

جامعة ميدلاندز



كلية العلوم الإنسانية

ماجستير قانون رقمي

التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي

في معالجة البيانات الشخصية في البيئة الرقمية

إعداد الطالب /

سلطان بن عابد الخوري

251001709

إشراف /

د. الفیصل عبد الحمید محمد حسن

العام الدراسي:

2025

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

(يَا أَيُّهَا الَّذِينَ آمَنُوا اتَّقُوا اللَّهَ وَقُولُوا قَوْلًا سَدِيدًا يُصْلِحْ لَكُمْ أَعْمَالَكُمْ وَيَغْفِرْ لَكُمْ ذُنُوبَكُمْ
وَمَنْ يَطِيعِ اللَّهَ وَرَسُولَهُ فَقَدْ فَازَ فَوْزًا عَظِيمًا)

صدق الله العظيم

سورة الأحزاب ، رقم الآية (70).

الإهداء

إلى من منحوني الحب والدعم بلا حدود... إلى من كانوا إلى السند والقُدوة...
إلى والدي العزيز، رمز القوة والإصرار، الذي عَلمني أن الطريق إلى النجاح لا يُعبد إلا بالصبر
والمثابرة - وأن الجِدَّ لا يضيع أجره أبداً.
وإلى والدتي الحبيبة، نبع العطاء الدائم، القلب الذي لا يعرف إلا الدعاء، والحنان الذي رافقني
في كل مراحل حياتي، فكانت نوري في دروب العلم والعمل.
إلى زوجتي الغالية، نبض القلب وسرّ النجاح، شريكة كل إنجاز، ورفيقة كل لحظة صبر وسعي
كانت كلماتك دافعا، وعبرك زادي في طريق طويل من البحث والسير، لك أهدي هذا
الجهد، فهو ثمرة دعمك ووجودك بجاني.
إلى إخوتي وأخواتي الذين شاركوني كل لحظة تعب وفرح، لذين شاركوني فطانت السعي
والإنجاز.

إلى كل من آمن بي وساندني ووقف إلى جوارِي في مسيرتي العلمية،

أهدي ثمرة جهدي هذه، عربون وفاء وتقدير،

راجيا أن يكون لبنة ناعمة في صرح العلم وخدمة الوطن.

شكر وتقدير

أتوجه بخالص الشكر وعظيم التقدير إلى أساذي الفاضل الأستاذ الدكتور /

عني إشرافه الكريم وتوجيهاته العلمية الثمينة، وصبره الواسع الذي كان عوناً لي في كل مراحل إعداد هذه الرسالة.

لقد تعلمت منه معنى الدقة في البحث، والصدق في العمل العلمي، فله مني جزيل الشكر والامتنان.

كما أتقدم باسحي آيات النكر والتقدير إلى أعضاء لجنة الماقتنة المحترمين:

الأستاذ الدكتور /

والأستاذ الدكتور /

لما بذلوه من جهد ووقت في قراءة الرسالة ومناقشتها، وما أبدوه من ملاحظات علمية قيمة أسهمت في تطوير هذا العمل وإثرائه.

ولا أنسى أن أعبر عن امتناني العميق لكل من قدم لي دعماً أو تشجيعاً أو كلمة طيبة خلال هذه الرحلة، وأسأل الله أن يجزيهم جميعاً خير الجزاء، وأن يجعل هذا العمل خالصاً لوجهه الكريم، نافعاً للعلم والمجتمع.

المنهج

أصبح الذكاء الاصطناعي أحد أبرز العوامل التي تُعيد تشكيل مفهوم الخصوصية في العصر الرقمي، هدف البحث لتسليط الضوء حول التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في معالجة البيانات الشخصية في البيئة الرقمية. اعتمد البحث على استخدام منهج الوصفي التحليلي، الذي يقوم على جمع وتحليل وتفسير المعلومات المتعلقة بموضوع الدراسة بهدف خصوصية البيانات الشخصية في الفضاء الإلكتروني، وقد توصلت الدراسة لعدد من النتائج منها أنه في إطار تعزيز حماية البيانات الشخصية في المملكة العربية السعودية، صدر نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، الذي يعد الأساس النظامي لتنظيم جمع البيانات واستخدامها في المملكة، فقد بدأت عدة دول مثل المملكة العربية السعودية والإمارات ومصر في تبني تشريعات رامية لحماية البيانات الشخصية، إلا أن الإطار القانوني لاستخدام الذكاء الاصطناعي ما يزال في طور التطور والتشدد. توصي الدراسة بضرورة إعداد تشريع خاص بالذكاء الاصطناعي يتضمن ضوابط واضحة لمعالجة بيانات الشخصية ضمن أنظمة الذكاء الاصطناعي.

الكلمات المفتاحية: التحديات القانونية – الذكاء الاصطناعي – البيانات الشخصية – البيئة الرقمية.

Abstract:

Artificial intelligence has become one of the most prominent factors reshaping the concept of privacy in the digital age. The aim of this research is to shed light on the legal challenges arising from the use of artificial intelligence in processing personal data in the digital environment. The research relied on the use of a descriptive and analytical approach, which is based on collecting, analyzing, and interpreting information. Related to the subject of the study is the violation of the privacy of personal data in cyberspace. The study reached many results, including that within the framework of enhancing the protection of personal data in the Kingdom of Saudi Arabia, the Personal Data Protection System was issued by Royal Decree No. (M/19) dated 2/9/1443 AH, which is the regulatory basis for regulating the collection and use of data in the Kingdom. Several countries, such as Saudi Arabia, the UAE, and Egypt, have begun adopting national legislation to protect personal data. However, the legal framework for the use of AI is still in the process of development and crystallization. The study recommends the development of specific AI

legislation that includes clear controls for the processing of personal data within AI systems.

Keywords: Legal challenges – Artificial intelligence – Personal data – Digital environment.

المحتويات

الإهداء	3
شكر وفضل	4
ملخص	5
مقدمة	9
مشكلة البحث	10
أسئلة البحث	11
هدف البحث	12
أهمية البحث	12
منهج البحث	13
الدراسات السابقة	14
خطة البحث	17
الفصل الأول	17
الإطار النظري والمفاهيم والمفاهيم لبيانات الشخصية والذكاء الاصطناعي	17
البحث الأول: ماهية البيانات الشخصية	19
المطلب الأول: مفهوم البيانات الشخصية ارفقيه	20
المطلب الثاني: سمات البيانات الشخصية	23
المطلب الثالث: أنواع البيانات التي يجمعها النظام السعودي	27
البحث الثاني: أهمية الذكاء الاصطناعي وتطبيقاته في معالجة البيانات	30
المطلب الأول: المقصود بمفاهيم الذكاء الاصطناعي	31
المطلب الثاني: الطبيعة القانونية للذكاء الاصطناعي	32
المطلب الثالث: اتفاق مبادئ شريعات هذه البيانات الشخصية المعالجة بواسطة هذه الذكاء الاصطناعي	36
الفصل الثاني	43
التحديات القانونية المتعلقة بالذكاء الاصطناعي في معالجة البيانات الشخصية	43
البحث الأول: صعوبة الحصول على موافقة صريحة من الأفراد	45
البحث الثاني: ضمانات هذه البيانات الشخصية في النظام السعودي	53
المطلب الأول - ضمانات سابقة على معالجة البيانات الشخصية	54

المطلب الثاني: سمات معاصرة لنموذج القيادات الشخصية.....	57
المطلب الثالث: سمات لائحة نموذج القيادات الشخصية.....	60
المحلل الثالث.....	63
الأساس المنهجي منه خصائص معلومات في ظل تطبيقات الذكاء الاصطناعي في الملكية العربية السعودية.....	63
نموذج الأول: خصائص النظم المنهجي منه خصائص معلومات في ظل تطبيقات الذكاء الاصطناعي.....	65
المطلب الأول: مصادر جديد حق الخصوصية.....	
المعلوماتية.....	64
المطلب الثاني: النشاط الجزئي خاص مناهج القيادات الشخصية.....	71
المبحث الثاني: مستقبل التشريعات والسياسات التطبيقية للذكاء الاصطناعي.....	77
المطلب الأول: تنظيم القانون لخصائص الذكاء الاصطناعي في الملكية العربية السعودية.....	77
المطلب الثاني: النزوية المنية على خصائص الذكاء الاصطناعي.....	80
الخاتمة والدرج والتوصيات.....	86
نانياً: توصيات.....	87
قائمة المراجع والمصادر.....	88

المقدمة

أصبح استخدام الإنترنت أحد الوسائل المهمة ضمن وسائل تقنيات المعلومات التي ازداد استخدامها في كافة الوحدات والأجهزة بصفة عامة، مما أثر على أمن وسرية البيانات والمعلومات الشخصية، ومن هنا خلق قلق الإنسان في حماية بياناته الشخصية وعدم افشائها، لأنه عند حوشر وأساس حماية خصوصية الأفراد ضد الانتهاكات وعدم تدعى الغير فيها، وبذلك تتحقق مصلحة كل شخص في حماية بياناته الشخصية⁽¹⁾ ومع تزايد تعامل الذكاء الاصطناعي مع البيانات الحساسة، تزايد المخاطر التي تهدد الخصوصية والامتنان أصبح الذكاء الاصطناعي اليوم أحد مكانة بارزة في حياة الإنسان، نظراً لدرجة الفعالية في معالجة المشكلات وتقدم الحلول المبكّرة في مختلف المجالات، إذ تغلغل في العديد من القطاعات وأصبح جزءاً من الحياة اليومية من خلال تطبيقات متنوعة مثل المساعدات الصوتية، وألعاب المحتوى، والتربويات. وتعدّ الذكاء وعمرها، ومع ذلك، فقد أثار الذكاء الاصطناعي حزمة من القضايا المتعلقة بحقوق الإنسان، وعلى وجه الخصوص الحق في الخصوصية. إذ تتمكّل التطبيقات الذكية الحديثة، وأيضاً هذا الحق الذي تكفله القوانين والمواثيق الدولية والأديان⁽²⁾.

ونتيجة لأهمية خصوصية المعلومات الشخصية للأفراد بشكل عام، وخصوصية البيانات والمعلومات الشخصية في ظل التحول الرقمي والفضاء الإلكتروني، تعدّ الخصوصية من أهم الحقوق المصنفة بالإنسان، وقد حظي هذا الحق باهتمام متزايد من قبل الأمم المتحدة ومجلس حقوق الإنسان وألجاناً مختلفة، حيث تم تكريسها منذ وقت مبكر في الإعلان العالمي لحقوق الإنسان لعام 1948. ثم في العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966 بموجب المادة (17)، ومع تطور التكنولوجيا وظهور مفهوم الخصوصية المعلوماتية أو البيانات الشخصية الرقمية، ازداد الاهتمام العالمي بضرورة حماية هذا الحق في البيئة الرقمية الحديثة⁽³⁾.

¹ محمد، مود، جيب، (2018)، أبحاث العمليّة الحق في الخصوصية، مجلة دراسات قانونية وسياسية، السنة السادسة، العدد المئوي عشر، ص 166.

² شياي، عبد الله، مود، (2023)، حق الخصوصية المعلوماتية في ضوء مبدأ الأخصائي، مجلة دراسات القانونية والسياسية، مج 6، ص 458.

⁽³⁾ - وحدة الأبحاث لمؤسسة حرية الفكر والتعبير، (2021)، الأبحاث والتعبير، في مصر (حرر كلاً: خصوصية الرقمية)، ملحق المؤتمرات - حرة الفكر والتعبير، ص 4.

وفي هذا الإطار، أصبح الذكاء الاصطناعي أحد أبرز العوامل التي تُعيد تشكيل مفهوم الخصوصية في العصر الرقمي. مع الاعتماد المتزايد على جمع البيانات الشخصية للتحسين المستمر للأداء والمنتجات والخدمات، يبرز إشكاليات قانونية معقدة تتعلق بمدى مسؤولية جمع هذه البيانات ومعالجتها وتخزينها ومشاركتها. فبينما تسعى الأنظمة الذكية إلى تحسين جودة الحياة والخدمات المقدمة للأفراد، فإنها في المقابل تُشجّع تحديات جديدة أمام المستهلكين والجهات الرقابية. خصوصاً فيما يتعلق بتحديد المسؤولية القانونية عن انتهاك الخصوصية أو إساءة استخدام البيانات. وكذلك مدى كفاية الأطر التشريعية الحالية في مواجهة هذا التطور السريع. ومن هنا تسعى من خلال البحث تحليل التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في معالجة البيانات الشخصية في بيئة الرقمنة، وتقديم حلول قانونية تضمن الاستخدام الآمن والمسؤول للذكاء الاصطناعي، بما يحقق التوازن بين التقهنة التكنولوجية وحماية خصوصية الإنسان وكرامته الرقمية.

مشكلة البحث.

مع بداية الألفية الثالثة مر العالم بمرحلة في التكنولوجيا المعلومات والاتصالات، التي أثرت على كافة فروع العلم والمجالات الحياة بوجه عام، وفروع القانون بوجه خاص. حيث ساهمت هذه التمرّد بشكل واضح في سهولة التبدّل والتوصّل إلى المعلومات والاتصال الفوري. مما فرض ذلك تحدي كبير وعصر في نفس الوقت، فعلى الرغم من الامتيازات التي وفّرتها لمستخدميها، إلا أن هذه التقنيات دائماً ما تُحمّل إنجازات ومسيئيات، كمثل حق الفرد في الخصوصية من أهم الحقوق الأساسية التي كفلتها الدساتير للفرد داخل كل مجتمع. أن هذا التطور التكنولوجي قد وضع خصوصية في مركز حساس يُعده أكثر عرضة للانتهاك والاستغلال⁽⁴⁾. فالتالي بعد ذلك الحق في خصوصية البيانات الشخصية للأفراد من أكثر الحقوق تراخاً بالخصوصية القانونية للإنسان وأحد هذه الحقوق التي تتمتع بالكرامة.

وفي ظل التطور المتسارع للتكنولوجيا الرقمية. بات الذكاء الاصطناعي يشكل محوراً رئيسياً في العديد من التطبيقات التي تعتمد على جمع ومعالجة وتحليل البيانات الشخصية، وهو ما أدى إلى نشوء بيئة رقمية شديدة التعقيد من حيث حجم البيانات وسرعة تدفقها وتنوع مصادرها. وبينما وفّر هذا التحول فرصاً غير مسبوقة

⁴ عربي- روني، معناه، (2021)، حماية شخصية الحق في الخصوصية المعلوماتية (دراسة مقارنة)، محمد عبد الله بن عبد الله (مراجعة) ومعرفة أبحاث علمية، عدد 1، العدد الثاني، الجزء الأول، ص 1025.

لتحسين الخدمات، وتعظيم الكفاءة، وتحقيق تصور نوعي في القطاعات المختلفة، برزت في المقابل إشكاليات قانونية متزايدة تتعلق بكيفية تنظيم هذه العمليات وحمايتها عند انتهاك الحقوق الأساسية للأفراد، وعلى رأسها الحق في خصوصية وحماية البيانات الشخصية.

وفي ضوء ما تقدم، تمثل مشكلة البحث في أن الاستخدام المتنامي لتقنيات الذكاء الاصطناعي في معالجة البيانات الشخصية داخل البيئة الرقمية في المملكة العربية السعودية، رغم ما يتجنى من فرص تنمية ورقمية واعداً، قد أفرز تحديات قانونية معقدة تجعل مدى كفاية الأطر التشريعية والتنظيمية القائمة لحماية الخصوصية وحمايا الاستخدام مسؤول لتلك البيانات، تمنع توسع تطبيقات الذكاء الاصطناعي في مجالات حكومية والتجارية والخدمات، أصبحت مسألة تحديد المسؤولية القانونية عن إساءة استخدام البيانات أو تعريضها أو معالجتها دون موافقة صريحة من أصحابها مسألة مثيرة للجدل. كما يثير هذا الصور تعقيدات حول مدى نجاح التشريعات السعودية، كقانون حماية البيانات الشخصية الصادر عام 2021، مع المعايير الدولية الحديثة في هذا المجال، ومدى قدرتها على موازنة التطور التقني السريع مع حماية حقوق الأفراد في الخصوصية الرقمية. ومن ثم، تعد إشكالية هذا البحث من السعي إلى فهم التحديات القانونية القائمة وتقييم فعالية الإطار النظامي السعودي في مواجهة تحديات الخصوصية والأخلاقية الناجمة عن استخدام الذكاء الاصطناعي في معالجة البيانات الشخصية، واقتراح سبل الكفيلة بعزيز حماية القانونية في ضوء التحولات الرقمية المتسارع.

أسئلة البحث:

السؤال الرئيسي : ما هي التحديات القانونية القائمة عن استخدام الذكاء الاصطناعي في معالجة البيانات الشخصية في البيئة الرقمية ؟

وينفرد من هذا السؤال التالي:

- 1- ما هو الإطار التنظيمي والقانوني للبيانات الشخصية والذكاء الاصطناعي؟
- 2- ما هي التحديات القانونية المتعلقة بالذكاء الاصطناعي في معالجة البيانات الشخصية؟
- 3- ما هو الأساس القانوني لحماية خصوصية المعلومات في ظل تطبيقات الذكاء الاصطناعي في المملكة العربية السعودية؟

هدف البحث :

هدف البحث لتبسيط المسألة حول التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في معالجة البيانات الشخصية في البيئة الرقمية. ومن أجل تحقيق هذا الهدف يسعى البحث لمعرفة التالي:

- 1- الإطار المفاهيمي والقانوني للبيانات الشخصية والذكاء الاصطناعي.
- 2- التحديات القانونية المتعلقة بالذكاء الاصطناعي في معالجة البيانات الشخصية.
- 3- الأسس القانونية لحماية خصوصية المعلومات في ظل تعقيدات الذكاء الاصطناعي في المملكة العربية السعودية.

أهمية البحث.

تشكلت الذكاء الاصطناعي دور هام في المجتمع من خلال مدى مساهمتها الفعالة في مزاكية التطورات التكنولوجية الحديثة على مستوى كافة المجالات. وبالتالي دورها في تقديم ورفقي المجتمعات. كما أن هذا النموذج التكنولوجي قد وضع الخصوصية في مركز حساس فعند أكثر عرضة للانتهاك والاستغلال⁽⁵⁾. فبالإضافة إلى ذلك الخلل في خصوصية البيانات الشخصية للأفراد من أكثر الحقوق انتهاكاً بالشخصية القانونية للإنسان وأيضاً، هذا الخلل الذي يتعلق بالكرامة، كما أن المؤتمر الرئيسي عند قياس مدى تحضر الأمم ورفقيها، وذلك من خلال جملة من الجوانب (المادية والمعنوية) الخاصة بشخصية الإنسان ومدى علاقته الموثقة وتداعيه الشديد بالحقوق والخبرات الأخرى وتعرض المجتمعات على احترامه، وأهميته حقاً مستقلاً قائماً بذاته. وبذلك تعد الدول والهيئات مسئولة عن حماية ذلك الحق من الانتهاك من خلال القيام بالعمل على وضع ضمانات جديدة تخفف من خطر الواقع على انتهاك خصوصية بيانات الشخصية في ظل تطبيق والاعتماد على تقنيات الفضاء الإلكتروني .

⁵ عربي، روني، سعود، (2021)، خدمات خدمة العملاء المحرك بالذكاء الاصطناعي، مجلة كلية الدراسات الإسلامية والعربية لبيروت، عدد 145، ص 1025.

أصبحت قضية أمن وحماية البيانات والمعلومات الشخصية في ظل تطبيق تقنية انقضاء الإلكتروني من أحد قضايا العصر، لذا يتم تسليط الضوء على دور التشريعات الدولية في حماية الحق في خصوصية بيانات الشخصية للأفراد في ظل تطبيق تقنيات انقضاء الإلكتروني. وبذلك تكون صياغة مشكلة البحث في الثاني

تتبع أهمية هذا البحث من كونه يتناول موضوعاً حديثاً وحيوياً في الوقت ذاته. يتناول في التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في معالجة بيانات الشخصية في بيئة الرقمية، وهو موضوع تزايد أهميته مع تسارع التحول الرقمي الذي تشهد المملكة العربية السعودية ضمن رؤية (2030)، التي تعتمد بشكل متزايد على البيانات والتقنيات الذكية في تطوير الخدمات الحكومية والاقتصادية والاجتماعية، وتبرز أهمية الدراسة من الناحية العلمية في سعيها إلى تحليل الإطار القانوني السعودي المنظم حماية بيانات الشخصية، ولا سيما في ظل صدور نظام حماية البيانات الشخصية لعام 2021. ويبيان مدى كفايته في مواجهة التطورات التقنية المرتبطة بالذكاء الاصطناعي. فضلاً عن رصد توجه المصوّر التشريعي والعملية التي قد تأخذ من فعاليتها في حماية الخصوصية الرقمية للأفراد.

تأما من الناحية العملية، فتجسّد أهمية البحث في أنه يسعى إلى تقديم مقترحات تشريعية وتنظيمية تعزز من فعالية المنظومة القانونية في المملكة، بما يضمن الاستخدام الآمن والمسؤول لتقنيات الذكاء الاصطناعي، ويحقق التوازن بين متطلبات الابتكار التقني وحماية الحقوق الفردية، وعلى رأسها الحق في الخصوصية. كما يساهم هذا البحث في دعم صانع القرار والمشرعين السعوديين بتوصيات عملية تمكن الامتداد إليها تطوير التشريعات الرقمية، بما يتوافق مع المعايير الدولية ويؤكد التحولات المستقبلية في مجال الذكاء الاصطناعي وحوكمة البيانات.

منهج البحث :

اعتمد البحث على استخدام منهج الوصفي التحليلي، الذي يقوم على تجميع وتحليل وتفسير المعلومات المتعلقة بموضوع الدراسة بهدف استخلاص خصوصية بيانات الشخصية في انقضاء الإلكتروني، وذلك من خلال الاضلاع على مراجع علمية متخصصة، المقالات العلمية العربية والأجنبية، والمذكرات الأكاديمية والمؤتمرات العلمية، والقوانين واللوائح والقرارات الوزارية، والكتب الثانوية المتعلقة بموضوع البحث، من أجل التوصل إلى أفضل قدر من النتائج والمقترحات.

الدراسات السابقة.

دراسة موسى وفريد (2025) التحديات القانونية لحماية البيانات الشخصية في سياق الذكاء الاصطناعي. هدفن الدراسة التعرف على طبيعة التحديات القانونية التي تتعلق بالحماية القانونية لبيانات الشخصية في عصر الذكاء الاصطناعي، واعتمدت الدراسة على المنهج الوصفي التحليلي، وتوصلت الدراسة إلى الاعتماد على قانون التعلم الآلي التي يتم بها تقنيات الذكاء الاصطناعي له سمات أخرى فالعالم الحديث بات اليوم ضمن مسارات هذه التقنيات في خلق ماضي معروفة وفي أدق تفاصيلها مساهمة بشكل كبير في تطور المجتمع وتحسين حياة الأفراد، توصي الدراسة بضرورة وضع أسس قانونية خاصة تنظم أحكام المسوية القانونية الجديدة لتطبيقات الذكاء الاصطناعي، ويتم إخراجها ضمن مسئولية المدين الخاصة⁶.

دراسة السعيد (2024) بحوث تقنية الذكاء الاصطناعي وحماية البيانات الشخصية – دراسة مقارنة. هدفن الدراسة لتسليط الضوء على تأثير تقنية الذكاء الاصطناعي على حماية بيانات الشخصية، واعتمدت الدراسة على المنهج التحليلي لخصائص الاتحاد لحماية البيانات الصادرة عن الاتحاد الأوروبي عام 2016 لبيان حقيقة العلاقة القانونية بين تقنيات الذكاء الاصطناعي وضرورة الحماية القانونية لبيانات الشخصية، وتوصلت الدراسة لعدم اتفاق الآراء على تحديد المقصود بتقنيات الذكاء الاصطناعي بسبب انشغال المفسرين والملاحق لتكنولوجيا المعلومات، إلا أن هذه الآراء تفق على أن هذه التقنيات بقصد استخدامها الآلة الحديثة بطريقة ممتدة لعمل بشري. وتوصلت الدراسة لتبرع المبرر بضرورة مواكبة التطورات التقنية من خلال إصدار التشريعات المناسبة لتوفير الحماية لبيانات الشخصية التي تستخدمها تقنية الذكاء الاصطناعي⁷.

⁶ موسى، عمر، وفريد، معوي، محمد، (2025)، تحديات الحماية لبيانات شخصية في سياق الذكاء الاصطناعي، مجلة معوي، نوع حق فكري وإبداع.

⁷ السعيد، محمد، حمدي، (2024)، تقنية الذكاء الاصطناعي وحماية البيانات الشخصية – دراسة مقارنة، مجلة آتس بعاد وعالم، ج

دراسة خيباني وبن ساد (2023) بعنوان حق الخصوصية المعلوماتية في ضوء الذكاء الاصطناعي. هدفت الدراسة لتعريف على محاور مرتبطة بأنظمة الذكاء الاصطناعي بشكل سريع في حياتنا اليومية. واختتمت الدراسة على النهج الوصفي التحليلي بوقوف على مفهوم الحق في الخصوصية وأخير التصور القانوني المتحققة المرتبطة بالمشروع، وتوصلت الدراسة أن استخدام الذكاء الاصطناعي دون رقابة وضوابط قانونية يعد خطراً يهدد خصوصية الأفراد وقد يؤدي إلى استخدام بياناتهم في ارتكابات جرمية أو في تطوير كيانات ذكية تعبر عن الإنسان. واقترحت الدراسة ضرورة العمل على اتخاذ إجراءات قانونية صارمة لحماية حقوق الإنسان ضماناً لسلامة بياناتهم.

دراسة حميسي (2019) بعنوان "التحديات القانونية في حماية البيانات الشخصية في أعضاء الرقعة"، هدفت إلى بيان أهم القضايا التي يفرها القانون لحماية الأفراد الطبيعيين في ظل الاعتماد المتزايد على تقنيات الفضاء الرقمي. عكست الدراسة إلى ضرورة أن تتم معالجة البيانات الشخصية بطريقة مشروعة وبنية تضمن احترام الحياة الخاصة للأفراد والحفاظ على سريتها من أي تعدي أو اختراق. وجمع استخداماً بوسائل غير قانونية، كما أكدت على أهمية وضع ضمانات قانونية واضحة تحل استخدام هذه البيانات في الأغراض التي جُمعت من أجلها فقط. وفي إطار أحكام القانون المتوافقة صراحة ومسبقاً من استخداماً بما يحقق التوازن بين منصات التطور التقني وحماية الحق في الخصوصية.

دراسة كريكف (2019) بعنوان "حق الخصوصية استخدام الفضاء الرقمي: التحديات والحلول"، هدفت إلى التعرف على أبرز التحديات والمخاطر التي تواجه خصوصية المستخدمين في بيئة الفضاء الرقمي. والتي تعبر أساساً في سوء استخدام البيانات الشخصية واستغلالها لأغراض تجارية أو مادية أو غيرها من الأغراض غير المشروعة. وقد خلصت الدراسة إلى ضرورة إقرار تدابير قانونية صارمة تشكل أداة وقائية وتنظيمية لحماية الخصوصية الرقمية. باعتبار أن التشريعات الوطنية على المؤسسة المراجعة لأي سلوك يمس حقوق الأفراد وحرياتهم. كما أكدت الدراسة على أهمية رفع الوعي الرقمي لدى المستخدمين واتخاذهم من المخاطر التي قد

⁸ خيباني، عبد الله، ساد بن ساد، (2023)، حق الخصوصية المعلوماتية في ضوء الذكاء الاصطناعي، مجلة الدراسات القانونية والاقتصادية، مج 6، ص 2.

⁹ حميسي، رضا، (2019)، قضايا الحقوق في حماية البيانات الشخصية في عصر الرقعة، المؤتمر الدولي الثاني للدراسات القانونية والاقتصادية، كلية الشريعة والدراسات الإسلامية، جامعة الزيتونة، تونس.

يعرضون هذا أثناء استخدام تطبيقات ومواقع الفضاء الرقمي. كما يسهم في تعزيز ثقافة الأمان والخصوصية في البيئة الرقمية¹.

التعليق على الدراسات السابقة

بعد عرض ملخص الدراسات السابقة تبين وجود اهتمام عني مستوى الباحثين والأكاديميين بموضوع حماية بيانات الشخصية في الذاكرة الاصطناعي. فقد مثلت هذه الدراسات إسهامات مهمة في موضوع العلاقة بين البيانات الشخصية والفضاء الرقمي أو الذاكرة الاصطناعي أو الخصوصية، فإن موسى وفريد ركزت على التحديات القانونية لبيانات الشخصية في سياق الذاكرة الاصطناعي. بينما السعيد قسّمت الدراسة مقارنة بين تشريعات استخدام الذاكرة الاصطناعي وحماية البيانات. وغياي وبين ساء تناولت حق الخصوصية التعديلية في الذاكرة الاصطناعي. أما حمسي فكتفت عن الضمانات القانونية لحماية البيانات الشخصية. وكر يكتف تناول المخاطر والتحديات التي تواجه الخصوصية في الفضاء الرقمي ورغم هذا النوع، فعالية هذه الدراسات لم تركز بصورة كافية على النموذج التشريعي السعودي أو على التفاعل بين الذاكرة الاصطناعي ومعالجة البيانات الشخصية في البيئة الرقمية في القانون المحلي. كما أن بعض الدراسات اقتصرت على تحليل نصوحي تشريعي أو مقارنة بين دول محددة، دون تغطية شاملة لمفهوم «المسؤولية القانونية الجديدة» أو تركيز على ما يترتب على الذاكرة الاصطناعي من التحديات التنظيمية في بيئة رقمية متقدمة.

وبناء على ذلك يتميز البحث الحالي بأنه يخصص لسياق السعودي. إذ يوجه النظر إلى «التحديات القانونية الناشئة عن استخدام الذاكرة الاصطناعي في معالجة بيانات الشخصية في البيئة الرقمية في القانون السعودي»، وهو مجال لم يُناقش بعمق في الدراسات السابقة. كما أن البحث يركز على الذاكرة الاصطناعي بمحده الواسع (المنموذج، القرار الآلي، معالجة البيانات الضخمة، تقنيات الذكاء (وليس فقط على بيانات الشخصية في الفضاء الرقمي التنفيذي. مما يجعله أكثر حداثة ومسايرة للتجولات التقنية.

