تحديات حماية المستهلك من خوارزميات الذكاء الاصطناعي

(دراسة تحليلية)

Challenges of Consumer Protection from Artificial Intelligence Algorithms (An Analytical Study)

أ.م.و. عامر غانم علوان
كلية القانون/ جامعة بغداد

الملخص

يهدف هذا البحث إلى دراسة حماية المستهلك من برمجيات الذكاء الاصطناعي، مع التركيز على التحديات التي يواجهها المستهلك في العصر الرقمي، تم تناول التشريعات العالمية مثل قانون الاتحاد الأوروبي بشأن الذكاء الاصطناعي، الذي يسعى إلى تنظيم استخدام الذكاء الاصطناعي وتعزيز حماية المستهلك من المخاطر المرتبطة بهذه التقنيات، كما تم النظر في المسؤولية القانونية المتعلقة بالأضرار الناتجة عن الذكاء الاصطناعي وصعوبة تحديد الفاعل والسببية في هذه الحالات، وتم التطرق أيضًا إلى أهمية حماية البيانات الشخصية، وكيف أن جمع البيانات وتحليلها يمكن أن يشكل تهديدًا لخصوصية المستهلكين.

الكلمات المفتاحية: حماية المستهلك، الذكاء الاصطناعي، الخصوصية، المسؤولية القانونية، الروح الرقمية.

Summary

This research aims to explore the protection of consumers from artificial intelligence (AI) software, with a focus on the challenges consumers face in the digital age. Global regulations such as the European Union's AI Act, which seeks to regulate the use of AI and enhance consumer protection against associated risks, were discussed. The legal responsibility for damages resulting from AI use, along with the difficulty in determining the responsible party and establishing causality, was also addressed. Additionally, the importance of protecting personal data was highlighted, noting how the collection and analysis of data could pose a threat to consumer privacy.

Keywords: Consumer protection, artificial intelligence, privacy, legal responsibility, digital soul.

المقدمّة

أولاً: جوهر فكرة البحث: تمثل حماية المستهلك من الأضرار التي تنجم عن تقنيات الذكاء الاصطناعي في سياق حماية المستهلك أحد التحديات القانونية المستجدة والمعقدة في العصر الرقمي، ففي ظل الانتشار الواسع لتقنيات الذكاء الاصطناعي، من السيارات الذاتية القيادة إلى التوصيات الموجهة عبر منصات التجارة الإلكترونية، يُطرح السؤال الأساسي: من يتحمل المسؤولية عندما يتسبب الذكاء الاصطناعي في أضرار للمستهلك؟ يواجه هذا السؤال صعوبة في الإجابة، نظرًا للطبيعة المعقدة لعمل الأنظمة الذكية التي تعتمد على خوارزميات معقدة قد لا تكون دائمًا قابلة للتفسير من قبل الأشخاص الذين صمموها أو الذين يشغلونها، إذًا، تكمن جوهر فكرة البحث في دراسة الأسس القانونية التي يمكن من خلالها حماية المستهلك من برمجيات الذكاء الاصطناعي من خلال تحديد المسؤولية في حالة الأضرار الناتجة عن هذه البرمجيات، مع تسليط الضوء على التحديات التي هذه المسألة.

ثانياً: أهمية البحث وأسباب اختياره: تكتسب هذه الدراسة أهميتها من الإقبال المتسارع على استخدام الذكاء الاصطناعي في شتى المجالات، بما فيها تلك التي لها تأثير مباشر على المستهلكين، مثل التوصيات والتوجيهات التجارية، الأنظمة المصرفية، والأنظمة الصحية، ولا تقتصر الأضرار الناتجة عن هذه البرمجيات على الأضرار المادية المباشرة فحسب، بل قد تتضمن أضرارًا معنوية أيضًا، مثل انتهاك الخصوصية أو التمييز الخوارزمي. كما أن هذه الأنظمة قد تتخذ قرارات بناءً على بيانات غير دقيقة أو خوارزميات يصعب تتبعها، مما يزيد من صعوبة تحديد الفاعل والمسؤول عن الضرر تحقيقاً للحماية المنشودة، فالحماية بلا جزاء تبقى مجرّد دعوات أو نصائح غير ملزمة، لهذا، فإن البحث في هذه القضية يكتسب طابعًا حيويًا لضمان حماية فعالة للمستهلكين، وتطوير إطار قانوني يتماشى مع التطورات التكنولوجية، باختيار هذا الموضوع، نأمل في تقديم مساهمة قانونية ملموسة تهدف إلى تطوير تشريعات جديدة أو تعديل التشريعات القائمة لتواكب هذا التحدي المستجد.

ثالثاً: إشكالية البحث: تتمثل إشكالية البحث في صعوبة تحديد المسؤولية القانونية في حالات الأضرار التي يسببها الذكاء الاصطناعي للمستهلكين تحقيقاً لحماية المستهلك من تطبيقات الذكاء الاصطناعي، فمع تطور الذكاء الاصطناعي وتعقد الخوارزميات التي يعتمد عليها، أصبح من الصعب تحديد الجهة التي يتحمل المسؤولية القانونية في حال حدوث ضرر، هل هي الشركة المصنعة للبرنامج؟ أم المستخدم الذي يقوم بتشغيل النظام؟ أم النظام نفسه باعتباره "كيانًا مستقلًا" يمكن أن يتحمل المسؤولية؟ كما أن العلاقة السببية بين الفعل الناتج عن النظام الذكي

والضرر الذي يلحق بالمستهلك قد تكون غير واضحة في كثير من الحالات، مما يثير إشكالية كبيرة في إثبات هذه العلاقة في محاكم القانون، وبعبارة أخرى، ليس من السهل دائمًا تتبع الروابط بين الفعل الضار والنتيجة الضارة عندما يتدخل الذكاء الاصطناعي كوسيط. وهذا جزء من البحث، الذي يبحث في كيفية تحقيق أنجع صورة لتلك الحماية.

رابعاً: أسئلة البحث: ومن خلال الإشكالية السالفة الذكر تنبثق التساؤلات البحثية الآتية:

١. كيف تتعامل الأنظمة القانونية المختلفة مع التحديات التي يطرحها الذكاء الاصطناعي في مجال المسؤولية المدنية؟

٢. هل تواكب التشريعات القانونية الحالية التطورات التكنولوجية في مجال الذكاء الاصطناعي وكيف يمكن تعديلها لتوفير حماية أكثر فعالية للمستهلكين؟

٣. ما هي التحديات التي قد يواجهها المستهلكون في محاولة للحصول على تعويضات عن الأضرار الناتجة عن برمجيات الذكاء الاصطناعي؟

٤. ما هي تجارب الدول "التشريعية" الناجحة في هذا المجال؟

خامساً: منهجية البحث: سيتبع هذا البحث منهجًا تحليليًا لدراسة التشريعات القانونية المعمول بها في مختلف الأنظمة القانونية، مثل الاتحاد الأوروبي، الولايات المتحدة، والصين، فيما يخص المسؤولية عن الأضرار التي يسببها الذكاء الاصطناعي، إذ سيتم فحص القوانين التي تهدف إلى حماية المستهلك في هذا المجال، مع تسليط الضوء على الآليات القانونية المتاحة لفرض المسؤولية في مثل هذه الحالات، وسيتم أيضًا تحليل عدد من الحالات القضائية التي تتعلق بالذكاء الاصطناعي لتوضيح كيفية تطبيق القوانين في الحالات الواقعية، كما سيتناول البحث الآراء الفقهية الحديثة حول كيفية تحديث القوانين لمواكبة التطورات في هذا المجال.

سادساً: هيكلية البحث: بمبحثين، تسبقهما مقدمة، وتعقبهما خاتمة، تناولنا موضوع بحثنا، ففي المبحث الأول تناولنا تأثير برمجيات الذكاء الاصطناعي على المستهلك وأهمية حمايته، وفي المبحث الثاني بحثنا في الآليات القانونية لحماية المستهلك من برمجيات الذكاء الاصطناعي.

المبحث الأول: تأثير برمجيات الذكاء الاصطناعي على المستهلك وأهمية حمايته

The First Topic: The impact of artificial intelligence software on consumers and the importance of protecting them

يُعدُّ الذكاءُ الاصطناعيُّ أحدَ أبرز الابتكارات التقنية التي أحدثت ثورةً في الحياة الاقتصادية والاجتماعية، إذ أصبح أداةً رئيسيةً في القطاعات التجارية والمالية والصحية، مما أثر بشكلٍ كبيرٍ على سلوك المستهلكين وقراراتهم، وتعمل

برمجياتُ الذكاء الاصطناعي من خلال تحليل البيانات الضخمة واستنباط أنماط السلوك، ما يتيح لها تقديم توصياتٍ مخصصةٍ، ولكنها في الوقت ذاته تُثير مخاطر قانونيةً عديدةً، من بينها انتهاك الخصوصية، التحيز الخوارزمي، والتأثير غير العادل على المستهلك. ولذلك، برزت الحاجةُ إلى تنظيمٍ قانونيٍّ يوازن بين تشجيع الابتكار وحماية حقوق المستهلكين.

وعلى هذا الأساس سنقسِّمُ هذا المبحث على مطلبين، نتناولُ في أولهما تأثير برمجيات الذكاء الاصطناعي على المستهلك، ونتوقف في المطلب الثاني مع دواعي حماية المستهلك من برمجيات الذكاء الاصطناعي.

المطلب الأول: تأثير برمجيات الذكاء الاصطناعي على المستهلك

The First Requirement: The impact of artificial intelligence software on the consumer

تُستخدم برمجياتُ الذكاء الاصطناعي في العديد من القطاعات لتقديم خدماتٍ محسّنةٍ تعتمد على تحليل سلوك المستهلك، غير أن هذا الاستخدام قد يؤدي إلى انتهاك حقوق المستهلك بطرقٍ غير مباشرة. ومن أبرز أوجه هذا التأثير ما سيتم توضيحه في الفروع الآتية:

الفرع الأول: جمع البيانات وتحليلها وتأثيرها على المستهلك

The First Subsection: Data collection and analysis and their impact on the consumer

تعتمد برمجيات الذكاء الاصطناعي[١] على جمع بياناتٍ ضخمةٍ من المستخدمين، مثل عمليات البحث، أنماط الشراء، مواقع الويب التي يزورونها، وحتى سلوكهم على منصات التواصل الاجتماعي، وعلى الرغم من أن هذا يُمكّن الشركات من تخصيص الإعلانات والعروض، إلا أن ذلك قد يُؤدي إلى انتهاك حقوق المستهلكين في الخصوصية، على سبيل المثال، في قضية "فيسبوك وكامبريدج أناليتيكا" (Cambridge Analytica & Facebook) الشهيرة[٢]، استُخدمت بياناتُ ملايين المستخدمين دون موافقتهم لتحليل توجهاتهم السياسية وتوجيه الإعلانات بناءً على تفضيلاتهم، مما اعتُبر انتهاكًا جسيمًا لقوانين حماية المستهلك، وقد نتج عن هذه الفضيحة فرض لجنة التجارة الفيدرالية الأمريكية (FTC) غرامةً ماليةً ضخمةً على فيسبوك بقيمة ٥ مليارات دولار، استنادًا إلى انتهاكها لقوانين الخصوصية[٣].

وعلى الصعيد التشريعي، أكدت اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي عام ٢٠١٨ على ضرورة أن يكون جمع البيانات الشخصية قائمًا على موافقة صريحة ومسبقة من المستهلك، مع منحه حق معرفة كيفية استخدام بياناته وحق طلب حذفها في أي وقت[٤]. تلك البيانات التي اصطلح أحدهم على تسميتها (الروح الرقمية)[٥].

الفرع الثاني: التأثير على قرارات المستهلك والتلاعب بخياراته

The second Subsection: Influencing consumer decisions and manipulating their choices

تُستخدم تقنيات الذكاء الاصطناعي في تحليل سلوك المستهلك لتوجيهه نحو قراراتٍ معينةٍ قد لا تكون في مصلحته، مثلاً، تعتمد شركات التجارة الإلكترونية مثل أمازون (Amazon) وعلي بابا (Alibaba) على خوارزميات تُظهر للمستهلك منتجاتٍ تتوافق مع اهتماماته، مما قد يُقلل من فرص استكشافه خياراتٍ أخرى بأسعارٍ أفضل[٦]. وقد أظهرت دراسات اقتصادية أن الخوارزميات قد تدفع المستهلكين إلى شراء منتجات غير ضرورية من خلال تقنيات التلاعب السلوكي، مثل " تغيير الأسعار الديناميكي" (Dynamic Pricing)، حيث تُظهر بعض المواقع أسعارًا أعلى لمستهلكين معينين بناءً على تحليل بياناتهم وسلوكهم الشرائي السابق[٧].

من جانِبها محكمة العدل الأوروبية (ECJ) في حكمها الصادر في القضية رقم C-673/17 لسنة ٢٠١٩ والمعروفة – أي القضية- باسم الاتحاد الألماني لمنظمات حماية المستهلك ضد شركة planet49 GmbH، والتي تناولت شرعية استخدام ملفات تعريف الاتباط COOKIES على مواقع الويب من دون موافقة صريحة من المستخدمين أصدرت قرارًا ينص على أن استخدام ملفات تعريف الارتباط (Cookies) لتوجيه الإعلانات وتحليل سلوك المستهلك يجب أن يكون مشروطًا بموافقة واضحة ومسبقة، مما يُؤكد على ضرورة حماية المستهلك من التلاعب الخفي بقراراته[٨]. مستندةً على عددٍ من الأسس القانونية منها المادة (٥) من توجيه الخصوصية الالكترونية Directive EC الصادر في ٢٠٠٢.

