جامعة محمد خيضر بسكرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

مذكرة ماستر

ميدان: الحقوق والعلوم السياسية
فرع: الحقوق
تخصص: القانون الجنائي والعلوم الجنائية
رقم: .....

من إعداد الطالبتين :

*** هنانو دينة** *** بن خرارة يسرى** .

يوم: .....

جريمة النصب والاحتيال الالكتروني في التشريع الجزائري

لجنة المناقشة:

العضو 1	الرتبة	الجامعة	رئيسا
أقوجيل نبيلة	أ د	جامعة محمد خيضر- بسكرة -	مشرفا
العضو 3	الرتبة	الجامعة	مناقشا

السنة الجامعية : 2025 - 2026


بسم الله الرحمن الرحيم



شكر وعرفان

الحمد لله رب العالمين، الذي بنعمته تتم الصالحات، وبتوفيقه تُنجز الأعمال وتُثمر الجهود. له الحمد والشكر على ما أنعم به علينا من عون وتيسير لإتمام هذا العمل.

ثم نتقدم بجزيل الشكر والامتنان إلى أستاذتنا المشرفة" أقوجيل نبيلة" على هذا العمل، لما قدّمته لنا من توجيهات قيمة ونصائح سديدة ومتابعة مستمرة كان لها الأثر الكبير في إنجاز هذه المذكرة.

كما لا يفوتنا أن نتقدم بالشكر لكل من مدّ لنا يد العون، ووقف إلى جانبنا من قريب أو بعيد، خلال مسيرتنا الدراسية.

فلكم جميعًا خالص التقدير والامتنان.



إهداء

إلى من كان دعاؤهم نور طريقنا، وسندهم

سبب نجاحنا... "والدينا كرام"

إلى من آمنوا بنا ورافقونا في كل خطوة من

هذا

الطريق " إخوتنا"

نُهدي هذا العمل المتواضع، عرفانًا بالجميل

وامتنانًا لا يُنسى.

مقدمة

مقدمة

شهد العالم في العقود الأخيرة تطور هائل في مجال تكنولوجيا الإعلام والاتصال، حيث أصبحت الوسائل الإلكترونية والرقمية جزء أساسي من الحياة اليومية، سواء في المعاملات التجارية أو الخدمات البنكية أو التواصل الاجتماعي , وقد ساهم هذا التطور في تسهيل حياة الأفراد وتسريع إنجاز مختلف العمليات، غير أنه في المقابل أفرز أنماط جديدة من الجرائم المستحدثة التي تستغل الفضاء الإلكتروني لتحقيق أغراض غير مشروعة، ومن أبرزها جريمة النصب والاحتيال الإلكتروني.

و هذه الجريمة من أخطر صور الإجرام الحديث لكونها تعتمد على وسائل تقنية متطورة وأساليب خادعة تستهدف الاستيلاء على أموال الغير , أو بياناتهم الشخصية بطرق احتيالية يصعب اكتشافها في كثير من الأحيان , و تتميز بسرعة التنفيذ واتساع نطاقها الجغرافي، وإمكانية ارتكابها عبر الحدود و يجعل مكافحتها أكثر تعقيد مقارنة بالجرائم التقليدية , وأمام تزايد هذا النوع من الجرائم و تدخل المشرع الجزائري بوضع مجموعة من النصوص القانونية الرامية إلى تجريم الأفعال المرتبطة بالنصب والاحتيال الإلكتروني، سواء من خلال قانون العقوبات أو القوانين الخاصة المتعلقة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك بهدف حماية الأفراد والمعاملات الإلكترونية وتعزيز الثقة في البيئة الرقمية.

ومن ثم فإن دراسة جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري تكتسي أهمية بالغة، بالنظر إلى انتشارها المتزايد وما تطرحه من تحديات قانونية وعملية، الأمر الذي يستوجب الوقوف على مفهومها، أركانها و صورها وكذا الآليات القانونية المقررة لمواجهتها والحد من آثارها.

أهمية الموضوع

تتمثل أهمية دراسة موضوع جريمة النصب والاحتيال الإلكتروني في كونه من الموضوعات الحديثة المرتبطة بالتطور التكنولوجي المتسارع الذي يشهده العالم، حيث أصبحت المعاملات الإلكترونية والتجارة عبر الإنترنت والخدمات الرقمية جزء لا يتجزأ من الحياة اليومية , وقد أدى هذا التحول الرقمي إلى ظهور أساليب إجرامية جديدة تستغل الوسائل الإلكترونية للإيقاع بالضحايا والاستيلاء على أموالهم أو بياناتهم الشخصية، مما يجعل هذا الموضوع جدير بالدراسة والتحليل لفهم أبعاده القانونية والعملية.

و تبرز أهميته في ازدياد عدد الضحايا واتساع نطاق هذه الجرائم، الأمر الذي يهدد الأمن الاقتصادي والاجتماعي ويزعزع الثقة في التعاملات الإلكترونية , وتظهر أهمية الموضوع أيضا من الناحية القانونية، إذ يساهم بحث جريمة النصب والاحتيال الإلكتروني في بيان مدى كفاية التشريع الجزائري لمواجهة هذا النوع من الجرائم، ومدى فعالية النصوص القانونية والإجراءات المعتمدة للردع والحماية , و يساعد في إبراز الصعوبات التي تواجه أجهزة العدالة والجهات المختصة في اكتشاف هذه الجرائم وإثباتها، خاصة أنها ترتكب بوسائل تقنية متطورة وعابرة للحدود.

أهمية عملية : إبراز الثغرات القانونية والتقنية التي تتيح للمجرمين مجال أوسع وأسهل لاستغلالها مستفيدين من الطابع اللامادي والافتراضي لهذه الجرائم إضافة إلى إمكانية توعية سلوك المستخدمين للفضاء الرقمي وتوعيتهم حتى لا يكونوا ضحايا الاحتيال والنصب وضمان حقوقهم في الأمن المعلوماتي .

أسباب اختيار الموضوع

يعود اختيار موضوع جريمة النصب والاحتيال الإلكتروني إلى مجموعة من الأسباب الشخصية والموضوعية التي جعلته محل اهتمام ودراسة.

فمن الناحية الشخصية ينبع هذا الاختيار من الرغبة في التعمق في موضوعات القانون الجزائي الحديثة، خاصة تلك المرتبطة بالتطور التكنولوجي والجرائم المستحدثة، إضافة إلى الفضول العلمي لفهم كيفية ارتكاب هذا النوع من الجرائم وأساليب مكافحتها في الواقع العملي.

أما من الناحية الموضوعية فتتمثل في الأهمية المتزايدة لجريمة النصب والاحتيال الإلكتروني في المجتمع الجزائري والعالمي، نتيجة انتشار المعاملات الإلكترونية وتزايد حالات الاحتيال عبر الإنترنت، و يستدعي دراسة الإطار القانوني لها ومدى فعالية التشريع الجزائري في مواجهتها والحد من آثارها.

أهداف الدراسة

تهدف هذه الدراسة إلى تسليط الضوء على جريمة النصب والاحتيال الإلكتروني من حيث مفهومها وأركانها وصورها المختلفة، وذلك من أجل فهم طبيعتها القانونية في ظل التطور التكنولوجي المتسارع , و تسعى إلى إبراز كيفية تعامل المشرع الجزائري مع هذا النوع من الجرائم من خلال النصوص القانونية المقررة لمكافحتها، وبيان مدى فعاليتها في توفير الحماية اللازمة للأفراد والمعاملات الإلكترونية , بالإضافة إلى ذلك تهدف الدراسة إلى تحليل الإشكالات العملية التي تطرحها هذه الجريمة في الإثبات والمتابعة القضائية، مع محاولة تقديم رؤية تساعد على تعزيز آليات الوقاية والردع في المجال الرقمي.

نجد أن هذا الموضوع حظي باهتمام جزئي من قبل الباحثين حيث تداولوه كجزئية أو كعنصر في موضوعاتهم العامة المتعلقة بالجرائم المعلوماتية.

الدراسات السابقة

في إطار الدراسات السابقة المتعلقة بموضوع جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري، نجد أن هذا الموضوع حظي باهتمام عدد من الباحثين من خلال مذكرات

الماجستير وأطروحات الدكتوراه والمقالات العلمية المحكمة، حيث تنوعت معالجاته بين الجانب الموضوعي والإجرائي.

الدراسة الأولى:

مذكرة ماجستير للباحث محمد أمين بن عيسى، بعنوان "جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري"، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1 بن يوسف بن خدة، (2018-2019)، تناول فيها الباحث مفهوم هذه الجريمة وأركانها وأهم صورها المرتكبة عبر الإنترنت كالاحتيال البنكي وانتحال الشخصية، ثم تطرق إلى العقوبات المقررة لها في قانون العقوبات والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وقد ركزت المذكرة على الجانب الموضوعي للجريمة، في حين تسعى دراستنا إلى التوسع في تحليل الآليات الإجرائية والوقائية لمكافحتها.

الدراسة الثانية :

مقال للدكتورة خديجة بلقاسم، بعنوان "جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري وآليات مكافحتها"، منشور بمجلة الحقوق والعلوم الإنسانية، جامعة وهران، العدد (2021-2022)، حيث ركزت الباحثة على الجوانب الإجرائية لمكافحة هذه الجريمة، كالتفتيش الإلكتروني واعتراض المراسلات الرقمية ودور الهيئات المختصة كالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وقد اقتصر المقال على الجانب الإجرائي، بينما تجمع دراستنا بين الجانبين الموضوعي والإجرائي مع تحليل أهم الإشكالات العملية التي تطرحها هذه الجريمة.

صعوبات الدراسة :

واجهتنا عدة صعوبات لدراسة موضوع جريمة النصب والاحتيال الإلكتروني تجسدت في حداثة الموضوع وتشعبه، إذ يعد من الجرائم المستحدثة المرتبطة بالتطور التكنولوجي

والرقمي السريع، ما أدى إلى قلة المراجع المتخصصة المتناولة لهذا النوع من الجرائم بشكل دقيق ومفصل.

من جهة أخرى تعد الطبيعة التقنية المعقدة لهذه الجرائم واعتمادها على وسائل رقمية متطورة، يجعل فهم آليات ارتكابها وإثباتها أمر غير سهل، خاصة في ظل التغير المستمر لأساليب الاحتيال الإلكتروني.

و تتمثل الصعوبة أيضا في الجانب التطبيقي، حيث واجهنا كباحثات إشكاليات تتعلق بمدى فعالية النصوص القانونية الجزائرية في مواجهة هذا النوع من الجرائم، والتي تسنبط من الأحكام والاجتهادات القضائية المتخصصة في هذا المجال حيث اتسمت بالمحدودية والسرية.

فضلا عن ذلك فإن الطبيعة العابرة للحدود لجريمة النصب والإحتيال الإلكتروني تزيد من تعقيد الدراسة، كونها تتطلب تنسيق دولي وتعاون بين عدة جهات لمكافحتها وهو ما يطرح تحديات إضافية على المستوى القانوني والعملي.

الإشكالية :

في ظل التطور التكنولوجي المتسارع وانتشار المعاملات الإلكترونية، برزت جريمة النصب والاحتيال الإلكتروني كإحدى أخطر الجرائم المستحدثة التي تهدد أموال الأفراد وأمنهم الرقمي.

ومن هنا نطرح الإشكالية التالية: إلى أي مدى استطاع المشرعالجزائري تحقيق التوازن بين فعالية التجريم والحماية القانونية في مواجهة جرائم النصب و الاحتيال الإلكتروني في ظل التطور المستمر التكنولوجيا الرقمية؟.