¹ الكركس، عائشة، (2019)، حق شخصية مستخدم الفضاء الرقمي: ملخص وتحديات، بحث خبير لمعهد الاقتصاد الرقمي والابتكار، العدد 18، العدد الثاني.

خطة البحث:

من أجل تحقيق أهداف البحث وحل مشكلته تم تقسيم البحث إلى التالي:

الفصل الأول: الإطار المفاهيمي والقانوني للبيانات الشخصية والذكاء الاصطناعي.

الفصل الثاني: التحديات القانونية المتعلقة بالذكاء الاصطناعي في معالجة البيانات الشخصية.

الفصل الثالث: الأساس القانوني لحماية خصوصية المعلومات في ظل تصنيفات الذكاء الاصطناعي في المملكة العربية السعودية.

الفصل الأول:

الإطار المفاهيمي والقانوني للبيانات الشخصية والذكاء الاصطناعي

المقدمة.

يشهد العالم في الوقت الراهن ثورة رقمية شاملة يفوقها الذكاء الاصطناعي. الذي أصبح يتسكن أحد أبرز محركات التنمية لتطور في مختلف مجالات الحياة، فقد باتت تقنياته تلعب دوراً محورياً في إعداد تشخيص أمراض القلب والانسحاب الصناعي الشري. حيث تخضع تطبيقاته في شتى القطاعات الحيوية من التعليم والصحة والصناعة والاتصالات والخدمات الحكومية وغاية، إلى امتدادات تشمل تفاصيل الحياة اليومية للأفراد. فمن خلال آليات الذكاء التي تدار بأنظمة قادرة على التحكم بالطاقة والأمن والراحة، إلى أنظمة الأتمتة التي تسهم في رفع كفاءة الإنتاج الصناعي وتقليل الأخطاء البشرية، ومن الترميزات الشخصية التي تقدمها منصات رقمية تحسن تجربة المستخدم إلى روبوتات الترددية التي توفر خدمات فورية وتفاعلية، أصبح الذكاء الاصطناعي جزءاً لا يتجزأ من الحياة المعاصرة. مؤثراً في كل جانب منها تقريباً¹¹.

ويجود هذا الانتشار الواسع إلى النمو السريع الذي تشهده تكنولوجيا الذكاء الاصطناعي بفضل الاعتماد المتزايد على البيانات بوصفها مورد الخيوي الذي يعاين أنظمة ويريد من قدراتها على التحم والتصور، فكل عملية يقوم بها الذكاء الاصطناعي تعتمد على تحليل كميات ضخمة من البيانات المجمعة من مصادر متعددة.

¹¹ صديري، أحمد، عبد عجاج حمدي، (2021)، ذكاء الاصطناعي ونظيره في نظم الإدارة العامة، في: مقترحة، جامعة لأهر كية لدراسات القاهرة، الطبعة الأولى، العدد 192، الجزء 2، ص 479.

سواء من سبوت المستخدمين، أو أجهزة الاستشعار، أو المعاملات الإلكترونية، أو البيانات المنشوعة على شبكة الإنترنت، ومع استمرار تطور هذه التقنيات، تزداد الحاجة إلى جمع المزيد من البيانات المنشوعة والذقية، مما يمكن أنظمة الذاكرة الاصطناعي من تقديم أداء أكثر كفاءة ونتائج أكثر موثوقية. غير أن هذا الاعتماد الكبير على البيانات يثير في المقابل مخاوف أمنية وأخلاقية بالغة الأهمية. إذ يؤدي تخزين كميات هائلة من المعلومات، ولا سيما البيانات الشخصية، إلى احتمالية تعرضها للاختراق أو التسريب أو الاستخدام غير المشروع، ومن ثم فإن الذاكرة الاصطناعي يُعد سلاحاً ذا حدين، فهو من جهة يشكل أداة قوية لتصور والابتكار. ومن جهة أخرى قد يتحول إلى مصدر تهديد الخصوصية والأمن إذا أسيء استخدامه أو أُلحقت ضوابطه القانونية والأخلاقية¹⁴.

ويرجع هذا المخاطر. فإن الذاكرة الاصطناعي تمتلك القدرة على أن يكون جزءاً من الحل وليس المشكلة، بفضل إمكاناته المتقدمة في تحليل البيانات الضخمة والتعرف على الأنماط والتحديات الأمنية بدقة وسرعة تفوق القدرات البشرية. ومن هذا المنطلق، بدأت العديد من المؤسسات والشركات حول العالم في تبني الذاكرة الاصطناعي كترسيمة فعالة لحماية بياناتها الحساسة والشفافية، مستفيدة من قدراته في الكشف المبكر عن محاولات الاختراق والتنبؤ بالمخاطر الأمنية المحتملة. إذ يمكن لأنظمة الذاكرة الاصطناعي والتعلم الآلي تحليل كميات هائلة من البيانات ودراسة أنماط القرصنة والتهديدات. الأمر الذي يساعد على تطوير آليات دفاعية أكثر تطوراً ومرونة. كما تستطيع هذه الأنظمة مراقبة الأنشطة لشبكة بشكل مستمر والتعرف على التسلوكيات غير المعتادة والإبلاغ عنها فوراً، مما يتيح التدخل السريع مع الأضرار قبل وقوعها¹⁵.

وبذلك يتحول الذاكرة الاصطناعي من مجرد تكنولوجيا تعتمد على البيانات إلى أداة قادرة على حمايتها وحفظها، يصبح عنصراً أساسياً في منظومة الأمن السيبراني الحديثة. ومع هذا التحول المتسارع، تبرز الحاجة الملحة إلى وضع أطر قانونية وأخلاقية واضحة تضمن الاستخدام المسؤول لتقنيات الذاكرة الاصطناعي، والحفاظ

¹⁴ الخالدي، ياسر حبيب، 1442هـ، حركة متجددة لذاكرة اصطناعي في العصر الرقمي، في مجلة الأبحاث في العلوم الإنسانية، العدد 144، ص 1027.

¹⁵ إبراهيم، محمد، فتحي محمد، خطبة تحت عنوان "تطبيقات ذاكرة الاصطناعي، محلة سموات المدينة و"العدد 144، ص 1027.

على التوازن بين متطلبات التطور التكنولوجي وحقوق الأفراد في الخصوصية والأمان. بحيث يُستفاد من حدود التكنولوجيا في خدمة الإنسانية دون الإضرار بالقيم الأساسية التي يقوم عليها المجتمع الرقمي.¹⁴

وتنقل ارتقى اندكاء الاصطناعي بتأثيره على نقاط النهاية إلى مستوى جديد من خلال تحليل كميات الإلكترونية وكيفية وحفظها بسرعة استناداً إلى دراسة سلوكية شاملة. يعتمد اكتشافات الخدمات الإلكترونية عادةً على الأنماط. ويمكن لاندكاء الاصطناعي أن يكون مفيداً للغاية في دراسة البيانات الخفية لتعرف على الأنماط المتخفية والتأثير في البيانات الجديدة.

البحث الأول: ماهية البيانات الشخصية

تُعدّ البيانات الشخصية تركيزاً أساسياً التي يمكن من خلالها التعرف على هوية الأفراد بدقة، سواء بطريقة مباشرة أو غير مباشرة. وتشمل هذه البيانات مجموعة واسعة من المعلومات مثل الأسماء وأرقام الهوية، بيانات ممتلكات، وغيرها من التفاصيل التي تميز كل شخص عن غيره. ونظراً لارتباطها الوثيق حياة الفرد وحرية. فإنها تُعدّ ذات طابع خاص من الخصوصية والحساسية، ومع انتشار التمييز في التطور التكنولوجي واستثمار الأجهزة الرقمية والشبكات الإلكترونية، ازدادت مخاطر تعرض هذه البيانات للتهجمات والاختراقات. إذ قد يتمكن القرصنة أو الجهات غير المصرح بها من الوصول إلى قواعد بيانات تحوي على معلومات حساسة، مما يؤدي إلى استغلالها في أعمال الإضرار، أو سرقة الهوية، أو لأغراض تجارية غير مشروعة، ولا يقتصر الأمر على الأفراد وحسب، بل يمتد ليشمل الأمن الاجتماعي والسياسي والاقتصادي للبلد. حيث يمكن أن يؤدي انتهاك الخصوصية إلى تماسخ بالحقوق السياسية أو الإساءة لسمعة الأشخاص داخل المجتمع.¹⁵

من هذا المنطلق، يصبح من الضروري إدراك أهمية البيانات الشخصية من منظور أخلاقي. فهي لا تُعد مجرد معلومات تُجمع وتُحزن وتُدار، بل هي حقوقاً أساسية يجب صياداً وحمايتها بكل الوسائل القانونية والفنية المتاحة. وينصب ذلك وضع أطر تشريعية وتنظيمية واضحة تُظمّ عمليات جمع البيانات ومعالجتها وتخزينها ومشاركتها، بما يضمن احترام إرادة الأفراد وحقوقهم في التحكم في معلوماتهم الشخصية. كما ينبغي أن يُشترط

¹⁴ مقال منشور على موقع "مشرق" عن الإنترنت، عنوانه: كيف يمكن اندكاء الاصطناعي أن يساعد في حماية البيانات الشخصية والمخترع، تاريخ الإصدار: 2025/10/23.

¹⁵ أستاذة، د. حنا حيدر حيدر، 2025، مفهوم بيانات الشخص وحمايتها، بحث منشور في المجلات، مع 25، 2،

المختصون على مرفقة حراسة من صاحب البيانات قبل استخدامها، مع تحديد الأفراد المسموح بها هذا الاستخدام. ووضع آليات صارمة مساءلة من يتجاوز أو يسيء استخدام هذه البيانات أو ينتهك الخصوصية. وفي جانب ثالث، يجب العمل على رفع مستوى الوعي المجتمعي بأهمية حماية البيانات الشخصية، بحيث يترك الأفراد حقوقهم وسبل حماية معلوماتهم. ويصبحوا أكثر قدرة على التعامل مع مخاطر والتحديات التي قد تواجههم في بيئة الرقمية الحديثة¹⁶.

المطلب الأول: مفهوم البيانات الشخصية الرقمية

تشير البيانات الشخصية الرقمية إلى مجموعة المعلومات المرتبطة بالأفراد، والتي يتم جمعها ومعالجتها عبر الوسائل الرقمية والتقنيات الحديثة. وتشمل هذه البيانات معلومات أساسية مثل الاسم والعنوان، بالإضافة إلى بيانات أكثر حساسية، كالمعلومات الصحية، والمالية، والمهنية، فضلاً عن الصور الشخصية ومقاطع الفيديو، وتولد هذه البيانات نتيجة لأنشطة الأفراد على شبكة الإنترنت، مثل استخدام منصات التواصل الاجتماعي، وتصفح مواقع الإلكترونيات، والتسوق عبر الإنترنت، واستخدام التطبيقات الذكية. وتؤدي هذه الأنشطة إلى إنتاج كميات ضخمة من البيانات، التي يمكن توظيفها في مجالات متعددة، منها استخدام الإعلانات، ولهي المسنوك الاستهلاكي. وتعرض البحث والسحب¹⁷.

ومع التوسع المتزايد في جمع واستخدام بيانات الشخصية الرقمية، أصبحت قضايا الخصوصية والأمن الرقمي من أبرز التحديات التي تواجه الأفراد والمؤسسات. ومن ثم، فإن على المؤسسات واتحادات اتخاذ تدابير مناسبة لحماية هذه البيانات وضمان استخدامها بشكل قانوني وآمن. كما يكفل احترام حقوق الأفراد في الحفاظ على خصوصيتهم وسلامتهم الرقمية.

أولاً: التعريف اللغوي

¹⁶ عيسى، أماني، *مدى اعتماد*، ص 2125. ومعه رغبة خدمة بيانات الشخصية، دراسة مقدمة، عرض محو

والترجمة، ص 25، 2.

¹⁷ عمار، طارق، (2017)، *تحديات الحماية للحياة الخاصة عبر الإنترنت*، دراسة مقدمة لجامعة القاهرة، كلية الحقوق، جامعة محمد

حضر، ص 81.

وفي المقابل فإن المصطلح المقابل في اللغة اللاتينية هو (DATUM) والتي يقصد بها شيء معطى أو مسدود، أو شيء ما يعرف أو مسدود بنسخه كتحقيق أو واقعة. وتقالها في اللغة الإنجليزية كلمة (DATA) والتي تعني حقائق التي تشير أو تصف موضوعا ما، أو فكرة، أو حالة أو أية عناصر أخرى إلخ.

ثانياً: التعريف الاصطلاحي

يُستخدَم مصطلح "نبييات" بشكلٍ واسع للإشارة إلى مجموعة من الخلفاء أو الأئمة أو الرموز التي تُعبّر عن موضوع معين أو حالة ما. وتشكّل الأساس الذي تُبنى عليه المعلومات. وقد وردت نبييات تعريفات متعددة في النجاشي المتخصصة في المكليات. تكّنه جيا معلومات. الاتصال³.

بعضي منهم الموسوعي فخصصناهم المنكبات والنعومات. نعرف البيانات بأنها مصطلح عام يستعمله للإشارة إلى أي من حقائق أو الأرقام أو الحروف أو الرموز، أو إلى حقائق تصف موضوعاً أو فكرة أو حالة أو شيء خواص أخرى. ويشمل هذا المفهوم للعناصر الأساسية للبيانات التي تسج من معالجة البيانات بواسطة الحاسب.

أما في معمل المضخات وتكنولوجيا المعومات والاتصال، فتحت بيانات النخبات حواء أو الأملية التي
تحتفظ بها أو نشاط معين، وهي بذلك تتكسر الأسس الذي بني عليه التحديد أو اتخاذ القرار.

¹⁸ زمری محمدی، *ان کے بارے میں*، 1987ء، نکل، ص 12۔ خیر، ص 290۔

¹⁹ محمد بن عبد الله بن عبد الوهاب، 2016: 5، نسخة محفوظة من مكتبة جامعة القاهرة، 2024.

جميعه. العدد 2017). الخدمة الخاصة بخدمات الحاسب (أ.م.م. ممدوح محمد د. الخدمة الخاصة بخدمات الحاسب (أ.م.م. ممدوح محمد د. 86

¹ عفاة بنت عبد الله بن عمر بن الخطاب، عمدة بني أسد، من بني أسد بن زيد بن كنانة بن خزيمة بن مدركة بن إلياس بن مضر بن نضلة بن معد بن عدنان.

في حين يعرفها قاموس الكمبيوتر العربي بأنها "تتمة معلومات أو بيانات. هذا المصطلح، التي تمت معالجتها أو زيادة معالجتها بواسطة الحاسوب". وتشتمل عمليات من التصنيف أو التجميع أو التخزين أو إجراء الحسابات.

كما توصف البيانات بأنها "التحسين أو العرض الاتفاقي لمعلومات في شكل معين، لتسهيل معالجتها والاعتماد عليها".⁸⁶

وفي تعريف آخر، تعرف البيانات بأنها "مجموعة من الحقائق أو القياسات أو المصطلحات، التي تتخذ شكل أرقام أو حروف أو رموز أو أشكال خاصة، وتغير عن فكرة أو موضوع أو حدث أو هدف معين"، ولذا لم فهي تعد بمثابة المادة الخام التي تحول من خلال الحاسوب إلى معلومات مفيدة.⁸⁷

تعرف البيانات أيضاً بأنها مجموعة من الحقائق التي تعبر عن مواقف أو أفعال معينة. سواء تم التعبير عنها بالكميات أو الرموز. وتعد البيانات، في صورتها الأولية، غير ذات فائدة عملية ما لم تخضع لتحويل أو لمعالجة. ومن هنا تبرز الحاجة إلى تطبيق عمليات حسابية أو منطقية عليها من أجل استخراج المعلومات اللازمة فيها. ونعني آخر، فإن البيانات تُعالج لتستخلص منها معلومات مفيدة. حيث تؤدي هذه المعالجة إلى تحويل البيانات الخام إلى معلومات ذات معنى ودلالة.

وعليه، يمكن القول إن المعلومات هي الناتج النهائي لمعالجة البيانات. سواء من خلال التحليل أو التركيب. لاستخلاص ما تتضمنه البيانات من مؤشرات أو علاقات أو منطقات أو كليات أو موريات أو معدلات وغيرها من الأبعاد ذات الدلالة.

والخلافاً من هذا التحصير، تُعهم البيانات على أنها حقائق أولية غير منظمة ولا تمتلك قيمة بذاتها، ولا خفاء قيمة عليها، لا بد من إخضاعها لمعالجة، والتي تعد الوسيلة الأساسية لتحويلها إلى معلومات مفيدة وقابلة للاستخدام.

ثالثاً: مفهوم البيانات الشخصية في النظام السعودي

⁸⁶ خالد محمد محمد، (2012)، فكرة خدمة المراجع جامد، (د)، جامعة خنيدة لت، الإسكندرية، مصر، 61.

⁸⁷ س.أ. محمد عبي، (مصحح حسن، عبد، 2007)، حزمة معلوماتية، خد مطلوب عين محمد جامعة، بن، مصر، 141، (عدد 2)، ص 86.

في إطار استمرجات الاعتماد في التمسك بحرية السعودية. عرّف النظام بيانات الشخصية بأنها: "كل بيان - بغض النظر عن مصدره أو شكله - يمكن أن يؤدي إلى التعرف على الفرد بشكل محدد. أو جعل من التمسك التعرف عليه بصورة مباشرة أو غير مباشرة".¹⁴ ويشمل هذا التعريف مجموعة واسعة من البيانات، مثل الاسم، ورقم هوية، والعناوين، وأرقام الاتصال، وأرقام الترخيص والسجلات والتمسكات، وحسابات البريد، والبيانات الائتمانية، بالإضافة إلى الصور الثابتة أو المتحركة، وغيرها من البيانات ذات الطابع الشخصي، ويعكس هذا التعريف السامع نطاق الحماية القانونية للبيانات الشخصية في النظام السعودي، حيث لا يقتصر على المعلومات الشخصية فحسب، بل تمتد لتشمل كل ما من شأنه الإحشاء إلى التعرف على هوية الفرد. سواء بشكل مباشر أو غير مباشر، الأمر الذي يتماشى مع معايير الدولية الحديثة في مجال حماية الخصوصية¹⁵.

بناءً على هذا التعريف، تُعد جميع العناصر، بما في ذلك بيانات شخصية محمية بموجب النظام السعودي، تُلحق وحسبها حماية قانونية خاصة، وفرض عقوبات على كل من يخالف هذه الحماية أو يُسخر خصوصية الأفراد. ولا تقتصر هذه الحماية على البيانات المالية فحسب، بل تمتد إلى جميع أنواع البيانات التي قد تسبب خصوصية الفرد. كالصور والأرقام والبيانات والمعلومات الإلكترونية الشخصية. وهذا يتوافق مع أحكام العديد من الأنظمة القانونية المقارنة، التي تؤكد على أهمية حماية البيانات الشخصية جميع أشكالها. سواء كانت رسمية أو تجارية. حالاً مما يؤدي إلى تحديد هوية الفرد. بشكل مباشر أو غير مباشر¹⁶.

تسم تعريف نظام البيانات الشخصية السعودي بوضوح ودقة ومهنية، مما يعكس التزام التشريع بتغطية مختلف أنواع البيانات التي قد تدرج تحت هذا المفهوم، مع مراعاة التطورات المتتالية في مجالات التقنية والمعلومات، ومن أبرز مميزات هذا التوجه تضمين عبارة عامة في نهاية التعريف: "وبغرضها من البيانات ذات الطابع الشخصي". بهدف استيعاب أي بيانات جديدة قد تنشأ مستقبلاً ولم تكن معروفة أو محددة وقت صدور القانون، وتعني هذه الصيغة المرونة أن أي بيانات جديدة تحمل سمات البيانات الشخصية وتؤدي إلى تحديد هوية الفرد تقع ضمن نطاق الحماية القانونية التي يوفرها القانون.

المطلب الثاني: خصائص البيانات الشخصية

¹⁴ مجلس وزير - سعودي، نظام حماية البيانات الشخصية، المادة الأولى، الفقرة ٢، صدر بمرسوم ملكي رقم ١٠١/ ١٤٣١هـ، وبلغ (١٤٣١/ ٢/ ١٤٤٣).

¹⁵ المرفعي، أحمد عبد الله، (٢٠١٧)، حرية المعلومات الإلكترونية، الحقوق الحديثة في المعلومات، مركز المعنى للإصدارات القانونية، القاهرة، ص ٣٧.

البيانات الشخصية الرقمية هي المعلومات التي يمكن جمعها أو استخدامها باستخدام التكنولوجيا الرقمية³⁷، تشمل هذه البيانات مجموعة واسعة من المعلومات التي تُصنّف الأفراد بشكل مباشر أو غير مباشر. مما يمكن الأنظمة والتطبيقات من استخدامها لأغراض مختلفة، من التحليلات، والإعلانات المستهدفة، واتّحات

أولاً: تربط البيانات الشخصية بنحوص وليهي

ترتبط البيانات الشخصية ارتباطاً مباشراً بالشخص الطبيعي، إذ يتضمن هذا أي معلومات تتعلق بفرد محدد أو يمكن تحديده. سواءً بشكل مباشر أو غير مباشر. وتعتمد هذه البيانات، على مبدأ المثال لا الحصر، الموقع، العنوان، رقم الهاتف، المعلومات المالية والبيانات الصحية. وإعادة ما تُخصص لحماية بيانات الشخصية بالأشخاص الطبيعيين. وهو ما تدرج عليه غالبية التشريعات حول المعاد.

إلا أن حظر الأنظمة القانونية قد وسّع نطاق الحماية ليشمل الأشخاص الاعتباريين أيضاً، كما هو الحال في التبرعات التمسدية والاستراتيجية والمروحية، ومن الجدير بالذكر أن حماية البيانات الشخصية تُعد من مسائل الجوهريّة التي تضمن حق الأفراد في الخصوصية وتُحول دون إساءة استخدام معلوماتهم. فعلى سبيل المثال، نصّت اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) على مجموعة من القواعد الصارمة التي تحكم كيفية جمع ومعالجة وحماية بيانات الشخص. والتي يجب أن تتم بطريقة قانونية، ماضة محددة.

ثانياً: القابلية للتعرف على الشخص

تعرف بيانات الشخصية بأنها أي معلومات تتعلق بشخص طبيعي يمكن التعرف عليه. سواء بشكل مباشر أو غير مباشر. وقد تكون هذه المعلومات، بحد ذاتها، كافية لتحديد هوية الشخص، أو قد تصح كذلك عند دمجها مع بيانات أخرى. ويتم عملية التعرف على الشخص إما من خلال معلومات واضحة ومباشرة مثل الاسم

١٠. د. خالد محمد جب، (٢٠١١)، *أحداث الغزو الكويتي ليست استثنائية في عقد القرنين*، دار ابن معزم، مكة المكرمة، ولائحة، (١٢)، ص ١٩٣.

8. مزید، لکھ، 2018، حدائق لغویہ لفظیات منتخب، درجہ ہدایہ فی علم، لکھنؤ، ص 8.

¹⁸ مولاي، انت محمد حجازي و ناصر بنزي لاج العتوب غزالي، مصر، (2015)، مجلة البحوث الفقهية، رقم 5، المجلد 18.

الكامل، تاريخ الميلاد، والمهنة، أو بشكل غير مباشر باستخدام وثائق رسمية مثل بطاقة الهوية الوطنية، جواز السفر، رخصة القيادة، أو من خلال عناصر فردية مثل السمات الفسيولوجية، النفسية، أو الحيوية¹⁵⁵.

وتبرز هنا أهمية التوازن بين حماية الخصوصية وضمنان الأمن، وهو من التحديات الكبرى التي تواجه المجتمعات الحديثة، ويتمثل هذا التحدي في تحديد الظروف التي يُسمح فيها بالوصول إلى البيانات الشخصية لأغراض أمنية أو قانونية، مع وضع ضوابط أخلاقية وتشريعية تمنع التعدي على حقوق الأفراد¹⁵⁶.

فمن جهة، تُعد حماية الخصوصية حقاً أساسياً من حقوق الإنسان، يجب الحفاظ عليه من أي اعتداء غير مبرر، ومن جهة أخرى، قد تبرز حالات تستدعي استخدام هذه البيانات لأغراض مشروعة، مثل التحقيقات الجنائية أو مكافحة الجرائم الإلكترونية، حيث تصبح هذه المعلومات ضرورية للمساعدة في الكشف عن المخالفات وضمنان الأمن العام.

يمكن التحدي في تحديد معايير تضمن قانونية جمع البيانات أو الوصول إليها ومبررها، وعرضها لمراقبة مناسبة، دون المساس بالحرية الفردية، وفي هذا الصدد، يشير الباحث إلى أهمية وجود تشريعات واضحة ومحددة، بما في ذلك آليات الرقابة، لضمان عدم استخدام البيانات الشخصية بما ينتهك الحقوق الأساسية للأفراد.

ثالثاً: البيانات الشخصية والحق في الخصوصية

تربط بيانات شخصية ارتباطاً وثيقاً بالحق في الخصوصية، إذ تمثل هذه البيانات امتداداً لحياة الإنسان وحياته الخاصة. ويُعد أي إهمال أو إساءة استخدام لها انتهاكاً مباشراً لحرة الفرد وكرامته. والخصوصية تُعد من الحقوق الأساسية التي أكدتها المواثيق الدولية، وفي العصر الرقمي، تتسع نطاق هذا الحق ليشمل حماية المعلومات الشخصية التي تُجمع أو تُخزن أو تُعالج إلكترونياً، مما استدعى وضع أنظمة وتشريعات – ك نظام حماية البيانات الشخصية في المملكة العربية السعودية – تهدف إلى ضمان سرية البيانات وتنظيم استخدامها وفق ضوابط محددة، وتوافقاً صارماً مع صاحبها.

¹⁵⁵ حبيب، عمرو محمد، (2001)، حصة جديدة في معالجة هذه المعلومات، ص 1، د: البيضا، عريه مشرف وشريوع، ص 155.

¹⁵⁶ بولاني، عبد الحميد جعفر، ومحمد جلال، (2025)، حصة، (2025)، مصدر سبق ذكره ص 19.

ويجسّر هذا التنظيم إلى تحقيق توازن دقيق بين مصلحة الجهات في استخدام البيانات لتطوير الخدمات، وبين حق الأفراد في حماية خصوصيتهم من أي تدخل أو إساءة استخدام، وتكمن أهمية هذا الحق في تعريف الثقة بين الأفراد والجهات المعالجة للبيانات، وترسيخ مفهوم الكرامة الإنسانية بوصفه أساساً لأي تعامل عادل في البيئة الرقمية.

رابعاً: البيانات الشخصية والقابلية للتملك بالنفاد

يشير النفاد في مفهومه القانوني إلى مرور مدة زمنية محددة يترتب عليها آثار قانونية معينة. كالكسب أو بالنفاد (النفاد الاكتسابي)، أو الغناء دعوى أو التزهد (النفاد المسقط أو الوقائي)، ويُعرف النفاد بأنه الخيار الذي تتوفر فيها الشروط القانونية خلال مدة زمنية تحددها القانون، وقد أقر مشرعون مدناً النفاد الاكتسابي بهدف حماية المراكز الظاهرة وتحقيق الاستقرار في المعاملات القانونية. وذلك من خلال منح الأفضلية لمن يجوز عقاراً أو حفاًعياً عليه، متى كانت حيازته مشروعة. هاذية. عليه. ومتراضنة دون انقطاع طوإل المدة القانونية المقررة. وهذا التحول. أصبح النفاد ليس مجرد واقعة قانونية، بل سبباً مستقلاً من أسباب اكتساب الملكية أو الحقوق العينية، وهو ما أكدته محكمة النقض في العديد من أحكامها. مما يعكس تطور مفهوم القانوني لـنفاد بوصفه وسيلة لإثبات الحقوق وترسيخ الاستقرار القانوني في المعاملات.³¹

نظراً لكون البيانات الشخصية تعد من الحقوق المرتبطة بشخصية الفرد، وبمس جلالة الحقوقي دون أن تتحق بدمته مالية، فإنها تخرج بصيغتها عن نطاق المعاملات المالية. وبالتالي لا تخضع لأحكام النفاد. بمعنى أدق. لا يمكن أن تكون البيانات الشخصية بالنفاد المكتسب، كما لا تسقط بعدم الاستعمال وفقاً لـنفاد المسقط. إذ إن قواعده لـنفاد تُطبق فقط على الحقوق المالية التي تقوم بالمال.

ومع ذلك. لا بد من التفرقة بين عدة قابلية لبيانات الشخصية وفقاً لـنفاد. وبين الحقوق المالية التي قد تنشأ نتيجة التعاقد عليها. فمثلاً، إذا تروى على انتهاك البيانات الشخصية معاقبة بتعويض مدني. فإن هذا التعويض

³¹ انظر في حكام المدعي كعمر و. احمد. مدني جمع السيد وعمر. حرم محجوب. دور شعبي في اكتساب ملكية عقاره على صريق لـنفاد في مدون الصوري. مجلد 3. عدد 3. ص 631.

– باعتباره حقاً مالياً – يخضع لأحكام التقادم وفقاً لنقود عدم النفاذ. ويبدأ احتساب التادم من تاريخ الحكم بانقضاء أو صدور الحكم النهائي³³.

من خلال تحيل نظام حماية البيانات الشخصية في المملكة العربية السعودية، يتبين أن النظام قد قسم البيانات التي تستوجب الحماية إلى عدة أنواع رئيسة، وهي³⁴:

المطلب الثالث: أنواع البيانات التي يحميها النظام السعودي

1) البيانات الشخصية.

2) بيانات الخدمات.

3) بيانات الصحة.

4) بيانات توثيقية.

5) بيانات الائتمانية³⁵.

وقد خص النظام كل نوع من هذه البيانات بأحكام وتعاريفات مستقلة. نيز هذا عن البيانات الشخصية العامة، ومن أبرز تلك التعريفات ما ورد بشأن البيانات الخدماتية. إذ عرفها النظام بأنها:

"كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو القبلي، أو معتقده الديني أو العقلي أو السياسي، أو ينسب على عضويته في جمعيات أو مؤسسات أهلية، وتحتل البيانات الخائلية والأمنية. أو بيانات

³³ السعودي، مسودح حيوي، 1983)، حماية الحياة الخاصة في عقود التأمين، درسه مقارنة، مجلة الدكتوراه مقدمة بحكمه حقوق جامعة القاهرة، ص 291، 292؛ د. محمد عمر علي السيد، حماية الحياة الخاصة في التأمين الصحي، مجلة الدكتوراه مقدمة بحكمه حقوق جامعة القاهرة، ص 157.