الفرع الثالث: التحيز الخوارزمي وأثره على العدالة الاستهلاكية

The third Subsection: Algorithmic bias and its impact on consumer fairness

يُعتبر التحيز الخوارزمي من أخطر التحديات التي تواجه المستهلك في ظل انتشار الذكاء الاصطناعي، حيث قد تُميز الخوارزميات ضد فئات معينةٍ من المستهلكين بناءً على العمر أو العرق أو الحالة الاجتماعية، ويقصد به:" التمييز أو التفضيل غير المنصف الذي يظهر في النتائج أو القرارات التي تتخذها الخوارزميات الحاسوبية أو نظم الذكاء الاصطناعي التي من شأنها التفرقة بين الأشخاص بناء على عوامل معينة مثل الجنس، العرق، الدين، الأصل الاجتماعي، أو أي سمات أخرى"[٩]، فعلى سبيل المثال، وجدت دراسةٌ أجرتها جامعة MIT عام ٢٠١٩ أن برمجيات التوظيف المعتمدة على الذكاء الاصطناعي لدى بعض الشركات كانت تُفضل المتقدمين الذكور على الإناث، نتيجةً لاعتمادها على بياناتٍ

تاريخيةٍ متحيزة، ففي عام ٢٠١٩، أجرى باحثون من معهد ماساتشوستس للتكنولوجيا (MIT) دراسة حول تحيز الذكاء الاصطناعي ضد النساء، وكشفت النتائج عن وجود فجوة واضحة في دقة تصنيف الجنس بناءً على لون البشرة والجنس، وأظهرت الدراسة أن أنظمة تحليل الوجوه، مثل Amazon Recognition[١٠]، كانت أقل دقة في التعرف على النساء، خصوصًا ذوات البشرة الداكنة، حيث أخطأت في تصنيفهن كذكور بنسبة تصل إلى ٣١%، بينما كان معدل الخطأ في تصنيف النساء ذوات البشرة الفاتحة أقل بكثير، هذه النتائج تعزز المخاوف بشأن التحيزات المدمجة في خوارزميات الذكاء الاصطناعي، والتي يمكن أن تعكس وتضخم التحيزات الاجتماعية القائمة، نظرًا لأن هذه الأنظمة تُدرَّب غالبًا على مجموعات بيانات غير متوازنة تمثل فئات معينة أكثر من غيرها، وقد دفعت الدراسة الشركات الكبرى مثل مايكروسوفت وأمازون إلى تحسين خوارزمياتها وتقليل أخطاء التصنيف من خلال استخدام مجموعات بيانات أكثر شمولًا وتنوعًا[١١].

وفي قضيةٍ بارزةٍ في الولايات المتحدة، رفعت وزارة الإسكان والتنمية الحضرية (HUD) دعوى قضائية ضد شركة فيسبوك، متهمةً إياها باستخدام الذكاء الاصطناعي لاستهداف إعلانات الإسكان بطريقةٍ تنتهك قانون الحقوق المدنية، حيث كانت الإعلانات تُستبعد تلقائيًا من الظهور لفئاتٍ معينةٍ من المستخدمين بناءً على عِرقهم أو وضعهم الاجتماعي، وبناءً على ذلك، أصدرت اللجنة الفيدرالية للتجارة (FTC) إرشاداتٍ جديدةً تُلزم الشركات بتدقيق أنظمتها الخوارزمية للتأكد من عدم وجود تحيزٍ في قراراتها، خاصةً في القطاعات المالية والإسكانية[١٢].

المطلب الثاني: دواعي حماية المستهلك من برمجيات الذكاء الاصطناعي

The First Requirement: The necessity of protecting the consumer from artificial intelligence software

في ظل التطور التكنولوجي المتسارع، أصبحت برمجيات الذكاء الاصطناعي جزءًا أساسيًا من حياتنا اليومية، حيث تدخل في العديد من القطاعات مثل التجارة، الرعاية الصحية، والتعليم، ومع ذلك، يواجه المستهلكون العديد من التحديات المرتبطة باستخدام هذه البرمجيات، والتي قد تتسبب في انتهاك خصوصياتهم، أو التلاعب في قراراتهم، أو إلحاق الأضرار بهم جراء الأخطاء التقنية، لذلك، أصبحت الحاجة إلى تشريعات تحمي المستهلكين من برمجيات الذكاء الاصطناعي ضرورة ملحة، وذلك لضمان توفير بيئة رقمية آمنة وشفافة. ويمكن بيان تلك الدواعي من خلال تقسيم هذا المطلب على الفروع الاتية:

الفرع الأوّل: حماية الخصوصية ومنع الاستغلال غير المشروع للبيانات
The First Subsection : Protecting privacy and preventing the unlawful exploitation of data

نظرًا لأن الذكاء الاصطناعي يعتمد على البيانات، فإن حماية المستهلك تستوجب وضع آلياتٍ صارمةٍ تضمن عدم إساءة استخدام بياناته، وقد أقرّت بعض التشريعات الحديثة، مثل قانون كاليفورنيا لحماية المستهلك (CCPA)[١٣]، بحق المستهلك في معرفة البيانات التي تجمعها الشركات عنه، والاعتراض على استخدامها، والمطالبة بحذفها عند الضرورة، ويعد قانون خصوصية المستهلك في كاليفورنيا CCPA من أكثر القوانين شمولاً لحماية البيانات في الولايات المتحدة، فيما يتعلق بجمع واستخدام البيانات الشخصية أو الخاصة، والذي يحتاج إلى الامتثال لهذا القانون هو جميع الكيانات الهادفة للربح التي تجمع وتعالج المعلومات الشخصية لسكان كاليفورنيا وتقوم بأعمال تجارية داخل الولاية، وبشروط ثلاثة[١٤] هي:

١- شركة تحقق إيرادات إجمالية سنوية تزيد على (٢٥) مليون دولار أمريكي.
٢- نشاط تجاري يشارك أو يتلقى معلومات شخصية لأكثر من ٥٠,٠٠٠٠ من سكان كاليفورنيا سنوياً.
٣- شركة تستمد ما لا يقل عن ٥٠% من إيراداتها السنوية عن طريق بيع معلومات شخصية لسكان كاليفورنيا. ويحمي هذا القانون الأشخاص الطبيعيين المقيمين في كاليفورنيا، سواءً كانت إقامتهم مؤقتة أم دائمة، ويحمي الحقوق الآتية[١٥]:

أ. **الحق في معرفة المعلومات الشخصية التي جمعتها الشركة وكشفت عنها وباعتها** : بموجب هذا الحق، يمكن للمستهلك أن يسأل أي شركة عن نوع المعلومات الشخصية التي تجمعها وتنشرها وتستخدمها وتبيعها، ويحق للمستهلك معرفة المصدر الذي جمعت منه الشركة معلوماته الخاصة، وكيف استخدمها، وقائمة بالأطراف الثالثة التي يشاركون أو يبيعون بياناتهم الشخصية معها.

ب. **الحق في طلب حذف المعلومات الشخصية**: بموجب قانون CCPA، سيكون للمستهلكين جميع الحقوق في الحصول على ملكية معلوماتهم الشخصية، ويمكنهم أن يطلبوا مباشرة من الشركة التي تجمع بياناتهم الشخصية وتعالجها إزالتها، وعند تلقي مثل هذا الطلب، يجب على الشركة اتخاذ جميع الخطوات اللازمة لمحو جميع البيانات الشخصية الخاصة بالمستهلك، ومع ذلك، في ظل ظروف محددة، يمكن للمنظمة أن تقرر ما إذا كانت ستمسح المعلومات أو

تحتفظ بها، كما لو كان لتحقيق الغرض الذي جمعت المنظمة البيانات من أجله في المقام الأول. عدا ذلك ، للالتزام بالعقد بين موضوع البيانات والعمل.

ت. **الحق في إلغاء الاشتراك في بيع المعلومات الشخصية**: يمكن لجميع المقيمين في كاليفورنيا ممارسة الحق في إلغاء الاشتراك في بيع بياناتهم الشخصية، ومع ذلك ، لممارسة هذا الحق ، يجب على المنظمة المعنية توفير رابط "لا تبيع معلوماتي الشخصية" [١٦]على الصفحة الرئيسية لموقعها على الويب، يعمل هذا الرابط كوسيلة تسمح للمستهلكين باختيار بيع معلوماتهم الشخصية.

ث. وفقا لقانون CCPA ، لا يسمح للشركة ببيع المعلومات الشخصية للمستهلك إذا كان عمره أقل من ١٦ عاماً، ومع ذلك ، إذا كان عمر المستهلك بين ١٣ و ١٦ عاماً أو أقل من ١٣ عاماً ، فيحق لوالديهم أو أولياء أمورهم إما التصريح ببيع المعلومات أو إلغاء الاشتراك فيها.

ج. **الحق في عدم التمييز لممارسة حقوق خصوصية المستهلك**: لدى CCPA منظور أوسع في منع الشركات من إعطاء معاملة غير تمييزية لجميع المستهلكين الذين يمارسون حقوق الخصوصية الخاصة بهم. بالإضافة إلى ذلك ، يحظر القانون على المنظمات فرض سعر مختلف أو تقديم سلع أو خدمات مختلفة للمستهلكين باستخدام حقوق CCPA الخاصة بهم، وبصرف النظر عن ذلك، يرتبط الاختلاف بشكل معتدل بالقيمة التي توفرها لك بياناتك[١٧].

ومن المفيد الإشارة في هذا المقام إلى تقنية تخصيص المحتوى للأفراد بوصفها انتهاك للخصوصية الالكترونية content personalization، حيث تستخدم منصات البث الرقمي ومواقع التواصل الاجتماعي تقنيات متقدمة في بناء المنصات الرقمية بحيث يتم تغيير المحتوى بتغيير سلوك المستهلك وطريقة بحثه وعرضه وتاريخ بياناته واهتمامه أيضاً، وتشيرNetflix إلى أنّها توفر ما يقارب من مليار دولار امريكي سنوياً بفضل قدرة تقنيات الذكاء الاصطناعي على ألية تدفقات المحتوى وتفاعل مع العملاء، ويمكن تحويل بيانات الجمهور إلى حملات فعالة للاحتفاظ بالعملاء وتخصيص المحتوى لإنشاء علاقة شخصية أكثر مع المشاهدين[١٨].

الفرع الثاني: منع التضليل والتلاعب بقرارات المستهلك

The Second Subsection: Preventing deception and manipulation of consumer decisions

لحماية المستهلك من الممارسات غير العادلة، ينبغي وضع قوانين تُلزم الشركات بالكشف عن كيفية عمل خوارزمياتها، وتمكين المستهلك من إيقاف

التوصيات المؤتمتة أو تعطيل جمع بياناته، كما ينص مشروع قانون الذكاء الاصطناعي في الاتحاد الأوروبي (EU AI Act)، الذي يُلزم الشركات بتوفير شفافيةٍ أكبر حول آليات اتخاذ القرار الآلي، ففي ظل الثورة التكنولوجية المتسارعة، أصبح الذكاء الاصطناعي جزءًا لا يتجزأ من الحياة اليومية، حيث يتم الاعتماد عليه في مجالات متعددة مثل الرعاية الصحية، الخدمات المالية، التجارة الإلكترونية، وأنظمة المراقبة، ومع تزايد الاعتماد على هذه التقنيات، برزت مخاوف قانونية وأخلاقية تتعلق بحقوق المستهلك، خصوصًا فيما يتعلق بالشفافية، الخصوصية، والمسؤولية عن الأضرار الناتجة عن القرارات التي تتخذها أنظمة الذكاء الاصطناعي[١٩].

لتنظيم هذا المجال المتنامي، تبنّى الاتحاد الأوروبي "قانون الذكاء الاصطناعي" (EU AI Act)، الذي يُعَدُّ أول إطار تشريعي شامل يهدف إلى تنظيم تطوير واستخدام أنظمة الذكاء الاصطناعي داخل الدول الأعضاء، ويهدف هذا القانون إلى تحقيق التوازن بين تشجيع الابتكار وحماية المستهلكين من المخاطر المحتملة لهذه الأنظمة، مما يجعله نموذجًا عالميًا للتشريعات المستقبلية في هذا المجال [٢٠].

يتميز قانون الذكاء الاصطناعي في الاتحاد الأوروبي بأنه قائم على نهج تصنيفي قائم على المخاطر (Risk-based Approach)، حيث يتم تصنيف أنظمة الذكاء الاصطناعي إلى أربع فئات رئيسية بناءً على مستوى تأثيرها على الأفراد والمجتمع:

١- **أنظمة الذكاء الاصطناعي ذات المخاطر الدنيا (Minimal Risk AI Systems):** تشمل هذه الفئة تطبيقات مثل أنظمة الذكاء الاصطناعي في الألعاب الإلكترونية أو البريد الإلكتروني المزعج (Spam Filters)، لا تفرض اللوائح أي قيود صارمة على هذه الأنظمة، ولكن يمكن لمطوريها تبنّي معايير أخلاقية طوعية[٢١].

٢- **أنظمة ذات مخاطر خاصة تتعلق بالشفافية (Limited Risk AI Systems):** تتطلب هذه الأنظمة مستوى معينًا من الشفافية لحماية المستهلك، على سبيل المثال، يجب على أنظمة الدردشة التفاعلية (Chatbots) إبلاغ المستخدمين بأنهم يتعاملون مع نظام ذكاء اصطناعي، مما يمنع الخداع والتضليل[٢٢].

