

المواجهة القانونية لجرائم الاحتيال الإلكتروني في عصر الذكاء الاصطناعي Legal Confrontation of Cyber-Fraud Crimes in the Era of Artificial Intelligence

نور الهدى محمودي أستاذ محاضراً⁽¹⁾

مخبر البحوث القانونية السياسية والشرعية

⁽¹⁾ جامعة عباس لغرور خنشلة (الجزائر)

mahmoudi.nourelhouda@univ-khenchela.dz

تاريخ النشر:

2026/10/31

تاريخ القبول:

2026/09/14

تاريخ الارسال:

2026/04/25

الملخص:

ان التطور المتسارع لوسائل التواصل الاجتماعي والمنصات الرقمية المختلفة أفرز أنماطا إجرامية مستحدثة، بلغت ذروتها مع دمج تقنيات الذكاء الاصطناعي. حيث يعمد الجاني إلى استغلال تكنولوجيا الاتصال المعاصرة لارتكاب سلوكيات تدليسية تندرج تحت مفهوم 'الاحتيال الإلكتروني'، وتكمن خطورة هذا السلوك الإجرامي في تداعياته الاقتصادية والاجتماعية الوخيمة، وما يترتب عليه من زعزعة للاستقرار والثقة في المعاملات الرقمية، الأمر الذي يضع السياسة الجنائية المعاصرة أمام تحدٍّ تشريعي وإجرائي مزدوج؛ يتطلب إرساء آليات استباقية قادرة على كبح التطور التكنولوجي للجريمة، وسد الفراغ التشريعي الناجم عن غياب النصوص الصريحة لضبط إساءة استخدام تقنيات الذكاء الاصطناعي.

الكلمات المفتاحية:

-الاحتيال الإلكتروني -الذكاء الاصطناعي -المنصات الرقمية -المواجهة القانونية -طبيعة الجريمة -الآليات التشريعية.

Abstract:

The crime of fraud has evolved significantly in the methods of unlawfully obtaining and misappropriating funds through various digital means and platforms, particularly social media. The fraudster uses digital communication tools to commit modern fraud, commonly

المؤلف المرسل: نور الهدى محمودي

referred to as cyber fraud. This crime is considered to be one of the most serious crimes, resulting in significant financial losses for the victims .

This study aims to make people aware of the dangers of this crime and to warn them against responding to these fraudulent messages. It emphasises the need to be vigilant and to check the credibility of the company they are dealing with before taking any action that could lead to financial loss. While this crime may be familiar to many in the context of digital transformation, its concept and implications for individuals and society remain largely unknown due to the lack of explicit legal texts at both local and international levels .

Key words:

Cyber-Fraud - Artificial Intelligence - Digital Platforms -Legal Confrontation - Implications of the Crime -Legislative Mechanisms

مقدمة:

تعددت وتباينت أنماط الجرائم المستحدثة مواكبة لتعدد مجالات الحياة المختلفة، ومن أهمها تلك الجرائم المرتبطة بالثورة التكنولوجية والرقمية عامة والالكترونية خاصة، التي أدت بدورها الى ظهور سلوكيات تمس الأمن الرقمي، وهو مصطلح أخذ في التوسع لدرجة قد أصبح محرما في كثير من الدول وتعاقب عليه الحكومات للحد من تفشيه في المجتمع، ومن بين أهم الجرائم المستحدثة التي عرفتها المجتمعات الحالية، وهي جريمة عصرية تهدد الأمن الرقمي وتشكل تهديدا حقيقيا في عصرنا الحالي وهي جريمة الاحتيال الالكتروني.

انتشرت ظاهرة الاحتيال الالكتروني مع التطور الذي شهده العالم في مجال الوسائل التقنية والمعلوماتية، ومع زيادة أعداد المستخدمين لمواقع التواصل الاجتماعي المختلفة والاستعانة بخدمات الذكاء الاصطناعي، وهو ما ساعد على استفحال وتفشي هذه الظاهرة والتي تأثرت بها الدول المتقدمة وحتى الدول النامية، فأصبحت ظاهرة عالمية. فبعد أن كان الاحتيال التقليدي يقوم على استخدام المحتال أساليب تسويقية أو خداعية لإقناع الأفراد أو الشركات بأنهم سيحصلون على شيء ذي قيمة معينة ليتم

استغلالهم أو سرقتهم، فالיום أصبح الفضاء الأزرق ملاذهم لتحصيل الأموال والحصول على البيانات الشخصية التي تنتهك خصوصية الأفراد دون جهد أو عناء ودون الإفصاح عن الهوية الحقيقية للمجرم المحتال، ونتيجة تطور الانترنت واستخدام الذكاء الاصطناعي في تغيير الأصوات والتأثير على طبيعة الصور والفيديوهات بدأت ظاهرة الاحتيال الالكتروني بالانتشار في العديد من الوسائط الرقمية وعلى رأسها التويتر والانستغرام والفايسبوك، حيث أصبحت مواقع التواصل الاجتماعي على اختلافها وتنوعها أداة لاستدراج الأشخاص بهدف ايقاعهم في الأنماط المستحدثة لهذا النوع من الاجرام.

تتضمن هذه الجرائم أنماطا متعددة من الاحتيال عبر البريد الالكتروني الذي يستهدف الحصول على معلومات شخصية أو عن طريق الفيس بوك وتويتر لاستدراج الأفراد الى مواقع مشبوهة وطلب المساعدة المالية ويروجون لرسائل أو إعلانات تدعي أنها تقدم فرصًا تجارية أو جوائز (المقاومة الغير مشروعة عبر الانترنت)، لكن الهدف هو سرقة المعلومات الشخصية والأموال أو الحصول على الصور والفيديوهات لابتزازهم فيما بعد، ويمكن أن يتخذ صور التجسس الالكتروني في بعض الأحيان أو ممارسة التجارة كبيع السلع الغير مشروعة عبر هذه الوسائط والمنصات الرقمية وغيرها.

ويتطلب التصدي لهذه الجرائم الوعي بالطرق المحتملة التي يمكن اتباعها واتخاذ التدابير الوقائية مثل تجنب مشاركة المعلومات الشخصية عبر مواقع غير موثوقة والتحقق من هوية المراسلين قبل الاستجابة لمثل هذه الرسائل وغيرها.

تكمن أهمية البحث في هذا الموضوع من خلال تسليط الضوء لدراسة ظاهرة الكترونية عصرية ألا وهي جريمة الاحتيال الالكتروني والتي تفشت نتيجة القصور التشريعي لتنظيم هذه الظاهرة التي تحولت الى ظاهرة سلبية استغلها المحتالون للربح المادي السريع والحصول على المعلومات الشخصية للأفراد بأقل جهد وفي وقت وجيز حيث يتطلب الأمر المعرفة بتقنية التكنولوجيا المعلوماتية ومداخلها فقط.