– بحدود المادة 1، أنه إذا كان فعل الاختلاس غير البيانات الشخصية بشكل حرمة جديده، فإن هذه الحرفة تستحق هي للاحترار والتعاطف لمرور عتدات من منعه وهو حرفة في المختارات، والمادة 1 من مواد خضع وحدث في التأمين، ص 1، والاحترار، ص 1 المختارات، والمادة 1 من مواد المختارات في التأمين، ص 1.

³⁴ السعودي، ص 1، ص 1، (2023)، (أخرى) عدمي حماية بيانات الشخصية في نفاذات مسكها العامة السعودية، درسه بحسبة ص 1654.

³⁵ نظام حماية الحياة، ص 1، ص 1، مسكها، مادة 1 من نفاذات 16، ص 16.

السمات الحيوية التي تحدد هوية أو البيانات الوراثية أو الائتمانية أو الصحية، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الهوية أو اسمه^{١٦}.

ويلاحظ من هذا التعريف أن المشرع السعودي قد تبني نطاقاً واسعاً لحماية البيانات الحساسة، ليشمل الجوانب المدنية والفكرية والجينية والصحية والأمنية، إذ إنَّه حظوظ هذه البيانات وما قد يترتب على إساءتها أو إساءة استخدامها من مساس مآثر شخصية الأفراد وكرامتهم.

أولاً- البيانات الحساسة: تُعد بيانات الحساسة من أكثر أنواع البيانات الشخصية أهمية وحظوظة في الوقت ذاته، نظراً لما تحمله من دلالات دقيقة على الهوية الفردية والجوانب الخاصة للشخص الطبيعي، ويترك النظام السعودي عبء هذه البيانات وما قد يترتب على إساءتها أو إساءة استخدامها من آثار تدل على كرامة الفرد وعرضه، ولذا بُدئ معها أولوية خاصة في الحماية القانونية تفوق تمت مقررذ بقية أنواع البيانات الشخصية^{١٧}.

وقد انعكس هذا الخوض بوضوح في نظام حماية البيانات الشخصية، حيث شدد المظم العقوبات على كل من يخفي أو يستعمل البيانات الحساسة على نحو يخالف لأحكام النظام، فنصَّ النظام على أن: "كل من أفصح عن بيانات حساسة أو نشرها مخالفاً أحكام النظام يعاقب بالسجن مدة لا تزيد على ستين، وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق مصلحة شخصية"^{١٨}.

ويظهر هذا النص أن المظم السعودي لا يكفي بمجرد حفظ غير بيانات الحساسة، بل تشدد العقوبة لتكفل ردعاً فعالاً لكل من يعمد انتهاك خصوصية الأفراد أو استعمال بياناتهم لأغراض شخصية أو غير مشروعة، كما أن النظام ربط حساسة العقوبة بنية القصد، إذ فُرق بين مخالفة ساذجة عن الإهمال وتلك التي تتم بقصد الإضرار أو تحقيق مصلحة شخصية^{١٩}.

^{١٦} نظام حماية بيانات شخصية في مساهمة عرب السعودية، ١٠ (٢٠١١).

^{١٧} عمرو، ص ١٤٤، (2021)؛ تطبق عدولي معاملة بيانات شخصية؛ دراسة تطبيقية على معالجة تحديات الهوية العربية.

المجلة العربية للدراسات والبحوث، ١٤ (٢٠٢٢)، ص ٣٢.

^{١٨} نظام حماية بيانات الشخص مادة ٣٥ فقرة ١.

^{١٩} الشمرى، عهدى، ع... (2023)، مصدر سبق ذكره ص 1655.

تأبى البيانات الشخصية الوراثية؛ بالنسبة إلى البيانات الوراثية، فقد أولى نظام السعودي هذا أهمية خاصة نظراً لطبيعتها الدقيقة وحساسية آثارها، حيث عرفتها بأنها: "كل بيان شخصي يتعلق بالصفات الوراثية أو الكنتية لشخص طبيعي، يحدد بشكل محدد السمات الفسيولوجية أو النفسية لثالث الشخص، ويستخلص من تحليل عينة بيولوجية لشخص كتحليل الأحماض النووية (DNA) أو أي عينة أخرى تؤدي إلى استخلاص بيانات وراثية"³⁹.

وتتبع خطوة هذه البيانات من كبرها تتعلق بأهمية البيولوجية والوراثية للفرد، ما يجعلها من أكثر أنواع البيانات عرضة للاستغلال في الجرائم الإلكترونية والأنشطة غير المشروعة، فقد نصحت البيانات الوراثية هدفاً لشبكات الجريمة المنظمة، التي قد تسعى إلى سرقتها أو الدلاع بها لتحقيق مكاسب غير قانونية، أو لاستخدامها في تمريض كس الحقوق الشخصية والإنسانية، من تزوير الهوية الجينية أو إلحاق نسب شخص بعز دويد، وهو ما يعد انتهاكاً جسيماً مستريفاً للإسلامية ونظيرين الرخصة على حد سواء⁴⁰.

لذلك، فإن التعامل مع البيانات الحساسة والوراثية في نظام السعودي يعكس وعياً تدبرياً متقدماً بأهمية تحسين الخصوصية الفردية، وحماية الكرامة الإنسانية، وضمان ألا تستخدم هذه البيانات إلا في حدود الضرورة المشروعة وبإشراف الجهات المختصة.

ثالثاً البيانات الشخصية الصحية: عرّف نظام السعودي بأنها: "كل بيان شخصي يتعلق بحالة الفرد الصحية، سواء الجسدية أو العقلية أو النفسية، أو المتعلقة بالخدمات الصحية الخاصة به"⁴¹.

وتعد هذه البيانات من أكثر أنواع البيانات حساسية، لما تتضمنه من تفاصيل دقيقة عن الوضع الصحي للفرد، والتي قد يؤدي تسريبها أو إساءة استخدامها إلى أضرار جسيمة كسر كرامة المريض وسلامته النفسية والاجتماعية. بل وقد تصل أضرارها ودوياً أيضاً، ومن هذا المنطلق، منح نظام هذه البيانات خصوصية عالية

³⁹ نظام حماية البيانات الشخصية، ١، مادة ١٦.

⁴⁰ الدكتور محمد عبد الله (2019)، حرمة الباطن عن الاستخدام غير المشروع لشبكات البيانات في البنية العربية، ص ٢، القاهرة.

ص ٣٣.

⁴¹ نظام حماية البيانات الشخصية، ١، مادة ١٣.

وحماية مشددة. بحيث لا يُسمح بالاطلاع عليها أو تداولها إلا من قبل الجهات أو الأشخاص الذين يؤمنهم النظام بذلك صراحة. تحقيقاً لهذا العنصر العنقوي وضعت وثيقة بين المريط والجهات الصحية⁴³.

رابعاً البيانات الشخصية الائتمانية: يتعلق بـ البيانات الائتمانية، فقد عرّفها النظام بأنها: كل بيان شخصي يتعلق بطلب الفرد الحصول على تمويل، أو حصوله عليه، سواء لغرض شخصي أو عائلي، من جهة تارز المصرف، بما في ذلك أي بيان يتعلق بقدرته على الحصول على القتمان أو بقدرته على الوفاء به أو بتاريخه الائتماني⁴⁴، وتقرر أهمية هذا النوع من البيانات في ارتقاء الائتم بالذمة المالية للأفراد، وسجلهم الائتماني، وما لذلك من تأثير على سجلهم المالية والاقتصادية. ولذلك، حدد النظام على ضرورة حفظ هذه البيانات بسرية تامة. وعنده إناحتها إلا في الحدود المقررة بهاماً، بما يضمن حماية الأفراد من أي ضرر قد ينجم عن إساءة استخدامهم، كالشهير أو الاستغلال المالي أو التمييز في المعاملات الائتمانية.

ويستفاد من استقراء هذه النصوص أن النظم السعودي قد أولى عناية كبيرة بتحديد أنواع البيانات الشخصية بدقة متناهية، فترق بين البيانات العامة والحساسة والصحية والمزانية والائتمانية. وعصر كل نوع منها بأحكام حماية خاصة تناسب مع طبيعت وعظورته، ويظهر هذا التفصيل التشريعي مدى حرص النظام على حفظ مفهوم خصوصية البيانات وضمان حمايتها من أي تعد أو انتهاك، تأمياً على التزمه بمسكة بحريز الثقة الرقمية وحماية الحقوق الفردية في البيئة التقنية الحديثة⁴⁵.

المبحث الثاني: أهمية الذكاء الاصطناعي وتطبيقاته في معالجة البيانات

يُقصد بالذكاء الاصطناعي تلك التقنية التي تهدف إلى تعيد مهام التي تتطلب عادةً قدرًا من الذكاء البشري، وعاماً ما يُستخدم مصطلح "الخوارزميات" للإشارة إلى تطبيقات الذكاء الاصطناعي. غير أن مفهوم الخوارزمية أوسع نطاقاً، إذ يشير إلى سلسلة من التعليمات المحددة بوضوح لتنفيذ مهمة معينة. وقد تفرّج

⁴³ المادة ١٧٢ من نظام حماية البيانات الشخصية، رقم ١٢٩ من مرسوم ١٤٤١ هـ، مادة ١ - ٤.

⁴⁴ المادة ١٧٢ من نظام حماية البيانات الشخصية، رقم ١٢٩ من مرسوم ١٤٤١ هـ، مادة ١ - ٤.

⁴⁵ الخوادم، أرمين سيم، (2021)، تمييز الاختلافات بين شبكات حوسبة سحابية المصاحب، غير المنشور، المؤسسة الخوادم مكاتب.

بروت، ص ٥٣.

عوارضيات بين السلسلة، مثل ترتيب الكميات تجديداً أو إيجاد القاسم المشترك بين رقمين. واعتقدت من عوارضيات تدوير الصفات، وحفظ البيانات الرقمية. والسيلو الثاني⁴⁵.

وفي بعض الحالات، استخدام البيانات الشخصية لإجراء التنبؤات والتقييمات المعتمدة على الذكاء الاصطناعي، مما يساعد في تحسين الخدمات ونتائج الخدمة على ذلك، واتخاذ القرارات المتعلقة بالأفراد، بطريقة مراعاة مبادئ المساواة وعدم التمييز. ومن الأمثلة على ذلك ربط المادح الطبية بأعراض الأفراد. أو المادح النفسية بسوء الأفراد على وسائل التواصل الاجتماعي⁴⁶.

كما يؤدي دمج تقنيات الذكاء الاصطناعي مع البيانات الضخمة إلى تحقيق العديد من مزايا من أبرزها تسهيل الوصول إلى المعلومات. وتوسيع نطاق إنتاج المعرفة وتوزيعها عالمياً، وتقليل التكاليف المالية. وتعزيز الإنتاج، وزيادة الشفافية، واحد من التحيز والتمييز غير المرئي، ويسهم هذا الدمج كذلك في تمكين الشركات من التوسع باتجاهات السوق واتخاذ القرارات المناسبة. ومساعدة المستهلكين في اتخاذ خيارات أكثر فائدة، فضلاً عن تمكين السلطات العامة من توقع مخاطر ومنع وقوع الأضرار⁴⁷.

المطلب الأول: المقصود بتقنيات الذكاء الاصطناعي

تعددت الآراء حول تحديد المقصود بتقنيات الذكاء الاصطناعي نظراً لظهور المصطلح والتسارع في مجال التكنولوجيا، إلا أن معظم هذه الآراء تتفق على أن المقصود بهذه التقنيات هو استخدام آلة الخدية بطريقة تحاكي الأداء البشري. حيث تُصمم خوارزمية من خلال تحليل البيانات والمواقع التي يُدعمها الإنسان. بما يمكنها من اتخاذ الإجراءات المناسبة بصورة مستقلة.

وقد عرف تقنيات الذكاء الاصطناعي بعدة تعريفات. من أبرزها أنها استجابة آلة بطريقة توصف بأنها ذكية. أو أنها "نظم الذي يسعى إلى محاكاة آلات أو أنظمة ذكية تمتلك قدرات مشابهة لقدرات العقل

⁴⁵ من إعداد: فهد، (2021) الذكاء الاصطناعي، معرفة تقنية، دور المساهمة في عالمنا الحديث، كتي ٢٠٢٠، ص ١٥٦.

⁴⁶ من إعداد: عيسى، (2022) ختم -، الخدية الذكاء الاصطناعي، قصة حول أحدث تطورات التقنية، العدد ٥٤، كتي ٢٠٢٢، ص ٥٣.

⁴⁷ خلافي، ياسر حمد، (٢٠٢٢) الذكاء الاصطناعي في العصر الرقمي، قراءة تمهيدية في سياق التحول الرقمي، نشر: اتحاد الذكاء الاصطناعي في آسيا، مجلة بحوث وتطبيقات الذكاء الاصطناعي، العدد ١٠، ص ١٦٢.

نيتشري". كما وصفت بأنها "الجم الذي يهدف إلى تمكين الحاسب الآلي من أداء المهام التي يقوم بها الإنسان. ولكن بكفاءة تعني منه"⁴³.

عرّف الفقيه مينسكي (Minsky) الذكاء الاصطناعي بأنه العلم الذي يتيح للألات تنفيذ مهام التي تقتضي ذكاءً فيما لو أدّتها الإنسان بنفسه.

كما عرّف العقيد كايو (Cairo) البروتوكولات بأنها كيانات اصطناعية وميكانيكية تتفاعل مع العالم الواقعي وتحتاج البيانات والمحركات التي تستقبلها من بينها⁴⁴.

أما عدد من فقهاء القانون فقد تناولوا المفهوم من منظور تقني. فعرفوا الذكاء الاصطناعي بأنه تكنولوجيا متقدمة تهدف إلى محاكاة لسلوك البشري للذكى، من خلال ابتكار برمجيات أو أجهزة قادرة على التفكير واتخاذ القرارات بصورة مستقلة عن تدخل الإنسان المبرمج⁴⁵.

وبناءً على ما سبق، يمكن القول إن تقنيات الذكاء الاصطناعي تشمل ما يلي:

- أنظمة الكمبيوتر ذات المهام المحدودة، التي تُرمج لتنفيذ وظائف معينة ضمن نطاق ضيق.
- أنظمة الذكاء الاصطناعي ذات المهام المتوسطة، التي تمكن قدرة أوسع على معالجة البيانات واتخاذ قرارات في سياقات متعددة.
- أنظمة الذكاء الاصطناعي ذات الأداء القوي. وهي الأنظمة المتقدمة التي تتجاوز في أدائها القدرات البشرية في بعض المجالات التقنية والتجديدية.

المطلب الثاني: الطبيعة القانونية للذكاء الاصطناعي

فهم الطبيعة القانونية للذكاء الاصطناعي أمر ضروري لتحديد المسؤوليات القانونية وتوفير الحماية اللازمة. وضمان استخدام التقنية بشكل مسؤول وأخلاقي. تشمل القضايا القانونية المرتبطة به حقوق الملكية الفكرية.

⁴³ محمد... محمد (2019). الذكاء الاصطناعي حد جديد لتجاوز مسارات في الآلات وإنجازات التقنية العدد ١٠، ١٢-١٣، ص ١٩٠.

⁴⁴ عبد الرؤف عيسى (٢٠٢٢)، ص ١٢٢٢. ص 1. د. سامح أنت وخراب، عماد (أردن)، ص ١٢.

⁴⁵ بكر، حبيب، حيدر، وحيد، عبد حمدة، ٢٠١٩-٢٠٢٠، مسؤوليت عن الأضرار التي تسببها الروبوتات، مجلة كلية الشريعة، العدد ٦، ص ١٩١.

الخصائية والأمان، المحديات الأخلاقية، ومسؤولية المادية والجانية، لما يستتبعه وضع أمر قانونية واضحة توازن بين الابتكار وحماية الحقوق الفردية والجمعية العامة^{١٢}.

أولاً: نظرية الاعتراف بالشخصية القانونية للذكاء الاصطناعي

تعد الشخصية القانونية مفهومًا أساسيًا في القانون، يُمنح توجيه الأشخاص والكيانات القانونية - كالأفراد والعيونات - حقوقًا وواجبات. تتيح هذه ممارسة الأنشطة القانونية وتحمل المسؤولية عن أفعالهم أمام القضاء.

وفي سياق تطور تقنيات الذكاء الاصطناعي، ظهرت نظرية تدعو إلى منح الذكاء الاصطناعي شخصية قانونية. بناءً على صفاته المميزة التي تمنحه نوعاً من الاستقلالية والقدرة على اتخاذ قرارات بشكل مستقل، بالإضافة إلى ذكاء خاص يسمح له بالاختيار والتفاعل ضمن نطاق محدد^{١٣}.

يشير أنصار هذه النظرية إلى أن الذكاء الاصطناعي يمتلك إمكانات متقدمة في بعض الجوانب تفوق القدرات البشرية، مما يبرر اعتباره ككيان قانوني له شخصية معنوية مستقلة.

ومن أبرز المبررات التي يستند إليها مؤيدو هذه النظرية، قرار المجلس الأوروبي لعام 2017، الذي دعا إلى مناقشة منح الروبوتات صفة الشخصية المعنوية، نظراً لتطورات البرمجة في مجال الذكاء الاصطناعي وتأثيره المتزايد في الحياة اليومية.

وعلى الصعيد العملي، برزت الشبكة العربية السعودية كمثال رائد في هذا المجال. حيث منحت الروبوتات "صوفي" الشخصية السعودية بموجب مرسوم ملكي صدر عام 2017 خلال منتدى مبادرة استثمار المستقبل في الرياض. في خطوة رمزية تعكس الاعتراف بالبريد بكيانات الذكاء الاصطناعي.

بالرغم من هذه التطورات، تظل نظرية الاعتراف بالشخصية القانونية للذكاء الاصطناعي ترواً جديدة تحتاج لمزيد من التحديات متعددة، منها^{١٤}:

- توسيع نطاق استخدام التكنولوجيا بحيث تحقق تفاعلاً أكثر تطوراً وديناميكية مع البيئة المحيطة.

^{١٢} المالكي، حمد بن عبد الرحيم بن حمد، 2024، مسؤولية الذكاء الاصطناعي في ضوء الرؤية الشرعية، جامعة الإمام محمد سعود بن عبدالعزيز، العدد التاسع والثمانون - ص 1792.

^{١٣} بكر، جب، جهنم، محمد، عبس، عود، ١٩٩٠-٩٥، مصدر سبق ذكره.

^{١٤} المالكي، حمد بن عبد الرحيم بن حمد، 2024، مصدر سبق ذكره ص 1793.

- تعزيز قدرات الذكاء الاصطناعي في مختلف التطبيقات، مما يساهم في تطوير حلول مبتكرة تعزز جودة الحياة البشرية.

ومع ذلك، يظل هذا المفهوم محط نقاش قانوني وأخلاقي مستمر، نظراً لما يشهد من تساؤلات حول مسؤولية الأفعال، وحقوق الكيانات غير البشرية، والآثار الاجتماعية والقانونية المترتبة على منح الذكاء الاصطناعي هذه الشخصية.

ثانياً: نظرية إنكار الشخصية القانونية للذكاء الاصطناعي

يرى أصحاب هذه النظرية أن الشخصية القانونية ليست مجرد اسم أو إطار تشكيلي يشبه الذئبة نائية، بل هي مجموعة من القدرات القانونية التي تشمل القدرة على اكتساب الحقوق وتحمل الالتزامات والواجبات القانونية، بحيث يتمتع الكيان القانوني بالمسؤولية القانونية الكاملة.

وبناءً على هذا التعريف، لا يمكن اعتبار الذكاء الاصطناعي كياناً ذا شخصية قانونية، لأنه في جوهره مجرد آلة أو نظام تقني لا تملك صفات الكيان القانوني، فهو لا يملك القدرة على التمييز بين الأفعال الصالحة والخطئة، ولا يتمتع بالوعي أو الإرادة الذاتية التي تؤهله لتحمل المسؤولية القانونية.

الذكاء الاصطناعي يعمل وفقاً لبرمجيات وخوارزميات تم تطويرها وتزويدها من قبل الإنسان، فلا تمتلك حرية الاختيار أو اتخاذ القرارات المستقلة بشكل مطلق، بل يعتمد على المعلومات والبيانات التي تزود إليه.

لذا، يؤكد أصحاب هذه النظرية أن منح الذكاء الاصطناعي الشخصية القانونية أمر غير ممكن ويفتقر إلى الأسس المنطقية والقانونية، لأن ذلك قد يؤدي إلى إضعاف مفهوم المسؤولية القانونية ويخلق فراغاً قانونياً، إذ إن المسؤولية تبقى دائماً على صانع أو مشغل النظام الذكي، وليس على الذكاء الاصطناعي ذاته.

ثالثاً: خصائص الذكاء الاصطناعي

يتميز عن البرمجيات السابقة أن للذكاء الاصطناعي طبيعة مميزة تفرقه عن الذكاء البشري، رغم وجود تشابهات بينهما في عدد جوانب، نذكر منها على سبيل المثال لا الحصر¹⁴:

¹⁴ الملاك، حمد بن عبد الرحيم بن حمد، (2024)، مسؤولية المذهب عن فعل الذكاء الاصطناعي في ضوء السعودية، دراسة حسية تأصيلية، مجلة بحوث الفقه والقانون، العدد السابع والأربعون - ص 1778.

1- التعلم والإدراك

يُدار الذكاء الاصطناعي بقدرته اللغوية على الإدراك والتعلم المستمر، مما يمكنه من تلبية احتياجات البشر بشكل متطور. فعلى مناهج الأساليب مرفقة بالسبوك البشري. من أجل تفضيلاته واحتياجاته يجب إتاحة ما يفضله ويتجنب ما يرفضه. وبمعنى ذلك يوضح في جزائريات برامج التواصل الاجتماعي التي تعد تفاعلي المستخدمين لتفاهل محتوى مخصص لهم.

في هذه المرحلة، أصبح الذكاء الاصطناعي قادراً على فهم الوسط المحيط به والتعرف على الأنماط المختلفة. حيث تمكنه التمييز بين الصور والأصوات. والمعرف على الأشياء وتغييرها. فقد أصبح من الشائع استخدام تقنيات التعرف على بصمة الوجه وبصمة اليد في الهواتف الذكية لأغراض الأمن. كما تطورت الآلات في فهم الأصوات، وتحليل الكلام إلى نصوص مكتوبة، وتوليد الترجمة الفورية بدقة عالية.^{٢٢}

2- القدرة على اتخاذ القرارات بشكل مستقل

بعد اكتسابه القدرة على التعلم والإدراك، أصبح الذكاء الاصطناعي قادراً على اتخاذ قرارات بشكل مستقل ضمن نطاق معين. وتعتمد هذه القدرة على الخوارزميات والبيانات التي تم تزويدها مسبقاً والتي تم تحليلها واستخدامها لتوجيه قراراته. ومع ذلك، تبقى قدرة الذكاء الاصطناعي على اتخاذ القرارات محدودة بالإطار الوظيفي أو المجال الذي صُمم للعمل ضمنه. فلا يمكن اتخاذ قرارات خارج هذا النطاق أو التعامل بالاعتصامات المبركة بلية ولا تضمن زيادة أو سيطرة تفوق تلك التي تم برمجتها عليها.^{٢٣}

يُمكن اعتقاد البعض أن الذكاء الاصطناعي سيصبح أقوى من البشر. بفضل قدرته على التعلم والإدراك وجمع المعلومات من جميع المصادر، سواء المكتبة أو مواقع الإلكترونية، وتحليلها واستخدامها للتأليف بسرعة. يعتقد

^{٢٢} حبيبة، نجاة، ٢٠١٠-٢٠١١، الذكاء الاصطناعي، مسعى الخفاء بشرى من نظريات شكوكية، هي خيرة لعمدة ملك، (نسخة لا إر)، ص ٢٦.

^{٢٣} الماك، حمد بن عبد الرحيم بن حمد، 2024، مصدر من ذكاء من 1771.

أصحاب هذا الرأي أن البشر سيستخدمون على الآلات التي صنعوها وحسن عزمها وصوروها، والأخطر من ذلك، اعتقادهم بأن الذكاء الاصطناعي سيكون سلباً في المقارن البشرية.^{٢٧}

3- معالجة كميات هائلة من البيانات بجودة عالية

تعتبر أنظمة الذكاء الاصطناعي تقديراً الخافضة على معالجة كميات ضخمة من بيانات بسرعة عالية ودقة عالية، دون أن تتأثر بعوامل التعب أو سوء النية عادة على الأداء البشري. هذه البروز تضمن استمرار هذه الأنظمة بكفاءة في مختلف الظروف، مما يسهم في تعزيز الإنتاجية وتقليل نسبة الأخطاء التي قد يرتكبها البشر. بالإضافة إلى ذلك، تتيح الدقة العالية في تنفيذ المهام التي توفرها هذه الأنظمة تحسناً جودة النتائج وموثوقيتها في مختلف التطبيقات، سواء في القطاعات الطبية أو الصناعية أو غيرها.^{٢٨}

4- القدرة على محاكاة السلوك الإنساني

تشير قدرة الذكاء الاصطناعي على محاكاة سلوك الإنساني إلى إمكانيةه في تقليد العمليات انسانية بشرية. وهو ما يعد من الأهداف الأساسية لفهم هذا النوع من التكاملات. فالغاية الرئيسية من دراسة الذكاء الاصطناعي تكمن في استغلال معالحة المعلومات بطريقة مشابهة للذكاء البشري، من فهم اللغة الطبيعية، وتحليل الصوريات الإنسانية، واتخاذ القرارات بناء على ذلك. ويعود ذلك إلى أن الإنسان هو المصدر الأصلي للذكاء الذي تُبنى عليه خوارزميات وأنظمة الذكاء الاصطناعي. حيث تقوم هذه الأنظمة بمحاكاة القدرات الإدراكية للبشر بغرض تحسين الأداء وتطوير الخبرات الذكية.^{٢٩}

المطلب الثالث: نطاق سريان تشريعات حماية البيانات الشخصية للمعالجة بواسطة تشبة الذكاء الاصطناعي

يقصر نطاق تطبيق تشريعات حماية البيانات الشخصية على الأشخاص الطبيعيين فقط، ولا تشمل الأشخاص الاعتباريين سواء كانوا جهات عامة أو خاصة، كما أن هذه التشريعات لا تميز بين الأشخاص من حيث الجنسية، إذ تُطبق الحماية القانونية بعض النص عما إذا كان الشخص وطنياً أو أجنبياً، شرط أن تكون معاملة

^{٢٧} أحميد، إدراج، الذكاء الاصطناعي مرجع سبقي، ص ٢٠.

^{٢٨} الملاكي، حمد بن عبد الرحيم بن حمد، 2024، مصدر سبق ذكره ص 177.

^{٢٩} شرف الدين، محمد، (٢٠١٩)، الذكاء الاصطناعي والشبكات العصبية، بغداد، إصدارات جامعة الإمام محمد عبد الوهاب، ص ٢٤.

البيانات يتم لشخص موجود داخل إحدى الدول الأوروبية التي توضع اللائحة الاتحاد الأوروبي حماية بيانات الشخصية¹⁴²⁹.

وتؤكد هذه اللائحة على ضرورة احترام القواعد والمبادئ الخاصة بحماية الأشخاص الطبيعيين عند معالجة بياناتهم الشخصية. بغض النظر عن مكان إقامتهم أو جنسيتهم. كما يطبق قانون الاتحاد الأوروبي على أي جهة تقوم بمعالجة بيانات شخصية داخل دول الاتحاد أو تمارس نشاطاً اقتصادياً داخلها، بالإضافة إلى ذلك، تسري أحكام اللائحة على كل من يحتاج البيانات حتى وإن كان خارج الاتحاد الأوروبي، حالما أن البيانات المعالجة تتعلق بأشخاص أوروبي أو شخص يقيم في إحدى دول الاتحاد الأوروبي¹⁴³⁰.

من الجدير بالذكر أن لائحة الاتحاد الأوروبي لحماية بيانات الشخصية لا تقتصر تطبيقها على المعالجة التي تتم باستخدام الوسائل الآلية فقط، بل تمتد لتشمل أيضاً المعالجة اليدوية لبيانات في حال كانت جزءاً من نظام حفظ الملفات أو يُخترط أن تكون كذلك. فقد أكدت اللائحة على ضرورة أن تكون حماية الأشخاص الطبيعيين محايدة من ناحية التقنية. حيث لا تعتمد فقط على نوع التقنية المستخدمة، بل يجب ضمان حماية البيانات الشخصية سواء تمت معالجتها آلياً أو يدوياً¹⁴³¹.

ومع ذلك، لا تسري أحكام اللائحة على الملفات أو الوسائل المستخدمة في إعدادها بشكل مطلق، إذ يعتمد تطبيقها على المعالجة اليدوية على وجود هدف حفظ بيانات ضمن نظام تقني، بناءً على ذلك، إذا كانت معالجة البيانات الشخصية تتم يدوياً ويتم حفظها في أرشيف ورقي فقط، فلا تصير أحكام اللائحة في حيزها الحالي.

ولم يرض القانون الفرنسي، على سبيل المثال، على تحديد نطاق سريان أحكامه المتبعة بالمعالجة الآلية لبيانات شخصية سواء بشكل كلي أو جزئي. كما يولي اهتماماً لمعالجة غير الآلية لنفس البيانات أو حسب الاختلاف عينيها في صفات¹⁴³².

¹⁴²⁹ 1) , Kart Pommier, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139 International Data Privacy Law, 2017, Vol.7, No. 29

¹⁴³⁰ السعيد، دواء حمدي، نصيب، مذكرة، «المصاحفي وعملات بيانات الشخصية»، ص 1429.

¹⁴³¹ Pether Carey, Data Protection, fifth edition, Oxford, 2018, p.46

¹⁴³² السعيد، دواء حمدي، مصدر سبق ذكره ص 1430.

