جامعة 20 أوت 1955 سكيكدة

كليّة الحقوق والعلوم السياسية

قسم الحقوق

جريمة النصب والاحتيال في ظل الذكاء الاصطناعي

مذكرة مكملة لنيل شهادة الماستر تخصص: قانون جنائي وعلوم جنائية .

من تقديم الطالب:

جغرود حسام

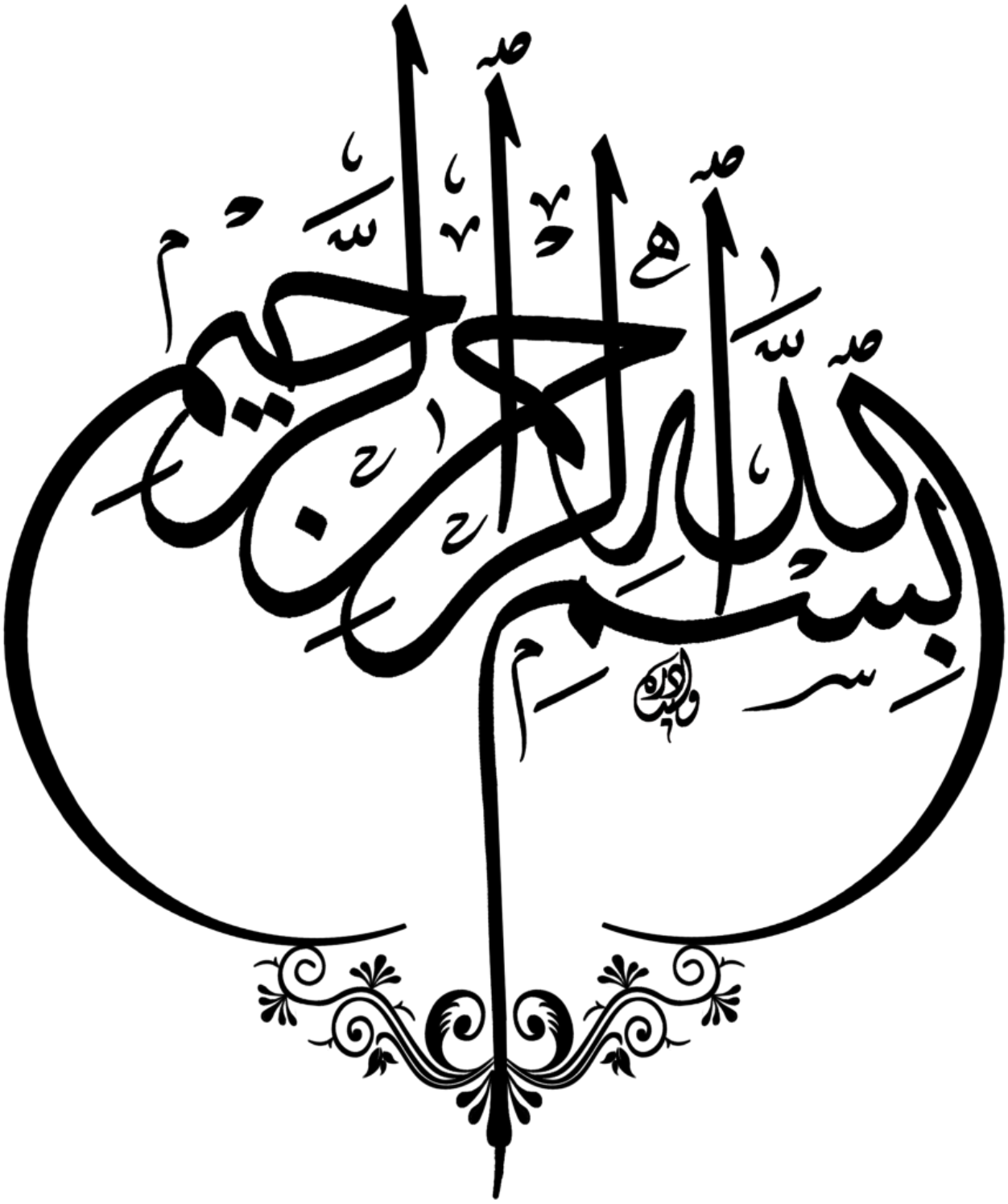
تحت إشراف:

أ. بركات قيسمون رامي

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
د.بوعزيز شهرزاد	أستاذ محاضر	رئيسا
د.فيلالي منصف	أستاذ محاضر	مناقشا
أ. بركات قيسمون رامي	أستاذ مساعد	مشرفا

دورة جوان 2026


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد الله الذي تتم بنعمته الصالحات، والصلاة والسلام على سيدنا محمد خاتم المرسلين وبعد:

أتقدم بالشكر الجزيل إلى الأستاذ المشرف: **بركات قيسمون رامي** الذي أشرف على هذا البحث وخصه برعايته واهتمامه.

شكر خاص **للدكتورة بوعزيز شهرزاد** بكلية الحقوق والعلوم السياسية جامعة 20 أوت 1955 سكيكدة التي لم تبخل علينا يوما بعلمها، نصائحها وتوجيهاتها القيمة التي كانت نبراسا نسير على خطاه، جزاك الله خير الجزاء ووفقك لما فيه خير للبلاد والعباد .

كما نتقدم بالشكر الجزيل لكل من مد لنا يد العون في إنجاز هذه المذكرة.

إهداء

إلى من جعلت الجنة تحت أقدامهما، إلى من قال فيهما الرحمن "**وقضى ربك ألا تعبدوا إلا إياه و بالوالدين إحسانا**" والدايَّ الكريمين، ربي يحفظهما ويمد في عمرهما ويرزقهما دوام الصحة والعافية.

إلى إخوتي وأخواتي، أصدقائي وزملائي، كل باسمه ومقامه، إلى عائلتي الصغيرة " **زوجتي**" وأبنائي " **جاد ، إياد، روان** " حفظهم الله ورعاهم وأنبتهم نباتا حسنا.

إلى كل أستاذ علمني و مهد لي طريق العلم و المعرفة أهدي عملي هذا.

" وما توفيقي إلا بالله "

مقدمة

جرائم النصب ليست بالحديثة العهد، لكنها من الجرائم التي تطورت صورها وأنماطها وأساليب ارتكابها، هي من الجرائم التقليدية مثلها في ذلك مثل السرقة وخيانة الأمانة، لكنها بالرغم من ذلك أخذت طابعا خاصا بين هذه الجرائم التقليدية، فقد تميزت عنها باتباع المحتال أساليب تقوم على أعمال الذهن والتفنن في ابتكار وسائل خداعية، بالإضافة إلى قدرتهم على تكييف هذه الأساليب والوسائل بما يتلاءم مع التطورات التقنية الحديثة والمتغيرات الاقتصادية والثقافية، ويساعدهم في ذلك أن ضحايا النصب يسعون بأنفسهم إلى شباك المحتالين بدافع الطمع وحب الثراء بطرق سريعة وسهلة كما يزينها لهم الجناة، فهم يعرضون بذكاء أكاذيبهم المدعومة بمظاهر خارجية براقة تسهم في إيقاع هؤلاء الضحايا في الوهم الذي يؤدي بهم إلى تسليم أموالهم إليهم طوعا واختيارا دون إكراه أو وسيلة ضغط على إرادتهم الحرة، لاسيما من تتوافر فيهم السذاجة وحسن النية.

لقد كانت جريمة النصب جريمة محلية ووطنية، لكن مع التقدم التكنولوجي والتحول الرقمي في شتى المجلات، ثم ظهور الذكاء الاصطناعي تعدت جريمة النصب الحدود الوطنية، وأصبحت جرائم عالمية، إذ اعتمد المحتالون على التطورات العلمية والتقنية لممارسة أساليبهم الخداعية خلف الشاشات والمواقع الإلكترونية بشكل مدروس ودقيق، لتصبح هذه الجريمة من أخطر الجرائم المستحدثة، نظرا للوسائل التقنية المستعملة من طرف المحتال، وكذا كونها جرائم عابرة للحدود الوطنية، مما استوجب تحديات جديدة على المنظومات القانونية، نظرا لقصور القواعد التقليدية في الإحاطة بهذه الأفعال المستحدثة، هذا ما ألزم تدخل المشرّع لسن قوانين ونصوص تواكب هذا التحول الرقمي، أين حاول المشرّع الجزائري على غرار باقي دول العالم مسايرة هذه التهديدات بسن أحكام قانونية لمكافحة الجرائم الإلكترونية، منها في إطار قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

في دراستنا هذه نتطرق لجريمة النصب التي يعتمد فيها المجرم على التقنيات الحديثة أهمها الذكاء الاصطناعي، ومدى تأثير هذه التقنية الغامضة التي يكون الدليل فيها رقميا في العالم الافتراضي وليس ملموسا مما يصعب كشف المجرمين في هذه الجرائم التي أصبح انتشارها الرهيب

في المجتمع يمس بأموال الأفراد وكذا اقتصاد البلد، مما أثار الكثير من التحديات أمام القانونيين والفقهاء لمحاربة هذه الجريمة المستحدثة .

أهمية الدراسة: وفي ظل تزايد هذا النوع من الجرائم ظهرت الحاجة لدراسة هذا الموضوع نظرا لأهميته من الناحية القانونية وكذا الاجتماعية، خاصة مع تزايد المعاملات المالية اليومية عبر مختلف الوسائط الإلكترونية مما يساهم في تنامي حالات النصب، هذا ما يستوجب وعيا قانونيا وتقنيا للتقليص من ذلك، كذلك هذا الموضوع يتقاطع مع تحديات العصر الرقمي الحديث من حيث الحماية القانونية للمعاملات الإلكترونية، ويجمع بين القانون الجنائي وتقنيات الذكاء الاصطناعي، كما تسهم هذه الدراسة في إثراء المكتبة القانونية بالدراسات المتخصصة في هذا المجال الذي لا يزال بحاجة إلى مزيد من البحث والتحليل. كذلك تبرز أهمية الدراسة في الكشف عن الأساليب الاحتيالية المعتمدة على تطبيقات الذكاء الاصطناعي وبيان مخاطرها على الأفراد والمؤسسات، مع التطرق لمدى كفاية النصوص القانونية القائمة لمواجهة هذه الجرائم، واقتراح آليات تشريعية وإجرائية تسهم في تعزيز الحماية القانونية والحد من انتشارها.

أهداف الدراسة: تهدف هذه الدراسة إلى التعرف على جريمة النصب الالكتروني وما تمثله من خطورة تهدد الأفراد خاصة مع تزايد المعاملات المالية عبر الوسائل الإلكترونية، كذلك من أجل تبيان النصوص القانونية التي وضعها المشرع الجزائري لتجريم هذه الأفعال، وإبراز التحديات القادمة للتماشي مع هذا التطور الرهيب في استعمال الذكاء الاصطناعي للنصب على الأفراد .

أسباب اختيار الموضوع: وقد تم اختيار دراسة هذا الموضوع لأسباب ذاتية وأخرى موضوعية، تتمثل الأسباب الذاتية في الاهتمام الشخصي بالجرائم السيبرانية المستحدثة والمتصلة بتكنولوجيات الإعلام والاتصال، وكذا الرغبة في مواكبة التحديات التي يفرضها العالم الرقمي الحديث، وتكوين معرفة قانونية وتقنية حول الإجرام المعلوماتي، أما الأسباب الموضوعية فتتمثل في التزايد الرهيب لانتشار هذه الجريمة من خلال استغلال الوسائط الرقمية من طرف المجرمين للنصب على الضحايا الذين يجهلون الطرق السليمة في المعاملات المالية واستعمالها بطريقة عشوائية.

الدراسات السابقة: من خلال بحثنا واطلاعنا لم نجد دراسة مقاربة لهذا الموضوع إذا ما استثنينا أطروحة لنيل شهادة دكتوراه تحت عنوان: جريمة الاحتيال الإلكتروني، من إعداد الطالبة قراوي كلثوم، جامعة الجزائر **01** ، ولكننا لا ننكر وجود دراسات في مجال النصب والاحتيال الالكتروني إلا أنها أكثر شمولية، لذلك حاولنا أن تكون دراستنا أكثر تخصصا، إذ اقتصرنا على تقنية إلكترونية واحدة وهي الذكاء الاصطناعي .

صعوبات الدراسة: أبرز الصعوبات في إنجاز البحث قلة الدراسات السابقة لهذا الموضوع المستحدث، ومحدودية الاجتهادات القضائية والتشريعات الخاصة بهذا النوع من الجرائم في بعض الأنظمة القانونية، و كذا تداخل المجال القانوني مع المجال التقني خاصة أن هذه الأفعال مستجدة بالنسبة للمشرع الجزائري على غرار باقي دول العالم مما يستوجب التفصيل للربط بين الجوانب التقنية والقانونية لفهم مختلف أبعاد الظاهرة محل الدراسة .

وهذا ما قادنا لطرح الإشكالية التالية: **كيف تعامل المشرع الجزائري مع جرائم النصب والاحتيال الالكتروني المستحدثة بتقنية الذكاء الاصطناعي ؟**

هذه الاشكالية تتفرع لأسئلة فرعية:

01- ما مفهوم جرائم النصب الالكترونية ؟

02- تمييز جرائم النصب والاحتيال عن بعض الجرائم الشبيهة بها ؟

03- تبيان الأطر القانونية والتقنية في الجزائر لحماية المعاملات المالية للأفراد والمؤسسات من النصب عبر الانترنيت؟

المنهج المتبع: اعتمدت على منهجين في هذه الدراسة، **المنهج الوصفي:** لأنه الأكثر ملاءمة للتعريف بالجريمة، وأركانها وخصائصها، والعمل على وصف المفاهيم التقنية والقانونية التي تستوجب الشرح، وكذا التحديات التي تواجه المشرع وفقهاء القانون لمواكبة هذا التطور التكنولوجي

ومحاربة الجرائم التي تقع في العالم الافتراضي، كما تم الاعتماد على **المنهج التحليلي:** لدراسة وتحليل النصوص القانونية المجرمة والمعاقبة لجريمة النصب المتصلة بتكنولوجيات الإعلام والاتصال.

وللإجابة على هذه الاشكالية قسمنا دراستنا إلى فصلين، تطرقنا في **الفصل الأول** إلى ماهية جريمة النصب والاحتيال عبر الفضاء الرقمي، وقسمناه إلى مبحثين **المبحث الأول** تطرقنا فيه لمفهوم جريمة النصب والاحتيال وخصائصها، والثاني تناولنا فيه أركان جريمة النصب الإلكتروني وأنواعها، وجاء **الفصل الثاني** بعنوان استغلال تقنية الذكاء الاصطناعي في جريمة النصب وآليات مكافحتها، قسم إلى مبحثين الأول ركزنا من خلاله على الآليات التقنية لأنماط جريمة النصب وتمييزها عن الجرائم الشبيهة بها في القانون الجزائري، والثاني تضمن الأطر القانونية والتقنية لمكافحة الاحتيال الإلكتروني في التشريع الجزائري .

الفصل الأول:

ماهية جريمة النصب والاحتيال عبر الفضاء الرقمي

الفصل الأول: ماهية جريمة النصب والاحتيال عبر الفضاء الرقمي

تشكل التكنولوجيا الحديثة ركيزة أساسية في المعاملات اليومية للإنسان، حيث وفرت الوقت والجهد وحولت العديد من العمليات إلى عالم رقمي، إلا أن هذه الإيجابيات تقابلها مخاطر قد تلحق ضرر جسيم بالأفراد والمؤسسات للاستيلاء على أموالهم أو الحصول على خدمة باستعمال التكنولوجيات الحديثة بطريقة غير مشروعة، حيث أصبحت جل التعاملات المالية تتم عبر شبكة الأنترنيت، مما يعرض الإنسان للوقوع ضحية لهؤلاء النصابون الذين يستغلون الفضاء الرقمي لاصطياد ضحاياهم، ومن خلال هذا الفصل سنتطرق لمفهوم جريمة النصب والاحتيال عبر الفضاء الرقمي (المبحث الأول)، ثم نعرج على أركان جريمة النصب والاحتيال الالكتروني وتبيان أنواعها (المبحث الثاني).

المبحث الأول: مفهوم جريمة النصب والاحتيال الإلكتروني

في ظل التقدم الهائل في وسائل الاتصال، وتغيير الظروف الاجتماعية والاقتصادية برزت هذه الجرائم الإلكترونية التي تتميز عن الجرائم التقليدية، خاصة من حيث الوسيلة المستعملة في النصب، فجريمة النصب قديمة حديثة ومن خلال هذا المبحث سنحاول التطرق لتحريم النصب في الشريعة الاسلامية ثم التعريف الفقهي والتشريعي للنصب والاحتيال (المطلب الأول) ثم نبين خصائص النصب المعزز بتقنية الذكاء الاصطناعي و كذا سمات المجرم الإلكتروني[1] (المطلب الثاني).

المطلب الأول: تعريف جريمة النصب والاحتيال شرعا وقانونا

جريمة النصب والاحتيال نوعا من أنواع الجرائم المنتشرة بكثرة، ورغم هذا الانتشار الواسع لهذه الجرائم إلا أن أغلب التشريعات لم يضعوا تعريفا يوضح معالمها بدقة نظرا لخصوصيتها، وهذه الجريمة ليست حديثة العهد فالشريعة الاسلامية حرمت النصب وهذا ما سنوضحه من خلال

[1] – مأمون سلامة، جرائم النصب المستحدثة الأنترنيت– بطاقات الائتمان – الدعاية التجارية الكاذبة، دار شتات للنشر والبرمجيات، مصر، 2007، ص 33.

دليل تحريمه في القرآن الكريم والسنة النبوية، ثم نتطرق للمقصود بجريمة النصب التقليدي والالكتروني وكذا فقها وقانونا عبر مختلف التشريعات.

الفرع الأول: دليل تحريم النصب في الشريعة الاسلامية

الشريعة الاسلامية ومن خلال القرآن الكريم وكذا السنة النبوية تضمنت أدلة تحرم النصب والاحتيال واعتبرته من قبائح الذنوب التي تخالف الدين الاسلامي ومن أدلة تحريمها ما يلي:

أولا: من القرآن الكريم:

قال الله تعالى: ﴿ **يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ تِجَارَةً عَنْ تَرَاضٍ مِنْكُمْ** ﴾ سورة النساء الآية **29** ، وجه الدلالة أن الآية دليل واضح وصريح على تحريم أكل أموال الناس بالباطل بالنصب والاحتيال عليهم، إلا أن تكون عن طريق التراضي ووفق ما أحله الله عز وجل في التجارة، وقد توسع الشيخ محمد الطاهر بن عاشور في الاستدلال بهذه الآية حيث اعتبرها أصلا من الأصول التي تقوم عليها المعاملات وأحد أهم الدعائم والمرتكزات التي يبنى عليها الاقتصاد، ومما لا شك فيه أن تعاليم الإسلام المقررة في جميع أبواب العقود التجارية، بل في كل المعاملات المالية تقوم على هذا المبدأ الإسلامي السامي[1].

ثانيا: من السنة النبوية:

عنْ أَبي بكْرةَ رضي الله عنه أنَّ رسُول الله ﷺ قَالَ في خُطْبتِهِ يوْم النَّحر بِمنىً في حجَّةِ الودَاعِ:" **إنَّ دِماءَكُم، وأمْوالَكم وأعْراضَكُم حرامٌ عَلَيْكُم كَحُرْمة يومِكُم هَذَا، في شهرِكُمْ هَذَا، في بلَدِكُم هَذَا، ألا هَلْ بلَّغْت** " متفقٌ عَلَيهِ [2].

وجه الدلالة أن في الحديث دلالة واضحة على تحريم أكل أموال الناس ظلما وتعديا بالنصب والاحتيال عليهم، وهو تنويه بشأن حفظ المال، وحافظه وعظم أثر المعتدي عليه، وإن كان ذلك حكم حفظ مال الأفراد، فحفظ مال الأمة أجل وأعظم [3].

---

[1] – الطاهر بن عاشور، التحرير والتنوير، الدار التونسية للنشر، ط5، تونس، 1984، ص 230 .

[2] – أخرجه البخاري، صحيح البخاري، كتاب الحج، باب حجة، رقم 1218، ص609.

[3] – الطاهر بن عاشور، المرجع السابق، ص 230 .

الفرع الثاني: التعريف اللغوي والاصطلاحي لجريمة النصب والاحتيال الالكتروني

للإحاطة بتعريف شامل لجريمة النصب والاحتيال الالكتروني، سنقوم بتعريفها من الناحية اللغوية والاصطلاحية وذلك كالآتي:

أولا: التعريف اللغوي

01/- النصب لغة يرتبط بدلالات المكر والخداع للإيقاع بالضحايا، فالنصب في اللغة هو رفع الشيء وإظهاره، كما جاء بمعنى الخداع والتدليس بقصد الاستيلاء على مال الغير دون وجه حق[1]، أما الاحتيال جاء من التحول والتحيل وكل هذا يدل عند العرب على دقة النظر والقدرة على التصرف، فالمحتال يتصف بالدقة في التصرف والمهارة في استدراج الهدف وهو مأخوذ من الحيلة، ويقصد كذلك التوصل لشيء معين بطريقة خفية تتسم بالخديعة والمكر، ومن ثم فإن كلا المصطلحين يحملان في الدلالة اللغوية استخدام غير مشروع للاستيلاء على مال أو حق الغير والإضرار بهم[2].

02/- أما النصب والاحتيال الإلكتروني لغة مركبة من " نصب واحتيال " و" إلكتروني " وتعني بذلك صورة حديثة من صور النصب تُرتكب باستعمال الوسائل الإلكترونية وشبكات الاتصال الرقمية، وتقوم على الخداع واستخدام طرق احتيالية وتدليسية للحصول على مال أو منفعة أو بيانات ذات قيمة من خلال استخدام مواقع الإنترنت أو البريد الإلكتروني أو تطبيقات التواصل المختلفة، فالنصب الإلكتروني هو كل سلوك احتيالي يُمارس عبر الوسائط الإلكترونية بهدف تحقيق منفعة غير مشروعة على حساب الغير[3].

[1] - عبد العزيز بن عبد الرحمان الشمري، جريمة النصب والاحتيال، مجلة العدل، عدد 39، وزارة العدل السعودية، 2000، ص 175 .

[2] - بهنام رمسيس، قانون العقوبات، الجرائم المضرة بالمصلحة العمومية ، دار المعارف، مصر، 1966، ص 1230.

[3] - علي عبيد، ناصر موفق وآخرون، ماهية جريمة الاحتيال الإلكتروني، مجلة كلية القانون والعلوم السياسية، مجلد 05 العدد19، جامعة تكريت، العراق، 2016، ص 338.

ثانيا: التعريف الاصطلاحي

هنا وجب التطرق للتعريف الاصطلاحي للنصب والاحتيال التقليدي ثم الالكتروني باعتباره جريمة مستحدثة:

01/- النصب والاحتيال التقليدي:

جاء في بعض التشريعات ومن بينها القانون المصري أنه: " الاستيلاء على مال مملوك للغير بطريقة احتيالية بهدف تملكه دون وجه حق "[1] ويتخذ هذا الاستيلاء صورة استخدام وسائل أو أساليب خادعة من شأنها إقناع الضحية بإعطاء أو إرسال ماله دون إكراه أو ضغط، نتيجة انخداعه بالمظاهر الكاذبة والمزيفة التي أوقعه في شباكها نسيج الجاني[2]، والذي يكون هناك تواصل مباشر بين الجاني والضحية، ويتضح من خلال هذا التعريف أن الجريمة لا تقتصر على مجرد انتزاع المال، بل ترتكز على عنصر جوهري وهو الحيلة والخداع، وهو الأداة الرئيسية في تنفيذ الجريمة وتحقيق غاية الجاني، وهي تملك مال الغير دون رضاه الحقيقي، وهنا يكون النصاب قد مارس سلوكا احتياليا مباشرا أدى لإيقاع الضحية في وهم وخداع حمله على التصرف في ماله على نحو ما كان ليقوم به لولا تلك الحيلة الغير مشروعة التي أثرت عليه[3] .

02/- النصب والاحتيال الالكتروني:

تعد من الجرائم المستحدثة وتقترن كلمة النصب والاحتيال بـ" إلكتروني " أي الوسيلة المستعملة إلكترونية ومرتبطة باستخدام المعالجة الآلية للمعطيات، مثل التسوق الإلكتروني والشراء عبر مواقع التواصل الاجتماعي، كأن يقوم الجاني بإنشاء صفحات مشابهة لشركات معروفة ويقوم بعرض للبيع عبر الأنترنيت تلك السلع، أين يقوم الضحية بطلب تلك السلعة عن بعد، ثم يطلب منه المجرم الإلكتروني بدفع مبلغ مسبق عبر حسابه البريدي ثم يكمل الباقي عند استلام سلعته، هنا يقع الضحية في شباك النصاب عند إرساله للمبلغ، وفور استلام هذا الأخير إشعار بوصول

[1] – بهنام رمسيس، المرجع السابق، ص 1233 .