٣- **أنظمة الذكاء الاصطناعي عالية المخاطر (High Risk AI Systems):** تشمل هذه الفئة الأنظمة المستخدمة في مجالات حساسة مثل[٢٣]:

أ. أنظمة الذكاء الاصطناعي المستخدمة في توظيف الموظفين، حيث يمكن أن تؤدي خوارزميات متحيزة إلى التمييز ضد فئات معينة، وخصوصاً تقنية التزييف العميق لبيانات الموظفين، والمسماة deep fake.

ب. أنظمة التشخيص الطبي القائمة على الذكاء الاصطناعي، والتي تتطلب دقة عالية لأن أي خطأ قد يؤدي إلى قرارات طبية خاطئة.

ت. أنظمة الذكاء الاصطناعي المستخدمة في التمويل، مثل تقييم الجدارة الائتمانية، حيث يمكن أن تؤثر على قرارات القروض. هذه الأنظمة يجب أن تمتثل لمجموعة من المعايير الصارمة، مثل توفير بيانات تدريبية عالية الجودة، ضمان التدقيق البشري، ووضع تدابير للتخفيف من المخاطر.

٤- **أنظمة الذكاء الاصطناعي غير المقبولة (Unacceptable Risk AI Systems)**: يحظر القانون بشكل صارم بعض التطبيقات التي تعتبر تهديدًا خطيرًا لحقوق الإنسان[٢٤]، مثل:

أ. التنميط الاجتماعي (Social Scoring) الذي تستخدمه بعض الحكومات لمراقبة سلوك الأفراد.

ب. الأنظمة التي تستغل ضعف الأفراد، مثل الأطفال أو الأشخاص ذوي الإعاقة، لتحقيق مكاسب غير عادلة.

يلعب هذا القانون دورًا محوريًا في حماية المستهلكين من الانتهاكات والمخاطر التي قد تنجم عن استخدام أنظمة الذكاء الاصطناعي، وذلك من خلال عدة آليات رئيسية:

الغصن الأوّل: تعزيز الشفافية ومنع التضليل :أحد أهم الجوانب التي يعالجها القانون هو إلزام الشركات بالإفصاح عن طبيعة أنظمة الذكاء الاصطناعي التي تتفاعل مع المستهلكينK فعلى سبيل المثال، في قطاع التجارة الإلكترونية، يمكن أن تؤثر خوارزميات الذكاء الاصطناعي على قرارات المستهلك من خلال التلاعب بالأسعار أو تقديم توصيات متحيزة، وبموجب القانون محل البحق، يجب على الشركات الكشف بوضوح عن كيفية عمل هذه الأنظمة، مما يمنح المستهلكين معلومات أكثر دقة لاتخاذ قرارات واعية.

تُعَدُّ الشفافية أحد المبادئ الأساسية التي يقوم عليها قانون الذكاء الاصطناعي في الاتحاد الأوروبي (EU AI Act)، حيث يُلزم مطوري ومشغلي أنظمة الذكاء الاصطناعي بتوفير معلومات واضحة حول طبيعة هذه الأنظمة، آلية عملها، والحدود التي تحكم قراراتها، تأتي هذه المتطلبات استجابةً للمخاوف المتزايدة من استخدام الذكاء الاصطناعي بطرق قد تؤدي إلى التضليل، التلاعب، وانتهاك حقوق المستهلكين، خصوصًا في المجالات التي يكون فيها المستخدمون عرضة لاتخاذ قرارات غير مستنيرة بناءً على مخرجات الذكاء الاصطناعي.

الغصن الثاني: مبدأ الشفافية في القانون[٢٥]: إلزام بالإفصاح وليس خيارًا: ينص قانون الذكاء الاصطناعي في الاتحاد الأوروبي على ضرورة كشف المستخدمين عن كونهم يتفاعلون مع أنظمة ذكاء اصطناعي، خصوصًا في التطبيقات التي تحاكي السلوك البشري مثل الشات بوتات (Chatbots)، والمساعدات الصوتية، والأنظمة التي تولد المحتوى تلقائيًا، على سبيل المثال، إذا كان المستهلك يتواصل مع روبوت محادثة للحصول على استشارات قانونية أو طبية، يجب أن يكون هناك إشعار واضح يوضح أن المتحدث هو نظام ذكاء اصطناعي وليس إنسانًا، مما يمنع تضليل المستخدمين أو إيهامهم بأنهم يتعاملون مع مختص بشري.

الغصن الثالث: تجنب التضليل في التجارة الإلكترونية والإعلانات الرقمية: مع انتشار تقنيات الذكاء الاصطناعي في مجال التجارة الإلكترونية والإعلانات الرقمية، بات من السهل التلاعب بسلوك المستهلكين عبر التوصيات الموجهة أو الإعلانات المستهدفة التي تعتمد على تحليل بياناتهم الشخصية وسلوكياتهم الشرائية، يفرض القانون قيودًا على الاستخدام غير الشفاف للخوارزميات التي تتحكم في الأسعار أو ترتيب المنتجات في منصات التجارة الإلكترونية، فعلى سبيل المثال إذا تم تعديل أسعار المنتجات بناءً على بيانات سلوك المستهلك دون علمه، يُعتبر ذلك انتهاكًا لمبدأ الشفافية، أو إذا تم التلاعب بترتيب المنتجات بحيث تُظهر الشركات الكبرى منتجاتها في الصفحات الأولى دون الإفصاح عن ذلك، فسيكون ذلك خرقًا للقانون، كما يُلزم القانون الشركات بالإفصاح عن استخدام المحتوى الاصطناعي (مثل النصوص أو الصور أو الفيديوهات المولدة عبر الذكاء الاصطناعي) في الإعلانات، مما يحمي المستهلكين من المعلومات المضللة[٢٦].

الغصن الرابع: الشفافية في أنظمة اتخاذ القرار الآلية (Automated Decision-Making Systems): أحد أكبر التحديات التي يواجهها المستهلكون هو عدم قدرتهم على فهم كيفية اتخاذ القرارات من قبل أنظمة الذكاء الاصطناعي، لا سيما في مجالات مثل التوظيف، القروض البنكية، والتأمين، وغيرها، يفرض قانون الذكاء الاصطناعي على الشركات والمؤسسات التي تستخدم الخوارزميات لاتخاذ قرارات تؤثر على المستهلكين توفير المعلومات التالية[٢٧]:

١. شرح واضح لكيفية اتخاذ القرار: إذا تم رفض طلب قرض بناءً على تحليل خوارزمية ذكاء اصطناعي، يجب توضيح السبب للمستهلك بطريقة مفهومة.

٢. إمكانية مراجعة القرار من قبل إنسان: يمنح القانون المستهلكين الحق في الطعن في القرارات التي تتخذها الأنظمة الآلية، وإعادة تقييمها من قبل شخص بشري عند الحاجة.

٣. توفير معلومات حول البيانات المستخدمة: يجب على الشركات توضيح نوع البيانات التي تم استخدامها في تدريب النظام، مما يساعد في منع التحيزات والتمييز غير العادل.

الغصن الخامس: مكافحة الأخبار المزيفة والتلاعب السياسي: في ظل الانتشار الواسع للذكاء الاصطناعي التوليدي، أصبح من الممكن إنشاء محتوى زائف بطريقة مقنعة، مثل الصور والفيديوهات والأخبار المزيفة (Deepfakes)، يحاول قانون الذكاء الاصطناعي الحد من هذه المخاطر عبر فرض متطلبات وضع علامات (Labeling) على المحتوى الذي يتم إنشاؤه بواسطة الذكاء الاصطناعي، مما يتيح للمستهلكين التمييز بين المحتوى الحقيقي والمزيف، على سبيل المثال، إذا تم استخدام الذكاء الاصطناعي لإنشاء فيديو سياسي خلال فترة الانتخابات، يجب وضع تحذير واضح بأن الفيديو تم إنشاؤه باستخدام الذكاء الاصطناعي، مما يحمي الناخبين من المعلومات المغلوطة والتلاعب بالرأي العام[٢٨].

الغصن السادس: التزامات الشركات والمطورين تحت طائلة المسؤولية: يُلزم القانون الشركات التي تطور وتستخدم أنظمة الذكاء الاصطناعي بضرورة الامتثال لمتطلبات الشفافية تحت طائلة العقوبات المالية الصارمة، ففي حال انتهاك معايير الشفافية أو استخدام الذكاء الاصطناعي بطرق مضللة أو خادعة، يمكن أن تفرض المفوضية الأوروبية غرامات تصل إلى ٦% من إجمالي الإيرادات السنوية للشركة المخالفة، وهي عقوبة مماثلة لتلك المطبقة في اللائحة العامة لحماية البيانات (GDPR).

من خلال فرض متطلبات الشفافية الصارمة، يسعى قانون الذكاء الاصطناعي في الاتحاد الأوروبي إلى خلق بيئة أكثر أمانًا للمستهلكين، بحيث يتمكن الأفراد من فهم كيفية عمل الأنظمة التي يتفاعلون معها، واتخاذ قرارات واعية بناءً على معلومات واضحة، وفي الوقت نفسه، يعزز القانون الثقة في الابتكارات التكنولوجية، حيث يُلزم الشركات بتطوير أنظمة ذكاء اصطناعي أكثر مسؤولية وأخلاقية، مما يؤدي إلى سوق رقمي أكثر عدلاً واستدامة على المدى الطويل.

الفرع الثالث: ضمان العدالة في الخدمات الرقمية

The Third Subsection: Ensuring fairness in digital services

إن ضمان المساواة بين المستهلكين في الوصول إلى الخدمات الرقمية أصبح ضرورةً قانونيةً، حيث ينبغي مراجعة البرمجيات الذكية بشكلٍ دوريٍّ للتحقق من عدم انحيازها لفئاتٍ معينة، وقد دعت منظمة التعاون والتنمية الاقتصادية (OECD) إلى ضرورة وضع لوائح تنظم آليات اتخاذ القرار المعتمدة

على الذكاء الاصطناعي لضمان عدم تمييز المستهلكين وفقًا لاعتباراتٍ غير موضوعية[٢٩].

يُظهر من ذلك أن برمجيات الذكاء الاصطناعي تمتلك قدرةً هائلةً على التأثير في المستهلكين، سواء من خلال جمع بياناتهم، أو التلاعب بقراراتهم، أو فرض معايير غير عادلةٍ في تقديم الخدمات، وقد أظهرت العديد من القضايا التشريعية والقضائية أن الحاجة إلى تنظيم هذا المجال أصبحت ضروريةً لضمان عدم استغلال المستهلكين بطرقٍ غير مشروعة. لذا، فإن الحل يكمن في إيجاد توازنٍ دقيقٍ بين الاستفادة من الابتكارات التكنولوجية من جهة، وحماية حقوق المستهلك من جهةٍ أخرى، وذلك من خلال وضع تشريعاتٍ صارمةٍ تُراعي التطورات التكنولوجية دون تقييد حرية الابتكار، وهو محور دراستنا في المبحث الثاني.

المبحث الثاني: الآليات القانونية لحماية المستهلك من برمجيات الذكاء الاصطناعي

The Second Topic: The legal mechanisms for protecting the consumer from artificial intelligence software

في ظل الانتشار الواسع لبرمجيات الذكاء الاصطناعي وتأثيرها العميق على مختلف جوانب حياة المستهلك، برزت الحاجة إلى وضع إطارٍ قانونيٍّ يُنظم استخدام هذه التقنيات، بحيث يُحقق التوازن بين مصلحة الشركات في الابتكار والتطوير، وحق المستهلك في عدم التعرض للمخاطر الناجمة عن هذه البرمجيات، فالذكاء الاصطناعي لم يعد مجرد أداةٍ تحليليةٍ تُستخدم لتحسين الخدمات، بل أصبح عاملاً أساسيًا في تحديد القرارات التجارية، وتسعير المنتجات، وتوجيه الإعلانات، بل وحتى اتخاذ القرارات المالية والقانونية، وهو ما يطرح تساؤلاتٍ قانونيةً حول مدى شرعية هذه الأنظمة، وإمكانية مساءلة مطوريها عند حدوث انتهاكاتٍ لحقوق المستهلك.

ويمكن تصنيف الآليات القانونية لحماية المستهلك من برمجيات الذكاء الاصطناعي إلى نوعين أساسيين: الأول يتعلق بالتشريعات والأنظمة القانونية التي تُحدد المعايير العامة لاستخدام الذكاء الاصطناعي في الأسواق الرقمية، والثاني يتناول المسؤولية القانونية للشركات المطورة لهذه البرمجيات، سواء من حيث المسؤولية المدنية أو الجنائية، وذلك بهدف ضمان عدم استغلال هذه التقنيات بطريقةٍ تضر بالمستهلكين أو تؤثر سلبًا على العدالة التجارية.

المطلب الأول: الإطار القانوني لحماية المستهلك من برمجيات الذكاء الاصطناعي

The First Requirement: The Legal Framework for Protecting the Consumer from Artificial Intelligence Software

إن وضع إطارٍ قانونيٍّ لحماية المستهلك من برمجيات الذكاء الاصطناعي يُعد ضرورةً ملحةً، نظرًا لأن القوانين التقليدية لحماية المستهلك لم تكن مصممةً لمواجهة تحديات الذكاء الاصطناعي، مما دفع العديد من الدول والمنظمات الدولية إلى إصدار قوانين وتشريعاتٍ جديدةٍ تُحدد ضوابط استخدام هذه البرمجيات، وتضع آلياتٍ لمساءلة الشركات عن أي ممارساتٍ غير عادلةٍ أو انتهاكاتٍ لحقوق المستهلك.

