ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

The role of artificial intelligence in combating electronic financial fraud in banks

Lect. Zeina Mohammed Saadoun

College of Islamic Sciences, Tikrit University, Salahaddin, Iraq

zinah.m.saadoon@tu.edu.iq

Article info.

Article history:
- Received 1 May 2024
- Accepted 21 October 2024
-Available online 1 December 2024

Keywords:

- electronic banking
- electronic financial fraud
- the Central Bank of Iraq
- artificial intelligence.

Abstract: The study aimed to define the concept of electronic financial fraud in banks , and to clarify the relationship of electronic banks to electronic fraud, while explaining the role of artificial intelligence systems in reducing these operations in banks, by clarifying the aspects of the legislative confrontation in Iraq for this type of fraud and requiring banks to strengthen their electronic infrastructure. To confront such activities that have a negative impact on the state's public finances.

© 2023 TUJR, College of Law, Tikrit University

دور الذكاء الاصطناعي في مواجهة الاحتيال المالي الإلكتروني في المصارف

م. زينه محمد سعدون

كلية العلوم الاسلامية، جامعة تكريت، صلاح الدين، العراق

zinah.m.saadon@tu.edu.iq

معلومات البحث :

تواريخ البحث:
- الاستلام : ١/ آيار/ ٢٠٢٤
- القبول : ٢١ / تشرين الاول/ ٢٠٢٤
- النشر المباشر :١/ كانون الاول/٢٠٢٤

الكلمات المفتاحية :
- المصارف الالكترونية
- الاحتيال المالي الإلكتروني
- البنك المركزي العراقي
- الذكاء الاصطناعي.

الخلاصة: هدفت الدراسة لتحديد مفهوم الاحتيال المالي الإلكتروني في المصارف، وتوضيح علاقة المصارف الإلكترونية بالاحتيال الإلكتروني، مع بيان دور أنظمة الذكاء الاصطناعي في الحد من هذه العمليات في المصارف، وذلك من خلال توضيح جوانب المواجهة التشريعية في العراق لهذا النوع من الاحتيال وإلزام المصارف بتعزيز بنيتها التحتية الإلكترونية لمواجهة مثل هذه الأنشطة ذات الاثر السلبي على المالية العامة للدولة, بالاعتماد على أحدث التطبيقات التكنولوجية ومنها تطبيقات الذكاء الاصطناعي، وتوصلت الدراسة إلى مجموعة من النتائج أهمها أنه تعتبر تطبيقات الذكاء الاصطناعي أداة قوية في مواجهة و درء خطر الاحتيال المالي الإلكتروني في المصارف، لدور هذه التطبيقات في كشف عمليات الاحتيال، وتقدم دعم أمان إلكتروني لعملاء المصارف. وابرز التوصيات تمثلت بضرورة قيام المصارف والمؤسسات المالية والمصرفية العمل على تطوير قدراتها الإلكترونية واستخدام تطبيقات الذكاء الاصطناعي لتوفير بيانات وتحليلات حول سلوك العملاء وغيرهم الأمر الذي يساعد على الكشف عن الاحتيال و بالتالي اتخاذ قرارات أكثر دقة في مواجهة الاحتيال المالي الإلكتروني.

© ٢٠٢٣, كلية القانون، جامعة تكريت

المقدمة : شهد العالم في السنوات الأخيرة ارتفاعًا ملحوظًا في حالات الاحتيال المالي، والذي تجلى في تزايد معدلات الجرائم المالية والفساد والتضليل في السجلات المالية، وقد أدى هذا الوضع إلى حدوث انهيارات مالية في عدة منظمات بمختلف أحجامها وأنواعها، والذي رافقه زيادة في حالات الاحتيال بصورة ملحوظة، وتنوعت لتشمل الاحتيال الضريبي، والاحتيال في بطاقات الائتمان والاحتيال الإلكتروني، والاحتيال في الأوراق المالية، وقد شكلت هذه الأنواع تحديات جديدة للمنظمات في تأمين أموالها وضمان نزاهة العمليات المالية.

فمعظم الجرائم المرتكبة بوساطة الوسائل الإلكترونية تُعد من الجرائم الخفية حيث يقع العديد منها لصعوبة اكتشاف الفاعل ويبدو أن طبيعة هذه الجرائم تنطوي على قدر كبير من الخداع والاحتيال، وتتسم هذه الجرائم بالتعقيد المتزايد، الأمر الذي يعوق عملية الكشف عنها أو حتى ملاحقة مرتكبيها وعقابهم لقدرتهم لفائقة على إخفائها.

ويعد تبني المنظمات عامة و المصارف خاصة للتحول الرقمي في جميع أنشطتها وعملياتها أحد أبرز التحديات التي باتت تواجهها في حماية العمليات المصرفية ، الأمر الذي زاد من أهمية تطبيقها لتقنيات الذكاء الاصطناعي للتغلب على هذه التحديات، لما تحققه من فوائد متمثلة في توفير الوقت، والسرعة والدقة في تحليل البيانات والحصول على رؤى وتصورات أكثر وضوحاً بشأن الأنشطة والعمليات التي يقوم بها المصرف، من خلال ما تتصف به من قدرة على تقليد المهارات المعرفية البشرية في تفسير البيانات والتعلم والتكيف. خاصة وأنه في ظل التطور الهائل في مجال استخدام الوسائل الإلكترونية وشبكة المعلومات الدولية ينطوي في داخله مخاطر تفوق كافة التصورات في تهديدها للأمن المالي و الاقتصادي وتحميل بعض المؤسسات المالية خسائر مالية كبيرة.

ومع التقدم التكنولوجي، أصبحت تقنيات الذكاء الاصطناعي عاملا أساسيا يعتمد عليه في عمليات التدقيق المستمر، وخاصة في مجال الحد من الاحتيال المالي، ويتم ذلك من خلال فحص المعلومات والبيانات والأنشطة والمهام بشكل دوري ومستمر، مما يسهم في تقييم دقة وصحة البيانات المالية، وتتيح التقنيات الحديثة فرصًا متقدمة للتحليل الضوئي لكميات هائلة من البيانات بسرعة وكفاءة والقادرة على اكتشاف أنماط واتجاهات غير عادية يصعب اكتشافها بوسائل تقليدية، يتيح أيضا استخدام الذكاء الاصطناعي تحسين فعالية عمليات التدقيق وتعزيز القدرة على التعرف على أي نشاط مشبوه أو احتيال محتمل. ومن هنا جاءت هذه الدراسة لتوضيح دور الذكاء الاصطناعي في الحد من الاحتيال المالي في المصارف و المؤسسات المالية.