أولاً: الأساس القانوني لمعالجة البيانات الشخصية عبر تقنية الذكاء الاصطناعي

تُعتبر معالجة البيانات الشخصية باستخدام تقنيات الذكاء الاصطناعي من الموضوعات الحساسة التي تتطلب إضماراً قانونياً صارماً يضمن حماية حقوق الأفراد وخصوصياتهم. وفي هذا السياق، أكدت المادة السادسة من اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي (GDPR)، على الأساس القانوني الذي يجب أن تقوم عليه معالجة البيانات الشخصية في هذا المجال. استناداً إلى حكم المادة الثامنة من الميثاق الأوروبي لحقوق الأساسيات التي تنص على وجوب معالجة البيانات الشخصية بما توافقه صراحة من الشخص المعني أو استناداً إلى نص قانوني يلزم ذلك⁵⁴.

وتنص المادة السادسة من اللائحة بشكل واضح على أن معالجة البيانات الشخصية تُعتبر قانونية فقط في حالة توافر أحد الشروط الأساسية التالية: موافقة صاحب البيانات؛ حيث يجب أن تكون موافقة الصريحة والمستبعدة على معالجة بياناته الشخصية، سواء كانت هذه البيانات تُجمع أو تُستخدم لأغراض محددة تحقق بنقبة الذكاء الاصطناعي.

ووجود حالة ضرورية وذلك عندما تكون معالجة البيانات ضرورية لتحقيق غرض مشروع، مثل إبرام عقد أو تنفيذ، أو الوفاء بالتزامات قانونية، أو حماية مصالح عامة كالصحة والسلامة، أو الدفاع عن مصالح مشروعة لم الأفراد المتجمع كذلك.

يعكس هذا الإطار القانوني التوازن الدقيق بين تكبير الابتكار التكنولوجي واستخدام الذكاء الاصطناعي في معالجة البيانات، من جهة، وبين ضمان حماية حقوق الأفراد وخصوصيتهم من جهة أخرى. إذ ينصب الاستخدام القانوني لتقنيات الذكاء الاصطناعي مبررة استثنائية والموضح في كيفية جمع البيانات، وأهداف من معالجتها، وضمان أن تكون هذه المعالجة محدودة بما يتناسب مع الغرض المشروع الذي تم جمع البيانات من أجله مع إتاحة حقوق الأفراد في الاعتراض على بياناتهم وتصحيحها أو حذفها⁵⁵.

⁵⁴ F. RASO, H. HILLIGOSS, V. KRISHNAMURTHY, C. BAVITZ, I. KIM, Artificial intelligence and Human rights, 1, September 25, 2018, 7.

⁵⁵ سعيد، دة حسني، مصدر سبق ذكره ص 1435.

والثاني، يُعدّ الالتزام الصارم بهذه المبادئ القانونية ضرورياً لضمان التوازن بين الحقوق المتقنة وحماية حقوق الإنسان في عصر الذكاء الاصطناعي.

ثانياً: تحديات حماية حق الخصوصية في ظل تطبيقات الذكاء الاصطناعي

تُعدّ تطبيقات الذكاء الاصطناعي في الوقت الراهن مساحة واسعة في الحياة اليومية للأفراد، نظراً لما توفره من حلول فعالة وقائمة في مواجهة العديد من التحديات وتلبية مختلف الاحتياجات. فقد أصبح الذكاء الاصطناعي عنصراً أساسياً في مجالات متعددة، مثل قطاع الصحة والتعليم، والمكان الذكي، ومكافحة الجريمة، وغيرها من المجالات الخيرية¹⁰⁰.

إلا أن هذا الانتشار الواسع لتطبيقات الذكاء الاصطناعي أوجدت فيه تحدياً من التحديات غير المسبوقة المتعلقة بحماية البيانات الشخصية للأفراد. فهذه التطبيقات لا تقتصر على معالجة بيانات الصحة وأمنيتها وتصنيفها وحسب، بل تتجاوز ذلك إلى استخدامها في التعلم الذاتي وتطوير نماذج قادرة على التكيف مع طريقة التفكير البشري. وإجراء ترات قابلة للتطبيق والتغيير. وتزداد خطورة هذه التحديات مع تطور استخدام تقنيات البيانات المستخدمة في الذكاء الاصطناعي. إذ إذا تمّ تمكين مساهمة إلى الحد الذي قد يجعل تصميم أو مزيج الأنظمة الذكية نفسه غير قادر على تفسير النتائج التي تنتجها هذه الأنظمة أو التحكم فيها.

1- التحدي من الاستخدام المتزايد لتطبيقات الذكاء الاصطناعي

على الرغم من انتقاده الكبير والتطور الهائل الذي حققه الذكاء الاصطناعي لصالح البشرية، فإن عدداً من الخبراء والشخصيات العامة والمتخصصين في هذا المجال قد وجهوا تحذيرات حادة بشأن مخاطر استخدامه هذه التقنية، ولا سيما ما يتعلق منها بالتهديدات التي تلحق بالخصوصية. وقد وصلت المفوضة السامية لحقوق الإنسان في الأمم المتحدة، في شهر سبتمبر من عام 2021، على ضرورة وقف بيع واستخدام أنظمة الذكاء الاصطناعي التي تشكل خطراً على حقوق الإنسان. إلى حين اعتماد ضمانات كافية لضمان سلامة عملها.

¹⁰⁰ Artificial Intelligence and Data Protection, Council of Europe, November 2019, On Site www.coe.int/AI

كما دعت إلى حظر استخدام التطبيقات الذكية التي لا تتماشى مع القانون الدولي لحقوق الإنسان. مؤكداً أن الأنظمة الذكية، رغم إسهامها في حل العديد من التحديات، قد تسبب مشاكلات كارتية إذا ما استخدمت دون مراعاة تأثيرها على حقوق الأفراد، وأكدت باتينيت كذلك على موجبات فرض الرقابة الصارمة على استخدام الذكاء الاصطناعي قبل اعتماد التدابير الضرورية لحماية حقوق الإنسان⁴³.

وفي السياق نفسه، أعاد فريقكم تذكركم، بخصوص التماسي حقوق الإنسان في الأمم المتحدة، التأكيد على عدد من النقاط في 18 فبراير عام 2023، معرباً عن قلقه من وتيرة التطور السريع للذكاء الاصطناعي، وداعياً إلى إيجاد حلول فعالة تضمن حماية حقوق الإنسان في ظل هذا التطور المتسارع (42).

وعلى الصعيد العربي، عقد مؤتمر دولي بتاريخ 21 يونيو 2022 بعنوان "التحديات حماية الحق في الخصوصية في ظل تطورات الذكاء الاصطناعي"، برعاية منصة العربية لحقوق الإنسان وبالتشراكة مع اللجنة العليا لحماية حقوق الإنسان. وقد تناول المؤتمر تأثير الذكاء الاصطناعي على حق الخصوصية وما قد يترتب على الإخلال به من انعكاسات على تفجير باقي حقوق الإنسان. إضافة إلى مناقشة مسؤوليات الدول والمنظمات الخاصة في حماية بيانات الأفراد، كما تهدف المؤتمر إلى تطوير التشريعات والأطر القانونية الخاصة بحماية البيانات في سياق التقنيات الذكية. وتعبير مصوغة حقوق الإنسان في العالم العربي.

2- أخلاقيات استخدام الذكاء الاصطناعي

حفاظاً على حق الخصوصية، كان من الضروري الامتناع لمجموعة من المبادئ والإجراءات لاستخدام الذكاء الاصطناعي لبيانات الشخصية تتوافقاً فيما يلي:

1- مبادئ معالجة بيانات الأفراد الشخصية

توجد ثلاث مبادئ أساسية للخصوصية في جمع البيانات تبع من مبادئ منظمة التعاون والتنمية الاقتصادية. هي كما يلي⁴⁴:

⁴³ سعيد، ودد حسني، مصدر سبق ذكره ص 1435.

⁴⁴ خبائي، عبد الله، جامعة محمد بن داغول، ص 2023، حق الخصوصية معروضة في ضوء لذكاء الاصطناعي، مجلة الدراسات الحقوقية والاقتصادية، العدد 6، ص 476.

- مبدأ تحديد الجمع: تعتمد التقنيات الذكية على جمع كميات هائلة من البيانات لتدريب وتصوير الخوارزميات. وغالباً ما تجمع هذه البيانات عبر الأجهزة الإلكترونية الذكية، والهواتف المحمولة، وتقنيات تتبع التوجيه، وغيرها من الوسائل. في كثير من الحالات، قد لا يكون الأفراد مدركين لكمية المعلومات التي يتم جمعها عنهم، ولا كيفية جمعها، مما يخلق تعارضاً بين حق الأفراد في تحديد جمع معلوماتهم الشخصية والوظائف التي تؤديها التقنيات الذكية.

- مبدأ تحديد استخدام المعلومات: يجب التأكد من أن البيانات التي تم جمعها تُستخدم فقط للأغراض التي أُجمعت من أجلها. ومع ذلك، في بعض الحالات يُسمح للشركات والمؤسسات باستخدام هذه البيانات لأغراض ثانوية. شرط أن يكون ذلك ضمن حدود معقولة. وهذا يعني أن الجهات المالكة لبيانات ضمان الاستخدام الصحيح والتقني للمعلومات.

- مبدأ تحديد الغرض: في ظل الانتشار الواسع لتطبيقات الذكاء الاصطناعي واستخداماته المتعددة، يكتسب تحديد الغرض من جمع بيانات أهمية بالغة في حماية خصوصية الأفراد ومنع إساءة استخدام بياناتهم. فجمع معلومات لبيانات خارج الإطار الضروري يعد من قدرة الأفراد على التحكم في معلوماتهم الشخصية¹⁰⁸.

ثالثاً: إرشادات استخدام الذكاء الاصطناعي

في سياق نسعي إلى اعتماد ثبات مناسبة لاستخدام تطبيقات الذكاء الاصطناعي بما يتوافق مع حق الأفراد في الخصوصية، هنـ الاتفاقية رقم (108) مجلس أوروبا على مجموعة من الإرشادات المتعلقة باستخدام الذكاء الاصطناعي وحماية البيانات. تتضمن هذه الإرشادات مجموعة من التدابير والإجراءات الأساسية التي يتوجب على الحكومات، وصانعي السياسات، ومطوري التقنيات الذكية الالتزام بها والاعتماد عليها لحماية حقوق الإنسان وكرامته، لا سيما في ما يخص حماية بيانات الشخصية، ويمكن تلخيص هذه الإرشادات كما يلي¹⁰⁹:

¹⁰⁸ Lilian Alitron "Data Protection: Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation? (GDPR) Artificial Intelligence-Proof? SSRN Electronic Journal, APRIL 2019, p 46.

¹⁰⁹ Guidelines on artificial intelligence and data protection (Convention 108), Council of Europe, 25 1 2019, On Site: www.coe.int/AI

- يترتب على مطوري التقنيات الذكية اعتماد منهجية المنصوص عليها في المادة (10) من الاتفاقية رقم (108)، والتي تحدد الالتزامات المتبادلة على عاتق المسؤولين عن معالجة البيانات الشخصية بشكل آلي.
- يجب عليهم تقييم الآثار السلبية المحتملة لتطبيقات الذكاء الاصطناعي على حقوق الإنسان والحريات الأساسية، واتخاذ التدابير الوقائية اللازمة لتجنب هذه المخاطر.
- من الضروري تجنب التحيزات، سواء كانت غير مقصودة أو عرقية، واتخاذ من مخاطر التحيز أو أي تأثيرات سلبية أخرى على حقوق الإنسان المرتبطة بالبيانات.
- يجب تقييم جودة وكمية البيانات الشخصية المستخدمة في مراحل تطوير وتدريب الأنظمة الذكية، والعمل على تحسين جميع البيانات غير الضرورية، مع مراقبة دقة النماذج بشكل مستمر.
- يتعين إعداد النظر في الآثار السلبية المحتملة لتطبيقات الذكاء الاصطناعي على الأفراد والمجتمع، خصوصاً فيما يتعلق بالبيانات التي تُستخدم خارج سياقها الأصلي ونماذج الخوارزميات المستخدمة في تطوير هذه الأنظمة⁷¹.
- يشجع على تأسيس لجان خبراء مستقلة من مختلف التخصصات، لتعزيز التعاون مع المؤسسات الأكاديمية، بهدف تصميم أنظمة ذكية تحترم حقوق الإنسان وأهم توجهاً أخلاقياً واجتماعياً.
- يجب تصميم جميع النماذج والمنهجيات التقنية حيث تضمن حق الفرد في عدم الخضوع لأي قرار يُتخذ بناءً على المعالجة الآلية للبيانات الشخصية دون الحصول على موافقته الصريحة والسبقة.
- تعزيز ثقة المستخدمين، يسعى توفير نطاق لتطبيقات الذكاء خلال مراحل تطويرها، مما يتيح للمستخدمين حرية الاختيار بين الخيارات المتاحة.
- يجب الاعتماد على حزم برمجيات رقابية وتعزيز آليات البقعة التي تكفي معالجة جميع أصحاب النسخة صول قدر ما تشهده التطبيقات الذكية، بهدف ضمان الامتثال للقوانين حماية البيانات، فضلاً عن القوانين والمبادئ المتعلقة بحقوق الإنسان.

⁷¹ شبلي، عبد الله، جامعة محمد بن داغين سعيد، 2023، مصدر سبق ذكره ص 477.

الفصل الثاني:

التحديات القانونية المتعلقة الذكاء الاصطناعي في معالجة البيانات الشخصية

المقدمة

شهد العالم في العقود الأخيرة تطوراً تكنولوجياً متسارعاً أحدثت طفرة نوعية في مختلف مجالات الحياة، وكان من أبرز هذه التحولات ظهور الذكاء الاصطناعي باعتباره أحد أهم ابتكارات الثورة الصناعية الرابعة. فقد أصبح الذكاء الاصطناعي أداة محورية تُستخدم في جميع وأكبر كميات هائلة من البيانات، بما في ذلك البيانات الشخصية للأفراد، وذلك بهدف استنبط الأنماط، وتحسين الخدمات، واتخاذ قرارات آنية في قطاعات متعددة من الصحة، التعليم، الأمن، والإدارة العامة¹.

غير أن هذا الاستخدام الواسع للذكاء الاصطناعي في معالجة البيانات الشخصية أثار العديد من الإشكاليات القانونية والأخلاقية، نضراً ما ينطوي عليه من مخاطر تضرر الحق في الخصوصية وحماية الحياة الشخصية للأفراد، فانظمة الذكاء الاصطناعي تعتمد في جوهرها على تحليل البيانات الضخمة (Big Data) وتعميم الأنماط السلوكية، وهو ما يستلزم الوصول إلى كمّ هائل من المعلومات الشخصية، قد تكون حساسة أو سرية بطبيعتها، ومع غياب الأطر القانونية الواضحة أو ضعف آليات الرقابة، يمكن أن يؤدي ذلك إلى انتهاكات جسيمة لحقوق الأفراد، سواء من خلال جمع البيانات دون موافقة صريحة، أو استخدامها لأغراض غير متوقعة أو غير مصرح بها².

ومن أبرز التحديات التي يواجهها المشرعون في هذا السياق، صعوبة تحديد المسؤولية القانونية عن الأضرار الناتجة عن قرارات الأنظمة الذكية، خاصة وأن هذه الأنظمة قد تتصرف باستقلال نسبي بناءً على خوارزميات معقدة يصعب تفسيرها، كما أن هناك إشكالية أخرى تتعلق بما يُعرف بـ "التعاقب الخوارزمية"، إذ إن الكثير

¹ أحمد، م. د. حسي، سعيد، (2024)، "الذكاء الاصطناعي وحماية البيانات الشخصية: دراسة مقارنة"، مجلة البحث والدراسة، ج 43، ص 1390.

² الفهمي، سامح عبد الوهاب، (2011)، "التحدي الجديد لبيانات شخصية: دراسة قانونية بحرية"، بحث في المجلد 13، جامعة الكويت، ص 11-20، مع 25، ص 25. وكذلك في بحث، الذكاء الاصطناعي: مفاهيم، تطبيقات، وأخلاقيات، ص 20-25، ص 25.

من ثقبات الذاكرة الاصطناعي تعمل كـ "مستودع سرود" لا يمكن معرفة كيفية اتخاذها لقرارات أو الأسباب التي أدت إلى نتائج معينة. مما يعجز مسألة الجهات المسؤولة قانونياً.⁷⁴

إضافة إلى ذلك، فإن استخدام الذاكرة الاصطناعي في تخزين البيانات الشخصية قد يؤدي إلى تمييز غير لائق ضد فئات معينة من المجتمع، نتيجة التحيزات الخفية في البيانات التي تم تدريب النظام عليها. وهو ما يعد مخالفاً لمبادئ العدالة والمساواة التي تقوم عليها الأنظمة القانونية الحديثة. كما أن نقل البيانات الشخصية عبر الحدود باستخدام مصفات الذاكرة الاصطناعي المسجلة يثير تساؤلات حول سيادة البيانات ومدى خصوصية القوانين الوطنية لحماية الخصوصية.

ومواكبة هذه التحديات، برزت على الساحة الدولية مجموعة من المبادرات القانونية والتنظيمية التي تسعى إلى وضع أطر تشريعية واضحة تضمنان الاستخدام المسؤول والآمن لذاكرة الذاكرة الاصطناعي في مجال معالجة البيانات الشخصية. ومن أبرز هذه المبادرات اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، التي تُرسن مبادئ الشفافية والمساءلة وتقييد البيانات. إضافة إلى مشروع قانون الذاكرة الاصطناعي الأوروبي (EU AI Act)، الذي يهدف إلى تنظيم الأنظمة عالية الخطورة ووضع التزامات قانونية على مطوريها ومستخدميها. أما على المستوى العربي، فقد بدأت عدة دول مثل المملكة العربية السعودية والإمارات ومصر في تبني تشريعات وطنية لحماية البيانات الشخصية. إلا أن الإصدار القانوني لاستخدام الذاكرة الاصطناعي ما يزال في طور التطور والمبهور.⁷⁵ وعيد، فإن دراسة التحديات القانونية لاستخدام الذاكرة الاصطناعي في معالجة البيانات الشخصية تعد من الموضوعات الخيرية التي تجمع بين البعد التقني والبعد القانوني. إذ تقصّب تحقيق توازن دقيق بين تشجيع الابتكار التقني من جهة، وحماية حقوق الأفراد الأساسية من جهة أخرى. ومن ثم، فإن البحث في هذا الموضوع يهدف إلى تحليل أبرز الإشكالات القانونية الناشئة عن هذا الاستخدام، واستعراض الجهود التشريعية القائمة، مع تقديم رؤية متكاملة نحو تحقيق الاستخدام الآمن والمسؤول لثقبات الذاكرة الاصطناعي في ظل احترام الخصوصية وحماية البيانات الشخصية.⁷⁶

⁷⁴ محام، عبد جبار حسن، (2023)، ذاكرة الاصطناعي: مفهومها وتطبيقاتها، مجلة المال والسياسة، 652، ص 12.

⁷⁵ العربي، ميرة مبد... (2024)، ذكر ذاكرة الاصطناعي عبر حوسبة سحابية، المؤل ونوعين نسوي الساع والعنبر... جمعية مكاتات شخصه عن الخبج العربي، ترحف ثقبات لذكاء في بنة مكاتات شخصه ومؤسسات لعمومات، مرجع: جمع المكاتات الشخصه، ص 584.

⁷⁶ بن عبد... فهد، (2021)، ذاكرة الاصطناعي: معرلة قانونية، دولة سياسة والعم... مع 12، ص 2، ص 157.

المبحث الأول: صعوبة الحصول على موافقة صريحة من الأفراد.

تُعد موافقة صاحب البيانات الشخصية على معالجتها مسألة قانونية بالغة الأهمية. إذ أصبحت مفهوماً جوهرياً يخصص باهتمام واسع في التشريعات الحديثة. لما تزدية من دور أساسي في ضمان حماية بيانات الشخصية وحسن معاملة الأفراد. وقد لاقى كل من المشرع الأوروبي والسعودي عناية خاصة بتنظيم هذه الموافقة. حيث ركزت الجهود التشريعية على وضع تعريف دقيق لها وتحديد النطاقات المشروعة لتعريض عنها. مع التأكيد على ضرورة مراعاة أشكال الموافقات الأخرى. ولا سيما تلك التي تُسمح في إطار العقود المدنية التقديرية وفقاً لمطابقة العامة للعقد. ورغم هذا الاهتمام. لا تزال النصوص القانونية في كل من النظامين الأوروبي والسعودي تغتفر في بعض جوانبها إلى تحديد واضح لمطابقة القانونية هذه الموافقة، مما يثير تساؤلات فقهية حول أساسيات القانوني ومدى توافقها مع مبادئ التقديرية لرضا في الأنظمة القانونية. خاصة في ظل التطور السريع لتقنيات معالجة البيانات وتحديات البيئة الرقمية الحديثة⁷⁷.

يصل نظام حماية البيانات الشخصية بشكل صريح على ضرورة حصول جهة التحكم على موافقة صاحب بيانات الشخصية قبل الشروع في معالجتها. إذ تعتبر النظام أن الموافقة هي الأساس في مشروعية المعالجة. وقد ورد في المادة الخامسة من النظام ما يلي: "يبدأ عدا الأجل المخصص عملياً في النظام. لا يجوز معالجة بيانات شخصية أو تخزين الغرض من معالجتها إلا بعد موافقة صاحبها. وتبين التوافق ضرورة موافقة، والأشكال التي يجب فيها أن تكون موافقة صريحة".

كما أكدت اللائحة التنفيذية لنظام هذا المدأ. وجعلت موافقة صاحب البيانات الشخصية أول المستويات النظامية المقررة لمعالجة البيانات، حيث جاء فيها: "مادة الثالثة: المستويات النظامية لمعالجة بيانات شخصية، يكون أي مما يلي مسبقاً نظامياً لمعالجة بيانات شخصية أو الإفصاح عنها وفقاً لما ورد في المواد (السادسة) و(العاشر) و(الحامسة عشر) من النظام"⁷⁸.

⁷⁷ الأستاذ محمد مهدي، موافقة غير المدعى الرقمية لبيانات شخصية كونه معرفة، المحلة بحرية لخدمة الشخص في الدراسات والبحوث الحديثة، ص 4264.

⁷⁸ المادة الثالثة من اللائحة التنفيذية لنظام حماية بيانات أصحاب (٢٠٢٣).

وبالإضافة إلى هذا، المبدأ في النظام السعودي يتوافق تماماً مع ما ورد في القانون العام لحماية البيانات الأوروبي (GDPR). إذ جاءت المادة السادسة من المقرر أن الحاجة تكون قانونية فقط إذا توفّر أحد المسوغات. ومن أبرزها: إن أعطى صاحب البيانات موافقته على معالجة بياناته الشخصية لغرض واحد أو أكثر من الأغراض المحددة.⁹ ومن ثم، يتّضح أن النظام السعودي والاتجاه التنفيذية قد تبنيّا ذات النهج المعتمد في التشريع الأوروبي، مع فروق صاغية طفيفة لا تمس الجوهر القانوني مبدأ ضرورة الموافقة المسبقة على معالجة بيانات الشخصية.

وتتمثل ضوابط الموافقة في التالي: -

الضابط الأول: أن تكون الموافقة بإرادة حرة.

يُعدّ هذا الضابط من أركان الضوابط التي نصّت عليها اللائحة التنفيذية لنظام حماية بيانات الشخصية. كما يُعتبر من أهمها وأعمقها أثرًا لما يتفرّع عنه من مسائل متعددة تنصبّ بجوهر حماية الإرادة الحرة لصاحب البيانات، ويقصد به الموافقة الصادرة بإرادة حرة تلك التي تمنحها صاحب البيانات تحضّر حيز ودون أيّ إكراه أو ضغط أو تأثير خارجي. سواء كان مباشرًا أو غير مباشر. إذ إن الإرادة التي تصدر تحت وطأة الإكراه لا تُعدّ الإرادة الحقيقية لصاحبها، وإنما تُعتبر عن إرادته الجهد التي أرغمت على إصدارها.¹⁰

ويتمد نطاق هذا الضابط ليشمل عدداً من المسائل الجوهرية. من أبرزها مسألة الخلط بين إرادة القويّ وبين صاحب البيانات وجهه التحكم. وتبرز هذه الإشكالية في الحالات التي تنامي فيها مراكز القوى، كما هو الحال في عقود الإذعان، حيث تمتدّ جهة التحكم قوة تفاديه أو سلطة مهيمّة تدفع صاحب البيانات إلى منح موافقة راعية عنه رعيه الحقيقية. وذلك إلقاء لسلطتها أو خشيته من تبعات الرفض.

وفي هذا الإطار، يُعدّ القطاع الحكومي من أبرز الأمثلة على الحالات التي يُخشى فيها تأثير حرية الإرادة. إذ قد يشعر الأفراد بالحاجة إلى منح موافقتهم خوفاً من نتائج الرفض أو رغبة في تخادي العقوبات الإدارية. وبذلك،

⁹ Meskenaité, Gabbi, (2022) An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality. Graduate Thesis.

Faculty of Law, Lund University

Page 26, <https://up.lub.lu.se/hur/download?func=downloadFile&recordId=90666798&fileId=90990573>.

لا يستحسن أن تعتمد الجهات الحكومية على الموافقة كأساس قانوني لمعالجة بيانات الشخصية، لما يشوبها من مشكلات تتعلق بحرية الإرادة، وبالأخص من ذلك، يتعلق على تلك الجهات الاعتماد على أحد الأسس الصاعقة الأخرى التي يصر عليها النظام في المادة السادسة، والتي جاء فيها ما يلي³⁵:

لا تخضع معالجة بيانات الشخصية للموافقة المشار إليها في المفقود (1) من المادة (الخامسة) من النظام، في الأحوال الآتية:³⁶

(أ) عندما تحقق المعالجة مصالحةً منسقةً لمعالجة البيانات وكان الاتصال به معذوراً أو كان من الصعب تحقيق ذلك؛

(ب) عندما تكون المعالجة تقتضي نظاماً آخر أو تنفيذاً لاتفاق سابق يكون صاحب البيانات الشخصية طرفاً فيه،³⁷

(ج) إذا كانت الجهة المسيطرة جهة خاضعة، وكانت هذه المعالجة مصوبة لأغراض أمنية أو لسياسة منصات قضائية،

والسبب هو أن الموافقة، عند وجود اختلاف في مبادئ الفري وحقوف صاحب البيانات من الجهة المسيطرة، تُعذر الموافقة غير مقبولة لأنها مُلحقة ضمنية،

ويطعن هذا أيضاً إذا كانت الجهة التي تسعى لمعالجة البيانات هي صاحب العمل، وكان صاحب البيانات عاملاً أو موظفاً في الشركة نفسها، وكانت الشركة ترغب في معالجة بيانات الشخصية لتحقيق مصالحها، على سبيل المثال، إذا أرادَت الشركة مراقبة سلوك الموظفين بكاميرات داخلية لتحديد أذواقهم الخفية ثم بيعها، فوفقاً للقانون، لا حق للشركة الخفاء بذلك دون الحصول على موافقة الموظفين، ومع ذلك، قد لا يتمكن الموظف من الرفض خوفاً من الشركة، أو من الفصل، أو عداة المظهر في ترقية أو غير ذلك العمل، لذلك، تكون الموافقة غير مقبولة لأنها لا تُمنح طواعية، في هذا السياق، تنص المادة السابعة من القانون، وتؤكد الملاحظة، على ما يلي: "لا يجوز أن تكون الموافقة المشار إليها في المفقود (1) من المادة (5) من القانون شرطاً

³⁵ كذا على عدد جرد من العدد 2023)، مع لغة صاحب، بيانات الشخصية معقدة بدرجة في نظام المعرفي، دراسة حبيبة مصرية
لجنة كندا للشريعة وعلوم، تعيناً لأخرى - ذهنية، العدد 3537، العدد 3537.

³⁶ عدد 1) من المادة (الخامسة) من النظام، التعديلات على حماية البيانات الشخصية (٢٠٢٣-٢٠٢٤)

لتقديم خدمة أو منفعة، إلا إذا كانت الخدمة أو المنفعة مرتبطة بمعالجة البيانات الشخصية التي مُنحت الموافقة بشأنها".⁸³

الضابط الثاني: أن تكون أغراض المعالجة واضحة ومحددة

كما هو دقائي يهدف إلى منع إساءة استخدام جهة التحكم بموافقة صاحب البيانات الشخصية. خصوصاً عندما تُصَب تلك الموافقة لأغراض عامضة أو غير محددة لكي تأويلها بطرق متعددة. اشترطت اللائحة التنفيذية أن يتضمن صلب الموافقة موضحاً من جهة التحكم إلى صاحب البيانات تحديدًا واضحاً ومسبقاً للأغراض التي سيتم المعالجة من أجلها، ويُفهم من هذا الشرط أن صاحب البيانات يجب أن يكون قادراً على فهم الأغراض المحددة والمعينة بوضوح قبل منح الموافقة حتى يتمكن من اتخاذ قراره بصراحة وإحدى وذلك من ممارسة سيطرته الفعلية على بياناته الشخصية، ويبين على هذا الضابط عدة متطلبات أساسية يمكن تفصيلها على النحو الآتي⁸⁴:

أولاً: تُعد موافقة غير مقبولة إذا كانت الأغراض التي تُذكر في صلب المعالجة عامضة أو مبهم، مثل أن تُذكر عبارات عامة كـ "أغراض تسويقية" أو "أغراض مستقبلية" أو "لحسين تجربة المستخدم" مستقبلاً. وذلك لأن هذه العبارات تفتقر إلى التحديد الكافي الذي يمكن لأصحاب البيانات من فهم الغرض الحقيقي من المعالجة. ومن باب أولى، تُرفض الموافقات العامة والمنطقية التي تحيز المعالجة لأي غرض كان. لافتقارها للتوضيح في مقابل، تكون الموافقة صحيحة ومعتبرة إذا كان الغرض محدد وواضحاً، مثل: دراسة أثر هذا الدواء على مستخدميه أو تطوير هذا النوع من الأجهزة وفق احتياجات المستخدمين.

ثانياً: يستلزم من المتراخ وشرح الأغراض أن يُستحصل موافقة مستقلة لكل غرض من أغراض المعالجة، ولا يكفي الموافقة واحدة شاملة لجميع الأغراض. وقد نصت اللائحة صراحة على ذلك في الفقرة (1^أ) من المادة الحادية عشر ذ. التي أوجبت أن تكون هناك موافقة مستقلة لكل غرض من أغراض المعالجة⁸⁵.