الأسئلة الفرعية:

1-ما المقصود بجريمة النصب والاحتيال الإلكتروني وما هي صورها المختلفة؟

2-ما هي الأركان القانونية المكونة لجريمة النصب والاحتيال الإلكتروني؟

3-ما مدى كفاية النصوص القانونية في التشريع الجزائري لمواجهة هذه الجريمة؟

4-ما هي أهم الآليات القانونية والعملية المعتمدة لمكافحة جريمة النصب والاحتيال الإلكتروني؟

المنهج المتبع :

اعتمدنا في هذه الدراسة على المنهج الوصفي والمنهج التحليلي باعتبارهما الأنسب لموضوع جريمة النصب والاحتيال الإلكتروني، حيث تم الاعتماد على المنهج الوصفي من خلال عرض مفهوم جريمة النصب والاحتيال الإلكتروني، وبيان صورها وأركانها وكذا الإطار القانوني الذي ينظمها في التشريع الجزائري، وذلك بهدف الإحاطة بالجانب النظري للموضوع وتوضيح مختلف مفاهيمه الأساسية.

ومن جهة أخرى تم استخدام المنهج التحليلي من خلال تحليل النصوص القانونية ذات الصلة بجريمة النصب والاحتيال الإلكتروني، ودراسة مدى فعاليتها في مكافحة هذا النوع من الجرائم، مع تفسير الأركان القانونية للجريمة وربطها بالواقع العملي، وذلك من أجل الوقوف على مدى كفاءة المنظومة القانونية في التصدي لها.

خطة الدراسة

من خلال ما سبق وللإجابة على الإشكالية المطروحة تم وضع خطة لدراسة موضوع جريمة النصب والاحتيال الالكتروني تجلت في تقسيم الدراسة إلى فصلين حيث تناولنا في الأول الاطار القانوني لجريمة النصب و الاحتيال الإلكتروني وذلك من خلال مبحثين، خصصنا في المبحث الأول: مفهوم جريمة النصب والاحتيال الالكتروني،

وفي المبحث الثاني: أركان جريمة النصب و الاحتيال الإلكتروني.

وجاء الفصل الثاني بعنوان: آليات الردع و الوقاية من جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري وقسمناه إلى مبحثين:

المبحث الأول: الأحكام الإجرائية لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

المبحث الثاني: وسائل الوقاية من جريمة النصب والاحتيال الإلكتروني .

الفصل الأول:

الاطار القانوني لجريمة النصب و الاحتيال الإلكتروني

المبحث الأول: مفهوم جريمة النصب والاحتيال الالكتروني

المبحث الثاني: أركان جريمة النصب و الاحتيال الإلكتروني.

إن موضوع جريمة النصب والاحتيال الإلكتروني من الموضوعات الحديثة التي فرضت نفسها بقوة في مجال القانون الجنائي، وذلك نتيجة التطور السريع في تكنولوجيا الإعلام والاتصال وما رافقه من انتشار واسع لاستخدام الوسائل الإلكترونية في مختلف المعاملات اليومية , وقد أدى هذا التطور إلى بروز أنماط جديدة من الجرائم التي تعتمد على أساليب احتيالية متطورة تستهدف الإيقاع بالضحايا والاستيلاء على أموالهم أو بياناتهم بطرق يصعب اكتشافها و جعل هذه الجريمة تشكل تحدي حقيقي أمام الأنظمة القانونية المعاصرة .

وانطلاقا من أهمية هذا الموضوع جاء هذا الفصل الأول للإحاطة بالإطار العام لجريمة النصب والاحتيال الإلكتروني، من خلال التطرق إلى مفهومها في المبحث الأول، وذلك بتحديد تعريفها وبيان مختلف خصائصها وأنواعها في ظل التطور التكنولوجي , و يهدف هذا المبحث إلى توضيح الطبيعة القانونية لهذه الجريمة وتمييزها عن غيرها من الجرائم المشابهة، بما يسمح بفهم أدق لخصائصها , أما المبحث الثاني فيتناول أركان جريمة النصب والاحتيال الإلكتروني، باعتبارها الأساس الذي تقوم عليه المسؤولية الجزائية، وذلك من خلال دراسة الركن الشرعي والركن المادي والركن المعنوي.

ويهدف هذا الطرح إلى إبراز العناصر القانونية التي لا تقوم الجريمة إلا بتوافرها، مع بيان خصوصية هذه الأركان في الجرائم الإلكترونية مقارنة بالجرائم التقليدية، ومنه إبراز مختلف صور الاحتيال الإلكتروني التي يتعرض لها الأفراد، وفهم كيفية تطورها بتطور التكنولوجيا و يساعد على إدراك خطورتها واتساع نطاقها في المجتمع المعاصر.

المبحث الأول: مفهوم جريمة النصب و الاحتيال الإلكتروني

من المفاهيم القانونية الحديثة التي ارتبطت ارتباط وثيق بتطور الوسائل التكنولوجية وانتشار استخدام الإنترنت في مختلف مجالات الحياة , وقد أصبح

تحديد هذا المفهوم ضرورة أساسية لفهم طبيعة هذه الجريمة وتمييزها عن غيرها من الجرائم التقليدية، خاصة وأنها تتميز بخصوصية ناتجة عن الوسيلة المستعملة في ارتكابها وهي الوسائل الإلكترونية.

ومن هذا المنطلق يهدف هذا المبحث إلى دراسة مفهوم جريمة النصب والاحتيال الإلكتروني من خلال التطرق إلى تعريفها وخصائصها في المطلب الأول، بما يسمح بتحديد الإطار النظري لها وإبراز أهم السمات التي تميزها عن غيرها من الجرائم , و يتناول هذا المبحث في المطلب الثاني أنواع جريمة النصب والاحتيال الإلكتروني، وذلك بالنظر إلى تنوع الأساليب والوسائل التي ترتكب بها هذه الجريمة في الفضاء الرقمي، سواء من خلال البريد الإلكتروني أو مواقع التواصل الاجتماعي أو المنصات المالية الإلكترونية وغيرها.

المطلب الأول: تعريف جريمة النصب و الاحتيال الإلكتروني و خصائصه

إن تحديد مفهوم جريمة النصب والاحتيال الإلكتروني خطوة أساسية لفهم طبيعتها القانونية وتمييزها عن غيرها من الجرائم التقليدية، خاصة في ظل التطور التكنولوجي الذي أفرز أنماط جديدة من السلوك الإجرامي.

فهذه الجريمة لم تعد تقتصر على الوسائل التقليدية بل أصبحت ترتكب عبر الوسائط الإلكترونية والرقمية، مما جعل تحديدها وتعريفها يخضع لاعتبارات قانونية وتقنية دقيقة.

ومن هذا المنطلق يهدف هذا المطلب إلى بيان التعريف القانوني لجريمة النصب والاحتيال الإلكتروني في الفرع الأول، مع إبراز أهم خصائصها في الفرع الثاني , و دراسة خصائص هذه الجريمة ضرورية لفهم أبعادها المختلفة، إذ تتميز بسمات خاصة ترتبط بوسائل ارتكابها وسرعة تنفيذها وصعوبة اكتشافها إضافة إلى طابعها العابر للحدود , وهو ما يجعلها جريمة مركبة ومعقدة مقارنة بالنصب التقليدي، ويستدعي تحليل دقيق لمميزاتها القانونية والتقنية و يساعد على الإحاطة الكاملة بمضمونها وآثارها في الواقع العملي

الفرع الأول: التعريف القانوني لجريمة النصب والاحتيال الإلكتروني

إن جريمة النصب والاحتيال الإلكتروني امتداد حديث لجريمة النصب التقليدية، غير أنها تتميز بكونها ترتكب عبر الوسائط الرقمية والأنظمة المعلوماتية، و أضفى عليها طابع أكثر تعقيد وخطورة , و اهتم الفقه القانوني بتحديد مفهومها باعتبارها كل سلوك تدليسي يستخدم فيه الجاني وسائل إلكترونية أو معلوماتية بهدف خداع الضحية والاستيلاء على أمواله أو بياناته دون وجه حق، وذلك باستعمال وسائل الكذب أو التضليل أو انتحال الصفات , ويؤكد الفقه أن جوهر هذه الجريمة يتمثل في عنصر الخداع الذي يؤدي إلى تسليم المال طوع من طرف الضحية نتيجة تأثير الوسائل الاحتيالية عليها[1].

ويرى جانب آخر من الفقه أن جريمة النصب والاحتيال تقوم على فكرة الاعتداء على الثقة في المعاملات المالية والاقتصادية، إذ يعتمد الجاني على خلق صورة وهمية أو تقديم معلومات كاذبة لإقناع المجني عليه بوجود مشروع أو فرصة استثمارية أو واقعة غير حقيقية , وتكمن خطورة هذه الجريمة في كونها لا تعتمد على القوة أو العنف وإنما على التأثير

[1] – أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص، الجزء الأول**، دار هومة، الجزائر، 2023، ص 324.

النفسي والإقناع الزائف، و يجعل الضحية تتصرف بإرادتها الظاهرة ولكن تحت تأثير الخداع وهذا ما يجعلها من الجرائم التي يصعب كشفها في كثير من الأحيان[1].

أما من الناحية التشريعية فقد عالج المشرع الجزائري جريمة النصب ضمن المادة 372 من قانون العقوبات، حيث اعتبرها كل فعل يقوم على الاستيلاء على أموال الغير باستعمال طرق احتيالية كاتخاذ اسم كاذب أو صفة غير صحيحة أو إيهام بوجود مشروع وهمي. ورغم أن النص لم يذكر صراحة الطابع الإلكتروني للجريمة، إلا أنه يمكن تطبيقه على الأفعال التي تتم عبر الإنترنت متى توفرت الوسائل التدليسية ذاتها , ويفهم من ذلك أن المشرع اعتمد معيار الوسيلة الاحتيالية وليس وسيلة التنفيذ[2].

وفي المقابل نجد أن التشريع الفرنسي قد عرف جريمة الاحتيال في المادة 313-1 من قانون العقوبات، حيث ربطها بفعل الخداع الذي يدفع الضحية إلى تسليم أموال أو التزام أو خدمة نتيجة استعمال وسائل احتيالية مثل الاسم الكاذب أو الصفة المزورة أو إخفاء الحقيقة , ويتميز هذا التعريف بأنه أكثر شمولا إذ يركز على النتيجة المتمثلة في الإضرار بالمجني عليه، سواء تعلق الأمر بالمال أو الخدمات وهذا يعكس تطور النظرة القانونية للجريمة باعتبارها اعتداء على الثقة العامة.[3]

ومن خلال المقارنة بين مختلف التعاريف الفقهية والتشريعية يمكن استخلاص أن جريمة النصب والاحتيال الإلكتروني تقوم على ثلاثة عناصر أساسية، وهي وجود وسيلة احتيالية وتأثيرها على إرادة الضحية، ثم تحقق ضرر مادي أو معنوي نتيجة هذا الخداع , أن استخدام الوسائط الإلكترونية يجعل الجريمة أكثر تطور وسرعة في التنفيذ وأصعب في

---

[1] – أسامة حمدان الرقب، **جرائم النصب والاحتيال: الأساليب والمظاهر والعلاج**، دار يافا، عمان,2012 , ص 81

[2] –_**المادة 372 من قانون العقوبات الجزائري، الأمر 66-156** المعدل والمتمم.

[3] – **article 313-1. Code pénal français** – dernière modification le 01 janvier 2021 – Document généré le 12 février 2021.

الإثبات , و يستوجب تطوير النصوص القانونية وآليات المكافحة لمواكبة هذا النوع من الإجرام المستحدث[1].