مشكلة الدراسة:

إن الاحتيال المالي الإلكتروني يعد من الموضوعات الحديثة التي فرضت نفسها بقوة على المستوى الوطني والدولي على حد سواء، والتي تطرح على المشرع القانوني ضرورة مواجهتها بترسانه قانونية حاسمة ورادعة لمكافحتها وعقاب مرتكبيها، لا سيما و انها تمس عصب سيادة الدولة (المال) لهذا تأتي إشكالية الدراسة على النحو التالي: هل وُفق المشرع العراقي في تطوير بيئته القانونية لمكافحة الاحتيال المالي الإلكتروني من خلال توظيف الذكاء الاصطناعي في المصارف وفق الأنظمة والتعليمات الصادرة من قبل

البنك المركزي للتحول الرقمي في الخدمات المصرفية؟. ويتفرع عن هذه الإشكالية عدة أسئلة فرعية سيتم الإجابة عنها في هذه الدراسة:

١. ما هو مفهوم الاحتيال المالي الإلكتروني في المصارف؟
٢. ما مدى أهمية دور أنظمة الذكاء الاصطناعي في الحد من عمليات الاحتيال المالي الإلكتروني في المصارف؟.

أهمية الدراسة:

يعد الاحتيال المالي الإلكتروني من القضايا الرئيسية للخدمات المالية عامة و المصارف خاصة، وقد ازداد الاهتمام بهذا النوع من الخطر مع ازدياد المعاملات المالية الإلكترونية، والتي نتج عنها تعدد وتنوع أشكال و طرق الاحتيال المالي وتفاقها سرعة انتشارها، فاستخدام التقنيات الحديثة في العمليات المصرفية عزز من فرص الاحتيال، وجعل بعض الأفراد يتلاعبون بأصول المصرف بطرق جديدة ومبتكرة، لهذا تتمثل أهمية الدراسة في توضيح كيف توظيف الذكاء الاصطناعي في الحد من هذه الجرائم.

منهج الدراسة:

ولمحاولة إثراء الموضوع من الزاوية التي يستحقها البحث سيتم الاعتماد على المناهج العلمية الآتية:

١. المنهج الوصفي: وذلك من خلال استعراض التشريعات والدراسات والبحوث التي تمت في مجال الاحتيال الإلكتروني بشكل عام ودور تقنيات الذكاء الاصطناعي في مواجهة الاحتيال المالي الالكتروني بشكل خاص وإنزالها على موضوع دراستنا.
٢. المنهج التحليلي: من خلال دراسة النصوص القانونية المتعلقة بجريمة الاحتيال الإلكتروني وتحليلها لبيان ما دلت عليه تلك النصوص وتحليل الدور الذي تلعبه تقنيات الذكاء الاصطناعي في الحد من هذه الجريمة في المصارف وفق التعليمات والأنظمة الصادرة من البنك المركزي في التحول الرقمي في الخدمات المصرفية في العراق.

المبحث الأول: ماهية جرائم الاحتيال المالي الإلكتروني في المصارف

إن عمليات الاحتيال الإلكتروني أو كما يطلق البعض عليها (الاحتيال المعلوماتي) هي من الجرائم المستحدثة، لذلك تعددت التعريفات التي تناولتها، وعليه سوف نبين تعريف جريمة الاحتيال في التشريع ومن ثم في الفقه والقضاء، وبيان محل هذه الجريمة في المصارف و الحسابات و العمليات المصرفية المالية لأنه يمكن أي يكون محلها معلومات ويمكن أن يون محلها نقود إلكترونية، وسيتم ذلك وفق الآتي:

المطلب الأول: التعريف بجرائم الاحتيال الإلكتروني

لم يورد المشرع العراقي تعريفاً خاصاً في قانون العقوبات لجريمة الاحتيال الإلكتروني شأنه في ذلك شأن أغلب التشريعات المقارنة، حتى لا يلزم نفيه بتعريفات قد تقيده أو تؤدي إلى عدم وجود المرونة في الأحكام القانونية، أما التعريف التشريعي لجريمة الاحتيال الإلكتروني في التشريعات المقارنة، فقد سارت أغلب التشريعات التي جرمت هذا النوع من الاحتيال بأن وضحته من خلال مرتكب الجريمة (المحتال) ومنها القانون الألماني[1] الذي أشار : "كل من يقوم بنية الحصول لنفسه أو لشخص ثالث على منفعة مادية غير مشروعة، بالإضرار بممتلكات الغير عن طريق التأثير في نتيجة المعالجة الآلية للبيانات من خلال برمجة غير صحيحة، أو استعمال بيانات غير صحيحة أو غير مكتملة، أو عن طريق الاستعمال غير المصرح به للبيانات، أو عن طريق التدخل غير المصرح به في عملية المعالجة ذاتها يعاقب...".

أما القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، المعتمد من قبل جامعة الدول العربية عام (٢٠٠٣)، فقد أورد وصفا لجريمة الاحتيال الإلكتروني والتي أطلق عليها تسمية جريمة الاحتيال عن طريق الشبكة المعلوماتية والحاسوب)، حيث أشار القانون المذكور[2]: "كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، إلى الاستيلاء لنفسه أو لغيره، على مال منقول أو على سند أو توقيع هذا السند، وذلك

---

[1]) المادة (٢٦٣) قانون العقوبات الألماني وله تعديلات كثيرة آخرها عام (١٩٩٤) ، ومتوفر على الموقع: www.iuscopm.org أشار له: د. موفق علي عبيد ماهية جريمة الاحتيال المعلوماتي، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، كلية القانون والعلوم السياسية، مجه، ع١٩، ص ٣٣٤ .

[2]) المادة (١٠) من القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية وأنظمة المعلومات وما في حكمها، متوفر على الموقع الإلكتروني: www.protectionproject.org/wp./١٢ . تم الدخول إلى الموقع بتاريخ : (٢٠٢٤/١٠/٢٣).

بالاستعانة بطريقة احتيالية أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب....".

قبل الدخول إلى التعريف الفقهي للاحتيال الإلكتروني، ارتأينا أن نتناول تعريف الاحتيال بصورته التقليدية كونه الأساس الذي انطلقت منه دراستنا، فالمستحدث فيها هو وسيلة الاحتيال على المجني عليه، وعليه فقد عرف الفقه الجنائي جريمة الاحتيال بمفهومها التقليدي على أنها "استيلاء على مال الغير باستعمال وسائل الخداع المؤدية إلى إيقاع المجني عليه في الغلط، ويؤدي إلى تسليمه ماله إلى الجاني"[1]. هذا هو تعريف جريمة الاحتيال بصورتها التقليدية، ولكن لا يختلف تعريف الاحتيال الإلكتروني عن تعريفه التقليدي من حيث الجوهر، حيث عرّفه البعض أنه "التلاعب بالبرامج والبيانات للتغيير منها بما يترتب عليه إيهام المجني عليه بصحتها بما يجعله يسلم بها".[2]

كما عرف أنه " التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات من أجل الحصول على ربح غير مشروع والحاق ضرر بالغير"[3]. ويتجه رأي آخر إلى تعريف الاحتيال الإلكتروني على أنه " إساءة استخدام الحاسبات الآلية والتلاعب في نظم المعالجة الإلكترونية للبيانات والمعلومات للحصول بغير حق على أموال أو أصول أو خدمات".[4]

أما بالنسبة للفقه العراقي فهناك من يعرف الاحتيال بوجه عام بأنها "الاستيلاء على شيء مملوك للغير بنية تملكه" وذلك بواسطة وسائل الاحتيال ولم يتطرق الاحتيال المعلوماتي[5]. ويبدو مما تقدم أن هذه التعريفات تشترك في بعض العناصر التي يتكون الاحتيال الإلكتروني منها وهي:[6]

---

1) علي عدنان ، الإجرام الإلكتروني: دراسة مقارنة، منشورات زين الحقوقية، بيروت، ص٢١١.