[2] – طنطاوي إبراهيم حامد، المسؤولية الجنائية لجرائم النصب والاحتيال، ط2، شركة ناس للنشر، مصر،2003، ص 10.

[3] – عبد العزيز بن عبد الرحمان الشمري، المرجع السابق، ص 177.

المبلغ عبر بريده الإلكتروني يقوم مباشرة بحضر الضحية عبر وسيلة التواصل الاجتماعي أو توقيف حسابه نهائيا، محاولة منه لإخفاء جريمته، وهذه الطريقة في النصب انشرت بكثرة في الآونة الأخيرة من خلال استغلال الوسائل الرقمية لإيهام الضحايا بعمليات مربحة بهدف سرقة أموالهم أو معطياتهم ذات الطابع الشخصي، كما يستعمل النصب الإلكتروني عدة أشكال من الاحتيال كإرسال رسالة مفبركة أو اتصال مزيف يطلب معلومات شخصية أو مصرفية، أو إنشاء مواقع لشركات معروفة واستغلال اسمها التجاري للنصب[1] .

الفرع الثالث: التعريف الفقهي لجريمة النصب والاحتيال والإلكتروني

بعد تطرقنا للتعريف اللغوي والاصطلاحي للنصب والاحتيال التقليدي وكذا الإلكتروني، نعرج على تعريف فقهاء القانون لهذه الجريمة خاصة أنها جريمة كانت تقليدية، ثم أصبح الفضاء السيبراني مسرحا لتنفيذها، فالتعريفات الفقهية تلاحظ وجود اختلاف بين النصب والاحتيال التقليدي والالكتروني من حيث الوسائل الخداعية المستعملة من طرف الجاني، حيث تغيرت مع التطور التكنولوجي وعليه وجب علينا التطرق لتعريف فقهاء القانون لهذه الجريمة التقليدية ثم الإلكترونية.

أولا/- النصب والاحتيال التقليدي:

يرى فقهاء القانون أن جريمة النصب والاحتيال التقليدية تعد من الجرائم الخطيرة التي تمس الذمة المالية للأفراد وتهدد الثقة في التعاملات المدنية والاقتصادية، ويقصد بالنصب كما يراه الطرح الفقهي: "كل فعل احتيالي يصدر عن الجاني بهدف الاستيلاء على مال مملوك للغير دون وجه حق، ذلك عن طريق استعمال وسائل تدليسية تتمثل في الكذب المقترن بمظاهر خارجية أو وقائع وهمية توهم المجني عليه بصدق ما يدعيه الجاني، مما يدفعه بمحض إرادته إلى تسليم المال " [2] .

[1]- علي عبيد، ناصر موفق وآخرون، المرجع السابق، ص 340 .

[2] - أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، جرائم ضد الاشخاص وجرائم ضد الأموال، ج 1، ط 10، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص 312، ص 324 .

ويشترط في هذا السلوك الإجرامي أن يكون الغرض منه تملك المال وليس حيازته مؤقتا فقط وهو ما يميز النصب عن جرائم أخرى مثل خيانة الأمانة، كما عرفه فقهاء آخرون بأنه:" سلوك ينطوي على استخدام وسائل غير مشروعة كإخفاء الحقيقة أو تقديم بيانات كاذبة، بقصد خداع الغير وحمله على القيام أو الامتناع عن عمل يترتب عليه إلحاق ضرر مادي أو معنوي بالضحية وتحقيق منفعة للجاني أو للغير[1]، وتعد المناورة والخداع من خصائص هذه الجريمة كونها تمارس بطرق ذكية ومقنعة تضعف من قدرة المجني عليه على التحقق أو الشك .

ثانيا: النصب والاحتيال الإلكتروني:

يرى الفقهاء أن جريمة النصب والاحتيال الإلكتروني تمثل صورة مستحدثة من جريمة النصب والتي تقع على مال منقول مملوك لشخص معين بغرض الاستيلاء عليه بدون وجه حق وذلك باستعمال نوع من الذكاء و الفطنة [2]، فهو سلوك إيجابي غير مشروع ومتعمد يهدف بموجبها المحتال الالكتروني الحصول على شيء ذو قيمة مادية أو معنوية وتكون الوسيلة المستعملة إلكترونية أو معالجة آلية للمعطيات وأنظمته لازمة لارتكاب هذه الجريمة، كما أن الأموال محل النصب الإلكتروني تكون رقمية و يتحصل عليها الجاني إلكترونيا وليس مباشرة من يد الضحية .

الفرع الرابع: التعريف التشريعي لجريمة النصب والاحتيال الإلكتروني

بعد تطرقنا للتعريف اللغوي والاصطلاحي ثم الفقهي لجريمة النصب والاحتيال، يقتضي المنهج العلمي أن نتناول هذه الجريمة من الزاوية القانونية و موقف التشريعات الوضعية منها، لأن تحديد المفهوم بدقة لا يكتمل إلا من خلال تبيان ذلك، لما لها من أثر في فهم الجريمة وكيفية تطبيق النصوص القانونية المتعلقة بها.

[1] – عبيد علي، ناصر موفق وآخرون، المرجع السابق، ص 337 .

[2] – هاشمي جبراني، جريمة الاحتيال في مواقع التواصل الاجتماعي، مجلة الحقوق والعلوم السياسية، جامعة مولاي الطاهر سعيدة، الجزائر، المجل 18، العدد03، 2025، ص 600 .

أولا/- التشريع الجزائري

نص المشرع الجزائري نص في المادة **372** من قانون العقوبات كما يلي: " كل من توصل إلى استلام أو تلقى أموالا أو منقولات أو سندات أو تصرفات أو أوراقا مالية أو وعودا أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه، إما 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 أي شيء منها ، يعاقب بالحبس من سنة **(1)** إلى خمس **(5)** سنوات وبغرامة من **100.000** دج إلى **500.000** دج، وإذا وقعت الجنحة على مجموعة تزيد عن ثلاثة **(3)** أشخاص، فيجوز أن تصل مدة الحبس إلى عشر **(10)** سنوات والغرامة إلى **1.000.000** دج، و في جميع الحالات، يجوز أن يحكم علاوة على ذلك على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة **9** مكرر **1** من هذا القانون وبالمنع من الإقامة وذلك لمدة سنة **(1)** إلى خمس **(5)** سنوات على الأكثر "[1] .

من خلال نص المادة **372** المشرع الجزائري يشترط أن تكون هذه الطرق الاحتيالية تأثر على إرادة الضحية بصفة مباشرة بتسليم ماله، هذا ما يعكس اعتداد المشرع الجزائري بالوسيلة الاحتيالية كعنصر لقيام جريمة النصب، كما جاءت نص المادة عامة فلم يخصص المشرع الجزائري استخدام وسائل الكترونية في عملية النصب، بل جرم كل الطرق الاحتيالية مثل استعمال صفات أو أسماء كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو إحداث آمال وهمية للاستيلاء على أموال الغير، وهذا ما يمكن إسقاطه على الطرق الاحتيالية المرتكبة باستعمال الوسائط الرقمية.[2]

[1] – المادة 372 من الأمر رقم:66-156 المؤرخ في:18 صفر عام 1386 الموافق لـ:08 يونيو 1966 المتضمن قانون العقوبات (الجريدة الرسمية عدد49 سنة 1966) المعدل والمتمم بالقانون رقم24-06 المؤرخ في28 أبريل سنة 2024 (الجريدة الرسمية العدد 30 لسنة 2024).

[2] – قراوي كلثوم، جريمة الاحتيال الإلكتروني، أطروحة لنيل شهادة الدكتوراه علوم القانون العام، جامعة الجزائر 01، 2025/2024 ص 36 .

ثانيا: التشريع المصري

عرفها المشرع المصري بأنها :" متى توصل الجاني إلى الاستيلاء على مال مملوك للغير باستخدام طرق احتيالية، من بينها اتخاذ اسم كاذب أو صفة غير صحيحة، أو عن طريق إيهام الضحية بوجود مشروع وهمي أو واقعة مزورة أو إقناعه بتحقيق ربح خيالي " ويفهم من هذا النص أن المشرع المصري قد ربط قيام الجريمة ووجود وسيلة تدليسية يتبعها الجاني بهدف التأثير على إرادة المجني عليه ودفعه إلى تسليم المال طواعية، معتقدا صحة الادعاءات المقدمة، فالخداع ليس مجرد عنصر شكلي بل هو ركن جوهري في بناء الجريمة ويجب أن يكون هو السبب المباشر والدافع الحقيقي لتصرف المجني عليه، ما يجعل الركن المادي للجريمة يقوم على الفعل الاحتيالي المصحوب بالنية الإجرامية [1].

ثالثا: التشريع الفرنسي

عرفتها المادة **313-1** أن جريمة الاحتيال ترتكب عندما " يقوم الجاني بخداع شخص طبيعي أو اعتباري باستخدام اسم كاذب أو صفة غير صحيحة أو عن طريق استغلال صفة حقيقية أو باستخدام وسائل احتيالية مما يدفع هذا الشخص إلى تسليم أموال أو ممتلكات أو تقديم خدمات أو قبول التزام أو إبراء ذمة مما يسبب له أو لطرف ثالث ضررا " [2] ويعاقب عليها بالسجن لمدة تصل إلى خمس سنوات وغرامة مالية.

المشرع الفرنسي يركز على عنصر الخداع كركن أساسي في جريمة النصب، ويشترط أن يكون الخداع والسبب المباشر لتخلي الضحية عن ماله للجاني أو تقديم خدمة أو الرضوخ إلى التزام، هذا ما يبرز النية الإجرامية والطرق الاحتيالية في قيام الجريمة.

التشريعات السالفة الذكر لم تنص صراحة على النصب والاحتيال عبر الفضاء السيبراني بل يعد شكلا من أشكال الاستغلال والخداع الذي ينفذ من مجرمين ذوي خبرة، فوسائل النصب

[1] – لحسين بن الشيخ، مذكرات في القانون الجزائي الخاص: جرائم ضد الأشخاص – جرائم ضد الأموال – أعمال تطبيقية، دار هومة للنشر، الجزائر، 2005، ص 187 .

[2] – المرجع نفسه، ص 187 .

الاحتيالية التقليدية تغيرت مع التطورات التكنولوجية الحديثة فأصبح المحتالون يستغلون المجال التقني للإيقاع بضحاياهم في فخ افتراضي للاستيلاء على أموالهم أو معطياهم ذات الطابع الشخصي لتحقيق أرباحا سريعة بطرق غير مشروعة [1].

المطلب الثاني: خصائص النصب بتقنية الذكاء الاصطناعي وسمات المجرم الالكتروني

إن تنامي اعتماد الأفراد والمؤسسات المالية المصرفية على المنظومات الرقمية الذكية، قابله انفتاح ثغرات جديدة يستغلها المجرمون بتوظيف وسائل إلكترونية على غرار تقنيات الذكاء الاصطناعي في ممارسة أنشطتهم الاجرامية والغير مشروعة، محولين هذه التقنية سلاح لتنفيذ جرائم الاحتيال الرقمي والاختراقات المصرفية، وعليه سنتطرق لمفهوم تقنية الذكاء الاصطناعي (الفرع الأول)، ومجالات استخدام هذه التقنية، لنعرج على خصائص جريمة النصب والاحتيال الالكتروني والتي تختلف عن التقليدية، كونها أصبحت ترتكب في الفضاء السيبراني ويصعب تتبع آثارها الرقمية، ويمكن أن تتعدى الحدود الجغرافية (الفرع الثاني)، ثم سنحاول تبيان صفات المجرم الالكتروني بالتفصيل والذي يتسم بالذكاء والتحكم في الوسائل التقنية (الفرع الثالث) .

الفرع الأول: تعريف تقنية الذكاء الاصطناعي intelligence Artificial

لقد أصبح من المُسلّم به اليوم أن الذكاء الاصطناعي أصبح يستغل في تسهيل ارتكاب طائفة واسعة من الجرائم المالية، الأمر الذي يزيد من صعوبة اكتشافها من قِبَل الأجهزة المختصة، فضلًا عن ابتكار أساليب احتيالية جديدة تستهدف الأفراد والمؤسسات، مما يُضاعف من تعقيدات التصدي لهذه الجريمة السيبرانية.

منذ اختراع أجهزة الكمبيوتر زادت قدرتها على أداء المهام المختلفة بشكل كبير حتى أن البشر طوروا قوته من حيث مجالات العمل المتنوعة الخاصة بهم لزيادة سرعتها وتقليل الحجم مع احترام الوقت، ومن أهم ما توصل إليه البشر من تطور في هذا المجال الذكاء الاصطناعي [2].

[1] – قراوي كلثوم، المرجع السابق، ص 37 .

[2] – عادل عبد النور ، أساسيات الذكاء الاصطناعي، ط01، دار الفيصل الثقافية، السعودية، 2005، ص 244 .

وضع الفقهاء والباحثون في مجال الإعلام الآلي تعريفات مختلفة لمصطلح الذكاء الاصطناعي، هناك من عرفه بأنه:" أنظمة وأجهزة تقوم بمحاكاة الذكاء البشري في أداء المهام وبإمكانها التحسين والتطوير من نفسها استنادا إلى المعلومات التي تجمعها " أي أنه الذكاء الذي تبديه الآلات والبرامج بما يحاكي القدرات الذهنية البشرية وأنماط عملها [1].

وفي تعريف آخر: هو أجهزة ونظم كمبيوتر مصممة للعمل بطريقة يمكن اعتبارها ذكية، وتتضمن الأنماط التكنولوجية التي تحاكي الأداء البشري من خلال التعلم والتوصل لاستنتاجاتها الخاصة عبر فهم المحتويات المعقدة والانخراط في حوارات مع الانسان وتعزيز الأداء المعرفي البشري في تنفيذ المهام الروتينية وغير الروتينية على حد سواء [2]، أي أنه قدرة الآلة على أداء الوظائف المعرفية التي نربطها بالعقول البشرية مثل الإدراك والاستدلال والتعلم والتفاعل مع البيئة وحل المشكلات وحتى ممارسة الإبداع.

كما يرى فقهاء آخرون: أنه استخدام التكنولوجيا لأتمتة المهمات التي عادة ما تحتاج إلى الذكاء البشري أي يعتقد بأنها تتضمن الذكاء عندما يؤديها الأشخاص، فبرامج الذكاء الاصطناعي مصممة بالضرورة لمطابقة البشر ذوو المهارات العالية مثل القدرات والتفكير المجرد وفهم المفاهيم، مهارات حل المشكلات العامة وغيرها من الوظائف الأخرى المرتبطة بالذكاء البشري، إذن رؤية الذكاء الاصطناعي تتضمن آلات تفكير ذات قدرات تلبي أو تتجاوز الإدراك على مستوى الإنسان [3].

كما عرفه البعض الآخر: أنه الذكاء الذي يصدر عن الإنسان بالأصل ثم يمنحه للآلة أو الحاسوب، فهو علم يعرف على أساس هدفه وهو جعل الآلات أو منظومات الحاسوب تعمل أشياء تحتاج للذكاء[4]، وبالنظر إلى الطبيعة متعددة التخصصات يمكن تعريف الذكاء الاصطناعي أنه:"

---

[1] – عادل عبد النور ، المرجع السابق، ص 244 .

[2] – كاظم أحمد، الذكاء الاصطناعي، جامعة الامام جعفر الصادق، العراق، 2012، ص 04 .

[3] – Artificial intelligence,eng,oxford living dictionaries, https://perma.cc/WF9V-YM7C,consult 09/05/2026 15 :32

[4] – ياسين سعد غالب، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، ط01، دار المناهج للنشر والتوزيع، الأردن، 2012، ص 114 .

هو مجال علمي تلاقى فيه التخصصات المختلفة بما فيها الرياضيات والفلسفة وعلم الأعصاب وعلم النفس وغيرها، بهدف إنشاء عوامل لديها القدرة على التعلم لإنشاء نماذج من تعلمهم لعمل التنبؤات على تلك النماذج والبيانات الجديدة، ثم اتخاذ قرارات مستقلة أو المساعدة في صنع القرار البشري بناء على تلك التنبؤات، فمجال واحد أو أكثر من هاته المجالات أو غيرها يمكنه المساهمة في بناء نظام ذكي "[1] .

أما فيما يخص الجانب القانوني فلا نجد تعريفا قانونيا صريحا للذكاء الاصطناعي، ولكن تم تقديم مسودة حديثة بشأن الذكاء الاصطناعي من قبل المفوضية الأوروبية فتم تعريفه في المادة الثالثة:" أنه برمجيات تم تطويها بواحدة أو أكثر من التقنيات أو الأساليب والمناهج القائمة على المنطق والمعرفة[2]" ، ويمكن بالنسبة لمجموعة معينة من الأهداف التي يحددها الإنسان توليد مخرجات مثل المحتوى أو التنبؤات أو التوصيات أو القرارات التي تؤثر على البيانات التي يتفاعلون معها[3] .

وتركز برمجة الذكاء الاصطناعي على ثلاثة جوانب معرفية:

-عمليات التعلم: يهتم هذا الجزء من برمجة الذكاء الاصطناعي بجمع البيانات وإنشاء قواعد لتحويلها إلى معلومات مفيدة.

-عمليات التفكير: يهتم هذا الجزء من برمجة الذكاء الاصطناعي بجمع وتحليل البيانات واختيار أفضل خوارزمية لتحقيق النتيجة المرجوة .

-عمليات التصحيح الذاتي: اتخاذ القرارات بناء على عملية تحليل البيانات السابقة [4].

---

[1] – عادل عبد النور، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم التقنية والنشر، السعودية، 2005، ص 07 .

[2] – ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، ط 01، دار النهضة العربية، مصر، 2020، ص 05 .

[3] – عبد الله محمد أبو تجار، المسؤولية عن مخاطر تقنيات الذكاء الاصطناعي، ط01، مؤسسة المعرفة لنشر وتوزيع الكتب، مصر،2024، ص 26 .

[4]– محمد علي الشرقاوي، الذكاء الاصطناعي والشبكات العصبية، المكتب المصري الحديث للنشر، مصر، 1998، ص 35-36

الفرع الثاني : مجالات استخدام الذكاء الاصطناعي

الذكاء الاصطناعي أصبح يستخدم في مجالات مختلفة نذكر أهمها:

أولا: خوارزميات البحث والتوصية

تعمل أنظمة التوصية الذكية هذه على تحليل نشاطنا وتفضيلاتنا عبر الانترنيت لتزويدنا بمحتوى مماثل، يتم الحصول على البيانات من الواجهة الأمامية وحفظها كبيانات كبيرة وتحليلها باستخدام التعلم الآلي والتعلم العميق، بعد ذلك يمكنه توقع تفضيلاتك وتقديم اقتراحات لإبقائك مستمتعا دون الحاجة إلى البحث عن شيء آخر[1].

ثانيا: وسائل التواصل الاجتماعي

تستخدم العديد من تطبيقات الوسائط الاجتماعية الذكاء الاصطناعي للمساعدة في تزويد المستخدمين بميزات ممتعة، فقد تكتشف الشبكات الاجتماعية نوع المحتوى الذي يحبه المستخدم ويوصي بمحتوى مشابه وتعد خوارزميات الذكاء الاصطناعي أسرع بكثير من البشر في اكتشاف وإزالة الرسائل مثلا التي تحتوي على كلام يحرض على الكراهية [2].

ثالثا: أنترنيت الأشياء

تعتمد على فكرة ايصال جميع الآلات والأجهزة المادية من حولنا بشبكة الانترنيت من خلال تقنيات ذكية ورقائق مدمجة ملحقة بهذه الأشياء، بحيث تكون هذه الأشياء قادرة على التواصل فيما بينها بطريقة تمكنها من تبادل البيانات، واتخاذ القرارات وحتى اصبح اليوم الانترنيت بمثابة الروح التي تبث في هذه الأجهزة الصماء والآلات الجامدة لتجعلها تحس وترى وتسمع وتسجل وتتواصل وتتفاعل من خلال برمجيات ذكية تحكم عملها[3].

---

[1] – فهد آل قاسم، الذكاء الاصطناعي، كتاب إلكتروني، ص 17 ، اطلع عليه بتاريخ:2026/05/09 الساعة:22:11 .عبر الرابط: https://www.moswrat.com/books_download_10231.html .

[2] – المرجع نفسه، ص 19 .

[3] – إيهاب خليفة، أنترنيت الاشياء– تهديدات أمنية متزايدة للأجهزة المتصلة بالأنترنيت– ، مجلة اتجاهات الأحداث الصادرة عن مركز المستقبل للأبحاث والدراسات المتقدمة، العدد 19– الامارات العربية المتحدة ، 2017، ص 59 .

رابعا: كشف الوجه والتعرف عليه

يمثل استخدام ميزة التعرف على الوجه لفتح الهواتف وتوظيف المرشحات الافتراضية أثناء التصوير، نموذجين تطبيقيين للذكاء الاصطناعي، وتعتمد هذه التقنية على خصائص مميزة للوجوه البشرية، إذ يتم تدريب الآلات الذكية على التعرف على إحداثيات الوجه بدقة، وإلى جانب الاستخدامات الفردية، تعتمد المنشآت الحكومية والمطارات على تقنية التعرف على الوجوه في مهام المراقبة والأمن [1].

الفرع الثالث: خصائص جريمة النصب والاحتيال المعزز بتقنية الذكاء الاصطناعي

نظراً لتطور جريمة النصب والاحتيال الالكتروني باستمرار، واستغلال المجرمين للوسائل الحديثة لتنفيذ أفعالهم عن بعد على غرار تقنية الذكاء الاصطناعي، صارت الحاجة ملحة لاستعراض الخصائص التقنية لهذه الجريمة المستحدثة:

أولا: ترتكب عبر الحاسوب في بيئة رقمية

حيث يتم ارتكاب هذه الجريمة الإلكترونية في الفضاء السيبراني عبر شبكة الأنترنيت، باستخدام إشارات إلكترونية غير ملموسة تتنقل بين الأنظمة المعلوماتية، وتعتمد هذه الجريمة بشكل أساسي على استغلال الثغرات ونقاط ضعف البنية التحتية الرقمية وتكنولوجيا المعلومات[2]، كما يمكن الولوج إلى الشبكة الدولية للمعلومات لتنفيذ عمليات الاحتيال بشتى أنواعها، مما يجعل هذه الجريمة مرتبطة بالتكنولوجيا وتحاكي الذكاء البشري من خلال التعلم ثم المحاكاة، ليصبح الفعل المجرم مرتبط بذكاء اصطناعي، ولا يمكن ممارستها إلا من خلال وسيط إلكتروني [3] .

[1] – إيهاب خليفة، المرج السابق، ص 60 .

[2] – عرب يونس، موسوعة القانون وتقنية المعلومات: جرائم الكمبيوتر والأنترنيت، ج01، اتحاد المصارف العربية للنشر، 2002، ص 234.

[3] – الخن محمد طارق، جريمة الاحتيال عبر الأنترنيت (الاحكام الموضوعية والأحكام الإجرائية)، ط01، منشورات الحلبي الحقوقية، 2011، ص 68 .

ثانيا: التخفي وصعوبة اكتشافها

تتميز جريمة النصب والاحتيال الإلكتروني بطابعها الخفي، حيث يعتمد المحتال على خبرته التقنية العالية لإتمام عملية النصب بسرعة، كسرقة معطيات ذات طابع شخصي خاصة التي يمكن من خلالها الولوج لتطبيقات أو حسابات بريدية أو بنكية، أو تحويل تلك البيانات وطلب فدية من الضحية[1] ، كونها تستغرق وقتا طويلا قبل اكتشافها، وغالبا لا يكشف عنها إلا عبر عمليات خبرة تقنية دقيقة من طرف رجال الضبطية القضائية المختصين في الجرائم السيبرانية، وعلى الرغم من ذلك إلا أنها تعد بسيطة من الناحية النظرية، حيث يمكن لهذا المحتال الإلكتروني الذي يمتلك مهارات تقنية أن ينفذ جريمته بسهولة للإيقاع بالضحية في شباكه [2].