تتجلى خصوصية جريمة النصب والاحتيال الإلكتروني في كونها لا تعتمد على الحضور المادي للجاني، بل تتم عبر فضاءات افتراضية تسمح له بإخفاء هويته الحقيقية واستعمال هويات مزيفة أو حسابات وهمية , وهذا ما يزيد من صعوبة تتبع مرتكبي هذه الجريمة، و خاصة مع إمكانية استخدام تقنيات التشفير وإخفاء البيانات , و هذه الطبيعة الرقمية تجعل الجريمة قابلة للانتشار السريع على نطاق واسع دون قيود جغرافية و يضاعف من حجم خطورتها.[2]

كما أن جريمة الاحتيال الإلكتروني ترتبط بشكل وثيق بالتطور التكنولوجي و يستغل الجاني منصات التواصل الاجتماعي، والمواقع الإلكترونية والتطبيقات البنكية في تنفيذ أفعاله الإجرامية , وغالبا ما يعتمد على أساليب متطورة مثل الروابط المزيفة أو الرسائل الاحتيالية، أو المواقع المقلدة للبنوك بهدف استدراج الضحية وإقناعها بإدخال بياناتها الشخصية أو البنكية وهذا يعكس الطابع التقني المعقد لهذه الجريمة.[3]

ومن الناحية القانونية فإن العنصر الأساسي في جريمة النصب والاحتيال يتمثل في وجود وسائل احتيالية تؤدي إلى تضليل المجني عليه، حيث لا يكفي مجرد الكذب البسيط بل يجب أن يكون مصحوب بوسائل خارجية أو مظاهر تدليسية توحي بالصدق , وقد أكد

[1] – محمد طارق رمضان، **جريمة الاحتيال عبر الإنترنت**، منشورات الحلبي الحقوقية، مصر،2011، ص 09.

[2] – إبراهيم حسني عبد السميع، **الجرائم المستحدثة عن طريق الإنترنت**، دار النهضة العربية، القاهرة، 2011، ص 62.

[3] – محمد عبد الله أبو بكر سلامة، **جرائم الكمبيوتر والإنترنت**، منشأة المعارف، الإسكندرية، 2006، ص 45.

الفقه أن هذه الوسائل يجب أن تكون السبب المباشر في دفع الضحية إلى تسليم المال وإلا انتفى قيام الجريمة.[1]

و المشرع الجزائري رغم عدم تخصيصه نص مستقل للنصب الإلكتروني، إلا أن النصوص العامة لقانون العقوبات قابلة للتطبيق على هذا النوع من الجرائم، خاصة المادة 372 إلى جانب النصوص الواردة في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال , وهذا يدل على مرونة التشريع الجزائري في استيعاب الجرائم المستحدثة ضمن القواعد العامة.[2]

وفي السياق المقارن نجد أن التشريع المصري يشترط لقيام جريمة النصب استعمال إحدى الطرق الاحتيالية مثل انتحال اسم أو صفة كاذبة أو إنشاء مشروع وهمي، وهو ما ينسجم إلى حد كبير مع ما جاء في التشريع الجزائري , غير أن التطور التكنولوجي أضاف بعد جديد لهذه الجريمة، حيث أصبح الخداع يتم عبر وسائط رقمية وليس فقط عبر التواصل المباشر[3].

أما الفقه القانوني الحديث فيميز بين النصب التقليدي والنصب الإلكتروني من حيث الوسيلة، حيث يرى أن النصب الإلكتروني يعتمد على أدوات تقنية حديثة تسمح بتوسيع دائرة الضحايا في وقت قصير، و يسمح للجاني بالتحكم عن بعد دون الحاجة إلى لقاء مباشر مع الضحية وهذا ما يجعل الجريمة أكثر تعقيد من الناحية القانونية والعملية.[4]

---

[1] – أحسن بوسقيعة، **المرجع السابق** ، ص 324.

[2] – **المادة 372 من الأمر 24-06** المعدل والمتمم **لقانون العقوبات الجزائري**،الجريدة الرسمية عدد 30 الصادرة في 30-04-2024.

[3] – طنطاوي إبراهيم أحمد، **المسؤولية الجنائية لجرائم النصب والاحتيال**، القاهرة، 1998، ص 87.

[4] – علي عبد القادر القهوجي، **الحماية الجنائية للبيانات المعالجة إلكترونيًا**، منشورات مؤتمر الإمارات، 2004، ص 120.

و هذه الجريمة تتسم بسرعة التنفيذ وسهولة ارتكابها إذ يمكن للجاني في ثوان معدودة إرسال رسائل احتيالية إلى آلاف الأشخاص , أو إنشاء موقع إلكتروني مزيف يستهدف عدد كبير من الضحايا وهذا ما يجعلها جريمة ذات طابع جماعي محتمل وليس فردي فقط.[1]

وتكمن خطورة الاحتيال الإلكتروني أيضا في صعوبة الإثبات حيث تعتمد هذه الجرائم على أدلة رقمية قد يتم حذفها أو تعديلها بسهولة، مما يتطلب خبرة تقنية متخصصة في جمع الأدلة وتحليلها , وعدم وعي بعض الضحايا بأساليب الاحتيال يزيد من نسبة نجاح هذه الجرائم.[2]

وبناء على ما سبق يتضح أن جريمة النصب والاحتيال الإلكتروني تمثل تطور خطير لجريمة تقليدية في قالب تكنولوجي حديث، حيث تجمع بين الخداع والتقنيات الرقمية لتحقيق أهداف إجرامية تمس الأموال والثقة في المعاملات الإلكترونية , وتنوع صورها وتعقيد أساليبها يجعلها من الجرائم التي تتطلب تحديث مستمر في التشريعات الوطنية وتعزيز آليات المكافحة على المستويين القانوني والتقني[3].

الفرع الثاني: خصائص جريمة النصب والاحتيال الإلكتروني

تتميز جريمة النصب والاحتيال الإلكتروني بجملة من الخصائص التي تجعلها مختلفة عن جريمة النصب التقليدية، حيث إنها ترتكب في بيئة رقمية افتراضية تعتمد على تكنولوجيا المعلومات وشبكات الاتصال الحديثة , و هذه البيئة غير المادية سمحت للجناة بتطوير أساليب جديدة في تنفيذ أفعالهم الإجرامية بعيد عن الرقابة المباشرة، و جعل الجريمة أكثر

[1] – الصغير جميل عبد الباقي، **الإنترنت والقانون الجنائي**، دار النهضة العربية، القاهرة، 2001، ص 57

[2] – عرب يونس، **موسوعة جرائم الكمبيوتر والإنترنت**، اتحاد المصارف العربية، 2002، ص 33.

[3] – محمد طارق رمضان، مرجع سابق، ص 49.

تعقيد وانتشار , ويؤكد الفقه أن الطبيعة الرقمية لهذه الجريمة تجعلها مرتبطة بشكل مباشر بالتطور التكنولوجي إذ كلما تطورت وسائل الاتصال كلما تطورت أساليب الاحتيال[1].

ومن أهم خصائص هذه الجريمة وقوعها في بيئة إلكترونية افتراضية تعتمد على الحواسيب والإنترنت كوسيلة أساسية في التنفيذ، ويتم تبادل البيانات والمعلومات عبر إشارات رقمية غير مرئية يصعب تتبعها بسهولة , والجاني يستغل الثغرات الأمنية في الأنظمة المعلوماتية للوصول إلى بيانات الضحايا، مما يجعل الجريمة قائمة على عنصر تقني أكثر منه مادي، وهو ما يميزها عن الجرائم التقليدية التي تعتمد على الاحتكاك المباشر بين الجاني والضحية[2].

تتميز كذلك بصعوبة اكتشافها في كثير من الأحيان، إذ لا يتم اكتشافها إلا بعد مرور فترة زمنية قد تكون طويلة وغالبا ما يتم ذلك عن طريق الصدفة أو من خلال شكاوى الضحايا أو عمليات تدقيق تقنية متخصصة , ويرجع ذلك إلى قدرة الجاني على إخفاء آثاره الرقمية باستخدام أدوات تقنية متقدمة، مثل التشفير وإخفاء الهوية و يصعب عملية التتبع الجنائي.[3]

ومن الخصائص المهمة أيضا سهولة ارتكاب هذه الجريمة من الناحية العملية، رغم تعقيدها التقني إذ يمكن لفرد واحد يمتلك مهارات تقنية متوسطة أو متقدمة أن ينفذ عمليات احتيالية واسعة النطاق في وقت قصير , ويعود ذلك إلى طبيعة الإنترنت المفتوحة وسهولة

[1] – عبد العزيز بن عبد الرحمن الشمري، "**جريمة النصب والاحتيال**"، مجلة العدل، عدد 39، 2000، وزارة العدل السعودية، ، ص 48.

[2] – عبيد علي ناصر موفق وآخرون، "**ماهية جريمة الاحتيال المعلوماتي**"، مجلة القانون والعلوم السياسية، المجلد 09 العدد 33 جامعة تكريت، بغداد، ص 67.

[3] – إبراهيم حسني عبد السميع، **مرجع سابق**، ص 133

الوصول إلى الضحايا عبر الرسائل الإلكترونية أو المواقع المزيفة، و يجعل الجريمة منخفضة التكلفة وعالية العائد بالنسبة للجاني[1].

و تتسم جريمة النصب الإلكتروني بالطابع الخفي وسرعة التنفيذ و يمكن ارتكابها دون مواجهة مباشرة بين الجاني والضحية، بل قد يتم الاحتيال أثناء تصفح موقع إلكتروني أو فتح رابط مشبوه دون إدراك الضحية لذلك , وتساعد التقنيات الحديثة مثل الفيروسات وبرامج التجسس في تسريع تنفيذ الجريمة وسرقة البيانات أو الأموال في وقت وجيز جد دون ترك آثار واضحة.[2]

وتعد خاصية الطابع العابر للحدود من أبرز السمات المميزة لهذه الجريمة و لا تعترف الحدود الجغرافية في الفضاء الإلكتروني، و يسمح للجاني بتنفيذ أفعاله من دولة معينة بينما يقع الضرر في دولة أخرى , وهذا ما يطرح إشكاليات قانونية كبيرة تتعلق بالاختصاص القضائي والتعاون الدولي، ويجعل من مكافحة هذه الجرائم أمر يتطلب تنسيق دولي فعال بين مختلف الدول.[3]

و تعتمد هذه الجريمة بشكل أساسي على استخدام الحاسوب وشبكة الإنترنت كوسيلة تنفيذ رئيسية و لا يمكن ارتكابها دون وسيط إلكتروني , فالحاسوب لا يعد فقط أداة مساعدة و هو العنصر الأساسي في تنفيذ الجريمة، سواء من خلال إنشاء المواقع المزيفة أو إرسال الرسائل الاحتيالية أو اختراق الأنظمة المعلوماتية، مما يربط الجريمة ارتباط عضوي بالتكنولوجيا الحديثة.[4]

---

[1] – الصغير جميل عبد الباقي، **مرجع سابق**، ص 52

[2] – محمد طارق رمضان، **مرجع سابق**، 68.

[3] – عرب يونس، **موسوعة القانون وتقنية المعلومات، الجزء الأول**، اتحاد المصارف العربية، 2002، ص 234.

[4] – محمد عبد الله أبو بكر سلامة، **جرائم الكمبيوتر والإنترنت**، منشأة المعارف، الإسكندرية، 2006، ص 123.

