر الذكاء الاصطناعي

في ظل تسارع التقدم التكنولوجي، أصبحت مسألة حماية الخصوصية ذات أهمية بالغة إذ يساهم الذكاء الاصطناعي في زيادة مخاطر جمع المعلومات الشخصية، مما يعزز القلق بخصوص خصوصية البيانات.

من الضروري أن نتعلم كيفية حماية البيانات من التسريب أو الاستخدام غير المصرح به. يمكن تحقيق ذلك من خلال إتباع ممارسات أمان فعالة أثناء استخدام الانترنت والتطبيقات، مثل اختيار كلمات مرور قوية والامتناع عن مشاركة المعلومات الحساسة.

إضافة إلى ذلك، يعد استخدام تقنيات التشفير وسيلة فعالة لحماية البيانات. و من هنا، فإن فهم كيفية حماية الخصوصية في ظل وجود الذكاء الاصطناعي يصبح أمرا لا غنى عنه.[21]

المطلب الأول

التقنيات الأساسية لحماية الخصوصية في عصر الذكاء الاصطناعي

لحماية البيانات بفعالية، يتعين على المنظمات أن تكون على دراية بالإطار القانوني المتعلق بحماية البيانات، مثل اللائحة العامة لحماية البيانات «GDPR» تعتبر هذه اللائحة قانونا أساسيا يضمن حقوق الأفراد في الخصوصية وحماية المعلومات الشخصية.

[21] محمد ناصر، كيف تحمي خصوصيتك في عصر الذكاء الاصطناعي، فيفري 2025، تم الاطلاع عليه بتاريخ2025/06/08،على الساعة 15:00 سا، في الموقع: https://techsmartdigest.com

تحتوي اللائحة «GDPR» على متطلبات صارمة تعزز معايير حماية البيانات وأمنها، لذا من المهم الالتزام بالقوانين المحلية المتعلقة بحماية البيانات الشخصية.

تحدد هذه اللوائح إرشادات دقيقة لجمع البيانات و تخزينها و معالجتها و الإفصاح عنها، مما يشمل التأكيد على حماية الخصوصية و أمن المعلومات الشخصية.[22]

الفرع الأول: التشفير وإخفاء الهوية

يساهم استخدام تقنيات التشفير في حماية البيانات الحساسة من الوصول غير المصرح به، حيث يضمن أن المعلومات تظل غبر قابلة للقراءة أو التحليل حتى في حالة حدوث اختراق.

فيما يتعلق بإخفاء الهوية، يتم ذلك عن طريق إزالة المعلومات الشخصية القابلةللتعريف «PII» من مجموعات البيانات. تعتبر هذه المعلومات حساسة وسرية للغاية، لأنها يمكن أن تستخدم لتحديد هوية فرد معين وتهديد خصوصيته. و بالتالي، يتعين على المنظمات غير الربحية مراعاة حماية خصوصية الأفراد أثناء استمرارها في استخدام البيانات لأغراض تحليلية.[23]

الفرع الثاني: التعلم الآمن و تنفيذ إجراءات أمنية قوية

تساهم إجراءات عمليات تدقيق دورية في كشف نقاط الضعف ومعالجتها في الوقت المناسب. يتوجب على المنظمات تقييم أنواع البيانات التي تجمعها والأشخاص الذين يمكنهم الوصول إليها، وكذلك كيفية مشاركتها، مما يساعد في تصميم إجراءات الأمان المناسبة.

---

[22] فيصل العتقي، حماية البيانات في عصر الذكاء الاصطناعي، أوت 2023، تم الاطلاع عليه بتاريخ2025/06/08 على الساعة 13:00 سا، في الموقع: https://www.mozn.ws

[23] فيصل العتقي، المرجع السابق.