ثالثا: عابرة للحدود الوطنية

لكون الطابع العالمي لشبكات المعلومات لم تعد هناك حدود جغرافية تشكل عائقا أمام ارتكاب جريمة احتيال إلكترونية والتي تحدث آثارا متزامنة في مناطق متعددة من العالم[3]، كما تُرتكب هذه الجرائم الرقمية داخل فضاء إلكتروني عبر شبكة الإنترنت، حيث تعتمد على نبضات إلكترونية غير محسوسة تتدفق بين النظم المعلوماتية، ويقوم أساس هذه الجريمة على استغلال الثغرات الضعيفة في البنية التحتية الرقمية وتقنيات المعلومات، كما يُمكن التسلل إلى الشبكة الدولية لتنفيذ عمليات احتيال بأنماط متعددة، مما يجعل هذه الجريمة مرتبطة حتمًا بالتكنولوجيا.

رابعا: استهداف مؤسسات حساسة ذات طابع مالي

بما أن البنوك والمؤسسات الصناعية والمتاجر الإلكترونية تمتلك قيمة مالية كبيرة ويسهل اختراقها إلكترونيًا، فهي أكثر عرضة لعمليات الاحتيال الرقمي، لذلك تسعى هذه المؤسسات إلى تعزيز أنظمتها الأمنية بحلول تكنولوجية متطورة للتقليل من الخسائر المحتملة، حيث اصبح الذكاء

---

[1] – إبراهيم حسني عبد السميع، الجرائم المستحدثة عن طريق الأنترنيت: دراسة مقارنة بين الشريعة والقانون، دار النهضة العربية للنشر، مصر، 2011، ص 133 .

[2] - منشاوي محمد عبد الله، جرائم الأنترنيت من منظور شرعي وقانوني، السعودية ،2002 ، ص 123 .

[3] – جميل الصغير عبد الباقي، الأنترنيت والقانون الجنائي: الأحكام الموضوعية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية للنشر، مصر،2002، ص 123 .

الاصطناعي يستعمل كوسيلة مضادة للكشف عن محاولات النصب من خلال استعمال هذه التقنية عبر خوادم المؤسسات وكذا مواقعها الرسمية وحتى كاميرات المراقبة داخل المؤسسات [1].

الفرع الرابع: سمات المجرم الإلكتروني

إن المجرم الذي يرتكب فعلا غير مشروع، ويتعدى فيه على حقوق الغير يعتبر في نظر القانون مجرما ويتعرض للعقاب، فالمجرم المعلوماتي كغيره من المجرمين يتحمل العقاب في حال اكتشاف جريمته الإلكترونية، فهذا المجرم الذي يرتكب جرائمه باستعمال تقنيات الإعلام الآلي وعلى قدر من المستوى التعليمي والذكاء[2] يكون إنسانا اجتماعيا ويمارس جميع حقوقه بصفة عادية، وهذه الصفات نتطرق لها كما يلي:

أولا: المجرم المعلوماتي مجرم ذكي محترف

تختلف جريمة الاحتيال الإلكتروني عن التقليدي، لكون المجرم في هذه الجريمة يتميز بذكاء وعلى دراية بالأسلوب المستخدم في الفضاء الرقمي، وكيفية الحصول على المعلومات التقنية لاستغلالها في عمليات الاحتيال[3] ، فالضبطية القضائية تعتمد على خبراء في الجرائم المعلوماتية عند وقوع هذا النوع من الجرائم لتتبع الأثر الرقمي لهذا المجرم المحترف، الذي يعمد إلى إخفاء الأدلة التقنية لجريمته كالتشفير[4]، أو من خلال استعمال تقنيات متعددة لتسهيل ارتكاب جريمته أو تعديل بيانات رقمية في وقت قياسي قصير، فهو يحقق أهدافه بهدوء فيطلق عليه اسم المجرم المتخصص .

[1] – عرب يونس، المرجع السابق، ص 238.

[2] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنيت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي للنشر، مصر، 2013، ص 38.

[3] – طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2009، ص 586.

[4] – المرجع نفسه، ص 586 .

ثانيا: المجرم المعلوماتي غير عنيف

المجرم المعلوماتي من المجرمين الذين لا يلجؤون إلى العنف إطلاقا في تنفيذ جرائمهم، لأنه ينتمي إلى إجرام الحيلة فهو لا يلجأ إلى العنف كونه ذكي ومتكيف اجتماعيا ولا يواجه عند ارتكابه هذه الجرائم شخصا حقيقيا، بل يواجه شخصا اعتباريا، كما يتمتع بالمهارة والمعرفة، فغالبا يكون مسالم وبشوش، بينما يكون خطير في العالم الافتراضي[1].

ثالثا: المجرم المعلوماتي على قدر كبير من المعرفة التقنية

المؤهل العلمي والمعرفة في مجال الاعلام الآلي والتطبيقات الإلكترونية من أهم سمات المجرم المعلوماتي، مما يجعله يختار مسرح جريمته عن بعد ودون ظهوره شخصيا في مكان جريمته، مما يصعب توقيفه فور ارتكاب احتياله أو تلقيه مبالغ مالية نتيجة نصبه، وبالتالي يكون له الوقت الكافي لمحاولة إخفاء الأدلة التي تورطه في جرمه [2].

رابعا: القدرة على التمثيل والحاجة لإثبات الذات

النصاب يتمتع بقدرة على رسم الأدوار المختلفة وتبرز له غريزة الحاجة لإثبات ذاته، وهو ما يبرزه كونه لا ينشد المكسب المادي فقط من وراء عملية النصب التي يقوم بها، ويعلل هذا بأن المحتال عادة ما ينتمي إلى الطبقة المتوسطة أو الدنيا في المجتمع [3]، ويجد في نفسه رغبة ملحة في الارتقاء إلى الأعلى والانتماء إلى الطبقة الغنية .

المبحث الثاني: أركان جريمة النصب والاحتيال الالكتروني وأنواعها

جريمة النصب والاحتيال الالكتروني لا تختلف عن أي جريمة تقليدية مقررة عن طريق القانون الجنائي، حيث أنها تتطلب لقيامها الأركان المتفق على ضرورة تحققها في أي جريمة، فالركن الشرعي الذي يعتبر شرط مبدئي فإنه يستلزم وجود ركن مادي لفعل غير مشروع يرتكبه الجاني

[1] – غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم خلال مؤتمر علمي بعنوان القانون والكمبيوتر والأنترنيت، كلية الشريعة والقانون، جامعة الإمارات، 2000، ص 35 .

[2] – عبد الرزاق سند ابراهيم ليلة، سيكولوجية النصاب، دار النهضة العربية للطباعة النشر والتوزيع، لبنان، 1999، ص 30 .

[3] – المرجع نفسه، ص 42 .

يسبب ضررا للغير، وركن معنوي يعبر عن توجه إرادة الجاني الحرة لارتكابه فعله غير مجبرا، مع علمه بسلوكه الإجرامي وكذا النتيجة الإجرامية التي تنجر عن ذلك الفعل، فلكل الأفعال الغير مشروعة ذات الصبغة الجزائية ثلاثة أركان : الركن الشرعي، المادي والمعنوي، (مطلب أول) كما سنتطرق إلى أنواع جرائم النصب والاحتيال الالكتروني (مطلب ثاني).

المطلب الأول: أركان جريمة النصب والاحتيال الالكتروني

يقتضي البناء القانوني لأي جريمة توافر الأركان القانونية اللازمة لنشوئها ووجودها، وتتمثل هذه الأركان أساسا في الركن الشرعي والركن المادي والركن المعنوي.

وعليه، يقتضي البحث في أركان جريمة النصب والاحتيال الالكتروني، تقسيم هذا المطلب إلى ثلاث فروع، خصص أولها لبيان الركن الشرعي، أما الفرع الثاني فلدراسة الركن المادي لجريمة النصب والاحتيال الالكتروني من حيث عناصره وصوره، ثم نتناول في الفرع الثالث الركن المعنوي من خلال دراسة القصد الجنائي اللازم لقيام هذه الجريمة .

الفرع الأول: الركن الشرعي

من المبادئ المتفق عليها في أغلب التشريعات العالمية أنه لتجريم مظهر من مظاهر النشاط للأشخاص سواء كان هذا الفعل أو امتناع عن فعل، لابد من تدخل المشرع بالنص عليه مقدما على هذا التصرف ليعلم الناس النهي عن إتيان الفعل من عدمه وتقرير عقوبة من يقوم بمخالفة النهي أو من يخالف الأمر بالامتناع، وهذا التدخل التشريعي هو ما يعرف بمبدأ شرعية الجرائم والعقوبات، فالنص القانوني من أهم الضمانات المقررة للحرية الشخصية، كما يمكن اعتباره ضمانة هامة لمنع تعسف السلطة القضائية في إنزال عقوبات سالبة للحرية أو غرامات مالية دون رقابة.

الركن الشرعي يمثل الأساس القانوني للتجريم والعقاب في القانون يمثل الاطار العام لتكييف الفعل غير المشروع مع النص الجزائي، وهذا الركن انعكاسا لقاعدة دستورية وقانونية معروف وهي" لا جريمة ولا عقوبة أو تدابير أمن بغير قانون "[1] ، وبالرجوع إلى قانون العقوبات الجزائري

[1] – المادة 43 من الدستور الجزائري، ج ر عدد 82، ص 12، 2020:" لا إدانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرم " والمادة الأولى من قانون العقوبات الجزائري: " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون " .

نجد الركن الشرعي في جريمة النصب والاحتيال هو النص العام الوارد في المادة **372** ، ويقصد بمبدأ الشرعية أنه لا يجوز تجريم فعل لم ينص القانون عليه صراحة، كما لا يجوز توقيع الجاني خلاف العقوبة المقررة في هذا النص القانوني، كما أن ركن الشرعية يخضع لشرطين أساسيين هما: وجود نص يجرم الفعل المرتكب، وعدم خضوع هذا الفعل لسبب من أسباب الإباحة:

أولا: خضوع الفعل لنص التجريم

يقصد بهذا المبدأ القانوني هو اشتراط حصرا خضوع الفعل غير المشروع لنص تشريعي واضح وصريح خاص بالتجريم والعقاب وهي نصوص موجودة في النصوص التشريعية المتمثلة في قانون العقوبات والقوانين الخاصة المكملة .

ثانيا: انعدام أحد أسباب الإباحة

توفر أحد أسباب الإباحة يخرج الفعل المجرم من دائرة التجريم إلى دائرة الإباحة ويمكن اعتبار أسباب الإباحة قيد تقع على نص التجريم فتعطل مفعوله حيث تعطل نص التجريم أو الركن الشرعي للجريمة وتجعل الفعل مباحا، وقد أورد المشرع الجزائري الأفعال المباحة في المادتين **39** و **40** من قانون العقوبات وتتلخص عموما في الأفعال التي أمر أو أذن بها القانون وحالات الدفاع الشرعي [1] .

الفرع الثاني: الركن المادي

الركن المادي في جريمة النصب والاحتيال الالكتروني هو سلوك الجاني في اعتماده على أساليب التدليس والخداع باستخدام وسيلة إلكترونية لتنفيذ الجريمة بغرض الحصول على مال الغير طواعية وبكل رضاه، وكذلك يجب تحقق النتيجة الإجرامية من هذا السلوك مع وجود علاقة سببية بينهما، فإن توفرت هذه العناصر أصبحت الجريمة كاملة تتمثل في سلوك يؤدي لنتيجة ولأنها تحمي مصلحة قانونية تتعلق بملكية المال المنقول، فهذا الركن لا يختلف عن الركن المادي لجريمة السرقة والفارق بينهما ليس إلا عنصر الغش والخداع [2].

[1] – هاشمي جبراني، المرجع السابق، ص 604 .

[2] – جلال ثروت، جرائم الاعتداء على المال المنقول، ج02، دار المطبوعات الجامعية، مصر، 1995، ص 143 .

أولا: النشاط الاجرامي

في جريمة النصب والاحتيال حتى تكون هناك مسؤولية يجب أن يستعمل الجاني التدليس أو الخداع لسلب مال الغير، وهذا ما جاء في نص المادة **372** من قانون العقوبات الجزائري على سبيل الحصر، ولن يكون هناك تدليس ما لم يقم على الكذب والاحتيال والكذب المجرد لا يكفي لتوفير الطريقة الاحتيالية مهما تنوعت صيغته[1] والنشاط الاجرامي هو ممارسة المحتال أساليب لا بد أن تكون محددة لمزاولة عملية النصب والاحتيال طبقا لنص المادة الأولى من قانون العقوبات الجزائري " لا جريمة ولا عقوبة إلا بنص قانوني "، أي أن الكذب لا يكون كافي لوحده لقيام النشاط الإجرامي، بل يجب أن تصاحبه أفعال مادية تجعل الضحية يقع في شباك المحتال ليعتقد بأن تلك الوقائع صحيحة، وذلك عن طريق انتحال صفات أو أسماء كاذبة، أو إيهام الضحية بالفوز بشيء ما أو الفوز بمبلغ مالي، كأن يقوم النصاب بفتح صفحة أو حساب عبر مواقع التواصل الاجتماعي ينشر من خلاله معلوماته الشخصية الانتحالية أو عن مشروعه أو شركته الوهمية ويفتح حساب بنكي ينشر بذات الصفحة، وكل هذا من المظاهر الخارجية الكاذبة التي تؤثر على عقلية وإرادة الشخص والهدف من هذا كسب مال غير مشروع[2] ومن أبرز هذه الوسائل الاحتيالية الرسائل الالكترونية المزيفة **phishing**، أو الاتصالات الهاتفية التي يدعي من خلالها المحتال أنه موظف ببنك أو مركز البريد ويطلب تحديث معلومات بطاقة بنكية، وهذا من أجل النصب على الضحية لسلب ماله، أو يطلب المحتال مساعدة مالية مستعجلة باستعمال وسيلة من وسائل التواصل الاجتماعي ومنتحلا صفة أو هوية كاذبة للإيقاع بضحيته[3] .

[1] – رحال بومدين وسعداني نورة، الحماية الجنائية الواقعة على أموال التجارة الإلكترونية(جريمة السرقة والنصب)، مجلة الواحات للبحوث والدراسات، مجلد 09، العدد2، جامعة غرداية، الجزائر، 2016، ص 100 و 101 .

[2] – أحمد شوقي أبو خطوة، العلاقة بين الجرائم الاحتيالية والإجرام المنظم، ندوة علمية، دار جامعة نايف العربية للعلوم الأمنية للنشر، السعودية، 2007، ص 07.

[3] – رحال بومدين وسعداني نورة، المرجع السابق، ص 100.

ثانيا: النتيجة الاجرامية

عبر المشرع الجزائري عن النتيجة الإجرامية في جريمة النصب والاحتيال بالعبارة:" كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات مالية أو وعود أو مخالصات أو إبراء عن التزامات أو إلى الحصول على أي منها أو الشروع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه" وهنا يقوم الضحية بتسليم ماله للجاني، وهنا تتحقق النتيجة الإجرامية التي كان المحتال يسعى ورائها وهي كسب المال الغير مشروع وبموافقة المجني عليه وهذه الموافقة قائمة على غش وخداع أفقداه الإدراك والتمييز السليم [1]، أما في جريمة السرقة فإن الاستيلاء على مال الغير يكون خلسة أو بالقوة ودون علم أو رضا الضحية.

وتتجلى خطورة هذه النتيجة الإجرامية أن الجاني لا يعتمد على العنف أو التهديد المادي، بل يعتمد على طرق نفسية ومعنوية، مما يجعل الضحية يتصرف بإرادته تحت تأثير الخداع، وهذا ما يجعل القانون يتعامل بأكثر جدية نظرا لما تسببه بمصالح الأفراد وكذلك في فقدان الثقة في المعاملات المالية أو المدنية [2].

ثالثا: العلاقة السببية

المراد بالعلاقة السببية هو ترتب نتيجة " الاستيلاء " بعد النشاط الإجرامي وهو الاحتيال، ولا يكفي لقيام جريمة النصب أن يرتكب الجاني إحدى وسائل الاحتيال المنصوص عليها حصرا في المادة **372** من قانون العقوبات باستيلائه على مال مملوك للغير وإنما يجب أن تقوم علاقة سببية بين وسائل الاحتيال التي استعملها الجاني وسلمه الضحية المال أي يجب أن يكون التسليم قد تم نتيجة لوسائل الاحتيال التي لجأ إليها الجاني[3]، لكن يلاحظ أن انتفاء العلاقة السببية لا يؤدي حتما إلى عدم العقاب وإنما قد تكون الواقعة شروعا في الاحتيال متى توافرت شروطه، مثلا

[1] – أسامة حمدان الرقب، جرائم النصب والاحتيال (الأساليب– المظاهر– العلاج)، ط 01، دار يافا العلمية للنشر والتوزيع، الأردن،2012، ص 63 .

[2]– المرجع السابق، ص 64 .

[3] – نظير فرج مينا، الموجز في الإجراءات الجزائية الجزائري، ط2، ديوان المطبوعات الجامعية، الجزائر،1992، ص 100.

إذا استنفذ الجاني أفعال الاحتيال ولكنها مع هذا لم يحقق النتيجة المبتغاة لسبب لا دخل لإرادة الجاني فيه كتفطن الضحية أو تدخل شخص آخر في وقت مناسب، فهنا نكون بصدد الشروع في النصب لأن أفعال الاحتيال قد بدأ في تنفيذها ولكن خاب أثرها بسبب خارج عن إرادة الجاني.

إذا استعمل الجاني الفضاء الرقمي كوسيلة في النصب، فتتجلى لنا العلاقة عندما يكون المجني عليه ضحية للخداع عبر وسائل التواصل الاجتماعي، كأن يصادف منشور لاقتناء سيارة مع تخفيض في سعرها شرط قيامه بصب مبلغ **10 %** مع إرسال الملف إلكترونيا، ليتم بعدها حضره فور إرساله للمبلغ المالي، فهنا قرار الضحية بإرسال المبلغ لم يكن ليقوم به لولا الطريقة الاحتيالية التي قام بها المحتال باستخدام وسائل إلكترونية، فهنا العلاقة السببية تعد محققة وتقوم أركان الجريمة بأكملها[1].

كما ينبغي التنويه أن إثبات الركن المادي في النصب باستعمال وسائل إلكترونية قد يكون أكثر تعقيدا من النصب التقليدي، وهذا لغياب الاتصال المادي المباشر بين الضحية والمحتال، حيث يلجأ هذا الأخير للفضاء السيبراني لتعقيد تتبعه، وهنا فإن مهمة ضباط الشرطة القضائية المختصين في التحقيق في هذا النوع من الجرائم تتطلب دقة كبيرة في جمع الأدلة الرقمية وربط الوقائع لإثبات الوسيلة الاحتيالية التي كانت السبب الذي دفع الضحية إلى تسليم ماله أو سنداته للجاني.

الفرع الثالث: الركن المعنوي

الركن المعنوي من أهم أركان الجريمة نظرا لارتباطه بشخصية المجرم، فلا يمكن قيام الجريمة بدون توافر الركن المعنوي بعنصريه العلم والإرادة، فهي جريمة عمدية، فمعظم التشريعات تكتفي لقيام هذا الركن بالقصد الجنائي العام أي العلم والإرادة[2]، في حين أن هناك تشريعات تتطلب قصد جنائي خاص وهو نية التملك للمال موضوع جريمة الاحتيال، فالدكتور رمسيس بهنام يعرف القصد الجنائي بأنه:" انصراف الإرادة إلى السلوك المكون للجريمة كما وصف نموذجها الإجرامي

[1] – رحال بومدين وسعداني نورة، المرجع السابق، ص 105.

[2] – بهنام رمسيس، النظرية العامة للقانون الجنائي، ط2، منشأة المعارف للنشر، مصر، 1971، ص 880 .

في القانون مع وعي بالملابسات التي يتطلب هذا النموذج إحاطتها بالسلوك في سبيل أن تتكون به الجريمة".

أولا: العلم

وهو القدرة الذهنية للجاني أن يكون على علم بممارسته لعملية الاحتيال، ويعرف في نفسيته أنه كاذب ويقوم بالخداع والتدليس، فهذا يثبت قيام الركن المعنوي للجريمة [1]، كذلك الشأن إذا استخدم المحتال وسيلة إلكترونية في عملية النصب، كونه فعلا غير مشروع من شأنه حمل المجني عليه على تسليم شيء ذا قيمة مالية بإرادته ودون قوة أو عنف، وبمفهوم المخالفة فالقصد الجنائي ينتفي في حالة إذا كان الفاعل لا يعلم أن فعله غير مشروع، أما بخصوص علمه أن هذا الفعل يشكل جريمة، فهو علم مفترض حيث لا يقبل من الجاني الدفع بجهله في القانون الجنائي فالعلم يقصد به العلم بالوقائع وليس بالقانون[2].

ثانيا: الإرادة

لا يكفي العلم بالنتيجة الإجرامية فقط، بل يجب أن تنصرف إرادة الفاعل إلى هذه النتيجة فأنصار هذه النظرية يرون أن القصد الجنائي يعني انصراف الإرادة إلى النتيجة الإجرامية وتعني إرادة الفعل والنتيجة معا، فهم يرون أن تأسيس المسؤولية الجزائية عل إرادة النتيجة يحقق العدالة أكثر من تأسيسها على العلم فقط[3]، وتظهر الإرادة في جريمة النصب والاحتيال باستعمال وسائل إلكترونية بولوج الجاني إلى نظام معلوماتي من أجل القيام بتعديل معطيات أو التلاعب فيها للحصول على أرباح مالية غير مشروعة وذلك بإرادته الحرة وغير مجبرا على ذلك، فإذا تجرد الإنسان من الإرادة فلا يعتد بفعله جريمة، كذلك يجب أن تصرف إرادة الجاني " النصاب " إلى تحقق النتيجة وهي الحصول على البيانات أو أموال[4].

---

[1] – أسامة حمدان الرقب، المرجع السابق، ص69 .

[2] – هاشمي جبراني، المرجع السابق، ص 607 .

[3] – عبد الفتاح مصطفى الصيفي، الأحكام العامة للنظام الجنائي في الشريعة الإسلامية والقانون، دار المطبوعات الجامعية للنشر، مصر، 2010، ص 292 .

[4] – محمد أمين الشوابكة، جرائم الحاسوب والأنترنيت(الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الأردن،2007، ص 221.

ثالثا: القصد الجنائي الخاص

وهو اتجاه نية الجاني للاستيلاء على مال الضحية الذي سلمه له طواعية نتيجة لخداعه، فإن لم تتوفر فيه نية التملك وسلب المال فلا يمكن مسائلته جزائيا لعدم وجود القصد الجنائي الخاص ومسألة إثبات القصد الجنائي تقع على عاتق النيابة العامة مع إثبات الواقعة المستندة إليه والوقائع التي تقوم عليها جريمة النصب مع تبيان الوسائل الاحتيالية التي استعملها الجاني لخداع الضحية وإيهامه للاستيلاء على أمواله أو بياناته الشخصية[1].

المطلب الثاني: أنواع جرائم النصب والاحتيال الالكتروني

تعد جرائم النصب الإلكتروني من أبرز الأنماط الإجرامية المستحدثة التي نتجت عن التطور الرقمي، إذ أصبحت تستعين بتقنيات متقدمة لتنفيذ أفعال إجرامية ترمي إلى الاستحواذ غير المشروع على أموال الآخرين وبياناتهم عبر العديد من الطرق الاحتيالية التي اتخذت أشكال وأنواع[2] بداية من منشورات تصيد احتيالي زائفة عبر مواقع التواصل الاجتماعي ، وانتحال هوية باستعمال تكنولوجيات الاعلام والاتصال وكذا التصيد الاحتيالي عبر تقنية الهندسة الاجتماعية، لذلك لا يمكن حصر جميع أنواع جرائم النصب والاحتيال الالكتروني، لكن سنتطرق للأكثر شيوعا في هذا المطلب بالتفصيل .

[1] – رؤوف عبيد، جرائم الاعتداء على الاشخاص والأموال، ط 08، دار الفكر العربي للنشر، مصر، 1985، ص 490 .

[2]– منشاوي محمد عبد الله، المرجع السابق، ص 133 .

