وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم الحقوق

المرجع: .....

**مذكرة نهاية الدراسة لنيل شهادة الماستر**

# انتهاك الخصوصية الشخصية في ظل أنظمة الذكاء الاصطناعي

ميدان الحقوق والعلوم السياسية

الشعبة: حقوق

التخصص: قانون قضائي

من إعداد الطالبة:

عتو هاجر

تحت إشراف الأستاذ:

بوسحبة الجيلالي

## أعضاء لجنة المناقشة

| | | |
|---|---|---|
| الأستاذ(ة) | زواتين خالد | رئيسا |
| الأستاذ(ة) | بوسحبة الجيلالي | مقرراً |
| الأستاذ(ة) | بن عوالي علي | مناقشا |

السنة الجامعية: 2024-2025

نوقشت في: 2025/06/22

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

# تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
# في إنجاز البحث

أنا الممضي أدناه،

السيد: ..... الصفة: ..... .....

الحامل لبطاقة التعريف الوطنية رقم: ..... والصادرة بتاريخ: .....

المسجل بكلية: ..... قسم: .....

والمكلف بإنجاز مذكرة ماستر بعنوان:

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: .....

إمضاء المعني

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها


بسم الله الرحمن الرحيم

# شكر وعرفان

ما سلكنا البدايات إلا بتيسيره، ولا بلغنا النهايات إلا بتوفيقه، وما حققنا الغايات إلا بفضله، فالحمد لله والشكر لله عزّ وجلّ على عظيم منّه وتوفيقه لإتمام هذا البحث.

كما أتقدم بجزيل الشكر وعظيم الامتنان إلى كل من علّمني حرفاً طيلة مساري الدراسي ولم يبخل عليّ بعطاءه، أساتذتي الأفاضل كل باسمه ومقامه. وأخص بالشكر والتقدير الأستاذ المشرف على هذه المذكرة على نصحه وإرشاده لي، كما أشكر لجنة المناقشة الموقّرة على قبولهم مناقشة هذا العمل وإثرائه بملاحظاتهم القيمة.

ولا يفوتني أن أشكر جميع الساهرين على كلية الحقوق والعلوم السياسية، وكذا مكتبة الكلية، على توفيرها لنا الكتب والمراجع المستحدثة، دون أن أنسى عمّال المكتبة على حسن استقبالهم وطيب تعاملهم معنا.

وأخيرًا، شكرٌ موصول لكل من مدّ لنا يد العون، بكلمة، أو دعاء، أو دعم معنوي، من الأقارب والأصدقاء، ومن عرفناهم أو لم نعرفهم، فلكم منّا أصدق الدعاء وخالص العرفان.

# إهداء

**الحمد لله على لذّة الإنجاز، والحمد لله عند البدء والختام**

انتهت الرحلة، ولم تكن سهلة، وليس من المفترض أن تكون كذلك، فطريق النجاح لا يُفرش بالورود، بل يُعبّد بالصبر والكدّ والسهر...

ومهما طالت، فستمضي بحلوها ومرّها، وها أنا الآن وبعون الله تعالى، أتممت هذا العمل وآخر ما يخطّه قلمي في هذه المذكرة، هو ما خُتمت به الدعوات الصادقة:

**(وَآخِرُ دَعْوَاهُمْ أَنِ ٱلْحَمْدُ لِلَّهِ رَبِّ ٱلْعَٰلَمِينَ)**

وبكل حب أهدي ثمرة جهدي ونجاحي:

إلى من أحمل اسمه بكل افتخار، إلى من كلّله الله بالهيبة والوقار...والدي العزيز.

إلى من جعل الله الجنة تحت أقدامها، إلى التي آثرت راحتي على راحتها، ولم تُحملني من أعباء البيت شيئًا، كي أتفرغ لإتمام هذه المذكرة وتحقيق النجاح...أمي الغالية.

أسأل الله أن يطيل في عمركم لأصل يومًا، وأردّ لكم بعضًا من جميلكم.

إلى من رزقني الله بوجودهم، وجمعني معهم تحت سقف واحد...أخوايَ وأختايَ الصغيرتين، أدامَكم الله ضلعاً ثابتاً لي.

إلى كليّتي...التي احتضنت مسيرتي، وأسهمت في صقل فكري وتوجيهي

أهدي لها هذا العمل المتواضع، راجية أن يكون لبنة تُضاف إلى رصيد البحث القانوني بها.

إلى نفسي التي راهنت على النجاح...

إلى تلك الروح التي تعثّرت، ووقفت، وثابرت...

أهديك هذا التعب، وهذه الثمرة، وهذا النبض الذي سُكِبَ في كل صفحة.

## قائمة المختصرات:

ص: الصفحة

ط: الطبعة

د ط: دون طبعة

ج ر: الجريدة الرسمية

AI : Artificielle Intelligence.

P : Page.

.op. cit : référence déjà citée

.ibid : même référence

J.O : Journal Officiel.

.n° : numéro

§ : paragraphe .

# المقدمة

## المقدمة:

شهد العالم في العقود الأخيرة طفرة تكنولوجية غير مسبوقة، تصدّرها الذكاء الاصطناعي باعتباره إحدى أكثر التقنيات تطورًا وتأثيرًا في حياة الإنسان، حيث يعتبر من بين أبرز التطبيقات الحديثة لتكنولوجيا الاتصال والمعلومات، إذ نشأ كأحد فروع علوم الحاسوب التي تُعنى بدراسة طبيعة الذكاء البشري ومحاكاته، بهدف تطوير جيل جديد من الحواسيب الذكية التي يمكن برمجتها لإنجاز الكثير من المهام المعقّدة التي تتطلب قدرات عالية على الاستنتاج والاستنباط والإدراك.[1]

وبفضل خصائصه المتطوّرة وميزاته اللامحدودة أصبح الذكاء الاصطناعي يسهم بفعالية في تسهيل أداء العديد من المهام اليومية، ويضطلع بدور مهم في الكثير من المهام الحسّاسة كالمساعدة في تشخيص الأمراض ووصف الأدوية والاستشارات القانونية والمهنية والتعليم التفاعلي والمجالات الأمنية والعسكرية وغيرها من المجالات الأخرى.[2]

غير أن هذا الاستعمال المتعاظم لتقنيات الذكاء الاصطناعي يوازيه تزايد الشكوك بشأن مدى قدرتها على حماية البيانات الشخصية، وذلك نظراً للحاجة الدائمة لخوارزميات الذكاء الاصطناعي إلى مدخلات مستمرة من البيانات وإلى تغذية وتحديث وتدريب دائم. حيث تتغذى هذه الخوارزميات على كم من هائل من المعلومات والبيانات التجريبية المبنية على الحياة الواقعية المستقاة من خبرات البشر ووعيهم وتفاعلهم مع هذه التقنية الحديثة، ما يفرض بالضرورة اطلاعها على بياناتهم الشخصية من أجل معالجتها وتحليلها.[3]

---

[1] مدحت محمد أبو النصر، الذكاء الاصطناعي في المنظمات الذكية، ط1، المجموعة العربية للتدريب والنشر، القاهرة، 2020، ص131.

[2] عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، د ط، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 2005، ص9.

[3] محمد الهادي السهيلي، تطوّرات الذكاء الاصطناعي ومقتضيات حماية الحقوق والحريات الأساسية، إدارة الشؤون القانونية بمنظمة الإيسيسكو (منظمة العالم الإسلامي للتربية والعلوم والثقافة)، المملكة المغربية، 2021، ص7.

وهو ما يجعل دراسة هذه الإشكالية ضرورة ملحّة في الوقت الحالي، خاصة في ظل التوجه المتسارع نحو الرقمنة وتقييد حياة الإنسان الخاصّة في سجلات إلكترونية، مما يسهل تعرضها للانتهاك سواء من قبل تقنيات الذكاء الاصطناعي ذاتها أو من طرف الجهات التي تقوم باستغلال هذه التقنيات لأغراض غير مشروعة، كالتجسس على الأفراد، أو جمع بياناتهم دون علمهم، أو بيعها لشركات تجارية. وتفتح هذه الانتهاكات الباب الواسع أمام ممارسات أكثر خطورة، كالابتزاز، أو التشهير، أو التلاعب بالسلوك الفردي.

الأمر الذي يقتضي تدخّل المشرّع لحمايته بالأسلوب الذي يتفق وطبيعة هذه المخاطر، في ظلّ تطوّر تطبيقات الذكاء الاصطناعي وسهولة انتهاك حق الخصوصية والبيانات الشخصية، التي أوجبت مزيداً من الحماية لهذا الحق.[1]

ويزداد الموضوع أهمية، كونه يتعلق بأحد أبرز حقوق الإنسان في العصر الرقمي وارتباطه الوثيق بكرامة الإنسان ألا وهو الحق في الخصوصية، والذي كفلته الشريعة الإسلامية الغراء، كما أقرّته مختلف الدساتير الوطنية والصكوك الدولية باعتباره من الحقوق الأساسية التي تضمن حرية الفرد وكرامته الإنسانية.

وتهدف دراستنا إلى التعرّف على مضمون الحق في الخصوصية والتطورات الحاصلة له بفعل التقدّم التكنولوجي، ممّا أدّى إلى تغير معالمه وبروز جانب جديد يعنى بخصوصية المعلومات والبيانات الشخصية. وكذا الوقوف على ماهية أنظمة الذكاء الاصطناعي باعتبارها آخر مخرجات الثورة التكنولوجية، وتسليط الضوء على أبرز الانتهاكات التي قد تمس الحق في الخصوصية في ظل الاستخدام المتزايد لهذه الأنظمة، كما تسعى الدراسة إلى اقتراح السبل الكفيلة لحماية هذا الحق، والبحث عن إمكانية تحقيق توازن فعّال بين متطلبات استخدام الذكاء

[1] نرمين عبد القادر إمبابي، تأثير استخدام روبوت المحادثة الذكية "شات جي بي تي" على حماية خصوصية بيانات المستفيدين: دراسة مسحية مقارنة، المجلة العلمية للمكتبات والوثائق والمعلومات، مجلد6، عدد19، كلية الآداب_جامعة القاهرة، يوليو 2024، ص45.

الاصطناعي والاستفادة من مزاياه، وبين ضرورة صون الحقوق الأساسية للأفراد وفي مقدّمتها الحق في الخصوصية.

ويعود اختيارنا لهذا الموضوع إلى مجموعة من الأسباب الموضوعية والذاتية، فمن الناحية الموضوعية، يفرض تسارع التطورات التكنولوجية، وعلى رأسها تقنيات الذكاء الاصطناعي، تحديات قانونية غير مسبوقة تهدّد حقوق الإنسان لاسيما الحق في الخصوصية، الذي أضحى عرضة لانتهاكات خطيرة بسبب طرق جمع البيانات وتحليلها واستخدامها دون رقابة كافية أو موافقة صريحة من الأفراد، وهو ما يجعل من الضروري إيجاد آليات قانونية كفيلة تواكب هذا التحول، وتضمن التوازن بين متطلبات التطور التكنولوجي وضمان حماية الحقوق والحريات الفردية.

أمّا من الناحية الذاتية، فقد انطلقت هذه الدراسة من اهتمام شخصي ببحث القضايا المستجدة لاسيما ما يتعلق بالذكاء الاصطناعي الذي أصبح اليوم حديث الساعة، وكوننا طلبة وباحثين في المجال القانوني فإن اهتمامنا ينصب حول دراسة الإشكالات القانونية بهدف إيجاد الحلول المناسبة لها، وأوّل مشكلة جالت في أذهاننا ولفتت انتباهنا هي مشكلة الخصوصية والتحديات التي تواجهها في عصر الذكاء الاصطناعي القائم في جوهره على جمع كميات ضخمة من البيانات، الأمر الذي يجعل حق الخصوصية على المحكّ. ضف إلى ذلك قلّة الدراسات المتخصصة في هذا الموضوع المهمّ، ممّا يستدعي إيلاءه بما يكفي من الاهتمام والبحث القانوني المعمق.

وبطبيعة الحال قد واجهتنا العديد من الصعوبات أثناء إنجاز هذا البحث، كان أبرزها ندرة المراجع العربية المتخصصة التي تتناول العلاقة بين الذكاء الاصطناعي والحق في الخصوصية، وهو ما دفعنا إلى اللجوء للمراجع الأجنبية والذي تطلّب ترجمتها وقتًا وجهدًا كبيرين. كما أنّ عدم وجود الدراسات الأكاديمية السابقة، من مذكرات ورسائل دكتوراه ذات الصلة المباشرة بالموضوع، أدّى بنا إلى الوقوع في بعض الإشكالات عند محاولة ضبط خطة

البحث وتقسيمه خاصّة فيما يتعلّق بصور الانتهاك، وما زاد الأمر تعقيدا هو الطبيعة التقنية لهذا الموضوع. ما سبّب لنا في كثير من الأحيان شعورًا بالإحباط وأثّر سلباً على نفسيتنا، غير أن شغفنا بالموضوع وإيماننا بأهميته كان دافعًا للاستمرار والمثابرة.

وانطلاقًا ممّا سبق، تبرز الإشكالية المحورية التي تسعى هذه الدراسة لمعالجتها، والتي يمكن صياغتها على النحو التالي:

**إلى أي مدى أصبح الذكاء الاصطناعي يشكل تهديدًا للحق في الخصوصية الشخصية؟**

وتتفرع عنها مجموعة من التساؤلات:

**كيف يمكن لأنظمة الذكاء الاصطناعي أن تنتهك خصوصيتنا؟**

**ماهي أغراض جمع البيانات الشخصية ومخاطرها على حياة الأفراد؟**

**ماهي السبل الكفيلة لحماية الحق في الخصوصية في ظل تطور أنظمة الذكاء الاصطناعي؟**

وللإجابة على هذه الإشكالية اعتمدنا المنهج الوصفي والتحليلي من خلال وصف الانتهاكات التي يتعرّض لها الحق في الخصوصية في ظل أنظمة الذكاء الاصطناعي، وتحليل الآليات القانونية والأطر الأخلاقية المخصّصة لحمايته. كما استعنا بالمنهج المقارن للوقوف على التجارب القانونية المختلفة في التعامل مع هذه الإشكالية، واستخلاص ما يمكن الاستفادة منه في سبيل تعزيز حماية هذا الحق في التشريع الجزائري.

وبناءً على ما سبق، فقد ارتأينا تقسيم هذه الدراسة إلى فصلين اثنين، يتناول الأول الإطار المفاهيمي للحق في الخصوصية والتحديات التي تواجهه في عصر الذكاء الاصطناعي، الذي بدوره ينقسم إلى مبحثين، يعالج الأول تطور مفهوم الحق في الخصوصية، أمّا الثاني فجاء بعنوان الذكاء الاصطناعي وانعكاساته على الحق في الخصوصية.

فيما خصّصنا الفصل الثاني لمعالجة آليات حماية الحق في الخصوصية في عصر الذكاء الاصطناعي، من خلال مبحثين، تطرقنا في المبحث الأول منه إلى الحماية القانونية للحق في الخصوصية، أما بالنسبة للمبحث الثاني فتضمن الحماية التقنية والأخلاقية.

# الفصل الأول

## الإطار المفاهيمي للحق في الخصوصية والتحديات التي تواجهه في عصر الذكاء الاصطناعي

## تمهيد

يعد الحق في الخصوصية من الحقوق اللصيقة بالشخصية، وهي الحقوق التي لا يستطيع الانسان العيش بدونها في حرية وبصورة طبيعية. وتؤول إلى الفرد لأنه بشر أي حقوقه كإنسان، التي يمتلكها الفرد ببساطة منذ مولده وحتى وفاته، فهي لصيقة بشخصه وتنبع من الكرامة المتأصلة في الشخصية الإنسانية.[1]

وبالتالي فإن هذا الحق هو من أقدم حقوق الانسان، ظهر بشكل ضمني في المجتمعات القديمة، حيث كانت التقاليد والعادات تفرض احترام الحقوق والحريات الخاصة للأفراد، سواء في المنازل أو المراسلات الشخصية، ثم تطور لاحقًا ليحظى باعتراف قانوني في دساتير وتشريعات الدول الحديثة.

ومع التطورات التكنولوجية، ولا سيما الثورة الرقمية وانتشار أنظمة الذكاء الاصطناعي، شهد مفهوم الحق في الخصوصية تغيرا جذريا، فلم يعد يقتصر على حق الفرد في حرمة مسكنه والعيش في حرية بعيدا عن تطفل الاخرين وتدخلهم في مختلف جوانب حياته الأسرية والعاطفية والصحية والمالية.... وإنما تعدى ذلك ليشمل الحق في حماية بياناته ومعلوماته الشخصية المخزنة على جهاز الحاسوب أو الهواتف الذكية أو غيرها من الوسائل التكنولوجية الحديثة التي أصبحت معرضة لانتهاكات لا حصر لها عبر الشبكة العنكبوتية وبفعل أنظمة الذكاء الاصطناعي على وجه الخصوص.

وعلى ضوء ما سبق سنعالج تطور مفهوم الحق في الخصوصية في (المبحث الأول) فيما سنخصص (المبحث الثاني) للذكاء الاصطناعي وانعكاساته على الحق في الخصوصية.

[1] وليد سليم النمر، حماية الخصوصية في الأنترنت، الطبعة الأولى، دار الفكر الجامعي ،الإسكندرية،2017، ص169.

## المبحث الأول: تطور مفهوم الحق في الخصوصية

شهد مفهوم الحق في الخصوصية تطورًا ملحوظًا عبر العصور، حيث ارتبط في بداياته بحماية الحياة الخاصة للأفراد من أي تدخل غير مرغوب فيه ومع تقدم المجتمعات وظهور التقنيات الحديثة، توسع هذا المفهوم ليشمل أبعادًا جديدة.

ولهذا كان من الضروري تبيان المفهوم التقليدي للحق في الخصوصية (المطلب الأول)

ومن ثم التعرف على المفهوم الحديث لهذا الحق في ضوء المستجدات التقنية في (المطلب الثاني).

### المطلب الأول: المفهوم التقليدي للحق في الخصوصية

لم تتفق التشريعات المقارنة على وضع تعريف للحق في الخصوصية أو الحياة الخاصة ويبدو أن ذلك راجع لصعوبة تحديد العناصر التي تشتمل عليها الخصوصية الفردية ، ورغم أن كلاّ من المشرع الجزائري والمشرع الفرنسي يتخذان من الحياة الخاصة مرجعا لردع المساس بحرمتها جزائيا إلا أنهما لم يعرفا مفهوم هذه العبارة ولم يحددا طبيعتها القانونية[1]

وأمام هذا الفراغ التشريعي ستتمحور دراستنا على تعريف الحق في الخصوصية من الناحيتين اللغوية والاصطلاحية وذلك في (الفرع الأول) ثم نتعرف على المفهوم الذي جاءت به شريعتنا الإسلامية (الفرع الثاني)، وأخيرا سنحاول عرض أبرز المحاولات الفقهية لتحديد مضمون هذا الحق (الفرع الثالث).

#### الفرع الأول: التعريف اللغوي والاصطلاحي

**أولا/ تعريف الخصوصية لغة**

لقد جاء في معجم لسان العرب أن لفظ "خصوصية" هو من الفعل "خصص" فيقال خصّه بالشيء يخُصّه خَصّاً وخُصوصاً وخَصُوصِيّةً وخُصُوصِيّةً والفتح أَفصح وخِصِّيصَى وخصّصَه

[1] نويري عبد العزيز، الحماية الجزائية للحياة الخاصة في القانونين الجزائري والفرنسي "دراسة مقارنة"، الطبعة الثانية ،دار هومة، بدون بلد النشر،2016، ص 55،61.

واخْتصّه أَفْرَدَه به دون غيره ويقال اخْتصّ فلانٌ بالأَمر وتخصّصَ له إذا انفرد وخَصّ غيرَه واخْتصّه بِبِرّهِ ويقال فلان مُخِصٌّ بفلان أَي خاصّ به وله به خِصِّية.[1]

وفي معجم اللغة العربية المعاصرة، "خصوصية" هي: مصدر خَصَّ، هذا الموضوع له خصوصيّة له أهمية تميّزه عن غيره. مؤنَّث خُصوصيّ: ما يتعلّق بشخص أو بمجموعة أو بشيء محدّد دون سواه "سيارة خصوصيّة، رسائل خصوصيَّة: سريَّة".

خصوصيَّات الشَّخص: شئونه الخاصّة به.[2]

فالخصوصية من وجهة النظر اللغوية تقترب من مفهوم السر، لكن لا يمكن اعتبارهما كلمتين مترادفتين، ذلك أن السرية تفترض الكتمان والتخفي ،في حين أنّ الخصوصية وإن كانت تفترض قدرا من الكتمان والتخفي لكنها قد تتوافر رغم انعدام السرية.[3]

**ثانيا/ تعريف الخصوصية اصطلاحا:**

الخصوصية في الاصطلاح تعني ذات المعنى في اللغة حيث يعبر عنها الفقهاء بذات المعنى اللغوي، بأنه كل ما يُخصّ بشيء دون غيره، فيقال إنّ هذا الشيء خصوصية له.[4]

وتتعدد التسميات التي تطلق على هذا الحق بين من يعتمد على مصطلح الحق في الخصوصية، وبين من يعتمد على مصطلح الحق في الحياة الخاصة، وإن كان هذا الأخير

[1] موقع لشرح المصطلحات، متاح على الرابط: https://www.arabdict.com، تاريخ الإطلاع:12-02-2025، على الساعة 19:00.

[2] المرجع نفسه.

[3] عماد حمدى حجازي، الحق في الخصوصية ومسؤولية الصحفي في ضوء أحكام الشريعة الإسلامية والقانون المدني، دط، دار الفكر الجامعي، الإسكندرية، 2008، ص 18-19.

[4] شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية(دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا)، مجلة البحوث القانونية والاقتصادية، العدد 57، أفريل 2015، ص5.

هو المصطلح الأول والتقليدي إلا أن المصطلح السائد والشائع اليوم هو الحق في الخصوصية، وغالبا ما يجمع الباحثون بين المصطلحين بالرغم من وجود بعض الفروق بينهما.[1]

لم تستخدم غالبية التشريعات لفظ الخصوصية ماعدا التشريع الأمريكي، فالاصطلاح المعروف في النظام القانوني الأنجلو ساكسوني هو اصطلاح الخصوصية (PRIVACY)

في حين أنّ الاصطلاح السائد في النظام القانوني اللاتيني عموما والفرنسي على وجه الخصوص والمعبرة عن ذات الحق ومرادفاته هو اصطلاح الحق في الحياة الخاصة

[2] Le droit à la vie privée

**الفرع الثاني: تعريف الحق في الخصوصية في الشريعة الإسلامية**

إنّ عدم ذكر مصطلح الخصوصية أو الحق في الحياة الخاصة من قبل فقهاء الشريعة الإسلامية جعل الكثيرين يظنون أنّها أغفلت هذا الحق ولم تجعله ضمن منظومتها التشريعية لكن الأمر عكس ذلك تماما، فالدين الإسلامي قد اعترف به منذ القدم وجعله ينطوي تحت مفهوم الحق عموما.[3]

فحقوق الانسان لا يعود الاعتراف بها الى الغرب وكتابات مفكريه، أو مما سجلته العهود والمواثيق الدولية كما يزعمون ، وإنما هي مبادئ أصيلة سبقت بها الشريعة الإسلامية، فهي من وضع المولى عزّ وجلّ.[4]

[1] بن حيدة محمد، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"، مذكرة ماجستير، تخصص حقوق وحريات كلية الآداب والعلوم الإنسانية، الجامعة الإفريقية العقيد أحمد دراية، أدرار،2009_2010 ،ص22

[2] يونس عرب، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات بنادي المعلومات العربي،2002، الأردن، ص3.

[3] خالد حسن أحمد، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية دراسة مقارنة، د ط، دار الكتب والدراسات العربية،2020،ص20.

[4] وليد سليم النمر، مرجع سابق، ص 226_227.

ويظهر ذلك في تكريم الإنسان وصيانة حرماته، كما جاء في قوله تعالى:" **ولقد كرّمنا بني آدم وحملناهم في البرّ والبحر ورزقناهم من الطيّبات وفضّلناهم على كثير ممن خلقنا تفضيلا**".[1]

وينبغي علينا التنويه بأنّ الشريعة الإسلامية قد أرست حرمة حقّ الانسان المسلم في الخصوصية بكافة صورها ومظاهرها وسنتعرض إلى بعض هذه الصور.

**أولا: حرمة المسكن**

يشكل المسكن ساحة الأمان التي يعيش الإنسان في إطارها وفي نطاقه يشبع الإنسان تلبية حاجاته التي تنعكس على نموه البيولوجي والاجتماعي والنفسي السليم، ولكي يحقق المسكن هذه الإشباعات فإنه ينبغي تأكيد مبدأ الخصوصية داخله الذي يحول دون المتطفلين وكشف أسراره وأسرار عائلته[2]. وفي هذا السياق قال الله تعالى: "**يا أيّها اللذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على أهلها ذلكم خير لكم لعلكم تذكرون**"[3] فلحماية بيوت المسلمين أوجب الله تعالى الاستئناس وهو الاستئذان ونهى عن دخول البيوت دون استئذان خوف الكشف عن المحرمات.[4]

[1] سورة الإسراء ،الآية 70.

[2] يسن عبد اللطيف عبد الحليم محمد ،أحكام المسؤولية الناشئة عن انتهاك حرمة الحق في الخصوصية عبر وسائل التقنية الحديثة "دراسة فقهية معاصرة"، مجلة كلية الدراسات الإسلامية والعربية للبنات بكفر الشيخ، المجلد الخامس، العدد الثاني 2018، ص 555.

[3] سورة النور، الآية 27.

[4] محمد راكان الدغمي، حماية الحياة الخاصة في الشريعة الإسلامية، الطبعة الأولى، دار السلام، القاهرة، 1985، ص21.

**ثانيا: تحريم التجسس:**

لقد نهى الإسلام عن التجسس لأنه ينطوي على كشف لما أراد الله تعالى ستره على المسلم، ولأن فيه انتهاك لحرمات وخصوصيات العباد وتدخل الغير فيما لا يخصه، وذلك في قوله تعالى: "**يا أيها الّذين آمنوا اجتنبوا كثيرا من الظنّ إنّ بعض الظنّ إثم ولا تجسّسوا**".[1]

والتجسس على الناس هو تتبع عوراتهم وهم في خلواتهم إما بالنظر إليهم من دون أن يشعروا بذلك، وإما باستراق السمع من دون علمهم وإما بالاطلاع على مكتوباتهم ووثائقهم وأسرارهم وهم يخفونه عن أعين الناس دون إذن منهم.[2]

**ثالثا: حفظ الأسرار وعدم كشفها:**

ولعلّ أول نموذج حق كل من الزوجين على الآخر ألاّ ينقل أسراره ولا يفشيها، والأصل فيه ما رواه عبد الرحمان بن سعد قال سمعت أبا سعيد الخدري يقول "**قال رسول الله صلى الله عليه وسلّم: إن أعظم الأمانة عند الله يوم القيامة الرجل يفضي الى زوجته وتفضي اليه ثم ينشر سرها**" [3]. ناهيك عن الأسرار التي تكون بين عامة الناس وأسرار المريض والميت وكذلك السر المهني.

وبهذا يتضح أن الشريعة الإسلامية بالرغم من عدم إتيانها تعريفا محددا للخصوصية إلا أنها قد أوضحت معالمها من خلال إبرازها لمختلف مظاهرها وتطبيقاتها في القرآن الكريم والسنة النبوية.

**الفرع الثالث: التعريف الفقهي**

تعدّ فكرة الحق في الخصوصية من الأفكار المرنة التي أثارت جدلا وخلافا كبيرين بين فقهاء القانون حول مضمون هذا الحق ووضع تعريف محدد له.

---

[1] وليد سليم النمر، مرجع سابق،247.

[2] عصام أحمد البهجى، حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية ، دون طبعة ،دار الجامعة الجديدة للنشر، الإسكندرية ،2005، ص 321.

[3] خالد حسن أحمد، مرجع سابق، ص22.

ولعلّ هذا راجع لنسبية هذا الحق، فهو يختلف من مجتمع الى آخر نظرا لاختلاف العادات والتقاليد، بل هو يختلف في المجتمع الواحد من حقبة زمنية إلى حقبة زمنية أخرى، أو بالأحرى من شخص إلى شخص آخر، فهناك من يفضّل أن تكون حياته الخاصة سرا غامضا، وهناك من يجعلها كتابا مفتوحا للجميع.[1]

وفي هذا الصدد انقسم فقهاء القانون الى اتجاهين:

**أولا: الاتجاه الإيجابي**

إنّ العوامل والصعوبات التي تحول دون وضع تعريف عام متفق عليه للحق في الخصوصية، لم تكن عائقا على بعض الفقه الذي راح يجتهد في هذا الشأن لاستنباط بعض المعايير التي يمكن الاستناد إليها لتحديد مدلول هذا الحق من خلال نظريات مختلفة أهمها:

**1/ نظرية العزلة أو الخلوة The Seclusion Theory**

نشأت هذه النظرية في الفقه الأمريكي على يد المحامين "**وارين براندیس**"، و "**صمويل وارين**" من خلال مقالة تم نشرها بمجلة "هارفارد" عام 1890، وصرحا بأن الحياة الخاصة (Being Let Alone)هو حق الانسان أو حق الفرد أن يترك ليكون وحيدا أو هي حاجة الأفراد في بعض الأوقات إلى الانسحاب من العالم.[2]

وفي ذات المعنى يعرف الفقيه "**ألان ويستن**" الخصوصية بأنها الانسحاب الاختياري للفرد من المجتمع عموما جسمانيا ونفسيا سواء أراد أن يعيش في عزلة أو في مجموعة صغيرة متآلفة أو أن يعيش في حالة تستر أو تحفظ عندما يكون بين مجموعات كبيرة.[3]

[1] إبراهيم داود، الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية(دراسة تحليلية مقارنة)،مجلة الحقوق للبحوث القانونية والاقتصادية بكلية الحقوق_ جامعة الإسكندرية، المجلد الثاني، العدد الأول ،2017، ص 321.

[2] وليد السيد سليم، ضمانات الخصوصية في الأنترنت، د ط، دار الجامعة الجديدة، الإسكندرية،2012، ص 69_70.

[3] عصام أحمد البهجى، مرجع سابق ، ص 54.

ويعرفها القاضي الأمريكي "**كولي**" بأنها الحق في أن يترك المرء وشأنه، أو حق الفرد في أن يترك وحده، لا يعكر عليه أحد صفو خلوته.[1]

كما اعتنق هذا المفهوم طائفة من الفقه الفرنسي الذي يرى أن لكل انسان نطاق من الحياة يجب أن يكون شخصيا له ومقصورا عليه، بحيث لا يجوز للغير أن يدخل إليه بدون إذن. معتمدين في تعريفهم هذا على فكرة الخلوة، والتي تتجسد عندما يبتعد الفرد عن المجتمع لفترة من الزمن، أو قد يجد خلوته ببعض الناس اللذين يألفهم.[2]

**2/نظرية السرية The Secrecy Theory**

ترتبط فكرة السرية ارتباطا وثيقا بفكرة الحياة الخاصة. بل أن الفقه والقضاء المقارن قد اعترفا بالحق في سريتها قبل الكلام عن الحق في احترامها.[3]

فالحق في الخصوصية في نظر أنصار هذا الاتجاه يعني أنه ليس لأحد أن يقتحم على غيره عالم أسراره ، وأن يدعه في سكينته ، لينعم بالألفة دون تطفل من قبل الاخرين.[4]

و يعرفه الفقيه الفرنسي "**جان كاربونيي**" بأنه المجال السري الذي يملك الفرد بشأنه سلطة استبعاد أي تدخل من الغير وهو حقه في أن يترك وحيدا هادئا.[5]

وعرفه "**نيرسون**" بأنه حق الشخص في الاحتفاظ بأسرار من المتعذر على عامة الناس معرفتها إلا بإرادة صاحب الشأن وتتعلق بصفة أساسية بحقوق شخصيته .[6]

---

[1] ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة ، د ط ، دار النهضة العربية ، القاهرة،2011 ص 222.

[2] خالد حسن أحمد، مرجع سابق، ص17.

[3] ممدوح خليل بحر، مرجع سابق، ص 218.

[4] عماد حمدى حجازي، مرجع سابق، ص 49.

[5] مريم أل سيدي الغازي و مارية بوجداين ، من الحق في الحياة الخاصة الى الحق في الخصوصية الرقمية ، مجلة القانون الدستوري والعلوم الإدارية، العدد الثالث، المركز الديمقراطي العربي، برلين، ماي 2019، ص 60.

[6] مجادي نعيمة ، الحق في الخصوصية بين الحماية الجزائية والضوابط الإجرائية للتحقيق دراسة مقارنة ، أطروحة دكتوراه، تخصص قانون إجرائي، كلية الحقوق، جامعة سيدي بلعباس،2019/2018، ص41.

كما تبنى هذا الاتجاه بعض الفقه المصري على رأسهم الدكتور "**أحمد فتحي السرور**"

الذي يرى أن الحياة الخاصة هي قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وصلاته الخاصة وخصائصه المتميزة، ولا يمكنه أن يتمتع بها إلا في إطار مغلق يحفظها ويهيئ لها سبيل البقاء، فيكون له عندئذ الحق في إضفاء السرية على مظاهرها وآثارها.[1]

**3/ نظرية الحرية The Liberty Theory**

يزعم أصحاب هذا الاتجاه أن الحياة الخاصة تتسم بميزة الحرية، فهما دائرتان متسعتان تكمن نقطة الالتقاء بينهما في الخصوصية الإنسانية، فالحرية تبرز في حق الفرد في ممارسة حياته بدون قيد، أي أن يكون حرا في عيش الحياة التي يريدها دون تدخل الآخرين[2]

وهو ما أكده المؤتمر المنعقد في ستوكهولم عام 1967.