علاوة على ذلك يعتبر تخزين البيانات و تحديثات البرامج المنتظمة عناصر أساسية في حماية البيانات، لذلك، يجب على المنظمات غير الربحية الاستثمار في أنظمة أمان قوية و ضمان أن يفهم الموظفون و يتبعون البروتوكولات المعتمدة للأمان.[24]

الفرع الثالث: تدريب الموظفين وتعزيز الشفافية

يعتبر تدريب الموظفين حول أفضل الممارسات لحماية البيانات والمخاطر المحتملة المرتبطة بالذكاء الاصطناعي أمرا حاسما لضمان حماية البيانات. ينبغي تقديم دورات تدريبية دورية تعرف الموظفين بأفضل ممارسات خصوصية البيانات، وتساعدهم على فهم التهديدات المحتملة وأساليب التصرف والاستجابة عند وقوع حوادث أمنية.

يساهم ذلك في تعزيز ثقافة الأمان داخل المنظمة، مما يجعل كل فرد مدركا لمسؤولياته في حماية البيانات والتعامل معها بحرص ووعي. بالإضافة إلى ذلك، يفيد تعزيز التواصل المستمر بين الموظفين وإدارة أمن المعلومات والمسؤولين عن البيانات في تبادل المعرفة وتقديم التوجيه عند مواجهة تحديات أمنية أو انتهاكات للبيانات.

و في الحالات التي يتم اتخاذ القرارات بشكل آلي، يمكن أن يكون من الصعب تحديد كيف و لماذا تم اتخاذ هذه القرارات، مما يطرح تحديات في مجالات مثل المسائلة و الشفافية.[25]

[24] فيصل العتقي، المرجع نفسه

[25] رمضاني مراد، **الذكاء الاصطناعي وعملية صنع القرار**، دار العيون للنشر الالكتروني، وهران،2024, ص14.

لذلك يجب على المنظمات غير الربحية توضيح سياسات حماية البيانات الخاصة بها بشكل صريح للأطراف المعنية، بما في ذلك المتبرعين، والمستفيدين، والمتطوعين. هذا يسهم في بناء الثقة و الشفافية ويطمئن المعنيين بأن معلوماتهم الشخصية تعالج بطريقة مسؤولة .[26]

المطلب الثاني

التحديات المستقبلية والحلول المبتكرة لحماية الخصوصية في عصر الذكاء الاصطناعي

بينما يوفر الذكاء الاصطناعي فرصا هائلة للإبداع والتنمية، يظل التحدي الأكبر هو ضمان عدم تحول هذه الفوائد إلى تضحيات لخصوصية الأفراد وحقوقهم الأساسية. يعود ذلك إلى أن الذكاء الاصطناعي يعتبر القوة المحركة للتقدم والنمو والازدهار في السنوات القليلة المقبلة.

مع هذا الاقتراب من التحول الرقمي، يصبح البحث عن التقدم و التصدي لتحديات المستقبل في ظل فلسفة الذكاء الاصطناعي من الأولويات الأساسية التي يجب أن تتصدر اهتمامات المفكرين و صانعي القرار في المجتمع.[27]

الفرع الأول: التحديات المستقبلية لحماية الخصوصية في عصر الذكاء الاصطناعي

يؤدي التقدم التكنولوجي والزيادة المستمرة في استخدام الذكاء الاصطناعي إلى ظهور مجموعة من التحديات والعقبات التي يجب التغلب عليها. تتوزع هذه التحديات إلى عدة فئات:

أ-تحديات تقنية:

[26] فيصل العتقي، **حماية البيانات في عصر الذكاء الاصطناعي**، المرجع السابق

[27] مجدي صلاح طه المهدي، "**التعليم وتحديات المستقبل في ضوء فلسفة الذكاء الاصطناعي**،"**مجلة تكنولوجيا التعليم و التعلم الرقمي**، المجلد2، العدد5، كلية التربية، جامعة المنصورة،2021، ص99.

1_يفتقر العديد من المنظمات الصغيرة وبعض المؤسسات الكبيرة إلى الموارد المالية والبشرية اللازمة.

2_*تعاني البنية التحتية الرقمية والاتصالات من الضعف، مما يؤثر على فعالية استخدام الذكاء الاصطناعي.

3_يواجه استخدام الخوارزميات صعوبات عندما يتعلق الأمر بالبيانات غير المكتملة أو السيئة.

4_تعتمد الخوارزميات على بيانات و فرضيات قد تكون خاطئة أو متحيزة، مما يؤدي إلى نتائج غير دقيقة.