الفرع الأول: انتحال الهوية باستعمال تكنولوجيات الاعلام والاتصال

انتحال هوية الغير باستعمال وسيلة إلكترونية من الجرائم المستحدثة[1] التي تستغل الاستعمال الواسع لمواقع التواصل الاجتماعي (**Facebook/Tiktok/Instagram**) التي يقوم من خلالها رواد هذه المواقع بنشر معلوماتهم الشخصية وصورهم وكذا وظائفهم [2]، أين يستغل المحتالون هذه المعطيات المنشورة لعامة الناس بفتح حساب مزيف منتحلا هوية الغير أو صفته (موظف أو رئيس جمعية..) ليقوم بعدها النصاب بالدردشة مع أصدقاء صاحب ذلك الحساب ويطلب مبالغ مالية، أو معلومات خاصة بالضحايا مثل رقم بطاقة بنكية أو أرقام سرية، وعند تنفيذ جريمته يقوم بحضر هؤلاء الضحايا من قائمة الأصدقاء لقطع الاتصال بهم[3] ، كما أن هذا الفعل قد يؤدي بالضحية لتقييد شكاوى ضد أصحاب تلك المعلومات دون علمه بانتحال هوية ذلك الشخص عبر مواقع التواصل الاجتماعي، حيث نص المشرع الجزائري في المادة **372** من قانون العقوبات الجزائري: " ....باستعمال اسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي..."[4] .

الفرع الثاني: تقنية التصيد الاحتيالي (Phishing) عبر البريد الإلكتروني

يعتبر التصيد الاحتيالي من أخطر الهجمات الإلكترونية التي يستخدمها المجرمون السيبرانيون لسرقة البيانات الشخصية والمالية للأفراد والشركات، لاسيما مع استخدام الأنترنيت والتقنيات الحديثة بشكل يومي مما أدت إلى تزايد المخاطر الرقمية، حيث تتضمن هجمات التصيد الاحتيالي استخدام الخدع والأساليب الاحتيالية لإيهام الأفراد أنهم يتعاملون مع جهة موثوقة وغير مشبوهة عن طريق الرسائل الإلكترونية بهدف الحصول على معلومات شخصية أو أرقام بطاقات بنكية

---

[1] – Frèderic Dechamps,Cariline Lambilot,Cybercriminalité état des lieux, Anthèmis,2016,p110

[2] – سويسي فتيحة، انتحال الهوية الرقمية، المجلة الجزائرية للقانون والعدالة، العدد 01 ، مجلد 11، مركز البحوث القانونية والقضائية للنشر، الجزائر، 2025، ص 89 .

[3] – محمد مهدي عجمي، جريمة انتحال الشخصية في مواقع التواصل الاجتماعي، مجلة الشريعة والدراسات الاسلامية، مجلد37، العدد 130،جامعة الكويت، 2022، ص 191 .

[4] – المادة 372 من القانون رقم24-06 المعدل والمتمم لقانون العقوبات الجزائري.

لسلب أموالهم عن بعد، وفي هذا السياق أشارت منظمة التعاون الاقتصادي والتنمية (**L' OCDE**) من خلال تقريرها المنشور سنة **2008** بخصوص سرقة هوية على الأنترنيت إلى تعريف التصيد الإلكتروني أنه:" كل اكتساب أو تحويل أو حيازة أو استخدام غير مرخص به لمعلومات شخصية سواء تتعلق بشخص طبيعي أو معنوي بغرض استغلالها لأغراض إجرامية أو ارتكاب أفعال احتيال أو أية أفعال أخرى " [1].

وجاء في تعريف آخر:" التصيد الإلكتروني يعتبر من تقنيات الهندسة الاجتماعية التي تستعمل من طرف المحتالين لأجل الحصول على معلومات شخصية بغرض انتحال هوية الغير عن طريق إيهام الضحية بأنها تتعامل مع شخص محل ثقة أي موثوق فيه على غرار البنك، الإدارة...بغرض الابتزاز وانتزاع منه معلومات شخصية، كلمة المرور، أرقام بطاقة الائتمان، تاريخ الميلاد...الخ، وهو شكل من أشكال الهجوم المعلوماتي الذي يستند أساسا على الهندسة الاجتماعية، ويمكن تنفيذ عملية التصيد الإلكتروني عن طريق البريد الإلكتروني، أو مواقع **web** مزيفة أو بأية وسيلة الكترونية أخرى "[2].

الفرع الثالث: الاحتيال عن طريق تطبيقات الدردشة والرسائل النصية

هنا يتم خداع الضحايا لإعطاء معلومات حساسة لمهاجم متخفٍ عبر الرسائل النصية القصيرة ويحدث ذلك على العديد من منصات المراسلة النصية للأجهزة المحمولة، حيث يكتب المحتال رسائل ستجعل المستلم يتخذ إجراءً في العادة، كأن يطلب من خلال الرسالة القصيرة **SMS** من المستلم أن يفتح رابط عنوان موقع داخل الرسالة الذي يتضمن برنامج خبيث **Malware** يثبت على جهاز الضحية، أو عن طريق دردشة بالخاص عبر تطبيق معين مثل تليغرام أو واتساب أو ميسنجر ثم يتم توجيه الضحية بعد ذلك إلى أداة تصيد احتيالي تطالبه بالكشف عن معلوماته الخاصة، من أجل الفوز بجائزة مالية، أو يطلب معلومات حسابه البريدي

[1] – Rapport OCDE,Le Vole d'identitè en ligne.http//:www.oecd/dataoecd/3/8/40699509

[2] – Myriam Quémeber,Yves Charpenel,Cybercriminalité droit pénal appliqué,Edition Economica,France,2010p253

أو البنكي من أجل إجراء تحيين روتيني لتلك البيانات [1]، وهنا وتحت ضغط السرعة وكذا ثقة الضحية يقع في شباك المحتال.

ومثال ما سبق التطرق له أنه في سبتمبر **2020**، ظهرت حملة تصيّد احتيالي عبر خدمات الرسائل القصيرة لإغراء الأشخاص بتقديم معلومات بطاقة الائتمان للحصول على جهاز **iPhone 12** مجانًا، حيث يستخدم النصابون فرضية تأكيد الطلب أين تدعي الرسالة النصية أنه تم إرسال الطرد إلى عنوان غير صحيح ويرسل رابط عنوان الموقع الموجود في النص، حيث تتظاهر بأنها برنامج روبوت للمحادثة من شركة **Apple** وتوجه الضحية خلال عملية المطالبة بجهاز **iPhone 12** المجاني الخاص لكنها تطلب حتمًا معلومات بطاقة الائتمان لتغطية رسوم شحن صغيرة وهنا يتم الوصول لحسابه البنكي ويتم تحويل مبالغ مالية منه[2].

الفرع الرابع: التطبيقات الخبيثة malware وبرامج الفدية ransomware

هذه البرامج من أخطر أدوات الجريمة الإلكترونية حيث يقوم الجاني بإرسال ملف خبيث عبر البريد الإلكتروني أو ضمن رابط أو من خلال موقع إليكتروني مزيف وبمجرد فتحه يتم تثبيت البرنامج تلقائيا على جهاز الضحية دون علمه[3]، حيث تتنوع أهداف هذه البرامج بين سرقة بيانات مثل صور شخصية أو كلمة سر، أو مراقبة نشاط المستخدم أو تشفير الملفات كليا ومطالبة الضحية بدفع مبلغ مالي كفدية مقابل استعادتها، وهو ما يعرف ببرامج الفدية **ransomware** كما أن هذه البرامج يمكن أن تصيب الأفراد أو المؤسسات أو الشركات وكذلك البنى التحتية الرقمية في الدولة مما يجعلها جريمة ذات طابع خطير، كون المهاجمون الذين يستخدمون برامج الفدية الضارة يستهدفون المؤسسات الكبيرة التي يديرها الإنسان[4]، لأن بإمكانهم دفع فدية بمبلغ

---

[1] – انظر موقع شركة تصميم وتطوير تقنيات حديثة للأمن السيبراني WWW.CEREBRA.SA اطلع عليه بتاريخ:02-05-2026 الساعة 20:41 .

[2] – محمد مهدي عجمي، المرجع السابق، ص 193 .

[3] – رؤى حمود، مقال بعنوان فيروس الفدية، المهاجم الأخطر للمؤسسات في العصر الرقمي، مجلة مجموعة ريناد، الموقع https://www.rmg-sa.com/% ، اطلع عليه بتاريخ:2026/05/03 الساعة 15:49 .

[4] – سويسي فتيحة، المرجع السابق، ص 106 .

أكبر من الشخص العادي، غالباً ما تقدر بملايين الدولارات، نظرًا للمخاطر العالية المرتبطة بخرق بهذا الحجم، كما تختار العديد من المنظمات دفع الفدية بدلاً من تسرب بياناتها الحساسة أو المخاطرة بهجمات أخرى، ومع ذلك لا يضمن الدفع منع وقوع أي من النتيجتين.

ملخص الفصل الأول

يتناول هذا الفصل الإطار الناظم لجرائم النصب والاحتيال المرتكبة عبر الوسائط الرقمية، مبرزاً مفهومها ومضمونها القانوني، ومسلطاً الضوء على خصوصية هذه الجرائم بوصفها نمطاً إجرامياً مستحدثاً واكب التطور التكنولوجي، وتتخذ من الأدوات الرقمية والتقنيات الحديثة وسيلةً رئيسية لتنفيذ الفعل الاحتيالي، ويتبين من هذا السياق أن هذه الجرائم ترتكز على الخداع الإلكتروني الهادف إلى الاستحواذ على أموال الغير، من خلال إيهام الضحايا بوقائع غير حقيقية، أو التلاعب بثقتهم عبر قنوات الاتصال الحديثة، دون حاجة إلى مواجهة مباشرة بين الجاني والمجني عليه.

كما يركز هذا الفصل على الأركان الأساسية التي تنهض بها هذه الجرائم، وفي مقدمتها الركن المادي المتمثل في استعمال أساليب احتيالية عبر الشبكة المعلوماتية، والركن المعنوي القائم على نية التملك غير المشروع. ويبرز الفصل أيضاً الطبيعة المركبة لهذه الجرائم، التي تتعدد صورها وتتنوع أساليب تنفيذها، مما يحول دون حصرها ضمن نسق إجرائي موحد، فهي جرائم تتسم بسمات فارقة تميزها عن نظيرتها التقليدية، أبرزها الطابع العابر للحدود، وسرعة التنفيذ، وصعوبة التتبع، فضلاً عن الطابع الرقمي المعقد لأدلتها الإثباتية.

الفصل الثاني:

استغلال الذكاء الاصطناعي في جريمة النصب وآليات مكافحتها

الفصل الثاني: استغلال الذكاء الاصطناعي في جريمة النصب وآليات مكافحتها

في ظل الانتشار المتزايد للجرائم الالكترونية وتزايد اعتماد الأفراد والمؤسسات على الوسائط الرقمية في معاملاتهم اليومية، أصبحت جرائم النصب والاحتيال ترتكب بوسائل إلكترونية عن بعد ويعتمد المجرمون على هذه التقنيات للاستيلاء على أموال الغير لصعوبة اكتشافها أوتتبع أثرها، وهذا ما يستوجب توفير آليات وقائية وردعية لحماية الأفراد والمؤسسات.

مما سبق، ظهرت الحاجة إلى تكاثف جهود مؤسسات وهيئات الدولة للحد من خطورة هذه الجريمة المستحدثة والمتطورة من حيث استغلال وسائل إلكترونية وشبكات الأنترنيت في أفعال مجرمة قانونا، فهنا وجب وضع قوانين وعقوبات تتناسب مع هذه الجريمة، مع وضع وسائل وقائية تعتمد على التقنيات الحديثة، وكذلك التحسيس عبر مختلف قنوات الاتصال ومن بينها وسائل التواصل الاجتماعي لتحقيق الأمن السيبراني، بتظافر وعي الأفراد وحماية المؤسسات الحكومية.

ومن خلال هذا الفصل سيتم التطرق لهذه الآليات التقنية لأنماط جريمة النصب المعزز بالذكاء الاصطناعي، مع تمييزها عن الجرائم الشبيهة بها في القانون الجزائري (مبحث أول)، ثم تبيان الأطر القانونية والتقنية لتجريم ومكافحة النصب والاحتيال الالكتروني، ودور المؤسسات الحكومية للتصدي لهذه الجريمة من الناحية الوقائية والردعية في التشريع الجزائري (مبحث ثاني)

المبحث الأول: الآليات التقنية لأنماط النصب المعزز بالذكاء الاصطناعي وتمييزها عن الجرائم الشبيهة بها في التشريع الجزائري

جرائم النصب والاحتيال أصبحت أكثر تعقيداً وخطورة بفعل توظيف أدوات الذكاء الاصطناعي في عمليات الخداع والتضليل، سواء من خلال تقنيات التزييف العميق (**Deepfake**) ، أو انتحال الشخصيات الرقمية، أو إنشاء محتويات مزيفة يصعب على الضحية التحقق من صحتها، من خلال النصب المعزز بالذكاء الاصطناعي، وهو نمط إجرامي يعتمد على الوسائل التقنية الحديثة لخلق أوهام ووقائع كاذبة تدفع المجني عليه إلى تسليم أمواله أو حقوقه طواعية تحت تأثير الخداع.

وفي ظل هذا الواقع، تبرز أهمية تبيان الآليات التقنية التي تقوم عليها أنماط النصب المعزز بالذكاء الاصطناعي(مطلب أول)، ثم نتطرق للتمييز بين جريمة النصب والاحتيال الالكتروني وبين الجرائم الشبيهة بها في التشريع الجزائري على غرار جريمة السرقة وخيانة الأمانة التزوير، ثم التدليس في القانون المدني الجزائري (مطلب ثاني).

المطلب الأول: الآليات التقنية لأنماط النصب المعزز بتقنية الذكاء الاصطناعي

تعتمد أنماط النصب المعزز بالذكاء الاصطناعي (**AI-Powered Fraud**) على تقنيات متقدمة تهدف إلى محاكاة السلوك البشري، تزييف الهوية، وتجاوز الأنظمة الأمنية التقليدية بدقة وسرعة فائقة[1]، وفيما يلي أبرز الآليات التقنية لأنماط النصب عبر تقنية الذكاء الاصطناعي :

الفرع الأول: التزييف العميق(Deepfake)

التزييف العميق محتوى مرئي وصوتي تم التلاعب به باستخدام برامج متطورة، فهي مجموعة من التقنيات المستخدمة لتركيب منتجات بصرية جديدة، ولكن كلمة **Deepfake** المتداولة أصبحت مرادفة لعملية استبدال الوجوه[2]، أين يتم تركيب صور شخص مستهدف على فيديو لشخص آخر(المصدر) وهو يقول ويفعل أشياء قام بها الشخص المصدر، وعملية استبدال

[1] – يحي إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد34، العدد82، 2019، ص15.

[2] – flourdi Luciano (artificial intelligence,deepfakes and the future of ectypes,philos.technol31,2018).p317.

وجه بوجه آخر ينتج عنه محتوى مخالف تماما للواقع، وعليه فالتزييف العميق في جوهره هو " تقول على شخص بشيء لم يقله ولم يفعله"، حيث صار من الممكن استخدام التكنولوجيا الرقمية للتلاعب بالصوت والصورة والتي يصعب اكتشافها[1]، حيث أصبحت هذه الفيديوهات المفبركة تضاهي في دقتها واحترافية إنشائها الفيديوهات الحقيقة، وصار من الصعب التمييز بينها وبين الصور الأصلية، سواء بالعين المجردة أو حتى باستخدام برامج كشف التزييف المتداولة.[2]

هذه التقنية وكما هو الحال مع دخول أدوات الاحتيال وطرائقه المختلفة إلى العالم الافتراضي سخر المجرمون تقنية التزييف العميق لخدمة أغراضهم الشريرة، حيث أصبح يستخدم على نطاق واسع في عمليات الاحتيال، فمثلا قام عدد من المحتالين (**scammers**) بتزوير شخصية رجل الأعمال الشهير إيلون ماسك بالترويج لنوع معين من العملات الرقمية، حيث أظهروه في الفيديو يقول:" أنا هنا لأخبركم عن العملة الرقمية نيورالينك (**Neuralink crypto token**) العملة التي سوف تغير العالم إلى الأبد "[3]، مما دفع البعض إلى الاستثمار في تلك الأموال معتقدين أن الفيديو بالحقيقة يعود لرجل الأعمال إيلون ماسك .

الفرع الثاني: التزييف الصوتي العميق (Audio Deepfakes)

استخدام تقنيات استنساخ الصوت (**Voice Cloning**) لتوليد كلام يحاكي أفراداً معينين، حيث يقوم المحتالون بتحليل مقاطع صوتية قصيرة للضحية ثم توليد عبارات جديدة لم ينطقوا بها أبداً، مما يجعل المكالمات الاحتيالية تبدو موثوقة جداً، كما يشار إليها باسم عمليات التلاعب بالصوت وهذا بدءًا من أوائل عشرينيات القرن الحادي والعشرين، أصبح متاحا على نطاق واسع باستخدام الأجهزة المحمولة البسيطة أو أجهزة الكمبيوتر الشخصية، حيث يتم نقل كميات هائلة

[1] – Sophia Hanson,robotic,available at :www.hansonrobotics.com,viewed on 14/05/2026 at 18M03

[2] – كريمة غديري، التزييف العميق: نشأة التقنية وتأثيراتها، مجلة الرسالة للدراسات الاعلامية، جامعة العربي التبسي الجزائر، المجلد 05، العدد 04، 2021، ص 123 .

[3] – علاء الدين منصور مغايرة، جرائم الذكاء الاصطناعي وسبل مواجهتها–جرائم التزييف العميق نموذجا –المجلة الدولية للقانون جامعة قطر، المجلد 13، العدد 02، 2024 ، ص 132–133.

من التسجيلات الصوتية يوميًا عبر الإنترنت، أين يستهدف مهاجموا التزييف الصوتي الأفراد والمنظمات، ومثال ذلك في عام **2019** واقعة احتيال باستخدام تقنية التزييف العميق، أين قام محتال سيبراني باستخدام صوت الرئيس التنفيذي لإحدى شركات الطاقة في ألمانيا وطريقة أسلوبه في الحديث بشكل تصعب معه معرفة حقيقة التزييف، ثم قام بالاتصال بالمدير العام لفرع الشركة في بريطانيا حتى اعتقد هذا الأخير أنه على اتصال مع المدير العام في ألمانيا، حيث طلب منه القيام بتحويل مبلغ **243** ألف دولار إلى حساب بنكي لعميل في دولة هنغاريا[1]، في أوائل عام **2020**، انتحلت نفس التقنية شخصية مدير شركة كجزء من مخطط متقن أقنع مدير فرع بتحويل **35** مليون دولار.

الفرع الثالث: التصيد الاحتيالي المُولّد آلياً

التصيد الاحتيالي المُولَّد آلياً **(AI-Generated Phishing)** نمط متطور من الاحتيال الإلكتروني يعتمد على استخدام تقنيات التعلم الآلي والشبكات العصبية الاصطناعية لإنتاج رسائل إلكترونية، أو رسائل نصية، أو مواقع ويب مزيفة تحاكي بدقة عالية المراسلات الرسمية للجهات الموثوقة، تختلف هذه الآلية عن التصيد التقليدي في قدرتها على تجاوز آليات الكشف القائمة على التوقيعات الثابتة، وذلك بسبب توليدها لمحتوى فريد لكل ضحية محتملة[2]، يشكل هذا النشاط انتهاكاً صريحاً للتشريعات الوطنية والدولية المتعلقة بالجرائم السيبرانية، لاسيما المواد المتعلقة بانتحال الشخصية والاحتيال عبر وسائل الاتصال عن بُعد، فعلى سبيل المثال، تُجرِّم المادة السادسة من اتفاقية بودابست الخاصة بجرائم الإنترنت "الاستخدام غير المشروع للأجهزة" بما فيها البرامج الضارة والذكاء الاصطناعي المُوَجَّه لارتكاب الاحتيال[3] .

---

[1] – J.Damiani, Avoice deepfake was used to scam a ceo out of 234$ 2019.http://forbs.com(last visited 11-05-2026)

[2] – عبد الله محمود أبو تجار، المسؤولية عن مخاطر تقنيات الذكاء الاصطناعي، ط01، مؤسسة المعرفة لنشر وتوزيع الكتب، الأردن،2024 ، 163-164 .

[3] – المادة 6 من اتفاقية بودابست(ETS 185) ، الفقرة 1.

كما أن التوليد الآلي للرسائل الاحتيالية يطرح إشكالية قانونية تتعلق بالإثبات، إذ يصبح من العسير إسناد الفعل الإجرامي إلى شخص طبيعي معين، بسبب إمكانية تشغيل النظم الذكية بشكل مستقل أو عن طريق وسطاء غير مدركين، ومن الناحية الموضوعية، تعتبر رسائل التصيد المُولَّدة آلياً "بيانات كاذبة" بالمعنى الوارد في القوانين المدنية والجزائية، أما على صعيد الحماية الوقائية، فإن المشرعين بدؤوا يدرجون نصوصاً تلزم مقدمي خدمات الذكاء الاصطناعي بتضمين نظمهم "علامات مائية رقمية" أو آليات تتبع للرسائل المُولَّدة آلياً، لتسهيل تمييزها من قبل المستخدمين والسلطات ومع ذلك، لا تزال التشريعات في معظم الدول متأخرة عن وتيرة التطور التقني، مما يخلق فجوة قانونية تستدعي تدخلاً تشريعياً عاجلاً على المستويين الوطني والدولي، كما يلاحظ أن عقوبات التصيد الإلكتروني تتفاوت بين الغرامات المالية والسجن، لكن التصيد المُولَّد آلياً قد يستوجب عقوبات أشد نظراً لكونه ظرفاً مشدداً يستند إلى استغلال وسائل عالية التطور.[1]

الفرع الرابع: أتمتة جمع المعلومات والهجمات :(Automation)

تعد أتمتة جمع المعلومات، والتي تعتبر المرحلة التمهيدية للهجمات الاحتيالية المعززة بالذكاء الاصطناعي، حيث تمكن الجناة من الحصول على كم هائل من البيانات الشخصية والمالية دون موافقة أصحابها، من الناحية القانونية يُعتبر تجاوز آليات الحماية أو شروط الخدمة الموضوعة للمنصات الرقمية بهدف جمع هذه البيانات فعلاً غير مشروع، وقد جُرّم في العديد من التشريعات تحت عنوان "الدخول غير المصرح به" أو "الحصول غير القانوني على بيانات من نظام معلوماتي ."فعلى سبيل المثال، واجهت شركات تقنية كبرى دعاوى قضائية ضد كيانات استخدمت ملايين الحسابات الوهمية لأتمتة عملية استخراج البيانات، وهو ما يشكل انتهاكاً صريحاً للعقود وقوانين الاحتيال الحاسوبي[2] .

[1] – علاء الدين منصور مغايرة، المرجع السابق، ص 138 .

[2] – موسى عبد الله، بلال أحمد حبيب، الذكاء الاصطناعي ثورة في تقنيات العصر،ط1، المجموعة العربية للتدريب والنشر، مصر، 2019، ص25–26 .

بعد تجميع هذه البيانات، يتم توظيفها في "هجمات احتيالية آلية" تشمل التصيد الاحتيالي عالي التخصيص **(Spear–Phishing)** باستخدام تقنيات توليد اللغة، وانتحال الشخصية عبر التزييف العميق**(Deepfakes)** "، مما يضفي شرعية مصطنعة على عمليات الاحتيال، كما شكل هذا المسار ثنائي المراحل (الجمع ثم الاستغلال) تحدياً كبيراً للمشرع، حيث يصبح من العسير الفصل بين الأدوات التقنية ذات الاستخدام المزدوج كأدوات شرعية أو إجرامية، وفي هذا السياق، بدأت بعض الهيئات القضائية والأكاديمية تدعو إلى تطبيق مبدأ "المسؤولية الموضوعية" على مطوري البرمجيات التي صُممت لغرض احتيالي، أو إهمالهم في وضع ضوابط تمنع استغلالها في أتمتة الجرائم[1]، علاوة على ذلك، فإن الطبيعة العابرة للحدود لهذه العمليات، حيث تُخزن البيانات المجمعة في خوادم خارج الولاية القضائية للضحية، تعيق تطبيق قواعد الاختصاص القضائي التقليدي وتستدعي آليات متطورة للتعاون القضائي الدولي.

وقد أشارت تقارير أممية حديثة إلى أن منظومة الجريمة المنظمة تستغل هذه الفجوات القانونية لتحويل عمليات الاحتيال إلى صناعة واسعة النطاق، مما يتطلب رداً تشريعياً يفرض التزامات وقائية على مقدمي الخدمات الرقمية، بناءً على ذلك، تستوجب مكافحة استغلال أتمتة جمع المعلومات في الاحتيال إقرار نصوص قانونية تجرم صراحة "الاستعداد للاحتيال الإلكتروني" عبر حيازة أدوات الجمع غير المصرح بها، وليس فقط تنفيذ الفعل الاحتيالي، كما يبقى التوازن بين الابتكار التكنولوجي وتجريم إساءة استخدامه رهيناً بتطوير تشريعات مرنة تعترف بـ"تقنية الحياد" ولكنها تشدد العقوبات بمقدار الضرر الاجتماعي الناتج عن تحويل هذه التقنيات إلى أدوات لجمع بيانات الضحايا للنصب عليهم وسلب أموالهم[2].