ومن مؤيدي هذا الاتجاه القاضي "**دوجلاس**" عضو المحكمة العليا في الولايات المتحدة الأمريكية الذي قرر أن الحق في الحياة الخاصة هو حق الفرد في أن يختار سلوكه الشخصي وتصرفاته في الحياة عندما يشارك في الحياة الاجتماعية مع الاخرين، كما يرى أن حق المرء في أن يترك وشأنه هو بداية كل الحريات.[3]

وقد تبنى الأستاذ "**جون شاتوك**" نفس الاتجاه، فهو يرى أن الحق في الخصوصية هو أن يعيش المرء كما يحلو له يستمتع بممارسة أنشطة خاصة معينة حتى ولو كان سلوكه مرئيا من الناس، أو ارتداء ما يجده مناسبا له أو اتخاذ هيئة تنفرد بها شخصيته.[4]

[1] خالد حسن أحمد، مرجع سابق، ص 17.

[2] مريم أل سيدي الغازي، مارية بوجداين، مرجع سابق، ص 63 .

[3] خالد حسن أحمد، مرجع سابق، ص14.

[4] ممدوح خليل بحر، مرجع سابق، ص 212.

كما عرفها البعض على أنها قيادة الإنسان في الكون المحيط به ،وذلك بقيادة جسمه فله الحرية في الإبصار والاستماع وحرية الحركة ...وقيادة ذاته النفسية من حرية في التفكير والشعور و التعبير.[1]

وبناء على ما سبق يمكن القول أنّه وبرغم المحاولات التي قام بها الفقه لإيجاد تعريف محدد للحق في الخصوصية إلا أنها تعرضت للانتقاد.

فرغم أهمية معيار العزلة أو الخلوة في تحديد مفهوم الخصوصية، إلا أنه يتعارض مع الطبيعة الاجتماعية للإنسان، كما له أن يتمتع بحقه في الخصوصية من دون الحاجة للانعزال عن المجتمع الذي يعيش فيه.[2]ونفس الشيء بالنسبة لمعيار السرية، فخصوصية الحياة تعني ألاّ تكون حياة الشخص غير العلنية عرضة لأن تلوكها الألسن ولو لم تكن الوقائع سرية، فيكفي ألاّ تكون معروفة على الملأ.[3]

أمّا عن معيار الحرية، فإن كان يتفق في بعض الجوانب مع الحق في الخصوصية إلا أنه لا يمكن التسليم بأنهما يحملان نفس المعنى، بل يبقى نطاق الحرية أكثر شمولا من الحق في الخصوصية.

وهنا يتبادر السؤال في أذهاننا؟ هل أفلح أنصار الاتجاه الثاني في تحديد مدلول هذا الحق؟

هذا ما سنحاول معرفته في النقطة التالية.

[1]وليد سليم النمر، مرجع سابق، ص 160_161.

[2]وليد سليم النمر، المرجع نفسه ،ص 159.

[3]عصام أحمد البهجى، مرجع سابق، ص 103.

**ثانيا: الاتجاه السلبي**

نظرا لصعوبة التوصل الى تعريف إيجابي للحق في الخصوصية ذهب جانب آخر من الفقه لإيجاد تعريف سلبي له، فالحياة الخاصة في نظرهم هي كل ما لا يعتبر من قبيل الحياة العامة للشخص، والتي تعد أكثر تحديدا وأضيق نطاقا فيكون من السهل تعريفها.[1]

وهي ما عرفت بنظرية التعريف بالضد لدى فقهاء القانون المقارن.

وعليه تعّرف الحياة العامة على أنها حياة الفرد في جانبها الاجتماعي التي تقتضي اشتراك المرء مع الآخرين، فتشمل أنشطة الفرد التي تتضمن مساهمته في المجتمع ومثال ذلك نشاطه المهني وأنشطته التي يمارسها علانية.[2]

ووفقا لتعريف الأستاذ "**ألبرت كولومبيني**" الحياة العامة هي كل ما يمكن ربطه بنشاط عام أو بمسألة عامة، وبعبارة أخرى كل فعل له انعكاسات سياسية أو اقتصادية أو اجتماعية والذي يمس وفقا لرأي بعضهم المصالح المادية والمعنوية للجماعة ويثير انعكاسا جماعيا بالموافقة أو الرفض .[3]

وتأسيسا على ما سبق يقوم أصحاب هذا الاتجاه بتعريف الحق في الحياة الخاصة انطلاقا من تعريف الحياة العامة لاستبعاد نطاقها من مضمون الحياة الخاصة، وهذا ما أضفى صعوبة جديدة على تعريف الحق في الحياة الخاصة تستدعي ضرورة البحث عن معيار يفصل بينها وبين الحياة العامة.[4]

---

[1] وليد سليم النمر، مرجع سابق، 167.

[2] أشرف توفيق شمس الدين ، الصحافة والحماية الجنائية للحياة الخاصة "دراسة مقارنة" ، الطبعة الأولى ، دار النهضة العربية، مصر،2007، ص 25_26.

[3] ممدوح خليل بحر، مرجع سابق، ص 197.

[4] وليد السيد سليم، مرجع سابق، ص 77.

يجد البعض أنه لا بدّ من الاستعانة بعدة معايير للتفرقة بين الحياة العامة والحياة الخاصة منها فكرة المصلحة العامة ومدى ارتباط العمل أو الفعل بالطابع العام لهذا النشاط، حيث أنه كلما كان النشاط عاما فإنه لا يتعلق بحياة الفرد الخاصة ويجوز للأخرين الاطلاع عليه.[1]

ويذهب آخرون إلى اعتماد معيار المكان للتفرقة بين الأمرين، فعندما تدور أحداث الحياة خلف الجدران نكون بصدد الحياة غير العلنية (الخاصة). أما عندما تدور أحداث الحياة أمام الجمهور وعلى مرأى ومسمع منه نكون بصدد الحياة العامة.[2]

في حين يرى البعض الآخر أن معيار التفرقة يكمن في شعور الإنسان بالحياء تجاه ألفة حياته وعندما يبدأ هذا الشعور بالظهور يبدأ نطاق الحياة الخاصة وتنتهي الحياة العامة.[3]

وعلى ضوء ما سبق ذكره، نخلص إلى أن كل المحاولات الفقهية التي جاءت بصدد تعريف الحق في الخصوصية لم تسلم من الانتقاد، سواء الاتجاه الإيجابي الذي بنى تعريفه على معايير محددة اتسمت بضيقها من ناحية ومن ناحية أخرى باتساعها وشموليتها.

أو الاتجاه السلبي الذي عرّف الحياة الخاصة انطلاقا من تعريفه للحياة العامة ظانّا منه أن هذه الطريقة مجدية، لكن في النهاية قد وقع في غموض كبير حول معرفة أين تنتهي الحياة العامة ومتى تبدأ الحياة الخاصة.

فنقول بأن هذه التعريفات قد باءت بالفشل لعدم تمكنها من إيجاد تعريف جامع مانع للحق في الخصوصية.

[1] إبراهيم داود، مرجع سابق، ص 332.

[2] عصام أحمد البهجى، مرجع سابق، ص40.

[3] إبراهيم داود، مرجع سابق، ص 332.

## المطلب الثاني: المفهوم الحديث للحق في الخصوصية

تغيّر مفهوم الحق في الخصوصية بفعل التغيرات الاجتماعية والتقدّم التكنلوجي، حيث أدّى ظهور الأنترنت إلى مشاركة الأفراد معلوماتهم الشخصية عبر الوسائل الرقمية، ممّا استوجب حمايتها من الوصول غير المصرح به أو إساءة استخدامها.

وتصاعدت المخاوف بشأن خصوصية الأفراد إثر بروز أنظمة الذكاء الاصطناعي التي تعتمد على جمع ومعالجة كميات هائلة من البيانات الشخصية على اختلاف أنواعها، وبذلك أصبحت محورًا رئيسيًا للأنظمة الذكية تُستخدم في تحليل السلوكيات واتخاذ قرارات مؤتمتة(آلية) قد تؤثر على الأفراد بطرق غير متوقعة.

وفي ظلّ هذه التحولات بات من الضروري إعادة النظر في مفهوم الحق في الخصوصية ليتماشى مع المستجدات التكنولوجية.

وبناءً على ذلك، من المهم التطرق إلى مفهوم الخصوصية الرقمية، ثم التعرف على البيانات الشخصية باعتبارها محلاً للخصوصية في سياق الذكاء الاصطناعي.

### الفرع الأول: تعريف الحق في الخصوصية الرقمية

وسميت بالخصوصية الرقمية نسبة إلى ظهورها في الفضاء الرقمي، الذي هو بمثابة نطاق تشغيلي محكم باستخدام الالكترونيات لاكتشاف المعلومات عبر أنظمة مترابطة ببعضها البعض وببنية تحتية لها[1].

كما تعدّدت تسمياتها، حيث يُطلق عليها البعض "الخصوصية الإلكترونية"، بينما يُفضل آخرون تسميتها بـ "الخصوصية المعلوماتية" أو "خصوصية المعلومات"، وكلها تعكس المفهوم ذاته المتعلق بحماية البيانات الشخصية وطرق استخدامها في البيئة الرقمية.

[1] ذيب محمد ،فارس فزاع ، الفضاء الالكتروني _مفاهيم ودلالات_ رؤية سوسيولوجية تحليلية ، مجلة التميز الفكري للعلوم الاجتماعية والإنسانية، جامعة الشاذلي بن جديد_ الطارف_، العدد الخامس، جانفي 2021، ص 150.

ويعود الفضل في صياغة مفهوم الحق في الخصوصية الرقمية كتعبير مستقل عن الخصوصية بالمفهوم العام إلى مؤلفين أمريكيين هما "**آلا ن ويستن**" في كتابه الخصوصية والحرية عام 1967 الذي عرفه على أنه حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين. و"**آرثر ميلر**" في كتابه الاعتداء على الخصوصية عام 1971 وعرفه بأنه قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم.[1]

وفي ذات الاتجاه صرّح الفقيه "**تشارلز فريد**" أن الخصوصية ليست ببساطة عدم وجود معلومات خاصة بنا لدى الآخرين أو في ذهنهم، بل هي بالأحرى التحكم في المعلومات المتعلقة بنا والتي بحوزتنا[2]. أي أنها تحكم الأفراد في مدى وتوقيت وظروف مشاركة حياتهم مع الآخرين، وتدخل الخصوصية كحق يمارسه الأفراد للحدّ من إطلاع الآخرين على مظاهر حياتهم والتي يمكن أن تكون أفكار أو بيانات شخصية .[3]

وعلى ضوء ما سبق يتضح جليا أن مفهوم الخصوصية الرقمية هو امتداد للحق في الخصوصية عموما، إلاّ أنه يختلف عن الأخير بكونه يتعلق أساسا بمعلومات الفرد الشخصية ومدى سيطرته على تدفقها عبر تكنولوجيات الإعلام والاتصال في زمن قد أضحى فيه كل شيء متاح عبر الأنظمة المعلوماتية والذكاء الاصطناعي خاصة، الذي يتغذى عن طريق جمع البيانات والتي يصعب تعقبها أو استرجاعها أو جعلها قابلة للنسيان.[4]

[1] يونس عرب، مرجع سابق، ص7.

[2] وليد سليم النمر، مرجع سابق، ص 208.

[3] معزوز دليلة ، حماية المعطيات الشخصية في البيئة الافتراضية ،مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 10، العدد الأول ،2021،ص128.

[4] مفيدة مباركية ، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، المجلد 7، العدد الأول ،2018، ص 461.

**الفرع الثاني: محل الخصوصية الرقمية**

كما ذكرنا سابقًا، فإن موضوع الحق في الخصوصية الرقمية ينصب حول البيانات الشخصية باعتبارها جوهر هذا الحق وأساس حمايته، فهي تمثل هوية الفرد في البيئة الرقمية.

**أولا: تعريف البيانات الشخصية**

البيانات بالمعنى العام هي مجموعة من الحقائق أو المفاهيم أو التعليمات والتي تتخذ شكلا محددا يجعلها قابلة للتبادل وللتفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية.[1]

لكن ما يهمنا في دراستنا هذه هو البيانات الشخصية، فما المقصود بها؟

**أ/ التعريف الفقهي:**

تعدّدت تعريفات فقهاء القانون للبيانات الشخصية للأفراد، حيث يرى جانب منهم أنها تلك البيانات التي يهدف كل شخص إحاطتها بسياج من السريّة، فهي تشمل كل ما يتعلّق بشخصه وصحته وثروته وحياته العائلية. فيما يرى البعض الآخر بأنها البيانات التي تتعلّق بشخص معيّن ولا يشترط فيها أن تكون متعلّقة بالحياة الخاصّة به وإنّما يكفي أن تتعلّق بالحياة المهنية، أو بحياته العامّة أو انتماءاته السياسية أو النقابية.[2]

وهناك من يعرّفها بأنها المعلومات المرتبطة بذات الشخص وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان، ورقم الهاتف، وحالة الدخل، والوضع الصحي، والعرق والجنس والعمر والاتجاهات الأخلاقية والسياسية. وعلى العموم هي كل المعلومات التي تكون ملازمة للشخص الطبيعي وتتصل به، فتجعله معروفا أو قابلا للتعريف.[3]

---

[1] محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية –دراسة مقارنة– ،ط1،دار الفكر والقانون للنشر والتوزيع، مصر ،2015، ص37.

[2] جمال مراي، حق الأفراد في حماية بياناتهم الشخصية وفقاً لقانون حماية البيانات الشخصية، مقال منشور في موسوعة حماة الحق للمحاماة، 19-12-2023، متاح على الموقع:https://jordan-lawyer.com ، تاريخ الاطلاع: 08-05-2025، على الساعة 22:00.

[3] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية "دراسة مقارنة"،ط1، مركز الدراسات العربية للنشر والتوزيع، البلد، 2017، ص 29.

**ب/ التعريف القانوني:**

حرصت معظم تشريعات الدول على وضع تعريف دقيق لمصطلح البيانات الشخصية بالرغم من اختلاف التسميات لها.

فالنسبة للمشرع الجزائري أطلق عليها تسمية "المعطيات ذات الطابع الشخصي" ويعرفها بموجب المادة 1/3من القانون رقم 18_07 [1] بأنها:

" كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرّف أو قابل للتعرّف عليه والمشار إليه أدناه، "الشخص المعني[2]" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدّة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيو مترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

في حين عرفها القانون الفرنسي رقم 7 لسنة 1978 المعدل بالقانون رقم801 لسنة 2004 الخاص بحماية البيانات الشخصية في المادة 02 بنصها على أنه: "يعتبر بيانا شخصيا أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة، سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه".[3]

وبخصوص المشرع المصري فقد عرف البيانات الشخصية بموجب المادة 01 من الفصل الأول من القانون الخاص بحماية البيانات الشخصية رقم 151 لسنة 2020 بأنها:" أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم أو الصوت أو الصورة، أو رقم تعريفي أو محدد

[1] القانون رقم 18_07 ،المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018، ج ر، عدد 34، الصادرة في 10 يونيو 2018.

[2] كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة، القانون 18-07، المرجع نفسه.

[3] Loi Françaises N° 801-2004 , du 06 aout 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, , et modifiant la loi no 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,J.O7 aout 2004.

للهوية عبر الأنترنت أو أي بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية"[1].

أمّا على المستوى الإقليمي، تعرّفها المادة 1/2 من التوجه الأوربي رقم 46/95 الصادر بتاريخ 24 أكتوبر 1995 بأنها:" كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، يعد قابل للتعرف عليه (الشخص المعني)، الشخص الذي يمكن معرفته بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو إلى عنصر أو عدة عناصر مميزة لهويته الطبيعية الفيزيولوجية، النفسية، الاقتصادية، الثقافية أو الاجتماعية"[2].

كما تعرفها الاتفاقية الأوربية رقم (108) الصادرة عن مجلس أوروبا على أنها: "كل معلومة تتعلق بشخص طبيعي معرف أو قابل للتعريف (الشخص المعني)[3]

هذا وتضمنت اللائحة الأوربية لحماية البيانات GDPR رقم (679) لسنة 2016 في المادة الرابعة منها تعريفا للبيانات الشخصية بأنها:" أي معلومات لها صلة بشخص تم التعرف على هويته بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى معرف شخصي مثل الاسم ورقم الضمان الاجتماعي وبيانات الموقع والمعرّف عبر الأنترنت (عنوان IP أو عنوان البريد الإلكتروني) أو لواحد أو أكثر من العوامل الخاصة بالهوية البدنية أو الفيسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص"[4]

---

[1] هبة رمضان رجب ، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية ،مجلة التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي، بدون ذكر المجلد والعدد وتاريخ النشر، ص 433.

[2] بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية ،المجلة العربية للعلوم و نشر الأبحاث، مجلد2، عدد5، يونيو2016، ص40 .

[3] اتفاقية حماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، مجموعة المعاهدات الأوروبية رقم 108 مجلس أوروبا، المادة02، الصادرة في28 يناير 1981، ستراسبورغ، نسخة مترجمة، متاحة على:https://rm.coe.int ، تاريخ الاطلاع: 13_04_2025، على الساعة 20:55.

[4] أميرة بدوى نجم، أخلاقيات الذكاء الاصطناعي في ضوء توصيات الأمم المتحدة (اليونسكو) ، ط1،دار الفكر الجامعي، الإسكندرية، 2024، ص 72_73.

يتضح من التعريفات السابقة أنّ أغلب التشريعات اعتمدت نهجًا موحدًا يتوافق مع المعايير الدولية المستقرّة في هذا المجال، وعلى رأسها ما جاءت به اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، حيث قدمت مفهومًا واسعا يشمل جميع العناصر التي تحدد هوية الشخص أو تمكّن من تحديده والتعرف عليه، من خلال ربطها بمعلومات أخرى مثل رقم التعريف، البيانات البيو مترية، أو المعرّفات الرقمية كعنوانIP .

كما تميزت هذه التعريفات بالمرونة، مما يسمح بتطويرها مستقبلاً لمواكبة المستجدات المتعلقة بطرق جمع البيانات ومعالجتها.

**ثانيا: أنواع البيانات الشخصية**

تتعدد أنواع البيانات الشخصية وتختلف باختلاف الزاوية التي ننظر منها، مما يستدعي منا ضرورة تصنيفها بدقة لتسهيل فهمها وحمايتها.

**1/ تصنيف البيانات الشخصية من حيث طبيعتها:**

تفرّق أغلب تشريعات الدول بين نوعين من البيانات الشخصية، البيانات الشخصية العادية والبيانات الشخصية الحساسة، حيث تفرض حماية مشددة على الفئة الأخيرة نظرًا لحساسيتها

"فالبيانات الشخصية العادية" هي تلك البيانات المتعلقة بالفرد، بحيث لا يوجد مانع من اطلاع الغير عليها، ومعرفتها لا يشكل انتهاكا لخصوصيته مثل الاسم ورقم الهاتف وتاريخ الميلاد.[1]وهي ما أشار إليها المشرع الجزائري باسم المعطيات ذات الطابع الشخصي في نص المادة 3 من القانون 07/18 المذكورة أعلاه.

أما عن "البيانات الشخصية الحساسة" فقد عرفها المشرع الجزائري في المادة 6/3 وأطلق عليها تسمية "المعطيات الحساسة"، وهي معطيات ذات طابع شخصي تبين الأصل العرقي أو

[1] هبة رمضان رجب، المرجع سابق، ص 424.

الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية .[1]

بينما يعتبر المشرع المصري البيانات الشخصية الحساسة بأنها تلك البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة.[2]

وتناولتها اللائحة العامة لحماية البيانات (GDPR) تحت عنوان "الفئات الخاصة من البيانات الشخصية"، وهي تشمل كل ما يكشف عن الأصل العرقي أو الاثني، الآراء السياسية، المعتقدات الدينية أو الفلسفية، العضوية النقابية، البيانات الجينية، البيانات البيومترية بهدف تحديد هوية الشخص، البيانات الصحية، وبيانات الحياة الجنسية أو التوجه الجنسي للفرد.[3]

فاللائحة تحظر معالجة هذا النوع من البيانات، لما ينطوي عليه من مخاطر جسيمة على خصوصية الأفراد، واحتمالية المساس بكرامتهم أو تعرضهم للتمييز أو الضرر.

**2/ تصنيف البيانات الشخصية من حيث إتاحتها:**

في هذا التصنيف يمكن التفرقة بين نوعين من البيانات:

"البيانات الشخصية المتاحة" وهي تلك البيانات المنشورة على المواقع الالكترونية المفتوحة للجمهور بحيث يمكن لأيّ كان الدخول إليها والاطلاع عليها وقتما شاء، كما هو الحال بالنسبة للمعلومات التي تنشر من قبل الوزارات والمؤسسات الحكومية في حدود القانون[4] لا سيما في ظلّ رقمنة الإدارة بمختلف قطاعاتها واستعمالها للتطبيقات الذكية لتسهيل وتسريع نشاطها.

---

[1] القانون رقم 18_07، المرجع السابق.

[2] أميرة بدوى نجم، المرجع السابق، ص 74.

[3] الاتحاد الأوربي ،اللائحة العامة لحماية البيانات، المادة 9، الصادرة بموجب اللائحة 2016/679، الجريدة الرسمية للاتحاد الأوربي، 2016.

[4] محمد كمال محمود الدسوقي، مرجع سابق، ص52.

تشمل أيضا البيانات التي يقوم الشخص المعني بنشرها أو إتاحتها للعامة طواعية، عبر الإنترنت مثل حسابات وسائل التواصل الاجتماعي، المنتديات العامة، السير الذاتية المنشورة على مواقع العمل، إلخ أو من خلال وسائل إعلام أو منصات مفتوحة.[1]

و"البيانات غير المتاحة" هي التي يقتصر العلم بها على شخص مالكها أو من يملك سلطة قانونية عليها، بحيث لا يكون للكافة الوصول إليها والاطلاع عليها وحفظها واستخدامها أو استغلالها دون شرط أو قيد، نتيجة للتدابير التي اتخذها مالك المعلومة للمحافظة على سريتها.[2]

وفي كلتا الحالتين أصبحت تقنيات الذكاء الاصطناعي قادرة على جمع وتحليل كميات هائلة من البيانات الشخصية المتاحة وغير المتاحة باستخدام أدواتها المتطورة.

**3/ تصنيف البيانات الشخصية من حيث شكلها:**

تتعدد أشكال البيانات الشخصية بحسب الطريقة أو السياق الذي تُجمع فيه، إذ لا تنحصر في نوع واحد أو مصدر محدد، بل تتنوع بتنوع أنشطة الفرد الرقمية واحتياجاته لمختلف الأجهزة والتقنيات الحديثة. ومن أبرز هذه الأشكال:

**أ/ البيانات الناتجة عن التصفح:**

تشمل هذه الفئة من البيانات كل المعلومات التي يتم استخلاصها من نشاط المستخدم أثناء تصفحه للإنترنت، وتُعرف عادةً بـ "بيانات النقر (Clickstream Data) "وهي البيانات التي يمكن للمواقع الإلكترونية جمعها تلقائيًا بمجرد ولوج المستخدم إليها، دون الحاجة لتفاعل مباشر كإدخال البيانات يدويًا. من بين أبرز هذه البيانات: عنوان بروتوكول الإنترنت(IP Adress)

أو بروتوكول التحكم في الإرسال(TCP) ، ونوع الجهاز المستخدم (حاسوب، هاتف ذكي...)، ونظام التشغيل، ونوع وإصدار المتصفح، بالإضافة إلى توقيت الدخول إلى الموقع، والمدة

[1] وليد سليم النمر، مرجع سابق، 109.

[2] محمد كمال محمود الدسوقي، المرجع نفسه، ص 53.

الزمنية التي قضاها المستخدم في التصفح، والمسارات التي اتبعها داخل الموقع، والروابط التي قام بالنقر عليها[1].

**ب/ البيانات الناتجة عن الاتصالات:**

تعد البيانات الناتجة عن الاتصالات من أهم أشكال البيانات الشخصية التي تُنتج بشكل غير مباشر أثناء استخدام وسائل الاتصال المختلفة، مثل الهواتف المحمولة، البريد الإلكتروني، وخاصة مواقع التواصل الاجتماعي التي أصبحت تحتوي على معلومات كل منّا وتوجهاته السياسية وتنقلاته اليومية.[2]

وفي هذا الشأن عرّف المشرع الجزائري بموجب المادة 11/3 "الاتصال الإلكتروني" على أنه: كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية.[3]

ونظراً لتطور وسائل الاتصال خاصة مع انتشار الهواتف الذكيّة، اتسع نطاق إنتاج البيانات الشخصية الناتجة عن الاتصالات. حيث أصبحت هذه الأجهزة مزوّدة بمستشعرات وإمكانيات متنوعة، مثل نظام تحديد المواقع (GPS) لتتبع الموقع، والكاميرات، والميكروفونات، ومقاييس التسارع، ممّا يؤدي إلى توليد بيانات بشكل مستمر، كما تقوم هذه الأجهزة بإرسال بيانات الموقع عبر تقنيات الـ(GPS)، وشبكات(WIFI) ، وأبراج الاتصالات.[4]

**ج/البيانات المتعلقة بالحالة الصحية:**

ويطلق عليها المشرّع الجزائري تسمية "معطيات في مجال الصحة" وهي كل معلومة تتعلق بالحالة البدنية و/أو العقلية للشخص المعني، بما في ذلك معطياته الجينية. ويقصد بهذه

[1] وليد سليم النمر، مرجع سابق، ص110.

[2] مريم أل سيدي الغازي، مارية بوجداين، مرجع سابق، ص67.

[3] القانون رقم 18_07، المرجع السابق، ص12

[4] MD Absarul Hasan, Compromising Privacy: The Role of AI in Smartphone Surveillance, International Journal for Multidisciplinary Research, vol. 7, no. 1, Janvier-fevrier 2025, p 01.

الأخيرة، كل معطيات متعلقة بالصفات الوراثية لشخص أو عدة أشخاص ذوي قرابة. حسب ما جاء في القانون 07/18 في المادة 3 فقرة 9 و8 على التوالي.[1]

وانطلاقا من التعريف نستنتج بأن البيانات الصحية هي كل المعلومات المرتبطة بالحالة الصحية للفرد، سواء الجسمية أو النفسية، كما تتعلّق أيضاً بالتشخيصات الطبية، والعلاجات، والتاريخ الطبي،،،، كما تمتد لتشمل البيانات الوراثية (الجينية)، أي تلك المرتبطة بالصفات الوراثية التي يحملها الشخص أو يشترك فيها مع أقاربه. وعادة ما تُجمع هذه البيانات ضمن ملفات طبية في المؤسسات الصحية، كما يمكن تخزينها رقميًا.

وتُعد هذه البيانات من أكثر أنواع البيانات الشخصية حساسية لدى الشخص المعني فيحرص على عدم إفشائها للآخرين لكيلا يقع في الإحراج أمامهم لاسيما إذا تعلق ببعض الحالات المرضية المستعصية كما هو الحال بالنسبة لمرض فقدان المناعة المكتسبة (VIH).[2]

والجدير بالذكر أن الذكاء الاصطناعي قد أحدث تحولًا جذريًا في مجال الرعاية الصحية وفي كيفية تقديم الخدمات الطبية، إذ أصبح قادر على تحليل البيانات الجينية والمعلومات الصحية بدقة عالية، مما يتيح تطوير خطط علاج شخصية تتناسب مع التركيبة الجينية لكل فرد، كما ساهم في تحسين إدارة البيانات الطبية وتحليلها، و رفع كفاءة التشخيص و تسريع اتخاذ القرارات العلاجية، و تخفيف العبء على الكوادر الطبية و التحسين من نتائج العلاج.[3] لكنه في الوقت ذاته يثير مخاوف جديّة بشأن حماية خصوصية المرضى وسلامة بياناتهم الحساسة.

**د/ البيانات المتعلقة بالحالة المالية:**

[1] القانون رقم 18_07، المرجع السابق.

[2] بن قارة مصطفى عائشة، مرجع سابق، ص41.

[3] نور الدين الشابي، "الذكاء الاصطناعي بين العدالة والنجاعة"، ضمن: عصام عيروط (مشرف)، مستقبل الذكاء الاصطناعي: تحديات قانونية وأخلاقية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية برلين "ألمانيا"، 2024، ص160.

أصبحت معظم المعاملات بين الأفراد تقام إلكترونيا، ومن بينها المعاملات التجارية من بيع وشراء البضائع والخدمات من خلال المواقع الإلكترونية، حيث تعرض السلع وتتم أعمال التداول في الفضاء الرقمي. وعلى إثر ذلك يتم تبادل العديد من البيانات المالية الحساسة فيما بين المتعاملين.[1] تتعلق هذه المعلومات بالوضع المالي للفرد، بما في ذلك دخله الشهري، والاتفاقات أو الصفقات المالية التي أبرمها، وحجم الديون المترتبة عليه. وتبرز بطاقات الدفع الإلكتروني كواحدة من أهم مصادر هذه البيانات، نظرًا لاعتمادها المباشر على الرصيد المالي للفرد والتزاماته.[2]

**هـ/ البيانات البيومترية:**

جاء تعريف "البيانات البيومترية" في اللائحة العامة لحماية البيانات الأوروبية(GDPR) بأنها البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تؤكد تحديد هوية ذلك الشخص الطبيعي بشكل فريد، مثل الصور الوجهية أو بيانات بصمات الأصابع[3].

فالتعرف على الأشخاص عبر البيانات البيو مترية يعني التعرّف الآلي على الأفراد استنادًا إلى سماتهم البيولوجية والسلوكية. وبالتالي فإنّ البيانات البيو مترية تعدّ بمثابة توقيعات بشرية فريدة يمكن قياسها، وقد تشمل بصمات الأصابع ومسح قزحية العين أو طريقة الفرد في فعل شيء ما (مثل الطريقة التي يسير أو يكتب بها). وهي إحدى أكثر الوسائل الموثوقة لإثبات الهوية المتاحة في حوزتنا، فمن الصعب للغاية تزييفها.[4]

---

[1] بوبكري تيسير، الحماية الجنائية للخصوصية الرقمية في التشريع الجزائري_ دراسة مقارنة_، مذكرة لنيل شهادة الماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2022/2021، ص27.

[2] يحي الشريف نصير، مزغيش عبير، الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 02، 2022، ص197-198.

[3] Voir : Règlement général sur la protection des données (RGPD), Règlement (UE) 2016/679, article 4, point 14, consulté sur : https://gdpr-info.eu, le29-04-2025 à 01:30.

[4] اللجنة الدولية للصليب الأحمر، « البيومترية »، الاجتماعات النظامية، متاح على الرابط التالي:
https://rcrcconference.org، تاريخ الاطلاع: 29-04-2025 على الساعة: 01:30.

مع انتشار أنظمة المراقبة بشكل أكبر، أصبح استخدام بيانات القياسات الحيوية—مثل بصمات الأصابع، التعرف على الوجوه، وفحوصات قزحية العين—يثير قضايا خصوصية خطيرة. على عكس كلمات المرور، فإن بيانات القياسات الحيوية دائمة، وإذا تم اختراقها، لا يمكن تغييرها. وهذا ما يجعلها هدفًا رئيسيًا لسرقة الهوية وأشكال أخرى من سوء الاستخدام. فدمج بيانات القياسات الحيوية في تطبيقات الذكاء الاصطناعي يطرح العديد من المعضلات الأخلاقية. على سبيل المثال، بينما يمكن لتقنية التعرف على الوجوه تعزيز تدابير الأمان، إلا أنها غالبًا ما تعمل بدون موافقة صريحة من الأفراد، مما يؤدي إلى مراقبة غير مبررة.[1]

## المبحث الثاني: الذكاء الاصطناعي وانعكاساته على الحق في الخصوصية

شهدت السنوات الأخيرة طفرة هائلة في مجال التكنولوجيا، كان من أبرز مظاهرها تطور تقنيات الذكاء الاصطناعي، التي أصبحت اليوم تؤثّر بشكل مباشر في مختلف جوانب الحياة العِلمية والعَملية، فقد أصبحت تُسهم بشكل فعّال في تقديم العديد من الخدمات في معظم الميادين كالطب والتعليم، الصناعة، التجارة، الزراعة، النقل وغيرها.

إلّا أن هذا التقدّم لم يَخلُ من التحديات، خاصّة فيما يتعلق باحترام الحقوق الأساسية للأفراد وعلى رأسها الحق في الخصوصية. فقد أثار توسّع استخدام الذكاء الاصطناعي العديد من الإشكاليات القانونية والأخلاقية، لا سيّما فيما يتعلّق بجمع البيانات الشخصية ومعالجتها واستعمالاتها ومدى مشروعيتها.

وبناءً على ما سبق، سنسعى من خلال هذا المبحث إلى التعرّف على ماهية الذكاء الاصطناعي لتكوين صورة شاملة عن الإطار المفاهيمي لهذه التقنية الحديثة.

[1] The growing data privacy concerns with AI: What you need to know, dataguard , https://www.dataguard.com Publié le 4 septembre 2024 à 09:02, mis à jour le 10 janvier 2025,Consulté le 24-04-2025 à 18 :00.

ثم سنعالج في نقطة ثانية انعكاسات هذه التقنية على الحق في الخصوصية، من خلال الوقوف على أبرز صور الانتهاكات التي قد تمس هذا الحق، وتداعياتها الخطيرة على حياة الأفراد.

## المطلب الأول: ماهية الذكاء الاصطناعي

للتعرّف على ماهية الذكاء الاصطناعي لابدّ من التطرق أولا إلى مفهومه، ودراسة نشأته وتطوّره، وصولا إلى آلية عمله. وذلك بهدف الإحاطة بجوانبه النظرية قبل الخوض في انعكاساته القانونية.

### الفرع الأول: مفهوم الذكاء الاصطناعي

سنتناول في هذا الفرع مفهوم الذكاء الاصطناعي من مختلف الجوانب، بدءًا بالتعريف اللغوي ثم الفقهي، وأخيرا سنحاول عرض الجهود التشريعية التي تمكّنت من صياغة تعريف قانوني لهذه التقنية الجديدة.