ب_تحديات مهنية:

1_تنوع حلول الذكاء الاصطناعي يجعل من الصعب تحديد الأنواع الأنسب للتكنولوجيا في سياقات معينة.

2_يؤثر استخدام أدوات وتقنيات الذكاء الاصطناعي على علاقة العملاء، مثل استبدال الوكلاء البشريين ب Chabots

3_قلة الوعي بأهمية توظيف تقنيات الذكاء الاصطناعي، إلى جانب عدم اقتناع صانعي القرار بأهميتها في الوقت الحالي.

4_محدودية الموارد البشرية المدربة في مجال الذكاء الاصطناعي.

5_خطر انتهاك الحقوق الشخصية أو خصوصية الأفراد عند جمع البيانات.

ج_تحديات اجتماعية:

1_يعتبر استخدام الذكاء الاصطناعي في بيئات العمل تهديدا للوظائف التي يشغلها حاليا موظفون بشر يون.

2_تواجه المؤسسات التي لا تعتمد على الذكاء الاصطناعي في اتخاذ القرارات انتقادات، و في نفس الوقت تلام إذا استخدمت المتدخلات التكنولوجية فقط.

د_تحديات أخلاقية:

1_حساسية البيانات المستخدمة في تغذية الخوارزميات تتطلب سرية تامة.

2_إمكانية حدوث التحيز نتيجة أخطاء في البيانات أو نقص في الكمية.

3_التركيز على الربح كهدف أساسي لاستخدام خوارزميات الذكاء الاصطناعي قد يؤدي إلى نتائج سلبية.[28]

الفرع الثاني: الحلول المبتكرة لمواجهة تحديات حماية الخصوصية فيعصر الذكاء الاصطناعي

في ظل التكنولوجيا الحديثة والتحديات التي نواجهها، يمكننا استعراض مجموعة من الحلول التي تساعد في التعامل مع المخاطر التي قد تهدد الخصوصية في عصر الذكاء الاصطناعي:

1_**تشفير البيانات:** يعتبر تشفير البيانات من أبرز الإجراءات اللازمة لحماية المعلومات الحساسة. ينبغي على الشركات والمؤسسات استخدام تقنيات تشفير قوية لضمان حماية البيانات المخزنة والمرسلة ضد الوصول غير المصرح به.

[28] مجدي صلاح طه المهدي، مرجع سابق.

2_**تطوير سياسة الخصوصية:** يتعين على الحكومات والمؤسسات وضع سياسة وقوانين واضحة لحماية خصوصية البيانات، كما يجب أن تشمل هذه السياسات معايير دقيقة لجمع البيانات وكيفية استخدامها، مع تحديد العقوبات المناسبة للانتهاكات. إن مثل هذه السياسات تسهم في بناء ثقة المستخدمين وتضمن استخداما آمنا للذكاء الاصطناعي.

3_**الوعي والتثقيف:** الخطوة الأولى لحماية أنفسنا تكمن في زيادة الوعي والتثقيف حول المخاطر المحتملة. يجب على الأفراد فهم كيفية جمع البيانات واستخدامها، بالإضافة إلى التعرف على التهديدات السيبرانية وكيفية التصدي لها.

4_**استخدام أدوات الأمان:** توجد العديد من الأدوات التي يمكن استخدامها لتعزيز الأمان الشخصي. من بين هذه الأدوات:

. برامج مكافحة الفيروسات: تعمل على حماية الأجهزة من البرمجيات الضارة والهجمات السيبرانية.

توفر طبقة إضافية من الأمان أثناء تصفح الانترنت، مما(vpn). الشبكات الخاصة الافتراضية: يسهم في حماية البيانات من التجسس.

. مديرو كلمات المرور: يساعدون في إنشاء كلمات مرور قوية وفريدة لكل حساب، مما يقلل من خطر الاختراق.

. الحذر من الروابط والملفات المشبوهة: ينبغي توخي الحذر عند التعامل مع أي روابط أو ملفات غير معروفة، حيث يمكن أن تكون وسيلة لانتشار البرمجيات الخبيثة أو سرقة البيانات.