وكذلك الوقوف على مدى فاعلية النصوص القانونية الحالية في الحد من هذه الظاهرة التي تحولت من اطارها التقليدي القديم الى الاحتيال في شكله الجديد باستخدام التقنيات والوسائل المتطورة التي ساهمت في انتشار هذه الأفة الاجتماعية بشكل رهيب، ومن جهة أخرى تحديد الوضعية القانونية للأفراد الذين يقعون ضحية لمثل هذه الجريمة.

وعليه تكمن الإشكالية المحورية لهذه الدراسة في كون جريمة الاحتيال الإلكتروني تشكل ظاهرة إجرامية مستحدثة شديدة التعقيد، تضع الأنظمة القانونية المعاصرة أمام تحديات جسيمة نتيجة الطبيعة الديناميكية والمتسارعة لتقنية المعلومات، فرغم المزايا المتعددة لطفرة الذكاء الاصطناعي، إلا أن إساءة توظيف تقنياته أفرزت تهديدات حقيقية مست بالحق في الخصوصية وقواعد المسؤولية القانونية، محولةً الاحتيال التقليدي إلى نمط رقمي مبتكر وعابر للحدود، وتتضاعف أبعاد هذه المشكلة أمام القصور التشريعي النسبي في مواكبة هذه التحولات الرقمية المتسارعة، الأمر الذي ينعكس سلباً على كفاءة أجهزة الضبطية القضائية في ملاحقة الجناة وإثبات الجريمة لغياب النصوص الصريحة، وإزاء هذه المفارقة بين الوجه الإيجابي للتطور التكنولوجي وإفرازاته السلبية التي تهدد الاستقرار الاقتصادي والمنظومة القيمية والنظام العام، تبرز الحاجة الملحة لتسليط الضوء على هذه الظاهرة، من خلال الإجابة على الإشكالية التالية:

ما مدى فعالية المنظومة التشريعية السارية في مواجهة جرائم الاحتيال الالكتروني،

خاصة في ظل التحديات التقنية المستحدثة التي يفرضها عصر الذكاء الاصطناعي؟

للإجابة على هذه الإشكالية تم الاستناد الى المنهج الوصفي لما تحتاجه هذه الدراسة من وصف لتطور الذي عرفته هذه الجريمة من شكلها البسيط الكلاسيكي والتقليدي الى صورته الحالية التي تأثرت بما وصل اليه العالم من تطور في مجال العلم والمعلوماتية والذي عرف بالاحتيال الالكتروني نسبة للوسط الافتراضي واللامادي الذي ترتكب فيه هذه الجريمة من جهة وصعوبة اثباتها من جهة أخرى، والتحليلي كونه الأداة الأكثر ملائمة في الدراسات القانونية التي تطلب تحليل معمق لمحتوى مختلف النصوص القانونية التي لها علاقة بموضوع الدراسة.

كما قد تمت الاستعانة بالمنهج التاريخي للوقوف على نشأة هذه الجريمة القديمة والجديدة في نفس الوقت ومبررات انتشارها في الأونة الأخيرة والتي أثرت بشكل مباشر على الفرد والمجتمع.

تم تناول الدراسة من خلال مبحثين، نتناول في الأول تحديد المفاهيم التي لها علاقة بالموضوع، وفي المحور الثاني يتم معالجة المواجهة القانونية لجرائم الاحتيال الالكتروني، وذلك على النحو التالي:

المبحث الأول: الإطار المفاهيمي لجريمة الاحتيال الالكتروني.

المبحث الثاني: المواجهة التشريعية لجرائم الاحتيال الالكتروني.

وفي نهاية هاته الورقة البحثية اختتمنا الموضوع بجملته من النتائج والتوصيات.

المبحث الأول: الإطار المفاهيمي لجريمة الاحتيال الالكتروني

ارتبط ظهور مصطلح الاحتيال الالكتروني بالبدايات الأولى لنشأة الشبكة العنكبوتية (الانترنت)، وما ساعد على انتشاره بسرعة فائقة هو تطور وسائل نقل المعلومات وانتشارها (الذكاء الاصطناعي)، حيث أصبحت تقريبا هاته الوسائل التكنولوجية في متناول جميع الطبقات في المجتمع، وهذا يعني أنها لم تعد تقتصر على غني أو فقير أو على جنس معين أنثى أو ذكر ولا على عمر معين، زيادة على معرفة كيفية استخدام الانترنت بسهولة دون عناء بفتح حسابات بأسماء وهمية وشخصيات مستعارة.

ونتيجة التكاليف البسيطة لممارسة هذه العملية فهي لا تحتاج سوى هاتف محمول أو جهاز اعلام آلي مع ربطه بشبكة الانترنت فقط، استغل المحتالون هذه الفرصة لممارسة الاحتيال أكثر من قبل، ونتيجة الثورة التقنية التي عرفتها هاته الوسائل على تنوعها تطورت أساليب ارتكاب جريمة الاحتيال الالكتروني والتي من خلالها يستطيع المحتال الوصول الى أكبر عدد من الضحايا، حيث يقوم المحتالون بتطوير أساليب جديدة للسطو على البيانات المالية والشخصية كإرسال رسائل وهمية تبدو كأنها صادرة من مؤسسات موثوقة لجمع معلومات حساسة واستخدام منصات للتواصل مع الضحايا المحتملين وعرض عروض مزيفة لاستدراجهم وكسب ثقتهم في التعامل معهم.

المطلب الأول: تعريف جريمة الاحتيال الالكتروني

الاحتيال هو المكر والخديعة والكيد لكل فعل يقصد فاعله به خلاف ما يقتضيه ظاهره، ويعد مرتكبا لجريمة الاحتيال الالكتروني كل من يقوم بالتأثير في المعلومات المبرمجة عن طريق برمجة غير سليمة، أو عن طريق التدخل أثناء تطبيق البرنامج، أو عن طريق استعمال بيانات غير سليمة أو غير مكتملة أو بأية طريقة أخرى، مما يترتب عليه حدوث

المواجهة القانونية لجرائم الاحتيال الإلكتروني في عصر الذكاء الاصطناعي
أضرار لممتلكات الغير، على أن يكون ذلك بنية اثناء نفسه أو غيره بريح غير مشروع¹ وفيما يلي نتطرق لمفهوم الاحتيال لدى علماء الاجتماع وكذا فقهاء القانون².

الفرع الأول: تعريف الاحتيال لدى فقهاء علم الاجتماع

فالاحتيال من وجهة نظر علماء الاجتماع هو ظاهرة اجتماعية وهي تشمل سلوكيات تتنافى والقيم الأخلاقية السائدة في المجتمع، لما لها من تأثير مباشر على الحياة الخاصة للفرد ويعد من الممارسات التي تتعارض مع القيم الإنسانية، وهذا يعني أن البيئة الاجتماعية تشكل وسطا خصبا لهذه الممارسات على اختلافها وتنوعها³.