#### أولا: تعريف الذكاء الاصطناعي

**أ/ لغة:** يتكون مفهوم الذكاء الاصطناعي من كلمتين. الأولى: الذكاء(Intelligence) والتي تعني القدرة على الفهم أو التفكير[1]، والثانية: الاصطناعي (Artificial)، مصدرها الفعل صَنَعَ، صَنَعَهُ يَصْنَعُهُ صُنْعًا، فهو مَصْنُوع وصُنْع: بمعنى عَمِلَه. والاصطناع هو افتعال من الصَنيعَة، واسْتَصْنَعَ الشيء أي دَعَا إلى صُنْعه. والاصْطنَاعي هو كل ما يدلّ على شيء مَصنُوع أي غير طَبيعي.[2]

[1] أميرة بدوي نجم، مرجع سابق، ص 23.

[2] عمار مراد غركان، التعاون الدولي للتصدي لخطر الإرهاب باستخدام الذكاء الاصطناعي، ضمن: عصام عيروط (مشرف)، مرجع سابق، ص 22_23.

**ب/التعريف الفقهي:**

أمّا عن التعريفات الفقهية للذكاء الاصطناعي فهي متعددة، وقد اختلفت وتباينت تفسيرات العلماء والباحثين له باختلاف منظور كل منهم وتخصّصه، ويرجع هذا التباين إلى الطبيعة المركبة لهذا المفهوم، وارتباطه الوثيق بالتطور التكنولوجي المتسارع. وفيما يلي أهم التعريفات التي وردت في هذا الشأن:

يرى "**اليان ريتش**" أن الذكاء الاصطناعي هو ذلك العلم الذي يبحث في كيفية جعل الحاسب يؤدي الأعمال التي يؤديها البشر بطريقة أفضل منهم.[1]

وهناك من يعرّفه على أنّه طريقة لصنع حاسوب أو روبوت يتم التحكم فيه بواسطة الكمبيوتر أو برنامج يفكر بذكاء، بنفس الطريقة التي يفكر بها البشر الأذكياء، فهو علم صنع الآلات التي تقوم بأشياء تتطلب ذكاء إذا قام بها الإنسان. [2]

أو هو العلم الذي يهتم بصناعة آلات تقوم بتصرّفات يعتبرها الانسان بأنّها ذكية، فهو يهدف أساساً إلى جعل الحاسوب وغيره من الآلات تكتسب صفة الذكاء، مما يجعلها قادرة على القيام بأشياء مازالت إلى عهد قريب حصرًا على الإنسان كالتفكير والتعلّم والإبداع والتخاطب.[3]

[1] المهندس عبد الحميد بسيونى، مقدمة الذكاء الاصطناعي للكمبيوتر ومقدمة برولوج، ط1، دار النشر للجامعات المصرية، مصر، 1994، ص18.

[2] عبد الله موسى، أحمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1، المجموعة العربية للتدريب والنشر، القاهرة، 2019، ص20.

[3] عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، د ط، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 2005، ص7.

وهناك من يعتبره جيل حديث من أجيال الحاسب الآلي، تتميز فيه البرامج الحاسوبية بخاصيات معينة، تجعلها قادرة على محاكاة القدرات الذهنية البشرية وأنماط عملها مثل القدرة على التعلم والاستنتاج وردّ الفعل على أوضاع لم تبرمج في الآلة. [1]

وعليه فالذكاء الاصطناعي هو مجموع أنظمة ذكيّة، تستطيع حلّ المشكلات الصعبة والمعقّدة تضاهي بها الانسان في كيفية حلّها، وهنا تكتسب الآلة خاصية الذكاء الذي يظهر في شكل نظام ذكي، يحاكي تمامًا مهارات الانسان وقدراته الفريدة.[2]

وحتى تكون كذلك؛ لا بدّ أن تكون هذه الأنظمة قادرة على التعلّم وجمع البيانات وتحليلها واتخاذ قرارات بناءً على عملية التحليل بصورة تحاكي طريقة تفكير البشر وهو ما يعني ضرورة توافر ثلاث صفات رئيسية هي:

1/ القدرة على التعلم: أي اكتساب المعلومات ووضع قواعد لاستخدامها.

2/ إمكانية جمع وتحليل هذه البيانات والمعلومات، وخلق علاقات فيما بينها، وهذا ما يساعد على الانتشار المتزايد للبيانات الضخمة (Big Data).

3/ اتخاذ قرارات، وذلك بناءً على عملية تحليل المعلومات، وليس فقط خوارزمية تحقق هدفا معينا.[3]

وخلاصة ما سبق، يمكن تعريف الذكاء الاصطناعي بأنه فرع من علوم الحاسوب يُعنى بتطوير أنظمة وبرمجيات ذكية قادرة على محاكاة التفكير البشري، من خلال التعلم، والتحليل، واتخاذ القرارات بطريقة تشبه العقل البشري.

---

[1] بوجمعة بتشيم، الذكاء الاصطناعي في منظومة العدالة الحديثة _على ضوء أحدث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022_، ط1، ألفا للوثائق للنشر والتوزيع، عمان (الأردن)،2023، ص38.

[2] مريم ساغي، مليكة مذكور، الذكاء الاصطناعي ومشكلة الخصوصية، مجلة روافد للدراسات والأبحاث العلمية في العلوم الاجتماعية والإنسانية، المجلد 08، العدد 02، ديسمبر 2024، ص523.

[3] حمده خلفان بالجافله، التكييف الفقهي لتطبيقات الذكاء الاصطناعي في المجال الاقتصادي والجنائي، ط1،دائرة الشؤون الإسلامية والعمل الخيري، دبي (الامارات العربية المتحدة)، 2024، ص 35.

**ج/ التعريف القانوني:**

مع تصاعد دور الذكاء الاصطناعي في مختلف مناحي الحياة، برزت الحاجة إلى وضع إطار قانوني واضح لهذه التقنية، يضبط نطاق استخدامها ويُسهم في رسم الحدود القانونية لها بما يتماشى مع القيم الدستورية والحقوق الأساسية.

ونظرا لكون الذكاء الاصطناعي مجالا متطورا ومعقدا، فإنّ تحديد تعريف قانوني دقيق له يستجيب لماهيته المتغيرة، يعتبر تحدياً جادّاً للقانونيين سيما وأنّ تعريفه التقني يتطور باستمرار.[1]

ومن أجل مواكبة هذا التطوّر، أصبحت الحاجة مُلحّة لأن يتدخل كل مشرّع على الأقل لتحديد مكونات هذا المفهوم، على غرار ما قام به كل من المشرّع الأمريكي والمشرّع الأوروبي. ففي الولايات المتحدة، تم الاقتراب من المسألة من منظور عملي، وذلك من خلال تحديد مكوناته التقنية وعملياته الخوارزمية، مما أتاح إمكانية التمييز بوضوح بين ما يندرج ضمن نطاق الذكاء الاصطناعي وما لا يندرج فيه.وعلى النقيض من ذلك، ركّزت المفوضية الأوروبية على المفاهيم الأخلاقية والانسانية، بدلاً من المفاهيم التكنولوجية.[2]

وفي هذا الصدد، نصّت المادة 02 من الاتفاقية–الإطار لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية ودولة القانون على ما يلي: لأغراض هذه الاتفاقية، يُقصد بـ "نظام الذكاء الاصطناعي" النظام القائم على الآلة الذي يستنتج لأهداف صريحة أو ضمنية، من المدخلات التي يتلقاها، كيفية توليد مخرجات مثل التنبؤات أو المحتوى أو التوصيات أو القرارات التي قد تؤثر على البيئات المادية أو الافتراضية. وتختلف أنظمة الذكاء

[1] أحمد حسني علي أشقر، الخصوصية الرقمية في عصر الذكاء الاصطناعي: قراءة في التشريعين الأردني والفلسطيني، مجلة جامعة القدس المفتوحة للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 66، جانفي 2025، ص35.

[2] بلهوط براهيم، التأطير القانوني للذكاء الاصطناعي، مجلة الدراسات والبحوث القانونية، جامعة اكلي محند اولحاج، البويرة، مجلد 9، عدد 2، 2024، ص14.

الاصطناعي في مستويات الاستقلالية وقابلية التكيف بعد النشر.[1] وهو تقريباً نفس التعريف الذي تبناه قانون الذكاء الاصطناعي للاتحاد الأوروبي، والذي عرّفه ضمن المادة 1/3 على أنه: نظام قائم على الآلة، صُمّم للعمل بدرجات متفاوتة من الاستقلالية، وقد يُظهر القدرة على التكيّف بعد نشره، وأنّه لتحقيق أهداف صريحة أو ضمنية يستنتج من المدخلات التي يتلقّاها، كيفية توليد مخرجات مثل التنبؤات أو المحتوى أو التوصيات أو القرارات التي يمكن أن تؤثر على البيئات المادية أو الافتراضية[2].

أمّا فيما يخص الدول العربية فما زالت تفتقر إلى تعريف قانوني للذكاء الاصطناعي، رغم ما قدّمته من تطور ملحوظ من خلال تبنيها لاستراتيجيات وطنية شاملة حول هذا المجال على غرار الإمارات العربية المتحدة2017 والمملكة العربية السعودية2019، قطر2020 ومصر2021.[3]

الجزائر هي الأخرى لم تقدم تعريفا قانونيا حول الذكاء الاصطناعي، إلا أنها قد أبدت اهتماما يومًا بعد يوم بهذا المجال كتكنولوجيا جديدة فرضت نفسها في السنوات الأخيرة، وذلك بإنشاء المدرسة العليا للذكاء الاصطناعي.[4]

كما اعتمدت رسميًا استراتيجية وطنية للذكاء الاصطناعي في ديسمبر 2024، وذلك خلال اختتام الطبعة الثالثة من المؤتمر الإفريقي للمؤسسات الناشئة بالجزائر العاصمة. ترمي إلى

[1] Conseil de l'Europe, Convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit, Série des traités du Conseil de l'Europe – n° 225, Vilnius, 5 septembre 2024, article02.

[2] établissant des règles harmonisées concernant l'intelligence artificielle (Loi sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, Journal officiel de l'Union européenne (JOUE), L 206, 12 juillet 2024, article 3, § 1. Disponible sur : www.eur-lex.europa.eu (15_04_2025) 12:00 h

[3] عصام الجوهري وآخرون، تقييم استراتيجيات الذكاء الاصطناعي المعلنة في الدول العربية، المجلة المصرية للتنمية والتخطيط، بدون مجلد وعدد وتاريخ النشر، ص2.

[4] المرسوم الرئاسي 21_323، المؤرخ في 22 أوت 2021، يتضمن إنشاء مدرسة وطنية عليا للذكاء الاصطناعي، ج ر، عدد 65، الصادرة في 26 أوت 2021.

مواكبة التطورات الحاصلة في مجال الابتكار التكنولوجي وتعزيز مكانة الجزائر في هذا المجال على المستوى الإفريقي والعالمي[1].

**ثانيا: أنواع الذكاء الاصطناعي:**

يمكن تصنيف أنواع الذكاء الاصطناعي بناءً على زاويتين مختلفتين، وذلك على النحو التالي:

**أ/الذكاء الاصطناعي تبعا للقدرات:**

يمكن تصنيف الذكاء الاصطناعي تبعاً لما يتمتع به من قدرات إلى ثلاثة أنواع مختلفة تتراوح من رد الفعل البسيط إلى الإدراك والتفاعل وتتمثل فيما يلي:

**1/ الذكاء الاصطناعي الضعيف:**

ويسمّى أيضا بالذكاء الاصطناعي المحدود، وذلك لأنّه مبرمج للقيام بوظائف معينة في إطار بيئة محدّدة، وبالتالي لا يمكن له العمل إلاّ في ظروف البيئة الخاصّة به ويعتبر تصرفه بمثابة ردّ فعل على موقف معيّن.[2]وغالبية تطبيقات الذكاء الاصطناعي الحالية تندرج ضمن هذا النوع ، ومثالها تصنيف الرسائل غير المرغوب فيها وأنظمة التوصيات، أو ترجمة غوغل أو تطبيق سيري.[3]

**2/الذكاء الاصطناعي القوي أو العام:**

وهو النوع الذي يمكن أن يعمل بقدرة تشابه قدرة الانسان من حيث التفكير، ويهدف إلى تطوير أنظمة ذكية قادرة على التفكير والتخطيط من تلقاء نفسها بطريقة تحاكي الذكاء البشري. إلا أنّه لحدّ الساعة لا يوجد أمثلة عمليّة لهذا النوع، إذ لايزال في طور البحث والدراسة. وتعدّ

[1] وكالة الأنباء الجزائرية، الجزائر تعتمد استراتيجية وطنية للذكاء الاصطناعي، مقال منشور بتاريخ 08 ديسمبر 2024، متاح عبر الموقع https://www.aps.dz، تاريخ الاطلاع:2025/04/22 على الساعة 21:00..

[2] أميرة بدوي نجم، مرجع سابق، ص27.

[3] أماني يحيى عبد المنعم النقيب، مرجع سابق، ص30_31.

طريقة الشبكة العصبية الاصطناعية من طرق دراسة الذكاء الاصطناعي العام، إذ تعنى بإنتاج نظام شبكات عصبية للآلة مشابهة لتلك التي يحتويها الجسم البشري. [1]

**3/ الذكاء الاصطناعي الخارق(الفائق):**

يفترض في هذا النوع من الذكاء الاصطناعي أنه يتجاوز مستوى الذكاء البشري، بحيث يكون قادرا على أداء المهام بشكل أفضل مما يقوم به الإنسان المتخصص وذو المعرفة.[2]وهو عبارة عن آلات مزوّدة بقدرات تفوق القدرات الذهنية لدى البشر، و غالبا ما تستخدم هذه الفكرة في أفلام الخيال العلمي ، إذ أنَّ الباحثين لم يتمكّنوا بعد من الوصول إلى تطبيق عملي له على أرض الواقع.[3]

**ب/ الذكاء الاصطناعي تبعاً للوظائف:**

كما يمكن تصنيف الذكاء الاصطناعي تبعا للوظائف التي يقوم بها، إذ يضمّ هذا التصنيف أربعة أنواع مختلفة هي كالآتي:

**1/ الآلات التفاعلية:**

يعدّ هذا النوع من أبسط أنواع الذكاء الاصطناعي، حيث يكون مبرمجًا لإنتاج استجابة محددة بناءً على مدخل معين. تقوم هذه الآلات دائمًا برد الفعل بنفس الطريقة في كل مرة تواجه فيها نفس الوضع، ولا تمتلك القدرة على التعلّم من التجارب أو تكوين تصوّر عن الماضي أو المستقبل. وأبرز مثال على هذا النوع هو"**Deep Blue** "، الحاسوب الخارق من شركة"**IBM**" الذي تغلّب على بطل العالم في الشطرنج "جاري كاسباروف"، حيث كان يعتمد فقط على تحليل تحركات الخصم في اللحظة نفسها دون الرجوع لأي معلومات سابقة[4].

---

[1] مدحت محمد أبو النصر، الذكاء الاصطناعي في المنظمات الذكية،ط1، المجموعة العربية للتدريب والنشر،القاهرة،2020 ص 141.

[2] مدحت محمد أبو النصر، المرجع نفسه، ص141.

[3] أماني يحيى عبد المنعم النقيب، مرجع سابق، ص31.

[4] Bernard Marr, Understanding the 4 Types of Artificial intelligence, Bernard Marr & Co, 2 juillet 2021. Disponible sur : https://bernardmarr.com, consulté le 18 avril 2025 à 21 :45.

**2/ الذاكرة المحدودة:**

تستطيع أنظمة الذكاء الاصطناعي التي تعتمد على الذاكرة المحدودة اتخاذ قرارات مدروسة ومحسّنة اعتمادًا على البيانات السابقة التي جمعتها. وتنتمي أغلب تطبيقات الذكاء الاصطناعي الحالية إلى هذا النوع من الأنظمة، بدءًا من روبوتات الدردشة والمساعدين الافتراضيين وصولًا إلى السيارات ذاتية القيادة[1]، والتي يتم عن طريقها تخزين السرعة الأخيرة للسيارات الأخرى ومقدار بعد السيارة عنها، والحدّ الأقصى للسّرعة وغيرها من البيانات الأخرى اللاّزمة للقيادة عبر الطرق.[2]

**3/ نظرية العقل:**

هذا النوع من الذكاء الاصطناعي سيمكّن الآلات من اكتساب قدرات حقيقية على اتخاذ القرار تشبه قدرات الإنسان. حيث ستكون قادرة على فهم المشاعر وتذكّرها، ثم تعديل سلوكها بناءً على تلك المشاعر أثناء تفاعلها مع الناس. لكن لا يزال هناك تحديات في تحقيق هذا النوع من الذكاء الاصطناعي، بسبب صعوبة محاكاة التغير السريع في المشاعر في التواصل البشري. ورغم ذلك، أُحرزت بعض التقدمات، مثل قدرة الروبوت "كيسمت" على تقليد مشاعر الوجه البشري، والروبوت "صوفيا" الذي يستطيع التعرف على الوجوه والتفاعل مع تعبيرات الوجه[3].

**4/ الإدراك الذاتي:**

يُعد الذكاء الاصطناعي ذو الإدراك الذاتي المرحلة الأكثر تقدمًا في تطور الذكاء الاصطناعي، إذ يُفترض أن تكون الآلات قادرة على إدراك مشاعرها الداخلية ومشاعر الآخرين، مما يمنحها وعيًا وذكاءً مشابهًا للبشر، مع امتلاكها لرغبات واحتياجات ومشاعر خاصة بها. وستكون الآلات المزودة بهذا النوع من الذكاء الاصطناعي مدركة لحالاتها العاطفية والعقلية

---

[1] Aditya Kumar, Types of AI Explained, simplilearn, dernière mise à jour le 11 avril 2025, Disponible à https://www.simplilearn.com, consulté le 18 avril 2025, à23:10 .

[2] مدحت محمد أبو النصر، مرجع سابق، ص142.

[3] Bernard Marr, op. cit.

الداخلية، وقادرة على استخلاص استنتاجات. لكن حتى الآن، لم يتم تطوير هذا النوع المتقدم من الذكاء الاصطناعي، ولم تُطوّر بعد الخوارزميات أو الأجهزة اللازمة لتحقيقه[1].

**الفرع الثاني: نشأة الذكاء الاصطناعي وتطوره**

لا يُعدّ الذكاء الاصطناعي وليد اللحظة، بل هو ثمرة حثيثة لتراكمات فكرية وعِلمية ممتدّة عبر عدّة قرون، فقد شغل مفهوم الذكاء اهتمام الفلاسفة والمفكرين منذ أكثر من ألفي سنة، حيث سعوا إلى فهم قدرات العقل البشري من حيث التعلّم، والذاكرة والعقلانية. بل وتساءل بعضهم عمّا إذا كان بالإمكان تقليد هذه العمليات أو القدرة على خلقها، ويظهر هذا الاهتمام المبكّر في آثار الحضارات القديمة، كالإغريق والمصريين القدامى اللّذين اهتموا منذ أمد طويل بفكرة صنع آلات ذكيّة تقلّد تصرف البشر.[2]

إلّا أن التحوّل الحقيقي نحو الذكاء الاصطناعي كعلم مستقل لم يبدأ إلا في منتصف القرن العشرين تحديداً عام 1950م، عندما قام العالم **آلان تورينج** "Alan Turing"بتقديم ما يُعرف باختبار تورينج "Turing Test" الذي يعنى بتقييم الذكاء لجهاز الحاسب الآلي، وتصنيفه ذكياً في حال قدرته على محاكاة العقل البشري.[3]

أمّا عن الانطلاقة الفعلية للذكاء الاصطناعي فقد كانت من مؤتمر في معهد "دارت موث" في صيف عام 1956م، والذي شارك في تنظيمه عدد من رواد هذا المجال من أبرزهم: جون مكارثي(John McCarthy) ، مارفن مينسكي(Marvin Minsky) ، ألين نيويل (Allen Newell)، وهربرت سيمون(Herbert Simon) وتمكّن هؤلاء من تطوير برامج قادرة على حلّ مسائل في الجبر وإثبات النظريات المنطقية باستخدام اللغة الإنجليزية.[4]

[1] Bernard Marr,ibid.

[2] عادل عبد النور بن عبد النور، مرجع سابق، ص18.

[3] مدحت محمد أبو النصر، مرجع سابق، ص136.

[4] أسامة عبد الرحمن، الذكاء الاصطناعي و مخاطره، ط1، دار زهور المعرفة والبركة، الجيزة(مصر)،2018،ص39.

خلال العقد الأول أو نحو ذلك بعد مؤتمر دارت موث ازدهر الذكاء الاصطناعي وشهد العديد من النجاحات الهامّة؛ بما في ذلك خوارزمية "آلان روبنسون" للتفكير المنطقي العام وبرنامج لعبة الدّامة الذي صمّمه "آرثر صامويل"، والذي طوّر من نفسه تدريجياً حتى تمكّن من التغلّب على صانعه.[1]

غير أن هذا الزخم لم يدم طويلًا؛ فبحلول السبعينيات بدأت خيبة الأمل تعانق هذا المجال لدرجة أن سميّت هذه الحقبة بشتاء الذكاء الاصطناعي "AI Winter" وكان ذلك لعدم وجود نتائج مرضية وفشله في تحقيق الوعود التي قطعها على نفسه سابقاً. وهذا راجع لصعوبة التنفيذ بسبب نقص القدرة الحاسوبية المتمثلة في أجهزة الكمبيوتر أنذاك، ما أدّى إلى تراجع التمويل والدعم الحكومي للمجال.[2]

لكن سرعان ما بدأ الذكاء الاصطناعي يستعيد أنفاسه خلال فترة الثمانينيات، وذلك بفضل ظهور ما يُعرف بـ "الأنظمة الخبيرة". وهي أحد برامج الذكاء الاصطناعي صُمّمت لمحاكاة المعرفة ومهارات التحليل لواحد أو أكثر من الخبراء البشريين، وقد لاقت هذه الأنظمة رواجًا كبيرًا خاصّة في المجالات الطبية والصناعية. وبحلول عام 1985 بلغت قيمة سوق الذكاء الاصطناعي أكثر من مليار دولار، فاستعاد بذلك ثقة الحكومات والشركات التي سارعت في تمويله من جديد. وبعد سنوات قليلة بدءا من انهيار سوق آلةLisp Machine (إحدى لغات البرمجة) في عام 1987 شهدت أبحاث الذكاء الاصطناعي انتكاسة أخرى وهذه المرّة دامت لمدة أطول.[3]

ومع مطلع الألفية الجديدة، شهد الذكاء الاصطناعي نهضة نوعية بفضل التقدّم الهائل في قدرات الحوسبة وتوافر كميّات ضخمة من البيانات(Big Data) ، إضافة إلى تطوّر تقنيات

[1] أميرة بدوي نجم، مرجع سابق، ص19.

[2] عبد الله موسى، أحمد حبيب بلال، مرجع سابق، ص36.

[3] أسامة عبد الرحمن، مرجع سابق، ص40.

تعلّم الآلة (Machine Learning) والتعلّم العميق (Deep Learning) والشبكات العصبية الاصطناعية(Artificial Neural Networks) .[1]

وقد ساهمت هذه العوامل مجتمعة في إخراج الذكاء الاصطناعي من المختبرات الأكاديمية إلى واقع الحياة اليومية، حيث أصبح يُستخدم على نطاق واسع في مجالات متعددة، كالخدمات اللّوجستية، واستخراج البيانات والتشخيص الطبي والعديد من المجالات الأخرى.[2]

وبهذا نكون قد قدّمنا أبرز المحطات التي مرَّ بها الذكاء الاصطناعي منذ ميلاده وإلى غاية صورته الحالية المعاصرة، مبيّنين كيف تطوّر من مجرّد تصوّرات فلسفية إلى تقنيات عمليّة توظف اليوم في شتى مجالات الحياة.

**الفرع الثالث: آلية عمل الذكاء الاصطناعي**

تُبنى آلية عمل الذكاء الاصطناعي على تفاعلٍ تكامليّ بين عنصرين أساسيين هما الخوارزميات والبيانات.

تُعرَّف الخوارزميات، استنادًا إلى معجم البيانات والذكاء الاصطناعي، بأنها مجموعة من التعليمات المحددة والمترابطة تُوضع لحل مشكلة أو تنفيذ مهمة معينة. ويُشتقّ مصطلح "خوارزمية" من اسم عالم الرياضيات الفارسي في القرن التاسع محمد بن موسى الخوارزمي، الذي تُرجم اسمه إلى اللاتينية بـ(Algoritmi)[3]

وتُعدّ الخوارزمية في جوهرها اختصارًا لما يُعرف بـ "التعليمات البرمجية"، إذ تمثل سلسلة من الأوامر التي يكتبها المبرمج ويجمعها لإنتاج وحدة قابلة للتنفيذ، وتُعرف كذلك باسم البرنامج.

[1] سالي محمد عبد، يسرى شاكر عجاج، مصطفى قصي علي وآخرون، الذكاء الاصطناعي مفاهيم وتقنيات–دليل تعليمي للطلبة، ط1، دار السرد للطباعة والنشر والتوزيع، بغداد(العراق)،2024،ص14.

[2] أسامة عبد الرحمن، مرجع سابق، ص40.

[3] مريم ساغي، مليكة مذكور، مرجع سابق، ص525_526.

وبذلك، فهي مجموعة من الإجراءات المرتبة وفق منطق معين، تسعى للوصول إلى هدف معيّن أو نتيجة مرجوّة.[1]

أمّا البيانات فهي تشكّل المادة الخام التي تعتمد عليها خوارزميات الذكاء الاصطناعي في أداء وظائفها، تشمل مجموعة من الحقائق أو القياسات أو المعطيات وقد تأتي في صور متعددة فيمكن أن تكون أرقاما أو حروفا أو صورا أو رموزا أو أشكالا خاصة، حيث تصف فكرة أو موضوع أو هدف معين[2].

ولقد أدّى التطور التكنولوجي المتسارع وانتشار الأجهزة المتصلة بالأنترنت والاستخدام المتزايد لوسائل الاعلام الرقمية من قبل المؤسسات من جهة والأفراد عبر وسائل التواصل الاجتماعي من جهة أخرى إلى إنتاج كميات هائلة من البيانات يومياً، تعرف بـ البيانات الضخمة (Big Data)،وهي مجموعة البيانات التي يتجاوز حجمها قدرة أدوات قواعد البيانات التقليدية من التقاطها وتخزينها وإدارتها وتحليلها.[3]

وقد شكّل ظهور البيانات الضخمة تحولًا جذريًا في قدرات الذكاء الاصطناعي، إذ ترتبط دقة نتائجه وفعالية أدائه ارتباطًا وثيقًا بحجم ونوعية البيانات التي تُغذّيه. فكلما زادت مدخلات النظام من البيانات، ازداد تعلّمه وارتفعت كفاءة مخرجاته. ومن ثم، يمكن القول إنّه لا وجود لذكاء اصطناعي فعّال دون قاعدة كبيرة من البيانات الضخمة، التي تمثّل المادة الأولية التي يُبنى عليها "ذكاؤه" وتُغذّى بها عملياته التحليلية والمعرفية. [4]

[1] عبد الله موسى، أحمد حبيب بلال، ص98.

[2] بوكر رشيدة، الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي بين تصاعد التهديدات وفرص تعزيز الأمن السيبراني، د ط دار إيلياء للنشر والتوزيع، الجزائر، 2024، ص24.

[3] بوبعاية نصيرة، ، دور البيانات الضخمة والذكاء الاصطناعي في مواجهة وباء فيروس كورونا_ تجارب دولية ناجحة_ مجلة وحدة البحث في تنمية الموارد البشرية، مجلد 16، عدد 03 الخاص (الجزء2)، نوفمبر 2021، ص 127_128.

[4] مريم ساغي، مليكة مذكور، مرجع سابق، ص527.

وتعتبر البيانات الشخصية للأفراد جزء لا يتجزأ من جملة البيانات التي تُغذّى بها تطبيقات الذكاء الاصطناعي باختلاف أنواعها ومجالاتها، فالبيانات الشخصية المستند إليها في المعالجة تعدّ وقوداً لتلك التقنيات والتطبيقات.[1]

وهي تحظى بقيمة كبيرة لتدريب أنظمة الذكاء الاصطناعي، ذلك لكونها صادرة عن أشخاص حقيقيين في مواقف حياتية يومية، إذ أنها تشمل كل شيء قد يقدمه المستخدم من نصوص التعليقات أو المراجعات، إلى الصور ومقاطع الفيديو، وحتى التسجيلات الصوتية. فبفضل تنوعها يمكن تدريب النظام الذكي على اكتشاف الأنماط، والتنبؤ بالاتجاهات المستقبلية، واتخاذ قرارات مدروسة. فكلما كانت البيانات عالية الجودة ومتنوعة زادت قدرة الذكاء الاصطناعي على أداء مهامه بشكل أفضل.[2]

وأمام هذه التطورات الهائلة في قدرات الذكاء الاصطناعي بات العالم يشعر بالقلق حيال خصوصيات الأفراد لا سيما الرقمية منها. ومن ثمّ برزت علاقة تضادّ محتملة بين الذكاء الاصطناعي والحق في الخصوصية بشكل عام.[3]

وعليه، أصبح من الضروري تسليط الضوء على الانعكاسات التي تُخلّفها تقنيات الذكاء الاصطناعي على الحق في الخصوصية، وهو ما سيتم تناوله في النقطة الموالية.

**المطلب الثاني: انعكاسات الذكاء الاصطناعي على الحق في الخصوصية**

في ظل الاستخدام المتزايد لتطبيقات الذكاء الاصطناعي في مختلف مناحي الحياة اليومية، أصبح الحق في الخصوصية على المحك. فقد أفرز هذا الواقع التقني الجديد انعكاسات خطيرة تمسّ بخصوصية الأفراد، لا سيما فيما يتعلق بأساليب جمع البيانات الشخصية، التي باتت تعتمد على تقنيات معقّدة وغير مسبوقة، كما لم يعد الخطر محصورًا في مجرد الوصول إلى

[1] هبة رمضان رجب، مرجع سابق، ص425.

[2] Data for AI : The Fuel That Supercharges Machine Learning, Revelate Blog, 30 août 2023, disponible sur : https://revelate.co/blog, consulté le 21 avril 2025 , à18:30.

[3] أحمد حسني علي أشقر، مرجع سابق، ص36.

هذه المعلومات، بل امتدّ ليشمل كيفية معالجتها واستعمالها في سياقات قد تتعارض مع مبدأ احترام الحياة الخاصة.

وانطلاقًا من ذلك، تقتضي دراسة انعكاسات الذكاء الاصطناعي على هذا الحق معالجة أبرز صور الانتهاكات التي تمارس بواسطة تقنياته المختلفة، بالإضافة إلى تحليل الأغراض والدوافع التي تكمن وراء جمع البيانات الشخصية وخطورة استخدامها على حياة الأفراد وحقوقهم الأساسية.

**الفرع الأول: صور انتهاك الذكاء الاصطناعي للحق في الخصوصية**

يتعرض الأفراد للعديد من الانتهاكات التي تهدّد خصوصيتهم نتيجة استعمالهم لتطبيقات الذكاء الاصطناعي المختلفة،وتتنوّع صور هذه الانتهاكات باختلاف التقنية المستعملة والسياق الذي توظف فيه. وفيما يلي أبرز هذه الصور:

**أولا: مراقبة سلوك المستخدم**

يُعد تتبع سلوك المستخدم أحد أبرز الأساليب التي تعتمدها أنظمة الذكاء الاصطناعي في جمع البيانات الشخصية، وغالبا ما يتم ذلك بشكل متواصل وغير محسوس، عبر مجموعة من المنصات الرقمية التي باتت تشكل جزءًا أساسياً من الحياة اليومية.

**أ/ محركات البحث:**

لقد أصبحت تقنيات الذكاء الاصطناعي توظف على مستوى أجهزة الحوسبة ومحركات البحث، حيث تقوم الخوارزميات الذكيّة بتتبع عادات تصفّح المستخدمين، بما في ذلك سجل البحث وزيارات الصفحات، وفي غالب الأحيان يكون ذلك بدون موافقة صريحة، ويتم استخدام هذه البيانات لبناء ملفات تعريف مفصّلة عنهم.[1]

[1] Andrea Granados, AI and Personal Data: Balancing Convenience and Privacy Risks, velaro, Dernière mise à jour le 15 novembre 2024, https://velaro.com, consulté le 24-04-2025 à19 :40.

ولعلّ من أشهر آليات تعريف هوية المستخدم الأقلّ شفافية هي ملفات تعريف الارتباط (Cookies)، والتي يتم تخزينها على جهاز المستخدم عند زيارته لموقع من المواقع وتصفحه على شبكة الأنترنت.[1] حيث تتيح هذه التقنية تتبع المستخدم منذ لحظة دخوله للموقع، وتخزين جميع البيانات المتعلقة به، كاسمه ونوع الجهاز المستخدم وطريقة اتصاله بالشبكة ومجالات اهتمامه وبحثه، إلى جانب تسجيل كافة البيانات الشخصية الحقيقية التي يجبر المستخدم على الإفصاح بها من أجل الوصول لمضمون معيّن، وغالباً ما يتمّ تفعيل هذه الملفات تلقائيا دون موافقة الشخص المعني؛ وهذا ما يعتبر انتهاكا للخصوصية.[2]

فتصفحنا مثلا لموقع رياضي معين يمكن الخوارزميات الذكية من تحديد رياضتنا المفضلة، كما يتيح مشاهدة أفلام معينة ومحتويات مرئية من التعرف على نوع أفلامنا المفضلة وما يعكسه ذلك حول طبيعة شخصيتنا[3]، بحيث تعكس هذه البيانات بشكل دقيق سلوك المستخدم واهتماماته على الشبكة.

**ب/وسائل التواصل الاجتماعي وتطبيقات الدردشة:**

أصبحت مواقع التواصل الاجتماعي فضاءً رقمياً يلجئ إليه الأفراد ويقضون فيه معظم أوقاتهم، يعبرون من خلاله عن أفكارهم ومعتقداتهم، ويتفاعلون مع المنشورات المختلفة ويبدون عن آرائهم، كما يقومون بمشاركة الصور ومقاطع الفيديو لتكون متاحة للجميع.