باستخدام هذه الحلول المبتكرة، يمكن للأفراد و المؤسسات تعزيز حماية الخصوصية في عصر الذكاء الاصطناعي.[29]

[29] مقال منشور على موقع الأمان و خصوصية البيانات عند استخدام الذكاء الاصطناعي، تحت عنوان الأمان و خصوصية البيانات عند استخدام الذكاء الاصطناعي،ديسمبر 2024، تم الاطلاع عليه بتاريخ 2025/06/07على الساعة 23:00 سا، في الموقع: https://uid.web.com

خاتمة

في ختام هذا البحث، يتضح أن الذكاء الاصطناعي يحمل في طياته إمكانية هائلة يمكن أن تسهم في تحسين جودة حياتنا، لكنه في الوقت نفسه يثير تحديات جمة تتعلق بحماية الخصوصية والحياة الخاصة للأفراد. فقد بينا أن الاعتماد المتزايد على تقنيات الذكاء الاصطناعي أدى إلى جمع كميات ضخمة من البيانات الشخصية، مما يثير مخاوف حقيقية من انتهاك الخصوصية وسوء استخدام هذه البيانات.

من خلال استعراضنا للأطر القانونية، والتقنيات الحديثة، ودور المجتمع، اتضح أن حماية الحياة الخاصة في عصر الذكاء الاصطناعي تتطلب تضافر الجهود بين الجهات التشريعية، التقنية، والمجتمعية. فالقوانين يجب أن تتطور بسرعة لتواكب الابتكارات، والحلول التقنية ينبغي أن تصمم بما يحترم الخصوصية من أساسها، بينما يلعب الوعي المجتمعي دورا حاسما في فض المساءلة والشفافية.

وفي ظل التحديات المستقبلية المتنامية، يبقى الالتزام بالمبادئ الأخلاقية والابتكار في حماية البيانات هو السبيل الأنجح لضمان تحقيق توازن بين التقدم التكنولوجي واحترام خصوصية الأفراد. إن مستقبل الذكاء الاصطناعي لا ينبغي أن يكون مصدر تهديد، بل فرصة لتعزيز الحقوق الرقمية وحماية الخصوصية في عالم متصل ومتطور.

من خلال بحثنا توصلنا إلى هذه النتائج التالية:

*معظم الأطر القانونية الحالية غير قادرة على مواكبة التطور التكنولوجي السريع.

*كذلك هناك حاجة ملحة لتحديد القوانين وإنشاء هيئات وطنية مستقلة تهتم بحماية المعطيات الشخصية.

*تعتبر حماية البيانات الشخصية من الحقوق الأساسية للأفراد، إذ تساهم في الحفاظ على الخصوصية، والتي تعتبر أحد العناصر الأساسية لحقوق الإنسان الرقمية في العصر الحالي.

*تتنوع أشكال التهديد التي تمثلها وسائل وأدوات التكنولوجيا على الحق في الخصوصية، بدءا من اختراق الأنظمة المعلوماتية، وصولا إلى الجرائم الناتجة عن الدخول غير المصرح به، والتصنت، وتوزيع الفيروسات، ورصد الاتصالات واعتراضها.

*في الجزائر، توجد جهة إدارية مخصصة للحفاظ على الحق في الخصوصية في الفضاء الرقمي، ويمكن اعتبارها ضمانة إدارية تعنى بحماية هذا الحق في ظل التطورات التكنولوجية، بالإضافة إلى الضمانات القانونية المنصوص عليها في الدستور.

*نتيجة لتأثير التكنولوجية الحديثة على الحق في الخصوصية، بدأ التركيز يتجه بشكل أكبر نحو حماية البيانات الشخصية، باعتبارها جانبا معنويا مهما في الحياة الخاصة.

في ضوء ما سبق، نقترح مجموعة من الاقتراحات في هذا المجال:

*ضرورة سن قوانين حديثة تتماشى مع المعايير الدولية.

*تعزيز ثقافة الوعي الرقمي والخصوصية لدى الأفراد.

*إنشاء هيئات وطنية مختصة بمراقبة ومعالجة الإنتهاكات الرقمية.

*يجب اتخاذ إجراءات قانونية صارمة لضمان حقوق الإنسان وحماية سلامة بيانات الأفراد.