ومن الخصائص أيضا استهدافها للمؤسسات المالية والاقتصادية ذات الطابع الحساس، مثل البنوك والمتاجر الإلكترونية وشركات الدفع الرقمي، نظرا لاحتوائها على بيانات مالية مهمة وسهولة تحويل الأموال إلكتروني , ويؤدي هذا الاستهداف إلى خسائر مالية كبيرة و دفع هذه المؤسسات إلى تطوير أنظمة حماية إلكترونية متقدمة لمواجهة هذا النوع من الجرائم.[1]

و تتسم بكون مرتكبيها غالبا من ذوي الخبرة في مجال التكنولوجيا والمعلوماتية، حيث يمتلكون مهارات في البرمجة وهندسة الشبكات تمكنهم من اختراق الأنظمة والتلاعب بالبيانات دون كشف هويتهم بسهولة , وهذا ما يجعل التحقيق في هذه الجرائم يتطلب خبراء متخصصين في الأمن السيبراني وتحليل البيانات الرقمية.[2]

الفرع الثالث: تمييز جرائم النصب والاحتيال الإلكتروني عما يشابهها من الجرائم الأخرى

تتشابه جريمة النصب والاحتيال الإلكتروني مع جريمة النصب التقليدية من حيث الجوهر، إذ تقوم كلتاهما على عنصر الغش والخداع بهدف الاستيلاء على أموال الغير دون وجه حق، وذلك من خلال التأثير على إرادة الضحية ودفعها إلى تسليم المال برضا ظاهري ناتج عن التضليل , و الهدف المشترك بينهما يتمثل في تحقيق منفعة غير مشروعة للجاني على حساب المجني عليه معتمد في ذلك على الحيلة والدهاء والقدرة على الإقناع.[3]

غير أن هذا التشابه لا ينفي وجود اختلافات بين الجريمتين و إن النصب التقليدي يتم غالبا بوسائل مادية ومباشرة تعتمد على التواصل الشخصي بين الجاني والضحية، في حين

---

[1] – عبد العزيز بن عبد الرحمن الشمري، **المرجع السابق**، ص 47.

[2] – فاطمة الزهراء رمضاني، "**القصور التشريعي في مجال الجريمة المعلوماتية**"، مجلة الأستاذ الباحث، جامعة المسيلة، المجلد 07، العدد 02، 2022، ص 89

[3] – عبد العزيز بن عبد الرحمن الشمري ، **المرجع نفسه** , ص 56.

أن النصب الإلكتروني يتم عبر وسائل رقمية غير مادية، مثل المواقع الإلكترونية البريد الإلكتروني والتطبيقات الرقمية , وهذا ما يجعل الجريمة الإلكترونية أكثر تعقيد من حيث الأسلوب وأوسع انتشار من حيث النطاق، إذ يمكن تنفيذها عن بعد دون أي لقاء مباشر بين الطرفين.[1]

و تمتاز بقدرة الجاني على تكرار الأفعال الإجرامية في وقت وجيز وبنفس الوسائل التقنية، و يمنحها طابع آلي ومنظم مقارنة بالجريمة التقليدية ويؤدي هذا التكرار إلى صعوبة تحديد عدد الجرائم المرتكبة، حيث يثار التساؤل حول ما إذا كانت الجريمة تعد فعل واحد متعدد النتائج أم عدة جرائم مستقلة، وهو ما يختلف باختلاف الوقائع وطبيعة النشاط الإجرامي.

ومن الناحية القانونية واجهت العديد من التشريعات صعوبة في إيجاد نصوص خاصة تنظم جريمة الاحتيال الإلكتروني، و دفعها إلى تطبيق النصوص التقليدية الخاصة بالاحتيال على الجرائم المعلوماتية، وهو ما أخذت به بعض الدول مثل بريطانيا وكندا وأستراليا , و ساهمت بعض الاتفاقيات الدولية والإقليمية مثل الاتفاقية الأوروبية للجرائم السيبرانية في وضع إطار عام لمكافحة هذا النوع من الجرائم العابرة للحدود.[2]

وفي الختام يمكن القول إن جريمة النصب والاحتيال الإلكتروني، رغم تشابهها مع النصب التقليدي في الهدف والنتيجة إلا أنها تختلف عنه اختلاف , من حيث الوسائل والطبيعة

[1] – عرب يونس، **موسوعة القانون وتقنية المعلومات ، المرجع السابق** ، ص 239.

[2] – النصيرات وائل، "**الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها**"، بحث مقدم إلى المؤتمر الدولي الأول لمكافحة الجريمة المعلوماتية، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2014، ص 21.

التقنية والطابع العابر للحدود، و يجعلها أكثر خطورة وتعقيد وهذا ما يستوجب تطوير التشريعات الوطنية وتعزيز التعاون الدولي لمكافحة هذا النوع من الجرائم بفعالية أكبر.[1]

المطلب الثاني: أنواع جريمة النصب والاحتيال الإلكتروني

تتخذ جريمة النصب والاحتيال الإلكتروني صور متعددة تتنوع بحسب الوسائل المستعملة في تنفيذها وطبيعة البيئة الرقمية التي ترتكب فيها، وهو ما يعكس مرونتها وقدرتها على التطور المستمر مع تطور التكنولوجيا الحديثة , فهذه الجريمة لم تعد مقتصرة على أسلوب واحد، بل أصبحت ترتكب عبر قنوات إلكترونية مختلفة تستهدف الأفراد والمؤسسات على حد سواء، الأمر الذي جعل من الضروري تصنيفها إلى أنواع تساعد على فهمها وتحليلها بشكل أدق.

وفي هذا الإطار يمكن التمييز بين النصب والاحتيال عبر وسائل الاتصال الإلكتروني، والنصب والاحتيال عبر المنصات الرقمية والمعاملات المالية الإلكترونية، حيث يبرز كل نوع بخصائص وأساليب مختلفة في التنفيذ، إلا أنها تشترك جميع في الهدف المتمثل في الاستيلاء غير المشروع على أموال أو بيانات الغير باستعمال وسائل احتيالية رقمية متطورة.

الفرع الأول: النصب والاحتيال عبر وسائل الاتصال الإلكتروني

من أبرز صور الجرائم المستحدثة التي ظهرت مع تطور تقنيات الاتصال الحديثة , و يعتمد الجاني في هذا النوع من الجرائم على استخدام وسائل الاتصال الرقمية مثل البريد الإلكتروني، والرسائل النصية وتطبيقات المراسلة الفورية من أجل التواصل مع الضحية وإقناعها بوقوعها في خطأ أو الاستجابة لطلب معين يؤدي إلى الاستيلاء على أموالها أو

[1] – عرب يونس، **موسوعة القانون وتقنية المعلومات، المرجع السابق**، ص 127

بياناتها , وتكمن خطورة هذا النوع من الجرائم في اعتماده على الإقناع النفسي والخداع غير المباشر و يجعل الضحية تتفاعل مع الجاني دون إدراك أنها في موقف احتيالي[1].

وتتميز هذه الجريمة بكونها تعتمد على أساليب متطورة من التضليل الإلكتروني، حيث يقوم الجاني بإرسال رسائل تحمل طابع رسمي أو شخصي يوهم فيها الضحية بأنها صادرة عن جهات موثوقة مثل البنوك أو المؤسسات الحكومية أو الشركات العالمية, وغالبا ما تتضمن هذه الرسائل روابط إلكترونية مزيفة تهدف إلى سرقة المعلومات الحساسة مثل كلمات المرور أو أرقام الحسابات البنكية، و يؤدي إلى وقوع خسائر مالية مباشرة للضحايا.[2]

من أهم صور الاحتيال عبر وسائل الاتصال الإلكتروني ما يعرف بأسلوب "التصيد الاحتيالي"، وهو أسلوب يعتمد على خداع المستخدمين من خلال إنشاء رسائل أو مواقع إلكترونية مزيفة تحاكي المواقع الأصلية , ويهدف هذا الأسلوب إلى دفع الضحية إلى إدخال بياناتها الشخصية أو المالية، و يسمح للجاني بالاستيلاء عليها واستغلالها في

عمليات غير مشروعة , ويؤكد الفقه أن هذا النوع من الاحتيال يمثل تهديد مباشر للأمن المعلوماتي للأفراد.[3]

ويلاحظ أن هذه الجرائم لا تتطلب وجود مادي للجاني بل يمكن تنفيذها عن بعد باستخدام أدوات إلكترونية بسيطة نسبيا، مما يجعل ارتكابها سهل مقارنة بالجرائم التقليدية , و تعدد وسائل الاتصال الحديثة وسهولة إنشاء حسابات وهمية يزيد من صعوبة تحديد

[1] – أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006، ص 45.

[2] – أحمد محمود مصطفى، **جرائم الحاسبات الآلية في التشريع المصري**، دار النهضة العربية، القاهرة، 2010، ص 78.

[3] – أسامة سمير حسين، **الاحتيال الإلكتروني الوجه القبيح للتكنولوجيا**، الجنادرية للنشر، عمان، 2006، ص 32.

هوية الجاني، وهو ما يشكل تحدي كبير أمام أجهزة التحقيق والعدالة الجنائية في كشف هذه الجرائم.[1]

ومن الخصائص المهمة لهذا النوع من الاحتيال أنه يعتمد بشكل كبير على العنصر النفسي، حيث يستغل الجاني ثقة الضحية أو خوفها أو طمعها من أجل دفعها لاتخاذ قرار خاطئ , وغالبا ما يتم ذلك عبر رسائل تحمل وعود بأرباح مالية كبيرة أو تهديدات مزيفة تتعلق بحسابات بنكية، مما يؤدي إلى استجابة الضحية دون تحقق مسبق من صحة المعلومات[2].

و التطور المستمر في وسائل الاتصال الإلكترونية ساهم في زيادة تنوع أساليب الاحتيال، حيث ظهرت تطبيقات ذكية ومحادثات فورية يتم استغلالها في عمليات النصب بشكل متطور , وقد أصبح الجاني يستخدم تقنيات حديثة مثل انتحال الهوية الرقمية واختراق الحسابات الشخصية و يزيد من خطورة هذه الجرائم واتساع نطاقها.[3]

وتكمن خطورة هذه الجرائم أيضا في صعوبة تتبعها قانونيا نظرا لاعتمادها على خوادم خارجية وشبكات دولية قد تكون خارج نطاق الدولة التي يقع فيها الضحية , وهذا ما يجعل التعاون الدولي ضرورة ملحة لمكافحة هذا النوع من الجرائم، خاصة في ظل الطابع العابر للحدود الذي يميز الجرائم الإلكترونية.[4]

ومن جهة أخرى فإن النصب عبر وسائل الاتصال الإلكتروني يستهدف فئات واسعة من المستخدمين دون تمييز، سواء كانوا أفراد عاديين أو مؤسسات اقتصادية أو مالية و يؤدي

---

[1] – أمير فرج يوسف، **جرائم المعلومات على شبكة الإنترنت**، دار المطبوعات الجامعية، الإسكندرية، 2009، ص 51.

[2] – أحمد عمرة حسبو، **حماية الحريات في مواجهة نظم المعلومات**، دار النهضة العربية، القاهرة، 2006، ص 120.

[3] – أسامة أحمد المناعسة، **جرائم الحاسب الآلي والإنترنت**، دار وائل للنشر، 2001، ص 66

[4] – أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة، الجزائر، 2007، ص 95.

إلى خسائر مالية كبيرة على المستوى الفردي والجماعي , و ضعف الوعي الرقمي لدى بعض المستخدمين يزيد من احتمالية وقوعهم ضحايا لهذه الجرائم.[1]

و يعتمد الجاني في كثير من الأحيان على أساليب متقدمة في إخفاء هويته مثل استخدام الشبكات الافتراضية الخاصة (VPN) أو برامج التشفير، مما يجعل عملية التتبع الأمني أكثر تعقيد , وهذا ما يفرض على الجهات المختصة تطوير أدوات تقنية متقدمة لمواجهة هذا النوع من الجرائم.[2]

وفي الختام يمكن القول إن جريمة النصب والاحتيال عبر وسائل الاتصال الإلكتروني تمثل أحد أخطر أشكال الجرائم المعلوماتية الحديثة، لما لها من قدرة على التوسع السريع والتأثير المباشر على الأفراد والمؤسسات, وتتطلب مواجهة قانونية وتقنية متكاملة وتقوم على تحديث التشريعات وتعزيز الوعي الرقمي وتطوير وسائل الحماية الإلكترونية للحد من انتشارها.