أصبحت أكبر الشبكات الاجتماعية تضمّ ملايين أو مليارات المستخدمين، بما في ذلك فيسبوك، وأنستغرام، وتيك توك،،، إلخ. إلاّ أنّ هذا النمو الكبير منحها وصولًا استثنائيًا وتأثيرًا في حياة المستخدمين. حيث تقوم شركات الشبكات الاجتماعية بجمع بيانات حساسة حول

[1] توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الأنترنت وحرية التعبير، منشورات اليونسكو، منظمة الأمم المتحدة للتربية والعلم والثقافة، مترجم بفضل مساهمة الوكالة السويدية للتعاون الإنمائي الدولي (سيدا)، فرنسا، 2012، ص39.

[2] عبد الله شيباني، وداد بن سالم، حق الخصوصية المعلوماتية في ضوء الذكاء الاصطناعي، مجلة الدراسات القانونية والاقتصادية، جامعة محمد لمين دباغين سطيف 2، المجلد 6، العدد 2، 2023، ص 469.

[3] مريم ساغي، مليكة مذكور، مرجع سابق، ص534.

أنشطة الأفراد واهتماماتهم وخصائصهم الشخصية وآرائهم السياسية وعاداتهم الشرائية وسلوكياتهم على الإنترنت[1]، فكل مرّة تقوم فيها بنشر صورة، كتابة تعليق، مشاركة منشور أو حتى الاعجاب به، يتم تسجيل هذه الأنشطة وتحليلها.[2]

ضف إلى ذلك أنّ جميع مواقع التواصل الاجتماعي تتطلب إدخال المستخدم لبعض من بياناته الشخصية التي تعدّ شرطا أساسياً لإتمام عملية التسجيل، كالإسم، العنوان، تاريخ الميلاد، الجنس،،،، وعليه تقوم هذه المواقع بتخزينها في قاعدة بياناتها.[3]

إنّ الكميات الهائلة من البيانات الشخصية التي تقوم منصات التواصل الاجتماعي بجمعها والاحتفاظ بها تظل عرضة للاختراق، والاستخلاص(scraping) ، وتسريبات البيانات، خاصة إذا فشلت هذه المنصات في تطبيق تدابير أمان قوية وقيود صارمة على الوصول إلى المعلومات[4].

كما أصبحت الخوارزميات الذكية توظف ضمن تطبيقات الدردشة بطرق قد تُشكّل تهديدًا بالغًا لخصوصية المستخدمين، فعادة ما تطلب هذه التطبيقات أذونات للوصول إلى الكاميرا، الميكروفون، الموقع الجغرافي، جهات الاتصال، التخزين، وسجلات الرسائل والمكالمات بزعم تحسين تجربة المستخدم. إلاّ أن هذا الوصول ينتج عنه عواقب وخيمة مثل التسجيل أو المراقبة غير المصرح بها، فضلاً عن تتبع تحركات الأفراد، قراءة الرسائل الشخصية دون إذن، وإساءة استخدام سجلات المكالمات[5].

[1] Social Media Privacy, Electronic Privacy Information Center (EPIC), (sans date), Disponible sur : https://epic.org, Consulté le 25-04-2025, à 22 :30 .

[2] رافي برازي، كيف تشكل بياناتك الشخصية على مواقع التواصل الاجتماعي وقوداً لنماذج الذكاء الاصطناعي، 04-07-2024، متاح على الرابط: https://bawabaai.com ، تاريخ الاطلاع :25 -04-2025، على الساعة21:25 .

[3] هبه رمضان رجب، مرجع سابق، ص 425.

[4] Social Media Privacy ,op.cit .

[5] Akanbi Caleb , App permissions and privacy concerns , Disponible sur : https://www.researchgate.net, Consulté le :26-04-2025 à 11 :45 .

**ج/ التسوّق الالكتروني:**

لم تعد عمليات الشراء عبر الإنترنت مجرّد وسيلة لاقتناء المنتجات والخدمات، بل أصبحت وسيلة فعّالة لجمع كميات هائلة من البيانات الشخصية. فالأنظمة الذكية تتبع خطوات المستخدم خلال كل عملية تسوّق، بداية من تصفّح المنتجات، مرورًا باختيار العناصر، ووصولًا إلى الدفع الإلكتروني.

تتطلّب عمليات الشراء وطلب الخدمات والمزادات في الأنترنت إدخال بيانات شخصيّة مثل الاسم ورقم الهاتف والعنوان والبريد الالكتروني وأحيانا بيانات بطاقته البنكية، وببساطة فإنّ هذه العمليات تتطلب معلومات تفصيليّة عن الشخص يغيب فيها القدرة على التخفّي خلافاً للعالم الواقعي[1]، ناهيك عن قدرة الخوارزميات الذكيّة على تحديد قائمة مشترياتنا التجارية، ونوعها وأهم الماركات العالمية التي تستقطب اهتمامنا، كما يمكن بواسطة الدفع الالكتروني تحديد مكان وزمان تواجدنا ومتجرنا المفضّل وقيمة مصاريفنا.[2]

ومن ثمّ، فإنّه ليس من باب الصدفة كما كنّا نعتقد حينما تظهر لنا إعلانات أو توصيات لمنتجات تتطابق تمامًا مع ما كنا نفكر به أو بحثنا عنه من قبل، بل وتتناسب حتى مع أذواقنا وميولنا الشخصية. فلا داعي للاستغراب فهذا كلّه نتيجة لتحليل سلوكنا الرقمي الذي تقوم به الخوارزميات الذكيّة.

**ثانيا: التفاعل المباشر مع الأنظمة الذكية**

يتزايد استخدام الأنظمة الذكية في حياتنا اليومية، بما في ذلك إنترنت الأشياء والمساعدين الأذكياء وروبوتات الدردشة مما يخلق طرقًا جديدة لجمع البيانات الشخصية للأفراد تتم عن طريق التفاعل المباشر. وفيما يلي أهم هذه الوسائل:

[1] خالد حسن أحمد، مرجع سابق، ص72.

[2] مريم ساغي، مليكة مذكور، مرجع سابق، ص 534.

**أ/ إنترنت الأشياء:**

وهو عبارة عن مجموعة من الأدوات، مثل: المنازل الذكية، الساعات الذكية، أجهزة التلفاز الذكية، الأدوات الطبية ... الخ، والتي ترتبط ببعضها البعض وبالإنترنت، فتقوم بجمع كم هائل من البيانات الخام وتحليلها دون تدخل بشري؛ فلها أن تتبادل المعلومات وتتخذ القرارات بشكل آلي ودقيق عبر بروتوكول الإنترنت[1]، بدءًا من تنظيم الروتين اليومي وصولاً إلى مراقبة المقاييس الصحية. ويعالج الذكاء الاصطناعي هذه البيانات لتوفير تجارب مخصصة، مثل تعديل الإعدادات أو تقديم التوصيات. ومع ذلك، تفتقر العديد من هذه الأجهزة إلى أنظمة أمان قوية، مما يجعلها عرضة للاختراق، خاصة مع محدودية قدرة المستخدمين على التحكم في عمليات جمع البيانات ومشاركتها، مما يفتح المجال لإساءة الاستخدام أو الوصول غير المصرح به من جهات خبيثة.[2]

**ب/ المساعدين الأذكياء:**

وهي عبارة عن مساعدات افتراضية تعمل بالصوت، تهدف الى تسهيل الحياة اليومية للمستخدمين، من خلال تنفيذ الأوامر والمهام مثل "Google Home" و" Amazon's Alexa".غير أن هذه الأجهزة بالرغم من مزاياها تُعدّ بمثابة أجهزة تنصّت، فهي تسجّل كل ما يتحدّث عنه المستخدمون أثناء جلوسهم في منازلهم أو أي مكان آخر، حيث تبقى في حالة "استماع دائم" لاستقبال الأوامر الصوتية، وتقوم بإرسال البيانات إلى الشركة الأمّ التي تخزّنها وتحلّلها، ومن ثمّ يمكن لها توقّع ما يتحدّث عنه المستخدمون بكل سهولة ومعرفة ماذا يفعلون وماهم على وشك القيام به، كما قد تستعملها من أجل تحسين أداء عمل هذه المساعدات أو لأغراض أخرى.[3]

---

[1] عبد الله شيباني، وداد بن سالم، مرجع سابق، ص470.

[2] Andrea Granados ,op.cit.

[3] حصة أحمد عبد الله التويم، وفاء أحمد عياض الغامدي، انتهاك الخصوصية في تقنيات الذكاء الاصطناعي: الواقع وسبل المواجهة من منظور التربية الإسلامية، مجلة شباب الباحثين، جامعة سوهاج(مصر)، عدد 12، ج3، 2023، ص845.

**ج/ روبوتات الدردشة:**

وأبرز مثال على ذلك "Chat Gpt" الذي أصبح رائجًا بين مختلف فئات المستخدمين. فعندما نطلب من الروبوت الإجابة عن سؤال أو أداء مهمة ما، فهو يقوم باستدراجنا عن طريق طرح بعض الأسئلة بهدف تقديم الإجابة المطلوبة، عندئذ سنجد أنفسنا نقدم له معلومات حساسة عنّا من دون وعي. كما أن سياسة الاستخدام لم تنص صراحة على أية إجراءات للحفاظ على البيانات الشخصية الحساسة أو تلك التي قد تكشف هوية المستخدم.[1]

وقد أعلنت شركة Open AI بتاريخ 24 مارس 2023 عن خطأ تقني تسبب في تسريب عناوين سجلات محادثات بعض مستخدمي "شات جي بي تي"، بالإضافة إلى تسريب بيانات مهمة تضمنت أرقام بطاقات ائتمان لمشتركي خدمة "Chat GPT Plus" المدفوعة.[2]

**د/ الروبوتات الطبية والمركبات الذكية:**

يمكن جمع البيانات الشخصية أيضا عن طريق الروبوتات، حيث تستخدم هذه الأخيرة بكثرة في العمليات الجراحية التي يتم برمجتها لذلك، فبعد تخزين المعلومات الصحيّة للمريض في قاعدة بيانات هذا الروبوت الطبي، قد تتسرّب إلى مختلف الجهات سواء من طرف الشخص المتحكم بتشغيله أو من الروبوت ذاته.[3]

من جهة أخرى، تعتمد المركبات ذاتية القيادة على نظام تحديد المواقع العالمي (GPS) وتحتاج لأن تكون متصلة بالإنترنت بصفة مستمرة، ما يجعل أنظمتها المعلوماتية معرضة للقرصنة، فضلاً عن إمكانية تتبع حركات الركاب وتسجيلها، خاصة إذا علمنا أن تأجير هذه

[1] أحمد محمد براك، مرجع سابق، ص 352.

[2] نرمين عبدالقادر إمبابي، تأثير استخدام روبوت المحادثة الذكية "شات جي بي تي" على حماية خصوصية بيانات المستفيدين: دراسة مسحية مقارنة، المجلة العلمية للمكتبات والوثائق والمعلومات، كلية الآداب – جامعة القاهرة، مجلد6، عدد 19، يوليو 2024، ص42.

[3] معزوز دليلة، والي نادية، مخاطر الذكاء الاصطناعي على الخصوصية الرقمية و آليات حمايتها، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة، مجلد 9، عدد3، سبتمبر 2024، ص822.

المركبات يتم بواسطة تطبيقات إلكترونية تتطلب تسجيل بعض البيانات الشخصية للمستخدم من أجل الاستفادة منها.[1]

**ثالثا: استخدام أساليب احتيالية**

يمكن توظيف تقنيات الذكاء الاصطناعي في تنفيذ أساليب احتيالية لخداع الأفراد وجمع بياناتهم الشخصية، وتمثل الهندسة الاجتماعية أهم هذه الأساليب. إذ تهدف إلى الحصول بشكل غير مشروع على معلومات تتسم بالحساسية والسرية، مثل كلمات السرّ أو اسم المستخدم عن طريق التلاعب أو التهديد، بهدف الوصول إلى البيانات ذاتها أو لسرقة الهوية.[2]

وفي هذا السياق، أسهم الذكاء الاصطناعي في تطوير أساليب الهندسة الاجتماعية، مما جعل عمليات الاحتيال أكثر دقة وخطورة. ومن أبرز هذه الأساليب:

**أ/ التصيّد الاحتيالي(Phishing)** : يلجئ المجرمون السيبرانيون إلى استخدام رسائل البريد الالكتروني أو مواقع الويب الاحتيالية التي تحاكي الكيانات الموثوقة لخداع الضحايا وإفشاء معلوماتهم الشخصية.[3]

وفي هذا السياق تُستغل أدوات الذكاء الاصطناعي بشكل خبيث لإرسال رسائل بريد إلكتروني مصممة بدقة عالية، مما يجعل من الصعب على الضحايا تمييزها عن الرسائل العادية. ووفقًا لصحيفة **فاينانشيال تايمز**، تعتمد هذه الهجمات على روبوتات ذكية تقوم أولاً بتحليل أنشطة المستخدمين على وسائل التواصل الاجتماعي لاختيار المواضيع التي تثير انتباههم، ثم تُرسل

[1] أحمد محمد براك، مرجع سابق، ص 342_343.

[2] سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، ط1، دار الفكر الجامعي، الإسكندرية، 2017، ص95.

[3] بوكر رشيدة، الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي بين تصاعد التهديدات وفرص تعزيز الأمن السيبراني، مرجع سابق، ص52.

رسائل احتيالية تبدو وكأنها صادرة عن أصدقائهم أو أفراد عائلاتهم، وبسبب الطابع الشخصي للبريد الإلكتروني، يصبح من الصعب على المتلقي التمييز بينه وبين البريد العادي.[1]

**ب/ التزييف العميق(Deepfake)** : هي إحدى تقنيات الذكاء الاصطناعي تقوم على صناعة محتوى مزيّف يتشكّل من صور ومقاطع فيديوهات، يعاد إنتاجها وصياغتها بطرق جديدة يصعب حتى التشكيك في مدى مصداقيتها ومعرفة ما إن كانت حقيقية أو احتيالية.[2] ويعتمد هذا النوع من الهجمات غالبًا على تحليل ملامح الوجه وحركات الجسد باستخدام تقنيات التعرف على الوجه.

وبناءً على ما سبق، فإنه لابدّ من توفّر صور أو مقاطع فيديو موجودة مسبقًا لاستنساخ ملامح الشخص المستهدف في الوقت الفعلي لتنفيذ عملية الاحتيال، غير أن الخبراء يحذرون من أنه مع تطور التكنولوجيا، قد يُستخدم الذكاء الاصطناعي لإنشاء مقاطع فيديو مزيّفة من البداية.[3]

تخيّل أن تتلقى مكالمة فيديو من مديرك في الشركة التي تعمل بها، يطلب منك بشكل عاجل تحويل أموال إلى حساب جديد لضمان إتمام صفقة تجارية حاسمة. يبدو الصوت، وحركات الجسد، والخلفية كلها واقعية تمامًا. ولكن في الحقيقة، هذا ليس مديرك ، بل نسخة مزيفة متقنة صمّمها مجرمون إلكترونيون باستخدام الذكاء الاصطناعي[4] ، من أجل الاحتيال على الأشخاص وسرقة بياناتهم الشخصية. وتزداد الخطورة عندما يتعلق الأمر بالبيانات المالية كما جرى في المثال.

[1] Brooke Katoe , Gmail, Outlook and Apple users urged to watch out for this new email scam: Cybersecurity experts sound alarm, 04-01-2025, https://nypost.com, consulté le 26-04-2025 à 21 :20.

[2] هواري صباح، الحياة الخاصة وتكنولوجيا التزييف العميق، مجلة العلوم القانونية و الاجتماعية، جامعة الجلفة، كلية الحقوق والعلوم السياسية، مجلد 9، عدد 2، جوان 2024، ص627.

[3] Cameron Micallef, The remarkably simple way hackers can access your phone , 09-02-2025 , Disponible sur :https://www.news.com , consulté le 26-04-2025 à 20 :50.

[4] Margaret concannon , AI in Social Engineering: The Next Generation of Cyber Threats , 16-07-2024, Disponible sur :https://www.ntiva.com , consulté le : 26-04-2025 à 22 :20.

وفي ظلّ اعتماد أغلب المؤسسات المالية خاصية الدفع الالكتروني، باتت البيانات المالية للأفراد أكثر عرضة للاختراق، إذ أصبح المحتالون يستغلون أدوات الذكاء الاصطناعي المتطورة لتوليد أصوات مزيفة تجيب على أسئلة الأمان البنكية، ما يمكّنهم من التسلّل إلى الحسابات وسرقة البيانات الحساسة. وقد شهدت معدلات هذا النوع من الاحتيال نمواً ملحوظاً في الآونة الأخيرة، مع تسجيل مبالغ مسروقة تفوق ما كان يتم في عمليات الاحتيال التقليدية.[1]

وبذلك نكون قد استعرضنا أبرز الانتهاكات التي يتعرض لها الحق في الخصوصية بواسطة تطبيقات الذكاء الاصطناعي، والتي تتعدد وتتنوع مخلّفة وراءها عدداً لا متناهياً من الانتهاكات التي يصعب حصرها.

**الفرع الثاني: مخاطر جمع البيانات الشخصية وتداعياتها على الأفراد**

هناك مخاطر كبيرة على حقوق الأفراد وحرياتهم في جمع ومعالجة البيانات الشخصية بواسطة الذكاء الاصطناعي، وهو أمر مختلف تماماً عن المخاطر التي تشكّلها خروقات البيانات التقليدية[2].

**أولا/ بيع البيانات واستغلالها**

مع تطور التكنولوجيا الرقمية، ظهر اقتصاد جديد يقوم أساساً على بيع البيانات الشخصية التي يتمّ جمعها من قبل المواقع والشبكات، وبفضل انخفاض تكلفة التخزين والمعالجة وسهولة جمع البيانات، قامت العديد من الشركات التجارية بإنشاء مواقع لها على الإنترنت تمكّنها من

[1] شيماء عبد المنعم، قوم اطمن على فلوسك.. هاكرز يستخدمون الذكاء الاصطناعي لسرقة مدخراتك، موقع صدى البلد، 17-04-2024، متاح على الرابط:https://www.elbalad.news ، تاريخ الاطلاع:26-04-2025، على الساعة:22:00.

[2] بوكر رشيدة، الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي بين تصاعد التهديدات وفرص تعزيز الأمن السيبراني، مرجع سابق، ص97.

تجميع كمّ هائل من المعلومات الشخصية للمستخدمين. وذلك من خلال تقديم عروض وخدمات خاصّة لهم عبر الإنترنت [1].

تقوم هذه الشركات باستغلالها في تخصيص الإعلانات لكل فئة من المستخدمين. ومع تطور هذه الصناعة، أصبحت هذه الخدمات عبارة عن منصّات غير أخلاقية أشبه بالمنصات الجاسوسية المتخصّصة في مراقبة أدق التفاصيل الخاصة بكل مستخدم؛ حتى تتمكن من تقديم كمية كبيرة من بيانات المستخدمين إلى شركات الدعاية لتحقيق أكبر قدر ممكن من الأرباح.[2]

وفي هذا السياق، أصبحت شركات مثل Facebook وGoogle لا تعمل في المقام الأول في مجال وسائل التواصل الاجتماعي، بل في مجال البيانات. فقد أصبحت البيانات الشخصية هي السلعة الأكثر قيمة في البيئة الرقمية، حيث يتمّ تداولها على نطاق واسع من قبل العديد من الشركات الكبرى.[3]

**ثانيا/ الابتزاز الالكتروني وتشويه سمعة الأفراد**

يمكن أن يتم اعتراض البيانات واختراق الحسابات الشخصية للأفراد من طرف بعض الفضوليين بغرض تهديد أصحابها أو ابتزازهم من خلال الاحتفاظ ببياناتهم الحساسة والتهديد بنشرها أو التشهير بهم عن طريق نشرها بطريقة مسيئة تمس بكرامتهم وسمعتهم.[4]

وتتم عملية الابتزاز عن طريق إجبار الضحايا على القيام بأفعال سيّئة تلحق الضرر بهم أو بالمجتمع ككل. أو أن يجبروهم على دفع مبلغ مالي. وفي هذا الشأن أشار رئيس قسم في المركز الوطني للإحصاء والمعلومات (G2_6) أنّ عمليات الابتزاز في ظلّ انتشار تقنيات الذكاء الاصطناعي تتصف بالتعقيد، نتيجة صعوبة معرفة ماهية الطرف الذي قام بالابتزاز؛

[1] خالد حسن أحمد، مرجع سابق، ص83.

[2] أميرة بدوي نجم، مرجع سابق، ص 75.

[3] خالد مدوي، مستقبل الخصوصية في ظل المعالجة الآلية للمعطيات الشخصية، حوليات جامعة الجزائر1، مجلد38 عدد 3، سبتمبر 2024، ص 46.

[4] خالد مدوي، المرجع نفسه، ص48.

هل هو فرد أم آلة؟ وذلك لقدرة هذه الأخيرة على محاكاة البشر، وهو ما شكّل صعوبة على المؤسسات الأمنية في التعامل مع هذه القضايا.[1]

كما يمكن استخدام البيانات التي تم جمعها وإضافة بعض المعلومات المغلوطة لها ثم إرسالها عبر الوسائط الاجتماعية أمام عامة الناس بغرض تشويه سمعة الفرد وتدميره نفسياً، كعرض صورته في وسائل التواصل الاجتماعي من بين المتشرّدين أو السّارقين. وكمثال على هذا فضيحة Cambridge Analyticak التي أضرّت بشدّة بسمعة Facebook.[2]

وفي هذا الصدد يمكن استعمال تقنية التزييف العميق، أو انتحال شخصية الأفراد وذلك باستخدام البيانات المسروقة، ما يتيح للمجرمين السيبرانيين التصرف بحرية تحت أسماء مستعارة وتشويه سمعة الأفراد.[3]

في هذه الحالة، اقتصر حديثنا على الابتزاز وتشويه السمعة من طرف المجرمين السيبرانيين الذين استغلوا تطبيقات الذكاء الاصطناعي لجمع البيانات الشخصية، دون التطرق إلى قيام كيانات الذكاء الاصطناعي نفسها بهذه الأفعال، باعتبار أن ذلك لم يحدث فعلياً حتى الآن. وتجدر الإشارة إلى أن بعض الدراسات الحديثة تنبّه إلى إمكانية تطور الذكاء الاصطناعي بشكل قد يؤدي إلى ممارسات ضارة، مثل الابتزاز أو تشويه السمعة، بشكل مستقل مستقبلاً.

**ثالثا/ تحيز الخوارزميات**

تشكل قضية التحيز في أنظمة الذكاء الاصطناعي إشكالية كبيرة ترتبط مباشرة بموضوع الخصوصية في الذكاء الاصطناعي. حيث أنّ الخوارزميات تتأثر بجودة البيانات المستخدمة

[1] ابتسام بنت سعيد الشهومية، سالم بن سعيد الكندي، محمد بن ناصر الصقري، تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية: دراسة حالة في سلطنة عمان، مجلة الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، مجلد 15، عدد 3، ديسمبر 2024، ص100_101.

[2] حصة أحمد عبد الله التويم، وفاء أحمد عياض الغامدي، مرجع سابق، ص848.

[3] سعيدى سليمة، حجاز بلال، مرجع سابق، ص94.

في تدريبها،[1] ولهذا قد يؤدي الجمع الغير عقلاني للبيانات الشخصية إلى تحيز في الخوارزميات، نظراً لاستخدام بيانات غير صحيحة أو معيبة أو متحيزة من قبل الأفراد.[2]

وتتجلى هذه التحيزات في عدة مظاهر، مثل التمييز العرقي أو الجنسي في أنظمة التوظيف أو إسناد القروض التي تفضّل فئات معينة على حساب أخرى، أو التحيز اللغوي حيث يتم التعامل بشكل أفضل مع لغات محددة، أو التحيز الاقتصادي عبر تفضيل أشخاص من خلفيات مالية معينة، كما هو الحال في أنظمة الجدارة الائتمانية التي تمنح أفضلية لأصحاب المداخيل المرتفعة، وغيرها.[3]

من الأمثلة البارزة على ذلك، ما حدث مع شركة "أمازون"، التي طورت سنة 2014 خوارزمية لأتمتة عملية التوظيف عبر تقييم السير الذاتية للمترشحين. وبعد فترة قصيرة، لاحظ القائمون على النظام ظهور تحيز ضد النساء في نتائج الاختيار. وعند التحقيق، تبيّن أن السبب يعود إلى نوعية البيانات التي تم تدريب الخوارزمية عليها، حيث كانت تعتمد أساسًا على سير ذاتية لرجال. وبناءً على ذلك، قرّرت الشركة وقف استخدام هذه الأداة في التوظيف.[4]

تجدر الإشارة إلى أن المخاطر التي تناولناها في هذا العنصر تنصبّ على حياة الأفراد وما يتعرضون له من تهديدات مباشرة نتيجة جمع بياناتهم الشخصية، غير أنّ تداعيات هذه الظاهرة قد تتجاوز الإطار الفردي، حيث يمكن استغلال البيانات المسروقة في شنّ هجمات سيبرانية تستهدف مؤسسات الدولة وبناها التحتية الحيوية، مما يشكّل تهديدا للأمن القومي وسيادة الدولة.

---

[1] الخصوصية في الذكاء الاصطناعي: تحديات وحلول عملية لعصرنا الرقمي_ آليات حماية البيانات الشخصية: من التشريعات إلى التقنيات الآمنة، مقال متاح على الرابط:https://aidalil.com ، آخر تحديث في: 12-03-2025، تاريخ الاطلاع: 15-05-2025، على الساعة 10:00.

[2] أحمد محمد براك، مرجع سابق، ص320.

[3] نور الدين الشابي، مرجع سابق، 161.

[4] نور الدين الشابي، المرجع نفسه، ص161.

# الفصل الثاني

## آليات حماية الحق في الخصوصية في عصر الذكاء الاصطناعي

تمهيد:

بعد أن تناولنا في الفصل الأول أبرز التهديدات التي تنصب على الحق في الخصوصية جرّاء الاستخدام المتزايد لأنظمة الذكاء الاصطناعي في شتى المجالات وما ينجم عنها من مخاطر تمسّ الحياة الخاصة للأفراد، كان من الضروري أن ننتقل في هذا الفصل إلى مناقشة سبل الحماية والتصدي لهذه الانتهاكات التي أصبحت تفرض تحديات قانونية وأخلاقية متزايدة تستدعي استجابة شاملة ومتكاملة تجمع بين الحماية القانونية الرادعة، والتدابير التقنية الوقائية، بالإضافة إلى المبادئ الأخلاقية التي تضمن احترام الكرامة وحقوق الإنسان.

ويأتي هذا الفصل استكمالًا لما تمّ طرحه سابقًا، حيث يعالج في مبحثه الأول الآليات القانونية المعتمدة لحماية الحق في الخصوصية في ظل تطور الذكاء الاصطناعي، سواء على الصعيد الدولي أو الإقليمي أو الوطني، من خلال عرض أهم الاتفاقيات والتشريعات ذات الصلة. أما المبحث الثاني فسيخصص لتسليط الضوء على الحماية التقنية، باعتبارها وسيلة عمَلية لمواجهة الاعتداءات الواقعة على هذا الحق، إلى جانب الأطر الأخلاقية ودورها في تعزيز ثقافة احترام الخصوصية أثناء تطوير النظم الذكية واستخدامها، وذلك على النحو التالي:

**المبحث الأول:** الحماية القانونية للحق في الخصوصية في ظل تطور الذكاء الاصطناعي.

**المبحث الثاني:** الحماية التقنية والأخلاقية للحق في الخصوصية في ظل تطور الذكاء الاصطناعي.

## المبحث الأول: الحماية القانونية للحق في الخصوصية في ظل تطور الذكاء الاصطناعي

يُعَدُّ الحق في الخصوصية من أبرز الحقوق الأساسية التي حظيت بعناية خاصة من قبل المواثيق والاتفاقيات الدولية، نظرًا لما يشكّله من دعامة جوهرية لكرامة الفرد وحريته. ويأتي في مقدّمتها الإعلان العالمي لحقوق الإنسان لسنة 1948[1] الذي نصّ في مادته الثانية عشرة على ضرورة حماية الأفراد من كل تدخل تعسفي في حياتهم الخاصة، كما جاء العهد الدولي الخاص بالحقوق المدنية والسياسية ليؤكد في مادته السابعة عشرة على ذات المبدأ[2]، مُكرّسًا بذلك ضمانة دولية صريحة لهذا الحق.

وانطلاقا مماّ سبق، برزت العديد من الآليات الدولية والإقليمية التي عملت على تعزيز حماية الحق في الخصوصية، لا سيما في ظل ما تفرضه تقنيات الذكاء الاصطناعي من تحديات جديدة، وهو ما سنتناوله في المطلب الأول. كما سعت بعض التشريعات الوطنية إلى ترجمة هذه المبادئ ضمن قوانينها الداخلية، نتعرف على أهمّها في المطلب الثاني.

[1] تنص المادة 12 من الإعلان العالمي لحقوق الإنسان على:" لا يجوز تعريض أحد لتدخل تعسّفي في حياته الخاصّة أو في شؤون أسرته أو بيته أو مراسلاته، ولا لحملات تمسّ شرفه وسمعته. ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخّل أو تلك الحملات"، الأمم المتحدة، الإعلان العالمي لحقوق الإنسان، متاح على الرابط التالي: https://www.un.org، تاريخ الإطلاع:03-05-2025، على الساعة: 9:30.

[2] تنص المادة 17 من العهد الدولي للحقوق المدنية والسياسية على:" لا يجوز تعريض أي شخص، على نحو تعسّفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمسّ شرفه أو سمعته. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"، الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، متاح على الرابط التالي:https://www.ohchr.org ، تاريخ الاطلاع: 03-05-2025، على الساعة: 9:45.

## المطلب الأول: الآليات الدولية والإقليمية لحماية الحق في الخصوصية

نظرا للمخاطر العديدة التي تشكلها التقنيات الذكية على خصوصية الأفراد، كرست مجموعة من الآليات ووسائل الحماية التي تقضي بتقليل وتقليص الخطر المحدق بالخصوصية والبيانات الشخصية، تنوّعت بين آليات دولية وأخرى إقليمية.

وبناءً عليه، سيتناول هذا المطلب أهم هذه الآليات، من خلال فرعين اثنين: يُخصَّص الأول للآليات الدولية، ويُعنى الثاني باستعراض الآليات الإقليمية المعتمدة في هذا السياق.

### الفرع الأول: الآليات الدولية

أثار الحق في الخصوصية اهتمام العديد من المنظمات الدولية، مما جعلها تقرّ مجموعة من الآليات القانونية لحماية هذا الحق من الانتهاكات التي قد يتعرّض إليها لا سيما في ظل التحديات الجديدة التي يفرضها العصر الرقمي. وستقتصر دراستنا على أهمها.

**أولا/ منظمة التعاون الاقتصادي والتنمية:**

في ظلّ غياب اتفاقية دولية شاملة نجد أنّ أوّل الجهود الدولية المتخصّصة في مجال حماية البيانات الشخصية تتمثّل في المبادئ التوجيهية بشأن حماية الخصوصية ونقل المعطيات الصادرة عن منظمة التعاون الاقتصادي والتنمية ( OECD) بتاريخ 23 سبتمبر 1980، والتي تضم 29 دولة منها :أمريكا، تركيا وبريطانيا.[1]

وضعت هذه المنظمة قواعد إرشادية من أجل حماية الخصوصية ونقل البيانات، وأوصت الأعضاء بالالتزام بها، والتي تطبق على القطاعين العام والخاص، حيث تشمل البيانات المتعلقة بالأشخاص الطبيعيين سواء كانت معالجة آليًا أو غير معالجة. إلاّ أنّها لا تتمتّع بالقوة الإلزامية ، بل تبقى مجرد إرشادات وتوصيات.[2]

[1] خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والاقتصادية، جامعة سطيف 02، مجلد5، عدد1، جوان 2022، ص1644.

[2] بن قارة مصطفى عائشة، مرجع سابق، ص 43.

وفي 22 تموز/يوليو 2013 اعتمد مجلس منظمة التعاون والتنمية في الميدان الاقتصادي توصية منقّحة بشأن المبادئ التوجيهية الخاصة بحماية الخصوصية وتدفق البيانات عبر الحدود، هذا التنقيح هو الأول منذ الإصدار الأصلي للمبادئ التوجيهية لعام 1980. وقد جاء استجابة لدعوة من الوزراء في إعلان سيول بشأن مستقبل اقتصاد الإنترنت لعام 2008 لتقييمه المبادئ التوجيهية في ضوء "تغير التكنولوجيات والأسواق وسلوك المستعملين والأهمية المتزايدة للهويات الرقمية". تتمثل هذه المبادئ فيما يلي: مبدأ تقييد التحصيل، مبدأ جودة البيانات، مبدأ مواصفات الغرض، استخدام مبدأ التقييد، مبدأ الضمانات الأمنية، مبدأ الانفتاح، مبدأ المشاركة الفردية، مبدأ المساءلة.[1]

ورغم كون التوصيات الصادرة عن منظمة التعاون الاقتصادي والتنمية غير ملزمة تجاه الأعضاء، إلاّ أنها كانت مرجعاً توجيهياً للعديد من التشريعات خصوصاً الدول الأوروبية.[2]

**ثانياً/ منظمة الأمم المتحدة:**

تعتبر الأمم المتحدة جهة فاعلة في تعزيز حقوق الإنسان بما في ذلك الحق في الخصوصية، كما تهتم بالتطورات التكنولوجية وتأثيرها على الإنسانية. وكان لها العديد من القرارات في هذا الشأن والتي أسهمت في ترسيخ حماية هذا الحق على المستوى الدولي، ومن أبرز هذه القرارات ما يلي:

**أ/ قرار الجمعية العامة للأمم المتحدة رقم 68/167:**

في الثامن عشر من كانون الثاني/ديسمبر 2013 أصدرت الجمعية العامّة للأمم المتحدة قرارها بشأن الخصوصية في العصر الرقمي، الذي جاء إزاء القلق الشديد بشأن القدرة المتنامية

[1] بوكر رشيدة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الانسان والحريات العامّة، مجلد 7، عدد2، ديسمبر 2022، ص78-79.