الفرع الأول: التشريعات الدولية لحماية المستهلك في البيئة الرقمية

The First Subsection: International Legislation for Consumer Protection in the Digital Environment

إنَّ الحديث عن التشريعات الدولية لحماية المستهلك في البيئة الرقمية يقتضي تقسيم هذا الفرع على نقاط، مع التذكير إنّ ما سيرد أدناه هو على سبيل المثال لا الحصر، فهنالك الكثير من التشريعات التي سُنّت لهذا الغرض، ومنها ما يلي:

١. **اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي**: تُعد هذه اللائحة من أقوى القوانين في مجال حماية المستهلك في العصر الرقمي، حيث وضعت قواعد صارمةً تحكم جمع البيانات الشخصية واستخدامها، وخاصةً عندما يكون الذكاء الاصطناعي هو المسؤول عن معالجة هذه البيانات[٣٠]. وتنص اللائحة على مبادئ هامة[٣١]:

أ. وجوب الحصول على موافقةٍ صريحةٍ من المستهلك قبل جمع بياناته أو تحليلها بواسطة برمجيات الذكاء الاصطناعي.

ب. حق المستهلك في الاعتراض على القرارات المؤتمتة التي تؤثر على حياته، مثل القرارات المتعلقة بمنح القروض، أو تسعير التأمين.

ت. حق المستهلك في طلب حذف بياناته، وهو ما يُعرف بـ"الحق في النسيان الرقمي" (Right to be Forgotten)[٣٢]، مما يمنع الشركات من الاحتفاظ بالبيانات لفتراتٍ غير مبررةٍ.

وقد تم تطبيق هذه اللائحة بصرامةٍ، حيث فُرضت غراماتٌ ضخمةٌ على شركاتٍ مثل جوجل (Google) وأمازون (Amazon) بسبب انتهاكها لقوانين الخصوصية الرقمية[٣٣].

٢- **قانون كاليفورنيا لحماية المستهلك (CCPA):** يهدف هذا القانون إلى منح المستهلكين في ولاية كاليفورنيا الحق في معرفة البيانات التي تجمعها الشركات عنهم، كما يمنحهم القدرة على منع بيع بياناتهم لأطرافٍ ثالثةٍ. ويُعد هذا القانون خطوةً رائدةً في الولايات المتحدة، إذ أنه:

أ. يُلزم الشركات بتوفير إشعارٍ واضحٍ للمستهلك حول كيفية استخدام بياناته.

ب. يمنح المستهلك الحق في رفض بيع بياناته الشخصية، مما يُحد من قدرة شركات الذكاء الاصطناعي على استغلال بيانات المستهلك لأغراضٍ تجاريةٍ بحتةٍ.

ت. يفرض عقوباتٍ صارمةً على الشركات التي تفشل في الامتثال لهذه القواعد، بما في ذلك فرض غراماتٍ تصل إلى ملايين الدولارات.

٣- مشروع قانون الذكاء الاصطناعي في الاتحاد الأوروبي (EU AI Act):

يُعد هذا القانون من أهم التشريعات المقترحة لتنظيم الذكاء الاصطناعي، حيث يُصنف أنظمة الذكاء الاصطناعي إلى أربع فئاتٍ وفقًا لمستوى المخاطر التي تشكلها على المستهلكين، ومن بين الضوابط التي يفرضها هذا القانون:

أ. حظر الأنظمة التي تنطوي على مخاطر عاليةٍ جدًا، مثل أنظمة المراقبة الجماعية، أو التلاعب السلوكي الذي قد يؤثر على قرارات المستهلكين.

ب. إلزام الشركات بإجراء تقييماتٍ للمخاطر قبل طرح أي منتجٍ أو خدمةٍ تعتمد على الذكاء الاصطناعي.

ث. فرض الشفافية في الخوارزميات، بحيث يكون للمستهلك الحق في معرفة كيفية اتخاذ القرارات التي تؤثر عليه، مثل أسعار التأمين، أو القروض، أو التوصيات التجارية.

الفرع الثاني: التشريعات الوطنية لحماية المستهلك من مخاطر الذكاء الاصطناعي

The Second Subsection: National legislation for protecting the consumer from the risks of artificial intelligence

إلى جانب القوانين الدولية، قامت العديد من الدول بإصدار تشريعاتٍ وطنيةٍ لحماية المستهلك من مخاطر الذكاء الاصطناعي، ومن أبرز هذه التشريعات:

أولاً: فرنسا: تفرض قوانين حماية المستهلك الفرنسية على شركات التجارة الإلكترونية توضيح كيفية عمل خوارزميات التسعير، وذلك لمنع استخدام الذكاء الاصطناعي في استغلال المستهلكين أو تقديم عروضٍ غير عادلةٍ لهم، ويمكن تتبع المشهد العام في فرنسا، من خلال ما يلي:

١. الإطار التشريعي الأوروبي وتأثيره في فرنسا: تلتزم فرنسا بتنفيذ قانون الذكاء الاصطناعي الأوروبي (EU AI Act)، الذي يضع قواعد صارمة على أنظمة الذكاء الاصطناعي عالية المخاطر، بما في ذلك الأنظمة المستخدمة في القطاعات الحساسة مثل الصحة، والتمويل، وهذا القانون يحظر الممارسات التي تشكل "خطراً غير مقبول"، مثل استخدام الذكاء الاصطناعي في التصنيف الاجتماعي للأفراد أو الاستغلال غير المشروع للبيانات البيومترية. تطبق فرنسا هذه

التشريعات من خلال سلطاتها الوطنية، وخاصة اللجنة الوطنية للمعلوماتية والحريات (CNIL)، التي تعمل على مراقبة الامتثال لهذا القانون .

٢. دور اللجنة الوطنية للمعلوماتية والحريات (CNIL): تعد CNIL الجهة التنظيمية الرئيسية المسؤولة عن تطبيق اللائحة العامة لحماية البيانات (GDPR) في فرنسا، وهي تتولى أيضاً ضمان توافق أنظمة الذكاء الاصطناعي مع متطلبات حماية البيانات الشخصية، ومن بين إجراءات CNIL[٣٤]:

أ. معاقبة الشركات التي تنتهك قوانين حماية البيانات عند استخدام الذكاء الاصطناعي، مثل فرض عقوبات على جمع الصور من الإنترنت بشكل غير قانوني لإنشاء قواعد بيانات التعرف على الوجه .

ب. إطلاق خطط إرشادية للشركات حول كيفية الامتثال لقوانين الذكاء الاصطناعي الجديدة، وتقديم استشارات بشأن استخدام تقنيات مثل تحليل البيانات الضخمة وتعلم الآلة .

ت. إجراء مشاورات عامة لمعرفة مخاوف المجتمع المدني والمطورين حول كيفية تطبيق هذه التشريعات عملياً.

٣. القيود المفروضة على برمجيات الذكاء الاصطناعي لحماية المستهلك: بموجب قانون الذكاء الاصطناعي الأوروبي، تفرض فرنسا قيوداً على استخدامات الذكاء الاصطناعي التي قد تؤثر سلباً على المستهلكين، مثل الحد من استخدام الذكاء الاصطناعي في تحديد الأسعار أو التمييز بين المستهلكين بطريقة غير عادلة، وكذلك تنظيم استخدام روبوتات الدردشة والأنظمة التلقائية في التعامل مع العملاء، مع فرض متطلبات إفصاح واضحة حول ما إذا كان المستهلك يتعامل مع نظام ذكاء اصطناعي أم إنسان. وأيضاً إلزام الشركات بتوفير شفافية في كيفية اتخاذ القرارات المؤتمتة، خاصة عند استخدام الذكاء الاصطناعي في القروض أو التوظيف أو التأمين.

٤. المبادرات المستقبلية لتعزيز حماية المستهلك في تعمل فرنسا على دمج "صناديق اختبار تنظيمية" (Regulatory Sandboxes) تتيح للشركات تجربة أنظمة ذكاء اصطناعي مبتكرة ضمن بيئة قانونية خاضعة للرقابة، مما يسمح للجهات التنظيمية بفهم المخاطر المحتملة والتعامل معها قبل الإطلاق التجاري. كما تشارك فرنسا في تطوير معايير موحدة أوروبياً لضمان الامتثال لقوانين الذكاء الاصطناعي في جميع الدول الأعضاء [٣٥].

إذاً، فإنَّ فرنسا تتبع نهجاً شاملاً لحماية المستهلك من مخاطر الذكاء الاصطناعي، من خلال مواءمة تشريعاتها مع القوانين الأوروبية، وتعزيز دور هيئات الرقابة مثل CNIL، وفرض قيود على الممارسات التي قد تضر

بالمستهلكين. هذه الجهود تضمن تطوير تقنيات ذكاء اصطناعي آمنة ومسؤولة، مع الحفاظ على حقوق الأفراد في الخصوصية والشفافية والعدالة الرقمية.

ثانياً: المملكة المتحدة: تتبع المملكة المتحدة نهجًا مرنًا وتدريجيًا في التعامل مع برمجيات الذكاء الاصطناعي وتأثيرها على المستهلك، حيث تعتمد على القوانين الحالية وتوجيهات تنظيمية بدلاً من فرض تشريع شامل على غرار الاتحاد الأوروبي. ويعتمد هذا النهج على تمكين الهيئات التنظيمية القائمة، مثل مكتب مفوض المعلومات (ICO) وهيئة المنافسة والأسواق (CMA)، لتطبيق القوانين ذات الصلة بحماية البيانات والخصوصية والممارسات التجارية العادلة .

١. دور الإرشادات التنظيمية في حماية المستهلك: في مارس ٢٠٢٣، أصدرت الحكومة البريطانية الكتاب الأبيض حول تنظيم الذكاء الاصطناعي، والذي شدد على أهمية حماية حقوق المستهلك عبر خمسة مبادئ أساسية: الأمان، الشفافية، الإنصاف، المساءلة، وقابلية الطعن، هذا يعني أن الشركات التي تقدم خدمات قائمة على الذكاء الاصطناعي مطالبة بضمان أن أنظمتها غير متحيزة وقابلة للمساءلة، خاصة عندما تُستخدم في قطاعات مثل القروض والتوظيف والتأمين[٣٦].

٢. الشفافية في اتخاذ القرار المؤتمت: من أبرز المخاوف بشأن برمجيات الذكاء الاصطناعي هو الغموض في طريقة اتخاذ القرارات، خاصة في أنظمة التوصيات والتسعير الديناميكي. لهذا السبب، تشدد هيئة المنافسة والأسواق (CMA) على ضرورة أن تكون الشركات واضحة بشأن كيفية عمل خوارزمياتها، بحيث يتمكن المستهلك من فهم سبب حصوله على عرض معين أو توصية محددة[٣٧] .

٣. حماية البيانات ومنع التمييز الخوارزمي: إنَّ القوانين البريطانية، بما في ذلك قانون حماية البيانات (٢٠١٨) ولوائح UK GDPR، تفرض على الشركات التي تستخدم الذكاء الاصطناعي في معالجة بيانات المستهلكين أن تضمن عدم إساءة استخدام البيانات الشخصية في أنظمة الذكاء الاصطناعي، ووجود آليات واضحة لطلب مراجعة بشرية للقرارات التي تؤثر على المستهلك بشكل جوهري، مثل قرارات القروض والائتمان، وإجراء تقييمات تأثير منتظمة لضمان أن الخوارزميات لا تميز ضد فئات معينة، كما حصل مع بعض أنظمة القروض التي أظهرت تحيزًا غير مقصود ضد النساء والأقليات العرقية .

ثالثاً: الصين: على النقيض من النهج البريطاني، تتبنى الصين نموذجًا أكثر صرامة وتدخّلًا مباشرًا في تنظيم الذكاء الاصطناعي، حيث ترى الدولة أن التكنولوجيا يجب أن تخضع لضوابط حكومية قوية لضمان عدم الإضرار بالمستهلكين والمجتمع. لذلك، أصدرت الصين قوانين ولوائح محددة تستهدف تنظيم استخدام برمجيات الذكاء الاصطناعي في الأسواق والخدمات الرقمية، ويمكن تتبع المشهد العام في الصين من خلال الآتي: .