[1] – هاو كارين، هيفين دوجلاس، لماذا حققت تقنية التزييف العميق انتشارا واسعا في 2020، Mit review https://technologyreview.ae ، تم الاطلاع بتاريخ:2026/05/11 الساعة:02:28 .

[2] – حمزة غندور، سليمة قواسمية، أنظمة الذكاء الاصطناعي في مكافحة الاحتيال الالكتروني، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد 10، العدد 01، 2025، ص 33 .

المطلب الثاني: تمييز جريمة النصب والاحتيال عن الجرائم الشبيهة بها في التشريع الجزائري

تتقاسم جريمة النصب والاحتيال خصائص مشتركة مع عدة جرائم شبيهة تهدف إلى الاستيلاء على أموال الغير، حيث يعمد الجاني إلى خداع المجني عليه بأساليب احتيالية، ونظراً لكون الاحتيال يندرج ضمن جرائم الاعتداء على الملكية المنقولة، فإنه يتشابه مع كل من جريمة خيانة الأمانة، والسرقة، وجريمة التزوير، كذلك يتداخل النصب مع التدليس المدني عمليا، وسنتناول فيما يلي التمييز بين جريمة النصب والاحتيال وكل من هذه الجرائم على حدى، ثم نعرج على تميزها عن التدليس في القانون المدني الجزائري.

الفرع الأول: تمييز جريمة النصب والاحتيال عن جريمة السرقة

نص المشرع الجزائري في المادة **350** من قانون العقوبات السرقة بأنها "اختلاس شيء غير مملوك للغير"، ويستفاد من هذا النص أن جريمة السرقة تتحقق بإزالة حيازة المال من المجني عليه دون رضاه، معتمدةً على جهد جسماني من الجاني لنقل الحيازة إليه. وفي مقابل ذلك، تقوم جريمة النصب على جهد معنوي يتمثل في إيهام المجني عليه وخداعه، مما يدفعه لتسليم ماله بإرادة تبدو طواعية لكنها معيبة. [1]

يكمن الفرق بين الاختلاس في جريمة النصب والاختلاس في جريمة السرقة في رضا المجني عليه وآلية انتقال الحيازة. ففي النصب، ينتقل المال من يد الضحية إلى يد الجاني برضاه التام، وإن كان هذا الرضا ناتجًا عن خداع وتضليل أدى إلى تكوين قناعة باطلة لديه. أما في السرقة، فيتم سلب حيازة المال كرهاً عن المجني عليه، دون علمه أو موافقته، وفي غياب أي تسليم إرادي وبالتالي، يتميز النصب عن السرقة بطبيعة الوسيلة المستخدمة: ففي السرقة، يستولي الجاني على المال خفية أو بالقوة دون أن يتسلمه الضحية طواعية، بينما في النصب، يدفع الجاني الضحية، عبر الإيحاء بأمر مخالف للحقيقة، إلى تسليم ماله بمحض إرادته الظاهرية [2] .

[1] – أحمد بسيوني أبو الروس، جرائم النصب، دار المطبوعات الجامعية، مصر، 1986 ، ص 18 .

[2] – المرجع نفسه، ص 25 .

الفرع الثاني: تمييز جريمة النصب والاحتيال عن جريمة خيانة الأمانة

تندرج جريمة خيانة الأمانة ضمن جرائم المساس بالأموال، إلا أن آلية تسليم المجني عليه ماله فيها تختلف تماماً عما هو حاصل في جريمة النصب والاحتيال، ففي النصب يكون الجاني قد ترك بصمته الخادعة التي أوقعت الضحية في الغلط، بينما في خيانة الأمانة يتم التسليم بناءً على علاقة ائتمانية قائمة بموجب عقد من العقود التي أقرها المشرع الجزائري، كالوديعة أو العارية، ولولا هذا العقد لما أقدم الضحية على تسليم أمواله طواعية للمتهم، وبالتالي لما تحقق الأساس الذي تقوم عليه خيانة الأمانة، ليستولي الأخير بعد ذلك على المال على وجه غير مشروع آخذاً إياه بالباطل[1]. وتختلف جريمة خيانة الأمانة عن جريمة النصب والاحتيال من حيث مدى سلامة إرادة المجني عليه عند تسليم المال، ففي النصب والاحتيال تُعد إرادة المجني عليه مشوبة بعيب الغلط، حيث أوقعه الجاني في حيلة جعلته يسلم ماله تحت تأثير قناعة خاطئة، بينما في جريمة خيانة الأمانة، يستند تسليم المال إلى عقد ائتمان منصوص عليه في المادة **376** من قانون العقوبات، ولا يتم هذا التسليم إلا بناءً على إرادة صحيحة وسليمة تماماً، خالية من أي عيب من عيوب الرضا كالغلط أو التدليس أو الإكراه[2].

ويقصد بالأمانة أن يُسلَّم مال أو أي شيء لشخص معين بدافع الحفاظ عليه، على أن يعيده إلى مالكه بعد مدة محددة. وهذا ما يُسمى قانوناً بـ"نقل حيازة ناقصة" (حيازة دون نقل الملكية). ونجد أن جريمة خيانة الأمانة تتشابه مع جريمة النصب في نقطة واحدة، أن الاعتداء في كل منهما يقع على الملكية، وليس على الحيازة التي سبق أن نقلها المجني عليه طواعية للجاني، أما الفرق فيظهر في زمن تحقق الاستيلاء، ففي النصب يعتبر فعل التسليم نفسه هو الاستيلاء غير المشروع على المال، بينما في خيانة الأمانة يتم التسليم أولاً بموجب عقد ائتمان صحيح (كالإعارة،

[1] – عبد العزيز سعد، جرائم الاعتداء على الأموال العامة والخاصة، ط 04 ، دار هومة، الجزائر، 2007، ص118 .

[2] – محمد عبد الحميد مكي، العلاقة الاحتيال وتسليم المال في قانون العقوبات، منشورات جامعة طنطا،مصر، 1995، ص 130

الوديعة، الرهن) ويأتي الاستيلاء لاحقاً، فلا تقوم الجريمة إلا بفعل تالٍ للتسليم كالاختلاس أو الإنكار[1].

الفرع الثالث: تمييز جريمة النصب و الاحتيال عن جريمة التزوير

يتحقق التزوير حين يُقدم الفاعل عن عمد على تحريف وقائع أو بيانات في سندٍ أو وثيقة، مما يلحق ضرراً مادياً أو معنوياً أو اجتماعياً بالغير، وأساس التفرقة هنا أن جريمة التزوير تقوم على التحريف في ذاته، دون حاجة إلى نتيجة أخرى، في حين أن الاحتيال – وإن اتخذ من تحريف الحقيقة وسيلةً للاعتداء على المال – لا يقوم على مجرد هذا التحريف، ولهذا فإن المشرّع يطلب في الطائفة الأولى من الجرائم، عناصر إضافية تُكسب الفعل خطورة اجتماعية جديرة بالتجريم، وهي عناصر لا يُشترط توفرها في الاحتيال[2].

يختلف التزوير عن الاحتيال في طبيعتهما ومحلهما، ذلك أن التزوير جريمة لا تقع إلا على المحررات، سواء كانت رسمية أم عرفية، وتتمثل في تحريف الحقيقة الواردة فيها، وهي جريمة قائمة بذاتها ومستقلة، لا يُشترط لقيامها أن يلحق ضرر بالغير، إذ يمكن للفاعل أن يُضرَّ بمصلحته هو شخصياً، أما الاحتيال فيقوم على إيهام شخص آخر بوسائل احتيالية بهدف محدد، وهو حمله على القيام بعمل أو تسليم مال.

الفرع الرابع: تمييز جريمة النصب والاحتيال عن التدليس المدني

يُعد التمييز بين جريمة النصب والاحتيال في قانون العقوبات والتدليس في القانون المدني الجزائري أمراً جوهرياً، لاختلاف طبيعة كل منهما ونطاق تطبيقه، حيث تنص المادة **372** من قانون العقوبات الجزائري على جريمة النصب بأنها استخدام وسائل احتيالية للإيقاع بالضحية، بغرض الاستيلاء على أموالها أو ممتلكاتها أو حملها على توقيع مستندات، وهي بذلك جريمة جنائية قائمة بذاتها، يتحقق ركنها المادي بالكذب أو التزوير أو الاحتيال في العقود، وركنها

[1] – عبد العزيز سعد، المرجع السابق، ص 121 .

[2] – السعيد كامل، شرح قانون العقوبات الاردني: الجرائم الواقعة على الأموال، ط02، دار الثقافة للنشر والتوزيع، الأردن،1993، ص 851 .

المعنوي بتوافر النية الإجرامية لدى الجاني، إضافة إلى ضرورة تحقق نتيجة إجرامية هي الضرر الفعلي الذي يصيب الضحية.

أما التدليس فيُعد أحد عيوب الرضا التي تنظمها أحكام القانون المدني الجزائري، فهو ليس جريمة جنائية مستلقة بذاتها، بل هو سبب من أسباب بطلان العقد، يقوم على استعمال طرق احتيالية يلجأ إليها أحد المتعاقدين للتأثير على إرادة المتعاقد الآخر وحمله على التعاقد[1]، لولا هذه الطرق لما أقدم عليه، فالاحتيال ينصب على الاعتداء على الملكية ويعاقب عليه بالحبس والغرامة، بينما التدليس يُبطل رضا المتعاقد ويؤدي إلى قابلية العقد للإبطال لمصلحة من وقع عليه.

ومن الفروق الجوهرية أيضاً أن جريمة الاحتيال لا تقوم إلا بتوافر قصد جنائي خاص هو نية الاستيلاء على مال الغير، أما التدليس فيكفي فيه مجرد استعمال الوسائل الاحتيالية للتأثير على الإرادة دون اشتراط نية إجرامية، وتجدر الإشارة إلى أنه قد يتداخل الاحتيال والتدليس عملياً، فمن يستعمل التدليس لإبرام عقد والاستيلاء على مال قد يحاسب جنائياً عن جريمة الاحتيال، ويظل عقده قابلاً للإبطال مدنياً لقيام التدليس، وعليه فالاحتيال جريمة جنائية تحمي المال العام والخاص، بينما التدليس عيب رضائي يحمي سلامة الإرادة في المعاملات المدنية[2].

[1] – مأمون الكزبري، نظرية الالتزامات في ضوء قانون الالتزامات والعقود المغربية، ط02، مطبعة دار القلم، لبنان، 1972، ص 98 .

[2] – المرجع نفسه، ص 100 .

المبحث الثاني: الأطر القانونية والتقنية لمكافحة الاحتيال الإلكتروني في القانون الجزائري

في ظل الانتشار المتنامي للجرائم الإلكترونية، وتزايد اعتماد الأفراد والمؤسسات على الوسائط الرقمية في معاملاتهم اليومية، باتت جرائم النصب والاحتيال الإلكتروني تُشكّل أحد أخطر التهديدات التي تمس أمن المعلومات وتقوّض ثقة المتعاملين بالبيئة الرقمية، وتكمن خطورة هذه الجرائم في طبيعتها المتطورة، القائمة على توظيف وسائل تقنية معقدة وأساليب احتيالية يصعب – في كثير من الأحيان – اكتشافها أو التنبؤ بها، وهو ما يستوجب استجابة قانونية فاعلة وردعاً ملائماً لحماية الأفراد والمجتمع، وضمن هذا السياق، تبرز ضرورة وضع منظومة عقابية شاملة لتحقيق العدالة المنشودة، غير أن الاعتماد على الجزاءات وحدها لا يشكل رداً كافياً لمواجهة هذه الظاهرة، مما يحتم الأخذ بوسائل وقائية قوامها التكنولوجيا الحديثة والتوعية الإعلامية والاجتماعية، بغية بناء وعي رقمي يقلص فرص ارتكاب هذه الجرائم ويمكّن الأفراد من التصدي لها وعليه سنعالج في هذا المبحث مطلبين اثنين: الأول يتعلق بآليات تجريم الاحتيال الإلكتروني لإرساء الأمن السيبراني، والثاني سنتطرق من خلاله لدور المؤسسات الحكومية في مكافحة جريمة النصب والاحتيال الالكتروني وكذا سبل طرق الوقاية منها[1].

المطلب الأول: آليات تجريم النصب الإلكتروني وإرساء الأمن السيبراني

تُصنّف الجزائر ضمن الدول التي أولت مؤخراً عناية خاصة بمجال الأمن المعلوماتي والتصدي للإجرام الرقمي بشتى صوره، وفي مقدمتها جرائم النصب والاحتيال الإلكتروني، وقد تُرجم هذا التوجه عبر إعداد بيئة قانونية وتقنية مساندة للأمن المعلوماتي، والسعي إلى إرساء فضاء إلكتروني مأمون يضمن تحقيق الوقاية من جرائم النصب والاحتيال الإلكتروني، وإذا كان الدور الوطني لمؤسسات الدولة يشكل حجر الأساس في مكافحة هذه الجريمة فإن الطبيعة العابرة للحدود التي تتميز بها تجعل من التعاون الدولي ضرورة قصوى، ففي الفضاء الرقمي تتلاشى

[1] – أحسن بوسقيعة، من العدالة التقليدية إلى العدالة الرقمية: دور القضاء الجزائري في مواجهة الجريمة الإلكترونية في ظل التحول الرقمي والذكاء الاصطناعي، مداخلة في الملتقى الوطني بقصر الثقافة ولاية أدرار، بتاريخ:18 أفريل 2026 .

الحدود الجغرافية، وتصبح الأنشطة الإجرامية قادرة على اختراق الدول من دون حواجز، مما يحتم تنسيقاً دولياً وإقليمياً محكماً لمواجهتها بفعالية، وهو ما نوضحه على النحو الآتي:

الفرع الأول: الاتفاقيات والمواثيق الدولية

مع تنامي تقنية المعلومات وتصاعد الاهتمام الدولي بخطورة الجرائم السيبرانية – وفي طليعتها النصب والاحتيال الإلكتروني – أدرك المجتمع الدولي حجم التهديد الذي تشكله هذه الجرائم، خصوصاً وأنها بطبيعتها عابرة للحدود الوطنية على النحو الذي سبق بيانه عند تناول خصائص النصب الإلكتروني. وقد تجسّد هذا الإدراك في جملة من القرارات والمواثيق الدولية التي سعت إلى وضع أطر قانونية مشتركة للتصدي لهذه الظاهرة، وأبرزها ما يلي:

-القرار الصادر عن مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة السجناء هافانا **1990** بشأن الجرائم ذات الصلة بالكمبيوتر.

-مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات **1994** البرازيل بشأن جرائم الكمبيوتر.

-الاتفاقية الأوروبية (بودابست) لمكافحة جرائم المعلوماتية والاتصالات **2001**.[1]

-الاتفاقية العربية لمكافحة الجرائم المعلوماتية (الإلكترونية – الرقمية). [2]

وتُعد هذه الاتفاقية أبرز صك دولي انضمت إليه الجزائر في ميدان تكنولوجيا المعلومات، حيث تم التصديق عليها بموجب المرسوم الرئاسي رقم **14-252** المؤرخ في **08** سبتمبر **2014**، وهي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ **21** ديسمبر **2010**. وبإتمام إجراءات التصديق، تكون الجزائر قد أدرجت أحكام هذه الاتفاقية ضمن منظومتها

[1] – الاتفاقية الأوروبية بشأن الجريمة السيبرانية (إتفاقية بودابست)، 23نوفمبر 2001، فتح التوقيع في بودابست، دخول حيز التنفيذ 01 جوان 2004، رقم المعاهدة ETSN°185 .

[2] – خيدل أحمد، كيسي زهيرة، إجراءات جمع الأدلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 11، العدد 01 ، 2022، ص 371-391 .

القانونية الوطنية، مما يرتب عليها التزاماً قانونياً بإنفاذ مضمونها في مواجهة باقي الدول الأطراف فيها، كما يُلزم قضاءها الوطني بتطبيق أحكامها.

الفرع الثاني: التشريعات والقوانين الداخلية

– القانون رقم **15-04** المؤرخ في **10** نوفمبر **2004**، المعدل والمتمم لقانون العقوبات الجزائري[1]، الذي استحدث القسم السابع مكرر تحت عنوان: 'المساس بأنظمة المعالجة الآلية للمعطيات'. وقد ورد في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة قد أفرزا أنماطاً جديدة من الإجرام، مما أجبر العديد من الدول إلى تجريمها والمعاقبة عليها. والجزائر، على غرار هذه الدول، تسعى من خلال هذا المشروع إلى إرساء حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، كما أن هذه التعديلات من شأنها سد الفراغ القانوني القائم في هذا المجال.

ارتكز المشرّع الجزائري في فلسفته التجريمية على أن جوهر المنظومة المعلوماتية يتمثل في المعطيات، إذ تتحول هذه البيانات الخام بعد إدخالها ومعالجتها وتخزينها إلى معلومات، وانطلاقاً من ذلك أحاط هذه المعطيات بحماية متعددة الأوجه، وقد تجلّى هذا التوجه في اعتماده مصطلح "المساس بنظم المعالجة الآلية للمعطيات"، وهو مصطلح يتجاوز في مدلوله فكرة النظام والمعلومات إلى استيعاب شبكات المعلومات أيضاً، وقد ترتب على هذا الاختيار الاصطلاحي نتيجة جوهرية، وهي إخراج الجرائم التي تُرتكب باستخدام النظام المعلوماتي كأداة من نطاق هذا التجريم، وحصره حصراً في الأفعال التي تشكل اعتداءً مباشراً على النظام المعلوماتي ذاته.[2]

[1] – القانون رقم:04-15 المؤرخ في:27 رمضان 1425 الموافق لـ:10 نوفمبر 2004 المعدل والمتمم للأمر رقم:66-156 المتضمن قانون العقوبات، ج ر رقم:2004/71 .

[2] – فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها في التشريع الجزائري، المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية المنعقد يومي 24-2017/03/25 في طرابلس، مركز جيل للبحث العلمي والنشر بالتعاون مع جامعة تلمسان ، ص 115 .

– القانون رقم:**25-14** المؤرخ في:**03** أوت **2025** المتعلق بقانون الإجراءات الجزائية الجزائري، المواد التي تنظم الاختصاص المحلي والنوعي والإجراءات الخاصة بالتحقيق و التفتيش.[1]

– القانون رقم:**09-04** المؤرخ في:**05** أوت **2009** المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال[2]، يهدف هذا القانون إلى وضع نصوص إجرائية تتناسب مع الجرائم السيبرانية، أين تم استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في المادة **13**، ودخولها حيز التنفيذ في **2015** موجب المرسوم الرئاسي **268/15** .

وتأكيداً على عزم المشرّع الجزائري في التصدي لهذه الجريمة وتوفير الحماية للمعلومات والأشخاص على حد سواء، فقد أفرد الباب السابع من قانون العقوبات لمعالجة "المساس بأنظمة المعالجة الآلية للمعطيات"، في خطوة تهدف إلى إرساء الحماية الجنائية للمعاملات الإلكترونية، ولم يقف الأمر عند النص التجريمي فحسب، بل تجاوزه إلى إحداث آليات مؤسساتية وإجرائية، تمثلت في إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المرسوم الرئاسي رقم **15-261**، وعلى الصعيد الإجرائي، أتاح القانون رقم **09-04** جملة من الترتيبات التقنية التي تخوّل مراقبة الاتصالات الإلكترونية وتجميع محتواها وتسجيله في الزمن الحقيقي، إلى جانب إجراءات التفتيش والحجز داخل المنظومة المعلوماتية، وتندرج هذه التدابير جميعها في إطار سعي المشرّع للحفاظ على النظام العام، وتلبية متطلبات التحريات، وضمان الأمن المعلوماتي وذلك من خلال ما يلي:

[1] – القانون رقم:25-14 المؤرخ في:09 صفر عام 1447 الموافق لـ:03 غشت 2025 ج ر رقم:54-2025 المتضمن قانون الإجراءات الجزائية الجزائري .

[2] – القانون 09-04 المؤرخ في:14 شعبان 1430 الموافق لـ:05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر رقم:47/2009 .

– ضبط القانون لهذه الصلاحيات الاستثنائية بدقة، فلم يُبح مراقبة الاتصالات الإلكترونية وتجميع محتواها إلا بموجب إذن قضائي مكتوب، وفي حالات محددة على سبيل الحصر وهي: حالة الوقاية الاستباقية من جرائم الإرهاب والتخريب وأمن الدولة إذا بلغ التهديد حداً يطال البنى التحتية المعلوماتية الحيوية ويهدد كيان الدولة وأمنها واقتصادها. وكذا في حالة تعذّر إنجاز التحقيقات القضائية بوسائل أخرى، مما يجعل المراقبة ضرورة للوصول إلى الحقيقة. ثم في حالة الاستجابة لطلبات التعاون القضائي الدولي، كاشتراط جامع لضمان شرعية هذا الإجراء الخطير[1]

– كذلك وفي إطار تعزيز آليات البحث والتحري، خوّل المشرّع الجزائري للسلطات القضائية المختصة وضباط الشرطة القضائية صلاحية الدخول إلى أي منظومة معلوماتية أو جزء منها بغرض التفتيش، بما في ذلك المعطيات المخزنة في أي منظومة تخزين معلوماتي، وأجاز أن يتم هذا الدخول عن بُعد. ولم يقف نطاق هذا التفتيش عند حدود منظومة بعينها، بل امتد ليشمل أي منظومة معلوماتية أخرى إذا توافرت أسباب تدعو إلى الاعتقاد بأن المعطيات المبحوث عنها مخزنة فيها وبإمكانية الدخول إليها[2].

وتبرز أهمية هذه الصلاحية الاستثنائية في مواجهة جرائم مستحدثة كجريمة النصب الإلكتروني، التي تُعد من الجرائم الناشئة عن تطور استخدام الحاسوب والشبكة العنكبوتية، حيث يستغل الجاني هذه الوسائل التقنية المتطورة للاستيلاء على معلومات أو برامج أو معطيات الغير والاعتداء عليها، متخذاً من أساليب الخداع الإلكتروني المعقد وسيلة لإيقاع الضحايا، مما يصعّب عليهم اكتشافها، وتظل هذه الجريمة قائمة في جوهرها على وجود الشبكة العنكبوتية كركيزة لتنفيذها[3].

[1] – شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة دكتوراه، جامعة أدرار، الجزائر، 2021 ص 70 .

[2] – محمد جمال، التفتيش في الجرائم الالكترونية ماهيته وشروطه الشكلية، المجلة الأردنية في القانون والعلوم السياسية، عدد 03 جامعة الأردن، 2021، ص 84 .

[3] – المرجع نفسه، ص 86 .

الفرع الثالث: إرساء الأمن السيبراني

يضطلع الأمن المعلوماتي بدور فاعل في الحد من الجرائم المرتكبة عبر الإنترنت، ولا سيما النصب والاحتيال الإلكتروني، يتعيّن على كافة الحكومات والمنظمات المعنية التأكيد على أهمية اعتماد سياسات الأمن المعلوماتي والتوجيهات المنظّمة له، إلى جانب ضرورة تنسيق الجهود وتعزيز التعاون على تنفيذه على جميع المستويات، ومن هذا المنطلق تبرز الحاجة إلى تطوير وسائل الأمن السيبراني[1]، لمواجهة جريمة النصب الإلكتروني والتي تتمثل في:

- وضع معايير أمنية عالمية تتسم بالانسجام والتوافق مع الامتداد الجغرافي الواسع للشبكات المعلوماتية على أوسع نطاق في العالم، لإحصاء وتوقيف مجرمي النصب على المستوى الدولي إذ أن تطوير التوجهات والمعايير الأمنية يُعد نتاجاً تعاونياً مشتركاً بين مختلف الفاعلين وتسهيل نظام تسليم المجرمين في المجال المعلوماتي بين فيهم الحكومات والمنظمات الدولية[2].
- ترويج الخبرة الممارسة في معالجة جرائم النصب والاحتيال بين جميع الأطراف المعنية بأمن نظم المعلومات على مختلف مستوياتها، والعمل على تنويع هذه الخبرات عبر نشر الممارسات الفضلى في إعداد وتنفيذ سياسات محاربة جرائم النصب عبر الفضاء الرقمي، سعياً إلى الارتقاء بمستوى الخبرة والوعي بمفاهيم الممارسة الأمنية، وتأمين المؤسسات والأفراد من هذه الجريمة المستحدثة[3].
- إبرام عقود صحيحة وسليمة بين مختلف الأطراف المرتبطة بالمعاملات المالية الإلكترونية، وكذا بين المشاركين في عملية نقل المعلومات البنكية الإلكترونية، وتهدف هذه العقود إلى تمكين الأطراف من التحقق والتأكد أن المعلومات المرسلة هي ذاتها المعلومات المطلوبة، وأنها صادرة من مصادر معتمدة وموثوقة.