[2] محمد الهادي السهيلي، مرجع سابق، ص26.

للمؤسسات الحكومية على الوصول إلى خصوصيات الأفراد من خلال المراقبة عبر الوسائل التكنولوجية سواء كان الأشخاص المراقبين داخل الدولة أو خارجها.[1]

وأكّدت الجمعية العامة ضمن هذا القرار أن حقوق الأشخاص التي تكون داخل الفضاء الإلكتروني، يجب أن تحظى بنفس الحماية التي تتمتع بها خارجه. كما أهابت بجميع الدول أن تحترم وتحمي الحق في الخصوصية في الاتصالات الرقمية، وأهابت كذلك بجميع الدول أن تعيد النظر في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجمع المعطيات الشخصية مشدّدة على حاجة الدول إلى ضمان تنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان تنفيذا كاملاً وفعّالاً.[2]

وقد كلّفت الجمعية العامة مفوضية الأمم المتحدة السامية لحقوق الإنسان بإعداد تقرير مفصّل يتناول في الدراسة "حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية و/أو اعتراضها وجمع البيانات الشخصية، بما في ذلك على نطاق جماعي"، ولإعداد هذا التقرير فقد اضطلعت المفوضية السامية بأعمال بحث وتشاور مع مختلف الجهات المعنية، بما في ذلك الشركاء داخل منظومة الأمم المتحدة وخارجها، كما شجعت المفوضية جميع الأطراف المهتمة على تبادل المعلومات ووجهات النظر بشأن المسائل المثارة في هذا القرار.[3]

**ب/ تقرير المفوضية السامية لحقوق الإنسان:**

جاء هذا التقرير استجابة مباشرة للقرار رقم 7/34 المعتمد من مجلس حقوق الإنسان في دورته الرابعة والثلاثين بتاريخ23 مارس 2017، والذي دعا إلى توسيع نطاق الخصوصية

[1] خالد حسن أحمد، مرجع سابق، ص 100.

[2] بوكر رشيدة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مرجع سابق، ص81.

[3] محمد الهادي السهيلي، مرجع سابق، ص24.

لتشمل البيانات التي يتم جمعها وتحليلها بمختلف الوسائل التقنية والخوارزميات، مؤكّداً أن مجرّد الاطلاع أو المراقبة السرية للبيانات الشخصية يُعدّ مساسًا بحق الأفراد في الخصوصية.[1]

ومن أبرز مخرجات القرار دعوته إلى عقد ورشة خبراء حول الحق في الخصوصية في العصر الرقمي، وتكليف المفوض السامي لحقوق الإنسان بإعداد تقرير يقدم إلى الدورة التاسعة والثلاثين لمجلس حقوق الإنسان في سبتمبر 2018.[2]

جاء هذا التقرير ليسلّط الضوء على تأثيرات تقنيات الذكاء الاصطناعي على ممارسة الحق في الخصوصية والحقوق المرتبطة به وحقوق الانسان الأخرى، مقدّما توصيات مفادها ضرورة حماية حقوق الانسان عند جمع البيانات الضخمة المتعلقة بالأفراد ومعالجتها ونقلها وحفظها.[3]

كما أوصى بفرض قيود صارمة على استخدام تقنيات التعرف على الوجوه والقياسات الحيوية في الأماكن العامة، لما تمثله من تهديد لخصوصية الأفراد، وحظرها عند تعارضها مع القانون الدولي لحقوق الإنسان. و شدّد على ضرورة أن تخضع عمليات مراقبة البيانات لمبادئ الشرعية والتناسب، وأن تتم ضمن إطار قانوني واضح يضمن حماية الأفراد، كما أولى أهمية كبيرة لأدوات التشفير ووسائل الإخفاء الرقمي للهوية ، كما أكّد على وجوب تحقيق توازن بين حماية الخصوصية ومتطلبات الأمن القومي، دون اتخاذ هذه الأخيرة ذريعة لانتهاك الحقوق الأساسية للأفراد.[4]

**ج/ تقرير المقرر الخاص المعني بالحق في الخصوصية لعام 2021**

ومع أهمية التقارير السابقة، إلاّ أنّ التطوّر الأهم في إطار الحماية الدولية للحق في الخصوصية من مخاطر الذكاء الاصطناعي كان قد تجسّد في تقرير المقرّر الخاص المعني

[1] عبد الله شيباني، وداد بن سالم، مرجع سابق، ص465.

[2] UN resolution affirms surveillance that is not necessary or proportionate is against the right to privacy, 23-03-2017,Disponible sur: https://www.article19.org , consulté le 03-05-2025, à 10 :40.

[3] خالد مدوي، مرجع سابق، ص51.

[4] مفوضية الأمم المتحدة السامية لحقوق الإنسان، تقرير المفوض السامي لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي، الوثيقة رقم A/HRC /39/29، الدورة 39 لمجلس حقوق الإنسان، 3 آب/أغسطس 2018، النسخة العربية متاحة على: https://digitallibrary.un.org/ ، تاريخ الاطلاع: 02-05-2025 على الساعة 10:50.

بالحق في الخصوصية السيّد "جوزيف كاناتاشي" المقدم إلى مجلس حقوق الإنسان في دورته الـ 46 الصادر عام 2021 رقم A/HRC/46/37، تحت عنوان الذكاء الاصطناعي والخصوصية، وخصوصية الأطفال. وقد تضمّن هذا التقرير توصيفات دقيقة لمخاطر الذكاء الاصطناعي على الحق في خصوصية البيانات، واقترح العديد من الحلول والمسؤوليات في هذا الإطار.[1]

كما أعاد التقرير التأكيد على ضرورة التزام أنظمة الذكاء الاصطناعي بمبادئ الشرعية والتناسب والضرورة في جمع البيانات الشخصية واستخدامها، وهي المبادئ التي سبق إبرازها في تقرير المفوض السامي لعام 2018[2]. غير أنّ المقرّر الخاص ذهب أبعد من ذلك من خلال توسيع التحليل ليشمل الحاجة إلى أطر تنظيمية دقيقة تضمن إخضاع هذه الأنظمة لمبادئ الشفافية والمساءلة، لا سيما فيما يتعلّق بخوارزميات التصنيف، وأنظمة اتخاذ القرار التنبؤية. إلى جانب إرساء آليات مستقلة للرصد والمراجعة التقنية والقضائية، بما يضمن حماية الأفراد من الانتهاكات المحتملة الناتجة عن الخوارزميات المنحازة أو غير الخاضعة للمساءلة[3].

هذا بالإضافة إلى المقرر الخاص المعني بالحق في الخصوصية الصادر عن الجمعية العامة للأمم المتحدة لسنة 2022 رقم A/77/196، حيث يشير إلى المبادئ التوجيهية التي تستند إليها الخصوصية وحماية البيانات الشخصية في هذا المقرّر، معتبراً إياها جزءاً هيكلياً من النظم القانونية، كما تشكّل إرشادات للتفسير وتساعد في سدّ الثغرات القانونية، وهي تلزم المتحكمين في البيانات ومعالجي البيانات بالتصرّف على النحو الملائم لدي معالجة البيانات الشخصية باستخدام تكنولوجيا المعلومات والاتصالات.[4]

---

[1] أحمد حسني علي أشقر، مرجع سابق، ص 42.

[2] Privacy International, Soumission au Rapporteur spécial sur le droit à la vie privée concernant, l'intelligence artificielle et la vie privée, disponible sur : https://privacyinternational.org, consulté le 03-05-2025 à 16 :30.

[3] Factly, Le rapport des Nations Unies souligne la nécessité de transparence et de responsabilité dans l'utilisation des systèmes d'IA, 2021, disponible sur : https://factly.in , consulté le 03-05-2025 à 16 :30.

[4] بلباي إكرام، الذكاء الاصطناعي في القانون الدولي–دراسة في المفهوم والأطر والتطبيقات–، ط1، ابن النديم للنشر والتوزيع ومؤسسة الكتاب القانوني، الجزائر، 2024، ص90.

وبهذا نكون قد تطرّقنا إلى أبرز الآليات التي جاءت بها المنظمات الدولية، وفي مقدّمتها منظمة التعاون الاقتصادي والتنمية التي أرست الأسس المرجعية الأولى لوضع الضوابط والمعايير الكفيلة بحماية الخصوصية والبيانات الشخصية. كما تناولنا بالدراسة الدور المحوري الذي اضطلعت به منظمة الأمم المتحدة من خلال جملة من القرارات والتقارير، مركّزين على أبرزها لما تعكسه من التزام واضح بمواجهة التحديات المتنامية التي تفرضها تقنيات الذكاء الاصطناعي على الحق في الخصوصية.

**الفرع الثاني: الآليات الإقليمية**

إلى جانب المنظمات الدولية، سايرت العديد من التكتلات الإقليمية التطورات المتسارعة في مجال تقنية المعلومات، وسعت إلى إيجاد آليات قانونية تكفل حماية الحق في الخصوصية والبيانات الشخصية.

**أ/ المجلس الأوروبي:**

عمد مجلس أوروبا على حماية البيانات الشخصية في مجال المعلوماتية حتى أبرم الاتفاقية رقم 108 عام 1981 بمدينة ستراسبورغ، تهدف لحماية الأفراد في مجال المعالجة الآلية للمعطيات الشخصية ومواجهة الاجرام الالكتروني المتعلق بسرية البيانات الالكترونية، أي بيانات الخصوصية الرقمية، وطلبت من الدول الأعضاء في الاتفاقية مثل كندا، اليابان، جنوب إفريقيا والولايات المتحدة الأمريكية التصدي لهذه الجريمة.[1]

وتعدّ أوّل اتفاقية تحمل الطابع الإلزامي على عكس القواعد الإرشادية لمنظمة التعاون الاقتصادي، والتي كان لها الفضل في صدور هذه الاتفاقية.[2]

تهتم هذه الاتفاقية بمسائل نقل وتبادل المعطيات بين الدول المتعاقدة، حيث تحظر نقل المعلومات إلى خارج الحدود إلّا إلى الدولة التي توفر لها حماية موازية، مع استثناءات من هذه القاعدة. كما أنّ مجلس أوربا من خلال لجنة الخبراء العاملة في حقل حماية المعطيات قد

[1] معزوز دليلة، والي نادية، مرجع سابق، ص 824.

[2] عبد الله شيباني، وداد بن سالم، مرجع سابق، ص464.

أصدر سلسلة من الدلائل التوجيهية المعتمدة على الاتفاقية المذكورة، وهذه الدلائل التوجيهية ليست إلّا توصيات موجّهة إلى حكومات الدول الأعضاء، وتتعلق بما يلي :حماية المعلومات الطبية المؤتمنة، والإحصاءات، وقاعدة المعلومات الخاصة لأغراض التسويق، وقاعدة المعلومات الخاصة لأغراض الضمان الاجتماعي، أو لأغراض البوليس، والبيانات الجنائية، وقواعد المعلومات الخاصة بأغراض التوظيف وكذا خدمات الاتصال.[1]

كما دعا البروتوكول الاختياري الإضافي للاتفاقية المعتمد عام 2001 بشأن السلطات الإشرافية وتدفقات البيانات عبر الحدود، إلى إنشاء هيئات إشرافية لضمان حماية المعطيات واحترام الخصوصية في مشاركة المعطيات. وجاء بروتوكول آخر CETS رقم 223 لسنة 2018 كآخر بروتوكول تعديلي للاتفاقية إلى يومنا هذا، والذي سعى في تحديثها إلى تحقيق هدفين رئيسيين: التعامل مع التحديات الناتجة عن استخدام تقنيات المعلومات والاتصالات الجديدة وتعزيز التنفيذ الفعال للاتفاقية[2].

وينبغي الاعتراف، أن مجلس أوروبا يمتلك اليوم ترسانة قويّة من التوصيات المتعلقة بحماية حقوق الإنسان في البيئة الرقمية وعلى رأسها حماية الحق في الخصوصية. وهذه أهمها:

- توصية لجنة وزراء مجلس أوروبا رقم 6 (2014) حول دليل حقوق الإنسان لمستخدمي الإنترنت.
- توصية اللجنة البرلمانية رقم 2102 (2017) حول التقارب التكنولوجي والذكاء الاصطناعي وحقوق الإنسان.
- توصية لجنة الوزراء رقم 2 (2018) حول دور وسطاء الإنترنت ومسؤولياتهم.
- توصية مفوض حقوق الإنسان لعام 2019 حول الذكاء الاصطناعي.
- توصية مجلس الوزراء رقم 1(2020) بشأن آثار الأنظمة الخوارزمية على حقوق الإنسان.[3]

---

[1] بن قارة مصطفى عائشة، مرجع سابق، ص 44.

[2] بوكر رشيدة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مرجع سابق، ص 80.

[3] ليتيم نادية، مجلس أوروبا والذكاء الاصطناعي: أية ضوابط لحماية حقوق الانسان؟، مجلة التراث، مجلد 13، عدد4، ديسمبر 2023، ص 5-6-7.

**ب/ الاتحاد الأوروبي:**

حرص الاتحاد الأوروبي على مواكبة التطورات التقنية المتسارعة التي أثّرت بشكل مباشر على خصوصية الأفراد وحماية بياناتهم الشخصية، وقد تجلى هذا الحرص في إصداره للائحة العامة لحماية البيانات GDPR، التي أعدّها البرلمان الأوروبي ومجلس الاتحاد الأوروبي بتاريخ 27 أبريل 2016 لتدخل حيّز النفاذ في ماي 2018. حيث جاءت لتحلّ محلّ التوجيه الأوروبي رقم 46/95 EC/الصادر سنة 1995 والمطبق فعليًا منذ عام 1998، وتهدف اللائحة إلى توحيد الأطر القانونية المتعلقة بحماية البيانات الشخصية داخل الدول الأعضاء، بما يضمن تعزيز مبدأ الشفافية لدعم التوازن بين حقوق الأفراد ونموّ الاقتصاد الرقمي.[1]

فقد تمّ اعتماد هذه اللائحة من أجل حماية خصوصية المواطنين الأوروبيين وتحديد كيفية جمع ومعالجة وتخزين المعطيات الشخصية. كما تضمنت مجموعة من الحقوق للأفراد؛ تشمل الحق في الوصول إلى بياناتهم الشخصية، والحق في تصحيحها، وحذفها، ونقلها، بالإضافة إلى مجموعة من الاجراءات والمتطلّبات التي يجب على الشركات والمؤسسات الالتزام بها عند معالجة البيانات الشخصية.[2]

هذا وقد ذهب الاتحاد الأوروبي إلى أبعد من ذلك، عندما توصّل إلى اتفاق على تشريع غير مسبوق لتنظيم الذكاء الاصطناعي، وذلك في بروكسل بتاريخ 08 ديسمبر 2023 بعد مفاوضات مطولة بين الدول الأعضاء والبرلمان الأوروبي، في خطوة وصفها البرلمان بأنّها الأولى من نوعها على مستوى العالم.[3]

---

[1] شافعي أمال، شافعي أم السعد، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوروبي، مجلة الباحث القانوني، جامعة الحاج لخضر– باتنة 1، المجلد 1، العدد 2، مارس 2022 ص112.

[2] جمال فوزي، التحديات الأخلاقية والقانونية للرقمنة والذكاء الاصطناعي_ المملكة المغربية نموذجا_، ضمن عصام عيروط (مشرف)، مرجع سابق، ص356.

[3] ميموني وفاء، عماري نور الدين، الذكاء الاصطناعي بين مطرقة القانون وسندان الابتكار التكنولوجي، المجلة الجزائرية للحقوق والعلوم السياسية، مجلد 09، عدد02، 2024، (بدون صفحة).

وتعود الأشغال التحضيرية لهذا القانون داخل أروقة الاتحاد الأوروبي إلى 21 أبريل 2021، حيث قدّمت المفوضيّة الأوروبية اقتراحها "للائحة تضع قواعد منسّقة بشأن الذكاء الاصطناعي".[1]

وقد تُوّجت هذه الجهود باعتماد قانون الذكاء الاصطناعي رسميًا في يونيو 2024[2]، يهدف إلى ضمان سلامة وحقوق المواطنين والشركات. ويقوم على تصنيف أنظمة الذكاء الاصطناعي استنادًا إلى المخاطر المرتبطة بها، ويُطبّق قواعد محددة لكل فئة، بما يعزز استخدام الذكاء الاصطناعي بشكل قانوني، وأخلاقي في جميع أنحاء الاتحاد الأوروبي[3].

وتُعتبر أنظمة الذكاء الاصطناعي التي تؤثر سلبًا على السلامة أو الحقوق الأساسية ذات مخاطر عالية، وتُقسم إلى فئتين؛ الأنظمة المستخدمة في المنتجات وتخضع لتشريعات سلامة المنتجات في الاتحاد الأوروبي ويشمل ذلك السيارات، الأجهزة الطبية والمصاعد. أمّا الفئة الثانية فتتمثل في الأنظمة التي تندرج ضمن مجالات محددة ويجب تسجيلها في قاعدة بيانات تابعة للاتحاد الأوروبي كإدارة وتشغيل البنية التحتية الحيوية، التعليم والتدريب المهني، التوظيف وإدارة العاملين. ويتم تقييم جميع أنظمة الذكاء الاصطناعي ذات المخاطر العالية قبل طرحها في السوق و طوال دورة حياتها.[4]

وفي سياق حماية البيانات الشخصية، يضع قانون الذكاء الاصطناعي الأوروبي قيودًا صارمة على استخدام تقنيات الذكاء الاصطناعي، حيث يحظر استخدامه في رصد القياسات الحيوية مثل بصمة الوجه والصوت، ويُلزم مستخدمي الأنظمة الذكية بالإفصاح عن المحتوى الناتج عنها، والكشف عن أي مواد محمية بحقوق الملكية الفكرية. كما أنّ هناك مخاطر غير مقبولة

---

[1] رضوان الوهابي، من أجل قانون دولي لأخلاقيات الذكاء الاصطناعي– أضواء على الحراك العالمي لتنظيم أخلاقيات الذكاء الاصطناعي، ضمن: عصام عيروط (مشرف)، ص192.

[2] وسيُصبح قانون الذكاء الاصطناعي قابلًا للتطبيق بالكامل بعد 24 شهرًا من دخوله حيّز التنفيذ، إلا أن بعض أجزائه ستطبّق في وقت أقرب، للمزيد أنظر:

EU AI Act: first regulation on artificial intelligence, Publié : 08-06-2023, Dernière mise à jour : 19-02-2025,Disponible sur : https://www.europarl.europa.eu, consulté le 22-05-2025,à 14 :10.

[3] EU AI Act: How to Create an Effective Data Governance Strategy for Your Organization, Sans date, diponible sur : https://www.informatica.com, consulté le :22-05-2025, à15 :00.

[4] EU AI Act : first regulation on artificial intelligence, Op.cit.

أقرها الاتحاد الأوروبي والتي سيتم حظرها مثل التلاعب السلوكي كالألعاب الرقمية التي تشجع الأطفال على سلوكيات خطيرة.[1]

ويفرض القانون على الأنظمة التي تستخدم الذكاء الاصطناعي التوليدي مثل ChatGPT أو تلك التي تنشئ صوراً يتم التلاعب بها، توفير متطلبات أكبر للشفافية والكشف للناس أن هذا المحتوى النهائي تم إنشاؤه بواسطة الذكاء الاصطناعي. كما يحدّد قيوداً على برامج التعرّف على الوجه من قبل أجهزة إنفاذ القانون والحكومات مع وضع استثناءات ترتبط بالسلامة والأمن القومي. وقد تواجه الشركات التي تنتهك اللوائح الجديدة غرامات تصل إلى 7% من إجمالي مبيعاتها العالمية[2].

كما يقرّر تدابير صارمة لحماية خصوصية الأفراد، بالإضافة إلى وضع إرشادات حول معالجة البيانات بطريقة قانونية وعادلة وشفافة، مع ضرورة دمج اعتبارات الخصوصية في أنظمة الذكاء الاصطناعي منذ مرحلة التصميم الأولى، وهو مبدأ أساسي تم تقديمه من قبل اللائحة العامة لحماية البيانات(GDPR). وفي إطار حوكمة البيانات، ينص القانون على أحكام محدّدة تتعلق بأمن البيانات ومدة الاحتفاظ بها، تهدف إلى حماية البيانات الشخصية من الوصول أو الاستخدام أو الكشف غير المصرّح به، ومنح الأفراد الحق في الوصول إلى بياناتهم وتصحيحها و/أو حذفها[3].

وبناءً على ما سبق، يبدو أن كل من اللائحة العامة لحماية البيانات وقانون الذكاء الاصطناعي يشتركان في عدّة نقاط لاسيما فيما يتعلّق بمبدأ الشفافية والمساءلة، كما أنّ قانون الذكاء الاصطناعي يشير بشكل صريح إلى اللائحة بخصوص معالجة البيانات الشخصية،

[1] بلباي إكرام، مرجع سابق، ص131.

[2] بلباي إكرام، المرجع نفسه، ص94.

[3] The 6 principles of AI and data protection: how the AI act ensures data is safe,Disponible sur : https://www.imprivata.com, consulté le :22-05-2025,à19 :40.

مما يجعل كلا الإطارين التشريعيين غالبًا قابلين للتطبيق في الوقت ذاته، وهذا ما يعكس نهجًا تكامليًا يعزز حماية البيانات الشخصية على مستوى الاتحاد الأوروبي.[1]

**ج/ اتفاقية بودابست للإجرام المعلوماتي:**

أو اتفاقية بودابست بشأن الجريمة السيبرانية، والتي أبرمت في 23-11-2001 من طرف 26 دولة من أعضاء الاتحاد الأوروبي، دخلت حيّز النفاذ في سنة 2006 واعتمدت الاتفاقية تقريرها التفسيري من طرف لجنة وزراء أوروبا في دورته التاسعة بعد المائة، وتعدّ من أهم المعاهدات الدولية التي كافحت الجرائم المعلوماتية المتعلّقة باستعمال الإنترنت ووسائل الاتصال المعلوماتي وكلّ أشكال جرائم الحاسب الآلي وكانت واضحة في مكافحة هذه الجريمة.[2]

وجاء الفصل الثاني من الاتفاقية بعنوان " الإجراءات الواجب اتخاذها على المستوى الإقليمي"، كما ورد في مضمون المادة 02 التي ضبطت قضية الدخول غير القانوني للحواسيب بدون وجه حق، ووضعت الشروط التي تثبت وقوع هذه الجريمة التي تهدّد سلامة وسريّة النظم المعلوماتية للأفراد.[3]

كما نصّت على الاعتراض غير القانوني باستخدام الوسائل الفنية للبيانات المتداولة إلكترونياً بين الحواسيب عبر شبكة الإنترنت، فيما اختصت المادة الرابعة بالنص على ضرورة توحيد أطراف الاتفاقية للجهود بغية تبني الإجراءات التشريعية التي تجرّم الاعتداء على سلامة البيانات من أجل ضمان سلامة المنظومة البيانية للاتصالات الالكترونية.[4]

---

[1] Pour plus d'informations voir : Anthony De Bruyne, AI Act and GDPR: How These Regulations Work Together to Safeguard AI and Privacy, 27/12/2024,Consulté le :22-05-2025,à20 :30.

[2] بلعسل بنت نبي ياسمين، مقدر نبيل، الحق في الخصوصية الرقمية، مجلة المستقبل للدراسات القانونية و السياسية المجلد 5، عدد1، 2021، ص14.

[3] شعلال مختار، الحق في الخصوصية في الفضاء الرقمي وحمايته في القانون الدولي ( حماية خصوصية مستخدمي فيسبوك) _دراسة حالة_، أطروحة مقدّمة لنيل شهادة الدكتوراه، علوم الإعلام والاتصال، كلية العلوم الانسانية والعلوم الإسلامية، جامعة وهران1 أحمد بن بلّة، 2023/2022، ص150_151.

[4] الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والاقتصادية، مجلد1، عدد8، ديسمبر 2017، ص 151.

**د/ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:**

أبرمت الاتفاقية العربية لمكافحة الجرائم المعلوماتية بمصر في 21 ديسمبر 2010، وهي أوّل اتفاقية عربية تبنّتها جامعة الدول العربية لمكافحة جرائم المعلوماتية، وقد سارت على نهج المنظمات العالمية والاقليمية ذات الصلة بموضوع حماية واحترام حق الفرد في خصوصيته وعلى رأسها اتفاقية بودابست، ويتجلى هذا من خلال إقرارها في الفصل الأول بالهدف من الاتفاقية المتمثل في تعزيز التعاون بين الدول العربية في مجال تبادل المعلومات والتقنيات والخبرات الضرورية لمكافحة هذا النوع من الجرائم التي تهدد أمنها وسلامة مجتمعاتها وأفرادها.[1]

ولقد أقرّت الاتفاقية على التزام الأطراف بتجريم شتى أساليب الاعتداء على حقوق الأفراد في المجال الإلكتروني المنصوص عليها في الفصل الثاني منها والمعنون "بالتجريم" والذي ركّزت فيه على تجريم الدخول غير المشروع وكذا الاعتراض غير القانوني للبيانات الشخصية والاعتداء على سلامتها، لتأتي في نص المادة 14 منها وتنص بشكل مباشر على تجريم الاعتداء على الحق في الخصوصية بواسطة تقنية المعلومات[2].

**المطلب الثاني: حماية الحق في الخصوصية في التشريعات الداخلية**

بعد الجهود التشريعية الدولية الهادفة إلى ترسيخ المبادئ الأساسية لمكافحة جرائم تكنولوجيا المعلومات بشكل عام، والآليات المقرّرة لمواجهة الانتهاكات التي تمسّ الخصوصية بشكل خاص، جاء دور التشريعات الداخلية لوضع قواعد قانونية تحمي هذا الحق من مختلف الاعتداءات في البيئة الرقمية.

وفي هذا السياق، سنعالج أولا الحماية القانونية التي أقرّها المشرع الوطني لهذا الحق، ثم ننتقل إلى استعراض بعض نماذج التشريعات المقارنة.

[1] عبد الله شيباني، وداد بن سالم، مرجع سابق، ص465_466.

[2] الدهبي خدوجة، مرجع سابق، ص151.

**الفرع الأول: التشريع الجزائري**

يُعتبر الحق في الخصوصية أحد أهم الحقوق الأساسية المكرسة دستوريًا، وقد حظي باهتمام مبكر من طرف المشرع الجزائري، الذي أقرّ له حماية عبر مختلف الدساتير المتعاقبة، ابتداءً من دستور 1976 ووصولًا إلى التعديل الدستوري لسنة 2020، الذي ينص في المادة 47 منه على أنه: "لكل شخص الحق في حماية حياته الخاصّة وشرفه، ولكل شخص الحق في سريّة مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلاّ بأمر معلّل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي".[1]

يستخلص من نص المادة بأن المشرع الدستوري قد اعترف صراحة بالحق في الخصوصية من خلال التأكيد على صيانة الحياة الخاصة وسرية الاتصالات والمعطيات ذات الطابع الشخصي، غير أنه لم يتولّ تنظيم هذه الحماية بشكل تفصيلي تاركا تنظيم آليات هذه الحماية للتشريعات العادية كقانون العقوبات والقوانين الخاصة.

بداية، عمل المشرّع الجزائري إلى إرساء حماية جنائية للحق في الخصوصية من خلال إدراج عدد من الأحكام ضمن قانون العقوبات عبر تعديلات تشريعية متتالية استجابت للتحولات التقنية والاجتماعية.

ومن أبرز هذه التعديلات نجد؛ القانون رقم 04-15[2] المؤرخ في 10 نوفمبر 2004، والذي عالج فيه لأول مرّة الجرائم الالكترونية بشكل صريح، حيث أفرد له القسم السابع مكرر وسمّاه بالمساس بأنظمة المعالجة الآلية للمعطيات، في المواد من 394 مكرر إلى 394 مكرر7؛ الذي جرّم من خلالها فعل الدخول عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك. كما جرّم حيازة أو إفشاء أو نشر أو استعمال المعطيات

[1] التعديل الدستوري المصادق عليه في استفتاء 01 نوفمبر 2020، بموجب المرسوم الرئاسي رقم20-442، مؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر 2020، ج ر، عدد 82، الصادرة في 30 ديسمبر 2020.

[2] القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المتمم للأمر 66-156 المتضمن قانون العقوبات، ج ر، عدد 71، الصادرة في 10 نوفمبر 2004.

المتحصّل عليها من إحدى الجرائم الماسّة بنظم المعالجة الآلية لأي غرض كان، وهذا ما يمكن اعتباره حماية غير مباشرة للحق في الخصوصية من مخاطر تقنية نظم المعلومات والاتصالات[1].

ثم أصدر الأمر رقم 06-23[2] المؤرخ في 20 ديسمبر 2006، ليجرّم بعض الأفعال الماسّة بخصوصية الأفراد؛ حيث جاء في نص المادة 303 مكرر:

يعاقب بالحبس من 06 أشهر إلى 03 سنوات كل من تعمّد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك:

1_ بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سريّة بغير إذن صاحبها أو رضاه .

1_ بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

ويتبيّن من نص المادة أن المشرع الجزائري يعاقب على انتهاك حرمة المحادثات الشخصية، عن طريق التنصت أو التسجيل أو النقل، وكذا الاعتداء على الحق في الصورة؛ والتي تعد من أهم المظاهر التي يرد عليها الحق في الخصوصية نظراً لقدسيتها وارتباطها المباشر بالفرد بواسطة جهاز من الأجهزة التكنولوجية الحديثة ومن دون أخذ تصريح من الأفراد للقيام بذلك.

كما نصّ في المادة 303 مكرر 1على أنه: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون".[3]

[1] بوكر رشيدة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مرجع سابق، ص90.

[2] القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-156، المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج ر، عدد 84، الصادرة في 24 ديسمبر 2006.

[3] المادة 303 مكرر 1 من قانون العقوبات.

تستهدف الأفعال المجرمة في هذه المادة التسجيلات السمعية والسمعية البصرية، والصور والوثائق، وغيرها من البيانات الشخصية المتحصل عليها جراء احدى الجرائم المنصوص عليها في المادة السابقة (الالتقاط أو التسجيل أو النقل) ويكتمل الركن المادي بإتيان أحد أفعال: الاحتفاظ، أو الوضع أو السماح بوضعها في متناول الجمهور أو الغير، أو الاستخدام بأية وسيلة كانت.[1] وهو بذلك يضع سياجا لحماية خصوصية الأفراد تحسبا للاستخدام السيئ للوسائل التكنولوجية الحديثة عن طريق الكمبيوتر أو الهاتف النقال وما يرتبط بها من تقنيات.

كما أنه لم يكتف بالحماية الجزائية للحق في الخصوصية، بل تعدّى ذلك إلى توفير حماية إجرائية من خلال استحداث إجراءات تحقيق تتفق وطبيعة الجريمة المعلوماتية، فسنّ قانون رقم 09-04 المؤرخ في 05-08-2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[2] وهذا بضمان عدم المساس بالحياة الخاصة للأفراد في حالة قيام السلطات المختصة بعمليات المراقبة لكل الاتصالات الالكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة[3].

ولم يكتف المشرع الجزائري بهذا الحدّ، بل قطع أشواطاً أخرى في اتجاه فرض حماية جنائية على الحياة الخاصة للأفراد عن طريق استحداث قوانين جديدة؛ من بينها القانون رقم 15-04[4] المتعلق بالتوقيع والتصديق الالكترونيين، الذي ألزم بموجبه مؤدي خدمات التصديق الالكتروني بالحفاظ على سرية البيانات، مع اشتراطه الحصول على الموافقة الصريحة للمعني، وحظر استعمالها لأغراض أخرى غير الغرض الذي حدّده القانون، وذلك بموجب المادتين 42 و43 من القانون سابق الذكر.[5]

---

[1] مفيدة مباركية، مرجع سابق، ص476.

[2] بن قارة مصطفى عائشة، مرجع سابق، ص48.

[3] بلعسل بنت نبي ياسمين، مقدر نبيل، مرجع سابق، ص17.

[4] القانون رقم 15_04، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المؤرخ في 01 فبراير 2015، ج ر عدد 06، الصادرة في 10 فبراير 2015.

[5] يحي الشريف نصير، مزغيش عبير، الآليات القانونية المكرّسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري مجلة البحوث في العقود وقانون الأعمال، مجلد7، عدد2، 2022، ص201.

يضاف إليه القانون رقم18-04[1] المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية الذي ألزم بمقتضى المادة 16 منه كل موظفي سلطة الضبط بالسرّ المهني حفاظًا على المراسلات والاتصالات الالكترونية، كما أكّد على ضرورة احترام خصوصية البيانات والمعلومات التي تمّ ايصالها بواسطة شبكات الاتصالات الالكترونية، وكذا شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي، وهذا ما جاء في نص المادة 97 فقرة 2و3.

ليصدر بعد ذلك القانون 18_05[2] المتعلق بالتجارة الالكترونية وخصّ المادة 26 منه التي تلزم المورد الالكتروني بحماية بيانات الزبائن، حيث جاء نص المادة كالآتي:

"ينبغي للمورّد الالكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكّل ملفات الزبائن والزبائن المحتملين، ألاّ يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية. كما يجب عليه الحصول على:

موافقة المستهلكين الإلكترونيين قبل جمع البيانات،

ضمان أمن نظم المعلومات وسرية البيانات،

الالتزام بالأحكام القانونية والتنظيمية المعمول بها في هذا المجال،

يتم تحديد كيفيات تخزين المعطيات ذات الطابع الشخصي وتأمينها وفقا للتشريع والتنظيم المعمول بهما.

وأخيرا أصدر المشرع الجزائري القانون رقم 18-07 ليكون أول قانون خاص يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي حرص بموجبه وتحديداً في المادة 2 منه على أن تتم عملية المعالجة مهما كان مصدرها أو شكلها،

[1] قانون رقم 18_04 ، يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية، المؤرخ في 10 ماي 2018، ج ر، عدد27، الصادرة في 13ماي 2018.