فالاحتيال مرده البيئة الاجتماعية التي نشأ فيها المحتال، لأن هذا الأخير هو ضحية ظروف اجتماعية بالدرجة الأولى دفعته لكسب المال عن طريق امتحان الاحتيال، فهو بهذا المعنى صورة من صور الخلل الاجتماعي التي كانت كنتيجة حتمية لتدني المستوى المعيشي للمحتال في بعض الأحيان والعكس صحيح، حيث أننا في الغالب نجد معظم المحتالين ميسوري الحال وهنا يثور الاشكال.

تعود الجذور التاريخية لميلاد الاحتيال الإلكتروني بدايات الثمانينات من القرن الماضي تحديدا سنة 1981، طفا على السطح مفهوم جديد لجرائم الحاسوب ارتبط بعمليات اقتحام نظم الحواسيب عن بعد وأنشطة زراعة الفيروسات الالكترونية، التي تقوم بعمليات تدمير الملفات والبرامج وبدأت عملية تحديد سمات مرتكبي جرائم الحاسوب والانترنت وظهر مصطلح الاحتيال الإلكتروني⁴.

¹ . Zamouche Ouidah et Yadjed Mohand Amziane, le phénomène de la mendicité entre un besoin réel et une forme du travail, Mémoire de fin de cycle en vue de l'obtention d'un diplôme de mastère, Université Abderrahmane Mira, Bejaia, 2014/2015 p 08.

² . Moayad Hosni Al-Khawaldah ،Abdullah Ahmed Al-Khesailat ،The crime of Begging ،a comparative study of the jordan ،French ،Belgian and german laws ، Turkish online journal of qualitative inquiry ،volume 12 ،issue3، July 2021، research article. P 324.

³ . طاهر جليل الحبوش، جرائم الاحتيال الأساليب والوقاية والمكافحة، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض 2001، ص 28.

⁴ . بولحية شهيرة، سوبح دنيا زاد، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس بركة، العدد 04، ديسمبر 2019، ص 42

ونتيجة لكل ذلك كان لابد من مواجهة هذه الأنواع من الجرائم وخاصة الاحتيال الالكتروني بشكل خاص التي بدأت تعرف على نطاق واسع بأنها نوع جديد من الجرائم، فتمت أول مواجهة تشريعية لهذه الجرائم من خلال قانون البيانات السويدي سنة 1973 الذي عالج قضايا الاحتيال عن طريق الحاسوب إضافة الى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول عليها بطريقة أو بأخرى، ثم صدر عام 1978 قانون فلوريدا لجرائم الحاسوب في الوم أ حيث تم تجريم الاحتيال على الحاسوب، ومع بداية الثمانينات بدأت معظم دول العالم تصدر تشريعات مماثلة فقامت كندا سنة 1983 بتعديل قانونها الجزائي لمكافحة جرائم الحاسوب، كما صدر القانون الأمريكي للاحتيال وإساءة استخدام الحاسوب عام 1984 وتم تعديله تبعا سنة 1986 الى غاية سنة 1990، كما صدر في بريطانيا قانون إساءة استخدام الحاسوب عام 1994 الذي جرم الاحتيال الالكتروني صراحة في الفصل الثالث منه¹.

الفرع الثاني: تعريف الاحتيال لدى فقهاء القانون الجنائي

أما الاحتيال لدى فقهاء القانون فليس بعيدا عما اتجه اليه علماء الاجتماع، حيث عرف على أنه كل تدليس يقصد به إيقاع شخص في الغلط الذي كان واقعا فيه لحمله على تسليم مال في حيازته، وترتب عليه تسليم المال للفاعل أو لغيره سواء كان التدليس بالقول أو الكتابة أو الإشارة².

أما الاحتيال لدى فقهاء القانون الجنائي هو كل بيان أعطي عن أمر واقعي ماضي أو حاضر، مع علم الشخص الذي أعطاه بأنه كاذب أو عدم اقتناعه بصحته، وكل إخفاء مقصود أو بيان كاذب مقصود عن صحة أمر يعتبر احتيالا على الناس³.

يمكن تعريفه (الاحتيال الالكتروني أو المعلوماتي) على أنه آفة اجتماعية تتخذ البيئة الافتراضية أداة لممارسة هذا النوع من الاجرام، كما تتطلب معرفة دقيقة بالتقنية المعلوماتية واحترافية في استعمال أسلوب الاحتيال عن طريق قيام الجاني بإيقاع الغير في

¹ . بولحية شهيرة، المرجع السابق، ص 43.

² . طاهر جليل الحبوش، المرجع السابق، ص 30.

³ . محمود نجيب حسني، شرح قانون العقوبات - القسم الخاص، ط 3، دار النهضة العربية، القاهرة، 1988، ص 985 وما بعدها.

المواجهة القانونية لجرائم الاحتيال الالكتروني في عصر الذكاء الاصطناعي
الغلط عن طريق تغيير الحقيقة أو الحيلة، فيجلب لنفسه أو لغيره نفع غير مشروع مسببا بذلك ضررا بالغير¹.

تجدر الإشارة هنا الى أن الاحتيال الالكتروني كغيره من الجرائم له عدة عوامل تدفع الى ارتكابه، وهذا ما يميزه عن باقي الجرائم الأخرى كجريمة النصب والتسول والسرقة والرشوة وغيرها، وعلى الرغم من عزوف أغلب التشريعات عن متابعة مرتكبي جريمة الاحتيال الالكتروني وهذا راجع لعدة أسباب أهمها التطور الذي يشهده العالم اليوم في مجال المعلوماتية التي يستغلها المحتالون لارتكاب جرائمهم وهي تتفاوت من دولة الى أخرى فأثرت في نسب ارتكاب هذه الجريمة والاقبال على ارتكابها على حسب تقدم الدولة سياسيا واقتصاديا واجتماعيا.

فالاحتيال الالكتروني وفقا لما سبق هو سلب المال والحصول على المعلومات الشخصية من رواد ومستخدمي المنصات الرقمية على تنوعها (الانستغرام، تويتر، فايس بوك، واتساب، البريد الالكتروني.... وغيرها)، ويتم ذلك باستغلال هاته الفضاءات الرقمية مع عدم الإفصاح عن الهوية الحقيقية للجاني المحتال باستخدام تقنية الذكاء الاصطناعي ودون بذل أدنى جهد أو عناء، على خلاف الاحتيال التقليدي الذي يتم عبر الفضاءات العمومية أو الخاصة.

المطلب الثاني: تعريف المنصات الرقمية وتطبيقات الذكاء الاصطناعي

هي منصات برمجة الكترونية عبر الانترنت يقوم الأفراد من خلالها بفتح حسابات تكون في الغالب بأسماء لشخصيات افتراضية ومنهم من يفصح على هويته لمصالح شخصية²، بغرض تبادل المعلومات وإقامة علاقات متنوعة سواء في إطار العمل أو الاشهار أو الدراسة أو البيع والشراء... وغيرها.