فعلى سبيل المثال، إذا كان لأصاحب البيانات أكثر من جهاز، وأرادت الشركة النسخة معالجة البيانات المتعلقة بكل جهاز لأغراض تطويره، فلا يجوز الاكتفاء بالموافقة واحدة تشمل جميع الأجهزة بل يجب إصدار موافقة

⁸³ المادة (السادس) من اللائحة التنفيذية جاء صلبه البيانات الشخصية (٢٣-٢٤).

⁸⁴ انظر: عبد العزيز بن محمد، (2023) مصدر سبق ذكره ص 3539.

⁸⁵ المادة 1^أ من المادة الحادية عشرة ذ. من اللائحة التنفيذية جاء صلبه بيانات الشخص.

مستقلة لكل عرض على حدة، وإذا حصلت التفرقة على موافقة واحدة شاملة لكافة الأعراض، فإن هذه الموافقة تعدّ غير مقبولة نظاماً وفقاً لأحكام اللائحة.

ثالثاً: يتجلى من هذا التنظيم مبدأ مهم يعرف بمبدأ محدودية الموافقة، ومعناه أن الموافقة تكون محصورة في العرض الذي صدرت من أجله، ولا يجوز جهة التحكم التوسع في استخداماتها لمعالجة بيانات أخرى أو لتحقيق أغراض مغايرة، فإذا صدرت الموافقة من أجل تطوير جهاز معين، لا يجوز استخدام هذه الموافقة لتطوير جهاز آخر أو العرض تسويقي مختلف، وعلى جهة التحكم أن تحصل على موافقة جديدة ومستقلة عند ظهور أي عرض جديد لمعالجة ذلك.

رابعاً: نصّت اللائحة على وجوب أن تُمنح الأعراض لصاحب البيانات عند غلب الموافقة أو قبده، وهو ما يمكن تعريفه جوهرياً بمعنى أيضاً الشفافية والوضوح، فلا يجوز لجهة التحكم أن تطلب الموافقة أولاً ثم تُمنح الأعراض لاحقاً، إذ تُعد الموافقة في هذه الحالة باطلة وغير محصورة نظاماً، والوضوح والإفصاح عنصران أساسيان لقبول الموافقة.

خامساً: ينبغي أيضاً أن يزود صاحب البيانات بمعلومات كافية وواقعية حول الأعراض التي ستُعالج بياناته من أجلها، وبمدرجة وشرح مكثف من اتخاذ قراره عن علم وبصيرة، فإذا كانت المعلومات المقدمة غير كافية أو موجهة بنغية تقنية معقدة تجعل مستهلك فهم الشخص العادي، فإن الأعراض لا تُعد واضحة بالقدر الكافي. وتسمح الموافقة الناتجة عنها غير صالحة قانوناً، ويُعد هذا المنع من الضوابط الأساسية التي يجب على الجهات والشركات الالتزام بها، خصوصاً عند تعاملها مع المستخدمين العاديين الذين لا يملكون معرفة تقنية متخصصة، إذ يجب أن تُقدّم المعلومات بمستوى لغوي ومعرفي يناسب مع إدراكهم، تحقيقاً لمبدأ الشفافية والتمكن العمومي لصاحب البيانات³⁵⁴⁰.

المضابط الثالث: أن تكون الموافقة صريحة

يُعدّ اشتراط الصراحة في الموافقة من الضوابط الجوهرية التي أكدت عليها اللائحة التنفيذية لنظام حماية البيانات الشخصية، وذلك تجزئاً لمبدأ وشرح الإرادة وضماناً لحماية صاحب بيانات من أي التماس أو استغلال في

³⁵⁴⁰ انظر: عبد الحميد بن محمد، 2023، مصدر سبق ذكره، ص 3540.

³⁵⁴¹ Alekemaite, Gabbi, 2022, P.3٠٠.

تفسير رضاد، وقد نصت الفقرة الثانية من المادة الحادية عشرة من اللائحة على ما يلي: "يشترط في الموافقة أن تكون مبرجة في الأحوال الآتية"⁸⁷:

(1) في حال كانت الموافقة هي المسوّغ النظامي الوحيد لمعالجة البيانات الشخصية.

(2) في حال تضمنت معالجة بيانات حساسة.

(3) في حال تضمنت المعالجة بيانات إسمية.⁸⁸

ويتضح من النص أن استمرار الصراحة في الموافقة يكون واجباً في ثلاث حالات محددة، تبعاً جميعها من المواضيع التي تستدعي مستوى أعلى من الحماية القانونية بالنظر إلى صعوبة البيانات أو إلى انعدام وجود مسوّغ نظامي بديل.⁸⁹

أولاً: حالة كون الموافقة المسوّغ النظامي الوحيد للمعالجة

يُفصّل هذه الحالة أن تكون الموافقة الأساس القانوني الوحيد، الذي تستند إليه جهة التحكم في معالجة البيانات الشخصية، حيث لا يوجد مسوّغ نظامي آخر يجيز تلك المعالجة وفق أحكام النظام. وقد حددت المادة السادسة من نظام حماية البيانات الشخصية المبررات النظامية التي تُخفي عن استمرار الموافقة على النحو الآتي: لا تخضع معالجة بيانات الشخصية للموافقة اعتباراً فيما في الفقرة (1) من المادة (الخامسة) من النظام. في الأحوال الآتية"⁹⁰:

(1) عندما تخضع المعالجة مصنفة متحققة بحساب البيانات وكان الاتصال به متعبداً أو كان من الصعب تحقيق ذلك.

(2) عندما تكون المعالجة تقتضي نظام آخر أو تعيقاً لاتفاق سابق يكون صاحب البيانات الشخصية طرفاً فيه.

(3) إذا كانت جهة التحكم جهة عامة. وكانت تلك المعالجة مطلوبة لأمر من أمية أو لاستيفاء منصات قضائية.

⁸⁷ نصت الفقرة الثانية من المادة الحادية عشرة من اللائحة التفصيلية على ما يلي: "تتطلب الموافقة أن تكون مبرجة في الأحوال الآتية: 1- في حال كانت الموافقة هي المسوّغ النظامي الوحيد لمعالجة البيانات الشخصية. 2- في حال تضمنت معالجة بيانات حساسة. 3- في حال تضمنت المعالجة بيانات إسمية".

⁸⁸ انظر: عبد العزيز بن محمد، 2023، مصدر سبق ذكره، ص 354.

⁸⁹ المادة السادسة من اللائحة التفصيلية على ما يلي: "تتطلب الموافقة أن تكون مبرجة في الأحوال الآتية: 1- في حال كانت الموافقة هي المسوّغ النظامي الوحيد للمعالجة. 2- في حال تضمنت معالجة بيانات حساسة. 3- في حال تضمنت المعالجة بيانات إسمية".

(4) عندما تكون المعالجة ضرورية لتحقيق مصالح مشروعة لجهة التحكم، ما لم يخل ذلك إختراق صاحب بيانات شخصية أو يعارض مع مصالحه، ولم تكن تمت البيانات بيانات حساسة، وتبين المراجع الاستكشاف والضرورة المتحققة بذلك.³⁵⁴

وبناءً على ذلك، إذا تمت هذه المبررات، فإن معالجة البيانات لا تكون مشروعة إلا بتوافق صراحة من صاحب البيانات، بوضعها النوع الوحيد للمعالجة في هذه الحالة.

ثانياً: حالة معالجة البيانات الحساسة

أوجب اللائحة أن تكون الموافقة صريحة وواضحة عندما تتعلق بمعالجة بيانات حساسة. بالنظر إلى ضرورة طبيعتها وتأثيرها المحتمل على الخصوصية، وقد تحركت النقاش في المادة الأولى من البيانات الحساسة بأنها تلك التي تكشف عن أصل الفرد العرقي أو معتقداته الدينية أو آرائه السياسية أو انتمائه الفكري أو الثقافي، أو ما يتعلق بحالته الصحية أو الوراثية أو الجنسية أو بياناته الحمضية أو السموية أو بياناته الجينية، أو غيرها من البيانات التي تفسر خصوصيته على نحو بالغ.³⁵⁵

وبغض عن ذلك أن المشرع قد أولى البيانات الحساسة درجة حماية أعلى، مما يقتضي أن تكون الموافقة بمثابة مباشرة وصريحة وغير ضمنية، معاً لأي شخص أو استعمال في زيادة صاحبها.

ثالثاً: حالة معالجة البيانات الائتمانية

كما نصت اللائحة على اشتراط أن تكون الموافقة صريحة في حال كانت معالجة تتعلق بـ بيانات الائتمانية. نظراً لطبيعتها الخاصة وتأثيرها المباشر على السمعة المالية للفرد ومركزه الائتماني، وقد تحركت النظام في مادته الأولى البيانات الائتمانية بأنها البيانات الشخصية المتعلقة بالالتزامات المالية لصاحب البيانات، ومدى وفائه بها، وتاريخ تعاملاته الائتمانية مع الجهات المالية.

ومن ثم، فإن معالجة هذه النوع من البيانات لا يجوز أن تتم إلا بتوافق صراحة ومسقة من صاحبها، فيما لا يمتد انتهاك للمصلحة المالية أو إساءة في استخدامها.

³⁵⁴ نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م) ١٠١، وتاريخ ١٩٤٣/٢/٩هـ.

³⁵⁵ الفقرة ١ من المادة ٢١، مصدر سبق ذكره ص 354.

ويلاحظ أن اشتراط الصراحة في الموافقة في هذه الحالات يُجبر عن توجه المشرع السعودي نحو تعزيز مبدأ الشفافية والوضوح في معاملة البيانات، والاستعداد عن الموافقات الضمنية أو المستدركة التي قد تُفهم من سلوك أو مكونات حساب البيانات، فالموافقة الصريحة في هذا السياق تُشكّل حماية قانونية أساسية سواء لحماية الأفراد أو لتجديد المسؤولية النظامية على جهة التحكم عند وقوع المخالفة.

الضابط الرابع: أن توثق الموافقة بوسائل تتيح التحقق منها مستقبلاً

تتوزع هذه القاعدة بحية المحكمة بحفظ موافقات التي حصلت عليها من أصحاب البيانات والاستعداد لها للتحقق منها مستقبلاً، في حال حدوث خرق لبيانات وإفصاح صاحب البيانات عن بياناته الشخصية للجهة المحكمة بشكل غير قانوني، أو في حال اعتراض صاحب البيانات على معالجة الجهة المحكمة لبياناته الشخصية. يجب على الجهة المحكمة تخزين هذه البيانات حتى تتمكن السلطات من التحقق من الموافقة والالتزام من أسبقاتها للمتطلبات التنظيمية، لا يجوز للجهة المحكمة الادعاء بأنها أتت من تخزين أو لا تحتفظ به، حيث أنها في هذه الحالة تتحمل المسؤولية الكاملة حتى لو تم الحصول على الموافقة بطريقة قانونية وسليمة⁴³.

يتمكن عادة هذا يعني أن عبء الإثبات يقع بالموافقة في حالة وجود نزاع يقع على عاتق جهة المحكمة، يجب عليها إثبات أن الموافقة التي اعتمدت عليها كمبرر قانوني لمعالجة بيانات الشخصية كانت صحيحة وتم احترامها وفقاً للمتطلبات التنظيمية المنصوص عليها في القانون والوائح⁴⁴.

⁴³ Breen, S et al. (2023). GDPR: Is your consent valid?. Business Information Review (BIR), (XVI), 10, 1177-1266382120903254.

⁴⁴ انظر: عبد العزيز بن محمد، 2023، مصدر سبق ذكره ص 3543.

البحث الثاني: ضمانات حماية البيانات الشخصية في النظام السعودي

تعتمد الأنظمة القانونية التقييدية، بما في ذلك المسؤولية المدنية التقديرية، على إثبات ثلاثة عناصر رئيسية: خطأ، ونظر، والعلاقة السببية بينهما. عندما يتسبب نظام ذكي في ضرر نتيجة خطأ خوارزمي "ناتج عن التعلم الذاتي" بدلاً من خطأ بشري واضح في الترميز، يصبح إثبات عنصر "خطأ" التقني أمرًا شبه مستحيل، وتتفاقم الصعوبة بسبب تعدي "المصدوق الأسود"، الذي يجعل من المستحيل على المتضرر إثبات أو نظرو ناتج بشكل مباشر عن تصرف الخوارزمية، وليس عن مداخلات بيانات أو عوامل خارجية⁴⁴.

لمعالجة تعدي إثباتات في سياق المسؤولية المدنية، تتميز الدراسات القانونية إلى أن نظام المعاملات المدنية السعودي عالج المسؤولية عن الأضرار تحت باب "مسؤولية عن الضرر الناجم عن الأخطاء"، يمكن تكليف المالك المخطئ، على الرغم من قدراته المعرفية، كـ "شخص" خضع لمراقبة شخص (يسمى الخادم).

إن تطبيق نظرية المسؤولية عن الأخطاء مع المتضرر مساهم قانونياً فعالاً لتعويض. حيث تكون المسؤولية في هذه الحالة موضوعية (بدون الحاجة لإثبات خطأ) على "حارس الشيء" الذي يملك السيطرة الفعلية على النظام. هذا التكليف العكسي يضع عبء التعويض على حارس النظام (جهة التحكم/المستخدم)، ويضمن حماية الحقوق الاقتصادية والمدنية للمتضررين، متجاوزاً بذلك معضلة إثبات خطأ بشري أو خوارزمي. ومع ذلك، لا يكفي هذا الحل لتعويض عن الأضرار بعد وقوعها، بل يجب استكماله بالتدابير الاستباقية. من أبرز جهة التحكم باتيات حفاة مع الأضرار في نظام الأول، استناد إلى الأعراف الأخلاقية سدياً التي تنزه المتضررين من التعويض.

تحدد القوانين المنظمة لحماية البيانات الشخصية الضوابط والقيود التي يجب الالتزام بها عند معالجة هذه البيانات، ووفقاً للمادة (1/5) من نظام حماية البيانات الشخصية، تُعرف المعالجة بأنها أي عملية تُجرى على بيانات الشخصية بأي وسيلة كانت، سواء يدوية أو آلية، وتشمل على سبل: الجمع والتسجيل، والحفظ والتعبئة، والتوزيع والتسويق والتخزين، والتعديل والتحديث، والدمج، والاسترجاع والاستخدام، والإفصاح والنقل والتسليم، والمشاركة أو ربط البيانات، إضافة إلى سحب ومسح والإزالة⁴⁵.

⁴⁴ المحامي أحمد محمد، (2023)، حل في خصوصية بيانات شخصية ومعلومات حياتية في عصر التحول الرقمي: دراسة حالية في نظام سعودي، (دورة العمل، ص 49).

⁴⁵ المادة (1/5) من نظام حماية البيانات الشخصية.

وترتبط ضمانات حماية البيانات الشخصية ارتباطاً وثيقاً بحقوق الحق في الخصوصية. وقد نص النصاب على مجموعة من الضمانات التي تنقسم إلى ثلاث فروع رئيسية: ضمانات تمتع عممية المعالجة وأخرى ترافقها أثناء التنفيذ. وتلكه تبيها لضمان سلامة الناتج وحماية الحقوق⁴⁹⁶.

المطلب الأول - ضمانات سابقة على معالجة البيانات الشخصية

تتضمن الضمانات السابقة على معالجة البيانات الشخصية مجموعة من الإجراءات التي أقرها النظم بهدف تعزيز مستوى الحماية لبيانات الأفراد. وتلكه يراها على النحو الآتي:

أولاً: اعتماد سياسة واضحة لخصوصية البيانات الشخصية

يعد وجود سياسة خصوصية واضحة من أبرز الضمانات التي تسبق عممية معالجة البيانات الشخصية، وذلك استناداً إلى ما نصت عليه المادة الثانية عشرة من نصاب حماية البيانات الشخصية. إذ توجب النظام على جهة التحكم - وهي أي جهة عامة أو أي شخصية صيغية أو اعتبارية خاصة تحدد الغرض من معالجة البيانات ووظيفتها سواء قامت بها نفسها أو من خلال جهة معالجة - أن تعتمد سياسة خصوصية عامة ومتكاملة تكفي حماية البيانات الشخصية، وأن تُتاح هذه السياسة للأفراد المعنيين قبل جمع بياناتهم.

ويهدف ذلك إلى تمكين الأفراد من ممارسة حقوقهم في الموافقة أو الرفض على معالجة بياناتهم عن علم ودرية. انسجاماً مع مبادئ الشفافية والمشاركة. الذين يقتضيان إبلاغ صاحب البيانات مسبقاً بجميع الإجراءات التي ستُخذ بشأن بياناته في حال موافقته على المعالجة، وبالتشري مع ذلك. كُرمت المادة الثالثة عشرة من النظام جهة التحكم - عند جمع البيانات الشخصية من صاحبها مباشرة - باتخاذ الوسائل الكافية لإحاطته علماً بعدد أفراد قبل البدء في الجمع. وهي⁴⁹⁷:

- التسوية النظامية أو العملي الذي يور جمع بياناته الشخصية.
- العرض من الجمع. وبيان ما إذا كان إلزامياً أو اختيارياً. مع التأكيد على أن البيانات لن تُعالج لاحقاً بما يخالف الغرض الأصلي أو في غير الحالات المنصوص عليها في المادة (العاشرة) من النظام.
- هوية الجهة التي تجمع البيانات وتحتفظ بها. لأغراضها. ما لم يكن الجمع لأغراض أمنية.

⁴⁹⁶ المحامي أحمد محمد. 2023، مصدر سبق ذكره ص 496.

⁴⁹⁷ المادة ثلث عشرة من النظام. لتعريف نصاب جمع البيانات الشخصية.

- الجهات التي ستفصح عن البيانات الشخصية وحفظها، وبيان ما إذا كانت البيانات ستبقى أم تحتاج خارج المؤسسة.

- الآثار والمخاطر المحتملة المترتبة على عدم إتباع عملية جمع البيانات الشخصية.

وتعد هذه الخطوات خطوة أساسية لضمان عدم الأفراد بكيفية التعامل مع بياناتهم، وتعزيز ثقتهم بالجهات التي تتولى معالجتها.

ثانياً: الموافقة المسبقة

تعد المسألة في المادة الخامسة من نظام حماية البيانات الشخصية على حفظ معاملة البيانات الشخصية أو تغيير العرض من معالجتها إلا بعد الحصول على موافقة مسبقة من صاحب البيانات، وبأن هذا الالتزام يستلزم مع مبدأ احترام الحق في الخصوصية، إذ مع نظام تصاحب البيانات الحق في الرجوع عن موافقته في أي وقت⁴⁹.

ومن الخدي بالذات أن النظام لم يحدد ما إذا كانت الموافقة المطلوبة يجب أن تكون صريحة أم يمكنها بالتضمنية، غير أن الرأي الراجح يذهب إلى أن الموافقة الصريحة هي التي ينبغي اعتمادها، نظراً لأن معاملة بيانات الشخصية تمس خصوصية الأفراد بشكل مباشر، كما يستلزم وضوح الرضا وعدم الاكتفاء بأي دلالة ضمنية عليه، فإذ اللائحة التنفيذية نظام يفترض أن تقتض صراحة على اشتراط الموافقة الصريحة، حتى لا تفقد موافقة مسبقة قيمتها القانونية والمواقعة إذا تم الاكتفاء بالرضا التضمني⁵⁰.

ومع أن الأصل هو ضرورة الحصول على الموافقة المسبقة من صاحب البيانات، إلا أن نظام أخبار استثناءات محددة على هذا الأصل في بعض الحالات التي تنصها الضرورة. وذلك وفقاً لما ورد في المادة السادسة، ومن أبرزها⁵¹:

1. إذا كانت المعالجة تحقق مصلحة متحققة لصاحب البيانات، وكان الاتصال به متعدياً أو صعب التحقيق.
2. إذا تمت المعالجة بموجب نظام آخر، أو تنفيذاً لاتفاق سابق يكون صاحب البيانات طرفاً فيه.
3. إذا كانت جهة الحكم جهة عامة، وكانت المعالجة مضمونة لأمر من أمانة أو إرفاء بمتطلبات قضائية.

⁴⁹ المادة الخامسة من نظام حماية نظام حماية البيانات الشخصية.

⁵⁰ المحامي أحمد محمد، 2023، مصدر سبق ذكره ص 497.

⁵¹ المادة السادسة من نظام حماية نظام حماية البيانات الشخصية.

كما أجاز النظام - بموجب المادة السابعة والعشرين - جمع البيانات الشخصية أو معالجتها لأغراض عملية أو تقنية أو إحصائية دون الحاجة إلى موافقة صاحبها. وذلك في الحالات التالية¹⁰¹:

1. إذا لم تتضمن البيانات الشخصية ما يدل على هوية صاحبها تحديدًا.
2. إذا كان سيتم إتلاف ما يدل على هوية صاحب البيانات أثناء المعالجة وقبل الإفصاح عنها لأي جهة أخرى. بشرط ألا تكون البيانات حساسة.
3. إذا كانت عملية الجمع أو المعالجة تهدف الاعتراف بتسند إلى نظام آخر أو إلى اتفاق سابق يكون صاحب البيانات طرفًا فيه.

وبذلك، فإن الموافقة المستنيرة تبقى هي القاعدة العامة في معالجة البيانات الشخصية، ولا يجوز الإخلال بها إلا في الحالات الاستثنائية التي نلص عنها النظام على سبيل الحصر.

ثالثاً- معالجة البيانات في حدود الغرض المخصص

أقرّ النظام - كما هو مذكور أعلاه - حظر معالجة البيانات الشخصية بغرض العرض لأغراض أخرى غير الغرض المخصص. إلا أن ذلك عني جهة التحكم الإلكتروني في تضاريف نطاق الغرض المحدد عند جمع البيانات، وعدم تجاوز هذا النطاق أو استخدام البيانات في أغراض أخرى غير مصرح بها. وبعد هذا التمهيد من أن أكثر الأساسيات لحماية الخصوصية وضمن الاستخدام المشروع لبيانات الشخصية¹⁰².

إلا أن النظام أجاز - استثناءً من هذا الأصل - معالجة بيانات غير الغرض المخصص في حالات محددة نصت عليها المادة العاشر ذ. وتنص في الآتي¹⁰³:

- موافقة صاحب البيانات الشخصية على المعالجة بغرض آخر. وفقاً لأحكام النظام.
- إذا كانت البيانات الشخصية مباحة للعموم، أو جرى جمعها من مصادر عامة متاح للجميع.

¹⁰¹ المادة السابعة والعشرين من الدستور المنقحة الصادرة عام 2011م تحت إشراف المحكمة الدستورية.

¹⁰² المحامي أحمد محمد، (2023) بر مصدر على ذلك ص 497.

¹⁰³ المادة العاشر ذ من الدستور المنقحة الصادرة عام 2011م تحت إشراف المحكمة الدستورية.

- إذا كانت جهة التحكم جهة عامة، وكان جمع البيانات من غير صاحبها مباحاً أو معالجتها لغرض مختلف مطلقاً لأغراض أمنية، أو تنفيذ نظام آخر، أو لوفاء بالتطلبات قضائية، وذلك وفق الضوابط التي تحددها النواحي التنفيذية.
 - إذا كان الالتزام بحظر المعالجة قد يُنتهك ضرراً بصاحب البيانات الشخصية أو يؤثر على مصالحه الحيوية، وذلك وفقاً للأحكام والإجراءات التي تحددها النواحي.
 - إذا كانت المعالجة ضرورية لحماية الصحة أو السلامة العامة، أو لحماية حيازة فرد أو مجموعة من الأفراد أو صحتهم، على أن تُحدد النواحي الضوابط والإجراءات المنظمة لذلك.
 - إذا كانت البيانات الشخصية لن تُسحق أو تُحفظ بصيغة تُتيح تحديد هوية صاحبها بصورة مباشرة أو غير مباشرة مع مراعاة الضوابط والإجراءات التي تُبينها النواحي التنفيذية.
- وبناءً على ذلك، فإن الأصل هو تقييد معالجة البيانات الشخصية في حدود العرض الذي جُمعت من أجله، ولا يجوز تجاوز هذا القيد إلا في الحالات الاستثنائية المنصوص عليها نظاماً، وبما يضمن تحقيق التوازن بين متطلبات الصحة العامة وحماية خصوصية الأفراد¹⁴.

المطلب الثاني: ضمانات معاصرة لمعالجة البيانات الشخصية

نظراً لما يكتنه بيانات شخصية من أهمية كبيرة، لا يكتف النظام بوضع ضمانات سابقة على معالجتها، بل يحرص أيضاً أيضاً على مجموعة من الضمانات المعاصرة أثناء المعالجة، بهدف تعزيز مستوى حماية المقررة لها بما يتناسب مع حساسيتها وأثرها المباشر على خصوصية الأفراد. ومن أبرز هذه الضمانات ما يلي:

أولاً: إشعار صاحب البيانات بأي تسرب أو تلف أو وصول غير مشروع إلى بياناته الشخصية

يُعدّ اتخاذ المشرعين من نظام حماية بيانات شخصية على ما يلي:

- 1- تنبّه جهة التحكم بإشعار الجهة المختصة فور علمها بحدوث تسرب أو تلف في بيانات الشخصية، أو بحدوث وصول غير مشروع إليها.

¹⁴ المحمدي، محمد محمد، 2023، مصدر سبق ذكره ص 497.

2- تُحدد النواحي التنفيذية الحالات التي يجب فيها على جهة التحكم إشعار صاحب البيانات الشخصية عند حدوث أي من تلك الوقائع.

وبذا تكتل من شأن السرب أو الكشف أو الوصول غير المشروع إحقاق ضرر حسيماً بصاحب البيانات أو بيانات الشخصية، فيجب على جهة التحكم إشعاره فوراً.

وتكمن أهمية هذا الإشعار في تمكين صاحب البيانات من اتخاذ ما يلزم من إجراءات حماية حقوقه ومصالحه من العدول عن موقفه السابق على المعالجة، أو طلب تعديل بياناته أو حذفها إذا اقتضى الأمر ذلك، ويستفاد من نص المادة أن النظام فرّق بين حالتين:

- الحالة الأولى: إذا كان السرب أو الكشف أو الوصول غير المشروع ناتجاً عن ضرر حسيماً على صاحب البيانات أو على نفسه، فالإشعار واجب على الفور.
- الحالة الثانية: إذا لم يكن هناك ضرر حسيماً، فإن النواحي التنفيذية هي التي تُحدد الأحوال التي تستوجب إشعار صاحب البيانات.

وبذلك، يظهر حرص النظام على تحقيق التوازن بين مصلوات الأمن العمومي وحقوق الأفراد في المعرفة والشفافية، بما يعزز الثقة في الجهات التي تترتب معالجة بيانات الشخصية ويضمن استجابة فورية لأي عرق قد يمس خصوصية الأفراد أو ياتقهم.

ثانياً: حق صاحب البيانات في الوصول إلى بياناته الشخصية

يعد حق الوصول إلى البيانات الشخصية من الضمانات المعاصرة للأشخاص التي أقرها النظام لتعزيز حماية الأفراد وحفاظية المعالجة. إذ نصت الفقرة السابعة من المادة الرابعة من نظام حماية بيانات الشخصية على أن لصاحب البيانات الحق في الوصول إلى بياناته الشخصية المعروفة لدى جهة التحكم، ويشمل ذلك الإطلاع عليها والوصول على نسخة منها بصيغة واضحة ومطابقة لمضمون السجلات، ويهدف هذا الحق إلى تمكين صاحب بيانات من التحقق من دقة معلوماته وسلامتها، ومطابقته من أن معالجتها تتم وفقاً للأغراض النظامية المقررة¹¹⁵.

¹¹⁵ الفقرة ثمانية من مادة السابعة من نظام حماية بيانات الشخصية.

ومن الناحية الصياغية، يمكن القول - كما يلاحظ - أن استخدام المصطلح «وصول إلى البيانات» قد يكون غير ضروري، إذ إن الوصول يُفهم صمماً من معنى الاختلاع، فلا يمكن الاختلاع دون وصول فعلي إلى البيانات، لذلك، ولتحسين الصياغة، كان يمكن الاكتفاء بمصطلح الاختلاع على البيانات الشخصية دون أن يحدث ذلك أي نقص في المعنى أو التضمين¹⁰⁶.

ثالثاً: حق صاحب البيانات في تصحيح بياناته أو تحديثها أو إلغاؤها

من الحقوق الجوهرية التي قررها النظام لصاحب البيانات الشخصية حقّه في التحكم بحقوق بياناته، وذلك غير متكبّه من طلب تصحيح بياناته إذا كانت خاطئة، أو إلغاؤها إذا كانت ناقصة، أو تحديثها عند حدوث تغيير، أو إلغاؤها في حال انتهاء الغرض من جمعها.

وقد نصّت المادة الرابعة من النظام على أن لصاحب البيانات، وفقاً للأحكام النظامية، الحقوق الآتية¹⁰⁷:

- 1- حق في طلب تصحيح بياناته الشخصية أو إلغاؤها أو تحديثها.
 - 2- حق في طلب إلغاف بياناته الشخصية المتوفرة لدى جهة التحكم لما انتهت الحاجة إليه منها.
- ويلاحظ أن المصطلح المستخدم مصطلح الإلغاف بدلاً من الحذف وهو غير دقيق له دلالة قانونية وتقنية، فالإلغاف يعني إنهاء صلاحية البيانات كلياً وجعلها غير قابلة للاسترجاع أو الاستخدام، حتى وإن بقيت مادية أو رقمية في النظام، بينما الحذف يعني إزالة وجودها فقط دون ضمان عدم إمكانية استعادتها. ولم يترك النظام هذا الحق مطلقاً، بل قيده بعدد من الاستثناءات التي وردت في المادة الثامنة عشرة، حيث نصت على ما يلي:

1. تنزه جهة التحكم بالإلغاف البيانات الشخصية فور انتهاء الغرض من جمعها.
2. ومع ذلك، يجوز لها الاحتفاظ بالبيانات بعد انتهاء الغرض من جمعها إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد، وذلك وفق الضوابط التي تحددها المراجع التشريعية.

¹⁰⁶ المحمدي، أحمد محمد، 2023، مصدر سبق ذكره ص 498.

¹⁰⁷ المادة الرابعة من نظام حماية بيانات أصحاب.

3. كما أجاز النظم الاحتفاظ بالبيانات حتى بعد انتهاء الخراف في الحالات التي تستوجبها متطلبات نظامية أو قانونية معينة. وفق ما تحدده المراجع.