[2] القانون رقم 18_05، المتعلق بالتجارة الالكترونية، المؤرخ في 10ماي 2018، ج ر، عدد 28، الصادرة في 16 ماي 2018.

في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألاّ تمس بحقوق الأشخاص وشرفهم وسمعتهم.[1]

ولتحقيق الهدف المنشود والمتمثل في ضمان حق الأفراد في حماية خصوصيتهم في ظل معالجة البيانات الشخصية، أقرّ المشرّع مجموعة من الأسس والضوابط التي تحكم عملية المعالجة، فضلاً عن إقرار جملة من الحقوق التي يتمتع بها صاحب البيانات من جهة، وفرض بعض الالتزامات التي تقع على عاتق الشخص المسؤول عن المعالجة من جهة أخرى.[2]

وأفرد الفصل الثالث من الباب السادس للأحكام الجزائية، حيث قام بوضع نصوص تجرّم الانتهاكات الماسة بالمعطيات الشخصية أثناء معالجتها، وأقرّ مجموعة من العقوبات على الجهات التي لا تحترم مقتضيات هذا القانون[3].

وسعياً من المشرّع الجزائري على ضمان تطبيق الأحكام القانونية التي تضمنها هذا القانون، تم استحداث سلطة إدارية مهمّتها السهر على تطبيق هذا القانون وسميت بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، تتمثل صلاحياتها في منح الرخص والتراخيص للمسؤولين الراغبين في معالجة هذه المعطيات، والقيام بمهام التحقيق وتسليط العقوبات على كل من يخالف أحكام هذا القانون.[4]

يتضح من خلال ما سبق أن حماية الخصوصية في الجزائر تطوّرت بشكل تدريجي، بدءًا بتعديلات على قانون العقوبات لمواجهة الجرائم المعلوماتية بصفة عامة، ثم سنّ قوانين خاصة في قطاعات حساسة كالاتصالات والتجارة الإلكترونية، مع إدراج أحكام صريحة لحماية

[1] المادة 2، القانون 18_07، مرجع سابق.

[2] خالد مدوي، مرجع سابق، ص 52.

[3] خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والاقتصادية، مجلد 5، عدد1، 2022، ص1642.

[4] معزوز دليلة، حماية المعطيات الشخصية في البيئة الافتراضية في التشريع الجزائري(الواقع والتحديات)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، مجلد 10، عدد1، 2021، ص137.

المعطيات الشخصية، وصولًا إلى إصدار القانون 18-07 الذي كرّس حماية شاملة ومتكاملة للبيانات الشخصية في العصر الرقمي.

**الفرع الثاني: التشريعات المقارنة**

اتجهت مختلف التشريعات المقارنة إلى حماية الحق في الخصوصية في ظل مخاطر التكنولوجيا الرقمية، وعليه سنتطرق أولا للتشريعات الغربية، ثم ننتقل إلى التشريعات العربية.

**أولاً: التشريعات الغربية**

في إطار دراستنا لحماية الحق في الخصوصية ضمن التشريعات الغربية، ارتأينا معالجة نموذجين رائدين، أولهما ينتمي إلى النظام اللاتيني ممثَّلًا في التشريع الفرنسي، وثانيهما إلى النظام الأنجلوساكسوني ممثَّلًا في التشريع الأمريكي. وذلك بهدف إبراز أوجه التباين في معالجة كل نظام لمسألة حماية البيانات الشخصية.

**أ/ التشريع الفرنسي:**

يُعد القانون الفرنسي من بين أوائل التشريعات الأوروبية التي أولت اهتمامًا لحماية البيانات الشخصية، حيث تم إصدار قانون المعلوماتية والحريات بتاريخ /06 /01 /1978 والذي تمّ تعديله عدّة مرات.[1] ويُشرف على تنفيذ مقتضيات هذا القانون هيئة مستقلة تُعرف باللجنة الوطنية للمعلومات والحريات(CNIL) ، والتي تضطلع بدور محوري في حماية حقوق الأفراد وحرياتهم من خلال ضمان احترام قواعد حماية البيانات الشخصية ، وقد توسّعت صلاحيات هذه الهيئة بعد تعديل سنة 2004 بمقتضى القانون رقم 801 ، الذي خوّلها سلطة إصدار تعليمات ومعايير متعلقة بمعالجة البيانات الشخصية، كما أُنيط بها سلطة توجيه الإنذارات للجهات المخالِفة لأحكام القانون، بالإضافة إلى إمكانية توقيع عقوبات مالية على المخالفين.[2]

[1] بن قارة مصطفى عائشة، مرجع سابق، ص46.

[2] ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية دراسة تحليلية مقارنة مجلة روح القوانين، كلية الحقوق جامعة طنطا، العدد 97، يناير 2022، ص117_118.

وآخر تعديل له كان بموجب القانون رقم 2018/493 الصادر في 20 يونيو 2018 المتضمن حماية المعطيات الشخصية، والذي أقرّ جملة من الشروط والضوابط التي يجب اتباعها في مجال معالجة بيانات الأفراد ذات الطابع الشخصي، إضافة إلى مجموعة من المبادئ الخاصة بجمع البيانات وتحليلها لتحقيق الشفافية والنزاهة.[1]

**ب/ التشريع الأمريكي:**

يُعد القانون الفيدرالي الأمريكي الصادر بتاريخ 31 ديسمبر 1974 بموجب القانون رقم 93-579 أول نص تشريعي في الولايات المتحدة يعالج مسألة حماية الخصوصية بشكل مباشر. وهو ينظم جمع ومعالجة واستخدام البيانات الشخصية في القطاع العام فقط، ويشتمل على أهم المبادئ والقواعد الارشادية لمنظمة التعاون واتفاقية مجلس أوروبا بالرغم من صدوره قبلها.[2]

وقد أعقب ذلك صدور عدّة قوانين قطاعية أخرى، نذكر منها قانون خصوصية الاتصالات الالكترونية لعام 1986، قانون حماية خصوصية المستهلك، قانون حماية خصوصية الضمان الاجتماعي، وقانون خصوصية المعطيات والتي صدرت كلها في نفس السنة وذلك عام 1997.[3]

وبعد ذلك صدر قانون باتريوت آكت الأمريكي في أعقاب هجمات 11 سبتمبر 2001، والذي منح السلطات الفيدرالية صلاحيات واسعة في مجال جمع البيانات ومراقبة الاتصالات الإلكترونية، بحكم تعزيز الأمن القومي ومكافحة الإرهاب إلاّ أن هذا القانون تلقى معارضة شديدة خلال السنوات القليلة الماضية، نظرا لما تضمّنه من أحكام جعلت من السهل جمع الملايين من سجلات اتصالات الأمركيين وتوسيع المراقبة الإلكترونية من طرف الحكومة وهذا ما يعد مساساً بخصوصية الأفراد.[4]

---

[1] عبد الله شيباني، وداد بن سالم، مرجع سابق، ص466.

[2] حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها-دراسة مقارنة-، ط1، مكتبة بدران الحقوقية، صيدا(لبنان)، 2017، ص326.

[3] شريف يوسف خاطر، مرجع سابق، ص22_23.

[4] خالد حسن أحمد، مرجع سابق، ص 117.

وهو ما أدّى إلى صدور قانون حرية الولايات المتحدة الأمريكية "USA FREEDOM Act" سنة 2015 والذي جاء بهدف تضييق المراقبة الالكترونية للاتصالات والبيانات الشخصية، ممّا يعزّز حماية الخصوصية الرقمية. وتدعيما لهذا القانون تمّ إصدار قانون إعادة تفويض الحريّة في الولايات المتحدة الأمريكية سنة 2020 والذي يعيد التفويض حتى 01 ديسمبر 2023 ويعدّل الأحكام المتعلقة بقانون مراقبة الاستخبارات الأجنبية، وذلك من خلال اشتراط الإذن القضائي قبل القيام بعمليات المراقبة[1].

ومن خلال ما تمّ عرضه، يتضح بأنّ التشريع الأمريكي لا يعتمد على قانون موّحد شامل لحماية الخصوصية كما هو الحال في التشريع الفرنسي، وإنّما يقوم على قوانين متفرقة تحكم جمع واستخدام المعلومات الشخصية، بحيث أنّ كل قانون يحمل عنوان محدد و يغطي قطاعاً معيناً.[2]

**ثانيا: التشريعات العربية**

سنحاول في هذا العنصر تسليط الضور على أبرز التشريعات العربية التي عنت بحماية الحق في الخصوصية، بحيث سنعالج نماذج من تشريعات دول المغرب العربي في النقطة الأولى، فيما سنخصص النقطة الثانية لدراسة بعض تشريعات دول المشرق العربي.

**أ/ التشريع التونسي والمغربي والمصري.**

تعد تونس من الدول العربية السبّاقة التي بادرت بإصدار قانون خاص بحماية المعطيات الشخصية، المتمثل في القانون الأساسي عدد63 لسنة 2004 المؤرخ في 27 جويلية 2004، والذي نصّ في الفصل الأول منه على أنّ " لكل شخص الحق في حماية المعطيات الشخصية المتعلقة بحياته الخاصة باعتبارها من الحقوق الرئيسية المضمونة بالدستور..."[3]، وبموجب هذا القانون أصبح يحظر جمع البيانات الشخصية إلاّ في أغراض مشروعة ومحدّدة وواضحة

[1] خالد مدوي، مرجع سابق، ص54.

[2] وليد سليم النمر، مرجع سابق، ص450.

[3] بن قارة مصطفى عائشة، مرجع سابق، ص47.

مع اشتراط وجوب أخذ موافقة الشخص المعني بالأمر، وتمّ استحداث الهيئة الوطنية لحماية المعطيات الشخصية التي أنيط لها صلاحية منح تصاريح الحصول على البيانات.[1]

كما اتجه المغرب إلى إصدار القانون 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي في سنة 2009، حيث وضع القانون إجراءات للحفاظ على سرية المعطيات للأشخاص، وأوجب القيام بإجراءات تقنية وتنظيمية ملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف أو الإذاعة، بالإضافة إلى حمايتها من أي شكل من أشكال المعالجة غير المشروعة[2].

ولضمان حسن تطبيق هذا القانون أحدث المشرع المغربي لجنة وطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، مهمتها التحقق من أنّ عملية معالجة المعطيات الشخصية تتم وفق القانون ولا تمس بالحياة الخاصة لأصحابها[3].

أماّ بالنسبة للمشرع المصري، فقد اكتفى لفترة طويلة بتكريس حماية الخصوصية من خلال النصوص الدستورية، لا سيما دستور 2014 الذي أكّد على هذا الحق في مادته الرابعة، بالإضافة إلى تضمينها في عدد من القوانين الخاصة، وعلى رأسها القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.[4]

ونتيجة للانتقادات التي وجّهت للمشرع المصري لعدم وجود تشريع خاص بحماية البيانات الشخصية، تمّ إصدار القانون رقم 151 لسنة 2020 بتاريخ 15 يوليو الذي نص فيه على مجموعة من الالتزامات فيما يتعلق بمعالجة البيانات الشخصية على المتحكم والحائز والمعالج تضمن حماية هذه البيانات في مختلف مراحلها، منذ لحظة الجمع وإلى غاية مرحلة الاستخدام. كما نصّ هذا القانون على إنشاء مركز لحماية البيانات الشخصية، يتبع الوزير المختص

[1] خالد حسن أحمد، مرجع سابق، ص125_126.

[2] ياسر محمد اللمعي، مرجع سابق، ص123.

[3] محمد الهادي السهيلي، مرجع سابق، ص40.

[4] خالد مدوي، مرجع سابق، ص54.

ويهدف إلى تنظيم المعالجة والإتاحة، ومنح التراخيص والتصاريح المتعلقة بحماية البيانات الشخصية.[1]

**ب/ التشريع الإماراتي والسعودي والبحريني:**

تُطَبّق دولة الإمارات مجموعة من القوانين التي تهدف إلى حماية الخصوصية والبيانات الشخصية، من أبرزها القانون الاتحادي رقم (12) لسنة 2016 المتعلق بمكافحة جرائم تقنية المعلومات، والذي يتضمن أحكامًا تجرّم انتهاك البيانات الشخصية عند استخدام وسائل التواصل الاجتماعي.[2] كما أصدرت القانون رقم (4) لسنة 2020 المتعلق بمعالجة تقنية الطائرات بدون طيار، الذي يحرص بموجبه على اتخاذ كل الإجراءات اللازمة، للحفاظ على حُرمة المساكن، وعدم انتهاك خصوصية الأشخاص، وأسرارهم الخاصة والتجارية سواء من خلال التصوير، التسجيل، أو استخدام تقنيات الاستشعار.[3]

ليتمّ بعد ذلك إصدار القانون الاتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية والذي دخل حيز التنفيذ في يناير 2022، حيث يضع هذا القانون الأسس القانونية لحماية البيانات الشخصية للمواطنين والمقيمين والشركات العاملة في الدولة، ويهدف إلى حماية حقوق الأفراد فيما يتعلق بجمع ومعالجة وتخزين البيانات الشخصية.[4]

وبالنسبة للمشرّع السعودي فقد أصدر قانون مكافحة الجرائم المعلوماتية لسنة 2007 الذي تضمن جملة من المواد تتعلق بحماية البيانات الشخصية المعالجة آلياً[5]، فيما تمّ إقرار نظام لحماية البيانات الشخصية عام 2021 بموجب المرسوم الملكي م/19 بتاريخ 1443/02/09هـ (الموافق 16 سبتمبر 2021)، ويهدف إلى حماية البيانات الشخصية

[1] ياسر محمد اللمعي، مرجع سابق، ص111_112.

[2] خالد حسن أحمد، مرجع سابق، ص130.

[3] محمد بن راشد يصدر قانون تنظيم الطائرات بدون طيار في دبي، مقال منشور من طرف: دبي – الإمارات اليوم، بتاريخ 05-07-2020، متاح على الموقع: www.emaratalyoum.com، تاريخ الإطلاع:08-05-2025،الساعة15:45.

[4] حماية البيانات الشخصية في الامارات، مقال منشور من طرف: الصَفَر ومشاركوه، بتاريخ 27-05-2024، متاح على الموقع: https://ae.linkedin.com، تاريخ الاطلاع: 08-05-2025، الساعة 16:35.

[5] بلعسل بنت نبي ياسمين، مقدر نبيل، مرجع سابق، ص18.

لمقيمي المملكة العربية السعودية فيما يتعلق بجمع هذه البيانات ومعالجتها سواء داخل المملكة أو خارجها.[1]

وفي 27 مارس 2023 الموافق ل 1444/9/5هـ خضع هذا النظام لتعديلات جوهرية بموجب المرسوم الملكي رقم م/148، من أجل تعزيز أحكامه وتحديثها بما ينسجم مع المعايير الدولية في مجال حماية البيانات.[2]

ويشرف على تنفيذ نظام حماية البيانات الشخصية هيئة حكومية تعرف "بالهيئة السعودية للبيانات والذكاء الاصطناعي" (سدايا)، التي أنشئت بأمر ملكي في 30 أغسطس 2019، تعمل على تطوير أنظمتها السياسية للبيانات، من خلال حماية حرية البيانات وخصوصيتها وتصنيفها وتبادلها.[3]

أمّا عن المشرّع الأردني، فقام بإصدار قانون حماية البيانات الشخصية رقم 24 لسنه 2023 بتاريخ 17 سبتمبر 2023، ليدخل حيّز التنفيذ في 17 مارس 2024. يهدف هذا القانون إلى تعزيز الخصوصية والثقة الرقمية، وحماية البيانات، من خلال تنظيم ومعالجة البيانات الشخصية، وضمان حقوق الأفراد في الوصول إلى بياناتهم، وتصحيحها، وحذفها والاعتراض على استخدامها، بما ينسجم مع الحقوق الدستورية ويوازن بين حماية الأفراد ومتطلبات المعالجة في البيئة الرقمية.[4]

[1]Quinn Emanuel Urquhart & Sullivan, LLP, Recent Amendments to the Saudi Arabia Personal Data Protection Law, sans date, disponible sur : www.quinnemanuel.com, consulté le : 8 mai 2025 à 20:15

[2] Natasha G. Kohne, Sahar Abas, Mazen Baddar , Kingdom of Saudi Arabia Approves Amendments to Personal Data Protection Law and Confirms September 2023 Effective Date , 26-04-2023, disponible sur : **https://www.akingump.com** , consulté le : 08-05-2025, à21 :45.

[3]محمد الهادي السهيلي، مرجع سابق، ص34.

[4]لينا رياض الرمحي، الحماية القانونية للبيانات الشخصية في المعاملات الالكترونية في ظل التشريع الأردني والتشريع الأوروبي GDPR دراسة مقارنة، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، المجلة العربية للنشر العلمي، الإصدار الثامن، العدد السابع والسبعون، جامعة عمان العربية – كلية القانون، 02 مارس 2025، ص 427.

وخلاصة لما سبق، يتضح بأن معظم التشريعات أدركت حجم التحديات التي تفرضها التكنولوجيات الرقمية على خصوصية الأفراد، فسارعت إلى سنّ قوانين خاصة بحماية البيانات الشخصية في محاولة لمواكبة الركب التكنولوجي.

لكن يبقى التساؤل مطروحًا: هل الآليات القانونية وحدها كفيلة لحماية البيانات الشخصية في ظل تنامي قدرات الذكاء الاصطناعي وشهيّته اللامحدودة لجمع البيانات ومعالجتها؟

من الواضح أنه، ورغم أهمية ما تمّ تكريسه من قواعد قانونية، دوليًا ووطنيًا، لضمان حماية الخصوصية، إلا أنّ هذه الآليات تبقى غير كافية أمام تعقيد الوسائل التقنية المستخدمة في جمع البيانات وتحليلها، مما يجعل من الضروري استكمالها بآليات تقنية متطورة، إضافة إلى اعتماد قواعد أخلاقية صارمة تنظم استخدام الذكاء الاصطناعي.

وهو ما سنحاول معالجته في المبحث الثاني المعنون بـ :**الحماية التقنية والأخلاقية للحق في الخصوصية في ظل تطور الذكاء الاصطناعي.**

## المبحث الثاني: الحماية التقنية والأخلاقية للحق في الخصوصية في ظل تطور الذكاء الاصطناعي

في ظل تسارع التطورات التكنولوجية واتساع نطاق استخدام الذكاء الاصطناعي في شتى مجالات الحياة، باتت البيانات الشخصية عرضة لانتهاكات متزايدة ومعقّدة، يصعب مواجهتها بالآليات القانونية وحدها.

فمع تنامي قدرة الأنظمة الذكية على جمع وتحليل كميات هائلة من المعلومات، أصبح من الضروري استحضار وسائل حماية مكمّلة، تتمثل في الحماية التقنية التي تعزز أمن البيانات على مستوى الأنظمة والأدوات، إضافة إلى وضع قواعد أخلاقية تضبط سلوك مطوري ومستخدمي تقنيات الذكاء الاصطناعي.

وسنحاول من خلال هذا المبحث الوقوف على أهم الوسائل التقنية التي تضمن حماية للبيانات الشخصية، ثم ننتقل إلى مناقشة الجوانب الأخلاقية الضرورية لبناء بيئة رقمية مسؤولة تحترم خصوصية الأفراد وحقوقهم الأساسية.

### المطلب الأول: الأطر التقنية لحماية البيانات الشخصية

نظرًا إلى الكم الهائل من البيانات التي يعتمد عليها الذكاء الاصطناعي وتداعيته الخطيرة على خصوصية الأفراد، وجب اتخاذ تدابير أمان قوية لحمايتها من أي انتهاك أو استخدام غير مشروع. وتحقيقًا لهذه الغاية، يمكن الاستعانة بعدد من التقنيات التي رأينا تصنيفها على النحو التالي:

#### الفرع الأول: التقنيات التقليدية

شكّلت التقنيات التقليدية نقطة الانطلاق في مجال أمن البيانات منذ سنين، أي أنها تعود إلى ما قبل ظهور الذكاء الاصطناعي. حيث كانت تستخدم لمواجهة مختلف التهديدات التي قد تتعرض لها البيانات والنظام المعلوماتي بصفة عامّة. لهذا رأينا أنه لابدّ من الوقوف عند أبرزها:

**أولا: التشفير**

يعتبر التشفير وحدة البناء الأساسية في أمن البيانات، وهو أبسط الطرق وأهمها التي تستخدم لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض غير مشروعة.[1]

ويعرّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة بحيث تبدو غير ذات معنى، وذلك لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة،[2] وذلك عن طريق استخدام عمليات رياضية معقدة، تقوم بتحويل البيانات النصية الواضحة (Plaintext) إلى بيانات مشفرة(Ciphertext) ، لتبدو وكأنها رموز غير مفهومة لأي شخص لا يمتلك المفتاح الصحيح لفكها.[3]

وبالنسبة للتعريف القانوني؛ لم يعرّف المشرع الجزائري صراحة تقنية التشفير إلاّ أنه أشار من خلال نص المادة الثانية في الفقرتين 8و9 من القانون 15_04 المتعلق بالتوقيع والتصديق الإلكترونيين إلى مفتاحي التشفير العمومي والخاص[4]، في حين أنّ المشرع التونسي قام بتعريفه في المادة 3/5 بأنه: استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها.[5]

---

[1] أميرة بدوى نجم، مرجع سابق، ص81.

[2] حسين محمد الغول، مرجع سابق، ص91_92.

[3] Petar Radanliev, Omar Santos, Ethics and Responsible AI Deployment, Sans date, Cisco Systems, RTP, Caroline du Nord, États-Unis ; University of Oxford, P03.

[4] مفتاح التشفير الخاص: هو عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقّع فقط، وتستخدم لإنشاء التوقيع الالكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي. مفتاح التشفير العمومي: هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الالكتروني، القانون 15_04، مرجع سابق.

[5] حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية – قراءة في أحكام المرسوم الرئاسي 05_20 مجلة الحقوق والعلوم الإنسانية، جامعة بومرداس، المجلد 13، العدد3، أكتوبر 2020، ص175_176.

كما تعرفه اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري في المادة الأولى من الفقرة التاسعة بأنه منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونياً بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة[1].

ولتوضيح الصورة أكثر نورد المثال التالي:

فلنفرض أنه لديك رقم مثل 779900، وتريد تشفيره وفق خوارزمية MD5(أحد أشهر خوارزميات التشفير) فستحصل على هذا النص:

284692BA1391AF100984722BD1FFADD0

هذا يعني أنّه لا يمكن لأحد غيرك معرفة النص الأصلي، لأنّ النص المشفر غير قابل للقراءة والفهم وهو مولّد عن طريق خوارزميات معقدة لا يمكن كسرها أو فك شفرتها.[2]

أما من حيث طرق التشفير، يمكن تقسيمه إلى نوعين رئيسيين هما:

**التشفير المتماثل:** يستخدم فيه مفتاح شفرة واحد لكل من عمليتي التشفير وفك الشفرة.[3] ويعتمد مفهوم التشفير المتماثل على معيار DES (Data Encryption Standard) ، لكنه واجه ثغرة كبيرة سببها تبادل المفتاح السري دون أمان، مما أدى إلى تراجع استخدام هذا النوع من التشفير ليصبح شيئًا من الماضي.[4]

**التشفير غير المتماثل:** يستخدم زوجًا من المفاتيح: مفتاح عام ومفتاح خاص. المفتاح العام يمكن مشاركته مع أي شخص، بينما يبقى المفتاح الخاص سريًا. يتم استخدام المفتاح العام

[1] حسين محمد الغول، مرجع سابق، ص92.

[2] محمد هاني صباغ، دليل الأمان الرقمي تعرّف على مفهوم الأمان والخصوصية وكيفية حماية نفسك في العالم الرقمي، ط 1، أكاديمية حسوب، بدون بلد النشر، 2021، ص22.

[3] محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط 1، دار الحامد للنشر والتوزيع، الأردن–عمان، 2007، ص118.

[4] حسين محمد الغول، مرجع سابق، 93.

لتشفير البيانات، ويمكن فقط للمستقبل الذي يمتلك المفتاح الخاص فك تشفيرها. يوفر هذا النوع من التشفير مستوى عالٍ من الأمان، لكنه قد يكون أبطأ مقارنة بالتشفير المتماثل[1].

**ثانيا: الجدار الناري**

هو برنامج أمني يمكن أن يكون على هيئة جهاز متكامل أو برنامج يتم تحميله في الحاسب الآلي بمواصفات جيدة. تتمثل وظيفته في حماية شبكة الحاسب الآلي الداخلية وشبكة الإنترنت، من خلال مراقبة كل البيانات الداخلية والخارجية من الشبكة، والتأكد من مطابقتها لشروط المستخدم التي يحددها للبرنامج مسبقا.[2] وتستفيد الخوادم بصورة كبيرة من الجدران النارية، فهي أحد الدعامات الأساسية في حمايتها من المتطفلين والمخترقين، وتمنعهم من الوصول إلى الخدمات الحسّاسة التي يجب ألاّ يصل إليها أحد من خارج الخادم نفسه.[3]

**ثالثا: المصادقة الثنائية**

يوفر تنفيذ المصادقة الثنائية طبقة إضافية من الأمان للحسابات عبر الإنترنت. فهو يتطلب من المستخدمين تقديم نموذجين مختلفين للتحقق من الوصول إلى حساباتهم، مما يقلل من مخاطر الوصول غير المصرح به حتى لو تم اختراق كلمة المرور.[4]

وتكمن أهميّة المصادقة الثنائية أنّه عند تسجيل الدخول مرّة أخرى لإحدى مواقع الحسابات المختلفة ينبغي أن يتم تسجيل الدخول بشكل اعتيادي مع إدخال رمز المصادقة الثنائية، والذي

---

[1] التشفير وكسر التشفير وما هي الطرق المهمة والتعريفات عن أنواع التشفير، بدون تاريخ النشر، مقال منشور على: https://sumer-link.com، تاريخ الاطلاع: 14-05-2025، على الساعة 21:30.

[2] طارق إبراهيم الدسوقي عطيه، الأمن المعلوماتي -النظام القانوني لحماية المعلومات-، د ط، دار الجامعة الجديدة للنشر الإسكندرية، 2009، ص584_585.

[3] محمد هاني صباغ، مرجع سابق، ص27.

[4] الأمن السيبراني: حماية بيانات المستخدم عبر الإنترنت،28-06-2023، مقال متاح على الرابط التالي:= = https://www.databridgemarketresearch.com ، تاريخ الإطلاع:15-05-2025، على الساعة 20:15.

يتم تلقّيه عبر الهاتف الشخصي للمستخدم، وعادةً ما يتم طلبه عند كل تسجيل دخول جديد للتحقق من هوية المستخدم صاحب الحساب.[1]

**رابعاً: النسخ الاحتياطي:Back-up**

هو عملية نسخ الملفات إلى وسيط خارجي لحمايتها من الفقدان في حال تعرّضت النسخة الأصلية إلى التلف لأي سبب من الأسباب. فيمكنك مثلا نسخ صورك وملفاتك المهمّة من هاتفك المحمول إلى مكان آخر (خدمة مزامنة سحابية مثلا) لتتمكّن من استرجاعها لاحقا.[2]

ويعتبر النسخ الاحتياطي إجراءً احترازيًا إضافيًا، فلو كان نظام تأمين الحاسبات كفؤاً مع مراعاة طرق الحماية المذكورة أعلاه، لما كان هناك داع له. إلا أن احتمالية تلف البيانات أو ضياع الملفات نتيجة لأي خلل تقني أو هجوم إلكتروني، تظهر الحاجة إلى النسخ الاحتياطي.[3]

**خامساً: استخدام كلمات مرور قويّة:**

تعدّ كلمة المرور القوية جدار الحماية الأول ضد معظم الهجمات ومحاولات الاختراق للحسابات الشخصية، وحتى تكون كذلك يجب أن تتضمن مزيجًا من الأحرف الكبيرة والصغيرة، الأرقام، والرموز الخاصة، ومن الأفضل تجنب استخدام كلمات المرور البسيطة أو تلك التي تعتمد على معلومات شخصية يمكن الوصول إليها بسهولة، مثل تاريخ الميلاد أو الاسم الكامل، وهكذا تضمن عدم إمكانية تخمينها.[4]

كما ينصح باستخدام برامج إدارة كلمات المرور للحفاظ على أمان كلمات المرور الخاصة بجميع الحسابات، حيث يمكن باستخدام هذه البرامج إنشاء كلمات مرور قوية، وإدخال البيانات تلقائياً، والتذكير بتحديث كلمات المرور بشكل دوري.[5]

---

[1] أميرة بدوى نجم، مرجع سابق، ص82.

[2] محمد هاني صباغ، مرجع سابق، ص22.

[3] محمد دباس الحميد، ماركو إبراهيم نينو، مرجع سابق، ص113.

[4] 5 خطوات لتعزيز أمان بياناتك الشخصية على تطبيقات السوشيال، 19-09-2024،متاح على الرابط التالي: https://www.youm7.com، تاريخ الاطلاع: 15-05-2025، على الساعة 21:50.

[5] أميرة بدوى نجم، مرجع سابق، ص83.

**سادساً: استخدام برامج مكافحة الفيروسات والبرامج الضارة**

تعتبر برامج مكافحة الفيروسات خط الدفاع الثاني ضد البرمجيات الخبيثة، حيث تعمل هذه الأدوات على كشف وإزالة الفيروسات والبرامج الضارة التي قد تتسلل إلى أجهزتك، لذلك يجب التأكد من تثبيت برامج موثوقة وتحديثها دوريًا لضمان فعاليتها في التصدي للتهديدات المحتملة[1].

**الفرع الثاني: التقنيات الحديثة لحماية الخصوصية**

مع تطوّر أنظمة الذكاء الاصطناعي وتزايد التهديدات المرتبطة باستخدامه، كان لابدّ من إيجاد تقنيات متقدمة تهدف إلى تعزيز حماية البيانات الشخصية بشكل يتماشى مع تعقيدات العصر الرقمي، نتعرف على أهمها:

**أولا:الخصوصية التفاضلية(Differential Privacy)**

الخصوصية التفاضلية هي مفهوم رياضي يسمح بتحليل مجموعات بيانات مجمعة مع حماية خصوصية الأطراف المعنية، بحيث لا تؤثر إضافة أو حذف أي عنصر من عناصر البيانات على النتائج الإجمالية لأي تحليل أو دراسة بشكل ملحوظ. ويتحقق ذلك عن طريق إضافة "ضوضاء (noise) "إلى البيانات أو إلى الاستعلامات التي تُجرى عليها، مما يجعل تعقّب الأفراد أمرًا صعبًا أو مستحيلًا. وتُستخدم هذه التقنية في تحليلات البيانات مع الحفاظ على خصوصية المستخدم، وتدريب نماذج التعلم الآلي[2].

تقنيات الخصوصية التفاضلية تحسن من تحليل البيانات الحساسة، ولهذا فهي تستخدم بكثرة في المجالات التالية:

- الرعاية الصحية: تسمح الخصوصية التفاضلية بتحليل سجلات المرضى وتقييم فعالية الأدوية مع ضمان سرية المريض. بالإضافة إلى ذلك، يستخدمها الباحثون عند تدريب

[1] دليل شامل عن: اهمية الامن السيبراني وحماية الاتصالات، منصة برق، متاح على الرابط التالي: https://br2seo.com، تاريخ الاطلاع: 15-05-2025، على الساعة 20:40.

[2] Petar Radanliev , Omar Santos, op,cit.

نماذج الذكاء الاصطناعي على الصور الطبية، مما يمكّن النماذج من التعلم دون كشف المعلومات الصحية الخاصة بالأفراد.

- المالية: تستخدم المؤسسات المالية الخصوصية التفاضلية في كشف الاحتيال ومشاركة البيانات بأمان، مستخلصة رؤى من بيانات المعاملات دون الكشف عن التفاصيل المالية الفردية.
- التكنولوجيا: تجمع شركات التكنولوجيا بيانات سلوك المستخدمين، مثل تفضيلات الرموز التعبيرية وعادات التصفح، لتحسين المنتجات والخدمات.
- الحكومة: تستخدم وكالات مثل مكتب تعداد الولايات المتحدة الخصوصية التفاضلية لحماية سرية بيانات التعداد أثناء نشر المعلومات الديموغرافية للاستخدام العام[1].

**ثانيا:الحوسبة الآمنة متعددة الأطراف(Secure Multi-Party Computation - SMPC)**

تمكّن الحوسبة الآمنة متعددة الأطراف –عدة أطراف من تنفيذ عمليات حسابية بشكل مشترك على بياناتهم المجمعة دون الكشف عن المدخلات الفردية لكل طرف. ويتم ذلك من خلال بروتوكولات تشفيرية تضمن خصوصية البيانات مع السماح في الوقت نفسه بالحصول على النتيجة المطلوبة[2].

**ثالثا:التعلم الفيدرالي:(Federated Learning)**

تعدّ هذه التقنية ثورة في مجال التعلم الآلي، حيث تسمح بتدريب النماذج على أجهزة المستخدمين مباشرة دون نقل البيانات الأصلية إلى خوادم مركزية. تتعلم الخوارزمية من تحديثات النموذج المحلية، مما يقلل مخاطر تسرب البيانات الحساسة ويعزز الخصوصية في

[1]Marko Aleksic, What Is Differential Privacy in AI?,25-03-2025, Disponible sur : https://phoenixnap.com, consulté le :15-05-2025,à14 :30.
[2] Privacy-Preserving AI: Techniques & Frameworks, 23-05-2024, Disponible sur : https://dialzara.com, consulté le :15-05-2025, à10 :00.

مواجهة أنظمة الذكاء الاصطناعي[1]. ويُعد التعلم الفيدرالي مفيدًا بشكل خاص في الحالات التي تكون فيها البيانات موزعة بطبيعتها، مثل الأجهزة المحمولة أو شبكات إنترنت الأشياء[2].