ومن أبرز خصائص هذه الوسائل أن مجالها مفتوح وغير محدود نتيجة طبيعتها اللامادية والتي جعلت العالم عبارة عن قرية مصغرة حيث سهلت الاطلاع على كل ما يجري على المستوى العالمي دون تحمل أعباء التنقل ودون تحمل أي جهد مادي أو معنوي.

¹ . المرجع نفسه

² . محمد حسين منصور، النظام القانوني للمنصات الرقمية والمعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2023، ص 45 وما بعدها .

ويجدر بنا التفرقة بين المنصات الرقمية والمواقع الالكترونية فهذه الأخيرة وجودها يقتصر فقط على الشبكة العنكبوتية (الانترنت)، في حين أن المنصة Platform (البوابة) فهي أشمل وأوسع من الموقع لأنها تجمع بين خاصيتين، الأولى هي تقديم خدمات تفاعلية متنوعة والخاصية الثانية والتي تشترك فيها مع المواقع وهي تقديم معلومات في مجالات متعددة وتكون تابعة لهيئات عمومية أو خاصة على خلاف الموقع الالكتروني Websit الذي يكون الهدف منه هو تقديم معلومات معينة في موضوع محدد فقط¹ وهناك أكثر من نوع من أنواع المنصات الرقمية وهي تشمل ما يلي:

الفرع الأول: الفايسبوك والتويتر

هو أحد المواقع التي يستخدمها العديد من رواد مواقع التواصل الاجتماعي وهو الأكثر استعمالاً، فمن خلاله يمكن إقامة العديد من العلاقات وال صداقات والميزة الأساسية للفيس بوك أنه يسمح بنشر مختلف الملفات وتحميلها سواء دراسات أو فيديوهات والصور والتطبيقات والرسائل النصية، كما يحتوي على العديد من الخصائص مثل غرفة الدردشة (الماسنجر) والخريطة الذكية وعرض السلع والخدمات وغيرها، وهذا ما جعله يتصدر القائمة في الاقبال عليه وانشاء صفحات من قبل العديد من المحتالين². أما التويتر فينتهي الى مواقع التواصل الاجتماعي وهو موقع يتسم بعرض بيانات النشر للتغريدات، ويعد أداة لتمكين البرمجيات والنظم المختلفة من استخدام المحتوى الذي تنشره العديد من المواقع³. ويعد من التطبيقات التي تمكن المستخدمين من متابعة آخر الأخبار لمختلف المواقع دون الحاجة لزيارة كل موقع على حدي.

¹ . أسماء نوري ومحمد عبود، البوابات والمنصات الرقمية، سلسلة محاضرات في مادة المراجع العربية التقليدية والالكترونية، المحاضرة 14، 2021، دون دار النشر، صفحات دون ترقيم المتاحة على الموقع الالكتروني:

https://uomustansiriyah.edu.iq/media/lectures/8/8_2021_03_31!12_28_08_AM.pdf
تاريخ الدخول: 2023/10/22 الساعة 20:43م.

² . محمد حسين منصور، المرجع السابق، ص 46.

³ . محمد هشام صالح عبد الفتاح، جريمة الاحتيال، أطروحة مقدمة لاستكمال متطلبات درجة الماجستير في القانون العام، كلية الدراسات العليا، نابلس، فلسطين، 2008 ص 52.

الفرع الثاني: الانستغرام والواتساب

الانستغرام عبارة عن نظام تشغيل خاص بالهواتف المحمولة وقد صاحب ظهوره ظهور الهواتف الذكية، بدأ تطبيقه سنة 2007 ومن أهم ميزاته أنه يعمل على مشاركة الصور والفيديوهات عبر شبكات التواصل الاجتماعي ويعمل بخاصية الهاشتاج، زيادة على هذا فهو يحتوي على خيارات التعديل وتفعيل المؤثرات على الصور عن طريق الفلتر والأدوات المخصصة لذلك.¹

الواتساب وهو تطبيق مجاني بحيث يطرح للاستخدام دون مقابل مادي، ونتيجة لزيادة الاقبال على هذا التطبيق تغير الواتساب من خدمة مجانية الى خدمة مدفوعة في ديسمبر 2009، ويعمل بخاصية الرسائل المركزية عبر الأنظمة الأساسية الخاصة بخدمة نقل الصوت عبر شبكة الانترنت.²

الفرع الثالث: الذكاء الاصطناعي

هو عبارة عن أنظمة تقنيات حاسوبية لها القدرة على محاكاة تصرفات الانسان لأداء العمليات المختلفة بذكاء، فهي بذلك مزيج بين الطبيعة البشرية وبين البرمجيات التقنية التي تؤثر بشكل أو بآخر في اكتشاف المهام التي تقدمها هاته الخوارزميات وتلك الأفعال التي يقوم بها الانسان ككائن بشري طبيعي.³

المبحث الثاني: المواجهة التشريعية لجرائم الاحتيال الالكتروني

الاحتيال الالكتروني جريمة ليس لها آثار مادية ملموسة يمكن رفعها من مسرح الجريمة التي ارتكبت فيها، فهي جريمة تقع في الوسط الرقمي الافتراضي يتم استغلالها من المحتالون في تبادل المعلومات وتداولها بالموجات الرقمية الغير مرئية، كما أنها لا تترك أثارا فيما تعلق بهوية مرتكبيها، هذا ما ساعد على تفشيها وسرعة انتشارها نتيجة التعقيد التقني عموما والفراغ التشريعي خصوصا.

¹ . أسماء نوري ومحمد عبود، المرجع السابق، صفحات دون ترقيم.

² -Hamada Khair Mahmoud, The crime of electronic begging and ways to confront it, international journal to Advanced research on Law and gouvernance, volume 4, issue 2, 2022. p 270.

³ . عمر نافع رضا العباسي، النظام القانوني للذكاء الاصطناعي، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2019، ص 35.

المطلب الأول: الطبيعة القانونية لجرائم الاحتيال الإلكتروني

الخصائص المميزة لهذا النوع من الاجرام التركيز على كل ما هو مستحدث في المجال المعلوماتي والتقني ما جعل ارتكابها ينحصر في فئة معينة تتمتع بدرجة من الذكاء والمعرفة الرقمية فطابع هذه الجريمة يختلف عن باقي الجرائم الأخرى كسرقة الأموال أو المنقولات وغيرها، ذلك أن كل من يقع ضحية لهذه الجريمة فانه يمنح أمواله للغير بمحض ارادته لأن المحتال الإلكتروني قد تمكن من استعمال طرق احتيالية باتخاذ اسم كاذب أو صفة غير صحيحة أو تقرير أمر كاذب عن واقعة معينة متى كان من شأن ذلك خدع المجني عليه وحمله على التسليم، وكذلك هذه الجريمة قد تخلف الألاف من الضحايا من خلال نداء كاذب واحد من قبل المحتال وفي وقت وجيز يمكن أن يحقق أرباحا معتبرة وهذا ما جعل الكثير يمتن هذه السلوكيات وهذا ساهم في انتشارها بشكل رهيب أكثر من الاحتيال التقليدي، ولا يقتصر الاحتيال الإلكتروني على فعل سلب المال بل يتعدى ذلك مثل جرائم الاحتيال عبر البريد الإلكتروني والابتزاز الإلكتروني والتجسس الإلكتروني.... وغيرها¹.