2) إياد حسين عباس ، جريمة الاحتيال في القانون العراقي، مطبعة عصام، بغداد، ص١٦٥.

3) جميل عبد الباقي ، الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية، القاهرة، ص٦٥.

4) ريهام محمود ، دور الذكاء الاصطناعي في تحسين أداء الخدمات المصرفية، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، عدد٣، مجلد٩، ص٦٧-٩٦.

١. الحصول على ربح غير مشروع وإلحاق خسارة بالمجني عليه عن طريق الاحتيال.

٢. استعمال الكومبيوتر للمساعدة على إتمام فعل الاحتيال.

وعلى ذلك، نجد أنَّ هذه التعريفات لا تتضمن العناصر كافة التي تميز الاحتيال الإلكتروني عن الاحتيال في صورته التقليدية، فالحصول على ربح مادي غير مشروع وإلحاق الخسارة بالمجني عليه من سمات الاحتيال بصفة عامة حتى مع إشارة هذه التعريفات إلى الدور المساعد للكومبيوتر على إتمام الجريمة إلا أنَّها لم توضح طبيعة هذا الدور ومدى أهميته كما أنَّها لم تشر إلى الطبيعة الخاصة للمال محل هذا الاحتيال.

كما يتبين لنا من التعريفات السابقة أن جوهر الاحتيال الإلكتروني هو التلاعب بالبيانات والمعلومات التي يحتويها نظام المعلومات والذي يشمل إدخال البيانات والمعلومات بشكل غير مصرح به حيث يتم الاحتيال بواسطة التلاعب بها، سواء في صورة إدخال بيانات غير صحيحة أو تعديل بيانات موجودة بالفعل، أو غير ذلك متى تم بصورة عمدية، بينما محل هذه الأفعال المادية والقصد المكونين هو القيم المادية التي تمثلها هذه المعلومات من أجل تحقيق ربح مادي غير مشروع لمصلحة الجاني أو لغيره، والذي قد يتحقق بشكل مباشر كتحويل الجاني مبلغ مالي لحسابه، أو بشكل غير مباشر كالتخلص من سداد مبلغ مالي عليه التزام أدائه.

لذا يتضح من خلال استقصاء التعريفات أنه لا يوجد تعريف جامع ومانع لعمليات الاحتيال المالي الإلكتروني يمكن الرجوع إليه، بناء على ما تقدم يمكن أن نعرف الاحتيال المالي الإلكتروني بأنه : كل من استخدم الشبكة المعلوماتية أو جهاز الحاسوب أو هاتف محمول أو ما في حكمهما، للاستيلاء على مال أو معلومات أو بيانات مصرفية أو برامج عن طريق خداع المجني عليه، ليتحصل على نفع غير مشروع لنفسه أو لغيره، أو إلحاق الضرر به.

وفيما يخص التعريف القضائي، فبعد البحث والاطلاع على الأحكام الصادرة من محكمة التمييز الاتحادية العراقية بصفتها الجزائية، والمتعلقة بجريمة الاحتيال الإلكتروني، وفي معرض ممارسة المحكمة دورها الرقابي على الأحكام القضائية الصادرة من محاكم الموضوع، نلاحظ بأن المحكمة وعلى الرغم من دورها القضائي المهم، إلا أنها لم تقوم بوضع تعريف خاصة للاحتيال الإلكتروني وذلك حسب اطلاع الباحث، ويرى الباحث أن موقف المحكمة له ما يبرره؛ حيث أن القضاء شأنه شأن التشريع

---

[5]) يونس عرب ، جرائم الكومبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث، أبو ظبي، ص٩.

[6]) المادتين ٢٥٦ و ٤٥٧ من قانون العقوبات العراقي.

يبتعد عن وضع تعريفات معينة، وذلك لتلافي حالة التقييد والجمود التي قد ترافق تعريف محدد لهذه الجريمة، وذلك لتعدد صور وأنماط ووسائل الاحتيال الإلكتروني.

المطلب الثاني: المصارف الإلكترونية و الاحتيال المالي الإلكتروني

شهدت السنوات الأخيرة تطوراً هائلاً في مجال الخدمات المصرفية الإلكترونية، مما سهل على الأفراد والشركات إجراء معاملاتهم المالية عبر الإنترنت. ومع ذلك، فإن هذا التطور فتح الباب أمام عمليات الاحتيال الإلكتروني التي تستهدف العملاء والمؤسسات المالية على حد سواء.

فمن أخطر الوسائل التكنولوجية الحديثة التي تعرف بنظام البنوك عبر الانترنت، وهي في الواقع ليست بنوكاً بالمعنى الشائع والمألوف، إذ أنها لا تقوم بقبول الودائع مثلاً، أو تقدم التسهيلات المصرفية أو غيرها من العمليات المصرفية المعتادة، لكنها عبارة عن وسيط في القيام ببعض العمليات المالية وعمليات البيع، حيث يقوم المتعامل مع. هذا النظام بإدخال الشفرة السرية من أرقام أو خلافه وطباعتها على الكومبيوتر ومن ثم يستطيع تحويل الأموال بالطريقة التي يأمر بها الجهاز.[1]

وواضح أن هذا المصرف يقدم خدمة ممتازة تتيح لغاسلي الأموال نقل أو تحويل كميات ضخمة من الأموال بسرعة وأمان، فهذه المصارف تعمل في محيط من السرية الشاملة إذ لا يكون المتعاملون فيها معروفي الهوية فضلاً عن أن هذه المصارف غير خاضعة لأي لوائح أو قوانين رقابية.[2]

وتمتاز هذه المصارف أيضاً بأنها تقدم خدمة بنكية في جميع الأوقات، وطوال أيام الأسبوع بلا انقطاع وذلك باستخدام الاتصال التليفوني عن طريق الانترنت حيث يقوم العميل من محل اقامته أو من سيارته أو من مكتبه بطلب رقم معين ويقوم جهاز خاص محمول عليه برنامج معلومات بالرد عليه، ويطلب منه ادخال – الرقم السري الذي سبق وأن أعطاه المصرف له، ثم يقوم هذا الجهاز بتحويل المكالمة إلى موظف يطلق عليه خادم العملاء يوجد داخل مركز الاتصال، وفي هذه اللحظة تظهر صورة العميل الحية على شاشة الكومبيوتر الموجود أمام الموظف، كما تظهر صفحة بها كل بيانات العميل.[3]

---

1) حسن يوسف ، جريمة غسيل الأموال بالطرق التقليدية وعبر شبكات الانترنت وبنوك الويب، مكتبة الملك فهد الوطنية، الرياض، ص٤٤.