**رابعًا: التشفير التجانسي_(Homomorphic Encryption)**

هذا النوع من التشفير مختلف تماما عن النوعين السابقين، حيث يسمح بإجراء العمليات الحسابية على البيانات وهي مشفّرة، وبالتالي يكون الناتج النهائي مشفّرًا أيضًا، وعند فك تشفيره يعطي نفس نتيجة العمليات التي لو أُجريت على البيانات الأصلية غير المشفّرة. لذا يمكن تدريب النماذج الذكية على بيانات مشفّرة دون الحاجة لرؤية البيانات الفعلية، أي أن النموذج يتعلّم من أنماط البيانات دون فك تشفيرها، مما يضمن بقاء البيانات الحساسة محمية وآمنة طوال عملية التدريب[3].

**خامسًا: المصادقة والتحكم في الوصول**

المصادقة البيومترية: تعمل أنظمة القياسات الحيوية التي تعمل بالذكاء الاصطناعي على تعزيز مصادقة المستخدم من خلال التحقق من السمات الجسدية أو السلوكية الفريدة.

كما تقوم الأنظمة الذكية بتحليل أنماط سلوك المستخدم لتحديد الحالات الشاذة، والوصول غير المصرّح به المحتمل، ممّا يعزز تدابير مراقبة الوصول.[4]

ومما سبق يتبين أن تقنيات حماية البيانات تلعب دورًا أساسيًا في الحفاظ على خصوصية الأفراد وحماية معلوماتهم الشخصية، إلاّ أنها تشهد بعض النقائص مما يجعلها أقلّ فعالية أمام التقنيات الذكية التي أصبحت قادرة على استخراج البيانات وإعادة تعريف الهوية. لذلك، تظهر

[1] الخصوصية في الذكاء الاصطناعي: تحديات وحلول عملية لعصرنا الرقمي_ آليات حماية البيانات الشخصية: من التشريعات إلى التقنيات الآمنة، مرجع سابق.

[2] Privacy-Preserving AI: Techniques & Frameworks, op.cit.

[3] 6 Ways to Preserve Privacy in Artificial Intelligence,18-12-2023, Disponible sur : https://privacera.com, Consulté le :15-05-2025,à15 :10.

[4] بوكر رشيدة، الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي_بين تصاعد التهديدات وفرص تعزيز الأمن السيبراني_= =مرجع سابق، ص110.

الحاجة الملحّة إلى تطوير مستمر لهذه التقنيات لمواكبة التحديات الجديدة وضمان حماية موثوقة لبيانات الأفراد.

## المطلب الثاني: الأطر الأخلاقية المنظمة لاستخدام الذكاء الاصطناعي

أمام عدم كفاية آليات حماية الخصوصية سواء القانونية أو التقنية التي أظهرت أنّها وسائل كلاسيكية وضعيفة الأداء والفعالية في مواجهة الخوارزميات الذكيّة، الأمر الذي جعل معادلة حماية الخصوصية غير متكافئة، برزت الحاجة إلى ضرورة وضع الأنظمة الذكية ضمن إطار أخلاقي يوجّه عملها ويقنّنه بما يتماشى مع احترام حقوق الإنسان.[1]

لذلك اتجهت العديد من المنظمات الدولية والإقليمية و كذا المؤسسات البحثية إلى صياغة مجموعة من المبادئ والإرشادات التي يمكن عن طريقها مواجهة هذه التحديات والمعضلات الأخلاقية، لضمان تطوير أنظمة ذكاء اصطناعي موثوقة وآمنة.[2]

### الفرع الأول: الأطر الأخلاقية الدولية

اتجهت أغلب المنظمات الدولية إلى دراسة ومعالجة المشاكل الأخلاقية الناجمة عن التقدّم الهائل في مجال الذكاء الاصطناعي من خلال وضع أطر توجيهية تضمن تطويراً مسؤولاً وآمناً لهذه التقنيات الذكية، ولعلّ أبرزها تلك التي أطلقتها منظمة التعاون الاقتصادي والتنمية، واليونسكو، والأمم المتحدة.

#### أولاً: مبادئ منظمة التعاون والتنمية الاقتصادية بشأن الذكاء الاصطناعي

أنشأت لجنة سياسات الاقتصاد الرقمي التابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) في ماي 2018 فريقاً من الخبراء يُعنى بالذكاء الاصطناعي في المجتمعات. وكان الهدف من إنشائه استحداث مبادئ للسياسات العامة والتعاون الدولي تعزّز الثقة في استخدام تكنولوجيا الذكاء الاصطناعي وتشجّع على اعتمادها، لتصبح هذه المبادئ

[1] مريم ساغي، مليكة مذكور، مرجع سابق، ص537-538.

[2] نرمين عبد القادر إمبابي، مرجع سابق، ص25.

في النهاية الأساس الذي استندت إليه توصية المجلس المتعلّقة بالذكاء الاصطناعي التي أصدرتها المنظمة.[1]

وقد تمّ اعتمادها في 22 ماي 2019، لتكون أول وثيقة معيارية دولية حكومية بشأن الذكاء الاصطناعي، وتلتزم بمبادئها أكثر من 46 دولة فضلاً عن الاتحاد الأوروبي. وقد وضعت هذه المبادئ من أجل توجيه الجهات الفاعلة في مجال الذكاء الاصطناعي في جهودها الرامية إلى تطويره ليكون جديراً بالثقة، كما ترمي إلى تزويد واضعي السياسات بتوصيات لجعل سياسات الذكاء الاصطناعي فعّالة.[2] وسنعالج هذه المبادئ وكذا السياسات فيما يلي:

**أ/ مبادئ الإدارة المسؤولة للذكاء الاصطناعي الجدير بالثقة:**

تحدد التوصية خمسة مبادئ متكاملة تستند إلى القيم من أجل الإدارة المسؤولة للذكاء الاصطناعي الجدير بالثقة، وتدعو الأطراف الفاعلة في مجال الذكاء الاصطناعي إلى الترويج لهذه المبادئ وتنفيذها:[3]

**1/ النموّ الشامل والتنمية المستدامة والرفاهية**

يجب على أصحاب المصلحة أن ينخرطوا بشكل استباقي في الإدارة المسؤولة للذكاء الاصطناعي الجدير بالثقة سعيًا إلى تحقيق نتائج مفيدة للشعوب ولكوكب الأرض مثل زيادة القدرات البشرية وتعزيز الإبداع والنهوض بدمج الشعوب الغير الممثلة تمثيلاً وافياً والحد من أوجه عدم المساواة الاقتصادية والاجتماعية وحماية البيئات الطبيعية ومن ثم تفعيل النمو الشامل والتنمية المستدامة والرفاهية.

[1] الاتحاد الدولي للاتصالات، الاتجاهات التكنولوجية الناشئة: الذكاء الاصطناعي والبيانات الضخمة لأغراض التنمية جنيف، 2021، ص73.

[2] رضوان الوهابي، مرجع سابق، ص189.

[3] بلباي إكرام، مرجع سابق، ص96.

**2/ القيم المتمحورة حول حقوق الإنسان، والإنصاف:**

يجب على الأطراف الفاعلة في الذكاء الاصطناعي احترام سيادة القانون وحقوق الإنسان والقيم الديموقراطية في جميع مراحل دورة حياة نظام الذكاء الاصطناعي. وتشمل هذه القيم الحرية والكرامة والاستقلالية والخصوصية وحماية البيانات وعدم التمييز والمساواة والتنوع والإنصاف والعدالة الاجتماعية وحقوق العمل المعترف بها دولياً.

**3/ الشفافية والقابلية للتفسير:**

يجب على الأطراف الفاعلة في الذكاء الاصطناعي الالتزام بالشفافية والإفصاح المسؤول فيما يتعلق بنظام الذكاء الاصطناعي. وتحقيقًا لهذه الغاية، يجب على الأطراف الفاعلة تقديم معلومات مفيدة وملائمة للسياق ومتسقة مع آخر المستجدات:

- ✓ لتعزيز الفهم العام لنظم الذكاء الاصطناعي؛ ولتوعية أصحاب المصلحة بتفاعلاتهم مع نظم الذكاء الاصطناعي بما في ذلك في مكان العمل؛ ولتمكين أصحاب المصلحة المتأثرين بنظام الذكاء الاصطناعي من فهم النتائج؛ وتمكينهم من تحديدها استناداً على معلومات واضحة وسهلة الفهم.

**4/ المتانة والأمن والسلامة:**

يجب أن تكون نظم الذكاء الاصطناعي متينة وآمنة وسليمة طوال دورة حياتها بالكامل لكي تعمل على النحو المناسب ولا تشكّل خطرا غير معقول على السلامة، وذلك في ظروف الاستخدام العادي أو المتوقع أو سوء الاستخدام أو غيرها من الظروف غير المواتية.

وتحقيقاً لهذه الغاية، يجب على الأطراف الفاعلة في هذا المجال ضمان إمكانية التتبع ما في ذلك ما يتعلق بمجموعات البيانات والعمليات والقرارات المتخذة خلال دورة حياة نظام الذكاء الاصطناعي[1]، لتمكين تحليل نتائجه والاستجابات للاستفسارات بما يلائم السياق ويتّسق مع

[1]دورة حياة نظام الذكاء الاصطناعي: تعني العملية الدورية التي يتوقع من مطوري الذكاء الاصطناعي اتباعها لتصميم وبناء وإنتاج نظام قوي وآمن يقدّم قيمة عملية ورؤى من خلال الالتزام بطريقة موحّدة ومنظمة لإدارة تنفيذ وتسليم نموذج الذكاء الاصطناعي. الهيئة السعودية للبيانات والذكاء الاصطناعي، مبادئ أخلاقيات الذكاء الاصطناعي، الإصدار الأول

آخر المستجدات. كما عليها أن تطبق نهجاً منتظماً لإدارة المخاطر في كل مرحلة من مراحل دورة حياة النظام على أساس متواصل للتصدّي للمخاطر ذات الصلة بما في ذلك الخصوصية والأمن الرقمي والسلامة والتحيّز.

**5/ المساءلة:**

يجب أن تكون الأطراف الفاعلة في مجال الذكاء الاصطناعي مسؤولة عن الأداء السليم لنظم الذكاء الاصطناعي وعن احترام المبادئ المذكورة أعلاه وفقاً لأدوارها ووفقاً للسياق وبما يتسق مع آخر المستجدّات.[1]

**ب/ السياسات الوطنية والتعاون الدولي من أجل الذكاء الاصطناعي الجدير بالثقة:**

إلى جانب المبادئ، تقدم توصية مجلس منظمة التعاون الاقتصادي والتنمية خمس توصيات لواضعي السياسات المتعلقة بالسياسات الوطنية والتعاون الدولي من أجل الذكاء الاصطناعي الجدير بالثقة، وتتمثل فيما يلي:

- ✓ الاستثمار في البحث والتطوير في مجال الذكاء الاصطناعي.
- ✓ تعزيز نظام بيئي رقمي ملائم لتطور الذكاء الاصطناعي.
- ✓ خلق بيئة تمكينية للسياسات من أجل الذكاء الاصطناعي.
- ✓ بناء القدرات البشرية والاستعداد لتحوّل سوق العمل.
- ✓ التعاون الدولي من أجل الذكاء الاصطناعي الجدير بالثقة[2].

وننوّه إلى أنّ هذه التوصية قد تمّ تحديثها في ماي 2024 من أجل مسايرة التطوّرات التكنولوجية والسياسية الجديدة. وقد حظت باهتمام كبير لدرجة أن أصبحت مبادئها دستوراً

---

سبتمبر 2023، ص6.

[1] منظمة التعاون الاقتصادي والتنمية، توصية مجلس منظمة التعاون الاقتصادي والتنمية بشأن الذكاء الاصطناعي، رقم الوثيقة OECD/LEGAL/0449، 2021.

[2] منظمة التعاون الاقتصادي والتنمية، المرجع نفسه.

لسياسة الذكاء الاصطناعي في الغرب، واعتبرت منطلقاً للمبادرات في مختلف الدول[1]، على رأسها مجموعة السبعG7 سنة 2019 ومجموعة العشرينG20 في سنة 2022.[2]

**ثانيا/ توصية اليونسكو بشأن أخلاقيات الذكاء الاصطناعي**

انعقد المؤتمر العام لمنظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) في دورته الحادية والأربعين بمدينة باريس في الفترة الممتدة من 9 إلى 24 نوفمبر من عام 2021، وتمّ بالإجماع اعتماد أوّل صكّ دولي من نوعه بعنوان توصية بشأن أخلاقيات الذكاء الاصطناعي، والتي جرى الأخذ بنهج شامل لإعدادها باعتبارها وثيقة تقنينية تستند إلى القانون الدولي وتركّز على كرامة وحقوق الإنسان، وكذلك على المساواة بين الجنسين والعدالة والتنمية الاجتماعية والاقتصادية والسلامة الجسدية والنفسية والتنوّع والترابط والشمول وحماية البيئة والنظم الإيكولوجية، يمكن أن توفّر الإرشادات اللازمة لتوجيه وسائل تكنولوجيا الذكاء الاصطناعي توجيهاً مسؤولاً.[3]

وترمي هذه التوصية إلى وضع الأسس اللازمة لتسخير نظم الذكاء الاصطناعي الصالح للبشرية والأفراد والمجتمعات والبيئة والنظم الإيكولوجية مع السعي في الوقت نفسه لدرء الضرر، كما ترمي أيضا إلى الحث على استخدام نظم الذكاء الاصطناعي استخداما سلمياً من خلال إقرار مجموعة من القيم والمبادئ تتقاطع إلى حدّ كبير مع تلك التي أقرّتها منظمة التعاون الاقتصادي والتنمية، لا سيما فيما يتعلق بمبادئ الشفافية، والمسؤولية، والعدالة، وعدم التمييز، واحترام حقوق الإنسان.[4]

[1] رضوان الوهابي، مرجع سابق، ص189.

[2] للمزيد أنظر: بلباي إكرام، مرجع سابق، ص 100-101.

[3] اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي، باريس،2021، تحت رقم: SHS/BIO/PI/2021/1

[4] اليونسكو، المرجع نفسه.

وتفاديًا للوقوع في التكرار، فإن تحليلنا سينصبّ تحديدًا على موقف اليونسكو بشأن حماية الحق في الخصوصية والبيانات الشخصية باعتباره أحد المبادئ التي أقرّتها التوصية ونظراً لكون دراستنا تتمحور في هذا الجانب.

لقد أولت توصية اليونسكو بشأن أخلاقيات الذكاء الاصطناعي أهمية خاصة لحماية الخصوصية، واعتبرته حقاً ضرورياً لصون كرامة الإنسان والذود عن استقلاليته وحماية أعماله، يجب احترامه وتعزيزه طوال دورة حياة نظام الذكاء الاصطناعي. وعليه من المهم جمع البيانات وتبادلها بطريقة تتوافق مع القانون الدولي، وكذلك مع القيم والمبادئ المنصوص عليها في هذه التوصية، وفي ظلّ التقيد بالأطر القانونية الوطنية والإقليمية والدولية.[1]

كما تدعو إلى الأخذ بنهج متعدّد الأطراف لوضع أطر ملائمة لحماية البيانات ووضع آليات مناسبة تحظى بحماية النظم القضائية، وتستند إلى المبادئ والمعايير الدولية لحماية البيانات فيما يخصّ جمعها ومعالجتها في إطار ممارسة الأشخاص المعنيين بالبيانات لحقوقهم، مع وجود غرض أو هدف مشروع وأساس قانوني سليم لمعالجة البيانات الشخصية، وتضم متطلبات ذلك الحصول على موافقة مستنيرة من أولئك الأشخاص،[2]وهذا ما ينسجم مع القواعد العامة المعمول بها في حماية الخصوصية، مثل ما ورد في اللائحة العامّة لحماية البيانات (GDPR)، مما يعكس محاولة لإرساء معايير عالمية موحّدة في هذا الشأن.

كما تحرص التوصية على ضرورة إجراء عمليات تقييم كافية للنظم الخوارزمية نظراً لعواقبها على الخصوصية مع مراعاة الاعتبارات المجتمعية والأخلاقية لاستخدامها، وتدعو إلى إتباع نهج مبتكر يراعي الخصوصية طوال عملية تصميم الأنظمة، مع التأكيد على ضرورة خضوع الجهات الفاعلة في مجال الذكاء الاصطناعي للمساءلة عن تصميم واستخدام هذه النظم، من

[1] أنظر المادة 32 من توصيات اليونسكو الخاصة بأخلاقيات الذكاء الاصطناعي.

[2] أنظر المادة 33 من توصيات اليونسكو الخاصة بأخلاقيات الذكاء الاصطناعي.

أجل ضمان حماية المعلومات الشخصية طوال دورة حياة أي نظام من نظم الذكاء الاصطناعي.[1]

هذا وتحدّد التوصية 11 مجالاً من مجالات العمل الاستراتيجية التي تمكّن واضعي السياسات من ترجمة القيم والمبادئ الأساسية إلى إجراءات فعلية، ويركّز مجال العمل الثالث على تطوير سياسات شاملة ومتكاملة لحوكمة البيانات. فضلاً عن تدابير الرصد والتقييم والتطبيق والترويج لها.[2]

**ثالثا/ قرار الجمعية العامة بشأن اغتنام الفرص التي تتيحها نظم الذكاء الاصطناعي "المأمونة والمؤمّنة والموثوقة" لأغراض التنمية المستدامة:**

اعتمدت الجمعية العامة للأمم المتحدة في 21 مارس 2024 بالإجماع القرار A/78/L.49 بشأن "اغتنام فرص أنظمة الذكاء الاصطناعي الآمنة والمأمونة والجديرة بالثقة لتحقيق التنمية المستدامة"، وقد شارك في رعايته 125 دولة. وهو يعتبر أول قرار على الإطلاق تعتمده الأمم المتحدة بشأن مسألة الذكاء الاصطناعي، مما يجعله محطة بارزة في مسار تنظيم هذا المجال.[3]

يحذّر القرار من "تصميم أو تطوير أو نشر أو استخدام أنظمة الذكاء الاصطناعي بشكل غير ملائم أو خبيث، مثل القيام بذلك دون ضمانات كافية أو بطريقة تتعارض مع القانون الدولي،[4] وهذا ما يشكل مخاطر قد تعيق التقدم نحو تحقيق أجندة 2030 للتنمية المستدامة وتوسع الفجوات الرقمية بين الدول وداخلها، وتعزز عدم المساواة البنيوية والتحيزات، وتؤدي إلى التمييز، وتقوض نزاهة المعلومات والوصول إليها، وتضعف حماية وتعزيز وتمتع حقوق

[1] أنظر المادة 34 من توصيات اليونسكو الخاصة بأخلاقيات الذكاء الاصطناعي.

[2] رضوان الوهابي، مرجع سابق، ص190.

[3] International: The United Nations adopts its first resolution on AI, 15-04-2024, Disponible sur : https://insightplus.bakermckenzie.com, consulté le :20-05-2025,à10 :20.

[4] Edith M.Lederer ,The UN adopts a resolution backing efforts to ensure artificial intelligence is safe,22-03-2024,Disponible sur : https://apnews.com, Consulté le :20-05,2025,à10 :50.

الإنسان والحريات الأساسية، بما في ذلك الحق في عدم التعرض لتدخل غير قانوني أو تعسفي في الخصوصية، وتزيد من المخاطر المحتملة للحوادث وتفاقم التهديدات من الجهات الخبيثة[1].

واعترف القرار بالتسارع الكبير في تطوير واستخدام الذكاء الاصطناعي، ما يستوجب التوصّل العاجل إلى توافق عالمي بشأن أنظمة الذكاء الاصطناعي الآمنة والموثوقة والخاضعة للضوابط. وعليه دعاَ جميع الدول الأعضاء وأصحاب المصلحة إلى تطوير ودعم نُهج وأطر تنظيمية وحوكمية فعّالة، مع التأكيد على ضرورة مساعدة الدول النامية في الوصول إلى فوائد التحول الرقمي وأنظمة الذكاء الاصطناعي الآمنة، مع ضمان احترام وحماية حقوق الإنسان والحريات الأساسية طوال دورة حياة أنظمة الذكاء الاصطناعي.[2]

**الفرع الثاني: الأطر الأخلاقية الإقليمية (الأوروبية)**

لقد كان للتجربة الأوروبية دور ريادي في صياغة مبادئ أخلاقية وتوجيهات تضبط استخدام الذكاء الاصطناعي، سواء على المستوى الإقليمي وحتى العالمي. ويتجلّى هذا التوجه من خلال إصدار الميثاق الأخلاقي الأوروبي بالإضافة إلى اعتماد الاتفاقية الإطار بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون.

**أولا/ الميثاق الأخلاقي الأوروبي لاستخدام الذكاء الاصطناعي في الأنظمة القضائية وملحقاتها**

مع تزايد أهمية الذكاء الاصطناعي في المجتمع المعاصر، ودمج تكنولوجيا المعلومات والاتصالات على نطاق واسع في إدارة العدالة، برزت الحاجة إلى تبنّي مدونة أخلاقية تنظّم استخدام هذه التقنيات، تمثلت في الميثاق الأخلاقي الأوروبي لاستخدام الذكاء الاصطناعي في الأنظمة القضائية وملحقاتها، المعتمد من طرف المفوضية الأوروبية لفعالية العدالة في نهاية عام 2018. كأول أداة إقليمية أوروبية تتصور إطارًا من المبادئ الأخلاقية التي يمكن

[1] Viviana Munoz Tellez, UNGA adopts first resolution on Artificial Intelligence, SouthViews, no 269, South Centre, 16-07-2024, p02.
[2] Edith M.Lederer,OP,Cit.

أن تساعد المشرّعين وصنّاع القرار، وكذلك القائمين على قطاع العدالة، على مواكبة التطورات المتسارعة لتقنيات الذكاء الاصطناعي وتطبيقاتها القضائية.[1]

وقد أكّد الميثاق على ضرورة أن يتم استخدام هذه التقنيات في النظم القضائية بطريقة مسؤولة، بما يضمن تحسين كفاءة وجودة العدالة وتعزيزها، تماشياً مع احترام الحقوق الأساسية للأفراد المنصوص عليها في الاتفاقية الأوروبية لحقوق الإنسان واتفاقية حماية البيانات الشخصية وغيرهما من صكوك مجلس أوروبا المعنية بحقوق الإنسان.[2]

كما أن هذا الميثاق قد حدّد خمسة مبادئ أخلاقية يجب مراعاتها عند استخدام الذكاء الاصطناعي في تطبيق القانون وتتضمّن ما يلي:

- ✓ مبدأ احترام الحقوق الأساسية: أي أن يكون تصميم وتطبيق خدمات وأدوات الذكاء الاصطناعي في أنظمة القضاء يتوافق مع احترام الحقوق الأساسية للإنسان.
- ✓ مبدأ عدم التمييز: يُمنع إنشاء أو تطوير أو تخصيص تطبيقات للذكاء الاصطناعي التي قد تؤدي إلى التمييز بين الأفراد في المحاكم.
- ✓ مبدأ الجودة والأمن: ينبغي استخدام مصادر تكنولوجية آمنة ومعتمدة، يتمّ تزويدها بالمعلومات والبيانات القضائية وقرارات المحاكم.
- ✓ مبدأ الشفافية والحياد والنزاهة: تبسيط أساليب معالجة البيانات وإصدارها بطرق واضحة وسهلة الفهم، مع ضمان خضوعها لعمليات تدقيق خارجي.
- ✓ مبدأ تحت سيطرة المستخدم: وذلك بتمكين كل مستخدم من أن يكون فاعلاً ومطّلعاً على حقوقه، وسيّد القرار في اختياراته.[3]

[1] Irina Moroianu Zlătescu, Petru Emanuel Zlătescu, Implementation of the European ethical charter on the use of artificial intelligence in judicial systems and their environment, Supplement of Law Review, 2019, p.238–239.

[2] إكرام بلباي، مرجع سابق، ص113.

[3] ميموني وفاء، عماري نور الدين، الذكاء الاصطناعي بين مطرقة القانون وسندان الابتكار التكنولوجي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 9، العدد 2، 2024، (لا يوجد ترقيم).

**ثانياً/ الاتفاقية الإطارية بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون:**

جرى إعداد هذه الاتفاقية في إطار مجلس أوروبا الذي يضمّ 46 عضواً، تمّ اعتمادها من طرف لجنة الوزراء خلال دورتها 133 المنعقدة بستراسبورغ في 17 ماي 2024. على أن يبدأ نفاذها وفق المادة 30 منها في اليوم الأول من الشهر التالي لانقضاء فترة ثلاثة أشهر على التاريخ الذي أعربت فيه خمس دول موقعة بما فيها ثلاث دول أعضاء بمجلس أوروبا على الأقل عن موافقتها على الالتزام بهذه الاتفاقية، كما أن الاتفاقية مفتوحة أيضاً لانضمام دول أخرى غير أعضاء في مجلس أوروبا.[1]

تعدّ هذه الاتفاقية أول صكّ دولي ملزم قانوناً في هذا المجال. وتهدف إلى ضمان أن تكون الأنشطة التي يتمّ تنفيذها في إطار دورة حياة أنظمة الذكاء الاصطناعي متوافقة تماماً مع حقوق الانسان والديمقراطية وسيادة القانون، مع كونها مواتية للتقدّم التكنولوجي والابتكار.[2]

وقد جاءت هذه الاتفاقية نتيجة عمل استمر عامين من قبل هيئة حكومية دولية، تسمىّ لجنة الذكاء الاصطناعي(CAI) ، والتي جمعت لصياغة المعاهدة الدول الأعضاء الـ 46 في مجلس أوروبا، والاتحاد الأوروبي و11 دولة غير عضو بالإضافة إلى ممثلين عن القطاع الخاص والمجتمع المدني والأوساط الأكاديمية، الذين شاركوا كمراقبين[3].

وفي هذا السياق يقول رئيس لجنة الذكاء الاصطناعي "توماس شنايدر": تهدف هذه الاتفاقية إلى وضع قواعد قانونية ملزمة للدول الأعضاء بمجلس أوروبا لضمان التطبيق المستمرّ والموحّد لحقوق الإنسان ومبدأ سيادة القانون، في السياقات التي تساعد فيها أنظمة الذكاء الاصطناعي أو تحلّ محل صنع القرار البشري، أو تؤدي مهام أخرى ذات الصلة، بطريقة لا

---

[1] رضوان الوهابي، مرجع سابق، ص191.

[2] مجلس أوروبا، الاتفاقية الإطارية بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون، النسخة العربية، متاحة على الموقع:WWW.COE.INT /AI ، تاريخ الاطلاع: 21-05-2025، على الساعة 19:40.

[3] مجلس أوروبا يعتمد أول معاهدة دولية ملزمة بشأن الذكاء الاصطناعي، مكتب التحرير في موقع آنلوك بلوك تشين، 17-05-2024، متاح على الموقع: https://www.unlock-bc.com، تاريخ الاطلاع: 21-05-2025، على الساعة 19:00.

تعرّض العملية الديمقراطية للخطر أو تقوضها بشكل مباشر أو غير مباشر،،،،لتطوير مجموعة من المبادئ الأساسية المشتركة التي تنطبق على تصميم وتطوير وتطبيق الذكاء الاصطناعي؛ بحيث تكون هذه المبادئ قوية وواضحة، وتراعي منطق وثقافة الأنظمة القانونية للدول وتقاليدها.[1]

وقد جاءت هذه الاتفاقية بعدد من الالتزامات العامّة وكذا التدابير المفروضة على كلّ طرف من أطرافها لحماية حقوق الانسان ونزاهة العمليات الديمقراطية واحترام دولة القانون. في حين تركّز في فصلها الثالث على عدّة مبادئ أساسية تخضع لها الأنشطة المنفذة في دورة حياة أنظمة الذكاء الاصطناعي، تتمثّل فيما يلي: كرامة الإنسان واستقلاله الشخصي؛ الشفافية والرقابة؛ المسائلة والمسؤولية؛ المساواة وعدم التمييز؛ احترام الخصوصية وحماية البيانات الشخصية؛ المصداقية؛ الابتكار الآمن.[2]

ومما سبق، نستنتج بأنّ حماية الخصوصية في عصر الذكاء الاصطناعي تمثّل قضية العصر والتي تهمّنا جميعًا، ومن الضروري التعامل مع هذا التحدي من خلال مقاربة متعددة الأبعاد تشمل تعاون الحكومات والمؤسسات والأفراد على حد سواء.

فيجب على الحكومات أن تضع تنظيمات تضمن تطوير واستخدام الذكاء الاصطناعي بطريقة تحترم خصوصية الأفراد وغيرها من الاعتبارات الأخلاقية. كما ينبغي على المؤسسات أن تراعي الخصوصية ضمن القيم الأساسية وأن تعتمد سياسات قوية لحماية البيانات تحترم خصوصية الأفراد. وأخيرًا، ينبغي تمكين الأفراد من خلال منحهم الشفافية والتحكم في بياناتهم الشخصية. ومن خلال إعطاء الأولوية للخصوصية وتبني سياسات قوية لحماية البيانات، يمكننا المساهمة في ضمان تطوير واستخدام تكنولوجيا الذكاء الاصطناعي بشكل فعّال ومحترم

[1] إكرام بلباي، مرجع سابق، ص93.

[2] رضوان الوهابي، مرجع سابق، ص192.

للخصوصية، مما يؤدي في النهاية إلى مستقبل يتمكن فيه الأفراد من الاستفادة من القوة التحويلية للذكاء الاصطناعي دون التضحية بحقهم الأساسي في الخصوصية[1].

[1] Dr Mark van Rijmenam, CSP, Privacy in the Age of AI: Risks, Challenges and Solutions,16-02-2023,Disponible sur : https://www.thedigitalspeaker.com, consulté le :21-05-2025, à20 :10.

# الخاتمة

## خاتمة

وفي ختام دراستنا، تبيّن لنا أنّ الحق في الخصوصية يعتبر من أبرز حقوق الإنسان وأشدها ارتباطًا بكرامة الفرد وحريته، وقد كُرّس هذا الحق في المواثيق الدولية والدساتير الوطنية، كما أقرّته الشريعة الإسلامية ضمن مقاصدها الرامية إلى صيانة الحرمات والأنفس. ورغم هذه المكانة، لم يحظَ الحق في الخصوصية بتعريف جامع مانع، حيث انقسمت آراء الفقهاء إلى اتجاهين: أحدهما إيجابي حاول وضع تعريف لهذا الحق انطلاقًا من نظريات مختلفة؛ في حين أدرك الاتجاه الآخر صعوبة تحديد تعريف دقيق له، فاكتفى بالتمييز بين الحياة الخاصة والحياة العامة بناءً على مجموعة من المعايير. وهذا لم يكن مانعاً في إقرار حماية قانونية لهذا الحق بدءً من التشريع الأسمى في البلاد وصولاً إلى التشريعات العادية.

ومع التطور التكنولوجي المتسارع، طرأت تحوّلات عميقة على مفهوم الخصوصية، إذ لم يعد محصورًا في حمايته التقليدية المتعلّقة بحرمة المسكن والمراسلات،،،، بل توسّع ليشمل جانب جديد يتعلق بحماية البيانات الشخصية، فيما يُعرف اليوم بالخصوصية الرقمية، والتي باتت أكثر عرضة للانتهاك بفعل تقنيات الذكاء الاصطناعي و استخداماته المتزايدة في مختلف مجالات الحياة. وقد أفرز هذا الواقع تهديدات خطيرة تطال جوهر الحق في الخصوصية الشخصية، مما يستدعي ضرورة إيجاد آليات تكفل حماية هذا الحق واتخاذ تدابير فعالة لمواجهة الانتهاكات والحدّ منها قبل أن تتفاقم آثارها على الأفراد والمجتمعات. واستنادً على ما سبق من تحليل، توصلت دراستنا المتواضعة إلى جملة من النتائج نستعرضها كالآتي:

**أولا/ النتائج:**

1. لقد ساير المشرّع الجزائري التطورات التكنولوجية الحاصلة وأدرك خطورتها على الحق في الخصوصية، فقام بإصدار تشريع خاص يعنى بحماية البيانات الشخصية والمتمثل في القانون 18-07 على غرار ما شهدته التشريعات المقارنة.

2. أفلح المشرّع الجزائري في تعريفه للبيانات الشخصية من خلال القانون 18-07، الذي حدد فيه أنماط البيانات الشخصية المكفولة بالحماية وأعطى أمثلة عنها، كما ترك المجال مفتوحاً لإدراج أنواع جديدة من البيانات مستقبلاً لمواكبة المستجدات المتعلقة بطرق جمع البيانات ومعالجتها.
3. يعتبر الحق في الخصوصية من أكثر حقوق الإنسان تأثراً بالأنظمة الذكية، وذلك لكونها تتغذى من البيانات الشخصية وتتخذها وقوداً لها لتدريب خوارزمياتها والتحسين من أدائها، وهذا ما يثير مخاوف جدية حول تخزين البيانات واستخدامها والوصول إليها.
4. تُعدّ الانتهاكات التي تمسّ الحق في الخصوصية بفعل أنظمة الذكاء الاصطناعي أكثر خطورة وتعقيدًا من الاعتداءات التقليدية، نظراً لقدرتها المتطوّرة على التتبع والتحليل والتنبؤ وهذا ما يثير إشكالية مدى ملائمة التشريعات الحالية لمتطلبات حماية الخصوصية.
5. عجز الآليات القانونية وحدها عن توفير حماية فعاّلة للبيانات الشخصية، كما أن وسائل الحماية التقنية تبقى ضئيلة في مواجهة القدرة الهائلة للخوارزميات الذكية على جمع البيانات وتحليلها، ممّا استدعى ضرورة التفكير في أطر أخلاقية توجه الأنظمة الذكية نحو ابتكار آمن ومسؤول، ما يؤدي إلى توازن دقيق بين الاستفادة من قدرات الذكاء الاصطناعي وبين الحفاظ على الحقوق والحريات الأساسية للأفراد.