الفرع الأول: جريمة الاحتيال الإلكتروني جريمة مستحدثة

الاحتيال الإلكتروني هو جريمة مستحدثة وتعتبر احدي أشكال الجرائم الإلكترونية والتي يصعب اكتشافها وإثباتها²، فالجرائم الإلكترونية التي لا يمكن فيها الاستدلال بالشهود ولا يمكن استجوابهم زيادة على هذا فإنها عابرة للحدود من هنا تبرز تداعيات وصعوبة الكشف عن هذه الظاهرة؛ حيث أن وجودها صاحب التقدم التكنولوجي والمعلوماتي مما أدى إلى انتشار واستفحال هذه الجريمة في المجتمع في الأونة الأخيرة بشكل لافت خاصة فيما يتعلق بتعدد المنصات والمواقع التي يستعين بها المحتال في ممارسة هذه الجريمة، حيث أن السبب المباشر هو عزوف غالبية التشريعات والقوانين عن ملاحقة مرتكبي هذه الجريمة والاكتفاء بالنصوص التي كرسست لمواجهه الاحتيال التقليدي.

¹ . أحمد لطفي السيد، جرائم المعلوماتية والاحتيال الإلكتروني، دار النهضة العربية، القاهرة، الطبعة الأولى، 2024، ص 88.

² . خالد ممدوح، التحقيق الجنائي في الجرائم الإلكترونية وصعوبة الإثبات، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2024، ص 112.

كما أن هذا النوع من الاجرام لا يعتد بالمجال الإقليمي والمحلي للدول في ارتكابها، فمع انتشار الشبكة العنكبوتية بين دول العالم ومختلف الأقاليم أمكن ربط العديد من أجهزة الحاسوب بهذه الشبكة¹، حيث يمكن أن يكون الجاني في بلد والضحية في بلد آخر فساعد التطور التكنولوجي على تقليص المسافات وتعزيز الترابط بين مختلف بقاع العالم انعكس هذا على الطبيعة الاجرامية التي يعتمد فيها المجرم إلى استخدام هذه الوسائل في خرق النصوص القانونية، وهذا يعنى أن مسرح جريمة الاحتيال الالكتروني لم يعد محليا بل تعدى ذلك ليصبح عالمياً، فالمجرم لا يتواجد في مسرح الجريمة، بل يرتكب الجريمة عبر الشبكة العنكبوتية وعن بعد.

الفرع الثاني: خصائص المجرم المحتال الكترونيا

نتيجة للطبيعة القانونية لهذه الجريمة والتي ترتكب لإشباع حاجات فردية وتحقيق الربح المادي ويكون أهم دوافعها الجشع والطمع هذا جعل نسبة انتشار الاحتيال التقليدي تراجع مقارنة بالاحتيال الالكتروني²، ذلك أن الاحتيال المعلوماتي هو اجرام يتطلب درجة من الذكاء لممارسته بالمقارنة بالاحتيال التقليدي الذي يميل إلى التركيز على المظهر الخارجي وانتحال الشخصيات التي تعبر عن مدى صدقه في تقديم خدمات واستثمارات وهمية الأمر الذي جعل الكثير ينتقل من الاحتيال التقليدي الى الاحتيال الالكتروني المستحدث³.

كما أن مرتكبي الاحتيال الالكتروني يتمتعون بمعرفة عالية للجانب التقني والمعلوماتي والمأمهم بكل ما هو مستجد في مجال الوسائل الالكترونية ومعرفتهم بكل أنواع شبكات التواصل الاجتماعي المتعددة والمختلفة ؛ ونتيجة لتعدد هذه التقنيات المرتبطة بالجريمة التي تمكنهم من ارتكاب جرائمهم بدقة واحترافية غير متناهية، حيث إن الجماعات الاجرامية المنظمة والمنفذة لهذا النوع من الاجرام أصبح مرتكبوها لا يقيمون دائماً في مدن محددة، بل أصبح بإمكانهم التنقل بكل حرية وفي سرية تامة عبر مختلف

¹ . Rania Atia, Electronic begging its social and economic impact on jordanian society from the point of view of a sample of Facebook users, journal of humanities and social sciences, volume 5, issue 4, 30 mars 2021, p 64.

² . جميل عبد الباقي الصغير، الجرائم المعلوماتية: دراسة مقارنة، دار النهضة العربية، القاهرة، الطبعة الثانية، 2024، ص 154.

³ . المرجع نفسه.

المواقع حول العالم، كما يمكنهم تبادل المعلومات والتخطيط لها وتحديد مواعيد وأوقات محددة لتنفيذها من خلال المراسلات عبر منصات البريد الإلكتروني وشبكات التواصل الاجتماعي التي لم تعد تخص دولة دون الأخرى، وهذا يشكل صعوبة في البحث عن الأدلة العلمية التي يتم رفعها من الوسط الافتراضي التي تتطلب تقنية التكنولوجيا المعلوماتية، وهذا ما ساعد مرتكبو هذه الجريمة في وقتي قياسي أن يتمكنوا من طمس والتلاعب بالبيانات والمعلومات المتواجدة في جهاز الكمبيوتر، لذا فإن صعوبة اكتشافها وثباتها جعلت من هذه الجريمة مهنة يمتنها العديد من الأشخاص في المجتمع¹.

المطلب الثاني: الأليات القانونية للحد من خطورة الاحتيال الإلكتروني

نتيجة لغياب النصوص القانونية لردع هذه الجريمة وملاحقة مرتكبيها وأمام عدم احاطتها بالأليات المتعلقة بالضوابط الاجتماعية لهذه الجريمة لدى الكثير من الدول على خلاف الاحتيال التقليدي والذي عالجته معظم المنظومات التشريعية للدول حيث تم تحديد الركن المادي والركن الشرعي والركن المعنوي لكل منها²، كما حددت الأفعال المنهى عنها ونصت صراحة عن عدم مشروعيتها، وفي المقابل حددت العقوبات المقررة لها على حسب جسامتها وهذا ما اتجه اليه المشرع الجزائري بموجب قانون العقوبات.