١. **قانون تنظيم خوارزميات التوصية (٢٠٢٢)**: القانون الصيني الذي ينظم خوارزميات التوصية يُعرف باسم "اللوائح الإدارية لخدمات التوصية بالخوارزميات لخدمات معلومات الإنترنت"، تم إصدار هذه اللوائح من قبل إدارة الفضاء الإلكتروني الصينية (CAC) بالتعاون مع وزارة الصناعة وتكنولوجيا المعلومات ووزارة الأمن العام وهيئة تنظيم السوق، ودخلت حيز التنفيذ في ١ مارس ٢٠٢٢ [٣٨]. ومن أبرز أحكام القانون شفافية الخوارزميات وحق المستخدم في المعرفة، وهو يلزم القانون مزودي خدمات التوصية بالخوارزميات بالكشف عن الأساسيات التشغيلية للخوارزميات، وأهدافها، وآليات عملها، مما يمنح المستهلكين حق الاطلاع على كيفية تخصيص المحتوى أو المنتجات لهم، وكلك الحد من إساءة استخدام البيانات والتحكم في التلاعب بالسوق، ويُحظر استخدام الخوارزميات لإنشاء حسابات وهمية، أو التلاعب بتصنيفات البحث أو المحتوى، أو تنفيذ ممارسات احتكارية. كما يمنع "تمييز الأسعار" (Price Discrimination) بناءً على عادات المستهلكين، وهي ممارسة كانت تُستخدم لاستغلال المستخدمين عبر تسعير مخصص لكل فرد بناءً على تحليل بياناته، فضلاً حماية الفئات الضعيفة، مثل القاصرين وكبار السن والمستهلكين، ويمنع القانون استخدام الخوارزميات لإغراق القاصرين بمحتوى قد يؤدي إلى الإدمان الرقمي[٣٩]. كما يُلزم المنصات بتوفير أدوات تجعل الخدمات الرقمية أكثر سهولة لكبار السن، ويمنع التلاعب بالخوارزميات لتضليل المستهلكين بشأن الأسعار أو جودة المنتجات وكذلك يعمل على إلزام المنصات بالامتثال لآليات الرقابة الحكومية، إذ يجب على الشركات تسجيل خوارزميات التوصية الخاصة بها لدى الحكومة الصينية في غضون ١٠ أيام من بدء تشغيلها، كما أن السلطات لها الحق في التدخل وإجراء عمليات تدقيق لضمان الامتثال، القانون يمثل خطوة غير مسبوقة في تنظيم الذكاء الاصطناعي لحماية المستهلكين، حيث يمنحهم خيارات لإيقاف توصيات الخوارزميات، ويحد من ممارسات استغلال البيانات، كما يعزز من الشفافية والمساءلة في كيفية عرض المنتجات والخدمات على المنصات الرقمية، وإن هذه الخطوة الصينية تعد نموذجًا قد تلجأ إليه دول أخرى مستقبلاً لمواجهة تحديات الذكاء الاصطناعي في التجارة الرقمية[٤٠].

وعليه، فقد فرضت الصين لوائح تُلزم الشركات التي تستخدم أنظمة التوصيات المدعومة بالذكاء الاصطناعي بأن تضمن عدم استغلال الخوارزميات في التلاعب بسلوك المستهلكين أو دفعهم نحو قرارات غير واعية (مثل التسويق الخفي أو التسعير التمييزي)، مع إمكانية تعطيل التوصيات الآلية وإتاحة الفرصة للمستهلك لاختيار توصيات غير مخصصة، وحظر الخوارزميات التي تشجع على

الإدمان الرقمي، مثل الأنظمة المستخدمة في تطبيقات الفيديو القصير والتجارة الإلكترونية[٤١].

٢. **الرقابة على الذكاء الاصطناعي التوليدي (٢٠٢٣):** مع تصاعد استخدام نماذج الذكاء الاصطناعي التوليدي مثل ChatGPT، فرضت الصين قيودًا جديدة تُلزم مقدمي هذه الخدمات بـالتأكد من أن المحتوى المُنتج لا ينتهك القوانين المحلية أو يروج لمعلومات مضللة، وإخضاع البيانات المستخدمة في تدريب النماذج لمراجعة حكومية لمنع التحيزات والممارسات غير القانونية، وإلزام الشركات بتوفير آليات واضحة للمستهلكين للإبلاغ عن الأخطاء أو الانتهاكات [٤٢]. وكان ذلك وفقاً للائحة التي سميت باللائحة المؤقتة لإدارة خدمات الذكاء الاصطناعي التوليدي التي دخلت حيز التنفيذ في ١٥/ ٢٠٢٣/٨[٤٣].

رابعاً: العراق: منذ ظهور التقنيات الحديثة وتوسع استخدامها في شتى المجالات، أصبحت حماية المستهلك من تطبيقات الذكاء الاصطناعي قضية جوهرية تثير اهتمامًا متزايدًا في مختلف أنحاء العالم، بما في ذلك العراق، ورغم التقدم الذي شهدته العديد من الدول في هذا المجال، إلا أن العراق لا يزال في مرحلة الاستكشاف والتطوير فيما يتعلق بحماية مستهلكيه من مخاطر هذه التقنيات المتطورة، ويمكن القول إن هناك فجوة تشريعية واضحة لا تغطي بشكل شامل الأضرار التي قد تترتب عن استخدام برمجيات الذكاء الاصطناعي، مما يخلق تحديات قانونية تتطلب معالجتها بأسلوب قانوني دقيق ومرن[٤٤].

فقانون حماية المستهلك رقم ١ لسنة ٢٠١٠ يشكل الإطار الأساسي لحماية المستهلك في العراق، ولكن هذا القانون لا يتناول بشكل مباشر التحديات التي تطرأ من استخدام التقنيات الحديثة مثل الذكاء الاصطناعي، يتناول هذا القانون بشكل رئيسي حماية المستهلك من الممارسات التجارية الجائرة أو غير المشروعة، مثل الغش التجاري والتلاعب في الأسعار، لكنه لا يشير إلى الأضرار التي قد تنتج عن التطبيقات الذكية التي قد تؤثر على حقوق المستهلكين بشكل غير مباشر، كالتطبيقات التي تقوم بتخزين بيانات شخصية أو استخدام خوارزميات معقدة لاتخاذ قرارات قد تتسبب في أضرار للمستهلك[٤٥].

ورغم أن قانون حماية المستهلك العراقي يوفر بعض الحماية للأفراد في حالات الفشل في المنتجات والخدمات، فإنه يفتقر إلى آليات محددة للتعامل مع الأضرار الناجمة عن برمجيات الذكاء الاصطناعي، على سبيل المثال، لا توجد نصوص تحدد المسؤولية القانونية في حالة تعرض المستهلك لضرر نتيجة لاستخدام تطبيقات تعتمد على الذكاء الاصطناعي، مثل تلك التي تستخدم في التسويق الإلكتروني أو في تقديم خدمات الصحة الإلكترونية.

القرارات الحكومية والقضائية في العراق لا تركز بشكل خاص على مسألة الذكاء الاصطناعي، بل تقتصر على تطبيق النصوص العامة في قانون حماية المستهلك، في حالات نادرة، يمكن أم تطبق المحاكم المبادئ التقليدية لحماية المستهلك، ولكن بدون الاستناد إلى إطار قانوني خاص بالذكاء الاصطناعي، على سبيل المثال، في حالة حدوث ضرر بسبب تطبيق إلكتروني، قد يعتمد القضاء على مبادئ المسؤولية العقدية[٤٦] أو التقصيرية العامة، دون أخذ في الاعتبار الخصائص الفريدة لتقنيات الذكاء الاصطناعي، هذا يعني أن المستهلك العراقي قد لا يكون محميًا بالشكل المطلوب عند تعرضه للضرر الناتج عن خوارزميات معقدة أو أنظمة ذكية.

الحاجة الملحة لتطوير التشريعات تكمن في ضرورة وضع قوانين أكثر تخصصًا تتعامل مع التحديات المرتبطة باستخدام الذكاء الاصطناعي. فعلى سبيل المثال، لا بد من وجود نصوص قانونية تنظم العلاقة بين المطورين والمستهلكين عندما يتعلق الأمر بتقنيات الذكاء الاصطناعي، وتحديد من يتحمل المسؤولية عن الأضرار التي قد تنتج عن تطبيقاتها. يجب أن يتضمن هذا التعديل التشريعي تشريعات جديدة تحكم المسائل المتعلقة بالخصوصية، وتحدد آليات معتمدة للتعويض في حال تضرر المستهلكين جراء الاستخدام غير السليم لهذه الأنظمة[٤٧].

ختامًا، تظل حماية المستهلك من تقنيات الذكاء الاصطناعي في العراق مسألة مفتوحة تحتاج إلى مزيد من البحث والتطوير، يظل القائمون على وضع السياسات والتشريعات أمام تحدٍّ كبير يتمثل في تحديث القوانين لتواكب التطور التكنولوجي، وابتكار آليات قانونية توفر حماية فعالة للمستهلكين في ظل هذه التقنية الحديثة.

المطلب الثاني: المسؤولية القانونية للشركات المطورة لبرمجيات الذكاء الاصطناعي

The Second Requirement: The legal liability of companies providing artificial intelligence software

يُعدّ الذكاء الاصطناعي أحد أعظم الابتكارات التكنولوجية في العصر الحديث، حيث أحدث ثورة في مختلف المجالات، من التجارة الإلكترونية إلى الخدمات الصحية والمالية، ومع ذلك، فإن استخدامه المتزايد يثير تحديات قانونية معقدة، خاصة فيما يتعلق بالمسؤولية المدنية عن الأضرار التي قد تلحق بالمستهلك نتيجة الأخطاء أو العيوب البرمجية، وإزاء الطبيعة الذاتية والمتطورة لهذه الأنظمة، يثور التساؤل حول من يتحمل المسؤولية عند وقوع الضرر: هل هو المطوّر، أم المستخدم، أم النظام نفسه؟ وكيف يمكن ضبط العلاقة بين الأطراف المختلفة لضمان عدم الإضرار بالمستهلكين؟

وللإجابة عن هذه الإشكالات، يُقسم هذا المطلب إلى فرعين، يتناول الأول الأساس القانوني للمسؤولية المدنية الناشئة عن استخدام الذكاء الاصطناعي، بينما

يعالج الثاني الإشكاليات القانونية التي تواجه تطبيق هذه المسؤولية في ظل التطورات التقنية الحديثة.

الفرع الأول: الأساس القانوني للمسؤولية المدنية الناشئة عن برمجيات الذكاء الاصطناعي

The **First Subsection: The legal basis of civil liability arising from artificial intelligence software**

يستند تحديد المسؤولية المدنية الناشئة عن الأضرار التي تصيب المستهلك بسبب برمجيات الذكاء الاصطناعي إلى النظريات القانونية التقليدية، والتي تشمل المسؤولية التقصيرية والمسؤولية العقدية، إضافةً إلى بعض الاتجاهات الحديثة التي تميل إلى فرض مسؤولية موضوعية على الأطراف الفاعلة.

أولاً: المسؤولية التقصيرية (Liability in Tort Law): وفقًا للقواعد العامة في المسؤولية التقصيرية[٤٨]، يكون الفاعل مسؤولًا عن الأضرار التي تلحق بالغير إذا ثبت ارتكابه خطأً، وتسبب هذا الخطأ في وقوع الضرر، في سياق الذكاء الاصطناعي، يمكن أن يكون المطوّر أو المشغّل مسؤولًا عن الأضرار إذا ثبت أن هناك إهمالًا في تصميم البرمجية، أو عدم اتخاذ الاحتياطات الكافية لمنع حدوث الأضرار، مثلًا، إذا أدى خطأ في خوارزمية توصية المنتجات في منصة تجارة إلكترونية إلى توجيه المستهلكين نحو منتجات غير آمنة، فقد تتحمل الشركة المطوّرة المسؤولية وفقًا لهذه النظرية[٤٩].

ثانياً: المسؤولية العقدية (Contractual Liability): تنشأ المسؤولية العقدية عندما يكون هناك عقد بين المستهلك ومزوّد الخدمة الذي يستخدم الذكاء الاصطناعي[٥٠]، ويتم الإخلال بأحد الالتزامات المنصوص عليها في العقد. فإذا كانت شروط الخدمة تتضمن التزامًا بتقديم توصيات دقيقة أو تحليل طبي صحيح، لكن الذكاء الاصطناعي أخطأ في ذلك، فقد يكون لمزود الخدمة التزام تعاقدي بتعويض المستهلك عن الضرر الناتج عن الإخلال بهذه الالتزامات[٥١].

ثالثاً: المسؤولية الموضوعية (Strict Liability): في بعض التشريعات، خاصة في الاتحاد الأوروبي، يتم تبني مبدأ المسؤولية الموضوعية في حالات معينة، مما يعني تحميل المطوّرين أو الشركات المشغّلة المسؤولية حتى في غياب أي خطأ تقصيري أو تعاقدي، ويُطبق هذا النهج في الحالات التي يكون فيها المنتج المزوّد بالذكاء الاصطناعي خطيرًا بطبيعته أو يستخدم في أنظمة ذات حساسية عالية، مثل السيارات ذاتية القيادة أو الأنظمة الطبية الذكية[٥٢].

الفرع الثاني: التحديات القانونية في تطبيق المسؤولية المدنية على الذكاء الاصطناعي

The Second Subsection: The legal challenges in applying civil liability for artificial intelligence

بالرغم من أن المبادئ العامة للمسؤولية المدنية توفر إطارًا نظريًا لمعالجة الأضرار الناجمة عن برمجيات الذكاء الاصطناعي، فإن تطبيقها الفعلي يواجه

عدة تحديات نظرًا للطبيعة التقنية لهذه الأنظمة، ويستوي الأمر بالنسبة للضرر الذي يلحق المستهلك في البيئة الرقمية، ومن أبرز هذه التحديات ما يلي:

أولاً: تحديد الفاعل المسؤول (Attribution of Liability): يمكن بسهولة تحديد المسؤول عن الضرر، سواء كان شخصًا طبيعيًا أو معنويًا في ظل القوانين المدنية بالنسبة للمسؤولية المدنية التقليدية، لكن مع الذكاء الاصطناعي، تتوزع المسؤولية بين عدة أطراف، مثل الشركة المطوّرة، والمزوّد بالخدمة، والمستهلك، وفي بعض الحالات، قد يكون الضرر ناجمًا عن قرارات يتخذها النظام بشكل مستقل، مما يجعل من الصعب تحديد المسؤول الرئيسي فعلى سبيل المثال، إذا ارتكب نظام ذكاء اصطناعي معتمد في التوظيف تمييزًا غير قانوني ضد مرشحين معينين، فمن الذي يجب أن يُحاسب؟ الشركة التي استخدمت النظام، أم المطوّر، أم أن هناك حاجة لإنشاء إطار جديد لمساءلة النظام نفسه؟. وبمجرّد توافر تلك النظريات فإنّ المستهلك لا خوف عليه، فيجب تعويضه في جميع الأحوال، وهنا تتحقق الحماية المرجوة.