2) خالد الحمادي ، غسيل الأموال في ضوء الاجرام المنظم أطروحة دكتوراه مقدمة إلى كلية الحقوق جامعة القاهرة غير منشورة، القاهرة، ص ١٠٠.

3) حسن يوسف يوسف ، مرجع سابق، ص٤٥.

ومن بين الجرائم المعلوماتية الأكثر خطورة وانتشارا جريمة الاحتيال المالي الإلكتروني، ولا يخفى أن هذه الجريمة أصبح لها أشكالا متنوعة ومدروسة تهدف جميعها إلى الاستيلاء على أموال وممتلكات الغير، وسنورد فيما يلي بعض أشكال الاحتيال المالي الإلكتروني في المصارف:

أولاً: التلاعب في المدخلات بهدف الاحتيال المالي إلكترونياً. تتمثل عمليات التلاعب في المدخلات من خلال تغذية الكومبيوتر ونظامه بالمعلومات والبيانات المراد معالجتها، ويمكن أن يكون الشخص المتلاعب حسن النية أو سيء النية كما في بعض الأحيان[1]. فقد يقوم أن يتضمن حدقاً لأي جزء منها، وذلك بنية الحصول على ربح غير مشروع من خلال تغيير معنى المعلومة لتصبح غير معبرة عن الحقيقة وبالتالي فإن ذلك يعد من الطرق الاحتيالية، كما يمكن أن يكون التلاعب بالبيانات من خلال حذف المعلومة كاملة، أو جزء منها لتغيير الحقيقة تمهيداً لإجراء عملية احتيال، وقد تتم إعاقة المعلومة عن أداء وظيفتها عن طريق الإضرار في سير في النظام المعلوماتي.[2]

ثانياً: التلاعب في البرامج تمهيداً للاحتيال المالي. يتمثل هذا الأسلوب في تغيير البرامج المطبقة بالفعل داخل المؤسسة المجني عليها وذلك بإدخال تعديلات غير مرخص بها على البرامج المستخدمة يمكن أن تتم عن طريق استخدام البرامج الخبيثة كالفايروسات.[3]

ثالثاً: استخدام شيفرة غير صحيحة للدخول إلى نظام مدفوع الأجر. بعد استعمال شيفرة غير صحيحة للدخول إلى نظام مدفوع الأجر من صور الاحتيال الإلكتروني إذ يمكن أن يتمكن الفاعل من الحصول على مكاسب مادية من خلال الحصول على الشيفرة فالمقصود هنا ليس أن تكون الشيفرة ذاتها، وإنما تستمد عدم صحتها من استخدامها من قبل شخص لا حق له في ذلك.[4]

رابعاً: التلاعب في البيانات التي يتم تحويلها عن بعد. إن التلاعب بواسطة وسائل الاتصالات أو التلاعب عن بعد هو الوسيلة الأكثر شيوعاً في عملية في الاحتيال المالي وخاصة لجهة التمويل الإلكتروني، ويمكن أن يتم من خلال انشاء مواقع وهمية خاصة بـ مشابهة للمواقع الأصلية للشركات والمؤسسات التجارية المتعاملة بالتسويق عبر الانترنت وغيرها من المواقع على شبكة الويب.

---

1) محمد أمين الشوابكة, اجرائم الحاسوب والإنترنت "الجريمة المعلوماتية"، ط١، دار الثقافة للتوزيع والنشر، عمان، الأردن، ص٢٢٣.

2) نائلة عادل فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ص٤٣٨.

3) احمد أمين الشوابكة، مرجع سابق، ص١٦٧.

4) نائلة عادل فريد، مرجع سابق، ص ٤٥٠.

يتم من خلال هذه المواقع الوهمية على شبكة الانترنت استقبال جميع المعاملات التجارية والمالية، ومن بينها البيانات والمعلومات الخاصة والسرية كالبيانات الخاصة ببطاقة الدفع الإلكتروني والرسائل الإلكترونية المتعلقة بالموقع الأصلي حيث يظهر الموقع الوهمي بمظهره ، ويستخدم أسلوب الخداع أكثر مما يستخدم في نطاق احتيال بطاقة الائتمان، إذ يتم من خلاله التقاط البيانات المتعلقة ببطاقات ائتمان المتعاقدين عبر الموقع الوهمي، مما يثير المشاكل القانونية ولاسيما إذا تم سحب رصيد العميل أو إجراء تحويلات إلكترونية لرصيده حول طبيعة التسليم الإلكتروني للنقود.[1]

وقد تتم عملية التلاعب بأشكال مختلفة، فقد تتم عن طريق الالتقاط الذهني للبيانات بالنظر أو الاستماع، وقد تتم عن طريق نسخ البيانات المخزنة إلكترونياً داخل الكومبيوتر سواء كانت مخزنة داخل نظام الكومبيوتر أم على وسائط التخزين الأخرى المتعارف عليها، وقد ترتكب عملية الاقتحام عن طريق اعتراض معطيات الكومبيوتر خلال عملية نقلها.

المبحث الثاني: دور أنظمة الذكاء الاصطناعي في الحد من جرائم الاحتيال الإلكتروني في المصارف

أدى التطور الحاصل في المجال التكنولوجي لعلوم الحاسوب وبرمجياته خلال السنوات الأخيرة الى ظهور العديد من التقنيات الحديثة والتي تحظى بالاهتمام في الوقت الحالي ومن بين هذه العلوم علم الذكاء الاصطناعي الذي يعتبر حصيلة تجارب وخبرات الانسان، حيث خرج من طور البحث الى الاستعمال وقد تبينت كفاءته في مجالات متعددة صناعية واقتصادية وخدمية، وذلك لأهمية الذكاء الاصطناعي في تحقيق الاهداف، الأمر الذي أدى الى ازدياد الاهتمام به من قبل الباحثين، ويتوقع أن يفتح الباب لابتكارات لا حدود لها، فهو تقنية تعمل على رفع قابلية العاملين والذي يمكن من تحقيق العديد من المزايا مثل عملية اتخاذ القرار التي تعتبر محور أساسي لضمان بقاء المنظمة (البنك) واستمراريتها ونموها .[2]