*تعزيز دور الدولة في وضع ضوابط واضحة لاستخدام تقنيات الذكاء الاصطناعي داخل البلاد.

*إعادة تقييم القوانين الحالية لضمان حماية شاملة وفعالة للمواطنين ضد الاستخدام غير المشروع لبياناتهم في سياق تطبيقات الذكاء الاصطناعي.

*توسيع نطاق تطبيق تقنيات حماية الخصوصية، مثل استخدام وسائل التشفير، وتطوير استراتيجيات التستر، وضمان سرية البريد الالكتروني.

*ضرورة تنظيم دورات تدريبية متخصصة للقضاة والمحامين لتثقيفهم حول ما يعرف بقانون المعلومات الشامل.

*ينبغي أن تكون الحلول التقنية والقانونية والتنظيمية متكاملة لمواجهة المخاطر المتعددة التي تهدد خصوصية الأفراد في العصر الرقمي. كما ينبغي توفير إطار قانوني ملائم، بالإضافة إلى إنشاء لجنة مستقلة تهتم بضمان حماية الخصوصية الرقمية للأفراد في الفضاء الرقمي.

قائمة المراجع

أولا: باللغة العربية:

أ_الكتب:

1_آلان بونيه، **الذكاء الاصطناعي**، دار علم المعرفة، الكويت، 1993.

2_أشرف توفيق شمس الدين، الصحافة والحماية للحياة الخاصة (دراسة مقارنة)، دار النهضة العربية، مصر، 2008.

3_رمضاني مراد، **الذكاء الاصطناعي وعملية صنع القرار**، دار العيون للنشر الالكتروني، وهران، 2024.

4_فاضل باسم محمد، **حماية الخصوصية عبر البيئة الرقمية**، دار الفكر الجامعي، الإسكندرية، 2021.

5_فايز البرشة، **حماية ونزع حماية البرامج "منظومة MSDOS"**، دار الطبيعة الجديدة، سوريا، 1997.

6_موسى عبد الله، **الذكاء الاصطناعي**، دار الكتب المصرية، القاهرة، 2019.

7_كامل الأهواني حسام الدين، **الحق في احترام الحياة الخاصة الحق في الحياة الخصوصية**، دراسة مقارنة، د.ط، دار النهضة العربية، 1978.

ب_ الرسائل والمذكرات الجامعية

1_رسائل الدكتوراه

1_عابد جميل السفياني، **إيجابيات الذكاء الاصطناعي وسلبيات الذكاء الاصطناعي على المنظومة التعليمية**، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص: إدارة أعمال، جامعة ستاردوم، تركيا، 2024.

*2*_كحلاوي عبد الهادي، **الحماية القانونية للبيانات الشخصية في التشريع الجزائري**، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص حقوق وحريات، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2022.

2_مذكرات الماستر

1_جوزي نور الهدى، أثر تطبيق الذكاء الاصطناعي و الذكاء العاطفي على جودة اتخاذ القرار، مذكرة لنيل شهادة الماستر، تخصص إدارة أعمال، كلية العلوم الاقتصادية و التجارية و علوم التسيير،جامعة ابن خلدون، تيارت،2022 .

2_حيدة سعاد، استخدام الذكاء الاصطناعي في تحسين عملية اتخاذ القرار في المؤسسة الاقتصادية، مذكرة لنيل شهادة الماستر، تخصص إدارة أعمال، كلية العلوم الاقتصادية، التجارية وعلوم التسيير، جامعة أحمد دراية، الجزائر، 2020.

3_عثماني رجاء، الحماية القانونية للحق في جريمة الحياة الخاصة، مذكرة لنيل شهادة الماستر، تخصص قانون عام، كلية الحقوق، جامعة بلحاج بوشعيب، عين تيموشنت، 2023.

4_مرزوق فاطمة، الحماية القانونية للحق في الحياة الخاصة عبر الانترنت، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2015.

5_نصر الله خيرة، جرائم تطبيقات التواصل الاجتماعي في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي و علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة د.مولاي الطاهر، سعيدة، 2022.