الفرع الثاني: النصب والاحتيال عبر المنصات الرقمية والمعاملات المالية الإلكترونية

يعد النصب والاحتيال عبر المنصات الرقمية والمعاملات المالية الإلكترونية من أخطر صور الجرائم المستحدثة في العصر الرقمي حيث ارتبط تطوره بالانتشار الواسع للتجارة الإلكترونية والخدمات البنكية عبر الإنترنت[3], فقد أصبحت المنصات الرقمية بيئة خصبة لارتكاب هذا النوع من الجرائم بسبب اعتمادها على التفاعل غير المباشر بين المستخدمين وإتمام المعاملات عن بعد، مما يتيح للجاني استغلال الثقة الرقمية بين الأطراف , وتتميز

[1] – أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة، 1994، ص 312.

[2] – أحمد عمرة حسبو، **المرجع السابق** , ص 121

[3] – أحمد خليفة الملط، **المرجع السابق**، ص 87

هذه الجرائم بأنها تستهدف بشكل مباشر الأموال والبيانات المالية وهو ما يجعلها تمس الاقتصاد الرقمي والأمن المالي للأفراد والمؤسسات على حد سواء.[1]

وتتجلى خطورة هذا النوع من الاحتيال في كونه يعتمد على إنشاء منصات إلكترونية مزيفة أو تطبيقات وهمية تحاكي المنصات الأصلية للبنوك أو الشركات التجارية، حيث يتم إقناع الضحية بإدخال بياناتها البنكية أو الشخصية بدعوى إتمام عملية شراء أو استثمار , وبعد الحصول على هذه البيانات يتم استخدامها في عمليات سحب غير مشروعة أو تحويل الأموال , ويؤكد الفقه أن هذا الأسلوب يعتمد على تقنيات متقدمة في التزوير الإلكتروني يصعب كشفها في كثير من الأحيان.[2]

و من أبرز صور الاحتيال في هذا المجال ما يتعلق ببطاقات الائتمان، حيث يقوم الجاني بسرقة بيانات البطاقة أو نسخها باستخدام وسائل تقنية متطورة، ثم استخدامها في عمليات شراء إلكترونية أو سحب أموال دون علم صاحبها , وقد اعتبر الفقه هذا النوع من الجرائم من أخطر الجرائم المالية الإلكترونية نظرا لصعوبة تتبع العمليات المالية الرقمية وسرعة تنفيذها عبر شبكات الدفع العالمية.[3]

وتتميز هذه الجرائم كذلك بارتباطها الوثيق بالتجارة الإلكترونية و يستغل الجاني عمليات البيع والشراء عبر الإنترنت للإيقاع بالضحايا, من خلال عروض وهمية أو منتجات غير موجودة أصلا , وغالبا ما يتم إنشاء متاجر إلكترونية مزيفة تبدو حقيقية من حيث الشكل والتصميم، مما يمنح الضحية شعور بالثقة ويجعلها تقدم على الدفع دون تحقق مسبق , ومن الخصائص المهمة لهذا النوع من الاحتيال أنه يعتمد على تقنيات التوقيع الإلكتروني

[1] – حسن طاهر داوود، **جرائم نظم المعلومات**، منشورات أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص 75.

[2] – خالد محمد المهيري، **جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية**، معهد القانون الدولي، دبي، ص 313.

[3] – رياض فتح الله بصلة، **جرائم بطاقات الائتمان**، دار الشروق، القاهرة، 1995، ص 44.

والمعاملات الرقمية، حيث يتم التلاعب بهذه الأنظمة أو تزويرها لتحقيق أهداف غير مشروعة , وقد أدى ذلك إلى ظهور إشكالات قانونية تتعلق بحجية التوقيع الإلكتروني ومدى إمكانية الاعتماد عليه كوسيلة إثبات في المعاملات القانونية و دفع العديد من التشريعات إلى تنظيم هذا المجال بشكل خاص.[1]

و هذه الجرائم تتسم بالطابع المنظم في كثير من الحالات حيث لا ترتكب بشكل فردي فقط، بل قد تنفذها شبكات إجرامية متخصصة تعمل بشكل منظم عبر الإنترنت، وتقوم بتقسيم الأدوار بين أعضائها، مثل إنشاء المواقع واستدراج الضحايا وتحويل الأموال وهذا ما يجعل مكافحتها أكثر تعقيدًا من الجرائم الفردية التقليدية.[2]

وتبرز خطورة الاحتيال عبر المنصات الرقمية في كونه يعتمد على استغلال الثقة في النظام المالي الإلكتروني، حيث يشعر المستخدم بالأمان عند التعامل مع تطبيقات الدفع أو البنوك الإلكترونية، وهو ما يستغله الجاني لإقناعه بتنفيذ عمليات مالية غير صحيحة و أن سرعة تنفيذ المعاملات الإلكترونية تجعل من الصعب إيقاف العملية الاحتيالية بعد بدئها.[3]

ومن الناحية القانونية واجهت التشريعات صعوبة في مواكبة هذا النوع من الجرائم و أدى إلى اعتماد العديد من الدول على القوانين العامة للسرقة والنصب لتجريم الأفعال الإلكترونية، مع إضافة نصوص خاصة لاحق لتنظيم الجرائم المعلوماتية وقد ساهمت بعض التشريعات

[1] – سامح محمد عبد الحكيم، **الحماية الجنائية لبطاقات الائتمان**، دار النهضة العربية، القاهرة، 2003، ص 60.

[2] – خالد مصطفى فهمي، **النظام القانوني للتوقيع الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2007، ص 91.

[3] – حسين بن سعيد الغافري، **السياسة الجنائية في مواجهة جرائم الإنترنت**، دار النهضة العربية، القاهرة، 2009، ص 110.

العربية في تطوير إطار قانوني خاص لمكافحة الجرائم الإلكترونية وحماية المعاملات الرقمية.[1]

و التحقيق في هذه الجرائم يتطلب خبرة تقنية متقدمة و نظرا لاعتمادها على بيانات رقمية معقدة مثل عناوين IP والسجلات الإلكترونية وعمليات الدفع الرقمية , ويواجه المحققون صعوبات كبيرة في تتبع الأموال أو تحديد هوية الجناة، خاصة إذا تم استخدام وسائل إخفاء الهوية أو التحويل عبر دول متعددة.[2]

ومنه يمكن القول أن النصب والاحتيال عبر المنصات الرقمية والمعاملات المالية الإلكترونية يمثل أحد أخطر صور الإجرام المعاصر، لما له من تأثير مباشر على الاقتصاد الرقمي والثقة في الأنظمة المالية الإلكترونية , و تطوره المستمر يفرض على المشرع ضرورة تحديث النصوص القانونية وتعزيز التعاون الدولي وتطوير وسائل الحماية الإلكترونية لضمان أمن المعاملات الرقمية.[3]

المبحث الثاني: أركان جريمة النصب و الاحتيال الإلكتروني

تعد الأركان من أهم الجوانب القانونية التي يتعين التطرق إليها لفهم هذه الجريمة فهما دقيقا، باعتبار أن قيام المسؤولية الجزائية لا يتحقق إلا بتوافر أركانها القانونية المتمثلة في الركن الشرعي والركن المادي والركن المعنوي , وتكتسي دراستها أهمية خاصة في ظل الطبيعة التقنية المعقدة لهذه الجريمة، حيث تختلف في بعض مظاهرها عن الجرائم التقليدية

[1] – طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي والنظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة، 2009، ص 146.

[2] – إبراهيم منصور الشحات ، **الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية**، دار النهضة العربية، القاهرة، 2002، ص 75.

[3] – خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة، عمان، 2000، ص 93.

نتيجة اعتمادها على الوسائل الإلكترونية في التنفيذ، مما يثير إشكالات قانونية تتعلق بالتكييف والإثبات.

ومن هذا المنطلق تناول هذا المبحث في مطلبه الأول الركن الشرعي باعتباره الأساس الذي يقوم عليه مبدأ الشرعية الجنائية في تجريم النصب والاحتيال الإلكتروني، ثم جاء في المطلب الثاني الركن المادي من خلال بيان السلوك الإجرامي والنتيجة الإجرامية وعلاقة السببية، ليختتم في المطلب الثالث بدراسة الركن المعنوي الذي يعكس القصد الجنائي بنوعيه العام والخاص في هذه الجريمة

المطلب الأول: الركن الشرعي

يُعدّ الركن الشرعي الأساس الذي تقوم عليه المسؤولية الجزائية في جريمة النصب والاحتيال الإلكتروني[1]، إذ لا يمكن وصف فعلٍ ما بأنه جريمة ولا توقيع عقوبة على مرتكبه إلا بمقتضى نص قانوني سابق على ارتكابه، تطبيقًا لمبدأ الشرعية الجنائية الذي تكرّسه المادة الأولى من قانون العقوبات الجزائري.

وقد تعامل المشرع الجزائري مع جريمة النصب والاحتيال الإلكتروني وفق منهج مزدوج يقوم على تطبيق النص العام للنصب التقليدي المقرر في المادة 372 من قانون العقوبات، إلى جانب النصوص الخاصة المتعلقة بالجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات

[1] – خالد محمد المهيري، **مرجع سابق**، ص 314.

الواردة في المادة 394 مكرر وما يليها من القانون ذاته، والتي أُدرجت بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدّل والمتمم لقانون العقوبات.[1]

ومن هذا المنطلق يتناول هذا المطلب في فرعه الأول مبدأ الشرعية الجنائية وتطبيقه على جريمة النصب والاحتيال الإلكتروني في ضوء المادتين 372 و394 مكرر من قانون العقوبات الجزائري، ويخصَّص الفرع الثاني لدراسة نطاق التجريم والعقاب المقرّر لهذه الجريمة وفق التشريع الجزائري.

الفرع الأول: مبدأ الشرعية الجنائية وتطبيقه على جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

كرّس المشرع الجزائري مبدأ الشرعية الجنائية بنصّه في المادة الأولى من قانون العقوبات على أنه «**لا جريمة ولا عقوبة أو تدابير أمن بغير قانون**».[2]، وهو ما يُعدّ ترجمة لما نصت عليه المادة **58 من دستور 2020** [3] التي تضمن مبدأ شرعية التجريم والعقاب. ومقتضى هذا المبدأ أنه لا يجوز تجريم أي فعل أو توقيع أي عقوبة عليه إلا بنص قانوني سابق على ارتكابه، حماية لحقوق الأفراد وحرياتهم من التعسف

[1]-**القانون رقم 04-15 المؤرخ في 10 نوفمبر** 2004 المعدّل والمتمم **للأمر رقم 66-156** المتضمن **قانون العقوبات**، ج.ر، العدد 71، الصادرة في 10 نوفمبر 2004.

[2] -**الأمر رقم 66-156** المؤرخ في 8 يونيو 1966 المتضمن **قانون العقوبات**، المعدّل والمتمم، **المادة 1.**

[3] -**دستور الجزائر2020**، المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية عدد 82، الصادرة في 02 نوفمبر 2024 .