فالذكاء الاصطناعي ميدان واسع له استخدامات عدة من أبرزها تهيئة أجهزة الحواسيب لتؤدي المهام المعقدة والصعبة التي تعتمد على الذكاء الإنساني بسرع وقت وأقل جهد، وتوفير الدقة والكفاءة في الأداء، ويعد لغة للمحاكاة بين أجهزة الحاسوب وسلوكيات الإنسان الذكية في البنوك وغيرها من المؤسسات المالية والتجارية التي تهدف إلى ريادة الأعمال بمختلف

---

[1] (خالد حسن احمد ، الذكاء الاصطناعي وحمايته من الناحية المدنية والجنائية، دار الفكر الجامعي، الإسكندرية، ص٤٦٠

[2]) Ali, M., Abdullah, A. & khattab, G. (2022). The Effect of Activating Artificial Intelligence techniques on Enhancing Internal Auditing Activities: Field Study. Alexandria Journal of Accounting Research, 6(3), 1-40.

أشكالها[1]. ومن خلال هذا المبحث سنقوم بتوضيح الأساس التشريعي لاستخدام تطبيقات الذكاء الاصطناعي في حماية المصارف والعمليات المصرفية الإلكترونية، ونتعرف على مدى فاعلية تطبيقات الذكاء الاصطناعي في الحد من الاحتيال المالي الإلكتروني في المصارف، وذلك وفق الآتي:

المطلب الأول: المواجهة التشريعية للاحتيال الإلكتروني

أن السلوك الاحتيالي الإلكتروني ينطوي على اتخاذ مظاهر كاذبة تؤدي إلى وقوع المجني عليه في حالة من الغلط والتوهم مما يترتب عليه فقدانه المال أو منفعة أو ميزة[2]، لذا فإن وسيلة الخداع، هي السلوك الإجرامي الموجه إلى إيقاع المجني عليه في الغلط الدافع إلى التسليم، ومن هنا نرى أن التشريعات العقابية المقارنة، حددت على وجه الحصر هذه الوسائل[3]. فالمشرع العراقي[4]، حدد وسائل الخداع التي تقوم بها جريمة الاحتيال، بثلاث وسائل، وهي:

١. استعمال طرق احتيالية.
٢. اتخاذ اسم كاذب أو صفة غير صحيحة.
٣. تقرير أمر كاذب عن واقعة معينة.

وهناك وسيلة احتيال أخرى أضافتها المادة (٤٥٧) من قانون العقوبات العراقي، وهي وسيلة الاحتيال بطريق التصرف في مال منقول أو عقار.

وفي مجال التشريعات التي نظمت عمل المصارف في الميدان الإلكتروني، وانطلاقاً من الدور لرئيس للبنك المركزي العراقي في تنظيم القطاع المالي والمصري وتنميته وتطويره بمختلف نشاطاته الرقمية وعملياته التنقية والمعلوماتية ولمواجهة التأثيرات الناتجة عن المخاطر والتهديدات الإلكترونية ومنها عمليات الاحتيال الإلكتروني نجد أن البنك المركزي العراقي أصدر الكثير من الأنظمة والتعليمات والضوابط والإرشادات لحماية البنى التحتية التقنية والأنظمة المالية والمصرفية، لمواجهة المؤسسات المالية والمصرفية في

---

[1]) دولى، لخضر، و نفيسة ناصري , دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. مجلة المؤشر للدراسات الاقتصادية، مج٢, ع٢ ، ص٥٢ – ٦٧.

[2]) خالد ممدوح ابراهيم , الجرائم المعلوماتية، ط٢، دار الفكر الجامعي، الاسكندرية ص١٣٣.

[3]) انظر نص المادة (٤٥٦) من قانون العقوبات العراقي.

[4]) انظر نص المادة (٤٥٦) من قانون العقوبات العراقي.

مواجهة التحديات التقنية والتهديدات التقنية والتنبؤ بمخاطرها، واحتوائها، والتعافي منها لعمل البنوك في هذا الفضاء الإلكتروني، وخاصة لتنظيم عمل الخدمات المصرفية الإلكترونية ، ومن ذلك ما نص عليه نظام خدمات الدفع الإلكتروني لسنة ٢٠١٤ في العراق[1] ولذي عرف أمن المعلومات بأنه: "مجموعة من الاجراءات والتدابير والادوات الخاصة بحماية المعلومات واصولها وتضمن الحفاظ على سلامتها وسريتها وتوافرها ومتطلبات استخدامها والوصول اليها ، ويعد أمن البيانات والأمن السيبراني للوقاية من المخاطر الإلكترونية والاستجابة لها جزء من نطاق امن المعلومات".[2]

وحدد المشرع العراقي أهداف نظام الدفع الإلكتروني في المادة الثانية منه بتنظيم عملية الدفع الإلكتروني وحماية حقوق الأطراف بعمليات الدفع الإلكتروني وتهيئة أدوات مراقبة فاعلة لنشاطات خدمات الدفع الإلكتروني والتي يمكن من خلالها استخدام تطبيقات الذكاء الاصطناعي لتحقيق هذا المراقبة الفعلة لنشاطات خدمات الدفع الإلكتروني.

وأيضاً ما نصت عليه ضوابط عمل وكلاء مزودي خدمات الدفع الإلكتروني في العراق لسنة ٢٠٢٠ في (الفصل الثالث/ثانياً/إدارة المخاطر) ولمواجهة أي عمليات احتيال إلكتروني في عمليات الدفع الإلكتروني جاء فيها: "يجب على مزود خدمة الدفع أن يضمن وجود إطار عمل لحوكمة وإدارة المخاطر بما يتلاءم مع القوانين والتعليمات والضوابط الصادرة عن هذا البنك لضمان تقديم خدمات الوكيل بجاهزية تامة من خلال: أ- تطوير برنامج إدارة المخاطر لخدمات وكيل الدفع التي تعكس استراتيجية وسياسات خدماته. ..... ك- امتلاك أنظمة وكادر للمراقبة والسيطرة الكافية على العمليات والخدمات المقدمة من وكلائه على أساس مستمر".[3]

وهناك الكثير من النصوص التنظيمية لعمل المؤسسات المالية والمصرفية في لعراق لتنظيم عمليها في الفضاء الإلكتروني والتي يمكن من خلال استخدام تطبيقات الذكاء الاصطناعي لتحقيق هذه الرقابة الفاعلة لتقديم خدمات مصرفية إلكترونية آمنة ومنعاً من حدوث أي تحايل مالي إلكتروني فيها.

---

[1]) نظام خدمات الدفع الإلكتروني للأموال رقم (٢) لسنة ٢٠٢٤ المنشور في جريدة الوقائع الرسمية رقم (٤٧٧١) في ٢٩/٤/٢٠٢٤ الصادر بقرار مجلس الوزراء رقم (٢٤٢٧٦) لسنة ٢٠٢٤.