---

[1] – حورية معمر، الجرائم المعلوماتية في التشريع الجزائري والمواثيق الدولية، دار هومة، الجزائر، 2017، ص 145.

[2] – تنص المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010) على "تشجيع التعاون بين الدول الأطراف لوضع معايير موحدة في مجال أمن المعلومات". وتجسيداً لذلك، يشكل المعيار الدولي ISO/IEC 27001:2022 الإطار الأشمل لإدارة أمن المعلومات، وقد تم تطويره بمشاركة خبراء من 170 دولة، ليكون ثمرة تعاون بين الحكومات والقطاع الخاص والمستخدمين، للمزيد ينظر د. مليكة راجعي، الجريمة المعلوماتية وآليات مكافحتها على ضوء التشريع الجزائري والدولي، دار الأمة، الجزائر، 2019، ص 198.

[3] – فايزة شريفي، السياسة الجنائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2018، ص 180.

- تخصيص المخاطر وتحديد المسؤولية القانونية استناداً إلى قواعد تتسم بالفعالية والكفاءة، تكون ملزمة لجميع الأطراف المنخرطة في إجراءات الأمن السيبراني من مخاطر الاحتيال الالكتروني، كمتعهدي الاتصالات ومقدمي الخدمات للمستخدمين وغيرهم من الفاعلين، ويمتد نطاق هذه القواعد ليشمل النظم المتعددة المستخدمة في نقل المعلومات الخاصة بالحسابات المصرفية أو البنكية أو بطاقات الائتمان، والتي قد تخرج عن سيطرة أو مراقبة معالج المعلومات المختص وتبرز الحاجة إلى وجود قواعد أمن معلومات ناظمة لتخصيص المخاطر والمسؤولية القانونية بشكل خاص في حالات السرقة والاحتيال الالكتروني أو القرصنة التي تنجر عنها فقدان الاعتمادات الإلكترونية[1].

– إقرار عقوبات وجزاءات رادعة تُعد أدوات محورية في مجال استخدام نظم المعلومات، وتهدف إلى حماية الأطراف المعتمدة على هذه النظم وضمان توافر بياناتها وسريتها في مواجهة شتى الهجمات الالكترونية التي قد تلحق بها ضرراً، سواء تمثلت في إفشاء المعلومات أو الاحتيال بمختلف أساليبه لسلب أموال أفراد أو مؤسسات مصرفية.

المطلب الثاني: دور المؤسسات الحكومية في مكافحة جريمة النصب والاحتيال الالكتروني

إذا كانت النصوص القانونية التي استنّها المشرّع الجزائري تشكّل خط الدفاع الأول في التصدي لجرائم النصب والاحتيال المعلوماتي، فإن الاكتفاء بها يُعد قصوراً استراتيجياً في مواجهة إجرام يتطور بوتيرة متسارعة ويتجاوز الحدود، وعليه تبرز الحاجة الملحّة إلى تبنّي مقاربة تشاركية شاملة، تدمج البُعد التشريعي في إطار أوسع يضم الجهود المؤسساتية والتقنية والمجتمعية، لتشكّل بمجموعها استراتيجية وطنية متكاملة لمكافحة الجريمة الإلكترونية، وهنا تبرز مسؤولية مؤسسات الدولة الأساسية في تطبيق سياسات الوقاية والردع ضد هذه الجرائم، ويتجلى دورها بأبعاده الأمنية والقضائية والتوعوية في بناء بيئة رقمية آمنة تقوم على احترام القانون وصون الحقوق، لا سيما في ظل تنامي حجم الهجمات الاحتيالية التي تستهدف الأفراد والمؤسسات على حد سواء، كما يقتضي

[1] –عبد القادر بوخالفة، النظام القانوني لمكافحة الجرائم الإلكترونية، دار العلوم للنشر، الجزائر، 2019، ص 310.

البحث في دور مؤسسات الدولة التوقف عند أهم الهيئات الوطنية المنشأة خصيصاً لمواجهة الجريمة الإلكترونية، وعلى رأسها النصب والاحتيال الرقمي. وسنعمل في هذا المطلب إلى بيان مهام هذه الهيئات وصلاحياتها القانونية وآليات تدخلها العملية.[1]

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

بموجب القانون **09-04** المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2]، أوجد المشرع الجزائري هذه الهيئة التي أنشئت بموجب المادة **13** من نفس القانون. وتُسند إليها عدة مهام، أبرزها تفعيل التعاون القضائي والأمني على المستوى الدولي، وتنسيق العمليات ذات الطابع الوقائي، وتقديم المساعدة التقنية للأجهزة القضائية والأمنية. كما يُمكن تكليفها بإجراء خبرات قضائية في حالات الاعتداء على منظومة معلوماتية، سواء كان ذلك الاعتداء يُشكل تهديدًا لمؤسسات الدولة، أو للدفاع الوطني، أو للمصالح الاستراتيجية للاقتصاد الوطني[3].

كما نصت المادة **14** من القانون **09-04** على المهام الأساسية للهيئة، والتي نذكرها كما يلي:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[1] – يتجسد التنسيق العملي بين هذه الهيئات في مبادرات مشتركة، من أبرزها الملتقى الوطني الموسوم بـ"النصب والاحتيال في العالم الافتراضي "الذي نظمته قيادة الدرك الوطني يوم 18 فبراير 2025، بمشاركة ممثلين عن وزارة الدفاع الوطني، ووزارة البريد والمواصلات السلكية واللاسلكية، والمديرية العامة للأمن الوطني، وخبراء في الأمن السيبراني، وأفضى إلى توصيات عملية لتعزيز آليات الوقاية والتنسيق بين الجهات المختصة وتطوير وسائل الحماية الرقمية، الموقع https://www.mdn.dz/site_cgn/ 18022025 تم الإطلاع عليه بتاريخ:2026/05/16 الساعة 03:55.

[2] – المرسوم الرئاسي رقم 15-261 المؤرخ في 28 سبتمبر 2015، المتضمن إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية ، العدد 52، السنة 2015، المادة 14.

[3] - عمار بوحوش، النظام القانوني للأمن السيبراني، دراسة في ضوء التشريع الجزائري والمواثيق الدولية، دار الكتاب الحديث، الجزائر، 2020، ص 245.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك جمع المعلومات وانجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وتحديد مكان تواجدهم .

تُعتبر هذه الهيئة سلطة إدارية مستقلة مرتبطة بوزير العدل، وتخضع في عملها لإشراف ومراقبة لجنة مديرة يرأسها وزير العدل نفسه. تضم هذه اللجنة أعضاء حكوميين معنيين بموضوع الجرائم الإلكترونية، بالإضافة إلى مسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يُعيَّنان بقرار من المجلس الأعلى للقضاء. كما تتشكل الهيئة من قضاة ضباط وأعوان شرطة قضائية ينتمون إلى مصالح الاستعلامات العسكرية، والدرك الوطني، والأمن الوطني .ووفقًا لقانون الإجراءات الجزائية، تُسند إلى الهيئة مهمة تجميع وتسجيل وحفظ المعطيات الرقمية، وتحديد مصدرها ومسارها، وذلك بهدف استغلالها في الإجراءات القضائية. كما تضمن الهيئة مراقبة الاتصالات الإلكترونية والوقاية منها، بغرض كشف الجرائم المنصوص عليها في قانون العقوبات أو غيرها من الجرائم، ويكون ذلك تحت سلطة القاضي المختص.[1]

الفرع الثاني: وحدات مكافحة الإجرام السيبراني للأمن والدرك الوطنيين

بذلت المديرية العامة للأمن الوطني وجهاز الدرك الوطني جهودًا ملموسة في مكافحة الجرائم السيبرانية، تمثلت في استحداث فرق متخصصة لهذا الغرض، والعمل على تكوين عناصرها في هذا المجال. ولم تقتصر هذه الجهود على الجانب البشري فقط، بل امتدت إلى تعزيز القدرات التقنية، حيث يمتلك كلا الجهازين مخابر للشرطة العلمية والتقنية مزودة بأحدث الأجهزة والتكنولوجيا المتطورة، مما يمكنهما من كشف هذا النوع من الإجرام بفعالية.

[1] – سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق جامعة تيزي وزو، المجلد 17، العدد 02، 2022، ص 563 .

أولا: فرق مكافحة الجرائم السيبرانية لسلك الأمن الوطني

تُمثل الجرائم السيبرانية تحدياً جديداً يستلزم استحداث هياكل تنظيمية مبتكرة، إلى جانب تعزيز الهياكل القائمة والمختصة في مكافحة الجريمة على مستوى المديرية العامة للأمن الوطني. وبناءً على ذلك، قررت المديرية العامة للأمن الوطني إنشاء مخابر، وفرق، وفصائل متخصصة في مكافحة الجرائم الإلكترونية. ولا تقتصر مهام هذه الفرق على الجانب الردعي فحسب، بل تمتد لتشمل عمليات التحسيس والتوعية، وذلك من خلال المشاركة في الملتقيات الوطنية والدولية، وكذا جميع التظاهرات الهادفة إلى توعية المواطنين، بالإضافة إلى تقديم دروس توعوية في مختلف الأطوار الدراسية[1].

01/- نيابة مديرية الشرطة العلمية على المستوى المركزي

يتكون هذا الهيكل من مخبر مركزي يوجد بمقر المديرية العامة للأمن الوطني بالجزائر العاصمة، بالإضافة إلى ثلاثة مخابر جهوية موزعة على التراب الوطني. ويضم كل مخبر دائرتين متكاملتين: دائرة مخصصة للشرطة العلمية، وأخرى للشرطة التقنية. وتتمثل المهمة الأساسية للمخبر المركزي في المساهمة، إلى جانب أجهزة العدالة، في كشف الحقيقة وإظهارها، وذلك من خلال تقديم المساعدات الفنية التي تطلبها الهيئات القضائية، والتي تتعلق بتفسير وتحليل الآثار المادية التي يتم العثور عليها في مسرح الجريمة أثناء عمليات التحري والتحقيق القضائي[2].

[1] – مجلة إلكترونية للشرطة الجزائرية بموضوع: لأجل مجتمع واع في الفضاء السيبراني، العدد 158، 2024، الموقع: https://www.algeriepolice.dz/IMG/pdf/chorta_site، أطلع عليه بتاريخ:2026/05/17 .

[2] – المرسوم التنفيذي رقم 08-55 المؤرخ في 23 صفر 1429هـ الموافق 1 مارس 2008، المتضمن تنظيم المديرية العامة للأمن الوطني، ولاسيما المواد المتعلقة بتنظيم مخابر الشرطة العلمية والتقنية.

02/- دائرة الأدلة الرقمية والآثار التكنولوجية على المستوى الجهوي

إلى جانب المخبر المركزي المتمركز في الجزائر العاصمة، توجد مخبران جهويان يقعان في كل من مدينتي قسنطينة ووهران، ويتوليان مهام البحث والتحري في مختلف أنواع الجرائم، بما في ذلك الجريمة الإلكترونية، وذلك تحت مسمى "دائرة الأدلة الرقمية والآثار التكنولوجية". كانت هذه الدائرة في بداية استحداثها سنة **2004** مجرد قسم بسيط، غير أنها تتكون حالياً من ثلاثة أقسام متخصصة، وهي: (قسم استغلال الأدلة الرقمية الناتجة عن الحاسوب والشبكات، قسم استغلال الأدلة الناتجة عن الهواتف النقالة، قسم تحليل الأصوات).

كما تم بتاريخ: **25 أكتوبر 2023** تدشين المقر الجديد للمصلحة المركزية لمكافحة الجرائم السيبرانية، التابع لمديرية الشرطة القضائية، والذي جهز بكافة الوسائل التقنية العالية المستوى المتصلة بالتكنولوجيات الحديثة، وبالمورد البشري المتخصص، وحاليا خلال سنة **2026** أصبح على مستوى مقر أمن الولايات **69** فرقة متخصصة لمكافحة الجرائم السيبرانية[1].

ومن خلال الحصيلة السنوية للمديرية العامة للأن الوطني لسنة **2025** سجلت وفيما يخص بمحاربة الجرائم السيبرانية سجلت **1387** قضية تتعلق بالنصب والاحتيال عبر الأنترنيت، وبيع السلع المحظورة عبر شبكة الانترنت[2].

كما نفذت المصلحة المركزية لمكافحة الجرائم السيبرانية للأمن الوطني **(SCLC)** وفرقها المتخصصة، عملية واسعة النطاق شملت كافة ولايات الوطن استهدفت شبكات النصب والاحتيال عبر الأنترنيت، حيث تم توقيف **197** محتال إلكتروني ينشطون ضمن شبكات التصيد والاحتيال عبر الأنترنيت، حيث تم تفكيك **32** شبكة إجرامية منظمة مختصة في النصب عبر الأنترنت، من بينها شبكة دولية ينطلق نشاطها من إحدى البلدان الآسيوية مع توقيف **05** من عناصرها و من بينهم **31** شخص محل أوامر بالقبض متعلقة بجرائم النصب، كما كشفت التحليلات الجنائية

[1] – الموقع الرسمي لمديرية العامة للأمن الوطني، https://www.dgsn.dz ، تم الاطلاع عليه بتاريخ:2026/05/17 الساعة 18:46 .

[2] – المرجع نفسه، موقع المديرية العامة للأمن الوطني:https://www.algeriepolice.dz .

للمعطيات، عن الأساليب المنتهجة لجمع المعلومات عن الضحايا، التي اعتمدت على الهندسة الاجتماعية، التصيد الاحتيالي والهجمات عبر برمجيات سرقة المعلومات، وانتحال هوية شركات عمومية وخاصة، والتي ألحقت بالضحايا ضررا ماليا بالعملة الوطنية فاق الـ **52** مليار **و900** مليون سنتيم، بالإضافة إلى مبالغ مالية أخرى بالعملات الأجنبية.[1]

ثانيا: وحدات مكافحة الإجرام السيبراني التابعة للدرك الوطني

أولت قيادة الدرك الوطني اهتماماً بالغاً بمسألة مكافحة الجريمة السيبرانية بكافة أشكالها وأنواعها، إدراكاً منها للخطر المتزايد الذي يشكله الإجرام المعلوماتي على أمن الدولة وسلامة المجتمع، وقد تجسد هذا الاهتمام من خلال استحداث هياكل متخصصة تابعة لها، تمثلت في إنشاء أربع وحدات تعمل في مجال الوقاية من الجريمة الإلكترونية ومكافحتها[2]، كما تضطلع مؤسسة الدرك الوطني بمهمة ملاحقة مختلف الجرائم المرتكبة عبر شبكة الإنترنت، في إطار السعي لتيسير إجراءات البحث والمعاينة والتفتيش بأنظمة الحواسيب، إلى جانب القيام بعمليات مراقبة الشبكات وفقاً للاختصاصات والصلاحيات المخولة قانوناً وطبيعة الجريمة المطلوب كشفها، وقد تم توزيع هذه الهيكلة على ثلاثة مستويات تنظيمية: المستوى المركزي، والمستوى الجهوي، والمستوى المحلي.

01/- على المستوى المركزي

تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم السيبرانية ودعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

- مديرية الأمن العمومي والاستغلال: هي الهيئة تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم السيبرانية .

[1] - منشور لبيان إعلامي عبر الصفحة الرسمية عبر تطبيق **facebook** للصفحة الرسمية للشرطة الجزائرية، تم الاطلاع عليه بتاريخ:17-05-2026 الساعة 19:22 عبر الرابط https://www.facebook.com/algeriepolice.dz .

[2] - مرسوم رئاسي رقم 23-313 المؤرخ في 03/09/2023 يعدل ويتمم المرسوم رقم 09_143 المؤرخ في 2009/04/27 المتضمن مهام الدرك الوطني و تنظيمه. جريدة رسمية عدد 59 ، 2023 .

- المصلحة المركزية للتحريات الجنائية: هي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيات الإعلام والاتصال.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام(**INCC**) : [1]يُعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بموجب المرسوم الرئاسي رقم **04-183** المؤرخ في **26 جوان 2004** وذلك في إطار مساعي عصرنة قطاع الدرك الوطني وتعزيز قدراته العلمية والتقنية في مكافحة الجريمة بشتى أنواعها وتتمثل المهام الأساسية للمعهد في مجال الجرائم المعلوماتية في تحليل الأدلة الخاصة بهذا النوع من الإجرام، وذلك من خلال:

- تحليل الدعامات الإلكترونية (الأقراص الصلبة، بطاقات الذاكرة، الأجهزة الرقمية).
- إنجاز المقاربات الهاتفية (تحليل بيانات الاتصالات وتحديد موقعها).
- تحسين التسجيلات الصوتية والفيديو والصورة وتثبيتها، بغية تسهيل استغلالها كدليل قضائي.
- المساعدة العلمية في التحريات المعقدة خاصة التي تتطلب أدلة رقمية .
- مساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام .

وإلى جانب هذه المهام التقنية، يضطلع المعهد بمهام أخرى تشمل إنجاز الخبرات والتحاليل بناءً على طلبات القضاة والجهات القضائية، وتقديم الدعم التقني لوحدات الدرك الوطني أثناء التحقيقات المعقدة، والمساهمة في الدراسات والبحوث المتعلقة بالوقاية من الإجرام، فضلاً عن تنظيمه دورات تكوينية في علوم الأدلة الجنائية وعلم الإجرام.[2]

[1] – المرسوم الرئاسي 23-313 ، المتضمن مهام الدرك الوطني وتنظيمه، المرجع السابق.

[2] – منشور عبر الموقع الرسمي للمعهد الوطني لعلم الإجرام والأدلة الجنائية للدرك الوطني، تم الاطلاع عبر https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar. بتاريخ:2026/05/17 الساعة 23:31 .

- مركز الوقاية من جرائم الإعلام الآلي والجرائم السيبرانية: تم إنشاء هذا المركز في الآونة الأخيرة، ليكون بمثابة آلية وطنية محورية لدعم عمليات البحث والتحقيق المتعلقة بالجرائم السيبرانية وتتوزع أبرز اختصاصاته على النحو التالي:

- المراقبة المستمرة والدائمة للشبكة العنكبوتية.
- مراقبة الاتصالات الإلكترونية في الحدود التي يسمح بها القانون، وذلك لفائدة وحدات الدرك الوطني والسلطات القضائية.
- مساندة الوحدات الترابية للدرك الوطني في عملية معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، وجمع الأدلة الرقمية من شبكة الإنترنت.
- الإسهام في مكافحة الجرائم السيبرانية عبر التنسيق مع مختلف مصالح الأمن والهيئات الوطنية المعنية.

02/- على المستوى الجهوي

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف وحدات الشرطة القضائية، إلى جانب دعمها بالوسائل التقنية والفنية الخاصة اللازمة لإجراء التحريات والأبحاث المعقدة، ولا سيما تلك المتعلقة بالجرائم السيبرانية.

03/- على المستوى المحلي

يضم الدرك الوطني فصائل بحث متخصصة، تتركب من أفراد يتمتعون بخبرة واسعة وكفاءة عالية في ميدان الشرطة القضائية. وتُسند لهذه الفصائل مهمة مكافحة الأشكال الخطيرة للإجرام المنظم، وفي مقدمتها الجرائم السيبرانية، وذلك من خلال إجراء تحقيقات تتطلب تحريات معقدة. وتساهم هذه الوحدات النوعية في تعزيز ودعم نشاط البحث والتحري الذي تقوم به الفرق الإقليمية للدرك الوطني[1].

[1] - المرسوم الرئاسي 23-313 ، المتضمن مهام الدرك الوطني وتنظيمه، المرجع السابق.

وبشأن مكافحة الإجرام السيبيراني سجلت قيادة الدرك الوطني خلال سنة **2025** ما يفوق **950** قضية نصب واحتيال سيبيراني، أي بنسبة **31 %** من إجمالي القضايا السيبرانية المسجلة والمقدرة بـ:**3064** قضية.[1]

الفرع الثالث: الهيئات القضائية الخاصة بالبحث في الجرائم الالكترونية

تتمثل الهيئات القضائية المختصة بالبحث في الجرائم الإلكترونية في الأقطاب القضائية المتخصصة، التي استحدثها المشرع الجزائري بموجب القانون رقم **04-14** المؤرخ في **10** نوفمبر **2004**، المعدل والمتمم لقانون الإجراءات الجزائية، تمتاز هذه الجهات القضائية المتخصصة باختصاصها النوعي في النظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المعلوماتية)، وهو ما يمثل نقلة نوعية في مجال مكافحة الجريمة الإلكترونية، ومن بين أبرز التعديلات الجديدة التي أدخلها المشرع في الشق التشريعي المتعلق بمكافحة الجرائم المعلوماتية، هو توسيع الاختصاص الإقليمي للأقطاب الجزائية المتخصصة، حيث نص صراحةً على تمديد الاختصاص المحلي ليشمل نطاقاً أوسع من الدائرة القضائية التقليدية[2].

أولا: الاختصاص الإقليمي للأقطاب الجزائية المتخصصة

استحدث المشرع الجزائري جهازاً قضائياً متخصصاً للنظر في القضايا الجزائية الخطيرة، تمثل في الأقطاب الجزائية المتخصصة، وذلك بموجب المرسوم التنفيذي رقم **06-348** المؤرخ في **12** رمضان **1427هـ** الموافق **5** أكتوبر **2006**، الذي تضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق .وقد حدد هذا المرسوم أربع محاكم على المستوى الوطني تتمتع باختصاص محلي موسع، وهي :محكمة سيدي امحمد بالجزائر العاصمة، محكمة قسنطينة، محكمة وهران، ومحكمة ورقلة.

[1] – عرض للحصيلة السنوية لسنة 2025 عبر الموقع الرسمي لجهاز الدرك الوطني تم نشره بتاريخ:2026/04/19، https://www.mdn.dz/site_cgn ، تم الاطلاع عليه بتاريخ:2026/05/16 الساعة 17:35 .

[2] – سوماتي شريفة،" القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص"، مجلة الدراسات القانونية، المجلد 8، العدد 2، جامعة المدية الجزائر، الصفحة 479.

ثم جاء الأمر رقم **21-11** المؤرخ في **25** أوت **2021**، المتمم لقانون الإجراءات الجزائية، ليستحدث القطب الجزائي الوطني المتخصص لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في خطوة متقدمة لتعزيز فعالية مكافحة الجريمة الإلكترونية على المستوى الوطني.

01/- محكمة سيدي امحمد

تقع محكمة سيدي امحمد بالجزائر العاصمة، وقد مُنحت بموجب المرسوم التنفيذي رقم **06-348**[1] اختصاصاً إقليمياً موسعاً يغطي محاكم تنتمي إلى دوائر اختصاص عشرة **(10)** مجالس قضائية موزعة في وسط وشمال القطر الجزائري. وهي بذلك تعد أداة قضائية محورية في إطار سياسة التخصص القضائي التي انتهجها المشرع لمواجهة أشكال الجريمة من بينها الجرائم السيبرانية.

02/- محكمة قسنطينة

تقع بمدينة قسنطينة ويمتد اختصاصها لـ:**12** مجلس قضائي يشمل إداريا ولايات الشرق وجنوب شرق الجزائر .

03/- محكمة وهران

تقع بولاية وهران ويمتد اختصاصها الإقليمي إلى نطاق اختصاص المجالس القضائية **14** أربعة عشر بالغرب وجنوب غرب الوطن.

04/- محكمة ورقلة

تقع في مدينة ورقلة ويمتد اختصاصها الإقليمي إلى نطاق اختصاص المحاكم التابعة للمجالس القضائية لكل من ولاية: ورقلة، تمنراست، إليزي، تندوف، غرداية، أدرار، أي يمتد إلى **06** ولايات بالجنوب الكبير .[2]

[1] - المرسوم التنفيذي رقم 06-348 المؤرخ في 12 رمضان 1427هـ الموافق 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق (الجريدة الرسمية، العدد 63، 2006)، لاسيما المادة 2 منه.

[2] - فرقاق معمر، رابح وهيبة، القواعد الإجرائية الخاصة بالأقطاب الجزائية المتخصصة، جامعة عبد الحميد إبن باديس مستغانم، مجلة البحوث القانونية والسياسية، العدد 03، 2014، ص 227 .