وتطبيقًا لهذا المبدأ، فإن جريمة النصب التقليدية يُجرّمها المشرع الجزائري بمقتضى المادة 372 من قانون العقوبات، التي تنص على أنه: «كل من توصّل إلى استلام أو تلقّي أموال أو منقولات أو سندات أو تصرّفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات، وذلك إما باستعمال أسماء أو صفات كاذبة، وإما باستعمال طرق احتيالية للإيهام بوجود مشروعات كاذبة أو سلطة أو ائتمان وهمي أو لإحداث الأمل في حصول ربح وهمي أو في إيقاع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوعها، أو لإحداث الاعتقاد بوجود دَين وهمي أو إعطاء مخالصة عنه، وبدّد أو شرع في تبديد كل تلك الأموال يُعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500 إلى 20.000 دج».[1]

غير أن هذا النص العام، على عمومه، لم يكن كافيًا وحده لاستيعاب الصور المستحدثة للنصب المرتكب عبر الوسائط الإلكترونية، الأمر الذي دفع المشرع الجزائري إلى التدخل بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدّل والمتمم لقانون العقوبات، ليُدرج القسم السابع مكرر تحت عنوان «المساس بأنظمة المعالجة الآلية للمعطيات» متضمّنًا المواد من 394 مكرر إلى 394 مكرر 7، استجابةً للالتزامات الدولية المترتبة على انضمام الجزائر إلى الاتفاقيات المتعلقة بمكافحة الجريمة المعلوماتية.[2]

[1] -**المادة 372 من الأمر رقم 66-156** المؤرخ في 8 يونيو 1966 المتضمن **قانون العقوبات**، المعدّل والمتمم. الجريدة الرسمية عدد 49 الصادرة في 11 يونيو سنة 1966.

[2] -أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص، الجزء الأول**، الطبعة الثانية عشرة دار هومة، الجزائر، ، 2023، ص 326.

وتنصّ المادة 394 مكرر من قانون العقوبات الجزائري على أنه: «يُعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. وتُضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج».[1]

كما تُكمّل هذا النصّ المواد 394 مكرر 1 و394 مكرر 2 التي تجرّم على التوالي إدخال معطيات في نظام المعالجة الآلية أو تعديلها أو حذفها أو إتلافها بطريق الغش، إضافة إلى تجريم تصميم أو حيازة أو نشر معطيات مخزّنة أو معالَجة أو مرسلة بنظام معلوماتي يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم. وعليه، فإن الركن الشرعي لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري يقوم على ازدواجية النصّ العام (المادة 372) والنصوص الخاصة (المادة 394 مكرر وما يليها)، بحيث يُكيَّف الفعل الإجرامي وفق ما إذا كانت الوسيلة الإلكترونية مجرد أداةٍ للاحتيال أم أن الجريمة قد طالت في حد ذاتها نظام المعالجة الآلية للمعطيات.[2]

---

[1]–**المادة 394 مكرر من قانون العقوبات الجزائري**، المضافة بموجب **القانون رقم 15–04** مؤرخ في أوّل فبراير سنة 2015 يحدد القواعد يحدد القواعد العامة المتغلقة بالتوقيع والتصديق الإلكتروني.، الجريدة الرسمية عدد 06 الصادرة في 10–02–2015.

[2]–**المادتان 394 مكرر 1 و394 مكرر 2 من قانون العقوبات الجزائري.**

ويترتب عن إعمال مبدأ الشرعية في هذا المجال أن يلتزم القاضي الجزائي بالتفسير الضيّق للنصوص الجنائية، فلا يجوز له القياس على المادة 372 لتجريم أفعال إلكترونية لا تتوافر فيها العناصر الموضوعية للنصب التقليدي، بل يتعيّن عليه الرجوع إلى النصوص الخاصة المقرّرة في المواد 394 مكرر وما يليها متى تعلّق الأمر بأفعال ماسّة بأنظمة المعالجة الآلية للمعطيات، ضمانًا لاحترام مبدأ شرعية التجريم والعقاب.[1]

الفرع الثاني: نطاق التجريم والعقاب في جريمة النصب والاحتيال الإلكتروني وفق المادتين 372 و394 مكرر

يمتدّ نطاق التجريم في جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري ليشمل صورتين متمايزتين: الأولى تتعلّق بالأفعال التي تتحقّق فيها أركان النصب التقليدي المنصوص عليها في المادة 372 من قانون العقوبات، حيث تُستعمل الوسيلة الإلكترونية مجرّد أداة لتنفيذ الاحتيال؛ والثانية تتعلق بالأفعال الماسّة مباشرةً بأنظمة المعالجة الآلية للمعطيات والمنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات.[2]

[1]–أحسن بوسقيعة، **المرجع السابق**، ص 330.

[2] –علي عبد القادر القهوجي، **قانون العقوبات – القسم الخاص، منشورات الحلبي الحقوقية**، بيروت، الطبعة الثانية، 2002، ص 285.

ففي إطار المادة 372 من قانون العقوبات، يقوم التجريم على توافر السلوك الاحتيالي المتمثل في استعمال أسماء أو صفات كاذبة أو طرق احتيالية، مع تسليم الضحية للمال ووجود نية الاستيلاء على مال الغير. ويستوي في ذلك أن تتم هذه الأفعال عبر وسائل تقليدية أو إلكترونية كالبريد الإلكتروني، أو المواقع المزيّفة، أو منصّات التواصل الاجتماعي، طالما توافرت العناصر الموضوعية للجريمة.[1]

أما في إطار المادة 394 مكرر وما يليها، فإن نطاق التجريم يمتدّ إلى الأفعال التي تستهدف نظام المعالجة الآلية للمعطيات في حدّ ذاته، كالدخول أو البقاء غير المشروعين، أو التلاعب بالمعطيات بإدخالها أو تعديلها أو حذفها بطريق الغش، أو استعمال معطيات متحصّل عليها من إحدى هذه الجرائم، وكذا تصميم أو حيازة أو نشر برامج معلوماتية تُستعمل لارتكابها. ويُلاحظ أن هذه النصوص تُجرّم السلوك بصرف النظر عن تحقّق الضرر المالي، وهو ما يعكس توجّه المشرع نحو الحماية الاستباقية للأنظمة المعلوماتية.[2]

وفيما يتعلّق بنطاق العقاب، فقد قرّر المشرع الجزائري في المادة 372 من قانون العقوبات عقوبة الحبس من سنة إلى خمس سنوات وغرامة مالية من 500 إلى 20.000 دج لكل من ارتكب جريمة النصب، مع إمكانية تشديد العقوبة إلى عشر سنوات حبسًا وغرامة قد تصل

[1] –أحسن بوسقيعة، **المرجع السابق**، ص 332.

[2] –**القانون رقم 09-04** المؤرخ في 5 أوت 2009 المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، ج.ر، العدد 47.

إلى 100.000 دج إذا كان الجاني قد لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أيّ سندات أخرى مماثلة لشركةٍ أو مؤسّسة تجارية أو صناعية، وذلك وفق الفقرة الثانية من المادة 372.[1]

أما في إطار المادة 394 مكرر، فقد تدرّج المشرع الجزائري في تقرير العقوبة وفق جسامة الفعل؛ إذ قرّر الحبس من ثلاثة أشهر إلى سنة وغرامة من 50.000 إلى 100.000 دج للدخول أو البقاء غير المشروعَين في نظام المعالجة الآلية، وضاعف العقوبة في حالة ترتّب حذف أو تغيير المعطيات، ورفعها إلى الحبس من ستة أشهر إلى سنتين وغرامة من 50.000 إلى 150.000 دج إذا نتج عن الفعل تخريب نظام اشتغال المنظومة. كما تصل العقوبة بمقتضى المادة 394 مكرر 1 إلى الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 إلى 2.000.000 دج بالنسبة للتلاعب بالمعطيات.[2]

وقد شدّد المشرع الجزائري العقوبة بموجب المادة 394 مكرر 3 لتُصبح الحبس من سنتين إلى عشر سنوات وغرامة من 5.000.000 إلى 10.000.000 دج إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسّسات الخاضعة للقانون العام. كما أضاف عقوبات تكميلية تتمثل في مصادرة الأجهزة والبرامج المستعملة في ارتكاب الجريمة وإغلاق المواقع التي

[1] –**المادة 372 الفقرة الثانية من قانون العقوبات الجزائري.**

[2] –**المواد 394 مكرر و394 مكرر 1 من قانون العقوبات الجزائري.**

ارتكبت بواسطتها وفق المادة 394 مكرر 6، فضلًا عن مسؤولية الشخص المعنوي بمقتضى المادة 394 مكرر 5.[1]

ويُستفاد ممّا تقدّم أن المشرع الجزائري قد تبنّى سياسةً جنائية متكاملة في مواجهة جريمة النصب والاحتيال الإلكتروني، تجمع بين النصّ العام للنصب الوارد في المادة 372 من قانون العقوبات والنصوص الخاصّة بالجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات الواردة في المادة 394 مكرر وما يليها، مدعّمةً بأحكام القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بما يضمن استيعاب مختلف الصور المستحدثة لهذه الجريمة وتحقيق الردع المطلوب في ظل التطور المتسارع للتكنولوجيا.[2]

المطلب الثاني: الركن المادي

في جريمة النصب والاحتيال الإلكتروني العنصر الظاهر الذي تتجسد من خلاله هذه الجريمة في الواقع، إذ لا تقوم المسؤولية الجزائية بمجرد النية أو التفكير وإنما يجب أن يصدر عن الجاني سلوك إجرامي ملموس يؤدي إلى إحداث نتيجة ضارة تمس أموال أو بيانات الغير.

وتزداد أهمية دراسة هذا الركن في الجرائم الإلكترونية لكونها تعتمد على أفعال غير مادية , و تتم عبر الوسائط الرقمية مما يطرح إشكالات خاصة في تحديد السلوك الإجرامي وإثباته

[1]-**المواد 394 مكرر 3 و394 مكرر 5 و394 مكرر 6 من قانون العقوبات الجزائري.**

[2] -أحسن بوسقيعة، **المرجع السابق**، ص 340.

, و في هذه الجريمة لا يقتصر على الفعل الاحتيالي فقط بل يمتد ليشمل النتيجة الإجرامية المتمثلة في وقوع الضرر المالي، إضافة إلى ضرورة وجود علاقة سببية تربط بين سلوك الجاني والنتيجة المتحققة.

ومن هذا المنطلق سيتم تناول هذا المطلب من خلال فرعين، حيث يتناول الفرع الأول السلوك الإجرامي المكون لجريمة النصب والاحتيال الإلكتروني، بينما يخصص الفرع الثاني لدراسة النتيجة الإجرامية وعلاقة السببية باعتبارهما عنصرين مكملين لقيام الركن المادي.