[2]) انظر المادة (٢) من نظام خدمات الدفع الإلكتروني للأموال رقم (٢) لسنة ٢٠٢٤.

[3])ضوابط عمل وكلاء مزودي خدمات الدفع الإلكتروني نسخة أيار لسنة ٢٠٢٠ البنك المركزي، دائرة المدفوعات صادرة بموجب ما جاء في الفصل الثامن من نظام خدمات الدفع الإلكتروني رقم ٣ لسنة ٢٠١٤

المطلب الثاني: إمكانية تطبيق الذكاء الاصطناعي لمواجهة عمليات الاحتيال الإلكتروني في المصارف

أن للذكاء الاصطناعي أهمية كبيرة في تعزيز كفاءة المصارف وزيادة تنوع الخدمات التي تقدمها، مما يعود بالفائدة على العملاء والمستثمرين والقطاع المصرفي بأكمله، فهو يساهم في تحسين تحليل البيانات واتخاذ القرار، وزيادة كفاءة العمليات وإدارة المخاطر، ومراقبة الأنشطة المالية والكشف عن أنماط غير طبيعية، وتحسين الخدمات المصرفية وتطويرها، وتوفير الوقت والجهد في ممارسة الأعمال الروتينية، وتوفير نظم حماية متطورة واستجابة سريعة للتهديدات الأمنية، بالإضافة إلى دعم البنوك في اكتشاف الفرص الجديدة والاتجاهات في السوق المالية وتوقع التغيرات في الاقتصاد.[1]

فهدف الذكاء الاصطناعي هو توليد المعرفة الجديدة وتفعيلها بشكل الكتروني بحيث يمكن استخدامها في صنع القرار وحل مشاكل الإدارة، ولا سيما المشكلات الاستراتيجية، وتخزين القواعد المنهجية بغية التواصل مع المعرفة المخزنة، ومعرفة التوظيف المثلى والخبرة العلمية والإجرائية مما يساعد البنوك على تحسين خدماتها وزيادة كفاءتها، وبالتالي زيادة قدرتها على التكيف مع التغيرات في البيئة المالية وضمان استدامتها.[2]

ويسعى الذكاء الاصطناعي للتصرف كما يتصرف الإنسان كالعقل البشري وهذا يتم من خلال البرامج المتطورة، حيث بإمكانه تعلم العديد من اللغات بكفاءة وسرعة عالية، بالإضافة إلى أداء مهام تعادل وتفوق الذكاء البشري، وتتمثل أهم الأساليب المتبعة في الذكاء في الاصطناعي والتي يمكن الاستفادة منها وتطبيقها في مجال العمل المصرفي والمالي الإلكتروني وتعمل على الحدّ من جرائم الاحتيال الإلكتروني نذكر منها:

أولاً: الجينات الخوارزمية، وهي إحدى تقنيات الذكاء الاصطناعي المستخدمة لإيجاد حل للمشكلة بطريقة فعالة وسريعة، فهي مبرمجة للعمل بالطريقة التي يحل بها الانسان المسائل، والخوارزميات الجينية تعتبر من أهم تطبيقات نظم الذكاء الاصطناعي في مجال انشطة الاعمال، وقد تم وصفها بالجينية نظرا لاعتمادها الشديد على محاكاة عمل الجينات الوراثية للتوصل للحل الامثل، حيث

---

[1]) دولى لخضر، و نفيسه ناصري، مرجع سابق، ص٥٢ – ٦٧.

[2]) علي أحمد ابراهيم , تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. المجلة القانونية، مج٩, ع٨ ، ص٢٨٠٩ – ٢٨٣٦.

تتنافس في الحلول مع بعضها البعض للوصول إلى الحل الأمثل والأفضل لمتخذي القرارات.[1] وتركز الخوارزميات على مجموعة من الخطوات الأساسية والمهمة لصياغة الحل والأفضل والأمثل لمسألة معينة، حيث تتميز الخوارزميات أنها تحتوي على خطوات متسلسلة ومترابطة، فلا يمكن تطبيق هذه الخوارزميات ما لم تطبق جميع الخطوات المتسلسلة، وإلا تفقد الخوارزميات قيمتها و فعاليتها وكفاءتها في إيجاد وتحسين الحل.[2]

ويتم تطبيق تقنية الجينات الخوارزمية في العديد من مجالات الذكاء الاصطناعي مثل (تصميم الأنظمة الحاسوبية والتحكم الآلي وتحسين جودة المنتجات وتحسين الخطط الاستراتيجية للمنظمات)، وبناء على ما سبق، ترى الباحثة أن الجينات الخوارزمية تمثل أداة قوية تمكن البنوك من تحسين أدائها وزيادة كفاءتها من خلال تقديم تحسينات مستمرة وزيادة قدرتها على التكيف مع التغيرات السريعة في السوق المالي والاقتصاد، فهي تسهم في تحسين إدارة المخاطر من خلال تحسين التنبؤ بالمخاطر المحتملة، وتحسين تقديرات الائتمان وعمليات اتخاذ القرار بشأن إدارة المخاطر المصرفية ومنها حمايتها من الاحتيال الإلكتروني، كما تسهم في تحسين عمليات التحليل الاستنتاجي والتنبؤ بتصرفات المجرمين المحترفين في الأسواق المالية الإلكترونية باستخدام البيانات الكبيرة، وتوفر إمكانية التحسين المستمر للعمليات والاستراتيجيات وتكييفها مع تغيرات سلوك المجرمين، وكل ذلك يوفر معلومات وقدرة للمؤسسات المالية والمصرفية في توفير معلومات لمواجهة جرائم الاحتيال الإلكتروني.

ثنياً: الوكلاء الاذكياء. وهو نظام يعتمد على قاعدة المعلومات والمعرفة المخزنة لديه حول عملية معينة أو شخص بهدف انجاز المهام التي تلبي الأهداف المرجوة واتخاذ القرارات وهي تطبيقات برمجية تعمل على مسك المهام الالكترونية مثل حالات الشراء والبيع حيث تعمل على تنبيه المستخدمين في حال حدوث أمر هام ومن الأمثلة على تطبيقات الوكيل الذكي البريد الالكتروني وبرامج الهاتف خلوي.[3]

---

[1] رانا مصباح عبدالمحسن , تأثير الذكاء الاصطناعي على الجريمة الإلكترونية. المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية، مج٢٢, ع١ ، ص٤٣٠ – ٤٣٧.

[2] A Complete History of Artificial Intelligence' (G), by Rebeca Reynoso, May Yo, Y. https://www.gt.com/articles/history-of-artificial-intelligence.