05/- القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

حرص المشرع الجزائري على استغلال التطور العلمي والتكنولوجي في الارتقاء بمستوى العمل القضائي من أجل التصدي للجرائم السيبرانية، حيث أنشأ القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال على مستوى محكمة مقر مجلس قضاء الجزائر من أجل متابعة والتحقيق في هذه الجرائم والجرائم المتصلة بها.

وتنص المادة **336** من قانون الإجراءات الجزائية الجديد **25-14** [1]على:" يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وقاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه، وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن والسكينة العامة أو استقرار المجتمع.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام و الأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
- جرائم التمييز وخطاب الكراهية. "

ثانيا: تمديد الاختصاص المحلي

من بين القواعد الإجرائية لمواجهة الجريمة السيبرانية تمديد الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية:

[1] - القانون رقم:25-14 المؤرخ في:09 صفر عام 1447 الموافق لـ:03 غشت سنة 2025 ج ر رقم 54، المتضمن قانون الإجراءات الجزائية .

01/- تمديد الاختصاص المحلي لوكيل الجمهورية

نصت المادة **91** من القانون **25-14** أنه يجوز لوكيل الجمهورية تمديد الاختصاص إلى المحاكم المتاخمة للمحكمة التي يزاول فيها مهامه لمتابعة تحرياته إذا اقتضى التحقيق ذلك .[1]

02/- تمديد الاختصاص المحلي لقاضي التحقيق

نصت المادة **91** من القانون **25-14** أنه يجوز لقاضي التحقيق تمديد المحلي إلى محاكم أخرى لمقتضيات التحقيق.

03/- تمديد الاختصاص المحلي لضباط الشرطة القضائية

وفقًا للمادة **24** من قانون الإجراءات الجزائية الجديد القانون رقم **25-14**، يتحدد المبدأ العام للاختصاص المكاني لضباط الشرطة القضائية في نطاق أدائهم لوظائفهم الاعتيادية، ويكون عملهم تحت سلطة وإدارة وكيل الجمهورية في مرحلة جمع الاستدلالات، كما يخضعون لإشراف قاضي التحقيق عند مباشرة التحقيق القضائي سواءً في موقع ارتكاب الجريمة أو مكان توقيف المشتبه فيهم أو محل إقامتهم. ويرد على هذا الأصل استثناءٌ يسمح لهم بامتداد اختصاصهم في حالات الاستعجال ليشمل دائرة المجلس القضائي كاملة أو حتى النطاق الوطني بطلب من القاضي المختص.[2]

مما تقدم، يتبين أن المنظومة المؤسساتية المكلفة بالتصدي للجريمة السيبرانية تتوزع بين هيئات فنية متخصصة في البحث والتحري عن الجرائم الإلكترونية، تشمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومصالح الأمن الوطني والدرك الوطني، وهيئات قضائية متخصصة في البحث عن هذه الجرائم، تتمثل في الاختصاص الإقليمي للأقطاب الجزائية المتخصصة وتمديد الاختصاص المحلي لضباط الشرطة القضائية.

[1] – المادة 91 من القانون 25-14، المتضمن قانون الإجراءات الجزائية .

[2] – بن عودة نبيل، نوار محمد: الصلاحيات الحديثة للضبطية القضائية للكشف وملاحقة مرتكبي الجرائم المتعلقة بالتمييز وخطاب الكراهية" التسرب الإلكتروني نموذجا"، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، المجلد 01، العدد 02، 2020، ص 326

الفرع الرابع: الوسائل الإعلامية للوقاية من النصب والاحتيال الإلكتروني

تجاوزت وسائل الإعلام دورها التقليدي في نقل الأخبار، لتُصبح دعامة محورية في جهود التوعية والتحسيس بمخاطر المعاملات الإلكترونية. وتتوزع هذه الوسائل بين فئتين: الإعلام التقليدي المتمثل في القنوات التلفزيونية والإذاعات والصحف الورقية، والإعلام الرقمي الذي يضم المواقع الإلكترونية وشبكات التواصل الاجتماعي والمدونات التوعوية، وقد اضطلعت هذه الوسائل بدور جوهري في إشاعة ثقافة الاستهلاك المأمون، من خلال برامج تحسيسية وحملات تنبيهية من جرائم النصب الرقمي، وبلاغات إرشادية تُوضح للمستهلكين سبل التأكد من موثوقية المتاجر الإلكترونية وقواعد التعامل الآمن عبر الشبكة[1].

وبفضل هذا الدور، تحولت الوسائل الإعلامية إلى إحدى أبرز أدوات القوة الناعمة الفاعلة في تشكيل وعي قانوني وتكنولوجي لدى المستهلك الرقمي، مما يُتمم الجهود التشريعية والإدارية المبذولة في هذا الشأن[2].

أولا: الحملات التحسيسية عبر وسائل الإعلام التقليدية

تضطلع وسائل الإعلام التقليدية، وعلى رأسها التلفزيون والإذاعة والصحافة المكتوبة، بدور محوري في ترسيخ الوعي بالأمن القومي والتصدي للجرائم السيبرانية، وذلك عبر برامج متخصصة تُعنى بشرح مفاهيم الأمن الرقمي، واستضافة خبراء لكشف أساليب الاحتيال الشائعة وتبيان سبل الوقاية منها. وتُسهم هذه الوسائل في توعية الجمهور بمخاطر الفضاء الإلكتروني، فضلاً عن تغطيتها لأخبار الجرائم المعلوماتية وتحليلها لطرق المحتالين، مما يُمكّن الأفراد من استشراف التهديدات المحتملة واتخاذ التدابير الوقائية الملائمة[3]. ومن أمثلة ذلك: بث حصص إذاعية من

[1] – عبد الله بن سعود السراني، دور الإعلام الأمني في الوقاية من الجريمة، الإعلام الأمني بين الواقع والتطلعات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، السعودية، 2012، ص 45 .

[2] – صليحة بوشنافة، دور وسائل الإعلام في التوعية بمخاطر الجريمة الإلكترونية، مجلة الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية بجامعة الأغواط، المجلد 08، العدد 01، 2022، ص 351 .

[3] – نادية بوعزة، الإعلام والأمن السيبراني في الجزائر، مجلة علوم الإعلام والاتصال، المجلد 05، العدد 02، 2021، ص 117.

قِبل مختصين تُحذّر من خطورة إفشاء بيانات البطاقة البنكية أو البريدية عبر مواقع التواصل الاجتماعي لأشخاص مجهولين، وهو ما يُعزز قدرة المواطنين على تجنب الاستيلاء على أموالهم من حساباتهم البريدية[1].

وعلاوة على ما سبق، تتعاون وسائل الإعلام مع الهيئات الأمنية (كمصالح الأمن الوطني والدرك الوطني) والهيئات القضائية، وذلك من خلال نشر البلاغات الرسمية والتحذيرات المتعلقة بالجرائم الإلكترونية. كما تشارك هذه الوسائل في الملتقيات الوطنية الهادفة إلى مناقشة التحديات المرتبطة بالأمن السيبراني وتبادل الخبرات، وتساهم في إنتاج محتوى مشترك للتوعية على المستويين القانوني والتقني. ويعزز هذا التعاون من فهم الجمهور للقوانين المتعلقة بالجرائم الإلكترونية وسبل الحماية منها، وهو ما يهدف إلى بناء مجتمع أكثر وعياً وقدرة على مواجهة التهديدات الرقمية المتزايدة[2].

ثانيا: الصحافة الإلكترونية والمواقع الإخبارية

تؤدي الصحافة الإلكترونية والمواقع الإخبارية دوراً محورياً في الوقاية من جرائم النصب والاحتيال عبر الأنترنيت، وذلك من خلال وظيفتها التوعوية والإعلامية التي تصل إلى شريحة واسعة من الجمهور بشكل فوري ومستمر، فبالإضافة إلى نقل الأخبار، باتت هذه الوسائل شريكاً استراتيجياً للهيئات الأمنية والقضائية في نشر ثقافة الحماية الرقمية. فهي تنشر تحذيرات أمنية دورية حول الأساليب المستحدثة التي يعتمدها المحتالون، كالرسائل الاحتيالية (**Fishing**) والروابط المزيفة وعمليات النصب عبر منصات التواصل الاجتماعي. كما تساهم في شرح القوانين المتعلقة بالجرائم الإلكترونية بلغة مبسطة، مما يمكن المواطن العادي من فهم حقوقه والإجراءات الواجب اتباعها عند التعرض لعملية احتيال، كما تتيح منصاتها التفاعلية مساحات للحوار المباشر بين الخبراء الأمنيين والجمهور، لطرح الاستفسارات وتلقي النصائح المخصصة، علاوة على ذلك، تنشر هذه المواقع

[1] – القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، 2018.

[2] – المادة 38 من القانون 09-04 تنص على "تتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تنشيط وتنسيق العمليات الوقائية والتوعوية بالتنسيق مع القطاعات المعنية، ومن بينها الإعلام "

قصصاً حقيقية لضحايا النصب الإلكتروني، بعد تحويلها إلى مواد توعوية تحلل أسباب سقوط الضحية وكيفية تجنبها.[1]

ومن مهامها أيضاً، فضح مواقع الويب والتطبيقات المشبوهة ونشر تقارير استقصائية تكشف خلفياتها، مما يحمي الجمهور من الوقوع في فخاخها. ولا يقتصر دورها على الجانب الوقائي فقط، بل تتوسع إلى رصد الجرائم المستجدة وتحليل أنماطها، وتقديم هذه المعطيات للجهات الرسمية لاستباق الهجمات. كما تساهم في تعزيز التعاون بين الإعلام والأمن بتغطية الحملات التحسيسية التي تشنها المصالح الأمنية ونقل رسائلها للجمهور دون تحريف. ومن المهم الإشارة إلى أن هذه المواقع تلتزم بمعايير مهنية رفيعة، كالدقة وعدم نشر الذعر، والتأكد من المعلومات قبل بثها، لما لذلك من تأثير بالغ على المصداقية والثقة الجماهيرية. هذا الدور المزدوج التوعوي والوقائي جعل من الصحافة الإلكترونية خط دفاع أول ضد الجرائم الرقمية، مما يسهم في بناء مجتمع أقل عرضة للاستغلال وأكثر قدرة على الصمود في وجه التهديدات الإلكترونية المتطورة.

ثالثا: الإعلام الرقمي ومنصات التواصل الاجتماعي

تتولى منصات التواصل الاجتماعي والإعلام الرقمي دورًا وقائيًا متزايد الأهمية في إطار سياسات الحد من جرائم الاحتيال الإلكتروني، وذلك من خلال آليات متعددة تندرج ضمن المسؤولية المجتمعية لهذه الوسائل، أولها نشر الوعي الحقوقي والقانوني للمستخدمين حول وسائل الحماية من هجمات التصيد الإلكتروني (**Phishing**) والهندسة الاجتماعية، وثانيها توفير نظم للإبلاغ الفوري

[1] – حملة تحسيسية وطنية أشرفت عليها وزارة البريد والمواصلات السلكية واللاسلكية حول النصب والاحتيال عبر الأنترنيت تحت شعار " لا تشارك معلوماتك الشخصية عبر الأنترنت. كن يقظا، فالمحتال ينتظر الفرصة" من 10 الى 30 ماي 2025، وهذا وبمساهمة كل وزارة الشؤون الدينية و الأوقاف ، وزارة التعليم العالي والبحث العلمي، وزارة التربية الوطنية، وزارة الاتصال، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، إلى جانب الوكالة الوطنية لأمن الأنظمة المعلوماتية، قيادة الدرك الوطني والمديرية العامة للأمن الوطني، تم الاطلاع عليه عبر الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية : https://www.mpt.gov.dz بتاريخ:2026/05/20 الساعة:00:30 .

عن الحسابات والصفحات المشبوهة، وثالثها التعاون الإلزامي مع السلطات القضائية والأمنية في تتبع مرتكبي هذه الأفعال[1].

وتُعد حملات التوعية التفاعلية الممنهجة عبر مختلف المنصات المعروفة مثل: "يوتيوب" و"إنستغرام" و"فايسبوك"و" تيك توك " من أنجح الوسائل الاستباقية في تحصين الجمهور من الجرائم الإلكترونية، خاصة مع اعتماد الشرطة التقنية لمقاربة الشراكة مع الخبراء الرقميين والمؤثرين لنشر رسائل وقائية بلغة مبسطة وأمثلة واقعية من الأحكام القضائية. كما تسهم المنصات في تفعيل مبدأ "الحماية بالتصميم (**Security by Design**) "من خلال تطوير سياسات الخصوصية وتفعيل أدوات المصادقة الثنائية وتنبيه المستخدمين عند استلام رسائل احتيالية. ومن المهم التأكيد على أن فاعلية هذه الأدوار ترتهن بتظافر الجهود بين القطاع الخاص (مالك المنصات) والمشرع، مع إلزامية تضمين إشعارات تحذيرية فورية عند اكتشاف محتوى احتيالي محتمل، وذلك وفقًا لالتزامات العناية الواجبة المقررة قانونًا على وسطاء الخدمات الرقمية. لذلك يتحول الإعلام الرقمي بموجب هذه المقاربة من مجرد فضاء لارتكاب الجريمة إلى حاجز وقائي معول عليه، شريطة أن يواكبه إطار تشريعي رادع وأن تترافق معه مبادرات لرفع درجة اليقظة الرقمية لدى العموم بتدريبهم على الإبلاغ السريع وإثبات الدليل الرقمي[2].

[1] – أحمد فتحي سرور، جرائم الاحتيال الإلكتروني: دراسة مقارنة بين القانون الجنائي وقانون المعاملات الإلكترونية، ط03 ، دار النهضة العربية للنشر، مصر، 2022، ص 189 .

[2] – سليمان بن عبد العزيز العمر، "آليات منصات التواصل الاجتماعي في مكافحة الاحتيال الإلكتروني: دراسة تحليلية لسياسات الحماية والإبلاغ"، مجلة الأمن والقانون جامعة نايف العربية للعلوم الأمنية، المجلد 31، العدد 2، 2024، الصفحة88 .

ملخص الفصل الثاني:

شهد العصر الرقمي تحولاً محورياً بفعل انتشار تقنيات الذكاء الاصطناعي، التي باتت سلاحاً ذو حدين، إذ تستخدم في تطوير الخدمات المالية والإنتاجية من جهة، وتوظف من قبل المجرمين لتنفيذ جرائم النصب والاحتيال الإلكتروني بأساليب متطورة يصعب اكتشافها من جهة أخرى، وقد تم إبراز من هذا الفصل أن المجرمين يستغلون آليات متعددة مثل: التزييف العميق **(Deepfake)** لتركيب صور وفيديوهات مزيفة تُنسب لأشخاص حقيقيين بهدف خداع الضحايا، والتزييف الصوتي لاستنساخ أصوات المسؤولين وطلب تحويلات مالية، والتصيد الاحتيالي المُولَّد آلياً الذي ينتج رسائل إلكترونية فائقة الدقة يصعب تمييزها عن المراسلات الرسمية، وأتمتة جمع المعلومات لاستخراج كميات هائلة من البيانات الشخصية والمالية دون موافقة أصحابها.

وفي مواجهة هذه الجرائم تم التطرق إلى الإطار القانوني الجزائري المجرم والمعاقب لهذه الأفعال المستحدثة، مستعرضاً أحكام قانون العقوبات المعدل والقانون رقم **09-04** المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فضلاً عن انضمام الجزائر للاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وعلى المستوى المؤسساتي، بيّن الفصل دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ووحدات مكافحة الجرائم السيبرانية في الأمن والدرك الوطنيين، والأقطاب القضائية المتخصصة التي وسّع المشرع اختصاصها المحلي لمتابعة هذه الجرائم العابرة للحدود. وخلص الفصل إلى أهمية الوسائل الإعلامية بمختلف أنواعها (التقليدية والرقمية ومنصات التواصل الاجتماعي) في نشر الوعي القانوني والتقني، عبر حملات تحسيسية وإشعارات فورية وآليات إبلاغ عن الحسابات المشبوهة، مما يجعلها خط دفاع أول في تحصين الجمهور من مخاطر النصب المعزز بالذكاء الاصطناعي.

الخاتمة

الخاتمة:

تُعد جرائم النصب والاحتيال المعززة بتقنيات الذكاء الاصطناعي من أبرز التحديات المعاصرة التي تواجه النظم القانونية على المستويين الوطني والدولي، وذلك لما تطرحه من إشكاليات مرتبطة بالتطور المتسارع لوسائل الاتصال، وما وفره التحول الرقمي من بيئات افتراضية جديدة تفلت غالباً من آليات الرقابة التقليدية. وتكمن خطورة هذه الجرائم بالأساس في قدرتها على تجاوز الحواجز المؤسساتية، بالإضافة إلى صعوبة تتبع مرتكبيها الذين يتوارون خلف تقنيات التشفير والهويات الرقمية المصطنعة.

لقد تناولت هذه الدراسة جريمة النصب والاحتيال في سياق استغلال الذكاء الاصطناعي بأبعادها المتعددة، سعياً إلى تقديم تحليل نقدي للإطار القانوني الجزائري المنظّم لهذه الجريمة، ومدى قدرته على مواكبة التحولات الرقمية الراهنة، خصوصاً في ظل تزايد المخاطر التي تتهدد الأصول المالية للأشخاص، سواء كانوا أفراداً عاديين أو فاعلين اقتصاديين، نتيجة الاستغلال الإجرامي للفضاء السيبراني.

خلصت الدراسة إلى أن جريمة النصب والاحتيال باستخدام الذكاء الاصطناعي أو أي وسيلة إلكترونية تتشابه من حيث الأركان الجوهرية مع نظيرتها التقليدية، إذ تقوم على سلوك احتيالي يهدف إلى خداع المجني عليه والاستيلاء على أمواله دون سند قانوني، بيد أن الجريمة الإلكترونية تتميز بخصائص تقنية وقانونية فريدة توجب معالجتها بأدوات خاصة، أبرزها الطبيعة غير الملموسة للوسيلة المستعملة كالصفحات والمواقع الإلكترونية المزيفة، والطابع العابر للحدود الوطنية الذي يميز الجرائم السيبرانية، فضلاً عن صعوبة تتبع الأدلة الرقمية للجريمة، مما يعيق إلقاء القبض على الجناة.

أما بالنسبة للتشريع الجزائري، فقد أثبتت الدراسة أن المشرع قطع أشواطاً إيجابية في التصدي لهذه الظاهرة الإجرامية، سواء بتعديل قانون العقوبات وإضافة أحكام متعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، أو بإصدار القانون رقم: **09-04** المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما أكدت الدراسة على أهمية الأمن السيبراني باعتباره آلية وقائية للحد من هذه الجرائم، وضرورة تعزيز القدرات الوطنية في مجال التحقيق الرقمي، وتنسيق العمل بين مختلف الهيئات المعنية كالهيئة الوطنية للوقاية من الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال، ومصالح الأمن والدرك الوطنيين، والشرطة العلمية والتقنية، مع التأكيد على الدور المحوري للإعلام والمجتمع المدني في نشر الوعي بمخاطر الفضاء الإلكتروني، كما خلصت الدراسة أيضاً أن الجهود القائمة تبقى غير كافية في مواجهة الوتيرة المتسارعة لتطور الجريمة الرقمية.

وعلى ضوء ما تقدم، تقترح الدراسة مجموعة من التوصيات الرامية إلى تعزيز فعالية المنظومة الجزائية في مواجهة النصب والاحتيال بواسطة الوسائط الرقمية والذكاء الاصطناعي، وهي كالتالي:

أولاً: تحديث الإطار التشريعي الجنائي من خلال مراجعة وتحيين القوانين الجنائية لتستوعب صور الاحتيال المستحدثة باستخدام الذكاء الاصطناعي، مثل التزييف العميق (**Deepfakes**)، والهندسة الاجتماعية المعززة بالخوارزميات، مع وضع تعريفات دقيقة للأفعال الإجرامية الرقمية.

ثانيا: تجريم الأدوات المستخدمة في الاحتيال الذكي مثل إنتاج أو توزيع أو استعمال البرمجيات والنماذج الذكية التي تُصمم خصيصًا لغايات احتيالية، مع التمييز بينها وبين الاستخدامات المشروعة.

ثالثا: تعزيز التعاون الدولي على اعتبار أن الجرائم الرقمية عابرة للحدود، ينبغي دعم آليات التعاون القضائي والأمني بين الدول لتسهيل تتبع الجناة وجمع الأدلة الرقمية وتسليم المجرمين.

رابعا: تطوير قدرات الأجهزة الأمنية والقضائية من خلال تدريب القضاة وأعوان الضبط القضائي على فهم تقنيات الذكاء الاصطناعي وأساليب الاحتيال الحديثة، حتى يتم التعامل مع الأدلة الرقمية بكفاءة ووعي تقني.

خامسا: تعزيز الحماية التقنية والوقائية بتشجيع المؤسسات المالية والمنصات الرقمية على اعتماد أنظمة كشف الاحتيال المعتمدة على الذكاء الاصطناعي، مثل أنظمة كشف السلوك غير الطبيعي والتحقق متعدد العوامل.

سادسا: نشر الوعي الرقمي لدى الأفراد من خلال إطلاق حملات توعية لتحذير المستخدمين من مخاطر الاحتيال الإلكتروني، خاصة عبر الروابط المزيفة، المكالمات المولدة بالذكاء الاصطناعي، والرسائل الاحتيالية.

سابعا: إرساء مسؤولية مزودي خدمات الذكاء الاصطناعي بفرض التزامات على الشركات المطورة للتقنيات الذكية لضمان عدم إساءة استخدام أدواتها، من خلال آليات مراقبة داخلية وسياسات استخدام واضحة.

ثامنا: دعم البحث العلمي في هذا المجال وتشجيع الدراسات القانونية والتقنية المتخصصة في الجرائم السيبرانية والذكاء الاصطناعي، لتطوير حلول استباقية بدل الاقتصار على الردع بعد وقوع الجريمة.

الملاحق

نداء للجمهور

طبقا للأحكام المادة 26من قانون الإجراءات الجزائية وعملا بالإذن الصادر عن نيابة الجمهورية لدى محكمة سكيكدة، تنهي مصالح أمن ولاية سكيكدة ممثلة في فرقة مكافحة الجرائم السيبرانية إلى علم المواطنين ، أن هذا الشخص الظاهر في الصورة المدعو"ب.ع.إ " المستغل للرقم الهاتفي، و الحساب البريدي المذكورين في الجدول أدناه، مشتبه في تورطه في قضايا النصب الموجه للجمهور عبر منصات التواصل الاجتماعي.

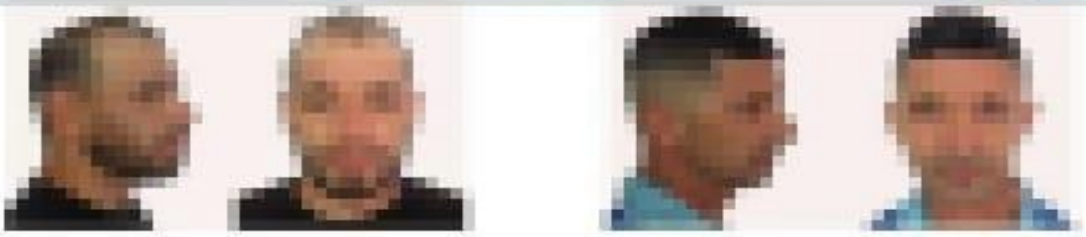
صفحة فايسبوك DET Al

الرقم الهاتفي	حساب بريدي
0561.89.53.86	24632966 مفتاح 79

في هذا الصدد، توجه مصالح أمن ولاية سكيكدة، نداء لكل شخص يكون قد وقع ضحية للسالف الذكر، أو له معلومات بوصفه شاهدا التقرب إلى النيابة الجمهورية بمحكمة سكيكدة ، او فرقة مكافحة الجرائم السيبرانية بأمن ولاية سكيكدة لتقييد شكوى أو الإدلاء بشهادة في قضية الحال .