الفرع الأول: السلوك الإجرامي المكوِّن لجريمة النصب والاحتيال

في جريمة النصب والاحتيال الإلكتروني العنصر الأساسي في قيام الركن المادي، إذ لا يمكن تصور هذه الجريمة دون وجود فعل إيجابي يصدر عن الجاني يتمثل في استعمال وسائل احتيالية تهدف إلى خداع الضحية وإيقاعها في الغلط , ويأخذ هذا السلوك صور متعددة تختلف باختلاف الوسائل المستعملة، غير أنه يجتمع في جوهره حول فكرة التدليس والخداع والتضليل من أجل الاستيلاء على مال الغير , وقد أكد الفقه الجنائي أن هذا السلوك هو التعبير الخارجي عن الإرادة الإجرامية التي تسعى إلى تحقيق منفعة غير مشروعة.[1]

ويتخذ السلوك الإجرامي في جريمة النصب والاحتيال الإلكتروني شكل أفعال مادية أو افتراضية تتم عبر الوسائط الرقمية، مثل إنشاء مواقع وهمية أو إرسال رسائل مزيفة أو انتحال صفة شخص أو جهة موثوقة , وتتميز هذه الأفعال بكونها غير مباشرة حيث لا يلتقي الجاني بالضحية وجه لوجه، بل يتم التواصل عبر بيئة إلكترونية تسمح بتعدد وسائل

[1] – حمزة بن عقون، "**السلوك الإجرامي للمجرم المعلوماتي**"، رسالة ماجستير، منشورة ،الدار الافريقية للكتاب، 2024، ص 31

الاحتيال وسهولة تنفيذها , وهذا ما يجعل السلوك الإجرامي في هذه الجريمة أكثر تعقيد من الجرائم التقليدية.[1]

و يقوم السلوك الإجرامي في كثير من الحالات على استخدام أساليب الخداع المعلوماتي، مثل التلاعب بالبيانات أو تزوير الروابط الإلكترونية أو إرسال إشعارات مالية وهمية , ويهدف الجاني من خلال هذه الوسائل إلى خلق صورة ذهنية كاذبة لدى الضحية تدفعها إلى التصرف في أموالها أو بياناتها دون تحقق.[2]

ويأخذ السلوك الإجرامي أيضا شكل انتحال الهوية الإلكترونية، حيث يقوم الجاني باستخدام أسماء أو صفات غير حقيقية لإيهام الضحية بأنه شخص أو مؤسسة ذات مصداقية , ويعد هذا الأسلوب من أكثر الأساليب انتشار في الجرائم الإلكترونية و نظرا لسهولة إنشاء حسابات وهمية على منصات التواصل الاجتماعي أو المواقع الإلكترونية , ويترتب على ذلك وقوع الضحية في الغلط ودفعها إلى تسليم المال أو البيانات.[3]

ومن خصائص السلوك الإجرامي في هذا النوع من الجرائم أنه يتميز بالتخطيط المسبق والتنظيم، حيث لا يكون مجرد فعل عفوي بل يعتمد على إعداد وسائل احتيالية مسبقة تهدف إلى تحقيق النتيجة الإجرامية , وقد أشار الفقه إلى أن الجاني في الجرائم المعلوماتية غالبا ما يمتلك مهارات تقنية تساعده على تنفيذ أفعاله بدقة عالية دون ترك آثار واضحة.[4]

و قد يتخذ صورة استغلال الثقة و يعتمد الجاني على بناء علاقة ثقة مع الضحية عبر التواصل الإلكتروني التدريجي، ثم استغلال هذه الثقة لاحق في تنفيذ عملية الاحتيال وهذا

---

[1] – نائلة قرة عادل محمد فريد، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي، 2005، ص 67.

[2] – الحسين بن شيخ، **مذكرات في القانون الجزائي الخاص**، دار هومة، الجزائر، 2012، ص 95.

[3] – الفريق طاهر جليل الحبوش، **جرائم الاحتيال: الأساليب والوقاية والمكافحة**، أكاديمية نايف، الرياض، 2001، ص 54

[4] – القهوجي علي عبد القادر، **جرائم الاعتداء على الإنسان والمال**، منشورات الحلبي، 2002، ص 110.

الأسلوب يعد من أخطر الأساليب لأنه يعتمد على العامل النفسي وليس فقط التقني، مما يجعل الضحية أقل حذر وأكثر عرضة للوقوع في الخداع.[1]

ويتميز السلوك الإجرامي في جريمة النصب والاحتيال الإلكتروني بمرونته العالية، إذ يمكن للجاني تغيير وسائله بسرعة وفق لتطور وسائل الحماية الإلكترونية، و يجعل اكتشافه صعب ,و هذا السلوك قد يمتد ليشمل جرائم أخرى مرتبطة مثل سرقة البيانات أو الاحتيال المالي عبر بطاقات الدفع الإلكتروني و يوسع من نطاق الجريمة ويزيد من خطورتها.[2]

وفي الختام يمكن القول إن السلوك الإجرامي في جريمة النصب والاحتيال الإلكتروني يمثل حجر الأساس في قيام الركن المادي، حيث يتجسد في مجموعة من الأفعال الاحتيالية التي تستهدف خداع الضحية عبر الوسائل الرقمية , و تطور التكنولوجيا ساهم في تنوع هذا السلوك وتعقيده و يفرض على المشرع والقضاء تطوير آليات قانونية وتقنية قادرة على مواجهته بفعالية أكبر.

الفرع الثاني:

تعد النتيجة الإجرامية والعلاقة السببية من العناصر الأساسية المكونة للركن المادي في جريمة النصب والاحتيال الإلكتروني، إذ لا يكفي لقيام الجريمة مجرد السلوك الاحتيالي، بل يجب أن يترتب عنه أثر مادي يتمثل في الإضرار بحقوق الضحية المالية أو المساس بذمتها المالية , وتتمثل هذه النتيجة أساسا في انتقال المال أو البيانات من المجني عليه إلى الجاني بطريقة غير مشروعة نتيجة الخداع والتدليس , ويؤكد الفقه الجنائي أن النتيجة الإجرامية تمثل الرابط الذي يترجم السلوك الإجرامي إلى ضرر ملموس يعاقب عليه القانون.[3]

---

[1] – محمد عوض ، **جرائم الأشخاص والأموال**، دار المطبوعات الجامعية، الإسكندرية، 2002، ص 89

[2] – علي عبد القادر القهوجي ، **المرجع السابق** , ص 117

[3] – محمود نجيب حسني، **شرح قانون العقوبات القسم الخاص**، دار النهضة العربية، القاهرة، 1988، ص 132

وفي جريمة النصب والاحتيال الإلكتروني تتخذ النتيجة الإجرامية طابعا ماليا في الغالب، حيث يتم الاستيلاء على الأموال عبر تحويلات إلكترونية أو سحب غير مشروع من الحسابات البنكية أو الاستيلاء على بيانات مالية حساسة , قد تتجسد النتيجة في فقدان الضحية لبياناتها الشخصية أو استخدامها في أغراض غير مشروعة , ويتميز هذا النوع من النتائج بكونه سريع الوقوع وصعب التدارك نظرا لطبيعة البيئة الرقمية التي تتم فيها الجريمة.[1]

وتكمن خطورة النتيجة الإجرامية في هذا النوع من الجرائم في كونها قد تمتد آثارها إلى أكثر من ضحية واحدة، خاصة في حالات الاحتيال الإلكتروني الجماعي أو المنظم حيث يتم استهداف عدد كبير من المستخدمين في وقت واحد , و الضرر الناتج لا يقتصر على الخسائر المالية فقط بل قد يشمل أضرار معنوية مثل فقدان الثقة في المعاملات الإلكترونية والخدمات الرقمية.[2]

أما علاقة السببية في جريمة النصب والاحتيال الإلكتروني، فهي تمثل الرابط القانوني الذي يربط بين السلوك الإجرامي الذي يقوم به الجاني وبين النتيجة الإجرامية المتحققة , أي أنه يجب أن يكون الفعل الاحتيالي هو السبب المباشر في وقوع الضرر , فإذا انقطعت هذه العلاقة أو تدخل عامل خارجي مستقل، انتفت المسؤولية الجنائية عن الجاني أو تم تقليصها بحسب الحالة.[3]

وتأخذ علاقة السببية في الجرائم الإلكترونية أهمية خاصة نظرا لتعقيد البيئة الرقمية وتعدد العوامل التقنية التي قد تتداخل في وقوع النتيجة , فقد يصعب أحيانا تحديد ما إذا كان

[1] – هيثم حمود الشلبي، **إدارة مخاطر الاحتيال في قطاع الاتصالات**، دار صفاء، عمان، 2009، ص 85.

[2] – محمد عبيد الكعيبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، 2009، ص 104.

[3] – الحسين بن شيخ، **مذكرات في القانون الجزائي الخاص**، دار هومة، الجزائر، 2012، ص 61

الضرر قد نتج مباشرة عن فعل الجاني أو عن خلل تقني أو خطأ من الضحية نفسها , لذلك يتطلب إثبات العلاقة السببية في هذا النوع من الجرائم خبرة تقنية دقيقة وتحليل للأدلة الرقمية.[1]

وقد استقر الفقه على أن علاقة السببية في جريمة النصب والاحتيال تقوم متى كان السلوك الاحتيالي هو العامل الحاسم في دفع الضحية إلى تسليم مالها أو بياناتها , بمعنى أن الخداع يجب أن يكون هو الدافع الأساسي الذي أدى إلى تحقق النتيجة , أما إذا تدخلت عوامل أخرى مستقلة تقطع هذا الرابط، فإن المسؤولية الجنائية قد تنتفي أو تتغير طبيعتها.[2]

وفي الجرائم الإلكترونية و قد تتعقد علاقة السببية بسبب تدخل أطراف متعددة في العملية الإجرامية، مثل شركات الاتصالات أو المنصات الرقمية أو حتى أخطاء تقنية في الأنظمة , ومع ذلك يبقى التركيز القانوني منصب على السلوك الأصلي للجاني ومدى تأثيره المباشر في إحداث النتيجة , وهذا ما يجعل تقدير السببية مسألة موضوعية تخضع لسلطة القاضي التقديرية المدعمة بالخبرة التقنية[3].

وفي الختام يتضح أن النتيجة الإجرامية وعلاقة السببية يشكلان عنصرين أساسيين لقيام الركن المادي في جريمة النصب والاحتيال الإلكتروني، حيث لا تكتمل الجريمة إلا بوقوع ضرر فعلي ناتج مباشرة عن السلوك الاحتيالي , وإن الطبيعة التقنية لهذه الجريمة تجعل من إثبات السببية أمر معقد يتطلب تطوير وسائل التحقيق والخبرة الفنية لضمان تحقيق العدالة الجنائية في هذا المجال المتطور.[4]ا

---

[1] – نائلة قرة عادل محمد فريد ،مرجع سابق 2005، ص 73

[2] – عبد العزيز سعد، **إجراءات ممارسة الدعوى الجزائية**، دار هومة، الجزائر، 2008، ص 149

[3] – خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة، عمان، 2000، ص 95.

[4] – طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي والنظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة، 2009، ص 126

لمطلب الثالث: الركن المعنوي

من أهم الأركان التي يقوم عليها قيام المسؤولية الجزائية في جريمة النصب والاحتيال الإلكتروني، إذ لا يكفي لقيام هذه الجريمة تحقق السلوك المادي والنتيجة الإجرامية، بل يجب أن يكون ذلك السلوك صادر عن إرادة واعية واتجاه نفسي آثم لدى الجاني.

فالعنصر النفسي في هذه الجريمة يعكس مدى إدراك الجاني لطبيعة فعله غير المشروع، ورغبته في تحقيق نتيجة معينة تتمثل في الاستيلاء على مال الغير عن طريق الخداع والتدليس , وتزداد أهمية دراسة هذا الركن في الجرائم الإلكترونية لكونها جرائم تعتمد على التخطيط والدقة واستعمال وسائل تقنية متطورة، مما يجعل إثبات النية الإجرامية فيها أكثر تعقيد مقارنة بالجرائم التقليدية.

ومن هذا المنطلق يتناول هذا المطلب في فرعه الأول القصد الجنائي العام في جريمة النصب والاحتيال الإلكتروني باعتباره عنصر الإدراك والإرادة في ارتكاب الفعل، بينما يخصص الفرع الثاني لدراسة القصد الجنائي الخاص الذي يتمثل في نية التملك وتحقيق الغاية الإجرامية المتمثلة في الاستيلاء غير المشروع على أموال أو بيانات الغير.