**ثانيا/ الاقتراحات:**

وبناءً على ما أفرزته الدراسة من نتائج، يمكن أن نلتمس بعض الاقتراحات التي من شأنها تعزيز حماية الحق في الخصوصية في ظل ما تشهده أنظمة الذكاء الاصطناعي من تطور متسارع، وتتمثل فيما يلي:

1. ينبغي على المشرّع الجزائري وضع إطار قانوني خاص بتنظيم الذكاء الاصطناعي، يُعرّف من خلاله المفاهيم الأساسية المرتبطة بهذه التقنية، ويُحدد المبادئ العامة لاستخدامها، بما في ذلك قواعد المسؤولية القانونية عند الإخلال بالحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية.

2. ضرورة تعديل القانون رقم 18-07 ليتماشى مع متطلبات المعالجة الآلية للبيانات في ظل الذكاء الاصطناعي، وذلك بفرض التزامات قانونية واضحة على المطوّرين والمستخدمين، تتعلق باحترام مبدأ تقليل البيانات، والحق في النسيان الرقمي، والشفافية، والحصول على موافقة صريحة، وضمان عدم استعمال البيانات لأغراض غير مشروعة.
3. ضرورة السعي نحو إعداد اتفاقية عربية شاملة تُنظّم الجانب الأخلاقي لاستخدام الذكاء الاصطناعي، على غرار الجهود الدولية والإقليمية المبذولة في هذا المجال. وذلك من أجل توحيد المبادئ الأخلاقية بالمنطقة العربية وضمان التوازن بين التكنولوجيا واحترام حقوق الإنسان.
4. تعزيز البنية التحتية الرقمية من خلال تحديث أنظمة الأمن السيبراني وتطوير شبكات الاتصال لضمان حماية فعالة للبيانات، مع تشجيع الأفراد على استخدام أدوات وتقنيات الحماية المتقدمة على أجهزتهم المحمولة وحواسيبهم، بما يساهم في التقليل من مخاطر انتهاك الخصوصية.
5. تشجيع الباحثين على الابتكار والأبحاث الآمنة في مجال الذكاء الاصطناعي التي تراعي مقتضيات الحق في الخصوصية، وكذا دعم الأبحاث التي تهدف إلى تطوير تقنيات جديدة لحماية البيانات الشخصية وتعزيز الأمن السيبراني.
6. إطلاق حملات توعوية تستهدف الجمهور العام، لتعريف الأفراد بحقوقهم الرقمية، ورفع الوعي بمخاطر انتهاك الخصوصية الناتجة عن استخدام تقنيات الذكاء الاصطناعي، مع التأكيد على ضرورة أخذ الحيطة والحذر فيما يتعلّق بنشر معلوماتهم الحسّاسة عبر الوسائط الرقمية.

# قائمة المصادر والمراجع

# قائمة المصادر والمراجع:

## أولاً/ باللغة العربية:

### القرآن الكريم:

### الدساتير:

1. التعديل الدستوري المصادق عليه في استفتاء 01 نوفمبر 2020، بموجب المرسوم الرئاسي رقم20-442، مؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر 2020، ج ر، عدد82، الصادرة في 30 ديسمبر 2020.

### الاتفاقيات:

1. مجلس أوروبا، اتفاقية حماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، مجموعة المعاهدات الأوروبية رقم108، المادة02، الصادرة في28 يناير 1981، ستراسبورغ، نسخة مترجمة، متاحة على:https://rm.coe.int ، تاريخ الاطلاع:13_04_2025 ، على الساعة 20:55.
2. الاتحاد الأوربي، اللائحة العامة لحماية البيانات، المادة 9، الصادرة بموجب اللائحة 2016/679، الجريدة الرسمية للاتحاد الأوربي، 2016.
3. مجلس أوروبا، الاتفاقية الإطارية بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون، النسخة العربية، متاحة على الموقع:WWW.COE.INT /AI ، تاريخ الاطلاع: 21-05-2025، على الساعة 19:40.

### القوانين:

1. المرسوم الرئاسي 21_323، المؤرخ في 22 أوت 2021، يتضمن إنشاء مدرسة وطنية عليا للذكاء الاصطناعي، ج ر، عدد65، الصادرة بتاريخ 30 أوت 2021، المتضمن إنشاء مدرسة وطنية عليا للذكاء الاصطناعي.
2. القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المتمم للأمر 66-156 المتضمن قانون العقوبات، ج ر، عدد 71، الصادرة في 10 نوفمبر 2004.
3. القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-156، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، ج ر، عدد 84، الصادرة في 24 ديسمبر 2006 .
4. القانون رقم 15_04، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المؤرخ في 01 فبراير 2015، ج ر، عدد 06، الصادرة في 10 فبراير 2015.

5. قانون رقم 18_04، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المؤرخ في 10 ماي 2018، ج ر، عدد27، الصادرة في 13ماي 2018.
6. القانون رقم 18_05، المتعلق بالتجارة الالكترونية، المؤرخ في 10ماي 2018، ج ر، عدد 28، الصادرة في 16 ماي 2018.
7. القانون رقم 18_07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018، ج ر، عدد 34، الصادرة في 10 يونيو2018.

**التوصيات:**

1. منظمة التعاون الاقتصادي والتنمية، توصية مجلس منظمة التعاون الاقتصادي والتنمية بشأن الذكاء الاصطناعي،2021، رقم الوثيقة:OECD/LEGAL/044 .
2. اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي، باريس،2021، تحت رقم: SHS/BIO/PI/2021/1.

**التقارير:**

1. مفوضية الأمم المتحدة السامية لحقوق الإنسان، تقرير المفوض السامي لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي، الوثيقة رقم A/ HRC /39/29، الدورة 39 لمجلس حقوق الإنسان، 3 آب/أغسطس 2018، النسخة العربية متاحة على:https://digitallibrary.un.org، تاريخ الاطلاع: 02-05-2025 على الساعة 10:50.

**الكتب:**

1. الاتحاد الدولي للاتصالات، الاتجاهات التكنولوجية الناشئة: الذكاء الاصطناعي والبيانات الضخمة لأغراض التنمية، جنيف، 2021.
2. أسامة عبد الرحمن، الذكاء الاصطناعي ومخاطره، ط1، دار زهور المعرفة والبركة، الجيزة (مصر)، 2018.
3. أشرف توفيق شمس الدين، الصحافة والحماية الجنائية للحياة الخاصة "دراسة مقارنة"، الطبعة الأولى، دار النهضة العربية، مصر،2007.
4. أميرة بدوى نجم، أخلاقيات الذكاء الاصطناعي في ضوء توصيات الأمم المتحدة (اليونسكو)، ط1، دار الفكر الجامعي، الإسكندرية، 2024.
5. بلباي إكرام، الذكاء الاصطناعي في القانون الدولي–دراسة في المفهوم والأطر والتطبيقات–، ط1، ابن النديم للنشر والتوزيع ومؤسسة الكتاب القانوني، الجزائر، 2024.
6. بوجمعة بتشيم، الذكاء الاصطناعي في منظومة العدالة الحديثة _على ضوء أحدث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022_، ط1، ألفا للوثائق للنشر والتوزيع، عمان (الأردن)،2023.

7. بوكر رشيدة، الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي بين تصاعد التهديدات وفرص تعزيز الأمن السيبراني، د ط، دار إيلياء للنشر والتوزيع، الجزائر، 2024.
8. توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الأنترنت وحرية التعبير، منشورات اليونسكو، منظمة الأمم المتحدة للتربية والعلم والثقافة، مترجم بفضل مساهمة الوكالة السويدية للتعاون الإنمائي الدولي (سيدا)، فرنسا، 2012.
9. حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها–دراسة مقارنة–، ط1، مكتبة بدران الحقوقية، صيدا(لبنان)، 2017.
10. حمده خلفان بالجافله، التكييف الفقهي لتطبيقات الذكاء الاصطناعي في المجال الاقتصادي والجنائي، ط1، دائرة الشؤون الإسلامية والعمل الخيري، دبي (الامارات العربية المتحدة)، 2024.
11. خالد حسن أحمد، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية دراسة مقارنة، د ط، دار الكتب والدراسات العربية،2020.
12. سالي محمد عبد، يسرى شاكر عجاج، مصطفى قصي علي وآخرون، الذكاء الاصطناعي مفاهيم وتقنيات–دليل تعليمي للطلبة، ط1، دار السرد للطباعة والنشر والتوزيع، بغداد(العراق)،2024.
13. سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، ط1، دار الفكر الجامعي، الإسكندرية، 2017.
14. طارق إبراهيم الدسوقي عطيه، الأمن المعلوماتي –النظام القانوني لحماية المعلومات–، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.
15. عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، د ط، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 2005.
16. عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، د ط، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 2005.
17. عبد الله موسى، أحمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، ط1، المجموعة العربية للتدريب والنشر، القاهرة، 2019.
18. عصام أحمد البهجى، حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية، دون طبعة، دار الجامعة الجديدة للنشر، الإسكندرية ،2005.
19. عماد حمدى حجازي، الحق في الخصوصية ومسؤولية الصحفي في ضوء أحكام الشريعة الإسلامية والقانون المدني، د ط، دار الفكر الجامعي، الإسكندرية، 2008.
20. محمد الهادي السهيلي، تطوّرات الذكاء الاصطناعي ومقتضيات حماية الحقوق والحريات الأساسية، إدارة الشؤون القانونية بمنظمة الإيسيسكو (منظمة العالم الإسلامي للتربية والعلوم والثقافة)، المملكة المغربية، 2021.

21. محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط 1، دار الحامد للنشر والتوزيع، الأردن–عمان،2007.
22. محمد راكان الدغمي، حماية الحياة الخاصة في الشريعة الإسلامية، الطبعة الأولى، دار السلام، القاهرة، 1985، ص21.
23. محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية –دراسة مقارنة–، ط1، دار الفكر والقانون للنشر والتوزيع، مصر،2015.
24. محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية "دراسة مقارنة"، ط1، مركز الدراسات العربية للنشر والتوزيع، بدون ذكر بلد النشر، 2017.
25. محمد هاني صباغ، دليل الأمان الرقمي تعرّف على مفهوم الأمان والخصوصية وكيفية حماية نفسك في العالم الرقمي، ط 1، أكاديمية حسوب، بدون بلد النشر، 2021.
26. مدحت محمد أبو النصر، الذكاء الاصطناعي في المنظمات الذكية، ط1، المجموعة العربية للتدريب والنشر، القاهرة،2020.
27. ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، د ط، دار النهضة العربية، القاهرة،2011.
28. المهندس عبد الحميد بسيونى، مقدمة الذكاء الاصطناعي للكمبيوتر ومقدمة برولوج، ط1، دار النشر للجامعات المصرية، مصر، 1994.
29. نويري عبد العزيز، الحماية الجزائية للحياة الخاصة في القانونين الجزائري والفرنسي "دراسة مقارنة"، الطبعة الثانية، دار هومة، بدون ذكر بلد النشر،2016.
30. الهيئة السعودية للبيانات والذكاء الاصطناعي، مبادئ أخلاقيات الذكاء الاصطناعي، الإصدار الأول، سبتمبر 2023.
31. وليد السيد سليم، ضمانات الخصوصية في الأنترنت، د ط، دار الجامعة الجديدة، الإسكندرية،2012.
32. وليد سليم النمر، حماية الخصوصية في الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2017.

**المجلات العلمية:**

1. ابتسام بنت سعيد الشهومية، سالم بن سعيد الكندي، محمد بن ناصر الصقري، تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية: دراسة حالة في سلطنة عمان، مجلة الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، مجلد 15، عدد 3، ديسمبر 2024.

2. إبراهيم داود، الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية (دراسة تحليلية مقارنة)، مجلة الحقوق للبحوث القانونية والاقتصادية بكلية الحقوق_ جامعة الإسكندرية، المجلد الثاني، العدد الأول ،2017.
3. أحمد حسني علي أشقر، الخصوصية الرقمية في عصر الذكاء الاصطناعي: قراءة في التشريعين الأردني والفلسطيني مجلة جامعة القدس المفتوحة للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 66، جانفي 2025.
4. بلعسل بنت نبي ياسمين، مقدر نبيل، الحق في الخصوصية الرقمية، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 5، عدد1، 2021.
5. بلهوط براهيم، التأطير القانوني للذكاء الاصطناعي، مجلة الدراسات والبحوث القانونية، جامعة اكلي محند اولحاج، البويرة، مجلد 9، عدد 2، 2024.
6. بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم و نشر الأبحاث، مجلد2، عدد5، يونيو2016.-
7. بوبعاية نصيرة، دور البيانات الضخمة والذكاء الاصطناعي في مواجهة وباء فيروس كورونا_ تجارب دولية ناجحة_، مجلة وحدة البحث في تنمية الموارد البشرية، مجلد 16، عدد 03 الخاص (الجزء2)، نوفمبر 2021.
8. بوكر رشيدة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الانسان والحريات العامّة، مجلد 7، عدد2، ديسمبر 2022.
9. جمال فوزي، التحديات الأخلاقية والقانونية للرقمنة والذكاء الاصطناعي_ المملكة المغربية نموذجا_، ضمن عصام عيروط (مشرف)، مستقبل الذكاء الاصطناعي: تحديات قانونية وأخلاقية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين "ألمانيا"، 2024.
10. جمال مراي، حق الأفراد في حماية بياناتهم الشخصية وفقاً لقانون حماية البيانات الشخصية، مقال منشور في موسوعة حماة الحق للمحاماة، 19-12-2023، متاح على الموقع https://jordanlawyer.com تاريخ الاطلاع: 08-05-2025، على الساعة 22:00.
11. حصة أحمد عبد الله التويم، وفاء أحمد عياض الغامدي، انتهاك الخصوصية في تقنيات الذكاء الاصطناعي: الواقع وسبل المواجهة من منظور التربية الإسلامية، مجلة شباب الباحثين، جامعة سوهاج(مصر)، عدد 12، ج3، 2023.
12. خالد مدوي، مستقبل الخصوصية في ظل المعالجة الآلية للمعطيات الشخصية، حوليات جامعة الجزائر 1، مجلد38، عدد 3، سبتمبر 2024.
13. خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والاقتصادية، جامعة سطيف 02، مجلد5، عدد1، جوان 2022.

14. الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والاقتصادية، مجلد1، عدد8، ديسمبر 2017.
15. ذيب محمد، فارس فزاع، الفضاء الالكتروني _مفاهيم ودلالات_ رؤية سوسيولوجية تحليلية، مجلة التميز الفكري للعلوم الاجتماعية والإنسانية، جامعة الشاذلي بن جديد_ الطارف، العدد الخامس، جانفي 2021.
16. رضوان الوهابي، من أجل قانون دولي لأخلاقيات الذكاء الاصطناعي– أضواء على الحراك العالمي لتنظيم أخلاقيات الذكاء الاصطناعي، ضمن: عصام عيروط (مشرف)، مستقبل الذكاء الاصطناعي: تحديات قانونية وأخلاقية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين ألمانيا"،2024.
17. شافعي أمال، شافعي أم السعد، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوروبي، مجلة الباحث القانوني، جامعة الحاج لخضر– باتنة 1، المجلد 1، العدد 2، مارس 2022.
18. شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية (دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا)، مجلة البحوث القانونية والاقتصادية، العدد 57، أفريل 2015.
19. عبد الله شيباني، وداد بن سالم، حق الخصوصية المعلوماتية في ضوء الذكاء الاصطناعي، مجلة الدراسات القانونية والاقتصادية، جامعة محمد لمين دباغين سطيف 2، المجلد 6، العدد 2، 2023.
20. عصام الجوهري وآخرون، تقييم استراتيجيات الذكاء الاصطناعي المعلنة في الدول العربية، المجلة المصرية للتنمية والتخطيط، بدون ذكر المجلد والعدد وتاريخ النشر.
21. عمار مراد غركان، التعاون الدولي للتصدي لخطر الإرهاب باستخدام الذكاء الاصطناعي، ضمن: عصام عيروط (مشرف)، مستقبل الذكاء الاصطناعي: تحديات قانونية وأخلاقية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين "ألمانيا"، 2024.
22. ليتيم نادية، مجلس أوروبا والذكاء الاصطناعي: أية ضوابط لحماية حقوق الانسان؟، مجلة التراث، مجلد 13، عدد4، ديسمبر 2023.
23. مريم أل سيدي الغازي، مارية بوجداين، من الحق في الحياة الخاصة الى الحق في الخصوصية الرقمية، مجلة القانون الدستوري والعلوم الإدارية، العدد الثالث، المركز الديمقراطي العربي، برلين، ماي 2019.
24. مريم ساغي، مليكة مذكور، الذكاء الاصطناعي ومشكلة الخصوصية، مجلة روافد للدراسات والأبحاث العلمية في العلوم الاجتماعية والإنسانية، المجلد 08، العدد 02، ديسمبر 2024.

25. معزوز دليلة، حماية المعطيات الشخصية في البيئة الافتراضية في التشريع الجزائري(الواقع والتحديات)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، مجلد 10، عدد1، 2021.
26. معزوز دليلة، والي نادية، مخاطر الذكاء الاصطناعي على الخصوصية الرقمية وآليات حمايتها، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة، مجلد 9، عدد3، سبتمبر 2024.
27. مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، المجلد 7، العدد الأول ،2018.
28. ميموني وفاء، عماري نور الدين، الذكاء الاصطناعي بين مطرقة القانون وسندان الابتكار التكنولوجي، المجلة الجزائرية للحقوق والعلوم السياسية، مجلد 09، عدد02، 2024.
29. نرمين عبد القادر إمبابي، تأثير استخدام روبوت المحادثة الذكية "شات جي بي تي" على حماية خصوصية بيانات المستفيدين: دراسة مسحية مقارنة، المجلة العلمية للمكتبات والوثائق والمعلومات، مجلد6، عدد19، كلية الآداب–جامعة القاهرة، يوليو 2024.
30. نور الدين الشابي، "الذكاء الاصطناعي بين العدالة والنجاعة"، ضمن: عصام عيروط (مشرف)، مستقبل الذكاء الاصطناعي: تحديات قانونية وأخلاقية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين "ألمانيا"، 2024.
31. هبة رمضان رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي، بدون ذكر المجلد والعدد وتاريخ النشر.
32. هواري صباح، الحياة الخاصة وتكنولوجيا التزييف العميق، مجلة العلوم القانونية والاجتماعية، جامعة الجلفة، كلية الحقوق والعلوم السياسية، مجلد 9، عدد 2، جوان 2024.
33. ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية دراسة تحليلية مقارنة، مجلة روح القوانين، كلية الحقوق جامعة طنطا، العدد 97، يناير 2022.
34. يحي الشريف نصير، مزغيش عبير، الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 02، 2022.
35. يسن عبد اللطيف عبد الحليم محمد، أحكام المسؤولية الناشئة عن انتهاك حرمة الحق في الخصوصية عبر وسائل التقنية الحديثة "دراسة فقهية معاصرة"، مجلة كلية الدراسات الإسلامية والعربية للبنات بكفر الشيخ، المجلد الخامس، العدد الثاني، 2018.

**المذكرات الجامعية:**

1. مجادي نعيمة، الحق في الخصوصية بين الحماية الجزائية والضوابط الإجرائية للتحقيق دراسة مقارنة، أطروحة دكتوراه، تخصص قانون إجرائي، كلية الحقوق، جامعة سيدي بلعباس،2019/2018.

2. شعلال مختار، الحق في الخصوصية في الفضاء الرقمي وحمايته في القانون الدولي (حماية خصوصية مستخدمي فيسبوك) _دراسة حالة_، أطروحة مقدّمة لنيل شهادة الدكتوراه، علوم الإعلام والاتصال، كلية العلوم الانسانية والعلوم الإسلامية، جامعة وهران1 أحمد بن بلّة، 2023/2022.
3. لينا رياض الرمحي، الحماية القانونية للبيانات الشخصية في المعاملات الالكترونية في ظل التشريع الأردني والتشريع الأوروبي– GDPR دراسة مقارنة–، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، المجلة العربية للنشر العلمي، الإصدار الثامن، العدد السابع والسبعون، جامعة عمان العربية – كلية القانون، 02 مارس 2025 .
4. بن حيدة محمد، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"، مذكرة ماجستير، تخصص حقوق وحريات، كلية الآداب والعلوم الإنسانية، الجامعة الإفريقية العقيد أحمد دراية أدرار، 2009_2010.
5. بوبكري تيسير، الحماية الجنائية للخصوصية الرقمية في التشريع الجزائري_ دراسة مقارنة_، مذكرة لنيل شهادة الماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2021_ 2022.

**المواقع الإلكترونية:**

1. مجلس أوروبا يعتمد أول معاهدة دولية ملزمة بشأن الذكاء الاصطناعي، مكتب التحرير في موقع آنلوك بلوك تشين،17-05-2024، متاح على الموقع:https://www.unlock-bc.com ، تاريخ الاطلاع: 21-05-2025، على الساعة 19:00.
2. اللجنة الدولية للصليب الأحمر، « البيومترية »، الاجتماعات النظامية، متاح على: https://rcrcconference.org، تاريخ الاطلاع: 29-04-2025 على الساعة: 01:30.
3. وكالة الأنباء الجزائرية، الجزائر تعتمد استراتيجية وطنية للذكاء الاصطناعي، مقال منشور بتاريخ 08 ديسمبر 2024، متاح عبر الرابط: https://www.aps.dz، تاريخ الاطلاع:2025/04/22 على الساعة 21:00.
4. رافي برازي، كيف تشكل بياناتك الشخصية على مواقع التواصل الاجتماعي وقوداً لنماذج الذكاء الاصطناعي، 04-07-2024، متاح على الرابط: https://bawabaai.com، تاريخ الاطلاع :25 -04-2025، على الساعة21:25.
5. شيماء عبد المنعم، قوم اطمن على فلوسك.. هاكرز يستخدمون الذكاء الاصطناعي لسرقة مدخراتك، موقع صدى البلد، 17-04-2024، متاح على الرابط:https://www.elbalad.news ، تاريخ الاطلاع:26-04-2025، على الساعة:22:00.

6. الخصوصية في الذكاء الاصطناعي: تحديات وحلول عملية لعصرنا الرقمي_ آليات حماية البيانات الشخصية: من التشريعات إلى التقنيات الآمنة، مقال متاح على الرابط:https://aidalil.com ، آخر تحديث في: 12-03-2025، تاريخ الاطلاع: 15-05-2025، على الساعة 10:00.
7. محمد بن راشد يصدر قانون تنظيم الطائرات بدون طيار في دبي، مقال منشور من طرف: دبي الإمارات اليوم، بتاريخ 05-07-2020، متاح على الموقع: www.emaratalyoum.com،تاريخ الإطلاع:08-05-2025،الساعة15:45.
8. حماية البيانات الشخصية في الامارات، مقال منشور من طرف: الصَفَر ومشاركوه، بتاريخ 27-05-2024، متاح على الموقع: https://ae.linkedin.com، تاريخ الاطلاع: 08-05-2025، الساعة 16:35.
9. التشفير وكسر التشفير وما هي الطرق المهمة والتعريفات عن أنواع التشفير، بدون تاريخ النشر، مقال منشور على: https://sumer-link.com، تاريخ الاطلاع: 14-05-2025، على الساعة 21:30.
10. دليل شامل عن: اهمية الامن السيبراني وحماية الاتصالات، منصة برق، متاح على الرابط التالي: https://br2seo.com، تاريخ الإطلاع:15-05-2025، على الساعة 20:15.
11. موقع لشرح المصطلحات، https://www.arabdict.com، تاريخ الإطلاع:12-02-2025، على الساعة 19:00.
12. الأمم المتحدة، الإعلان العالمي لحقوق الإنسان، متاح على الرابط التالي: https://www.un.org، تاريخ الإطلاع:03-05-2025، على الساعة: 9:30.
13. الأمم المتحدة، العهد الدولي الخاص بالحقوق المدنية والسياسية، متاح على الرابط التالي: https://www.ohchr.org، تاريخ الاطلاع: 03-05-2025، على الساعة: 9:45.
14. 5 خطوات لتعزيز أمان بياناتك الشخصية على تطبيقات السوشيال، 19-09-2024، متاح على الرابط التالي: https://www.youm7.com، تاريخ الاطلاع: 15-05-2025، على الساعة 21:50.
15. الأمن السيبراني: حماية بيانات المستخدم عبر الإنترنت،28-06-2023، مقال متاح على الرابط التالي:https://www.databridgemarketresearch.com ، تاريخ الاطلاع: 15-05-2025، على الساعة 20:15.

**ورشات العمل:**

1. يونس عرب، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات بنادي المعلومات العربي،2002، الأردن.

**ثانيا/ باللغة الأجنبية:**

**Les Textes juridiques :**


1. Loi Françaises N° 801-2004 , du 06 aout 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et modifiant la loi no 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,J.O7 aout 2004.
2. Règlement général sur la protection des données (RGPD), Règlement (UE) 2016/679, article 4, point 14, consulté sur : https://gdpr-info.eu, le29-04-2025 à 01:30.
3. Conseil de l'Europe, Convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit, Série des traités du Conseil de l'Europe – n° 225, Vilnius, 5 septembre 2024, article02.
4. établissant des règles harmonisées concernant l'intelligence artificielle (Loi sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, Journal officiel de l'Union européenne (JOUE), L 206, 12 juillet 2024, article 3, § 1. Disponible sur : www.eur-lex.europa.eu ,Consulté le : 15-04-2025,à 12:00 h.


**Les articles :**


1. 6 Ways to Preserve Privacy in Artificial Intelligence,18-12-2023, Disponible sur : https://privacera.com, Consulté le :15-05-2025,à15 :10.
2. Aditya Kumar, Types of AI Explained, simplilearn, dernière mise à jour le 11 avril 2025, Disponible à https://www.simplilearn.com, consulté le 18 avril 2025, à23:10 .
3. Akanbi Caleb, App permissions and privacy concerns , Disponible sur : https://www.researchgate.net, Consulté le :26-04-2025 à 11 :45 .
4. Andrea Granados, AI and Personal Data: Balancing Convenience and Privacy Risks, velaro, Dernière mise à jour le 15 novembre 2024, https://velaro.com, consulté le 24-04-2025 à19 :40.
5. Anthony De Bruyne, AI Act and GDPR: How These Regulations Work Together to Safeguard AI and Privacy, 27/12/2024,Consulté le :22-05-2025,à20 :30.
6. Bernard Marr, Understanding the 4 Types of Artificial intelligence, Bernard Marr & Co, 2 juillet 2021. Disponible à https://bernardmarr.com, consulté le 18 avril 2025 à 21 :45.
7. Brooke Katoe , Gmail, Outlook and Apple users urged to watch out for this new email scam: Cybersecurity experts sound alarm, 04-01-2025, https://nypost.com, consulté le 26-04-2025 à 21 :20.
8. Cameron Micallef, The remarkably simple way hackers can access your phone , 09-02-2025 , Disponible sur :https://www.news.com , consulté le : 26-04-2025, à 20 :50.

9. Data for AI : The Fuel That Supercharges Machine Learning, Revelate Blog, 30 août 2023, disponible sur : https://revelate.co/blog, consulté le 21 avril 2025 ,à18:30.
10. Dr Mark van Rijmenam, CSP, Privacy in the Age of AI: Risks, Challenges and Solutions,16-02-2023,Disponible sur : https://www.thedigitalspeaker.com, consulté le :21-05-2025, à20 :10.
11. Edith M.Lederer ,The UN adopts a resolution backing efforts to ensure artificial intelligence is safe,22-03-2024,Disponible sur : https://apnews.com, Consulté le :20-05,2025,à10 :50.
12. EU AI Act: first regulation on artificial intelligence, Publié le: 08-06-2023, Dernière mise à jour: 19-02-2025,Disponible sur : https://www.europarl.europa.eu, consulté le 22-05-2025,à 14 :10.
13. EU AI Act: How to Create an Effective Data Governance Strategy for Your Organization, Sans date, diponible sur : https://www.informatica.com, consulté le :22-05-2025, à15 :00.
14. Factly, Le rapport des Nations Unies souligne la nécessité de transparence et de responsabilité dans l'utilisation des systèmes d'IA, 2021, disponible sur : https://factly.in , consulté le 03-05-2025 à 16 :30.
15. International: The United Nations adopts its first resolution on AI, 15-04-2024, Disponible sur : https://insightplus.bakermckenzie.com, consulté le :20-05-2025,à10 :20.
16. Irina Moroianu Zlătescu, Petru Emanuel Zlătescu, Implementation of the European ethical charter on the use of artificial intelligence in judicial systems and their environment, Supplement of Law Review, 2019.
17. Margaret concannon , AI in Social Engineering: The Next Generation of Cyber Threats , 16-07-2024, Disponible sur :https://www.ntiva.com , consulté le : 26-04-2025 à 22 :20.
18. Marko Aleksic, What Is Differential Privacy in AI?,25-03-2025, Disponible sur : https://phoenixnap.com, consulté le :15-05-2025,à14 :30.
19. MD Absarul Hasan, Compromising Privacy: The Role of AI in Smartphone Surveillance, International Journal for Multidisciplinary Research, vol. 7, no. 1, Janvier-fevrier 2025.
20. Natasha G. Kohne, Sahar Abas, Mazen Baddar , Kingdom of Saudi Arabia Approves Amendments to Personal Data Protection Law and Confirms September 2023 Effective Date , 26-04-2023, disponible sur : **https://www.akingump.com** , cansulté le : 08-05-2025, à21 :45.
21. Petar Radanliev, Omar Santos, Ethics and Responsible AI Deployment, Sans date, Cisco Systems, RTP, Caroline du Nord, États-Unis ; University of Oxford.
22. Privacy International, Soumission au Rapporteur spécial sur le droit à la vie privée concernant, l'intelligence artificielle et la vie privée, disponible sur : https://privacyinternational.org, consulté le 03-05-2025 à 16 :30.

**23.**Privacy-Preserving AI: Techniques & Frameworks, 23-05-2024, Disponible sur : https://dialzara.com, consulté le :15-05-2025, à10 :00.
24.Quinn Emanuel Urquhart & Sullivan, LLP, Recent Amendments to the Saudi Arabia Personal Data Protection Law, sans date, disponible sur : www.quinnemanuel.com, consulté le : 8 mai 2025 à 20:15.
25.Social Media Privacy, Electronic Privacy Information Center (EPIC), (sans date), Disponible sur : https://epic.org, Consulté le 25-04-2025, à 22 :30 .
26.The 6 principles of AI and data protection: how the AI act ensures data is safe, Disponible sur : https://www.imprivata.com, consulté le :22-05-2025,à19 :40.
**27.**The growing data privacy concerns with AI: What you need to know, dataguard , https://www.dataguard.com, Publié le 4 septembre 2024, mis à jour le 10 janvier 2025 à 09:02, Consulté le 24-04-2025 à 18 :00.
28.UN resolution affirms surveillance that is not necessary or proportionate is against the right to privacy, 23-03-2017,Disponible sur: https://www.article19.org , consulté le 03-05-2025, à 10 :40.
29.Viviana Munoz Tellez, UNGA adopts first resolution on Artificial Intelligence, SouthViews, no 269, South Centre, 16-07-2024.

# الفهرس

# الفهرس

## الملخص:

أضحى الذكاء الاصطناعي إحدى أبرز مخرجات الثورة التكنولوجية المعاصرة التي فرضت نفسها كحتمية لا غنى عنها في شتى المجالات، بدءًا باستخدامه في المهام اليومية ووصولاً إلى بقية المجالات الحيوية الأخرى كالطب والتعليم والاقتصاد والزراعة...فأسهم بذلك في تسهيل حياة الفرد وتحقيق رفاهيته.
غير أنّ هذا التطور السريع والواسع النطاق رافقته تحديات جمّة، خاصة فيما يتعلق بحقوق الإنسان، وفي مقدمتها الحق في الخصوصية، الذي بات مهددًا بفعل اعتماد أنظمة الذكاء الاصطناعي على جمع ومعالجة كميات ضخمة من البيانات الشخصية لتدريب خوارزمياتها وتحسين أدائها، ما يجعلها عرضة للانتهاك والاستغلال في أغراض غير مشروعة. وتأتي هذه الدراسة لتسليط الضوء على أبرز الانتهاكات التي تمسّ الحق في الخصوصية بواسطة تطبيقات الذكاء الاصطناعي، وتداعياتها على حياة الأفراد. الأمر الذي يتطلب وضع هذه التقنية الجديدة ضمن إطار قانوني يحكم استخدامها، ويضبط جمع البيانات الشخصية، وتعزيزها بتدابير الحماية، إلى جانب ترسيخ المبادئ الأخلاقية التي تضبط هذه التكنولوجيا بما يضمن توظيفها على نحو مسؤول يصون كرامة الإنسان ويحترم حقوقه الأساسية.



**الكلمات المفتاحية:**

1/ الذكاء الاصطناعي. 2/ الخوارزميات. 3/ الانتهاكات.
4/ البيانات الشخصية. 5/ الحق في الخصوصية. 6/ المبادئ الأخلاقية.



**Abstract of Master's Thesis :**

Artificial intelligence has become one of the most prominent outcomes of the contemporary from technological revolution, imposing itself as an indispensable necessity in various fields its use in daily tasks to other vital sectors such as medicine, education, economy, and agriculture—thus contributing to facilitating individual life and achieving well-being.
However, this rapid and wide-ranging development has been accompanied by numerous challenges, particularly regarding human rights, foremost among them the right to privacy, which has become threatened due to artificial intelligence systems' reliance on collecting and processing vast amounts of personal data to train their algorithms and improve their performance. This makes such data vulnerable to violation and exploitation for unlawful purposes.
This study aims to shed light on the most significant violations affecting the right to privacy through artificial intelligence applications and their impact on individuals' lives. This situation requires placing this new technology within a legal framework governing its use, regulating the collection of personal data, reinforcing it with protective measures, and establishing ethical principles to guide this technology in a manner that ensures its responsible use while preserving human dignity and respecting fundamental rights.



**Keywords:**

1/ Artificial intelligence. 2/ Algorithms . 3/ violations.
4/ Personal data. 5/ The right to privacy. 6/ Ethical principles.