ثانياً: صعوبة إثبات العلاقة السببية (Causation Challenges): تتطلب المسؤولية المدنية إثبات وجود علاقة سببية بين الخطأ المرتكب والضرر الناتج عنه. ومع ذلك، فإن الذكاء الاصطناعي، خاصة في نماذجه التكيفية التي تتعلم من البيانات باستمرار، قد يتخذ قرارات لا يمكن التنبؤ بها أو تفسيرها بسهولة. وعليه، قد يكون إثبات أن الضرر كان نتيجة مباشرة لعيب في النظام الذكي أمرًا معقدًا، مما يضعف قدرة المستهلكين على المطالبة بالتعويضات[٥٣].

ثالثاً: المسؤولية عن التعلم الذاتي (Self-learning AI Liability): بعض أنظمة الذكاء الاصطناعي لا تظل ثابتة بعد إطلاقها، بل تتعلم وتتطور مع الوقت بناءً على المدخلات التي تتلقاها، وهذا يعني أن مطوّر النظام قد لا يكون على علم بكيفية تطوره في المستقبل، ما يثير تساؤلًا حول مدى إمكانية تحميله مسؤولية قرارات لم يكن يتوقعها أو يتحكم بها بشكل مباشر[٥٤].

رابعاً: محدودية الشفافية (Black Box Problem): تتمثل إحدى أكبر التحديات القانونية في أن بعض أنظمة الذكاء الاصطناعي، خاصة تلك المعتمدة على الشبكات العصبية العميقة، تعمل وفق خوارزميات معقدة تجعل تفسير قراراتها أمرًا صعبًا، وعليه، عندما يقع الضرر، قد لا يكون من الممكن تحديد سبب الخطأ، مما يعقّد مسألة تحميل المسؤولية القانونية لأي طرف معين[٥٥].

في ظل الانتشار المتزايد للذكاء الاصطناعي في الأسواق الاستهلاكية، أصبح من الضروري تطوير إطار قانوني أكثر وضوحًا ومرونة لتحديد المسؤولية المدنية عن الأضرار التي تلحق بالمستهلكين. وبينما توفر القواعد التقليدية بعض الحلول، إلا أن تعقيدات الذكاء الاصطناعي تتطلب إعادة التفكير في كيفية تطبيق

هذه القواعد بفعالية، من خلال وضع تشريعات جديدة تلزم الشركات بتحقيق الشفافية، وإنشاء آليات قانونية تضمن للمستهلكين الحماية الفعالة ضد الأخطاء والعيوب التقنية في الأنظمة الذكية.

الخاتمة

من خلال ما تم استعراضه من مفاهيم وأطر تشريعية، نجد أن حماية المستهلك من تطبيقات الذكاء الاصطناعي وبرمجياته أصبحت ضرورة ملحة في عصرنا الحديث، وإن التوسع السريع في استخدام هذه التقنيات قد أتاح العديد من الفرص، ولكنه في الوقت نفسه خلق تحديات قانونية وأخلاقية، تتعلق بتحديد المسؤولية عن الأضرار التي قد يتعرض لها المستهلك نتيجة لاستخدام هذه البرمجيات، فعلى الرغم من وجود بعض القوانين والتشريعات مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، إلا أن هذه التشريعات لا تزال تعاني من قصور في جوانب عدة تتعلق بالمسؤولية المدنية، وتحديد العلاقة السببية بين الأضرار الناتجة عن الذكاء الاصطناعي والضرر الفعلي الذي يصيب المستهلك. وأهم ما تمّ التوصل إليه ما يلي:

أولاً: النتائج: ويمكن بيانها كما يلي:

١. قصور التشريعات في مواجهة تطور الذكاء الاصطناعي، فبالرغم من الجهود الدولية في مجال حماية المستهلك، مثل تشريعات الاتحاد الأوروبي (GDPR)، إلا أن التشريعات الحالية لا تعالج بشكل كافٍ التحديات القانونية المرتبطة بتطبيقات الذكاء الاصطناعي، فتظل هناك ثغرات تتعلق بتحديد المسؤولية القانونية عن الأضرار الناتجة عن البرمجيات الذكية، مما يعيق تحقيق حماية فعّالة للمستهلكين في حال وقوع أضرار.

٢. تحديات في تحديد المسؤولية والشفافية، فمن أبرز النتائج التي برزت في هذا المجال هي صعوبة تحديد المسؤول عن الأضرار الناجمة عن الذكاء الاصطناعي، يُعزى هذا إلى غموض العلاقة بين النظام الذكي والمستهلك، وعدم وضوح المسئولية بين المطورين والمستخدمين والنظام نفسه، هذه التحديات تزداد تعقيدًا عندما يتعلق الأمر بتفسير الخوارزميات المعقدة التي تعتمد عليها هذه البرمجيات.

٣. ضرورة تطوير آليات تعويض فعّالة فمن خلال ما تم استعراضه، نجد أن أحد أبرز النتائج هو غياب آليات تعويض فعّالة وسريعة تتيح للمستهلكين الحصول على تعويضات عادلة عند حدوث الأضرار بسبب الذكاء الاصطناعي، وبالتالي، يتم التأكيد على الحاجة الماسة لتطوير نظم تعويض مبتكرة ومرنة تواكب تطور هذه التقنيات.

٤. أهمية الشفافية في تقنيات الذكاء الاصطناعي، يُعتبر غياب الشفافية في عمل الخوارزميات أحد التحديات الجوهرية التي تؤثر على قدرة المستهلكين على فهم وتفسير القرارات التي يتخذها النظام الذكي، وهنا مكمن الخطورة، فالتقنيات الحالية تفتقر إلى مستوى كافٍ من الشفافية، ما يعوق عمليات التقاضي ويزيد من صعوبة تحديد الأسباب والنتائج في الحالات القانونية المتعلقة بالأضرار.

ثانياً: المقترحات: ويمكن بيانها كما يلي:

١. وضع إطار تشريعي شامل فمن الضروري أن تقوم الحكومات بتطوير وتحديث التشريعات بشكل مستمر لمواكبة التطور السريع لتقنيات الذكاء الاصطناعي. يجب أن تشمل هذه التشريعات تحديد المسؤوليات القانونية بشكل واضح عند حدوث أضرار، مثل تحديد من يتحمل المسؤولية: الشركات المطورة للبرمجيات، المستخدمون، أو النظام نفسه، هذا سيساهم في توفير حماية قانونية أكثر وضوحًا وفعالية للمستهلكين، في الوقت الذي لم نجدّ فيه للعراق أية خطوات جادة في مجال حماية المستهلك من تطبيقات الذكاء الاصطناعي.

٢. تعزيز الشفافية إذ يجب على الشركات التي تطور برمجيات الذكاء الاصطناعي أن تضمن الشفافية في طريقة عمل الخوارزميات التي تعتمد عليها، فعلى سبيل المثال، يجب أن يتمكن المستهلكون من فهم كيف تتخذ الأنظمة الذكية قراراتها، ما يسهم في تسهيل عملية إثبات العلاقة السببية بين الأضرار التي تلحق بالمستهلك والقرارات التي اتخذها النظام.

٣. تطوير آليات فعّالة للتعويض إذ يجب أن تكون هناك آليات قانونية فعّالة تتيح للمستهلكين المتضررين الحصول على تعويض سريع وعادل عن الأضرار التي قد تلحق بهم نتيجة لاستخدام برمجيات الذكاء الاصطناعي، فيجب أن يتم ذلك بطريقة مرنة بحيث تكون القوانين قابلة للتكيف مع تطور هذه التكنولوجيا.

٤. تعزيز الرقابة والإشراف على البرمجيات إذ من الضروري أن تتوفر آليات رقابة دقيقة على تطبيقات الذكاء الاصطناعي من قبل الهيئات التنظيمية والرقابية على مستوى الدولة أو الاتحاد الأوروبي. هذه الرقابة يجب أن تشمل التأكد من أن هذه البرمجيات لا تسبب أضرارًا غير متوقعة للمستهلكين أو المجتمع بشكل عام.

٥. التوعية والتثقيف حيث يجب أن تتم توعية المستهلكين بكيفية استخدام هذه التقنيات بشكل آمن، مع توفير أدوات ومعلومات حول كيفية حماية بياناتهم الشخصية وحقوقهم في حالة حدوث أضرار نتيجة لتطبيقات الذكاء الاصطناعي.

مشروع قانون حماية البيانات الشخصية للمستهلك في ظل الذكاء الاصطناعي

المادة ١: تعريفات أساسية

١. **البيانات الشخصية**: جميع المعلومات التي تتعلق بشخص طبيعي أو معنوي يمكن تحديده بشكل مباشر أو غير مباشر، مثل الاسم، رقم الهوية، أو بيانات السلوك الإلكتروني مثل سجل التصفح في مواقع التواصل الاجتماعي أو مختلف التطبيقات الأخرى.

٢. **الذكاء الاصطناعي**: الأنظمة والتقنيات التي تستخدم الخوارزميات والمعالجة الآلية للبيانات لاتخاذ قرارات بشكل مستقل أو شبه مستقل عن التدخل البشري، بما في ذلك تطبيقات التوصية والمساعدات الذكية.

٣. **المستهلك**: أي فرد يستهلك الخدمات أو المنتجات الموفرة عبر الأنظمة الرقمية التي تعتمد على الذكاء الاصطناعي.

المادة ٢: جمع البيانات الشخصية:

١. يجب أن تتم عملية جمع البيانات الشخصية للمستهلكين بناءً على موافقة واضحة وموافقة مستنيرة، تُمنح من قبل المستهلك بحرية دون أي ضغط أو إكراه.

٢. يجب توضيح الأغراض التي سيتم من أجلها جمع البيانات للمستهلكين، ولا يجوز استخدام البيانات لأغراض غير تلك التي تم الإبلاغ عنها.

المادة ٣: حقوق المستهلك

١. الحق في الاطلاع: يحق للمستهلك الاطلاع على كافة البيانات التي تم جمعها عنه، مع تقديم توضيحات بشأن كيفية معالجتها واستخدامها.

٢. الحق في التصحيح: يحق للمستهلك تعديل البيانات غير الدقيقة أو غير الصحيحة.

٣. الحق في الحذف: يحق للمستهلك طلب حذف بياناته الشخصية في حال لم تكن هنالك مبررات قانونية أو تجارية تسمح بالاحتفاظ بها.

٤. الحق في النقل: يحق للمستهلك طلب نقل بياناته الشخصية إلى مزود خدمة آخر، بشرط أن يتم النقل بتنسيق منظم ومقروء آليًا.

٥. أية حقوق أخرى وردت في اتفاقيات دولية أنظم العراق إليها أو سينظم إليها في المستقبل.

المادة ٤: حماية البيانات

١. يجب على جميع الجهات التي تدير بيانات المستهلكين اتخاذ تدابير أمنية معقولة لحماية هذه البيانات من السرقة أو الوصول غير المصرح به.

٢. يجب على الشركات اتخاذ تدابير فنية وتنظيمية للحد من إمكانية استخدام الذكاء الاصطناعي في معالجة البيانات بطريقة تؤثر على خصوصية المستهلك أو تتسبب في أضرار.

المادة ٥: حقوق المستهلك في حالة الخرق

١. يجب على الشركات التي تستخدم الذكاء الاصطناعي إخطار المستهلك في غضون ٧٢ ساعة من اكتشاف أي خرق للأمن قد يهدد بياناته الشخصية.

٢. يُلزم المتحكم في البيانات بتقديم تعويضات للمستهلكين الذين تعرضوا لأضرار بسبب خرق للبيانات أو سوء استخدام لتقنيات الذكاء الاصطناعي.

المادة ٦: مراجعة التقنيات وتأثيرها على الخصوصية

١. يجب على الشركات إجراء تقييم دوري للمخاطر المتعلقة بمعالجة البيانات الشخصية باستخدام تقنيات الذكاء الاصطناعي، وذلك لضمان التوافق مع التشريعات المتعلقة بالخصوصية.

٢. يتم تقييم الأثر المحتمل لتقنيات الذكاء الاصطناعي على الخصوصية قبل استخدامها بشكل كامل، مع إمكانية تعديل أو إلغاء استخدامها إذا كان هناك تهديدات جادة لحقوق المستهلك.

المادة ٧: رقابة السلطات الوطنية

١. يتم إنشاء هيئة مستقلة تُعنى بحماية البيانات الشخصية للمستهلك، وتكون مسؤولة عن متابعة تطبيق هذا القانون، وتقوم بدور إشرافي على الشركات التي تقوم بجمع واستخدام بيانات المستهلكين، تتبع وزارة الداخلية بالتنسيق مع وزارة الاتصالات.

٢. للهيئة السلطة الكاملة لفرض غرامات مالية تصل إلى ٤% من الإيرادات السنوية للشركة في حالة المخالفات الجسيمة، بما في ذلك فشل الشركات في تطبيق التدابير اللازمة لحماية البيانات.