ج_المقالات

1_بن زيطة عبد الهادي، "آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون رقم18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،" **مجلة القانون و العلوم السياسية**، العدد01، كلية الحقوق و العلوم السياسية، جامعة أدرار،ص. ص115-117.

2_حلمي السعيد وفاء، "تقنية الذكاء الاصطناعي و حماية البيانات الشخصية"، **مجلة الشريعة و القانون**، العدد43، كلية الشريعة و القانون، جامعة الأزهر، 2024، ص.ص1402،1404 .

2_خلفي عبد الرحمان، "الحق في الحياة الخاصة في التشريع العقابي الجزائري"، **مجلة البحوث و الدراسات**، المجلد54، العدد03، كلية الحقوق، جامعة بجاية، الجزائر،2011، ص.ص95-97.

3_فرجان طيب، "أسس حماية الحق في الخصوصية بين القانون الدولي و القانون الوطني"، **مجلة الدراسات القانونية و الاقتصادية**، المجلد05، العدد03، جامعة المسيلة، الجزائر، 2023، ص.ص11596-1143 .

4_محمد الهادي، "تأثير الذكاء الاصطناعي و آثاره على العمل و الوظائف"، **مجلة الجمعية المصرية لنظم المعلومات و تكنولوجيا الحسابات**، المجلد37، العدد37، 2024، ص.ص01-03.

5_محمد عدنان محمد عبد الحميد، "_أثر تكنولوجيا المراقبة الحديثة على تحسين أداء حراس البلدية"، **مجلة المجتمع العربي لنشر الدراسات العلمية**، العدد74، الجزائر،2024، ص.ص112-114.

6_نور محمد عبد الله العزام،" دور الذكاء الاصطناعي في رفع كفاءة النظم الإدارية لإدارة الموارد البشرية"، **المجلة التربوية**، العدد04، كلية التربية، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية، 2021،ص.ص11-12 .

7_نرمين مجدي، "الذكاء الاصطناعي و تعلم الآلة"، **مجلة صندوق النقد العربي**، العدد03، الإمارات العربية المتحدة، أبو ظبي، 2020، ص.ص12-16 .

8_نزيه محمد علي،" دور التشريعات و القوانين الوطنية و الدولية الحاكمة لحماية أمن المعلومات"، **المجلة المصرية لبحوث الإعلام**، المجلد2025، العدد91، جامعة القاهرة، د.س.ن،ص.ص1287-1290.

د_**النصوص القانونية**

1_الدستور:

_الدستور الجمهورية الجزائرية الديمقراطية الشعبية، ج.ر.ج.ج، العدد76، المؤرخ في 08 ديسمبر 1996، المعدل بالقانون 02-03 مؤرخ في 10 أفريل 2002، ج.ر.ج.ج، العدد25 المؤرخ في 04 أفريل 2002، القانون 08-19 المؤرخ في 15 نوفمبر 2008، ج.ر.ج.ج، العدد 63 المؤرخ في 06 نوفمبر 2008، القانون رقم 16-01 المؤرخ في 06 مارس 2016، ج.ر.ج.ج، العدد 14، المؤرخ في 07 مارس 2016، المرسوم الرئاسي رقم 20-442، مؤرخ في 30 ديسمبر 2020، ج.ر.ج.ج، العدد 82، المؤرخ في 30 ديسمبر 2020.

2_**النصوص التشريعية**

1-قانون رقم 151، المؤرخ في 15 جويلية 2020، يتعلق بحماية البيانات الشخصية، ج،ر، عدد 28، المؤرخ في 15 يوليو 2020.

2_قانون رقم 18-07، مؤرخ في 10نوفمبر2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج، عدد34، المؤرخ في10 يونيو 2018.

3_قانون رقم09-04، المؤرخ في 5 أوت 2004، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، عدد47، المؤرخ في 16 أوت 2009.

4_قانون رقم 04-15، مؤرخ في 10 نوفمبر 2004، جٍ.ر.ج.ج، عدد71، المؤرخ في 10 نوفمبر 2004.

5_الأمر رقم 66-156، مؤرخ في 18 صفر1386، الموافق ل 08 يونيو 1996، متعلق قانون العقوبات، المعدل والمتمم.