[3] David Marc ROTHENBERG. Can Siri 10.0 Buy your Home? The Legal and policy Based Implications of Artificial intelligence Robots Owning Real property, Washington Journal of Law, Technology and Arts, Vol. 11.

ويتميز الوكلاء الاذكياء بالقدرة على التعلم المستمر وتحسين أدائه بشكل تلقائي، وذلك يسبب الخوارزميات التي تستخدمها، كما تعتمد الوكالة الأذكى على المعلومات المتاحة لها وتحليلها لاتخاذ القرارات المناسبة في الوقت المناسب، كما تعتبر إحدى التقنيات الحاسوبية المتطورة التي تساعد على تحسين الأداء وتوفير الوقت والموارد في مختلف المجالات، وتحسين العمليات الإنتاجية وتنبؤ المستقبل.[1]

ثالثاً: الشبكات العصبية، وهي عبارة عن نظام معلومات ديناميكي يتم تشكيله وبرمجته في عملية التدريب والتعلم خلال فترة التطوير بأكملها، بمعنى آخر هي أنظمة تتعلم من التجربة وتكتسب الخبرة والمعرفة من خلال التدريب والتعلم العملي، وبالتالي فهي أحد العناصر الرئيسة للذكاء الاصطناعي تحاكي أسلوب العقل البشري في اتخاذ القرارات الذكية.[2]

وعلى ذلك فجميع هذه الوسائل في الذكاء الاصطناعي يمكن لها مساعدة المصارف و المؤسسات المالية في مواجهة عمليات الاحتيال المالي الإلكتروني فيها من خلال الكشف المبكر عن الأنشطة المشبوهة، من خلال تحليل سلوك العملاء بشكل مستمر، ومقارنته بأنماط الاستخدام المعتادة، ورصد أي انحراف عن هذه الأنماط الذي قد يشير إلى نشاط احتيالي محتمل، وأيضاً يساهم في تطوير استراتيجيات دفاعية أكثر فعالية لمواجهة الاحتيال المالي الإلكتروني من خلال التعرف على الأنماط المتكررة في عمليات الاحتيال.

---

[1] (طارق إبراهيم أحمد فياض(٢٠٢٠)، جرائم كيانات الذكاء الاصطناعي، الكتاب الأول، دار النهضة العربية، القاهرة، ص٥٥.

[2] (خالد حسن احمد، مرجع سابق، ص٤٦٠

الخاتمة

وفي خاتمة الدراسة نشير أن التحول الكبير الذي طرأ على الأعمال المالية والمصرفية في المصارف جعلها مسرحاً لجرائم الاحتيال المالي الإلكتروني، وجعل المعلومات المالية والأموال الإلكترونية محلاً لها، لذلك كان على المصارف تطوير بنيتها الإلكترونية واللجوء إلى أحدث التقنيات الإلكترونية لمواجهة والتكيف مع المخاطر الإلكترونية وبالأخص الجرائم المالية الإلكترونية، وتأسيساً على ما سبق توصلت الدراسة إلى مجموعة من النتائج والتوصيات والتي يمكن تناول أبرزها وفق التفصيل الآتي:

أولاً: النتائج

١. أصبحت ظاهرة الاحتيال المالي الإلكتروني تشكل ظاهرة على مستوى عالي من الخطورة والقلق على الأموال وانتشرت حالات الاختراق بشكل غير مسبوق خاصة في ظل التحول الكبير في عمل المصارف والاعتماد على التقنيات الإلكترونية الحديثة في إنجاز العمل المصرفي والمالي.
٢. تعتبر تطبيقات الذكاء الاصطناعي أداة قوية في مكافحة الاحتيال المالي الإلكتروني في المصارف، لدور هذه التطبيقات في كشف عمليات الاحتيال، وتقدم دعم أمان إلكتروني لعملاء المصارف.
٣. تمثل تطبيقات الذكاء الاصطناعي أداة قوية تمكن المصارف من تحسين أدائها وزيادة كفاءتها من خلال تقديم تحسينات مستمرة وزيادة قدرتها على التكيف مع التغيرات السريعة في السوق المالي والاقتصاد، فهي تسهم في تحسين إدارة المخاطر من خلال تحسين التنبؤ بالمخاطر المحتملة، وتحسين تقديرات الائتمان وعمليات اتخاذ القرار بشأن إدارة المخاطر المصرفية ومنها حمايتها من الاحتيال الإلكتروني.

ثانياً: التوصيات

١. على المصارف والمؤسسات المالية والمصرفية العمل على تطوير قدراتها الإلكترونية واستخدام تطبيقات الذكاء الاصطناعي لتوفير بيانات وتحليلات حول سلوك العملاء وغيرهم الأمر الذي يساعد على الكشف عن الاحتيال على اتخاذ قرارات أكثر دقة من المصرف في مواجهة الاحتيال المالي الإلكتروني.
٢. العمل على معالجة النقص التشريعي في العراق وإصدار قانون للجرائم الإلكترونية والنص فيه صراحة على تجريم الاحتيال الإلكتروني بكافة صوره، نظراً للحاجة الماسة إلى هذا القانون، لأن الجرائم الإلكترونية أصبحت شائعة وتشكل خطراً

كبيراً، وأن النصوص التقليدية قد لا تسعف لمواجهة جميع الجرائم الإلكترونية وخاصة جرائم الاحتيال المالي الإلكتروني التي تتعرض لها الخدمات المالية والمصرفية التي تقدمها المصارف.

٣. العمل على بث الوعي المجتمعي بالنشر في وسائل الإعلام والمناهج التعليمية في الجامعات والمدارس لبيان مخاطر الاحتيال المالي الإلكتروني، كون هذه الجريمة على تماس مباشر مع معظم الأوساط المجتمعية.

٤. إلزام المؤسسات المالية والمصرفية نظراً لأهميتها وأهمية ما تقدمه من خدمات مالية تمس كافة المواطنين إلى توظيف وتطوير التطبيقات الحديثة للذكاء الاصطناعي التي يمكن من خلالها مواجهة عمليات الاحتيال المالي الإلكتروني التي ترتكب عبر الأنظمة والمواقع والمحافظ المالية وغيرها من الخدمات المصرفية والمالية الإلكترونية التي تقدمها المصارف.