وبذلك، ينص على أن النظم راعى في هذا الجانب تحقيق التوازن بين حق الأفراد في حماية بياناتهم واحتياجات الجهات في الاحتفاظ بها لأغراض مشروعة مع ضمان أن أي احتفاظ لاحق يتم بصورة تحول دون المساس بخصوصية الأفراد أو التعرف على هويتهم¹⁰⁸.

المطلب الثالث: ضمانات لاحقة لمعالجة البيانات الشخصية

تتبع الضمانات اللاحقة لمعالجة البيانات الشخصية إلى حماية جزائية وحماية مدنية وذلك على النحو الآتي:

أولاً - الحماية الجزائية للبيانات الشخصية:

بخلاف من ينظم بأهمية بيانات الشخصية وما تنسب من قيمة بالغة قرر إعطاء حماية جزائية عليها، فنص النظام على ثلاثة أنواع من العقوبات: عقوبات مالية (العقوبات)، وعقوبة الإعدام، وعقوبات مالية تعزيرية (حبس)، ويحدد نوع العقوبة بحسب طبيعة المخالفة المرتكبة.

1- مخالفة الإفصاح عن البيانات الحساسة أو نشرها بالمخالفة للنظام:

تنص المادة الخامسة والثلاثون على أن كل من أفصح عن بيانات حساسة أو نشرها بالمخالفة لأحكام النظام يعاقب بالسجن مدة لا تتجاوز سنتين، وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين. وذلك إذا كان النص قد تم بقصد الإضرار بصاحب البيانات أو لتحقيق منفعة شخصية¹⁰⁹.

وبذلك، يشترط لنظام نفي الإضرار وتوقيع العقوبة انصوحاً عنينا نوافي المقصد الخامس. والتمس في نية الإضرار بصاحب البيانات أو تحقيق مصلحة شخصية. أما إذا انطى هذا المقصد الحاصل، فلا يعني ذلك انشاء العقوبة كما هو بل يعاقب المعلن استناداً إلى وصف أعم ليعمل بوصفه مخالفاً لأحكام النظام وتطبق عليه حيثما عقوبة الإعدام أو الغرامة التي لا تتجاوز خمسة ملايين ريال. وفقاً للمادة السادسة والثلاثين من النظام¹¹⁰.

¹⁰⁸ المحامي أحمد محمد، 2023، مصدر سبق ذكره ص 491.

¹⁰⁹ المادة الخامسة والثلاثون من نص حماية بيانات الشخص.

¹¹⁰ المادة السادسة والثلاثون من نص حماية بيانات الشخص.

2- مخالفة نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارجية:

حظر المنظم على جهة التحكم نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارجية، إلا في حالات محددة، مثل تنفيذ التزامات ناشئة عن اتفاقية تكون المملكة طرفاً فيها، أو تحقيق مصلحة وطنية، أو لأغراض أخرى تحددها اللوائح. وذلك بخلاف استيفاء مجموعة من الضوابط المنصوص عليها في المادة التاسعة والعشرين من النظام، وهي¹¹¹:

- ألا يتناسب على عملية النقل أو الإفصاح أي مصلح بالأمن الوطني أو بمصالح المملكة الحيوية.
- توافره ضمانات كافية تكفل حماية البيانات الشخصية، معقولة أو المنصوح عنها، والخفاظ على سريتها.
- بحيث لا تقل معايير حماية المنطقة عن تلك المنصوص عليها في النظام واللوائح التنفيذية.
- أن يقتصر النقل أو الإفصاح على الحد الأدنى من البيانات الشخصية اللازمة لتحقيق الغرض المقصود.
- الحصول على موافقة الجهة المختصة على عملية النقل أو الإفصاح، وفقاً لما تحدده اللوائح.

وقد نصت الفقرة (ب) من المادة الخامسة والملايين على أن مخالفة هذه الأحكام تُعد جريمة يعاقب مرتكبها بالسجن مدة لا تتجاوز سنة واحدة، وبغرامة لا تزيد على مئتين ريال، أو بإحدى هاتين العقوبتين¹¹².

3- مخالفة أي حكم من أحكام النظام أو اللوائح في الحالات التي لم يرد بشأنها نص خاص:

على المنظم في المادة السادسة والملايين على أنه في حال ارتكاب أي مخالفة لأحكام النظام أو لوائحه التنفيذية دون أن يرد بشأنها نص خاص في المادة الخامسة والملايين، تُطبق على المخالف - سواء كان شخصاً طبيعياً أو اعتبارياً من حيث الخاضعة لنظام - عقوبة الإعدام أو الغرامة التي لا تتجاوز خمسة ملايين ريال، كما أنجار النظام مضاعفة الغرامة في حال تكرار المخالفة، حتى وإن تجاوزت الحد الأقصى المقرر هذه طريقة ألا تتجاوز ضعف هذا الحد¹¹³. ويتضح من ذلك، وبعد استعراض المخالفات والعقوبات المنصوص عليها، أن المنظم قد منح البيانات الشخصية أهمية مستوى أعلى من الحماية مقارنة بغيرها من البيانات إذ جعل عقوبة

¹¹¹ المادة التاسعة والعشرين من نظام حماية بيانات الشخص.

¹¹² الفقرة (ب) من المادة السادسة والملايين. وبالمقابل من نظام حماية بيانات الشخص.

¹¹³ المادة السادسة والملايين. وبالمقابل من نظام حماية بيانات الشخص.

الإفصاح عنها أو نشرها بانتهاكاً للنظام المعلن مدة لا تزيد على سنتين. ويعرّف هذا تجاوز ثلاثة ملايين ريال، أو إحدى حاتين العقوبتين. وهي أحد العقوبات المنصوص عليها في النظام¹¹⁴.

ثانياً: الحماية المدنية للبيانات الشخصية

في بقسم المنظم على تقرير الحماية الخالية للبيانات الشخصية، بل أقر أيضاً حماية مدنية بموجب المادة الأربعين من النظام، التي منحت كل من حقه ضرر نتيجة ارتكاب أي من المخالفات المنصوص عليها في النظام أو بوالته، الحق في المتابعة أمام المحكمة المختصة بالتعويض عن الضرر المادي أو المعنوي بما يتناسب مع حجم الضرر¹¹⁵.

وتقيد حق صاحب البيانات في التعويض، يجب توفر ثلاثة أركان أساسية:

- 1- **دكن الخطأ:** وينقسم في ارتكاب أحد الأفعال التي تعد مخالفة لأحكام النظام أو التراجع.
 - 2- **كن الضرر:** وهو أن يتسبب على الفعل ضرر لصاحب البيانات. سواء كان ضرراً مادياً كمصاريف مالية، أو ضرراً معنوياً كالتدليس بالسمعة أو الخصوصية.
 - 3- **رابطة السببية:** أي وجود علاقة سببية بين الخطأ المرتكب والضرر الناتج عنه.
- فعلى سبب المثال، قد يؤدي إنشاء البيانات المصرفية إلى إحراق ضرر مادي بصاحبها، بينما يؤدي إنشاء بيانات الصحية إلى ضرر مزدوج، مادي ومعنوي في آن واحد، ويقع عبء إثبات الضرر على عاتق صاحب البيانات الشخصية المتطابق بالتعويض¹¹⁶.

¹¹⁴ المحمدي، أحمد محمد، 2023، مصدر سبق ذكره ص 403.

¹¹⁵ المادة الأربعين، من نظام حماية البيانات الشخصية.

¹¹⁶ المحمدي، أحمد محمد، 2023، مصدر سبق ذكره ص 405.

الفصل الثالث:

الأساس القانوني لحماية خصوصية المعلومات في ظل تطبيقات الذكاء الاصطناعي في المملكة العربية السعودية.

يشهد العالم اليوم فترة حافلة في مجال الذكاء الاصطناعي، الذي أصبح أحد أهم أدوات التحول الرقمي والتنمية الاقتصادية والاجتماعية. فقد غيرت تطبيقات الذكاء الاصطناعي طريقة جمع وتخزين واستخدام بيانات الشخصية، إذ باتت تعتمد على تقنيات متقدمة قادرة على استخراج الأنماط المخفية وتنبؤات دقيقة حول الأفراد، مما جعل البيانات تُعد "النفط الجديد" في العصر الرقمي. غير أن هذا التوسع الكبير في معالجة بيانات الشخصية من خلال أنظمة الذكاء الاصطناعي أثار تحديات قانونية وأخلاقية عميقة تتعلق بحماية خصوصية الأفراد وضمان استخدام بياناتهم ضمن أطر مشروعة وأمنة¹¹⁷.

ويُعد الحق في الخصوصية من الحقوق الأساسية التي كفلتها الشريعة الإسلامية قبل أن تُقرها المواثيق الدولية، إذ أكد الإسلام على حرمة الحياة الخاصة وعدم التجسس أو إفشاء الأسرار، وهو ما يُعد الأساس الأخلاقي والقيمي لتدريعات حديثة في المملكة العربية السعودية، ومع التطور التقني الهائل الذي يشهده العالم، أدركت المملكة أهمية وضع إطار قانوني متكامل لحماية البيانات الشخصية وتنظيم استخدامها بما يتوافق مع رؤية السعودية 2030، التي تسعى إلى بناء اقتصاد رقمي متطور يحفظ الحقوق ويعزز الثقة في البيئة التقنية.

وفي هذا الإطار، صدر نظام حماية البيانات الشخصية السعودي، بموجب المرسوم الملكي رقم (د: 19) وتاريخ 9 / 2 / 1443هـ، ليكون الإطار التشريعي الرئيس الذي يطمح جمع بيانات الشخصية ومعالجتها وتخزينها وتقييمها، وقد وضع النظام مبادئ أساسية من شروط المراقبة الصريحة من صاحب البيانات، واتخاذ التدابير لمعالجتها وعدم الإفصاح عن بيانات إلا في حالات محددة، إلى جانب إدراج الجهات المعالجة بأحد التدابير الأمنية اللازمة لحماية بيانات من الاعتراق أو الاستخدام غير المشروع. كما أن النظام منح الأفراد حقوقاً قانونية واضحة، منها الحق في الإطلاع على بياناتهم، وطلب تصحيحها أو حذفها، وهو ما يندرج ركيزة لحماية الخصوصية الرقمية في المملكة.

¹¹⁷ محمد حسن عبد الله نظام سعودي حماية بيانات الشخصية (تدقيقاً قانونياً)، دراسة تأصيلية معاصرة في ضوء المنهجية القانونية وبعض التشريعات ذات الصلة، مجلة علوم القانون، جامعة محمد، كلية الحقوق، يوليو 2021، ص 53.

المبحث الأول: تحديات الناطق القانوني لحماية خصوصية المعلومات في ظل تطبيقات الذكاء الاصطناعي

إن بقرار قانون وطني أو تنظيم استراتيجي وحشية حماية أحد حقوق الإنسان يمكن أن يكون فعّالاً. ويعزى ذلك إلى توفر عنصر السيطرة والعيادة ووجود جهة مختصة بالرقابة ومنع الانتهاك أو استمراره بما يتيح أيضاً إمكانية التحويل وملاحقة المخالفين، إلا أن الوضع يختلف في ظل الذكاء الاصطناعي، الذي قد تمكنه أي فرد دون أن يكون مموناً لأي جهة محددة. حيث لا توجد سلطة مركزية أو جهة سيادية توفر الحماية أو تتيح وسائل حماية قانونية عند التعرض لانتهاك خصوصية الأفراد¹¹⁸.

ومن هذا المنطلق، ينصح أن البيانات الشخصية لدى اليوم الوجهة أصبحت حماية أكثر في الخصوصية في العالم الرقمي. كما أن جميعها ومعالجتها باستخدام الذكاء الاصطناعي يعد مسألة حساسة وحرجية تستدعي وعي المستخدمين والعامة، بل وحتى الحكومات، بأهمية حماية البيانات الشخصية واتخاذ آليات التعامل معها بشكل يضمن استخدامها بطريقة فعّالة وآمنة ضمن حدود القانونية المعمول بها.

المطلب الأول: مصادر تحديد حق الخصوصية المعلوماتية

يشير بعض الشخصيين إلى أن التكنولوجيا، أي السيطرة المتزايدة بحوسيب والأنظمة الرقمية، قد تصل إلى درجة كبيرة من القوّة حيث تعد من نضاق الحياة الخاصة للفرد. وترتبط حياة الإنسان وعائلته بهذه الأجهزة عندما تتفاعل مع مصالح اقتصادية أو اجتماعية محددة. في هذه الحالة، يصبح الإنسان محدود الإرادة ومستعداً في قراراته للترديد ومترغماً من جراء من شخصيته. ومن هذا المنطلق فإن الخطر على البشر قد لا يكون حرجياً بدرجة من قد يكون في السيطرة الرقمية بحوسيب على حياتهم.

وبالرغم من أن هذه الخطر قد تبدو مستعجلة ومبالغاً فيها من حيث تحديد الحوسيب للخصوصية، إلا أنها تعكس الفتن الحقيقي من الاستخدام غير المشروع لنظمية خاصة في ما يتعلق بالحوسيب وكل ما من شأنه الإخلال بالحق في الحياة الخاصة. ولتعد البيانات الشخصية مصدراً عملياً لتطبيقات الذكاء الاصطناعي، إذ يتم جمعها وتخزينها واستغلالها في تدريب النماذج الذكية وتمكين أدائها.

¹¹⁸ محمد م. خدي، (2023)، حق الخصوصية المعلوماتية في ضوء الذكاء الاصطناعي، مجلة دراسات بحوث في الاقتصاد، العدد

العدد 2، ص 468.

وفي هذا السياق، يمكن ملاحظة تخصيص النطاق الرئيسية لمصادر تحديد، حتى «حصرية المعلوماتية على النحو التالي:

الفرع الأول- جمع البيانات الشخصية

توجد العديد من الآليات والطرق التي تعتمد عليها التطبيقات الإلكترونية في جمع بيانات الأفراد الشخصية، ومنها:

أولاً: التجميع غير المشروع لبيانات الشخصية عبر تقنية الكوكيز (Cookies)

تعرف تقنية الكوكيز (Cookies) بأنها ملفات صغيرة يقوم موقع الويب بإرسالها وتخزينها على القرص لتسبب حينئذ استخدامه عند قيامه بزيارة الموقع أو تصفحه، وتكمن خطورتها في قدرتها على «تجميع وتخزين كميات كبيرة»¹¹⁶.

تتكون تقنية الكوكيز من أربعة عناصر رئيسة:

يشمل **العنصر الأول** في سطر ترويسة الكوكيز (Cookie Header Line) الذي يدرج ضمن رسالة الطلب المرسلة من متصفح المستخدم إلى خادم الموقع،

أما **العنصر الثاني** فهو رسالة الرد (Response Message) التي تتضمن معلومات الكوكيز المرسلة من الموقع إلى المتصفح،

ويأتي **العنصر الثالث** في صورة ملف كوكيز مخزن على الجهاز المحلي للمستخدم يُدار بواسطة المتصفح ويُستخدم لتتبع نشاطه وتخزين تفضيلاته،

في حين يشمل **العنصر الرابع** في قاعدة بيانات موجودة على خادم موقع الويب تُستخدم لإدارة المعلومات المجمعة من الكوكيز وتنظيمها بما يخدم أغراض الترويج التحليلية أو التسويقية¹¹⁷.

¹¹⁶ – Fabrice NAFTALSKY , ŒUVRE COLLECTIVE Sous LA DIRECTION DE PHILIPPE – HENRI DUTHIEL , Fonctionnement de l'association , partie 4 , 2016 ; actualization : Avril 2019 ; N:3.

– L'utilisation de cookies constitue un traitement de données – conseil d'Etat 6 juin 2018 – Le bon 2018 , Recueil Lebon – Recueil des décisions du conseil d'Etat 2018 www.Dalloz.fr – com.

تُعد عملية جمع البيانات الشخصية غير تقنية الكوكيز من أكثر القضايا إثارة للجدل في ميدان حماية الخصوصية الرقمية. ما تفتقر إليه من مخاطر متعددة الأبعاد نفس أمن وسرية المعلومات الشخصية المستخدمة، الإنترنت، هيئة التقنية، على الرغم من دورها في تحفيز تجربة التصفح وتسهيل المعاملات الإلكترونية، أصبحت اليوم أداة رئيسة في تجميع البيانات الشخصية على نطاق واسع. خاصة مع ازدياد الاعتماد على التجارة الإلكترونية، حيث تم معصم عمليات البيع والشراء غير المرفق التي تستخدم الكوكيز، مما يفرض على المستخدمين الإفصاح عن قدر كبير من بياناتهم الخاصة من معلومات الاتصال والبيانات المالية.

وتكمن الضرورة الحقيقية في أن هذه العمليات قد تتطور إلى بناء قواعد بيانات ضخمة ومتكاملة عن الأفراد، تتضمن تفاصيل دقيقة عن سلوكهم واهتماماتهم، وربما تُستخدم لأغراض تتجاوز ما هو مصرح به أو معترف به. ما يجعلها خطيرة، خاصة، خصوصية المستخدمين وأمنهم المعلوماتي، كما أن وسائل تجميع البيانات غير هذه التقنية لا تقتصر على التصفح العادي لمواقع الويب. بل تمتد لتشمل الاتصالات الرقمية المباشرة، والشبكات غير الشبكات الحديثة، وأجهزة الحوسبة المحمولة أو ما يُعرف بـ "كمبيوترات جيبي". إضافة إلى التقنيات المعتمدة على الاتصال عن بُعد مثل أنظمة الدفع الإلكتروني والأقمار الصناعية، الأمر الذي يزيد من تعقيد الرقابة القانونية والتقنية على عمليات جمع البيانات الشخصية واستخدامها.¹²¹

ويسمى تجميع البيانات الشخصية غير تقنية الكوكيز بالصفة السلبية، بمعنى أن له لا يعد أمراً مشروطاً أو غير مشروط بصورة مطلقة، بل إن المشروعية تدور في إطار الضابط العام الذي ذكره. وبعده مشروعية تدور في إطار مخالفة هذا الضابط، أي أن مشروعية تجميع البيانات غير هذه التقنية تتوقف على العرض من التجميع.¹²²

¹²¹ جيمس كورودا، كيث روس، شبكات الحوسبة، وإياتي، "أسس ومبادئ شبكات الإنترنت"، ترجمة د. سعيد محمد، الأخير، د. جمال سعيد، تحت إشراف د. أبيكاز، سنة 2011، ص 163. ... هذا الكتاب متاح عبر موقع شابر.

- <https://books.google.com.eg>.

¹²² سامح عامر، "تغير الإطار القانوني والعقوبات"، نشر د. مهدي، سنة 2013، ص 160.

¹²³ - Cécile CASTETS-RENARD, La protection des données personnelles dans les relations internes à l'Union européenne, Dalloz - Octobre 2018, N° 267.

ثانياً: التجميع غير المشروع للبيانات الشخصية عن طريق بيانات النشر

يُقصد ببيانات النشر المعلومات التي يعرفها الموقع عن المستخدم بمجرد قيام هذا الأخير بتصفح هذا الموقع. بمجرد دخول المستخدم إلى الموقع، يُكتشف عنوان يُعرف بالـ (IP/T (P)، يحصل المستخدم ونوع الحاسب الذي استخدمه الشخص والتصفح عبر الاستخدام. وبعض المعلومات عن هذا التصفح تكون حادثة وتاريخه وعنوان الموقع السابق الذي كان يتصفح الشخص قبل أن يتصفح الموقع الحالي¹²¹.

تمثل عترة عميات جمع البيانات الشخصية غير بيانات النشر في أن المدعوى إلى العديد من مواقع الويب يتصلب من المستخدم (إقصاد عن معلومات ذات طبيعة شخصية. الأمر الذي يعرض خصوصيته لمخاطر حقيقية، ولقد هذه المؤسسة من أكثر الأساليب شيوعاً من ناحية العملية في تتبع وجمع بيانات الأفراد. نظراً لأن معظم تعاملات مستخدمي الإنترنت تعتمد على التصفح المتكرر لمواقع مختلفة، حيث يمكن أن يقوم المستخدم خلال يوم واحد بزيارة عدد كبير من المواقع الإلكترونية، يُطلب منه خلالها إدخال بيانات شخصية متنوعة تمكنه من الحصول إلى محتواها أو الاستفادة من خدماتها.

وتبين طيلة هذه البيانات نوعاً لطيفة الموقع والمعرض من زيارته. فقد تتضمن معلومات تعريفية أساسية كاسم المستخدم وعنوانه وزيارته الإلكترونية، أو بيانات مالية تجارية في حال التعامل مع مواقع البيع والشراء الإلكترونية، وبذلك تصبح بيانات النشر وسيلة فعالة لجمع كم هائل من المعلومات الشخصية عن المستخدمين. مما يختر تساؤلات قانونية جوهرية تتعلق بمدى مشروعية هذا الجمع، وإمكانة استخدام هذه البيانات في نطاق محدد لا يمس خصوصية الأفراد أو يستعمل خارج الأغراض المصرح بها.

ثالثاً: التجميع غير المشروع للبيانات الشخصية عبر تقنية (RFID)

تُعرف تقنية الـ (RFID) باسم موجات الراديو. وتعتمد هذه التقنية على جهاز يُعرف بالـ (RFID Tag) (1). يتم وضعه بالمنتجات أو الحيوانات أو حتى الإنسان. ويحتوي هذا الجهاز على شريحة من

¹²¹ مبدع، وجد مبدع، 2012، ص 24. مصادر الشخص في الإنترنت، دار جامعة حدة، ص 224.

السينيكون، تخزني، تمتد، وخلفت في إرسال واستقبال البيانات والاستعلام عن موحات الراديو (RFID) 124.

وتتمثل خطورة جمع البيانات الشخصية عبر هذه التقنية، في أنها - أي تقنية (RFID) - تقنية ذات انتشار واسع وممتد لكثير من المجالات والأماكن، حيث يمكن استخدامها في بطاقات تحديد الهوية معروفة أعاكس تواجد أصحابها، وكذلك تحديد أماكن تواجد السيارات إذا كانت لوحة هذه السيارة تحمل شريحة سينيكون، وغض الأمر بالنسبة لجوالات السفر والداشيرات، وفي هذه الحالة الأخيرة تكون الشريحة مصدر كبير للإفصاح عن العديد من البيانات الشخصية أهمها صورة المسافر وحسينه واسمه وبعض المعلومات عن حاله الاجتماعية 125.

رابعاً: التجميع غير المشروع للبيانات الشخصية عبر مواقع التواصل الاجتماعي

يقصد بموقع التواصل الاجتماعي، تلك المواقع التقنية التي تُنشأ وتستخدم بقصد تدار المحتوى الإعلامي والتفاني الذي يميز بالطابع الشخصي بين طرفين أو أكثر، يعز عن أحدهم بالبريد الإلكتروني بالمتصفح، وذلك عبر شبكة اجتماعية كفيصل برك أو واتس آب مساء مع أعضاء لمربع حرية الإرسال وإعطاء المتصفح حرية التجارب مع التعليقات المرسلة 126.

تعد مواقع التواصل الاجتماعي في الوقت الراهن من أبرز الوسائل المتبعة في جمع البيانات الشخصية ومعالجتها، إذ تبرز الشبكات الرقمية، هناك نمطاً جديداً من الإعلام يُعرف بـ "الإعلام الشخصي"، الذي يمكن

124 - AVOINE, G., Sécurité de la RFID, Comprendre la technique sans être technicien, in la secrite de l'individu numérisé, réflexions prospectives et internationals sous la direction de LACOUR, S., L'Harmattan, 2008, p. 17 et s.

125 - أحمد جبر، تقنية RFID، ص 12.

- Règlement européen (UE, 2018 / 608 de la commission du la avril établissant les critères technique applicables aux etiquettes électronique pour les équipements marits, JOUE n°1 Loi, 20 avril 2018).

- Mike Puglia, Albert Puglia, V.Daniel Hunt, RFID, A Guide to Radio Frequency identification, John Wiley, Sans, 2007, p. 1 - 5.

126 المدون، بين أحمد، (2018)، مستعرض أدلة خاصة عن ممارسات غير مشروع غير مواقع التواصل الاجتماعي، دار الخدمة الحديثة، ص 25.

الأفراد من مشاركة تفاصيل حياتهم وآرائهم على نطاق واسع يخفق ما كان متاحاً عبر وسائل الإعلام التقليدية. وقد أصبحت هذه المواقع، مثل "فيسبوك"، و"إنستغرام" (تويتر سابقاً)، و"سكس" و"ساب" و"واتس"، جزءاً أساسياً من الحياة اليومية لمجتمع سعودي، مما يوفر من أدوات لتتبع والتواصل والتعمد. حتى بات استخدامها شبه حتمي في المجالات الاجتماعية والهيبة والتعبئة.

غير أن هذا الانتشار الواسع تزامن مع مخاطر قانونية تمس خصوصية الأفراد وأمن بياناتهم الشخصية. إذ ينصب التسبب في هذه المخاطر (الإفصاح عن كم كبير من المعلومات الشخصية، مثل الاسم الكامل، وتاريخ الميلاد، ورقم الهاتف، والعنوان، والجنس، والتربية، الإلكتروني، فضلاً عن الصور والأنشطة الاجتماعية والاهتمامات الشخصية، ونحن بحاجة المسح لاستخدام هذه التطبيقات، غالباً ما يُفصح المستخدمون عن هذه البيانات طوعاً دون إدراكهم) كتابياً بما قد يترتب على ذلك من انتهاك خصوصيتهم أو استغلال بياناتهم في أغراض تجارية أو تخريبية غير مصرح بها.

وفي هذا السياق، حرص النظام السعودي على وضع إطار قانوني متكامل لضمان حماية البيانات الشخصية من أي معاملة غير مشروعة، من خلال نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (د/19) وتاريخ 9 / 2 / 1443هـ. الذي يعد الأساس النظامي لتخصيص جمع البيانات واستخدامها في المسكفة، وقد نصّ النظام في مادته الخامسة على أنه «لا يجوز جمع بيانات الشخصية إلا لغرض محدد ومشروع، ولا يجوز معالجتها لاحقاً بما يتناقض مع ذلك الغرض». كما أكد على ضرورة الحصول على موافقة صريحة من صاحب البيانات قبل معالجتها أو الإفصاح عنها، وعلى التزام الجهة المعالجة باتخاذ التدابير التقنية والتنظيمية لحماية البيانات من التلويح غير المصرح به أو من التسريب أو التعديل.

كما تنص المادة السادسة للبيانات والذكاء الاصطناعي (مدايا) الإشراف على تنفيذ هذا النظام، وتعمل من خلال المركز الوطني للذكاء الاصطناعي والمركز الوطني للبيانات على وضع السياسات والمعايير الخاصة بحماية الخصوصية الرقمية وضمان الاستخدام المسؤول للبيانات. خصوصاً في بيئة المخاطر الرقمية ومواقع التواصل الاجتماعي.

وبناءً على ذلك، فإن جمع بيانات الشخصية عبر هذه المواقع دون التقيد بظوابط النظام يعد تجاوزاً للغرض المشروع من المعالجة، ويشير المسؤولية النظامية والالتزام على القائمين بعمليات الجمع أو المعالجة، ويعد هذا التسليم السعودي خطوة مهمة نحو تحقيق التوازن بين تمكين الأفراد من الاستفادة من التقنيات الحديثة وضمان

صوتن خصوصيتهم وحقوقهم الرقمية في ظل التوسع الكبير في استخدام تطبيقات الذكاء الاصطناعي وشبكات التواصل الاجتماعي في المملكة.

خامساً: التجميع غير المشروع للبيانات الشخصية عبر تقنية دمج المعلومات (Data Fusion)

تتطلب تقنية دمج المعلومات وجود مواقع غير مرتبطة ببعضها البعض. وفي الكثير من هذه المواقع قد يستخدم الأشخاص أسماء مستعارة تم بها تجنب وجود بعض بياناتهم الشخصية التي تم تجميعها. وذلك من خلال برنامج تقوم بتمسح قواعد البيانات المختلفة. والتي يكون لديها القدرة على معرفة المستخدم من المنتسبين أو المرتبطون بعضهم البعض¹²⁷. أي أنها عملية دمج مصادر بيانات متعددة لإنتاج معلومات أكثر اتساقاً ودقة عن المعلومات التي يوفرها أي مصدر بيانات بمفرده¹²⁸.

ويتم تجميع بيانات الشخصية عبر هذه التقنية باستخدام البرنامج سائفة الذكر على طريق قراءة معلومات عن شخص ما من قاعدة بيانات. وتخصص اسم له اسم مختلف من قاعدة معلومات أخرى. بمعنى أنه يوجد شخصان مختلفان إلا أن اثناء يحتمل على معلومة جديدة من قاعدة معلومات أخرى. لكنها تحتوي على معلومات أخرى تشترك مع الشخص الأول. كرقم رخصة القيادة ورقم الهاتف. ويفترض الطاء حينها أن هذه المعلومات مرتبطة بنفس الشخص¹²⁹.

المطلب الثاني: النشاط الجزائي الخاص بمعالجة البيانات الشخصية

قام المصمم المبرمج بوضع إطار تنظيمي خاص بمعالجة البيانات الشخصية. حيث إن الأصل في هذا الشأن هو حواز معالجة البيانات الشخصية وليس حفظها، شريطة الالتزام بالشروط التي حددها المصمم. وبعد الخروج عن هذه الشروط جريمة يعاقب عليها المصمم. حيث يتحول أي انتهاك هذه الأحكام إلى نشاط إجرامي.

¹²⁷ - مرسوم، قيد قيد مرقع سابق، ص 188.

¹²⁸ - <https://en.m.wikipedia.org/Wikipedia/Data-Fusion>.

¹²⁹ - مرسوم، قيد قيد مرقع سابق، ص 188، 189.

ونظراً لأن معالجة البيانات الشخصية تتضمن مرحلة تجميع البيانات ثم حفظها، فقد نص المخطط على شروط خاصة بكل من التجميع والحفظ إضافة إلى التزامات رضا الشخص المعني بمعالجة بياناته الشخصية، ومن هذا المنطلق، يتضح أن النشاط الجزائي في هذا المجال قد يندرج في ثلاث حالات رئيسية¹³¹:

- النشاط الجزائي بخصوص تجميع البيانات.
- النشاط الجزائي بخصوص مخالفة شروط حفظ البيانات.
- النشاط الجزائي بخصوص معالجة البيانات دون موافقة صاحبها.