وفي ظل هذا الفراغ التشريعي تزايدت مخاطر هذه الجريمة، وما ساعد على استفحالها وتفشيها هو غياب نصوص قانونية صريحة وواضحة التي تنص على تحديد الوسائل المستعملة بدقة كما هو الحال بالنسبة للاستعانة بالذكاء الاصطناعي، كما أدى هذا القصور التشريعي لإفلات المجرم من المساءلة والعقاب، حتى وان وجدت قوانين لمواجهة ومكافحة الجريمة فإنها مع التطور الحاصل في طرق ارتكاب جريمة الاحتيال الإلكتروني والامكانيات المتطورة في ارتكابها (الذكاء الاصطناعي مثلا) لم تعد هذه النصوص على قدر كافي لمواجهة أثارها السلبية بشكل كامل والحد من خطورة هذا النوع من الاجرام من جهة وانصاف الضحايا من جهة أخرى.

¹ . عبد الفتاح بيومي، عملة الجريمة الإلكترونية المنظمة وإشكاليات جمع الدليل الرقمي، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد 2، 2025، ص 310.

² . الكعبي محمد عبيد، الجرائم الناشئة عن الاستخدام الغير مشروع للإنترنت، دار النهضة العربية، القاهرة، ص 34.

الفرع الأول: الخصوصية الإجرائية لملاحقة جرائم الاحتيال الإلكتروني

تستلزم مواجهة الاحتيال الإلكتروني الخروج عن النمطية الإجرائية التقليدية، وذلك عبر إرساء قواعد إجرائية مرنة وقادرة على التعامل مع الدليل الرقمي سرعةً وحجّةً. وتتجلى هذه الخصوصية في تفتيش الأنظمة المعلوماتية المتطورة، وتذليل عقبات الاختصاص القضائي العابر للحدود، بما يضمن ملاحقة الجناة الذين يتخفون وراء خوارزميات الذكاء الاصطناعي المعقدة¹.

فلا يمكن حصر هذه الجريمة في نمط معين وتحديد مختلف الظروف التي كانت سبباً في إتهام هذا السلوك الإجرامي، كل هذا ساهم بشكل مباشر في افلات هؤلاء المحتالين الإلكترونيين من العقاب، كما أنها تحتاج إلى خبرة ودراية بمداخل ومخارج التقنيات الإلكترونية وهذا يتطلب من المحقق التعامل معها وفقاً للطبيعة التي تميزها عن باقي الجرائم الأخرى، لذلك يتعين على المحقق للتحقيق في هذه الجريمة وملاحقة مرتكبيها قضائياً أن يكون ملماً بالقدر الكافي في مجال المعلوماتية خاصة².

وفي المقابل لا بد من سن تشريعات تنظم الإجراءات الخاصة بهذا النمط من الاجرام بما يسمح بالتعامل مع الرقمنة والتطور الحاصل في هذا المجال، لذا يجب على الجهات المعنية بإنفاذ القانون تطوير قدراتها وتحديث أساليبها لمكافحة جرائم الإنترنت من خلال توفير التدريب المناسب لعناصر الضبطية القضائية، واستخدام التكنولوجيا الحديثة في جمع البيانات وتحليلها، بالإضافة إلى التعاون الدولي في مجال مكافحة جرائم الإنترنت وتبادل المعلومات بين الدول.

كما ينبغي أيضاً تشديد إجراءات البحث والتحري عن مرتكبي هذه الجرائم وإثباتها، بتعديل وتحسين ومسايرة التشريعات القانونية لمواجهة هذه الجرائم وتوفير الحماية للمجتمع الإلكتروني. وعلى المستخدمين أيضاً توخي الحذر واتباع إجراءات الأمان اللازمة عند التعامل عبر الإنترنت، للحد من انتشار جرائم الاحتيال والاختراقات الإلكترونية المختلفة.

¹ يوسف عبيد، إشكالية الاختصاص القضائي العابر للحدود في الجرائم المرتكبة عبر الذكاء الاصطناعي، مجلة الفقه والقانون السيبراني، جامعة الإمارات العربية المتحدة، المجلد 8، العدد 3، 2025، ص 42.

² . عبابنة محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005،

فهذا التزايد المستمر في خسائر الاحتيال الإلكتروني مقارنة بالخسائر في الاحتيال التقليدي ووقوع العديد من الأشخاص ضحايا لهذه التصرفات الرقمية وكذا تداعياته على المجتمع الناجمة عنه أصبحت مسألة النظر في هذه الجريمة يشكل ضرورة حتمية أكثر من ذي قبل، لأن سهولة التعرف على الاحتيال التقليدي من حيث مرتكبي هذه الجريمة، والفاعلون لها، وإمكانية التوصل إلى الأدلة والشهود بها. كل ذلك يؤدي إلى سرعة كشف أبعادها وضبط مرتكبيها بأقل قدر من التكلفة عكس ذلك فإن الاحتيال الإلكتروني زيادة على صعوبة كشفه وإثباته فإنه يتسم بالتكلفة الباهظة، سواء من حيث التخطيط لارتكابها أو بشأن الخسائر الناجمة عنه والتي تلحق بالأشخاص ضحايا هاته الجريمة¹.

لذلك يجب وضع استراتيجية عامة وشاملة وفاعلة للحد من خطورة الاحتيال الإلكتروني، حتى لا تكون جهود تقليص ومتابعة الظاهرة من ردود أفعال رادعة لمثل هذه النشاطات الاجرامية دون جدوى، وذلك من خلال محاولة متابعة ومواكبة كل ما من شأنه أن يساعد في تفشي مثل هذه السلوكيات في المجتمع، سواء كانت هاته الاستراتيجية على المستوى المحلي (الوطني) أو عربية أو حتى دولية فلا بد أن تكون شاملة من جميع النواحي للحد من تداعياتها السلبية ولا يمكن بأي شكل من الأشكال إهمال أي جزئية مهما كانت حتى لا تكون منفذا لهذه الجريمة أو أي محتمل يحترف الاحتيال الإلكتروني على حد سواء.

الفرع الثاني: مدى كفاية القواعد الموضوعية لمواجهة الاحتيال الإلكتروني

يتعين على السلطة التشريعية بصفة خاصة استحداث نصوص قانونية تعالج مسألة الاحتيال الإلكتروني الذي أصبح ظاهرة تهدد الأمن الرقمي في مختلف أنحاء العالم، فبالرجوع لمختلف التشريعات سواء على المستوى المحلي أو العربي أو حتى الدولي، تعاني من فراغ تشريعي وما تزال معظم نصوصها تحدد الأفعال والعقوبات المتعلقة بالاحتيال التقليدي فقط، هذا الأخير أصبح يختلف تماما عن الاحتيال بصورته الحالية، فهذا النمط من الاحتيال حديث العهد وهذا يستدعي تغليظ العقوبات وتشديدها بما يتناسب مع هذا النوع من الاجرام.

¹ . عيابة محمود أحمد، المرجع السابق، ص 17.