قائمة المراجع

أولاً: المراجع العربية

- خالد ممدوح ابراهيم (٢٠١٩)، الجرائم المعلوماتية، ط٢، دار الفكر الجامعي، الاسكندرية, ٢٠١٩ .
- علي أحمد. ابراهيم . تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. المجلة القانونية، مج٩, ع٨, ٢٠٢١.
- خالد الحمادي ، غسيل الأموال في ضوء الاجرام المنظم أطروحة دكتوراه مقدمة إلى كلية الحقوق جامعة القاهرة غير منشورة، القاهرة, ٢٠١٥.
- نفيسة ناصري و دولي الخضر , دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. مجلة المؤشر للدراسات الاقتصادية، مج٢, ع٢, ٢٠١٨ .
- ريهام محمود دياب، دور الذكاء الاصطناعي في تحسين أداء الخدمات المصرفية، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، عدد٣، مجلد٩ , ٢٠٢٢.
- محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت "الجريمة المعلوماتية"، ط١، دار الثقافة للتوزيع والنشر، عمان، الأردن, ٢٠٠٧.
- جميل عبد الباقي الصغير ، الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية، القاهرة, ١٩٩٢.
- طارق إبراهيم أحمد فياض , جرائم كيانات الذكاء الاصطناعي، الكتاب الأول، دار النهضة العربية، القاهرة, ٢٠٢٠.
- رانا مصباح عبدالمحسن , تأثير الذكاء الاصطناعي على الجريمة الإلكترونية. المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية، مج٢٢, ع١, ٢٠٢١.
- موفق علي عبيد ماهية جريمة الاحتيال المعلوماتي، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، كلية القانون والعلوم السياسية، مجه، ع١٩, ٢٠١٦.
- يونس عرب ، جرائم الكومبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث، أبو ظبي, ٢٠٠٢.
- إياد حسين عباس العزاوي ، جريمة الاحتيال في القانون العراقي، مطبعة عصام، بغداد ١٩٩٨.

- علي عدنان الفيل ، الإجرام الإلكتروني: دراسة مقارنة، منشورات زين الحقوقية، بيروت, ٢٠١٩.
- نائلة عادل فريد قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت, ٢٠٠٥.
- خالد حسن احمد لطفي ، الذكاء الاصطناعي وحمايته من الناحية المدنية والجنائية، دار الفكر الجامعي، الإسكندرية,٢٠٢١.
- حسن يوسف ، جريمة غسيل الأموال بالطرق التقليدية وعبر شبكات الانترنت وبنوك الويب، مكتبة الملك فهد الوطنية، الرياض, ٢٠١١.

ثانياً: المراجع الأجنبية

- A Complete History of Artificial Intelligence' (G), by Rebeca Reynoso, May Yo, Y. https://www.gt.com/articles/history-of-artificial-intelligence.
- Ali, M., Abdullah, A. & khattab, G. (2022). The Effect of Activating Artificial Intelligence techniques on Enhancing Internal Auditing Activities: Field Study. Alexandria Journal of Accounting Research, 6(3), 1-40.
- David Marc ROTHENBERG. Can Siri 10.0 Buy your Home? The Legal and policy Based Implications of Artificial intelligence Robots Owning Real property, Washington Journal of Law, Technology and Arts, Vol. 11.

ثالثاً: القوانين والأنظمة والتعليمات

- ضوابط عمل وكلاء مزودي خدمات الدفع الإلكتروني نسخة أيار لسنة ٢٠٢٠ البنك المركزي، دائرة المدفوعات صادرة بموجب ما جاء في الفصل الثامن من نظام خدمات الدفع الإلكتروني رقم ٣ لسنة ٢٠١٤
- القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية وأنظمة المعلومات وما في حكمها، متوفر على الموقع الإلكتروني: www.protectionproject.org/wp./١٢ . تم الدخول إلى الموقع بتاريخ : (٢٠٢٤/١٠/٢٣).
- قانون العقوبات الألماني وله تعديلات كثيرة آخرها عام (١٩٩٤) ، ومتوفر على الموقع: www.iuscopm.org .

- قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.
- نظام خدمات الدفع الإلكتروني للأموال رقم (٢) لسنة ٢٠٢٤ المنشور في جريدة الوقائع الرسمية رقم (٤٧٧١) في ٢٩/٤/٢٠٢٤ الصادر بقرار مجلس الوزراء رقم (٢٤٢٧٦) لسنة ٢٠٢٤.
- نظام خدمات الدفع الإلكتروني للأموال رقم (٢) لسنة ٢٠٢٤.

First: Arabic references

●Khaled Mamdouh Ibrahim (2019), Cybercrimes, 2nd ed., Dar Al Fikr Al Jami, Alexandria, 2019.

●Ali Ahmed. Ibrahim. Applications of artificial intelligence in confronting cybercrimes. Legal Journal, Vol. 9, No. 8, 2021.

●Khaled Al Hammadi, Money laundering in light of organized crime, unpublished doctoral thesis submitted to the Faculty of Law, Cairo University, Cairo, 2015.

●Nafisa Nasseri and Doli Al Khedr, The role of artificial intelligence in confronting cybercrimes. Al Moasher Journal for Economic Studies, Vol. 2, No. 2, 2018.

●Reham Mahmoud Diab, The Role of Artificial Intelligence in Improving the Performance of Banking Services, Arab Journal of Informatics and Information Security, Arab Organization for Education, Science and Arts, Issue 3, Volume 9, 2022.

●Muhammad Amin Al-Shawabkeh, Computer and Internet Crimes "Information Crime", 1st ed., Dar Al-Thaqafa for Distribution and Publishing, Amman, Jordan, 2007.

●Jamil Abdel-Baqi Al-Sagheer, Criminal and Civil Protection of Magnetic Credit Cards, an Applied Study in French and Egyptian Judiciary, Dar Al-Nahda Al-Arabiya, Cairo, 1992.

●Tariq Ibrahim Ahmed Fayyad, Crimes of Artificial Intelligence Entities, Book One, Dar Al-Nahda Al-Arabiya, Cairo, 2020.

●Rana Misbah Abdul Mohsen, The Impact of Artificial Intelligence on Cybercrime. King Faisal University Scientific Journal - Humanities and Administrative Sciences, Vol. 22, No. 1, 2021.

●Muwaffaq Ali Obaid, The Nature of the Crime of Information Fraud, Journal of the College of Law for Legal and Political Sciences, University of Kirkuk, College of Law and Political Science, Vol. 19, 2016.

●Younis Arab, Computer and Internet Crimes, a working paper presented to the Arab Security Conference, Arab Center for Studies and Research, Abu Dhabi, 2002.

●Iyad Hussein Abbas Al-Azzawi, The Crime of Fraud in Iraqi Law, Issam Press, Baghdad 1998.

●Ali Adnan Al-Feel, Electronic Crime: A Comparative Study, Zain Legal Publications, Beirut, 2019.

●Naila Adel Farid Qura, Economic Computer Crimes, Al-Halabi Legal Publications, Beirut, 2005.

●Khaled Hassan Ahmed Lotfi, Artificial Intelligence and Its Protection from the Civil and Criminal Perspective, Dar Al-Fikr Al-Jami'i, Alexandria, 2021.

●Hassan Youssef, The Crime of Money Laundering Using Traditional Methods and Through the Internet and Web Banks, King Fahd National Library, Riyadh, 2011.