الفرع الأول: النشاط الجزائي بخصوص جمع البيانات الشخصية

نورد المخطط السعودي شروطاً محددة لعملية جمع البيانات الشخصية لضمان أن تكون هذه البيانات مجمعة بطريقة نظامية وقانونية. وفي هذا السياق، يعد أي جمع غير مشروع لبيانات الشخصية جريمة يعاقب عليها النظام، ويشكل سبباً إجرامياً.

ففي تناول المخالفات، يحدد توضيح مفهوم الجمع نفسه، فقد عرف المخطط السعودي الجمع بأنه: "الحصول منهجياً لتحكم على البيانات الشخصية وفقاً لأحكام النظام، سواء ما تفرّد من صاحبها، أو من غيره¹³²، أو من جهة

وتكون عملية تجميع البيانات مشروعة، يجب توافر شروط رئيسية، أهمها:

الشرط الأول: أن يتم تجميع البيانات بطريقة نظامية

أول ما يتعين في تجميع بيانات أي فرد أن يكون الشخص على علم مسبق بأن بياناته الشخصية سيتم جمعها. ويجب أن يشمل هذا الإجراء طريقة جمع البيانات، والعرض من جمعها، ونوع البيانات الشخصية التي سيتم¹³³.

¹³¹ المحي، صالح عويش منصور، 2025، خدمة إلكترونية لتعديل بيانات الشخص في نظام السعودي، دراسة مقارنة، مجلة الأندلس لعلوم القانون والاختصاص، عدد 114، العدد 12، ص 159.

¹³² عدد 4، من المادة الأولى من نظام خدمة بيانات الشخص السعودي، رقم 19 تاريخ 9/2/1443 هـ.

¹³³ عرف، عدد 18، من المادة الأولى من عدد سعودي لخدمة بيانات الشخص، بأنه يجب التحكم في أية جهة عملاء، أو أي شخص ذات صلة يجب، أو غير ذلك، عدد العرض من معالجة بيانات الشخص والتعبئة، سواء أتمرت معالجة بيانات الشخص أم لم يمتدح جهة معاملة.

ويثبت على ذلك ما نصت عليه المادة الخامسة من النظام السعودي الخاص بالبيانات الشخصية. وإلى نص في فقرتها الأولى على أنه: "لا يجوز معالجة البيانات الشخصية أو تغيير العرض من معالجتها إلا بعد موافقة صاحبها. وفي الواقع شروط موافقة والأجور التي يجب فيها أن تكون الموافقة كتابية إضافة إلى الشروط والأحكام المتعلقة بالخصوص على موافقة ذوي الشريعة إن كان صاحب البيانات ناقص أو غيب الأهلية."¹³⁴ وبذلك، يصبح توافق رضا صاحب البيانات بطريقة جمعها وفق النظام شرطاً أساسياً لجعل عملية الجمع قانونية. وأي انتهاك لهذه الشروط يعد انتهاكاً إجرامياً يعاقب عليه النظام.

الشرط الثاني: أن يكون الجميع لغرض نظامي

لا بد أن يكون جميع البيانات الشخصية لغاية مشروع ونظامية. فالبيانات الشخصية نفسها ليست محظورة. وإنما يأتي الخطر لحماية صاحبها. وعندما يُسمح بجمع هذه البيانات، يجب أن يكون مرهوناً بتحقيق غرض مشروع.

فعلى سبيل المثال، إذا تم جمع البيانات الشخصية لصحية الفرد ما يخلف إجراء بحث علمي، فإن ذلك يعد غاية مشروع ونظامية. أما إذا تم جمع نفس البيانات لأغراض تجارية بحتة، فإن الغاية تكون غير مشروعة. وبالتالي يصبح الجميع غير نظامي.

وفي هذا الإطار، نصت المادة العاشرة من النظام السعودي الخاص بالبيانات الشخصية على أنه: "... ولا يجوز معالجة البيانات الشخصية إلا لتحقيق الغرض الذي سمح من أجله..."¹³⁵.

وتفصيلاً لحكمه الواردة في المادة السابقة، نصت المادة الحادية عشر من النظام على ما يلي¹³⁶:

- يجب أن يكون الغرض من جمع البيانات الشخصية مرتبطاً مباشرة بالغرض جهة التحكم وألا يتعارض مع أي حكم مقرر نظاماً.

¹³⁴ معيد، م.خ غرض مصر، 2025، مصدر سبق ذكره من 164.

¹³⁵ نصت المادة الخامسة من نظام السعودي الخاص بالبيانات الشخصية.

¹³⁶ نصت المادة الحادية عشر من نظام حماية البيانات الشخصية السعودي.

¹³⁷ المادة الحادية عشر من نظام حماية البيانات الشخصية السعودي.

- يجب ألا تتعارض طرق ومبادئ جمع البيانات الشخصية مع أي حكم مقرر نظاماً وأن تكون ملائمة لظروف صاحب البيانات، مباشرة، واضحة، آمنة، وعادلة من أنساب الخداع أو التضييق أو الاكراه، وبذلك، ينصح أن الطرق القانوني تعرض النظامية بعد، عنصر أساسياً يجعل جمع البيانات مشروعاً، وأي مخالفة هذه المتطلبات تعدر سلوكاً إجرامياً يعاقب عليه النظام¹⁶⁷.

الفروع الثاني: النشاط الجزائي بخصوص حفظ البيانات الشخصية

بعد، لجميع البيانات الشخصية تمييزاً لها حيثها، يشترط النظام السعودي توفر شروط أساسية لحفظ القانوني لبيانات:

الشرط الأول: أن يتم حفظ البيانات بدقة

تصل المادة الرابعة عشر من النظام السعودي الخاص بحماية البيانات الشخصية على أنه: لا يجوز أخذه التحكم أو تعالج البيانات الشخصية دون اتخاذ خطوات كافية لتحقيق من دقتها واكتمالها وحدتها وربطها بالعرض الذي جمعت من أصله وفقاً لأحكام النظام¹⁶⁸.

وقد جاء التأكيد على دقة البيانات لضمان عدم حفظها بشكل عشوائي، مما قد يعيق عملية معالجتها برمتها بخلافه ليرجع أو النظام، ومن هنا اشترط النظام أن يتم جمع البيانات مباشرة من صاحبها لضمان موثوقيتها ودقتها.

الشرط الثاني: تناسب مدة الحفظ مع غرض التجميع

إذاً أن لجميع البيانات يجب أن يكون له غرض مشروع ونظامي، فلا بد أن تكون مدة الحفظ مرتبطة بتحقيق هذا الغرض، وقد نصت غالبية القوانين والأنظمة أنظمة حماية البيانات الشخصية على أن مدة حفظ البيانات يجب ألا تتجاوز الفترة اللازمة لتحقيق الغرض من جمعها، وأنه عند انتهاء الغرض يجب إيقاف الحفظ وإزالة البيانات.

¹⁶⁷ المحي، مدخ غرض مصر، 2025، مصدر سبق ذكره ص 161.

¹⁶⁸ المادة الرابعة عشر من عدة حزم بيانات الشخصية السعودية.

وفي هذا الإطار، نص المظم السعودي في الفقرة الرابعة من المادة الحادية عشر على أنه: "إذا تضح أن البيانات الشخصية التي جمعت، لم تعد ضرورية لتحقيق الغرض من جمعها، فعلى جهة التحكم بالتوقف عن جمعها وإتلاف ما سبق جمعه فوراً"¹³⁹.

وعليه، يستحسن أن يتم تحديد مدة زمنية معيارية للحفاظ على شهر واحد لضمان عدم سوء استخدام البيانات وحماية الحياة الخاصة للأفراد.

الفرع الثالث: النشاط الجزائي بخصوص عدم رعا الشخص

إن معالجة البيانات الشخصية دون موافقة صاحبها هي نشاط إجرامي وبالتالي فإن انتهاك أحكام نظام حماية البيانات الشخصية يعد جريمة جنائية، وفي هذا الصدد نص المادة 5 على أنه¹⁴⁰:

1- فيما عدا الحالات المخصوص عليها في النظام، لا يجوز معالجة البيانات الشخصية أو تخزين الغرض من معالجتها إلا بموافقة صاحبها، وتحدد اللائحة شروط الموافقة والحالات التي يجب أن تكون فيها الموافقة كتابية والتدابير والأحكام المتبعة بالحصول على موافقة الوالي الشرعي إذا كان صاحب بيانات قاصراً أو عدم الأهلية.

2- في جميع الأحوال، يجوز لصاحب بيانات الشخصية سحب الموافقة المشار إليها في الفقرة (1) من هذه المادة في أي وقت، وتحدد اللائحة الضوابط اللازمة لذلك، وبينما هو المنصوص عليه في المصريح والسعودي على وجوب الحصول على موافقة الشخص الذي تتم معالجة بياناته، فإن المادة 7 من القانون نصت على حالات معينة يجوز فيها معالج بيانات الغير دون موافقة الشخص الذي تتم معالجة بياناته، حددت الحالات هي¹⁴¹:

أولاً: إذا كان هناك التزام قانوني أو تنصيص على الشخص الذي يقوم بالمعالجة؛ أي إذا كان هناك التزام قانوني يقوم الشخص الذي يقوم بالمعالجة بالقيام بذلك، فلا يحتاج إلى الحصول على موافقة الشخص الذي يقوم

¹³⁹ الفقرة الرابعة من المادة الحادية عشر من م.د. حرمة بيانات الشخص السعودي.

¹⁴⁰ المادة خمسة من نظام حماية بيانات الشخص السعودي.

¹⁴¹ الميعود، مدخل غرض مصر، 2025، مصدر سبق ذكره ص 162.

بمعالجة بياناته. يجب أن يكون هذا الالتزام قائماً على أساس قانوني، إن معالجة بيانات وفاء بالالتزام قانوني معروض على معالج البيانات يعقده من الحصول على موافقة الشخص الذي تتم معالجة بياناته.

ثانياً: حماية حياة الشخص الذي تتم معالجة بياناته، إذا كانت حماية حياة هذا الشخص تتطلب معالجة بياناته. فلا يحتاج الشخص الذي يقوم بمعالجة إلى الحصول على موافقة، كما لم تعرض شخص لحادث ويتم معالجة بياناته الصحية تعرض لإجراء عملية جراحية عاجلة.

ثالثاً: تلبية مهمة عامة يضيغها معالج، إذا كان الشخص الذي يقوم بمعالجة البيانات الشخصية بشخص متناً عاماً يتطلب منه معالجة البيانات الشخصية، فلا يحتاج إلى الحصول على موافقة الشخص الذي يقوم بمعالجة بياناته، طالما كان ذلك في حدود مصاصات وظيفته.

رابعاً: تنفيذ عقد يكون الشخص الذي تتم معالجة بياناته طرفاً فيه، يعني هذا الاستثناء أن الشخص الذي يُعالج بيانات الشخصية هو الطرف المتعاقد الآخر مع الشخص الذي تُعالج بياناته. وينحصر إلى معالجتها لتنفيذ العقد، مثال على ذلك قيام شركة بمعالجة بيانات عميل تعاقدت معه لتفاديه خدمة أو توصيل منتج إلى منزله. وغير ما تعاقدت عليه...

خامساً: إذا كان الشخص الذي يُعالج بيانات الشخصية يسعى لتحقيق مصلحة مشروعة، إذا كان الشخص الذي يُعالج بيانات الشخصية يسعى لتحقيق مصلحة مشروعة، فله الحق في معالجة بيانات الشخصية دون الحصول على موافقة الشخص الذي يُعالج بياناته. ضرورة أن يكون ذلك معصاه أو حقوقه وحرياته الأساسية، في الواقع، رُجِّحت التقادرات إلى هذا الاستثناء الأخير، إذ رأى القضاء أن هذا الاستثناء يعيقه الحفاظ، قد فتح الباب واسعاً أمام طرف الموافقة الذي تشترطه الهيئة التنظيمية كشرط أساسي لإجراء عملية معالجة البيانات الشخصية¹⁴².

¹⁴² المادة عاشر من نظام سعودي يخص خدمة بيانات الشخصية، رقم 19 تاريخ 1443/2/9 وندوة مساهمة من المعهد، التي تسمى بحماية بيانات الشخص.

المبحث الثاني: مستقبل التشريعات والسياسات التنظيمية للذكاء الاصطناعي

مع المصارع الكبير في تطوير تقنيات الذكاء الاصطناعي واعتمادها المتزايد في مختلف القطاعات الاقتصادية والاجتماعية، أصبح هناك إدراك عالمي لأهمية وضع أطر تشريعية وتنظيمية متقدمة لضمان الاستخدام الامن ومسؤول هذه التقنيات، ومن المتوقع أن يشهد المستقبل تطوير سياسات تنظيمية شاملة تجمع بين حماية الحقوق الفردية، خصوصاً البيانات الشخصية وحقوق الخصوصية، وبين تعزيز الابتكار والاستفادة الاقتصادية من الذكاء الاصطناعي. وستركز هذه السياسات على تنظيم الشفافية، والمسؤولية القانونية، ومساواة التطوير والاستخدام، وأخلاقيات استخدام الذكاء الاصطناعي. بما يوازن بين الابتكار التقني وإخداية القانونية لمجتمع، كما يشهد العالم بين نماذج تشريعية متكاملة على غرار ما يداره دول الاتحاد الأوروبي واليابان. مع إمكانية تكيف التشريعات الوطنية، مثل المملكة العربية السعودية، لتواكب هذه المعايير العالمية. بما يعزز بيئة آمنة للتطبيقات الذكاء الاصطناعي ويحمي الحقوق الفردية ويحفز الابتكار في الوقت ذاته.

إن العقل البشري هو ماضٍ التكنيف وأعظم العلم الذي أنعم الله بنا على البشرية، وقد شهد الإنسان منذ عهده على الأرض تطورات معرفية وعلمية ساهمت في الانتقال بأخلاق البشرية من مرحلة البدائية إلى عصر التكنولوجيا والمعرفة والابتكار، لهذا كان الإنسان صاحب العقل ومركز التفكير، وهو المنظم على التقنيات الحديثة، غير أن الواقع الحالي يشهد تغيراً ديناميكياً في طبيعة علاقة الإنسان بالآلة، فالיום، أصبحت الآلة تمتلك قدرة معرفية وإبداعية يمكنها من محاكاة تفكير الإنسان ومشتاغرة وسذكياته، فضلاً عن قدرتها على حل المسائل والأغوار واتخاذ القرارات وحل المشكلات المعقدة، وتشخيص الأمراض وإجراء العمليات الجراحية، فضلاً عن التنبؤ بالإحتكاليات المستقبلية وفيها المحورات والتواصل مع الآخرين بطريقة تفهم اللغاس البشري، وهكذا، تعد العلاقة بين الإنسان والتضيق مجرد علاقة أدوات تقنية، بل أصبحت تضاعفاً ديناميكياً يعني الآلة حريتك معرفياً قادراً على محاكاة القدرات البشرية بطرق كانت في عقود قليلة مجرد خيال عسى¹⁴³.

المطلب الأول: التنظيم القانوني لتقنيات الذكاء الاصطناعي في المملكة العربية السعودية

يقع التنظيم القانوني لتقنيات الذكاء الاصطناعي في المملكة العربية السعودية ضمن إطار مبادئ وأخلاقيات محددة، حيث نص قرار مجلس الوزراء رقم (292)، بتاريخ 1441/4/27هـ في فقرة ثمانية على أن التهيئة

¹⁴³ مدحمة، جواد محمد، (2023)، الذكاء الاصطناعي وأحدث أدوات الذكاء الاصطناعي، دار الفلاح للنشر والتوزيع، جدة، (الطبعة الأولى، 1444هـ، ص 10).

تسهردية لبيانات والذكاء الاصطناعي منظمة تنظيم قطاعات البيانات والذكاء الاصطناعي من خلال وضع سياسات ومعايير وضوابط تقنية تتواءم مع هذه التقنيات، وتحميها على الجهات ذات العلاقة سواء كانت حكومية أو غير حكومية، مع متابعة الأنظمة بها وفق الأسس النظامية ذات الصلة.

والتدقيق من التزام المنظمة بحقوق الإنسان وقيمها الثقافية، وامتثالاً مع المعايير والتوصيات الدولية لأخلاقيات الذكاء الاصطناعي. فقد اعتمدت الهيئة على المعايير ذات والمعايير العالية عند صياغة مبادئ أخلاقيات استخدام تقنيات الذكاء الاصطناعي، وقدرات هذه المبادئ إلى دعم جهود المنظمة ومساعدة الجهات المختلفة في تبني المعايير الأخلاقية عند بدء وتصميم الحلول القائمة على الذكاء الاصطناعي. بما يضمن الاستخدام الآمن وحماية خصوصية الأفراد وحقوقهم في ما يتعلق معالجة بياناتهم الشخصية.

وتتمثل أهم المبادئ الأساسية لأخلاقيات استخدام الذكاء الاصطناعي فيما يلي:

– **الزاهة والإنصاف:** يجب على منظري أنظمة الذكاء الاصطناعي، عند تصميم أو جمع أو تطوير أو نشر أو استخدام هذه الأنظمة، اتخاذ الإجراءات اللازمة لضمان عدم وجود تحيز أو تمييز أو تجاوزات، والسعي لتحدد منها قدر الإمكان¹⁴⁴.

– **المساءلة والمسؤولية:** يتحمل المصممون والمطورون والمسؤولون والأنظمة الذكاء الاصطناعي المسؤولية الأخلاقية عن القرارات والإجراءات الصادرة عن هذه الأنظمة، والتي قد تؤدي إلى مخاطر وأضرار منية على الأفراد والمجتمعات، ويستند ذلك تحقيق الشفافية البشرية والحوكمة والإدارة مناسبة خلال دورة حياة النظام بأكملها. لضمان وجود آليات فعالة لتجلب الأضرار وسوء الاستخدام مع الحفاظ على عدالة وسلامة واستدامة هذه الأنظمة. كما يجب على جميع الأطراف المعنية بتنظيم استخدام تقنيات الذكاء الاصطناعي مراعاة هذه المبادئ عند اتخاذ أي قرارات تتعلق بها¹⁴⁵.

¹⁴⁴ د. إبراهيم داود، خدمة عمالية لبيانات، منشور من مطبعي الخرج في مصر، للخدمة كخدمة لبحوث العالمية والاقتصاد، جامعة الإسكندرية، ص 2015.

¹⁴⁵ (ساج، مروة) من عائد، 2017، الخدمة عمالية لبيانات منشور من مطبعي الخرج في مصر، للخدمة كخدمة لبحوث العالمية والاقتصاد، جامعة الإسكندرية، ص 1-2017.

بعد هذا الاستعراض، يرى الباحثون أن الآلية التي تحكم وتنظم استخدام تقنيات الذكاء الاصطناعي في المملكة العربية السعودية قائمة بشكل أساسي على مبادئ والقرارات الصادرة عن الجهات المختصة، دون وجود نظام قانوني مستقل يظم بدقة المعايير القانونية لمسؤولية الجانية والذنية المتحققة باستخدام هذه التقنيات.

ففيما يتعلق بالتحقق من بيانات ومداخلات الأنظمة الذكاء الاصطناعي، يفرض منظم المسؤولية على المفوضين والمراجعين ومقيمي الأنظمة، اعتماداً على المدونات الأخلاقية والرجوع إلى الأنظمة ذات الصلة. بمعنى آخر، لا توجد حتى الآن جهة قانونية مستقلة تحدد المعايير التي تُبنى عليها المسؤولية، ولا إطار تنظيمي مستقل يسهل عمليات الإثبات بما يتوافق مع طبيعة الأعمال الصادرة عن تقنيات الذكاء الاصطناعي.

وفيما يخص الاستخدام القانوني والأخلاقي للبيانات المتولدة من الذكاء الاصطناعي، يعتبر مكتب إدارة البيانات الجهة الرقابية المسؤولة عن ضمان توافق البيانات المستخدمة مع مبادئ والسياسات والأنظمة المعمول بها في المملكة.

وعند النظر إلى الأنظمة المرتبطة بالأعمال الصادرة عن تقنيات الذكاء الاصطناعي، مثل أنظمة الأمن السيبراني، ونظام حماية البيانات الشخصية، ونظام الملكية الفكرية، ونظام مكافحة الجرائم المعلوماتية، يصبح أن هذه الأنظمة مرتبطة بإطار تنظيمي معين، لكنها لا تتوافق بالكامل مع التغيرات المستقبلية المتصاعدة التي قد تنتج عن استخدام الذكاء الاصطناعي، خصوصاً في ظل التطور السريع والمستمر للمملكة.

بناءً عليه، يبرز الحاجة إلى وضع إطار تنظيمي وتعيين جهات لاستخدام تقنيات الذكاء الاصطناعي، يصبح أبرز جملة القوانين الواضحة هذه التقنيات، كما يتضح:

- دواء الإشكالات القانونية القائمة عن الأعمال الصادرة من الذكاء الاصطناعي.
- تحديد المسؤولية المدنية والتعويضية والعقوبات الجنائية للأفعال المرتكبة من خلال هذه التقنيات.
- تمهيد عمل القضاء السعودي في تطبيق النص القانوني بما يتواءم مع الواقع التكنولوجي.
- ضمان حقوق الأفراد وتوضيح واجباتهم ومسؤولياتهم عند استخدام تقنيات الذكاء الاصطناعي.
- تحقيق التوازن بين مبادئ العدالة والمرونة المتصورة، غلبتها في القرارات والمبادئ الصادرة عن الهيئة السعودية لبيانات والذكاء الاصطناعي.

-

المطلب الثاني: المسؤولية المدنية على تفتيات الذكاء الاصطناعي

ذكرت المادة (121) من نظام معاملات المدنية في المملكة العربية السعودية مبدأ خطأ وانظر وانعلاق بينهما، حيث نصت على أن: «كل خطأ سبب ضرراً لمخبر يترتب ممتلكته بالتعويض»¹⁴⁶. كما نصت المادة (122) من ذات النظام على ما يلي:¹⁴⁷

- 1- يكون الشخص مسؤولاً عن الفعل الضار من حين منته وهو مخير.
- 2- إذا وقع الضرر من غير التمييز ولم يكن هناك من هو مسؤول عن الضرر أو تعدد الأشخاص على تعويض من المسؤول، لزم غير التمييز تعويضاً مائلاً تقادير المحكمة.

ينضح من هذه النصوص أن النظام المدني يزم الشخص غير التمييز بالتعويض في حال ارتكب فعلاً تسبب في ضرر، في حالة عدم إمكانية الرجوع على المسؤولين المباشر عن الفعل الضار (المشروع)¹⁴⁸.

الفرع الأول: المسؤولية العقدية في مجال الذكاء الاصطناعي

المسؤولية العقدية تعرف بأنها المسؤولية المترتبة على مخالفة الالتزامات التعاقدية، من امتناع البائع عن تسليم البضاعة المستخرجة، أو ما يترتب عليها من تعويض عن الأضرار المالية الناتجة عن العقد، ويستند في معيار المسؤولية العقدية إلى الأضرار المترتبة عن ما يقع منه الشخص التعاقد في ظروف مشابهة لتلك التي كان عليها متدين عند تنفيذ التزامه، وهو ما يحكم مدى التقصير أو الخطأ في أداء الالتزام¹⁴⁹.

وتجدر الإشارة إلى أن مجرد عدم الوفاء بالالتزام أو تأخره لا يحقق بالضرورة مسؤولية المتدين، إذ يجب أن يكون هذا الإخلال بالالتزام راجعاً إلى خطأ من المتدين، وقد نصت المادة (173) من نظام معاملات المدنية السعودي على ما يلي:¹⁵⁰

¹⁴⁶ المادة (121) من نظام معاملات المدنية في المملكة العربية السعودية.

¹⁴⁷ المادة (122) من نظام معاملات المدنية في المملكة العربية السعودية.

¹⁴⁸ على معاملات مدنية صادر بوحدة التمسك بسكي رقم 191، وتاريخ 29/11/1444هـ.

¹⁴⁹ انظر: د. علي بن أحمد، ومحمد، ومحمد بن محمد، (2024)، التمسك بالالتزامات العقدية (التمسك بالالتزامات العقدية)، المملكة العربية السعودية، وإدارة التمسك بالالتزامات العقدية، رقم 385.

¹⁵⁰ المادة (173) من نظام معاملات المدنية السعودي.

1- يجوز الاتفاق على إعفاء المدين من التعويض عن الضرر الناتج عن عدم تنفيذ التزامه التعاقدى أو تأخره فيه، إلا إذا كان الإخلال نتيجة خطأ أو خطأ جسيم من المدين.

2- لا يجوز الاتفاق على الإعفاء من المسؤولية المترتبة على الفعل الصادر.

وتوضح هذه المادة أن القانون السعودي يحمي الطرف المتضرر من العقد من الإعفاء من التعويض في حالات غش أو الخطأ الجسيم، مما يعكس أهمية عنصر الخطأ في إثبات المسؤولية العقدية، ويضمن تحقيق العدالة بين أطراف العقد.

الركن الأول: الخطأ العقدى (المعدي)

يقصد بالخطأ العقدى سلوك المتعاقد بطريقة تتنافى مع التزامه التعاقدى، ويعتبر مدين خطأً إذا امتنع عن تنفيذ ما التزم به أو تأخر في تنفيذه. وقد تناول الفقه المدين بقرينات الخطأ التعاقدى من حيث تدرج درجاته بدءاً من خطأ اليسر الذى لا يرتكبه المدين المتعاقد، وخطأ الشك المسبب إلى الشخص التهميم غير الخريص، وصولاً إلى الخطأ الجسيم الذى يقارب خطأ العمد.

وقد أسندت هذه النظرية من القانون الرومانى، وطورها فقهاء القانون الفرنسى لتصبح ما يعرف بنظرية الأخطاء الثلاثة، حيث يتم تقسيم الخطأ حسب جسامته إلى: الخطأ الجسيم، الخطأ اليسر، وخطأ باع اليسر¹⁵¹.

وقد اعتمد نظام المعاملات المدنية السعودى على نفس النظرية، مستخدماً ما معيار الشخص المتعاقد أى أن معيار تقييم الخطأ يكون وفق عناية الشخص المتعاقد بغض النظر عن تخصيصه أطراف العقد. وانتشرت عدة مواد في النظام إلى هذا المعيار لتوضيح متى تقع مسؤولية غنى المدين، ومن أمثلة ذلك:

المادة (168) من النظام، التى تنص على أنه إذا كان المتعثر من المدين محافظاً على الشيء أو إدارته أو توصى بحفظه في تنفيذ التزامه، فإنه يكون قد وفى بالتزامه إذا بذل عناية الشخص المتعاقد، ولو أنه يتحقق العرض المقصود، ما لم يمس نص نظامى على خلاف ذلك، أما إذا كان المتعثر تحقيق عناية محدودة، فلا يعد الوفاء قد تحقق إلا بتحقيق تلك العناية¹⁵².

¹⁵¹ الشومس، *مبادئ فقه المعاملات المدنية*، ج 1، ص 386، 2024، مصدر سبق ذكره ص 386.

¹⁵² المادة (168) من هذه المعاملات المدنية السعودى.

الركن الثاني: الضرر

في النظام السعودي، لا يكفي وقوع الخطأ من جانب لإقامة المسؤولية العقدية، بل يجب أن يترتب على هذا، خطأ ضرر يلحق بالمدعى، على سبيل المثال، إذا تعهد البائع بتسليم سيارة للمشتري في موعد محدد، وتأخر عن التسليم، فإن هذا يعد خطأً عقدياً، لكن مسؤولية البائع لا تتحقق إلا إذا تسبب هذا التأخير في ضرر فعلي للمشتري.

ويعرف الضرر في الفقه السعودي بأنه الأذى الذي يلحق الشخص نتيجة المساس الحق أو مصلحة مشروعة له، سواء تحقق ذلك بأشكال أو الخسار أو العرض أو الشرف أو الاعتبار.

وبعد الضرر شرطاً أساسياً لقيام المسؤولية العقدية، إلا أن مجرد إحلال الدين بالتزام لا يفرض التعويض ما لم يترتب عليه ضرر متعذر يلحق بالمدعى، فإذا لم يحصل أي ضرر، فلا يكون للمتضرر حق تعويض بالتعويض.

وقد عكس نظام التعويضات المدنية السعودي في المادة (121) على ذلك، حيث جاء فيها: "في خطأ سبب ضرر لغيره يترتب عليه التعويض"¹³³.

كما يثير الخطأ في المادة (122) إلى أن الشخص مسؤول عن الفعل الضار متى علمه به وهو مخير، وإذا وقع الضرر من غير التمييز ولم يكن هناك من هو مسؤول عنه، فهو غير التمييز تعويض مناسب تقدره المحكمة¹³⁴.

وبناء عليه، يتحقق التعويض في المسؤولية العقدية في نظام السعودي عند تحقق ثلاثة عناصر رئيسية:

- وقوع خطأ عقدي من المدين.
- حدوث ضرر فعلي يلحق بالمدعى نتيجة الخطأ.
- وجود علاقة سببية بين الخطأ والضرر.

وبهذا يتضح أن الضرر هو الركيزة الأساسية للتعويض في المسؤولية العقدية وفق القانون السعودي، فلا يكون التعويض إلا إذا تحقق الضرر الفعلي نتيجة إحلال الدين بالتزامه.

¹³³ مادة (168) من نصوص مدعولات أدب السعودي.

¹³⁴ المحلل، د. محمد بن حسن، المسؤولية المدنية على الفروع، دراسة مقارنة بين نظام السعودي، ونظمه الإسلامية، رسالة دكتوراه، كلية الشريعة، جامعة دار العلوم، دمشق، 1405هـ، ص 78 - 80.

الركن الثالث في المسؤولية العقدية هو العلاقة السببية

وهو الركن الذي يربط بين الخطأ والضرر، إذ لا يكفي بوجود خطأ أو وقوع الضرر، بل يجب أن يشك أن الضرر حدث نتيجة مباشرة لإخلال المدين بالتزامه العقدي. وفي سياق تقنيات المزاكاه الاصطناعي في المملكة العربية السعودية، تصبح هذه العلاقة أكثر تعقيداً نظراً لأن الأنظمة الذكية تحمي وفق خوارزميات رياضية معقدة، ولا تصرف بوعي ذاتي. لذا، فإن إثبات العلاقة السببية يعني توضيح أن الضرر الذي وقع لم يتعقد ناتج عن خطأ بشري في تصميم النظام، تطويره، تشغيله، أو صيانته، وليس مجرد نتيجة طبيعية لحمل النظام نفسه¹¹³⁵.