الملاحق:

نداء للجمهور



طبقا لنص المادة 26 من قانون الإجراءات الجزائية، وعملا بالإذن النيابي الصادر عن السيد وكيل الجمهورية لدى محكمة عين الكبيرة، تنهي مصالح أمن ولاية سطيف إلى علم المواطنين أن الشخصين الظاهرين بالصور أعلاه المدعوين (ع ل) و (ن ن) مشتبه فيهما في قضية النصب باستعمال تكنولوجيا الإعلام والاتصال، حيث يتصلان هاتفيا بضحاياهما على أساس أنهما عمال بمؤسسة "بريد الجزائر"، بعدها يطلبان منهم إرسال صور للبطاقات الذهبية عن طريق واتساب، ثم موافاتهما بالرمز المرسل إليهم، في نهاية العملية يقوم المشتبه فيهما بسحب وتحويل المبالغ المالية من حسابات الضحايا، كما يستعملان طريقة أخرى للنصب على ضحايا آخرين باستغلال موقع التواصل الاجتماعي فيسبوك، عن طريق إيهامهم بتسهيل شراء مركبات من الوزن الثقيل من ولاية باتنة بالتقسيط.

الأرقام الهاتفية	الأرقام الهاتفية	الحسابات البريدية الجارية
0773824810	0779443194	19492380 clé 81
0549160266	0563056931	22811511 clé 68
0668070448	0668408598	22541924 clé 21

اسم الصفحة	رقم الهاتف	الصورة التعريفية للصفحة
Tirsam Algerie	0668.84.56.63 0562.70.33.25	تيرصام TIRSAM Tirsam Algérie
TIRSAM ALGERIE	0668.84.56.63 0674.38.96.98 0562.70.33.25	 Tirsam Algérie

في هذا الصدد توجه مصالح أمن ولاية سطيف، نداء لكل شخص وقع ضحية للسالفي الذكر سواء التقى بهما شخصيا أو تعامل معهما عن طريق الهاتف أو مواقع التواصل الاجتماعي أو يملك معلومات بصفته شاهدا، الاتصال بنيابة الجمهورية لدى محكمة عين الكبيرة، أو أمن دائرة عموشة.

الملاحق:

نداء للجمهور

الجزائر يوم 15 ماي 2026



طبقا لأحكام المادتين 19 و 26 من قانون الإجراءات الجزائية، وعملا بالإذن الصادر عن السيد وكيل الجمهورية لدى محكمة عنابة، تنهي المجموعة الإقليمية للدرك الوطني بعنابة، إلى علم المواطنين أنها قامت بتوقيف الشخص الظاهر في الصورة المسمى (ب م س) المتورط في قضية سلب مال الغير عن طريق النصب والاحتيال التهديد الشفهي برسالة صوتية بإستعمال تكنولوجيا الإعلام والإتصال، وهذا باستغلال الأرقام الهاتفية والحسابات المذكورة في الجدول أدناه.

الأرقام الهاتفية	حسابات مواقع التواصل الاجتماعي فايس بوك	حساب التيك توك	حساب الإنستغرام
0659.99.94.20 0549.31.40.86	Samy Salvator Karim Ahlouche Ne Si Samy	Yaniss benz Ramiben413	Samy Salvador

في هذا الصدد توجه مصلحة البحث والتحري للدرك الوطني بعنابة، نداء لكل شخص يكون قد وقع ضحية نصب واحتيال من خلال التعامل معه عن طريق الهاتف أو عن طريق الحسابات السالفة الذكر، التقرب إلى نيابة الجمهورية لدى محكمة عنابة أو مقر مصلحة البحث والتحري للدرك الوطني بعنابة أو التقرب إلى أقرب فرقة للدرك الوطني عبر تراب الجمهورية، لتقييد شكوى أو الإدلاء بشهادة الحال.


الشرطة الجزائرية
2j
الإحتيال الإلكتروني
مصالح البريد - البنك
يرجى تحديث بياناتك فورا لتجنب تجميد حسابك، اضغط على الرابط التالي : www.poste/bank.com
يرجى تصوير بطاقتك البريدية /البنكية من الجهتين و إرسالها لتفوز معنا بقيمة مالية (00000000؟ دج)
يرجى إرسال رمز التحقق الذي تم إرساله في رقم هاتفكم (OTP)
- إشعارات -
لقد تم سحب مبلغ (100.000 دج)
من حسابك البريدي / البنكي
كيف تحمي نفسك
إحمي بياناتك الشخصية
موظف مصالح البريد أو البنك لا يطلب منك بياناتك الشخصية أو تصوير بطاقتك البريدية أو البنكية
إنتبه للرسائل المشبوهة
SPAM
WWW.SPAM.URL
إنتبه للرسائل المشبوهة و المواقع غير المحمية
لا تتواصل مع مجهولي الهوية
لا تتواصل مع مجهولي الهوية أو منتحل شخصية تأكد دائما من هوية الشخص الذي تتواصل معه
التبليغ
في حال تعرضك لمحاولة إحتيال أو تم النصب عليك يرجى تقييد شكوى لدى المصالح الأمنية أو تبليغ المصالح المختصة
182
10
62


وزارة البريد والمواصلات السلك...
10 mai 2025 ·
إطلاق حملة وطنية توعوية وتحسيسية حول النصب والاحتيال عبر الأنترنت... plus
+7
350
25
245

المصادر والمراجع

القرآن الكريم

أولا: المصادر الرسمية

01/- الدستور الجزائري، الجريدة الرسمية العدد **82**، بتاريخ:**30** ديسمبر **2020** .

02/- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، القاهرة، 21 ديسمبر **2010**، المصادق عليها بالمرسوم الرئاسي رقم:14-252 مؤرخ في:08 سبتمبر 2014،الجريدة الرسمية رقم العدد 57 المؤرخة في:28 سبتمبر 2014، ص 04 .

ثانيا: القوانين

01/- الأمر رقم:66-156 المؤرخ في:18 صفر عام 1386 الموافق لـ:08 يونيو 1966 المتضمن قانون العقوبات (الجريدة الرسمية عدد49 سنة 1966) المعدل والمتمم بالقانون رقم24-06 المؤرخ في28 أبريل سنة 2024 (الجريدة الرسمية العدد 30 لسنة 2024).

02/- القانون 09-04 المؤرخ في:14 شعبان 1430 الموافق لـ:05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر رقم:47/2009 .

03/- القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، 2018.

04/- القانون رقم:25-14 المؤرخ في:09 صفر عام 1447 الموافق لـ:03 غشت 2025 ج ر رقم:54-2025 المتضمن قانون الإجراءات الجزائية .

ثالثا: المراسيم التنظيمية

05/- المرسوم الرئاسي رقم 15-261 المؤرخ في 28 سبتمبر 2015، المتضمن إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 52، السنة 2015.

06/- مرسوم رئاسي رقم 23-313 المؤرخ في 03/09/2023 يعدل ويتمم المرسوم رقم 09_143 المؤرخ في 2009/04/27المتضمن مهام الدرك الوطني و تنظيمه. جريدة رسمية عدد 59 لسنة 2023 .

07/- المرسوم التنفيذي رقم 06-348 المؤرخ في 12 رمضان 1427هـ الموافق 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة

التحقيق (الجريدة الرسمية، العدد 63، 2006).

08/- المرسوم التنفيذي رقم 08-55 المؤرخ في 23 صفر 1429هـ الموافق 1 مارس 2008، المتضمن تنظيم المديرية العامة للأمن الوطني، ولاسيما المواد المتعلقة بتنظيم مخابر الشرطة العلمية والتقنية.

رابعا: الاتفاقيات الدولية غير مصادق عليها

- اتفاقية بودابست، المتعلقة بالجريمة الالكترونية، اعتمدها مجلس أوروبا في 23 نوفمبر 2001 في بودابست، ودخلت حيز التنفيذ في 1 يوليو 2004، مجموعة المعاهدات الأوروبية ETS رقم:185.

خامسا: المراجع

01/- إبراهيم حسني عبد السميع، الجرائم المستحدثة عن طريق الأنترنيت: دراسة مقارنة بين الشريعة والقانون، دار النهضة العربية للنشر، مصر،2011.

02/- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، جرائم ضد الأشخاص وجرائم ضد الأموال، ج01 ، ط 10، دار هومة للطباعة والنشر والتوزيع، الجزائر،2014.

03/- أحمد بسيوني أبو الروس، جرائم النصب، دار المطبوعات الجامعية، مصر، 1986.

04/- أحمد فتحي سرور، جرائم الاحتيال الإلكتروني: دراسة مقارنة بين القانون الجنائي وقانون المعاملات الإلكترونية، ط3، دار النهضة العربية للنشر، مصر، 2022.

05/- أسامة حمدان الرقب، جرائم النصب والاحتيال (الأساليب-المظاهر- العلاج)، ط 01، دار يافا العلمية للنشر والتوزيع، الأردن،2012.

06/- بن الشيخ لحسين، القانون الجزائي الخاص: جرائم ضد الاشخاص-جرائم ضد الأموال- أعمال تطبيقية، دار هومة للنشر، الجزائر،2005.

07/- بهنام رمسيس، قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العمومية، دار المعارف، مصر،1966.

08/- بهنام رمسيس، النظرية العامة للقانون الجنائي،ط2، منشأة المعارف للنشر،مصر،1971.

09/- جلال ثروت، جرائم الاعتداء على المال المنقول،ج2، دار المطبوعات الجامعية، مصر، 1995.

10/- جميل الصغير عبد الباقي، الأنترنيت والقانون الجنائي: الأحكام الموضوعية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية للنشر، مصر،2002.

11/- حورية معمر، الجرائم المعلوماتية في التشريع الجزائري والمواثيق الدولية، دار هومة، الجزائر، 2017.

12/- الخن محمد طارق، جريمة الاحتيال عبر الأنترنيت (الأحكام الموضوعية والأحكام الاجرائية)، ط1، منشورات الحلبي الحقوقية، 2011.

13/- السعيد كامل، شرح قانون العقوبات الاردني- الجرائم الواقعة على الاموال،ط2، مكتبة دار الثقافة للنشر والتوزيع، الأردن،1993.

14/- صحيح البخاري، كتاب الحج، باب حجة، رقم 1218.

15/- الطاهر بن عاشور، التحرير والتنوير، الدار التونسية للنشر، ط5، تونس، 1984.

16/- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي والنظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2009.

17/- طنطاوي إبراهيم حامد، المسؤولية الجنائية لجرائم النصب والاحتيال،ط2، شركة ناس للطباعة والنشر، مصر، 2003 .

18/- عادل عبد النور، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عب العزيز للعلوم التقنية، الرياض السعودية، سنة 2005.

19/- عبد الرزاق سند ابراهيم ليلة، سيكولوجية النصاب، دار النهضة العربية للطباعة النشر والتوزيع، لبنان، 1999.

20/- عبد العزيز سعد، جرائم الاعتداء على الأموال العامة والخاصة، ط4 ، دار هومة للنشر، الجزائر، 2007.

21/- عبد الفتاح مصطفى الصيفي، الأحكام العامة للنظام الجنائي في الشريعة الإسلامية والقانون، دار المطبوعات الجامعية للنشر، مصر، 2010.

22/- عبد القادر بوخالفة، النظام القانوني لمكافحة الجرائم الإلكترونية، دار العلوم للنشر، الجزائر، 2019.

23/- عبد الله بن سعود السراني، دور الإعلام الأمني في الوقاية من الجريمة، الإعلام الأمني بين الواقع والتطلعات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، السعودية، 2012.

24/- عبد الله محمد أبو تجار، المسؤولية عن مخاطر تقنيات الذكاء الاصطناعي، مؤسسة المعرفة لنشر وتوزيع الكتب، مصر، ط 01، سنة 2024.

25/- عبد النور عادل ، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم التقنية والنشر، السعودية، 2005.

26/- عرب يونس، موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والأنترنيت، ج1، اتحاد المصارف العربية للنشر، 2002.

27/- عمار بوحوش، النظام القانوني للأمن السيبراني، دراسة في ضوء التشريع الجزائري والمواثيق الدولية، دار الكتاب الحديث، الجزائر، 2020.

28/- رؤوف عبيد، الاعتداء على الاشخاص والأموال،ط8، دار الفكر العربي للنشر، مصر، سنة 1985.

29/- فايزة شريفي، السياسة الجنائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2018.

30/- فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها في التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المعقد في طرابلس، لبنان، يومي 24-2017/03/25.

31/- كاظم أحمد، الذكاء الاصطناعي، جامعة الامام جعفر الصادق، العراق، 2012.

32/- مأمون الكزبري، نظرية الالتزامات في ضوء قانون الالتزامات والعقود المغربية،ط2، مطبعة دار القلم للنشر، لبنان، 1972.

33/- مأمون سلامة، جرائم النصب المستحدثة الأنترنيت-بطاقات الائتمان – الدعاية التجارية الكاذبة، دار شتات للنشر والبرمجيات، مصر، 2007.

34/- محمد أمين الشوابكة، جرائم الحاسوب والأنترنيت (الجرائم المعلوماتية)، دار الثقافة للنشر والتوزيع، الأردن، 2006 .

35/- محمد بن مكرم بن منظور، لسان العرب، ج 12، دار المعارف، مصر،1998.

36/- محمد عبد الحميد مكي، العلاقة الاحتيال وتسليم المال في قانون العقوبات، منشورات جامعة طنطا، مصر، 1995.

37/- محمد علي الشرقاوي، الذكاء الاصطناعي والشبكات العصبية، المكتب المصري الحديث للنشر، مصر،1998.

38/- مليكة راجعي، الجريمة المعلوماتية وآليات مكافحتها على ضوء التشريع الجزائري والدولي، دار الأمة، الجزائر، 2019.

39/- ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، ط 01، دار النهضة العربية، مصر، 2020.

40/- منشاوي محمد عبد الله، جرائم الأنترنيت من منظور شرعي وقانوني، السعودية،2002.

41/- موسى عبد الله، بلال أحمد حبيب، الذكاء الاصطناعي ثورة في تقنيات العصر،ط1، المجموعة العربية للتدريب والنشر، مصر، 2019.

42/- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنيت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، 2013.

43/- نظير فرج مينا، الوجيز في الإجراءات الجزائية الجزائري،ط2، ديوان المطبوعات الجامعية،الجزائر،1992.

44/- ياسين سعد غالب، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات،ط1، دار المناهج للنشر والتوزيع، الأردن، 2012.

سادسا: المجلات العلمية

01/- إيهاب خليفة، أنترنيت الاشياء- تهديدات أمنية متزايدة للأجهزة المتصلة بالأنترنيت- مجلة اتجاهات الأحداث الصادرة عن مركز المستقبل للأبحاث والدراسات المتقدمة- العدد 19، الإمارات العربية المتحدة، 2017.

02/- بن عودة نبيل، نوار محمد: الصلاحيات الحديثة للضبطية القضائية للكشف وملاحقة مرتكبي الجرائم المتعلقة بالتمييز وخطاب الكراهية " التسرب الإلكتروني نموذجا" ، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، المجلد 01، العدد 02، جامعة إيليزي الجزائر، 2020.

03/- حمزة غندور، سليمة قواسمية، أنظمة الذكاء الاصطناعي في مكافحة الاحتيال الالكتروني، مجلة العلوم القانونية والاجتماعي، جامعة زيان عاشور بالجلفة الجزائر، المجلد 10، العدد الأول، 2025.

04/- خيدل أحمد، كيسي زهيرة، إجراءات جمع الأدلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 11، العدد 01 ، 2022.

05/- رؤى حمود، مقال بعنوان فيروس الفدية، المهاجم الأخطر للمؤسسات في العصر الرقمي، مجلة مجموعة ريناد،2018 .

06/- سليمان بن عبد العزيز العمر، "آليات منصات التواصل الاجتماعي في مكافحة الاحتيال الإلكتروني: دراسة تحليلية لسياسات الحماية والإبلاغ"، مجلة الأمن والقانون جامعة نايف العربية للعلوم الأمنية، المجلد 31، العدد 2، 2024.

07/- سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق جامعة تيزي وزو، المجلد 17، العدد 02، 2022.

08/- سوماتي شريفة،" القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص" مجلة الدراسات القانونية، المجلد 8، العدد 2، جامعة المدية الجزائر،2022 .

09/- سويسي فتيحة، انتحال الهوية الرقمية، المجلة الجزائرية لقانون والعدالة، العدد 1 ، مجلد 11، مركز البحوث القانونية والقضائية للنشر، الجزائر، 2025.

10/- صليحة بوشنافة، دور وسائل الإعلام في التوعية بمخاطر الجريمة الإلكترونية، مجلة الدراسات القانونية والسياسية، المجلد 08، العدد 01، كلية الحقوق والعلوم السياسية بجامعة الأغواط، 2022.

11/- عبد العزيز بن عبد الرحمان الشمري، جريمة النصب والاحتيال، مجلة العدل، عدد 39، وزارة العدل السعودية، 2000.

12/- علاء الدين منصور مغايرة، جرائم الذكاء الاصطناعي وسبل مواجهتها-جرائم التزييف العميق نموذجا -المجلة الدولية للقانون جامعة قطر، المجلد 13، العدد 02، 2024.

13/- علي عبيد ، ناصر موفق وآخرون، ماهية جريمة الاحتيال الإلكتروني، مجلة كلية القانون والعلوم السياسية، مجلد 05، عدد 19، كلية الحقوق، جامعة تكريت، العراق،2016 .

14/- فرقاق معمر، رابح وهيبة، القواعد الإجرائية الخاصة بالأقطاب الجزائية المتخصصة، جامعة عبد الحميد إبن باديس مستغانم، مجلة البحوث القانونية والسياسية، العدد 03، 2014.

15/- كريمة غديري، التزييف العميق: نشأة التقنية وتأثيراتها، مجلة الرسالة للدراسات الاعلامية، جامعة العربي التبسي الجزائر، مجلد 5، العدد4 ،2021 .

16/- مجلة إلكترونية للشرطة الجزائرية بموضوع: لأجل مجتمع واع في الفضاء السيبراني، العدد 158، سنة 2024، الموقع:www.algeriepolice.dz/IMG/pdf/chorta_site .

17/- محمد جمال، التفتيش في الجرائم الالكترونية ماهيته وشروطه الشكلية، المجلة الأردنية في القانون والعلوم السياسية، ع 03 جامعة الأردن، 2021.

18/- محمد مهدي عجمي، جريمة انتحال الشخصية في مواقع التواصل الاجتماعي، مجلة الشريعة والدراسات الاسلامية، مجلد37،العدد130، جامعة الكويت، 2022.

19/- رحال بومدين وسعداني نورة، الحماية الجنائية الواقعة على أموال التجارة الإلكترونية(جريمة السرقة والنصب) مجلة الواحات للبحوث والدراسات، مجلد 09، العدد 2 ،جامعة غرداية، 2016.

20/- نادية بوعزة، الإعلام والأمن السيبراني في الجزائر، مجلة علوم الإعلام والاتصال، المجلد 05، العدد 02، 2021.

21/- يحي إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد 34، العدد 82، 2019.

22/- هاشمي جبراني، جريمة الاحتيال في مواقع التواصل الاجتماعين مجلة الحقوق والعلوم الانسانية، جامعة مولاي الطاهر سعيدة، الجزائر، المجلد 18، العدد 03، 2025.

سابعا: الأطروحات الجامعية

01/- قراوي كلثوم، جريمة الاحتيال الإلكتروني، أطروحة لنيل شهادة الدكتوراه علوم القانون العام، جامعة الجزائر 01، 2025/2024 .

02/- شنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة دكتوراه، جامعة أدرار، الجزائر، 2021 .

ثامنا: المداخلات

01/- أحسن بوسقيعة، " من العدالة التقليدية إلى العدالة الرقمية: دور القضاء الجزائري في مواجهة الجريمة الإلكترونية في ظل التحول الرقمي والذكاء الاصطناعي"، مداخلة في الملتقى الوطني:بتاريخ:18 أفريل 2026 قصر الثقافة أدرار .

02/- غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مداخلة خلال مؤتمر القانون والكمبيوتر والأنترنيت، كلية الشريعة والقانون، جامعة الإمارات، سنة 2000.

تاسعا: الندوات العلمية

01/- أحمد شوقي أبو خطوة، ندوة علمية حول العلاقة بين الجرائم الاحتيالية والإجرام المنظم، دار جامعة نايف العربية للعلوم الأمنية للنشر، 2007 .

عاشرا: المواقع الإلكترونية

Rapport OCDE,Le Vole d'identitè en ligne.http//:www.oecd/dataoecd/3/8/40699509 - /01

02/- موقع شركة تصميم وتطوير تقنيات حديثة للأمن السيبرانيWWW.CEREBRA.SA

Artificial intelligence,eng,oxford living dictionaries, https://perma.cc/WF9V-YM7C,consult3

04/- فهد آل قاسم، الذكاء الاصطناعي، كتاب إلكتروني، منشور عبر الرابط: https://www.moswrat.com/books_download_10231.html.

J.Damiani, Avoice deepfake was used to scam a ceo out of 234$ 2019.http://forbs.com-/05

06/- هاو كارين، هيفين دوجلاس، لماذا حققت تقنية التزييف https://technologyreview.ae العميق انتشارا واسعا في 2020.

Sophia Hanson,robotic,available at :www.hansonrobotics.com -/07

08/- الموقع الرسمي لمديرية العامة للأمن الوطني،. https://www.dgsn.dz

09/- الصفحة الرسمية عبر تطبيق facebook للصفحة الرسمية للشرطة الجزائرية، رابطها: https://www.facebook.com/algeriepolice.dz .

10/- الموقع الرسمي لجهاز الدرك الوطني ، https://www.mdn.dz/site_cgn .

11/- الموقع الرسمي لوزارة العدل الجزائرية www.mjustice.gov.dz

المراجع باللغة الأجنبية

01/-flourdi Luciano (artificial intelligence,deepfakes and the future of ectypes,philos.technol31,2018(

02/-Frèderic Dechamps,Cariline Lambilot,Cybercriminalité état des lieux, Anthèmis,2016.

03/-Myriam Quémeber,Yves Charpenel,Cybercriminalité droit pénal appliqué,Edition Economica,France,2010.

فهرس الموضوعات

فهرس الموضوعات

ملخص الدراسة

جريمة النصب من الجرائم التقليدية، غير أنها استحدثت صوراً جديدة بارتكابها عبر الوسائط الرقمية وتوظيف تقنيات الذكاء الاصطناعي، مما أكسبها طابعاً عابراً للحدود وصعوبة في الكشف والإثبات، الأمر الذي استوجب تدخل المشرع لمواكبة هذه التحولات الإجرامية. كما تم التطرق من خلال هذا البحث إلى التعريف بجريمة النصب الإلكتروني، وبيان خطورتها المتزايدة على الأفراد والاقتصاد الوطني، واستعراض النصوص القانونية التي وضعها المشرع الجزائري لمواجهتها، مع إبراز التحديات التي تطرحها تقنية الذكاء الاصطناعي في هذا المجال.

تم تبيان في بحثنا أن جريمة النصب الإلكتروني تقوم على أركانها التقليدية (الركن الشرعي والمادي والمعنوي) مع خصوصية تتعلق باستعمال وسائل احتيالية رقمية كالتزييف العميق و التصيد الاحتيالي، وأن المسؤولية الجزائية عن هذه الجرائم قد تتجاوز الجاني المحتال و تتوزع بين المبرمج والمالك للنظام الآلي، كما عرجنا في بحثنا أن المشرع الجزائري أرسى آلية مؤسساتية متكاملة شملت الهيئة الوطنية للوقاية من الجرائم السيبرانية، والأقطاب القضائية المتخصصة، ووحدات الشرطة التقنية، غير أن النصوص القانونية بحاجة إلى تحديث دوري لمواكبة التطورات السريعة خاصة تقنيات الذكاء الاصطناعي، مع ضرورة تفعيل آليات التعاون الدولي والإعلام الوقائي للحد من هذه الظاهرة.

الملخص باللغة الأجنبية:

The crime of fraud is among traditional offenses; however, it has taken on new forms through its commission via digital media and the use of artificial intelligence technologies, endowing it with a cross-border nature and posing difficulties in detection and proof. This has necessitated legislative intervention to keep pace with these criminal transformations. This research also addressed the definition of cyber fraud, highlighted its growing danger to individuals and the national economy, and reviewed the legal texts established by the Algerian legislator to confront it, while underscoring the challenges posed by artificial intelligence technology in this domain.

Our research demonstrated that cyber fraud is based on its traditional elements (the legal, material, and moral elements), with a particularity related to the use of digital fraudulent means such as deepfakes and phishing. Moreover, criminal liability for these crimes may extend beyond the defrauding perpetrator and be distributed among the programmer and the owner of the automated system. We also discussed that the Algerian legislator has established an integrated institutional mechanism encompassing the National Authority for the Prevention of Cybercrimes, specialized judicial hubs, and technical police units. However, the legal texts require periodic updating to keep pace with rapid developments, particularly artificial intelligence technologies, along with the necessity of activating international cooperation mechanisms and preventive awareness to curb this phenomenon.