فبالنسبة للمشرع الجزائري فقد تناول الاحتيال بموجب قانون العقوبات من خلال نص المادة 372 منه¹، حيث جعل من الاحتيال جريمة كل من توصل الى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو ابراء من التزامات، أو الى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه اما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل الى خمس سنوات على الأكثر أو بغرامة من 500 الى 20,000 دينار جزائري وشدد العقوبات الأصلية ورفع قيمة الغرامات المالية لتتناسب مع التضخم الاقتصادي ومع جسامه الأرباح التي يجنيها المحتالون إلكترونياً، وكذا المادة 394 مكرر وما بعدها من نفس القانون² التي نصت على أن يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، كل من يدخل أو يبقى، عن طريق الاحتيال، في كل أو جزء من منظومة للمعالجة الآلية للمعطيات.

وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير معطيات المنظومة أو اضطراب في سيرها وفقاً للقانون رقم 09/ 04 المؤرخ في الخامس من شهر أوت سنة 2009 والمتضمن الأحكام المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

كما عالج المشرع المصري جريمة الاحتيال بموجب المادة 336 من قانون العقوبات وقرر لها عقوبة الحبس كل من توصل الى الاستيلاء على نقود أو عروض أو سندات مخالصة أو متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها اما باستعمال طرق احتيالية من شأنها ايهام الناس بوجود مشروع كاذب أو واقعة مزورة أو احداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الاحتيال أو ايهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور، واما بالتصرف في مال ثابت أو منقول ليس مملوكا له

¹ . القانون رقم 24-06، المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، الصادرة بتاريخ 30 أبريل 2024.

² . المرجع السابق.

ولا له حق التصرف فيه، اما باتخاذ اسم كاذب أو صفة غير صحيحة، معنى ذلك أن الاحتيال ينال الاعتداء على حق ملكية المال العام المنقول والاستلاء على مال منقول مملوك للغير، وبهذا يكون المشرع المصري كذلك قد أخذ موقف المشرع الجزائري بخصوص جريمة الاحتيال¹.

وهذا على خلاف موقف باقي التشريعات في الدول المتقدمة كما هو الحال في السويد فتمت أول مواجهة تشريعية لهذه الجريمة (الاحتيال الالكتروني) من خلال قانون البيانات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسوب إضافة الى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول عليها بشكل غير مشروع².

كما صدر عام 1978 قانون فلوريدا لجرائم الحاسوب في الولايات المتحدة الأمريكية حيث تم تجريم الاحتيال على الحاسوب، ومع بداية الثمانينات بدأت معظم دول العالم تسن تشريعات مماثلة فقامت كندا عام 1983 بتعديل قانونها الجزائي لمكافحة جرائم الحاسوب، كما صدر القانون الأمريكي للاحتيال واساءة استخدام الحاسوب عام 1984 والذي عدل عدة مرات سنوات 1986 الى غاية 1990، كما صدر في بريطانيا قانون إساءة استخدام الحاسوب عام 1995 الذي جرم الاحتيال الالكتروني بموجب الفصل الثالث منه³.

أما على المستوى الدولي فقد عقدت عدة اتفاقيات في مجال الجرائم المعلوماتية عامة ولم تخصص أي معاهدات أو اتفاقيات تحد من انتشار الاحتيال الالكتروني وعلى الرغم من الطابع الدولي لهاته الجريمة العابرة للقارات وحدود الدولة الواحدة الى أنه لحد الساعة لم تلتفت الدول للتدخل باتفاقيات أو معاهدات تنظم هذه المسألة، فيما عدى بعض الاتفاقيات التي نصت على إجراءات البحث والتحري المتعلقة بالجرائم السيبرانية،

¹ . عادل الشاوي، الوسائل الاحتيالية بين التشريع الجنائي المصري والجزائري، دراسة تحليلية مقارنة، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 3، 2025، ص 94.

² . بولحية شهيرة، المرجع السابق، ص 42.

³ . المرجع نفسه.

فلا نجد ما يكبح هذه الظاهرة بل هي في تفاقم مستمر لدرجة أنه لم نعد نستطيع التفرقة بين الهيئات والمؤسسات والمنظمات المشروعة وتلك التي تعمل في إطار النصب والاحتيال¹. أما فيما يخص الآليات الإدارية والقضائية يقصد بها تلك الإجراءات المتخذة والمتبعة في حق هؤلاء المحتالين، ففي حالة ثبوت ارتكاب هذا النوع من الجريمة وكشفها يتعين التعمق في التحقيقات مع المجرم المحتال للوقوف على جميع الظروف والدوافع التي سهلت من ارتكابه لجريمته وفي حالة ثبوتها بحقه لابد من القيام باتخاذ كافة الإجراءات لاسيما مصادرة الأموال المتأتية من هذا الاحتيال، والوسائل والعتاد المستعمل في ممارسة هذا الفعل سواء هواتف ذكية أو برامج أو أجهزة الاعلام الآلي وغيرها وكذا احالته على الجهات القضائية المختصة.

خاتمة:

إن فاعلية المنظومة التشريعية السارية في مواجهة جرائم الاحتيال الإلكتروني تظل محدودة ونسبية لحد ما لأنها تتأرجح بين الكفاية الإجرائية الجزائية من جهة والقصور الموضوعي المستحدث من جهة أخرى، لذلك يبدو أن القواعد الإجرائية السارية تقف أمام تحدٍ تكنولوجي غير متكافئ؛ حيث يمنح الذكاء الاصطناعي المجرمين القدرة على طمس المعالم الرقمية للجريمة مما يسهم في تعقيدها وصعوبة كشفها واثباتها نتيجة تشفير الأدلة، وبالرغم من استحداث بعض آليات التحري الرقمي، إلا أن الأجهزة الضبطية والقضائية لا تزال تفتقر إلى أطر إجرائية مرنة عابرة للحدود تتيح الحصول على الدليل الفني وحمايته بسرعة تتماشى مع طبيعة الجريمة الرقمية عموماً، لذلك فمواجهة التحديات التقنية لعصر الذكاء الاصطناعي لا تتطلب مجرد تعديل القواعد الموضوعية، بل تستلزم صياغة سياسة جنائية استباقية متكاملة، تنبثق منها نصوص صريحة تجرم الأفعال التحضيرية المتمثلة في إساءة استخدام وتطوير البرمجيات الاحتيالية الذكية، بالتوازي مع تأهيل منظومة العدالة الجنائية تقنياً لضمان الأمن القانوني والمعاملاتي في

¹ . عبيد علي، ناصر موفق وآخرون، ماهية جريمة الاحتيال المعلوماتي، مجلة كلية القانون للعلوم القانونية، كلية الحقوق والعلوم السياسية جامعة تكريت بغداد.

البيئة الرقمية المعاصرة القائمة على استخدامات تطبيقات الذكاء الاصطناعي بأنواعه المختلفة.