المادة ٨: التعاون الدولي

١. تشجع هذه المادة على التعاون بين الدول والمؤسسات الدولية لضمان حماية البيانات الشخصية عبر الحدود.

٢. يتم التعاون مع المنظمات الدولية مثل الاتحاد الأوروبي وأمريكا لضمان توافق القوانين الوطنية مع التشريعات العالمية مثل اللائحة العامة لحماية البيانات (GDPR).

المادة ٩: السريان والنفاذ

١. يسري هذا القانون على جميع الشركات التي تقوم بجمع ومعالجة البيانات الشخصية لمستهلكين.

٢. يبدأ نفاذ هذا القانون بعد مرور ستة أشهر من تاريخ نشره في الجريدة الرسمية، ويجب على الشركات التأكد من التزامها بجميع أحكامه خلال هذه الفترة.

٣. يُسمح للشركات بتقديم خطط إصلاح أو تعديل مستمر لعمليات جمع البيانات في حال تم اكتشاف أي ثغرات في النظام.

المادة ١٠: العقوبات

١. تُفرض غرامات مالية تصل إلى ٤% من إيرادات الشركة السنوية العالمية في حال حدوث خرق جسيم لأحكام هذا القانون.

٢. في حال التكرار أو تعدد المخالفات، يمكن فرض عقوبات أخرى مثل تعليق العمليات التجارية أو حظر مزاولة الأعمال لمدة معينة.

الأسباب الموجبة

بغية حماية حقوق المستهلكين في مواجهة التحديات المتزايدة التي تطرأ بسبب استخدام الذكاء الاصطناعي، ولتوفير حماية فعّالة لخصوصية البيانات ويحدد أطر المسؤولية القانونية في التعامل مع هذه البيانات، شُرِّع هذا القانون.

الهوامش

١. [١] يقصد بالذكاء الاصطناعي:" عبارة عن أنظمة وبرامج حاسوب تحاكي سلوك البشر وتصرفاتهم، وذلك لا يعني أن أي برامج حاسوبية تعمل من خلال خوارزمية معينة من أجل القيام بوظائف محددة تعدّ ذكاءً اصطناعياً، بل يلزم لكي نعدّ هذه البرامج ذكاء اصطناعياً أن تكون قادرة على التعلم وجمع البيانات، وكذلك تحليل هذه البيانات من أجل اتخاذ القرارات على أساس عملية التحليل". لاحظ: د. إيهاب خليفة، مجتمع ما بعد المعلومات (تأثير الثورة الصناعية الرابعة على الأمن القومي)، دار العربي للنشر والتوزيع، أبو ظبي، ٢٠١٣، ص٤٠.

2. [1] For more, see: Micah William Cho, the facebook- Cambridge analytica sandal: an analysis of care, a research paper submitted to the department of engineering and society, 2024, p. 1-12.

3. [1] Cadwalladr, C. & Graham-Harrison, E. (2018, March 17). Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook- influence-us-election. Davies, H. et. al. (2018, April 24). How Academic at Centre of Facebook Scandal Tried – and Failed – to Spin Personal Data into Gold. The Guardian. https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica- facebook-data-business-ventures

٤. [١] لاحظ اللائحة كاملة على الموقع الالكتروني: www.ec.europa.eu، شوهد في ٢٠٢٥/٢/٧.

5. [1] Thomas M. Georges, digital soul, 1st, basic books, 2004.

٦. [١] لاحظ في هذا المجال: د. خالد محمود غازي، الاخبار في عصر الآلة، ط١، وكالة الصحافة العربية، مصر، ٢٠٢٤، ص١٤٦.

٧. [١] لاحظ في مجال الدراسات الاقتصادية: د. أحمد سيد محمد علي الخطيب، تأثير تقنيات التسويق الرقمي المدعومة بالذكاء الاصطناعي في السلوك الشرائي دراسة ميدانية على عملاء المتاجر الالكترونية، بحث منشور في مجلة جامعة الصالحية الجديدة للعلوم الإدارية والاقتصادية، العدد (٢/١)، ص١٥٩-٢١٩.

٨. [١] لاحظ في تفاصيل الدعوى: www.curia.europa.eu ، شوهد في ٢٠٢٥/٢/٧.

٩. [١] محمود سلامة الشريف، تجريم التحيّز الخوارزمي (دراسة تاصيلية تحليلية مقارنة)، بحث منشور في مجلة جامعة الزيتونة الأردنية للدراسات القانونية، اصدار خاص، ٢٠٢٤، ص٨٤٢.

10. [1] Yadong Cui, blue book on AI and role of law in the world 2020, 1st, springer, china, 2022, P. 110.

١١. [١] لاحظ التقارير الرسمية الصادرة عن اليونسكو بهذا الصدد منها: www.unesco.org، شوهد في ٢٠٢٥/٢/٧. والذي بعنوان (الذكاء الاصطناعي التوليدي: دراسة لليونسكو تكشف أدلة مقلقة على وجود قوالب نمطية رجعية بشأن قضايا الجنسين).

12. [1] Josh Simons, algorithms for the people, 1st, Princeton university press, 2023, P. 72.

١٣. [١] حيدر صلاح كَاطع، العقارات الرقمية: إطار قانوني لتنظيم الأصول غير المادية في العالم الافتراضي (دراسة تحليلية)، بحث منشور في مجلة الكوفة، العدد (٦٢)، ٢٠٢٥، ص١٣٧١.

١٤. [١]لاحظ الموقع الالكتروني www.questionpro.com شوهد في ٢٠٢٥/٢/٧.

١٥. [١]لاحظ في هذا المجال: دليل نظام حماية البيانات الشخصية لجهات التحكم والمعالجة، الهيئة السعودية للبيانات والذكاء الاصطناعي، الإصدار الأول، ٢٠٢٣، ص٥ وما يليها.

١٦. [١] وهذا الرابط يتيح هذه الخدمة: www.support.splus.sa، شوهد في ٢٠٢٥/٧/٢. ولاحظ في هذا الموضوع: لوري آندروز، أعرف من أنت ورأيت ماذا فعلت مواقع التواصل الاجتماعي وفقدان الخصوصية، نقله الى العربية: شادي الرواشدة، ط١، العبيكان للنشر، ٢٠١٥، ص٢٣٤.

١٧. [١] لاحظ فيما يعرف بالأمن الرقمي الذي له مساحة واسعة في مجال بحثنا: د. لبنى عبد الحسين عيسى السعيدي، الامن القضائي والعدالة الرقمية (دراسة مقارنة)، بحث منشور في مجلة الحقوق، عدد خاص، ٢٠٢٣، ص٢٧٤ وما يليها.

١٨. [١]د. نوره عبد الهادي الدسوقي، الذكاء الاصطناعي في مواجهة الأخبار الزائفة، العربي للنشر والتوزيع، من دون مكان نشر، ٢٠٢٣، ص٣٨.

١٩. [١] لاحظ للاستزادة: د. محسن محمد الخباني، التنظيم القانوني للذكاء الاصطناعي، دار النهضة العربية، مصر، ٢٠٢٣.

٢٠. [١]لاحظ في هذا المجال: د. نجم عبد خلف العيساوي، حوكمة الذكاء الاصطناعي، ط١، دار اليازوري العلمية، عمان، ٢٠٢٥، ص١٥٦.

21. [1] Bartosz Brozek, Olia Kanevskaia, Przemyslaw Palka, Research handbook on law and technology, EE Elgar, UK, 2024, P. 440.

22. [1] Yuval Reinfeld, the European union as a normative power, 1st, permission of taylor & francis, new York, 2024 P.91.

23. [1]Matthias Artzt, Oliver Belitz, Simon Hembt, Nils LOLFING, international handbook of AI law, 1st, Kluwer law international B.V., USA, 2025, P. 10.

24. [1] Dimitris Gritzalis, kim-kwang Raymond Choo, Constantions patsakis, malware, handbook pf prevention and detection, 1st, springer, usa, 2024, P. 139.

٢٥. [١]راجع للمزيد: د. لبنى عبد الحسين عيسى، د. جليل حسن بشات، قانون الذكاء الاصطناعي، ترجمة لائحة الاتحاد الأوروبي الصادرة في ٢٠٢٤/١/٢٦، ط١، شركة المؤسسة الحديثة للكتاب، بيروت، ٢٠٢٥، ص١٣١.

٢٦. [١]لاحظ وبنفس هذه الفكرة: .

27. [1] Simona Demkova, automated decision-making and effective remedies, 1st, edward elgar publishing, UK, 2023, P. 30.

٢٨. [١] لاحظ في هذه الأفكار: د. أحمد عبد المجيد عبد العزيز منصور، الذكاء الاصطناعي والأمن القومي، دار التعليم الجامعي، مصر، ٢٠٢٤، ص١١٨ وما يليها.

٢٩. [١]تقرير منظمة التعاون الاقتصادي والتنمية OECD، توصية مجلس منظمة التعاون الاقتصادي والتنمية بشأن الذكاء الاصطناعي، ٢٠٢١، ص٦.

٣٠. [١] وهي اختصار لـ GENERAL DATA PROTECTION REGULATION، وهي مجموعة من القواعد التي وضعها الاتحاد الأوروبي لحماية حقوق جميع مواطني الاتحاد، وتمت الموافقة عليها في ٢٠١٦/٤/١٤، من قبل المفوضية الأوروبية، وطبقت اللائحة في مايو/ ٢٠١٨، وتمنح اللائحة حق للمستخدم في إزالة بياناته بشكل كلي أو جزئي، من شبكة الانترنت. لاحظ: د. يحيى إبراهيم دهشان، الحماية الجنائية للبيانات في ظل التحول الرقمي، نشر خاص، مصر، ٢٠١٨، ص٣١.

٣١. [١] راجع بالتفصيل:

32. Aurelia Tamo- Larrieux, designing of privacy its legal framework, 1st, springer publishing, Switzerland, 2018.

٣٣. [١] نشأ الحق في النسيان الرقمي – الذي يعد من الحقوق المستحدثة التي ظهرت نتيجة الثورة الرقمية والبيانات الضخمة- من خلال الحكم الصادر عن محكمة العدل التابعة للاتحاد الأوروبي في ١٣/ مايو/ ٢٠١٤ في قضية

google Spain، وأقرته لائحة GDPR في المادة ١٧ منها، والذي يعطي لصاحب البيانات الحق في إزالة بياناته. وأكدته بعض التشريعات مثل قانون المعلوماتية والحريات الفرنسي رقم ١٧-١٩٨٧، وقانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠. وللمزيد حول هذا الحق، لاحظ: د. مها رمضان محمد بطيخ، الإطار القانوني للحق في النسيان عبر شبكة الإنترنت (دراسة تحليلية مقارنة)، بحث منشور في مجلة الدراسات القانونية، العدد (٦١)، ج١، ٢٠٢٣، ص٢١٦-٣٦٢.

٣٤. [١] لاحظ في تفاصيل ذلك: www.arabic.cnn.com، شوهد في ٢٠٢٥/٢/٨.

35. [1] David Ramiro TRoitino, E- governancein the European union, 1st, springer, Estonia, 2024, P. 130.

36. [1] See S. Ranchordas, Experimental lawmaking in the EU: Regulatory sandboxes, 2021; J. Truby and others, A sandbox approach to regulating high-risk artificial intelligence applications, 2021; G. Leimüller and S. Wasserbacher- Schwarzer, Regulatory sandboxes – Analytical paper for Business Europe, April 2020; and F. Pop and L. Adomavicius, Sandboxes for responsible artificial intelligence, European Institute of Public Administration (EIPA), September 2021.

٣٧. [١] د. شريف حمدي، تطبيقات الذكاء الاصطناعي وتعزيز الميزة التنافسية لمنظمات الاعمال، ط١، العربي للنشر والتوزيع، مصر، ٢٠٢٣، ص١٣٨.

38. [1] Charles Kerrigan, artificial intelligence: law and regulation, 1st, EE Edward Elgar publishing, UK. 2022, P. 208.

39. [1]Diego Todaro, the usa of artificial intelligence in the public sector in shanghai, 1st, springer, Italy, 2024, P. 90.

40. [1] Ajay Agrawal, Joshua Gans, Avi Goldfrab, the economics of artificial intelligence 1st, the university of Chicago press, usa, 2019, , P.583.

41. [1] Klaus Mathis, law and economics of the digital transformation, 1st, springer, Switzerland, 2023, P.177.

٤٢. [١] لاحظ الموقع الالكتروني: www.oimedia.news، شوهد في ٢٠٢٥/٢/٨.

43. [1]David Ramiro Troitino, Tanel Kerikmae, Ondrej Hamulak, dijital development of the European union, 1st, springer, Estonia, 2023, P. 363.

44. [1] Arthur J. Oconnor, organizing of generative AI and the productivity revolution, 1st, springer, new York, 2024, P. 121.

٤٥. [١] لاحظ بهذا الصدد: نجم حبيب جبل عبد الله المشايخي، التنظيم الدستوري للحق في الخصوصية وضماناته القضائية (دراسة مقارنة)، ط١، المركز العربي للنشر والتوزيع، مصر، ٢٠٢٠، ص٣١٦.

٤٦. [١] وعلى الرغم من خلو قانون حماية المستهلك رقم ١ لسنة ٢٠١٠ من آلية لحماية المستهلك في ظل تطبيقات الذكاء الاصطناعي إلا أنّ البيانات الشخصية لم ترد ضمن الدستور العراقي لسنة ٢٠٠٥، مما يبرر عدم تشريع قانون فيها لغاية الآن، وهذا قصور تشريعي.