6_الأمر رقم 75-58، مؤرخ في 20 رمضان 1395، الموافق ل 26 سبتمبر1975، المتضمن القانون المدني، ج.ر، العدد78، الصادر في 24 رمضان1395، الموافق ل30 سبتمبر1975، المعدل و المتمم.

3_ النصوص التنظيمية

_المرسوم الرئاسي261/15 مؤرخ في 08 أكتوبر2015، يحدد لتشكيلة و تنظيم و كيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ج.ر.ج.ج، عدد53 صادر في 08 أكتوبر 2015.

ذ: الوثائق الالكترونية

1_أحمد المسلماني، الهيئة الوطنية للإعلام، مارس 2023، تم الاطلاع عليه بتاريخ 2025/06/03، على الساعة 12:30 سا، في الموقع:
https://www.maspero.eg

2_أبيرامي فينا، لوائح الذكاء الاصطناعي الجديدة في كاليفورنيا، التركيز على الذكاء الاصطناعي الأخلاقي، أكتوبر 2024، تم الاطلاع عليه بتاريخ 2025/06/07، على الساعة 21:00 سا، في الموقع:https://www.ultralytics.com

3_ فيصل العتيقي، حماية البيانات في عصر الذكاء الاصطناعي، أوت 2023، تم الاطلاع عليه بتاريخ 2025/06/08، على الساعة 13:00 سا، على الموقع:https://www.mozn.ws

4_محمد ناصر، كيف تحمي خصوصيتك في عصر الذكاء الإصطناعي، فيفري 2025، تم الاطلاع عليه بتاريخ 2025/06/08، على الساعة 15:00 سا، على الموقع:https://techsmartdigest.com

5_ مقال منشور على الموقع IBM تحت عنوان قائمة التحقق من الإمتثال للائحة العامة لحماية البيانات GDPR، يناير 2024، تم الاطلاع عليه بتاريخ 2025/05/03، على الساعة 15:45 سا، على الموقع:https://www.ibm.com

5_مقال منشور على موقع welcome to the unitednationsتحت عنوان التعاهد الرقمي العالمي، أفريل 2025، تم الاطلاع عليه بتاريخ 2025/06/03، على الساعة 18:40 سا، على الموقع: https://www.un.org

6_مقال منشور على الموقعEuropean union Agency for FundamtalRightsتحت عنوان دليل قانون حماية البيانات الأوروبي، أبريل 2018، تم الاطلاع عليه بتاريخ 2025/06/03، على الساعة 19:07 سا، على الموقع: https://fra.eurpa.eu

7_مقال منشور على الموقع solixtechnologies,Inc. تحت عنوان ما هو قانون LIL ؟، يونيو 2025، تم الاطلاع عليه بتاريخ 2025/06/07، على الساعة 20:46 سا، على الموقع: https://www.solix.com

8_ La loi 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et libertés, plus connue sous le nom de loi informatique et libertés, est une loi française qui règlemente le traitement des données personnelles, sur le site : WWW.legifrance.fr

ثانيا: باللغة الفرنسية

Ouvrages :

1_Baffard William, Le système de traitement des infractions constatées et la protection des données personnelles , Mémoire de anti-narcotique informatique ET droit, Faculty of law de droit, Université de Montpellier 1 ,2003, p15.

2_ANCEL(Jean-Pierre) : Protection de la personne : Image et vie privée, Gazette du palais, No.254 ,1994,P.13-14.

فہرس

مقدمة: 6

الفصل الأول

الذكاء الاصطناعي كعامل تهديد متزايد للخصوصية:

المبحث الأول:جمع و معالجة البيانات الشخصية في عصر الذكاء الاصطناعي..... 7

المطلب الأول:مركزية البيانات الشخصية في عمل الذكاء الاصطناعي 7

الفرع الأول: تعريف البيانات الشخصية:..... 8

أولا: البيانات التعريفية:..... 9

ثانيا: البيانات الشخصية:..... 10

الفرع الثاني: مصادر البيانات الشخصية: 12

المطلب الثاني:أدوات و تقنيات المراقبة و انعكاساتها على الخصوصية..... 13

الفرع الأول: الأنظمة الذكية المتقدمة في المراقبة والتحليل:..... 13

الفرع الثاني: مخاطر الاستخدام في القطاعين العام والخاص: 14

المبحث الثاني:نماذج واقعية مهددة للخصوصية 17

المطلب الأول:قضية كامبريدج أنال تكيا 17

الفرع الأول: استغلال بيانات المستخدمين: 18

الفرع الثاني:شركةClearview AI 19

المطلب الثاني:التطبيقات اليومية و تأثيرها على الخصوصية..... 19

الفرع الأول: وسائل التواصل الاجتماعي: 20

الفرع الثاني: التجسس والمراقبة الالكترونية: 20

الفصل الثاني

الإطار القانوني لحماية الخصوصية في عصر الذكاء الاصطناعي

المبحث الأول:القوانين و التشريعات الدولية و الوطنية لحماية الخصوصية في ظل الذكاء الاصطناعي..... 24

المطلب الأول:القوانين و التشريعات الدولية 25

الفرع الأول: اللائحة العامة لحماية البيانات (GDPR) 26

الفرع الثاني: المبادئ والتوصيات الدولية: 27

أولا: توصية اليونسكو حول أخلاقيات الذكاء الاصطناعي:..... 28

ثانيا: إعلان الحقوق الرقمية للأمم المتحدة:..... 28

ثالثا: مبادرات مجلس أوروبا و لجنة حماية البيانات الأوربية:..... 29

المطلب الثاني:التشريعات الوطنية 30

الفرع الأول: قانون حماية البيانات في فرنسا (Loi informatique libertes)..... 31

الفرع الثاني: التشريعات العربية: 33

الفرع الثالث: الحماية الجنائية والمدنية للبيانات الشخصية في القانون الجزائري: 34

أولا: الحماية الجنائية للبيانات الشخصية: 34

ثانيا: المسؤولية المدنية عن انتهاك الخصوصية: 36

المبحث الثاني:الحلول التقنية لحماية الخصوصية في عصر الذكاء الاصطناعي..... 37

المطلب الأول:التقنيات الأساسية لحماية الخصوصية في عصر الذكاء الاصطناعي 37

الفرع الأول: التشفير وإخفاء الهوية:..... 38

الفرع الثاني: التعلم الآمن و تنفيذ إجراءات أمنية قوية: 38

الفرع الثالث: تدريب الموظفين وتعزيز الشفافية: 39

المطلب الثاني:التحديات المستقبلية و الحلول المبتكرة لحماية الخصوصية في عصر الذكاء

الاصطناعي..... 40

الفرع الأول: التحديات المستقبلية لحماية الخصوصية في عصر الذكاء الاصطناعي: 40

الفرع الثاني: الحلول المبتكرة لمواجهة تحديات حماية الخصوصية فيعصر الذكاء الاصطناعي:42

خاتمة: 46

قائمة المراجع 50

الملخص بالعربية:

تشكل هذه المذكرة مسألة مت إذا كان الذكاء الاصطناعي يشكل خطرا على الخصوصية. استعرضت المذكرة التحديات التي يطرحها الذكاء الاصطناعي من حيث جمع و تحليل البيانات الشخصية، و أبرزت الأطر القانونية الوطنية و الدولية لحماية الخصوصية، بالإضافة إلى الحلول التقنية مثل التشفير و التعلم الآمن. كما تناولت دور المجتمع المدني و الأفراد في تعزيز حماية البيانات. و في ضوء التحديات المستقبلية، اقترحت المذكرة حلولا مبتكرة لضمان التوازن بين التطور التكنولوجي و احترام الخصوصية.

Résumé en français :

Ce mémoire traite de la question de savoir si l'intelligence artificielle constitue un danger pour la vie privée. Il analyse les défis posés par l'lA en matière de collecte et d'analyse des données personnelles, en mettant en lumière les cadres juridiques nationaux et internationaux de protection de la vie privée ainsi que les solutions techniques comme le chiffrement et l'apprentissage sécurisé. Le role de la société civile et des individus dans la protection des données est également abordé. Enfin, face aux défis futurs, des solutions innovantes sont proposées pour garantir un équilibre entre progrès technologique et respect de la vie privée.