تواجه إثبات العلاقة السببية في المزاكاه الاصطناعي عدة تحديات، فالنظم الذكية غالباً ما تكون معقدة وتحتوي على سلسلة من القرارات أو التفاعلات بين مكونات متعددة، مما يجعل من الصعب تحديد مصدر الخطأ بدقة. كما أن الاعتماد على بيانات غير دقيقة أو خاطئة قد يثير تساؤلاً حول مسؤولية المصور أو المشغل، ولا تسبب ذلك في ضرر، إضافة إلى ذلك، فإن التحديدات المستمرة لنظام قد تعجز سر كيانته وبالتالي، ما يزيد صعوبة تتبع الضرر إلى الخطأ الأساسي.

في حال هذه التعقيدات، يعتمد القضاء السعودي على مجموعة من الأدوات لإثبات العلاقة السببية. يتم اللجوء إلى خبراء في تقنيات المزاكاه الاصطناعي لتحليل البرمجيات وتحديد ما إذا كان الضرر نتيجة إخلال بالعقد أو عدم في التصميم أو التشغيل، كما ينبغي المحقق التوقيع بين المصور أو المزود والمستخدم دوراً أساسياً. إذ يحدد الالتزامات المتوقعة للبيانات، وأداء النظام، وصيانته، والتحديثات التوجيهية. كذلك تُستخدم سجلات تشغيل النظام وسجلات القرارات التي اتخذها لتحديد مصدر الضرر، والتقرير يُطبق معيار الرجوع العاد كما نصت عليه المادة (168) من نظام المعاملات المدنية السعودي، لتقييم ما إذا كان مظهر النظام قد اتخذ الإجراءات الوقائية والحماية اللازمة التي يُزعم من الشخص العادي القيام بها في ظروف مشابهة.

إثبات العلاقة السببية أمر بالغ الأهمية، إذ بدونها لا يمكن تحميل المطور أو المشغل مسؤولية التعويض، حتى لو تبين وجود خطأ أو ضرر، على سبيل مثال، إذا كان الضرر ناتجاً عن عدم في خوارزميات النظام نتيجة إهمال المطور، فإن العلاقة السببية قائمة والتي للمتطور المتأثر بالتعويض. أما إذا كان الضرر نتيجة سوء استخدام

¹¹³⁵ انظر: د. أحمد، ومحمد، سجاد، م. محمد، (2024)، مصدر سبق ذكره ص 387.

من الاستعداد أو ظروف خارجية لا علاقة لمسؤوله بها، فالعلاقة السببية تُعبر منقطة ولا يتحمل المنظر المسؤولية¹⁵⁶.

تكمّل أهمية أن تكون السببية في تحقيق العدالة القانونية، حيث يتم تحميل المسؤولية على الطرف الذي كان مسؤولاً فعلياً للضرر. وليس على القضاء الذي نفسه، كما يشجع هذا الركن المنظرين على تجنب أفضل ممارسات التصميم، وضمان جودة البيانات، وإجراء الاختبارات الدورية لنظام، بما في ذلك من المخاطر المستقبلية، وأخيرًا، يوضح هذا الركن إطاراً قضائياً واضحاً لتطبيق مبادئ نظام المعاملات المدنية السعودي، كما في ذلك المواد (120) م(168) و(173)، في سياق التعامل مع قضايا الذكاء الاصطناعي الحديثة. كما يتضمن حماية حقوق المتفاعلين وتحقيق العدالة في القضايا المتعلقة بهذه التقنيات.

الفرع الثاني: المسؤولية التقصيرية في مجال الذكاء الاصطناعي

تتمثل المسؤولية التقصيرية في الجزء المترتب على الإخلال بالتزامات قانونية المفروض على كل شخص بعدم الإضرار بالغير. حيث تُعد مسؤولية عن العمل الشخصي هي القاعدة العامة في المسؤولية التقصيرية، وتنطبق هذه القاعدة من مبدأ القائل بأن كل خطأ يسبب ضرراً يُعبر عنه فاعله بالتعويض. وعلى عكس مسؤولية العقدية التي تقوم على أساس إحلال المدين بالتزام تعاقدي محدد يختلف باختلاف شروط العقد، فإن مسؤولية التقصيرية تقوم على المبدأ القانوني ثابت وهو الالتزام بعدم الإضرار بالغير، وفي هذا السياق، يكون طرفاً المسؤولية العقدية مرتبطين بعقد محدد قبل تحقق المسؤولية، بينما في المسؤولية التقصيرية يفترض عدم وجود علاقة عقدية بين الطرفين. ويستند تحقيقها إلى فعل شخصي يرتكب ضرراً للغير. وينص هذا الفعل بأخصاً مع وجود رابطة سببية بين الضرر والخطأ حتى تترتب مسؤولية التعويض على منسب¹⁵⁷.

وقد أكد نظام المعاملات المدنية السعودي هذا المبدأ في المادة (120) التي تنص على أن كل خطأ سبب ضرراً للغير يترتب منه من ارتكبه التعويض¹⁵⁸، كما نصت المادة (123) على أن الشخص مسؤول عن الفعل الضار متى صدر منه وهو مميز، وإذا وقع الضرر من غير المميز ولم يكن هناك من هو مسؤول أو تعتبر الحصول على التعويض، لزم غير المميز تعويضاً مما إذا تقدره المحكمة، ويعني ذلك أن الركن الأساسي لمسؤولية التقصيرية

¹⁵⁶ انظر: د. عبد الحميد، وسمير، سبيد، في العقد، (2014)، مصدر سبق ذكره ص 387.

¹⁵⁷ انظر: د. حمدي، فاطمة عبد الله، (1441هـ)، المسؤولية المدنية مبرمج في نظام السعودي، كتيبة الشريعة، ص 44، د. الإسلام، جامعة عتب، ص 44.

هو تحقق الضرر كأساس لتعويض، بعض النظر عن الإدراك الكامل لنتائج. أي يجعل بعض أبعادها قريبة من النظرية الموضوعية.

ومع ظهور تقنيات الذكاء الاصطناعي، تسمح تطبيقات المسؤولية التقديرية أكثر تعقيداً. فإلا الذكاء التي تصنف بشكل مستقل لا يمكن أن تُنسب إليها شخصية قانونية. وبالتالي لا يمكن مساءلتها قانونياً كما هو الحال مع الأشخاص غير المتميزين. وفي الوقت نفسه، قد يكون من الصعب إنكار تحميل المالك أو المشتغل أو المستخدم المسؤولية إذا ما يكن هناك تقصير مباشر أو فعل مادي يؤدي إلى الضرر. خاصة إذا كانت الآلة ذاتية الحركة واتخاذ القرار مثل مركبات دتية القيادة. فالحظ والإعمال البشري يتوزعان على قدرات عقلانية مشتركة بين البشر. في حين أن خوارزميات الذكاء الاصطناعي لا تعمل وفق نفس الأسس العقلانية البشرية. وقد تنجح عنها نتائج غير متوقعة¹³⁸.

إضافة إلى ذلك، قد تختلف نتائج خوارزميتين مصممتين نفس القيمة بحسب اختلاف تصميميهما، بحيث يمكن أن تسبب خوارزمية واحدة في ضرر دون الأخرى. مما يستلزم عتبة عالية لتقييم وجود عيب في تصميمها. ويزيد الأمر صعوبة أن بعض البروتوكولات قد تستخدم برامج ما تضمنت من شركة المصنعة. وهو أمر متوقع في ظل التطور السريع لتقنيات الذكاء الاصطناعي. هذا التحديد يجعل من الصعب تطبيق قواعد الضرر والحفظ والعلاقة السببية التقديرية. وكذلك قواعد مسؤولية منتج. لتعويض الأضرار الناجمة عن استخدام هذه التقنيات. ويترك فجوة قانونية فيما يخص حماية المستهلكين أو مساعدة مصممي الأجهزة الذكية¹³⁹.

على سبيل المثال، في حالة وقوع حادث بسبب مركبة ذاتية القيادة أدت إلى أضرار مادية وجسدية للمتضرر. يطرح هذا سؤال المسؤولية: هل ينسب الحادث إلى مركبة نفسها كآلة ذكية. أم إلى مشغلها سواء كان مالكاً أو مستخدماً؟ فالإجابة المستفادة لاتخاذ القرارات تجعل من الصعب تحميل شخص بعينه المسؤولية المباشرة. ما يستدعي تطوير إطار قانوني خاص لتحديد مسؤولية التقديرية الناتجة عن استخدام تقنيات الذكاء الاصطناعي بما يتوافق مع نظام المعاملات المدنية السعودي ويحمي حقوق المتضررين.

¹³⁸ انظر: د. عبد الله بن محمد، ومحمد، محمد، بن محمد، (2024)، مصدر سبق ذكره ص 389.

¹³⁹ انظر: د. خالد بن محمد، ومحمد، محمد، بن محمد، (2024)، مصدر سبق ذكره ص 389.

الحاققة والنتائج والتوصيات .

بعد الانتهاء من رسالتنا التوضيحية للجهات ذات العلاقة عن استخدام الذكاء الاصطناعي في معالجة البيانات الشخصية في البيئة الرقمية، توصلنا للعديد من النتائج والذات نقتح بعض التوصيات كمثل في التالي :

أولاً: النتائج.

- 1- إن تنظيم ثقبات الذكاء الاصطناعي في شبكة يتفردح طقس إطار تنظيمي رفيع، هو محنت الحية السعودية لبيانات والذكاء الاصطناعي سعة تنظيم قطاعات البيانات والذكاء الاصطناعي من خلال وضع سياسات ومعايير وخطوط تكتيكية تتعامل مع هذه الثقبات، وتعميمها على الجهات الحكومية وغير الحكومية، ومناخه الاثرية بما وفق الأحكام النظامية ذات الصلة.
- 2- نورد النظم السعودي شروطاً محددة لعملية جمع البيانات الشخصية لضمان أن تكون هذه البيانات مجمعة بطريقة نظامية وقانونية. وفي هذا السياق، يعد أي جمع غير مشروع للبيانات الشخصية جريمة يعاقب عليها النظام، ويشكل سوءاً إجرامياً.
- 3- فقد بدأت عدة دول من الشبكة العربية السعودية والإمارات ومصر في تبني تشريعات وعية لحماية بيانات الشخصية، إلا أن الإطار القانوني لاستخدام الذكاء الاصطناعي ما يزال في طور التطور والشعور.
- 4- قام النظم السعودي بوضع إطار تنظيمي خاص بمعالجة بيانات الشخصية، حيث إن الأصل في هذا الشأن هو حوار معاملة البيانات الشخصية، وليس حظرها، شريطة الالتزام بالشروط التي حددها النظام، وبعد الخروج عن هذه الشروط جريمة يعاقب عليها النظام، بحيث يتحول أي انتهاك هذا الأحكام إلى مضاد إجرامي.
- 5- في إطار تعزيز حماية البيانات الشخصية في الشبكة العربية السعودية، صدر نظام حماية بيانات الشخصية بموجب المرسوم الملكي رقم (د/19) بتاريخ 1443/2/9هـ، الذي يعد الأساس النظامي لتنظيم جمع البيانات واستخدامها في الشبكة.
- 6- تحدّد القوانين النظمية لحماية البيانات الشخصية بالخطوط والضمانات التي يجب الالتزام بها عند معالجة هذه البيانات

- 7- دور الهيئة السعودية لبيانات والذكاء الاصطناعي (سدايا): تتولى هيئة الإشراف على تنفيذ النظام، وتعمل من خلال مركز الرقابة للذكاء الاصطناعي ومركز الرقابة للبيانات على وضع السياسات والمعايير الخاصة بحماية الخصوصية الرقمية وضمان الاستخدام المدروس لبيانات.
- 8- أكد المظالم في المادة الخامسة من نظام حماية بيانات الشخصية على حظر معالجة البيانات الشخصية لأغراض غير تلك التي تم جمعها لأجلها، إلا بعد الحصول على موافقة مسبقة من صاحب البيانات، وبأنه هذا الالتزام يستخدم مع مبدأ الحق في الخصوصية

ثانياً: الفوصيات

1. إعداد تشريع خاص للذكاء الاصطناعي يتضمن ضوابط واضحة لمعالجة البيانات الشخصية ضمن أنظمة الذكاء الاصطناعي. ويناقش المسائل مثل: الشفافية، تفسير القرارات الآلية، التحيز التمييزي، والمساءلة القانونية.
2. تعزيز آليات المراقبة والتقييم ضمن PDPL لضمان الامتثال في استخدام الذكاء الاصطناعي. وذلك عبر تحديد الجهة الرقابية والحاسبية، وتحديد العقوبات لمن يخالف الضوابط الخاصة بالبيانات الحساسة والمعالجة الآلية.
3. توعية مستخدمي الخدمات الرقمية والمؤسسات بتجارت استخدام الذكاء الاصطناعي على الخصوصية، وتشجيع ثقافة المراقبة الصريحة والحد من مشاركة البيانات غير الضرورية، باعتبار أن التوعية جزء لا يتجزأ من الحماية القانونية.
4. تبني حوكمة بيانات وصحية وبيانات مشتركة تتضمن معايير واضحة لنقل البيانات عبر الحدود ومعالجتها في سياق الذكاء الاصطناعي، بما يتناسب مع متطلبات الاقتصاد السعودي الرقمي ورؤية السعودية

2030

قائمة المراجع والمصادر:

أولاً: القرآن الكريم.

ثانياً: الكتب العلمية

- 1- بن عثمان، فريد، (2020)، الذكاء الاصطناعي، مقارنة قانونية، دفا تر السياسة والقانون المجمعة ١٢، الجزء الثاني، ٣٠٢٠.
 - 2- جيمس كروز، كيث روس، شبكات احاسب والإنترنت " أمن ومبادئ الشبكات والإنترنت"، ترجمة: د. السيد محمد الأنقر، دار رضوان السيد عبد العال، دار العيكان، سنة 2011، الطبعة الرابعة.
 - 3- احابت، أوديس مسود، (2020)، توثيق الاحتماد وإشكالية حماية البيانات الشخصية على الإنترنت، مؤسسة الحديثة للكتاب، بيروت.
 - 4- حسبو، عمرو احمد، (2000)، حماية الخريات في مواجهة نظم المعلومات، ج (1) دار النهضة العربية للنشر والتوزيع.
 - 5- عيفة، إيهاب، (٢٠٢٠م)، الذكاء الاصطناعي، مسبق الحيات البشرية في ظل التطورات التكنولوجية، مجلة نصرة العامة للكتاب، الصفة الأولى.
 - 6- عيفة، محمد، (2007)، الحماية الجنائية معطيات احاسب الآلي، بدون صفة دار الجامعة الجديدة للنشر، الإسكندرية، مصر.
 - 7- الدعيف، نجيب محمد، (2023)، الذكاء الاصطناعي (أحد) تحديات المسؤولية المدنية المعاصرة)، دار اتفاقية للنشر والتوزيع، عمان (الأردن)، الصفة الأولى، 1444هـ.
 - 8- الدوخ، إلهي احمد، (2018)، مسؤولية المدنية الناشئة عن الممارسات غير المشروعة عبر موقع التواصل الاجتماعي، دار الجامعة الجديدة.
 - 9- الدوازي، محمد بن أبي بكر بن عبد القادر، (1987)، مختار الصحاح، دار الكتاب الحديث، مصر.
 - 10- سامح، محمد عيسى، وهديج، حسون عيبد، (2007)، الحرية المعلوماتية تحت مستر غني مجلة جامعة باب، العراق، محمد (14)، العدد (2).
- سامح عامر، التميز الإداري في القرن الحادي والعشرين، سامر: دار النهج، سنة 2013.

- 11- السعيد. وفاء حنمل، تقنية الذاكرة الاصطناعي وحماية البيانات الشخصية، ص1429.
- 12- مسم، وليد السيد. (2012). صدارات الخصوصية في الإنترنت، دار الجامعة الجديدة.
- 13- سيد، محمد. (2018). الحماية القانونية لبيانات الشخصية: دراسة مقارنة في القانون البريطاني والإماراتي.
- 14- عدا، محمد محمد. (2012)، فكرة حماية البرامج بحاسب الآلي، دار الجامعة الجديدة للنشر. الإسكندرية، مصر.
- 15- الشرقاوي، محمد. (٢٠١١م). الذاكرة الاصطناعي والشبكات العصبية. بغداد: إصدارات جامعة الإمام محمد الصادق.
- 16- صا، مروة زين العايدى. (2017). الحماية القانونية الدولية لبيانات الشخصية عبر الإنترنت من القانون الدولي والقانون الوطنى - مركز الدراسات العربية - ط 1 - 2017.
- 17- عبد الرزاق، علاء، (١٩٩٩م). نظم المعلومات والذاكرة الاصطناعي، ط1، دار الشايع للنشر والتوزيع، عمان، الأردن.
- 18- العنبي، أمالي بن محمد بن سيف. (2025). الوظيفة الرقابية لحماية لبيانات الشخصية: دراسة مقارنة، جرش لبحوث والدراسات، مج 25، ع2.
- 19- فريد بن عثمان الاصطاعى مقارنة قانونية دوائر السياسة والقانون المجمعة ١٢، الجزء الثاني، ٢٠٢٠.
- 20- الكعبي، محمد عبيد، (2009). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، ط ٢، القاهرة.
- 21- الأهلواني، حسام الدين كامل وروند، طارق جمعة السيد وعنبي، جابر محجوب. دور التصفح في اكتساب الشبكة العنقارية عن طريق القادة في القانون المصري، المجلد 3، العدد3.
- 22- محمد اللغة العربية. (2005)، مجمع المصنف.

ثالثاً: الرسائل العلمية

- 1- التونسى، نيات بن أحمد، والعلم، سيمان بن محمد. (2024). الفراعند والإجراءات المنظمة لاستخدامات الذاكرة الاصطناعي بالشبكة العربية السعودية وأثارها القانونية (دراسة تحليلية مقارنة).

- 2- احمد، فايز بن حسن، المسؤولية المدنية لتأني الخوي (دراسة مقارنة بين النظام السعودي والفقه الإسلامي)، رسالة دكتوراه، كلية الشريعة والقانون، جامعة الأزهر الشريف، جمهورية مصر.
- 3- الشمرى، فهد بن غايده، (2023)، الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية: دراسة تحليلية.
- 4- عثمان، طارق، (2007)، الحماية الجنائية للحياة الخاصة غير الإنترنت: دراسة مقارنة، رسالة ماجستير، كلية القانون جامعة محمد عظيم، ص 81.
- 5- العجمي، أحمد محمد، (2023)، بحث في خصوصية البيانات الشخصية وخصائص حمايتها في عصر التحول الرقمي: دراسة تحليلية في النظام السعودي، الإدارة العامة.
- 6- العناني، ممدوح عيسى، (1983)، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، رسالة دكتوراه مقدمة كلية الحقوق جامعة القاهرة، دار محمد نصر على السيد، حماية الحياة الخاصة في القانون المدني، رسالة دكتوراه مقدمة كلية حقوق جامعة الزقازيق.
- 7- النمر عاوي، فاطمة عبد الله، (1440هـ)، مسؤولية المدنية لمتاح في النظام السعودي، كلية الشريعة والدراسات الإسلامية، جامعة القصيم، قسم الأنظمة.
- 8- القطيشة، ياسر فايز حمد والحداوان ممدوح حسن ملاح، (2022)، حماية الجنائية خصوصية بيانات الشخصية الرقمية: دراسة مقارنة، رسالة دكتوراه غير منشورة جامعة العلوم الإسلامية العالمية، عمان.
- 9- مرادي، أياد محمود حسنى و ناصر الندى نزار، يعقوب عادل ناصر، (2025)، حماية بيانات الشخصية الرقمية في التشريع الأردني (رسالة ماجستير غير منشورة) جامعة الشرق الأوسط، عمان.

ثالثاً: المقالات والدوريات

- 1- احمد، طارق جمعة السيد، (2019)، الحماية القانونية لخصوصية بيانات الشخصية في العصر الرقمي: دراسة مقارنة، مجلة القانون والاقتصاد، ج (92)،
- 2- ساه، كريمة عيسى، (2022)، الجوانب القانونية لتذكاء الاصطناعي، مجلة جيل الأبحاث القانونية، العدد 4، أكتوبر 2022، ص 20-22.
- 3- الصغير، محمد مهدي، الزهفة، عنى الحاجة الرقمية لبيانات الشخصية "دراسة مقارنة"، مجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية.

- 4- عمرو، فهد محمد. (2020)، تنظيم القانوني لمعالجة البيانات الشخصية: دراسة تطبيقية على معاملة تسجيلات المراقبة الجوية، الميمنة العلمية لعلوم والمواضع، الامارات.
- 5- الكرار، حبيب جيتون وحسام عيسى عزدود. (٢٠١٩م)، المسؤولية عن الأضرار التي يسببها الروبوت، مجلة كلية الإمام الكاظم، العدد ٦.
- 6- النكبي، خالد، بن عبد الرحيم بن حابر. (2024)، المسؤولية المدنية عن فعل الذكاء الاصطناعي في نظام السعودي دراسة تحليلية تأسيسية مجلة بحوث الفقهية والقانونية، العدد السابع والأربعين.
- 7- إبراهيم دؤود، الحماية القانونية لبيانات الشخصية من منظور الحق في الخصوصية، مجلة كلية الحقوق لبحوث القانونية والاقتصادية، "جامعة الإسكندرية"، عام 2015.
- 8- إبراهيم، محمد فتحي محمد، التطور التشريعي لتطبيقات الذكاء الاصطناعي، مجلة لبحوث القانونية والاقتصادية، العدد 81.
- 9- أحمد، وفاء حنفي السعيد سيد، (2024)، تقنية الذكاء الاصطناعي وحماية البيانات الشخصية: دراسة مقارنة، مجلة لشرعية والقانون، ع 43.
- 10- بن عثمان، فريدو. (2020)، الذكاء الاصطناعي: مقارنة قانونية، دفتر السياسة والقانون، مع 12، ع 2.
- 11- بومدين، محمد، (2019)، الذكاء الاصطناعي تحد جديد لقانون معارلات في الأبحاث والدراسات القانونية العدد ١٠، ٢٠١٩.
- 12- التهامي، سامح عبد الواحد. (2011)، الحماية القانونية لبيانات الشخصية: دراسة قانونية فرنسية، القسم الأول مجلة الحقوق جامعة الكويت، سبتمبر ٢٠١١، مع ٣٥، ع ٣.
- 13- الجعيد، صالح عوض منصور، (2025)، الحماية الخيرية لمعالجة البيانات الشخصية في نظام السعودي (دراسة مقارنة)، مجلة الأندلس لعلوم الإنسانية والاجتماعية، العدد (114) محمد (12).
- 14- الحسانات، حنان عظم حسن، (2025)، مفهوم البيانات الشخصية وحدودها، جرش محلات والدراسات، مع 25، ع 2.
- 15- حميسي، رضا، (2019)، الضمانات القانونية في حماية بيانات الشخصية في الفضاء الرقمي، المؤثر الدولي الثالث لقانون والتعددية، كلية لشرعية والقانون، العدد الأول، إصدار خاص.

- 16- الخالدي، إلياس حبيب، (1442هـ) حوكمة استخدام الذاكرة الاصطناعي في العصر الرقمي، قراءة قانونية في السياق الأخلاقي الأوروبي بشأن استخدام الذاكرة الاصطناعي في الصحة القضائية وبيئة المحاكم والدراسات التشريعية لعدد السادس عشر بعد المائة.
- 16- الخالدي، إلياس حبيب، (1442هـ)، حوكمة استخدام الذاكرة الاصطناعي في العصر الرقمي، قراءة قانونية في السياق الأوروبي بشأن استخدام الذاكرة الاصطناعي في الصحة القضائية وبيئة المحاكم والدراسات التشريعية لعدد السادس عشر بعد المائة.
- 17- السعيد، وفاء حمير، (2024)، تقنية الذاكرة الاصطناعي وحماية البيانات الشخصية - دراسة مقارنة، مجلة الشريعة والقانون، ج 43.
- 18- شياني، عبد الله جامعة محمد بن دباغر حبيب، (2023)، حق الخصوصية المعلوماتية في ضوء الذاكرة الاصطناعي، مجلة الدراسات القانونية والاقتصادية، العدد 6، العدد 2.
- 19- شياني، عبد الله، ساء بن وداو، (2023)، حق الخصوصية المعلوماتية في ضوء الذاكرة الاصطناعي، مجلة الدراسات القانونية والاقتصادية، مج 6، ج 2.
- 20- عبد الله شياني، (2023)، حق الخصوصية المعلوماتية في ضوء الذاكرة الاصطناعي، مجلة الدراسات القانونية والاقتصادية، العدد 6، العدد 2.
- 21- القرني، روي سعد، (2021)، الحماية القانونية لمحق في الخصوصية المعلوماتية (دراسة مقارنة)، مجلة كلية الدراسات الإسلامية والعربية لسات بامبور، العدد السادس، الإصدار الثاني، الجزء الأول.
- 22- القرني، روي سعد، (2021)، الحماية القانونية لمحق في الخصوصية المعلوماتية (دراسة مقارنة)، مجلة كلية الدراسات الإسلامية والعربية لسات بامبور، العدد السادس، الإصدار الثاني، الجزء الأول.
- 23- مجيد، موز حميد، (2018)، الحماية القانونية لمحق في البيانات الشخصية، مجلة دراسات قانونية وسياسية، العدد السادس، العدد الحادي عشر.
- 24- محارب، عبد العزيز قاسم، (2023)، الذاكرة الاصطناعي: مفهومه وتصنيفاته، مجلة المال والبنوك، ج 652.

- 25- محمد، حسن عبد الله النظام القانوني لحماية بيانات الشخصية المعالجة إلكترونيًا. دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة. مجلة للدراسات القانونية. جامعة عثمان كنية القانون، يوليو ٢٠٢١.
- 26- المراجع، أحمد عبد الله (2017). التجربة الإلكترونية ودور القانون الجنائي في أحد منها. المركز القومي للإصدارات القانونية، القاهرة.
- 27- مزين، عبد العزيز بن أحمد. (2023). موافقة صاحب البيانات الشخصية معاملة بياناته في النظام السعودي. دراسة تحليلية مقارنة مجلة كلية الشريعة والقانون بفتحها لأشرف - دقهية. العدد السابع والمئتم.
- 28- مقال منشور على مقال منشور على الإنترنت بعنوان: كيف تكفل الذاكرة الاصطناعي أن يساعد في حماية بيانات الشخصية وحصرية. تاريخ الإطلاع عليه 23/10/2025.
- 29- موسى، منور، وفريد، بعبدي فريد. (2025). التحديات القانونية لحماية بيانات الشخصية في سياق الذاكرة الاصطناعي. مجلة القانون العام الجزائري ومقارن.
- 30- الهداري، أحمد، عبد الفتاح حمدي. (2021). الذاكرة الاصطناعي وتطبيقاته في تطوير الإدارة الجامعية "رؤية مقترحة". جامعة الأزهر كلية الشريعة بالقاهرة. مجلة الشريعة، العدد 192، الجزء 2.
- 31- الهداري، أحمد، عبد الفتاح حمدي. (2021). الذاكرة الاصطناعي وتطبيقاته في تطوير الإدارة الجامعية "رؤية مقترحة". جامعة الأزهر كلية الشريعة بالقاهرة. مجلة الشريعة، العدد 192، الجزء 2.
- 32- وحدة الأبحاث بمؤسسة حرية الفكر والتعبير. (2020). الإنترنت والقانون في مصر (جزء الثالث): الخصوصية (رقمية)، الناشر مؤسسة حرية الفكر والتعبير.

رابعاً: المؤلفات العلمية

- الفقيه، مهدي سليمان. (2024). تأثير الذاكرة الاصطناعي على خصوصية البيانات والمستفيدين، المؤتمر والمعرض السنوي السابع والعشرون لجمعية المكتبات المتخصصة فرع الخليج العربي: توضيف التقنيات الذكية في بيئة المكتبات المتخصصة ومؤسسات المعلومات، النسخة: جمعية المكتبات المتخصصة.

خامساً: القوانين

- نظام حماية البيانات الشخصية الصادر بامر مرسوم الملكي رقم (م ١٩) وتاريخ 2/2/1443.
- وزارة الصحة السعودية، طريقة حقوق المرضى، ٢٠١٩.

سادس: المصادر الأجنبية

- 1- Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139. International Data Privacy Law, 2017, Vol.7.
- 2- Petter Carey, Data Protection, fifth edition, Oxford,2018
- 3- F. RASO, H. HILLIGOSS, V. KRISHNAMURTHY, C. BAVITZ, L. KIM, Artificial intelligence and Human rights, 1, September 25, 2018, 7
- 4- Artificial Intelligence and Data Protection, Council of Europe, November 2019, On Sit www.coe.int/AI
- 5- Lilian Mitrou, Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation? (GDRP) Artificial Intelligence-Proof? SSRN Electronic Journal, APRIL 2019.
- 6- Guidelines on artificial intelligence and data protection (Convention 108), Council of Europe, 25/1/2019, On Site: www.coe.int/AI
- 7- Meskenaite, Gabbi. (2022). An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality. Graduate Thesis. Faculty of Law. Lund University.
- 8- Breen, S et al. (2020). GDPR: Is your consent valid?. Business Information Review (BIR). (DOI: 10.1177/0266382120903254).
- 9- Fabrice NAFTALSKL, OEUVRE COLLECTIVE Sous LA DIRECTION DEPHILIPPE – HENRI DU THEIL, Fonctionnement de l'association, partie 4 , 2016 (actualization : Avril 2019).
- 10- L'utilisation de cookies constitue un traitement de données – conseil d'Etat 6 juin 2018 – Le bon 2018, Recueil Lebon – Recueil des decisions du conseil d'Etat 2018 www.Dalloz.fr.com.
- 11- Céline CASTETS-RENARD, La protection des données personnelles dans les relations internes à l'Union européenne , Dalloz , Octobre 2018. N: 267.
- 12- AVOINE (G.): Sécurité de la R F I D, Comprendre la technique sans être technician, in la secrete de l'individu numérise, réflexions prospectives et internationals, sous la direction de LACOUR (S), L'Harmattan , 2008.

- 13- Réglement européen (UE) 2018 / 608 de la commission du 14 avril établissant les critères techniques applicables aux étiquettes électroniques pour les équipements marins (JOUE n° L 110, 20 avril 2018).
- 14- Mike Puglia, Albert Puglia, V. Daniel Hunt, R F I D, A Guide to Radio Frequency identification, John Wiley, Sans , 2007 .