٤٧. [١]ويمكن قياس ما ورد في البحث التالي على حماية المستهلك: لاحظ: د. عامر غانم علوان، علا معن محمد حسن، أساس المسؤولية المدنية عن اضرار المركبات ذاتية القيادة في ظل قواعد المسؤولية التقليدية، بحث منشور في مجلة القادسية للقانون والعلوم السياسية، العدد (٢)، ج١، المجلد (١٥)، ٢٠٢٤، ص٤٩٧-٥٢٢.

٤٨. [١]وبهذا الصدد عقدت وزارة التخطيط العراقية ورشة عن حماية المعلومات الشخصية والمؤسساتية في الفضاء السيبراني جاء فيها:" عقدت وزارة التخطيط اليوم الثلاثاء، وبالتعاون مع وزارة الداخلية ورشة عمل عن حماية المعلومات الشخصية والمؤسساتية في الفضاء السيبراني . وهدفت الورشة إلى بيان أهمية خصوصية المُستخدمين وبياناتهم الشخصية، واهمية الحفاظ على المعلومات والبيانات الهامة للمستخدمين بشكل آمن ومأمون وسري،والتي تخضع لسياسة الخصوصية والقواعد العامة للتبادل عن طريق حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو السرقة، أو سوء الاستخدام ،أو التعديل أو الوصول غير المصرح به و ذات الصلة بجودة البيانات بعد التحقق من دقتها واكتمالها وتوقيتها . وتضمنت الورشة التي حاضرها العميد حسن هادي لذيذ مدير مركز الأمن السيبراني في وزارة الداخلية كيفية حماية مكوّنات الفضاء الإلكتروني ، بدءا من الشبكات والأنظمة إلى المواقع والبرامج والبيانات، وحماية المستخدمين، موضحا التحديات الأمنية التي تواجه الأصول المعلوماتية والتقنية للجهات، سواء كانت التهديدات ذات أصل داخلي أم خارجي . ولفت إلى أهمية رفع مستوى معايير الأمان الخاصة بهم والتحقق المستمر من سلامة أجهزتهم للمساهمة في بناء بيئة إلكترونية أكثر أمانًا. وكذلك اسباب الهجمات السيبرانية ، وماهي البرمجيات الضارة وطرائق انتشارها ، فضلا عن كيفية حماية المعلومات والبيانات رقميا. وفي ختام الورشة أوصى المحاضر بأهمية استمرار تنفيذ وتعزيز أدوات وسياسات الأمن السيبراني من قبل المستخدمين . وحضر الورشة السيد عباس عبدالكاظم محمد مدير عام دائرة تكنولوجيا

المعلومات وعدد من منتسبي دوائر الوزارة وتشكيلاتها اضافة الى عدد من ممثلي وزارة الداخلية". لاحظ الموقع الالكتروني: www.mop.gov.iq.

٤٩. [1] لاحظ في ذلك نصوص المسؤولية التقصيرية مثل ٢٠٤ من القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.

50. [1] Gabriel Hallevy, liability for crimes involving artificial intelligence system, 1st, springer, London, 2014, p. 10.

٥١. [1] لاحظ المادة ١٦٨ من القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.

52. [1] Martin EBERS, Susana Navas, algorithms and law, 1st, Cambridge university press, united kingdom, 2020, P. 12.

٥٣. [1] لاحظ في هذا الصدد: غزوان عبد الحميد شويش الجبوري، المسؤولية الموضوعية عن أضرار الروبوتات المبرمجة وفقاً لتكنولوجيا الذكاء الاصطناعي، أطروحة دكتوراه، جامعة تكريت/ كلية القانون، ٢٠٢٢.

54. [1]Jordi Vallverdu, causality for artificial intelligence, 1st, springer, spain, 2024, P. 53.

55. [1]Phillip Morgan, tort liability and autonomous systems accidents, 1st, EE, UK, 2023, P. 36.

56. [1]Parul Lchhpujani, sahil Thakur, artificial intelligence and ophthalmology, springer, india, 2021, P. 147.

المصادر

أولاً: الكتب:

I. د. أحمد عبد المجيد عبد العزبيز منصور، الذكاء الاصطناعي والأمن القومي، دار التعليم الجامعي، مصر، ٢٠٢٤.

II. د. إيهاب خليفة، مجتمع ما بعد المعلومات (تأثير الثورة الصناعية الرابعة على الأمن القومي)، دار العربي للنشر والتوزيع، أبو ظبي، ٢٠١٣.

III. د. خالد محمود غازي، الاخبار في عصر الآلة، ط١، وكالة الصحافة العربية، مصر، ٢٠٢٤.

IV. د. شريف حمدي، تطبيقات الذكاء الاصطناعي وتعزيز الميزة التنافسية لمنظمات الاعمال، ط١، العربي للنشر والتوزيع، مصر، ٢٠٢٣.

V. د. لبنى عبد الحسين عيسى، د. جليل حسن بشات، قانون الذكاء الاصطناعي، ترجمة لائحة الاتحاد الأوروبي الصادرة في ٢٠٢٤/١/٢٦، ط١، شركة المؤسسة الحديثة للكتاب، بيروت، ٢٠٢٥.

VI. د. محسن محمد الخباني، التنظيم القانوني للذكاء الاصطناعي، دار النهضة العربية، مصر، ٢٠٢٣.

VII. د. نجم عبد خلف العيساوي، حوكمة الذكاء الاصطناعي، ط١، دار اليازوري العلمية، عمان، ٢٠٢٥.

VIII. د. نوره عبد الهادي الدسوقي، الذكاء الاصطناعي في مواجهة الأخبار الزائفة، العربي للنشر والتوزيع، من دون مكان نشر، ٢٠٢٣.

IX. د. يحيى إبراهيم دهشان، الحماية الجنائية للبيانات في ظل التحول الرقمي، نشر خاص، مصر، ٢٠١٨.

X. لوري آندروز، أعرف من أنت ورأيت ماذا فعلت مواقع التواصل الاجتماعي وفقدان الخصوصية، نقله الى العربية: شادي الرواشدة، ط١، العبيكان للنشر، ٢٠١٥.

XI. نجم حبيب جبل عبد الله المشايخي، التنظيم الدستوري للحق في الخصوصية وضماناته القضائية (دراسة مقارنة)، ط١، المركز العربي للنشر والتوزيع، مصر، ٢٠٢٠.

ثانياً: البحوث:

I. د. أحمد سيد محمد علي الخطيب، تأثير تقنيات التسويق الرقمي المدعومة بالذكاء الاصطناعي في السلوك الشرائي دراسة ميدانية على عملاء المتاجر الالكترونية، بحث منشور في مجلة جامعة الصالحية الجديدة للعلوم الإدارية والاقتصادية، العدد (٢/١).

II. حيدر صلاح كَاطع، العقارات الرقمية: إطار قانوني لتنظيم الأصول غير المادية في العالم الافتراضي (دراسة تحليلية)، بحث منشور في مجلة الكوفة، العدد (٦٢)، ٢٠٢٥.
III. د. عامر غانم علوان، علا معن محمد حسن، أساس المسؤولية المدنية عن اضرار المركبات ذاتية القيادة في ظل قواعد المسؤولية التقليدية، بحث منشور في مجلة القادسية للقانون والعلوم السياسية، العدد (٢)، ج١، المجلد (١٥)، ٢٠٢٤.
IV. د. لبنى عبد الحسين عيسى السعيدي، الامن القضائي والعدالة الرقمية (دراسة مقارنة)، بحث منشور في مجلة الحقوق، عدد خاص، ٢٠٢٣.
V. د. مها رمضان محمد بطيخ، الإطار القانوني للحق في النسيان عبر شبكة الإنترنت (دراسة تحليلية مقارنة)، بحث منشور في مجلة الدراسات القانونية، العدد (٦١)، ج١، ٢٠٢٣.
VI. محمود سلامة الشريف، تجريم التحيّز الخوارزمي (دراسة تاصيلية تحليلية مقارنة)، بحث منشور في مجلة جامعة الزيتونة الأردنية للدراسات القانونية، اصدار خاص، ٢٠٢٤.

ثالثاً: الاطاريح:

I. غزوان عبد الحميد شويش الجبوري، المسؤولية الموضوعية عن أضرار الروبوتات المبرمجة وفقاً لتكنولوجيا الذكاء الاصطناعي، أطروحة دكتوراه، جامعة تكريت/ كلية القانون، ٢٠٢٢.

رابعاً: القوانين:

I. دستور جمهورية العراق لسنة ٢٠٠٥.
II. القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.
III. قانون المستهلك العراقي رقم ١ لسنة ٢٠١٠.
IV. قانون المعلوماتية والحريات الفرنسي رقم ١٧-١٩٨٧.
V. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.

خامساً: التقارير:

I. تقرير منظمة التعاون الاقتصادي والتنمية OECD، توصية مجلس منظمة التعاون الاقتصادي والتنمية بشأن الذكاء الاصطناعي، ٢٠٢١.
II. دليل نظام حماية البيانات الشخصية لجهات التحكم والمعالجة، الهيئة السعودية للبيانات والذكاء الاصطناعي، الإصدار الأول، ٢٠٢٣.

سادساً: المواقع الالكترونية:

I. الموقع الالكتروني: www.mop.gov.iq.
II. الموقع الالكتروني www.arabic.cnn.com.
III. الموقع الالكتروني: www.oimedia.news، شوهد في ٢٠٢٥/٢/٨.
IV. الموقع الالكتروني: www.support.splus.sa، شوهد في ٢٠٢٥/٧/٢.
V. الموقع الالكتروني www.questionpro.com شوهد في ٢٠٢٥/٢/٧.
VI. الموقع الالكتروني: www.unesco.org.
VII. الموقع الالكتروني: www.ec.europa.eu.، شوهد في ٢٠٢٥/٢/٧.
VIII. الموقع الالكتروني: www.curia.europa.eu ، شوهد في ٢٠٢٥/٢/٧.

سابعاً: المصادر الأجنبية:

I. Ajay Agrawal, Joshua Gans, Avi Goldfrab, the economics of artificial intelligence 1st, the university of Chicago press, usa, 2019.
II. Arthur J. Oconnor, organizing of generative AI and the productivity revolution, 1st, springer, new York, 2024.
III. Aurelia Tamo- Larrieux, designing of privacy its legal framework, 1st, springer publishing, Switzerland, 2018.
IV. Bartosz Brozek, Olia Kanevskaia, Przemyslaw Palka, Research handbook on law and technology, EE Elgar, UK, 2024.

V. Cadwalladr, C. & Graham-Harrison, E. (2018, March 17). Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook- influence-us-election.
VI. Charles Kerrigan, artificial intelligence: law and regulation, 1st, EE Edward Elgar publishing, UK. 202.٢
VII. David Ramiro TRoitino, E- governancein the European union, 1st, springer, Estonia, 2024.
VIII. David Ramiro Troitino, Tanel Kerikmae, Ondrej Hamulak, dijital development of the European union, 1st, springer, Estonia, 2023.
IX. Davies, H. et. al. (2018, April 24). How Academic at Centre of Facebook Scandal Tried – and Failed – to Spin Personal Data into Gold. The Guardian. https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica- facebook-data-business-ventures
X. Diego Todaro, the usa of artificial intelligence in the public sector in shanghai, 1st, springer, Italy, 2024.
XI. Dimitris Gritzalis, kim-kwang Raymond Choo, Constantions patsakis, malware, handbook pf prevention and detection, 1st, springer, usa, 2024.
XII. Gabriel Hallevy, liability for crimes involving artificial intelligence system, 1st, springer, London, 2014.
XIII. Jordi Vallverdu, causality for artificial intelligence, 1st, springer, spain, 2024.
XIV. Josh Simons, algorithms for the people, 1st, Princeton university press, 2023.
XV. Klaus Mathis, law and economics of the digital transformation, 1st, springer, Switzerland, 2023.
XVI. Martin EBERS, Susana Navas, algorithms and law, 1st, Cambridge university press, united kingdom, 2020.
XVII. Matthias Artzt, Oliver Belitz, Simon Hembt, Nils LOLFING, international handbook of AI law, 1st, Kluwer law international B.V., USA, 2025.
XVIII. Micah William Cho, the facebook- Cambridge analytica sandal: an analysis of care, a research paper submitted to the department of engineering and society, 2024.
XIX. Parul Lchhpujani, sahil Thakur, artificial intelligence and ophthalmology, springer, india, 2021.
XX. Phillip Morgan, tort liability and autonomous systems accidents, 1st, EE, UK, 2023.
XXI. S. Ranchordas, Experimental lawmaking in the EU: Regulatory sandboxes, 2021; J. Truby and others, A sandbox approach to regulating high-risk artificial intelligence applications, 2021; G. Leimüller and S. Wasserbacher-Schwarzer, Regulatory sandboxes – Analytical paper for Business Europe, April 2020; and F. Pop and L. Adomavicius, Sandboxes for responsible artificial intelligence, European Institute of Public Administration (EIPA), September 2021.
XXII. Simona Demkova, automated decision-making and effective remedies, 1st, edward elgar publishing, UK, 2023.
XXIII. Thomas M. Georges, digital soul, 1st, basic books, 2004.

XXIV. Yadong Cui, blue book on AI and role of law in the world 2020, 1st, springer, china, 2022.
XXV. Yuval Reinfeld, the European union as a normative power, 1st, permission of taylor & francis, new York, 2024 .