ونتيجة اتصال هذه الجريمة بأنظمة الذكاء الاصطناعي والتي ساعدت بشكل كبير في تفشي واستفحال الظاهرة نجد أنه حتى ملاحقة ومتابعة هؤلاء المحتالين من الناحية الإجرائية الإدارية أو القضائية غير واضحة وهذا بالرغم من أن الجريمة الالكترونية قد صدرت بشأنها العديد من التشريعات على المستوى الوطني أو الدولي إلا أن غالبية الفاعلين يفلتون من العقاب والمساءلة خصوصا مرتكبي جريمة الاحتيال الالكتروني.

ووفقا لما سبق يتعين على المشرع الجزائري تعديل المواد المتعلقة بالاحتيال بموجب قانون العقوبات ومسايرة باقي الدول الغربية كما هو الحال في الولايات المتحدة الأمريكية والسويد، وذلك بوضع نصوص واضحة وصريحة بخصوص الاحتيال الالكتروني فهذه المواد المذكورة في متن هذه الورقة البحثية أصبحت غير كافية لمسايرة التطور الحاصل في هذا المجال خاصة في ظل الاستخدامات المختلفة لأنظمة الذكاء الاصطناعي وغيرها، مع تشديد العقوبات المتعلقة بالجرائم الالكترونية لاسيما الاحتيال الالكتروني ففي ظل الانتشار الواسع لهذه الظاهرة في الآونة الأخيرة التي أصبحت تتزايد بشكل رهيب يدعو للقلق في ظل غياب الردع العام والخاص على المستوى الدولي.

- ضرورة تسخير كل الإمكانيات المادية والبشرية في الكشف عن جريمة الاحتيال الالكتروني للحد من تداعياتها السلبية على الفرد والمجتمع ووضع تدابير استباقية تمنع وقوع هذا النوع من الجرائم.

- متابعة ومراقبة مختلف الفاعلين في هذا المجال في إطار قوانين خاصة، وتشجيع ثقافة التبليغ لدى المواطن في حالة تسجيل تجاوزات عبر مختلف مواقع التواصل الاجتماعي تتعلق بالنصب والاحتيال وطلب المساعدات والاعانات من أشخاص تحت مسميات لمنظمات ومؤسسات وهمية وشخصيات افتراضية خصوصا من وقع ضحية لمثل هذه السلوكيات المنافية للنظام العام والأداب العامة في المجتمع.

قائمة المصادر والمراجع:

أولا / قائمة المصادر:

- القوانين:

- 1/ القانون رقم 04/09 المؤرخ في أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، جريدة الرسمية العدد 47.
- 2/ القانون رقم 06-24، المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، الصادرة بتاريخ 30 أبريل 2024.

ثانيا / قائمة المراجع:

أ-الكتب:

- 1/ أحمد لطفي السيد، جرائم المعلوماتية والاحتيال الإلكتروني، دار النهضة العربية، القاهرة، الطبعة الأولى، 2024.
 - 2/ الكعبي محمد عبيد، الجرائم الناشئة عن الاستخدام الغير مشروع للإنترنت، دار النهضة العربية، القاهرة.
 - 3/ خالد ممدوح، التحقيق الجنائي في الجرائم الإلكترونية وصعوبة الإثبات، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2024.
 - 4/ جميل عبد الباقي الصغير، الجرائم المعلوماتية: دراسة مقارنة، دار النهضة العربية، القاهرة، الطبعة الثانية، 2024.
 - 5/ طاهر جليل الحبوش، جرائم الاحتيال الأساليب والوقاية والمكافحة، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض 2001.
 - 6/ عبابنة محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005.
 - 7/ عمر نافع رضا العباسي، النظام القانوني للذكاء الاصطناعي، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2019.
 - 8/ محمد حسين منصور، النظام القانوني للمنصات الرقمية والمعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2023.
 - 9/ محمود نجيب حسني، شرح قانون العقوبات -القسم الخاص، ط 3، دار النهضة العربية، القاهرة، 1988.
- ب-الرسائل الجامعية:
- 1/ محمد هشام صالح عبد الفتاح، جريمة الاحتيال، أطروحة مقدمة لاستكمال متطلبات درجة الماجستير في القانون العام، كلية الدراسات العليا، نابلس، فلسطين. 2012.

ج- المقالات في المجالات:

1/ بولحية شهيرة، سوبح دنيا زاد، الاحتيال الالكتروني، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس بركة، العدد 04، ديسمبر 2019.

2/ عادل الشاوي، الوسائل الاحتمالية بين التشريع الجنائي المصري والجزائري، دراسة تحليلية مقارنة، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 3، 2025.

3/ عبيد علي، ناصر موفق وآخرون، ماهية جريمة الاحتيال المعلوماتي، مجلة كلية القانون للعلوم القانونية والسياسية، كلية الحقوق، جامعة تكريت، بغداد.

4/ عبد الفتاح بيومي، عولمة الجريمة الإلكترونية المنظمة وإشكاليات جمع الدليل الرقمي، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد 2، 2025.

5/ يوسف عبيد، إشكالية الاختصاص القضائي العابر للحدود في الجرائم المرتكبة عبر الذكاء الاصطناعي، مجلة الفقه والقانون السيبراني، جامعة الإمارات العربية المتحدة، المجلد 8، العدد 3، 2025.

د. المقالات في المنتقيات والندوات:

1/ أحمد عاصم أحمد، رؤية قانونية حول ثبوت جرائم السب والكذب عبر الانترنت في القانون المصري، المؤتمر الدولي الأول الخصوصية وأمن المعلومات في قانون الانترنت، القاهرة، 2008.

ه- المقالات على مواقع الانترنت:

1/ أسماء نوري ومحمد عبود، البوابات والمنصات الرقمية، سلسلة محاضرات في مادة المراجع العربية التقليدية والالكترونية، المحاضرة 14، 2021، دون دار النشر، المتاحة على الموقع الالكتروني: https://uomustansiriyah.edu.iq/media/lectures/8/8_2021_03_31!12_28_08_AM.pdf تاريخ الدخول: 2023/10/22 الساعة 20:43م.

6- المراجع الأجنبية

1/ Rania Atia، Electronic begging its social and economic impact on jordanian society from the point of view of a simple of Facebook users، journal of humanities and social sciences، volume 5، issue 4، 30 mars 2021.

2/ Hamada Khair Mahmoud، The crime of electronic begging and ways to confront it، international journal to Advanced research on Law and governance، volume 4، issue 2، 2022.

3/ Moayad Hosni Al-Khawaldah ،Abdullah Ahmed Al-Khesailat ،The crime of Begging ،a comparative study of the jordan ،French ،Belgian and german laws ، Turkish online journal of qualitative inquiry ،volume 12 ،issue3، July 2021، research article.

4/ Zamouche Ouidah et Yadjed Mohand Amziane، le phénomène de la mendicité entre un besoin réel et une forme du travail، Mémoire de fin de cycle en vue de l'obtention d'un diplôme de mastère، Université Abderrahmane Mira، Bejaia، 2014/2015.