الفرع الأول: القصد الجنائي العام في جريمة النصب والاحتيال الإلكتروني

إن القصد الجنائي العام العنصر الأساسي في الركن المعنوي لجريمة النصب والاحتيال الإلكتروني، إذ يقوم على اتجاه إرادة الجاني إلى ارتكاب الفعل الإجرامي مع علمه بكافة عناصره ونتائجه المحتملة , ويعني ذلك أن الجاني يكون مدرك لطبيعة سلوكه الاحتيالي وأنه يستخدم وسائل خداع وتدليس من شأنها التأثير على إرادة الضحية , وقد

استقر الفقه على أن القصد الجنائي العام يتكون من عنصرين أساسيين هما العلم والإرادة، وهما أساس المسؤولية الجنائية في الجرائم العمدية[1].

وفي جريمة النصب والاحتيال الإلكتروني يتمثل عنصر العلم في إدراك الجاني أن الوسائل التي يستعملها، سواء كانت رسائل إلكترونية أو مواقع مزيفة أو انتحال هوية رقمية، هي وسائل غير مشروعة تهدف إلى تضليل الضحية , أما عنصر الإرادة فيتجسد في رغبة الجاني في استعمال هذه الوسائل لتحقيق نتيجة معينة تتمثل في إيقاع الضحية في الغلط ودفعها إلى تسليم مالها أو بياناتها.[2]

ويتميز القصد الجنائي العام في هذا النوع من الجرائم بكونه قصد مباشر في أغلب الحالات، حيث يكون الجاني واعي تماما بالفعل الذي يقوم به ونتائجه المحتملة فلا مجال للخطأ أو الإهمال في هذا السياق، لأن طبيعة جريمة النصب والاحتيال الإلكتروني تقوم أساسا على التخطيط المسبق واستخدام وسائل تقنية دقيقة لتحقيق الغرض الإجرامي.[3]

و المشرع الجزائري من خلال قانون العقوبات، المعدل والمتمم بالقانون رقم 24-06 قد أكد على تجريم الأفعال الاحتيالية التي تقوم على التدليس والخداع، مما يعكس أهمية توافر القصد الجنائي في هذه الجريمة , إذ لا يمكن مساءلة الجاني إلا إذا ثبت أنه تعمد استعمال وسائل احتيالية من أجل الاستيلاء على أموال الغير.[4]

ويلاحظ أن القصد الجنائي العام في الجرائم الإلكترونية يكتسي طابعا خاصا مقارنة بالجرائم التقليدية، نظرا لاعتماد الجاني على أدوات تقنية معقدة تتطلب معرفة مسبقة بكيفية

---

[1] – أحسن بوسقيعة، **المرجع السابق** ، ص 145.

[2] – أحمد الخمليشي، **القانون الجنائي الخاص، الجزء الثاني**، مكتبة المعارف، ط2، 1986، ص 90.

[3] – أحسن بوسقيعة، **المرجع السابق**، ص 148.

[4] – **الأمر رقم 66-156** المؤرخ في 8 يونيو 1966، المتضمن **قانون العقوبات**، الجريدة الرسمية عدد 49، المعدل **بالقانون رقم 24-06** المؤرخ في 28 أبريل 2024، الجريدة الرسمية عدد 30.

استخدامها , وهذا يعزز من فكرة أن ارتكاب هذه الجريمة لا يتم بصورة عفوية بل هو نتيجة تفكير وإرادة مسبقة تهدف إلى تحقيق منفعة غير مشروعة.[1]

وقد ذهب الفقه الجنائي إلى أن القصد الجنائي العام في جريمة النصب يقوم حتى في حالة عدم تحقق النتيجة كاملة، طالما أن الجاني قد بدأ في تنفيذ السلوك الاحتيالي مع علمه بطبيعته غير المشروعة, وهذا ما يجعل مجرد الشروع في الجريمة محل مساءلة جنائية إذا توافرت عناصر القصد.[2]

إن إثبات القصد الجنائي العام في الجرائم الإلكترونية يعد من المسائل الصعبة، نظرا لاعتماد الجاني على إخفاء هويته واستعمال وسائل تقنية معقدة , لذلك يلجأ القضاء إلى الاستدلال على القصد من خلال القرائن الرقمية مثل طبيعة الرسائل، وطريقة إنشاء الحسابات وسلوك الجاني أثناء تنفيذ الجريمة.[3]

وفي الختام يمكن القول إن القصد الجنائي العام يمثل الأساس الذي تقوم عليه المسؤولية الجنائية في جريمة النصب والاحتيال الإلكتروني، حيث يعكس علم الجاني وإرادته في ارتكاب الفعل الإجرامي , وإن تطور الوسائل الإلكترونية جعل من هذا العنصر أكثر تعقيد في الإثبات و يستوجب تطوير آليات التحقيق الجنائي الرقمي لفهم النية الإجرامية بدقة أكبر.[4]

الفرع الثاني: القصد الجنائي الخاص

[1] – أحمد الخمليشي، **المرجع السابق**، ص 92.

[2] – أحسن بوسقيعة، **المرجع السابق**، ص 150

[3] – أحمد الخمليشي، **المرجع السابق**، ص 95.

[4] – أحسن بوسقيعة، **المرجع السابق**، ص 152.

القصد الجنائي الخاص في جريمة النصب والاحتيال الإلكتروني عنصر لا يكتمل الركن المعنوي بدونه، إذ يتمثل في نية الجاني الواضحة والاتجاه الإرادي نحو تحقيق غاية محددة تتمثل في الاستيلاء على مال الغير أو تحقيق منفعة غير مشروعة , ويتميز هذا القصد بكونه يتجاوز مجرد العلم بالفعل الإجرامي إلى وجود هدف نهائي يسعى الجاني إلى تحقيقه من خلال سلوكه الاحتيالي، وهو ما يميز هذه الجريمة عن غيرها من الجرائم التي قد تقوم على القصد العام فقط[1].

وتتجسد نية الاستيلاء في رغبة الجاني في نقل ملكية المال أو السيطرة عليه بطرق غير مشروعة، سواء كان ذلك عبر تحويلات مالية إلكترونية أو الحصول على بيانات مصرفية أو استغلال منصات الدفع الرقمية , ويشترط في هذا القصد أن يكون سابق أو معاصر للسلوك الإجرامي و يكون الدافع الحقيقي وراء استعمال وسائل التدليس والخداع في البيئة الإلكترونية.[2]

أما عنصر تحقيق المنفعة غير المشروعة فيعني أن الجاني لا يهدف فقط إلى الإضرار بالضحية، بل يسعى إلى تحقيق مكسب مادي أو معنوي لنفسه أو لغيره دون وجه حق , وقد أجمعت أغلب الاتجاهات الفقهية على أن هذا العنصر يمثل جوهر القصد الجنائي الخاص في جريمة النصب لأنه يعكس الغاية النهائية من السلوك الاحتيالي[3].

وفي الجرائم الإلكترونية تتخذ نية الاستيلاء أشكال متعددة و حيث قد تتمثل في سرقة الأموال مباشرة أو تحويلها إلى حسابات أخرى , أو حتى الاستيلاء على بيانات حساسة يمكن استغلالها لاحق لتحقيق مكاسب مالية , وهذا ما يجعل القصد الجنائي الخاص في هذا

[1] – أحسن بوسقيعة , **المرجع نفسه**، ص 155.

[2] – أحمد الخمليشي، **القانون الجنائي الخاص، الجزء الثاني**، مكتبة المعارف، 1986، ص 98

[3] – الحسين بن شيخ، **مذكرات في القانون الجزائي الخاص**، دار هومة، الجزائر، 2012، ص 19

النوع من الجرائم أكثر تعقيد ، لأنه يرتبط بعالم رقمي سريع التطور ومتعدد الوسائل و يؤكد الفقه الجنائي أن القصد الجنائي الخاص لا يفترض وجوده، بل يجب إثباته من خلال الوقائع والقرائن المحيطة بالجريمة، مثل طبيعة السلوك الاحتيالي وطريقة تنفيذ العملية وسلوك الجاني قبل وبعد ارتكاب الفعل , فهذه العناصر تساعد القضاء على استخلاص النية الحقيقية للجاني.[1]

و في جريمة النصب الإلكتروني يتميز بكونه قصد مباشر في الغالب، حيث يكون الجاني واعي تمام بالهدف الذي يسعى إلى تحقيقه، وهو الحصول على منفعة غير مشروعة على حساب الغير , ولا يمكن تصور هذه الجريمة في شكلها العمدي دون توفر هذا العنصر لأنه يمثل الغاية النهائية للسلوك الإجرامي.[2]

ويواجه القضاء صعوبة في إثبات القصد الجنائي الخاص في الجرائم الإلكترونية بسبب طبيعتها التقنية واعتماد الجاني على إخفاء هويته واستعمال وسائل رقمية معقدة , لذلك يتم اللجوء إلى الأدلة الرقمية مثل الرسائل الإلكترونية وسجلات الدخول والعمليات المالية الإلكترونية لاستنتاج نية الاستيلاء وتحقيق المنفعة غير المشروعة , إذ يعكس الغاية الحقيقية للجاني المتمثلة في الاستيلاء على أموال الغير وتحقيق منفعة غير مشروعة , و إثبات هذا العنصر يعد من أهم التحديات في الجرائم الإلكترونية.[3]

ملخص الفصل الأول

[1] – نائلة عادل محمد فريد قورة ، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي، 2005، ص 41

[2] – طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي والنظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة، مصر،2009، ص 129

[3] – خالد عباد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة، عمان، 2000، ص 30

يتناول الفصل الأول الإطار العام لجريمة النصب والاحتيال الإلكتروني من خلال دراسة مفهومها وأركانها الأساسية، حيث يهدف إلى الإحاطة بهذه الجريمة من الناحيتين النظرية والقانونية , فقد خصص المبحث الأول لبيان مفهوم جريمة النصب والاحتيال الإلكتروني، من خلال تعريفها وتحديد أنواعها المختلفة التي تتنوع بتنوع الوسائل والأساليب المستعملة في ارتكابها، سواء عبر الوسائط التقليدية الحديثة أو عبر الفضاء الرقمي.

أما المبحث الثاني فقد تناول أركان هذه الجريمة، والمتمثلة في الركن الشرعي الذي يقوم على مبدأ الشرعية الجنائية ونطاق التجريم والعقاب، والركن المادي الذي يشمل السلوك الإجرامي والنتيجة الإجرامية وعلاقة السببية، ثم الركن المعنوي الذي يعكس القصد الجنائي العام والخاص.

وتكمن أهمية هذا الفصل في كونه يمهد لفهم الطبيعة القانونية للجريمة الإلكترونية وتمييزها عن غيرها من الجرائم التقليدية.

الفصل الثاني :

آليات الردع و الوقاية من جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

المبحث الأول: الأحكام الإجرائية لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

المبحث الثاني: وسائل الوقاية من جريمة النصب والاحتيال الإلكتروني .

تُعدّ جريمة النصب والاحتيال الإلكتروني من أبرز الجرائم الالكترونية انتشارًا، نظرًا لما توفّره الشبكة العنكبوتية من إمكانياتٍ واسعةٍ للجاني، تتيح له إخفاء هويته، والوصول إلى أعدادٍ كبيرةٍ من الضحايا في وقتٍ قصير، واستغلال ضعف الوعي الرقمي والثغرات التقنية لتحقيق مكاسب غير مشروعة بأقلّ جهدٍ ممكن.

وأمام هذه الإشكاليات، سعى المشرّع الجزائري إلى مواكبة التطوّر الحاصل، من خلال تبنّي منظومةٍ قانونيةٍ متكاملةٍ تجمع بين البُعد العقابي والبُعد الإجرائي والبُعد الوقائي. فمن جهة، تمّ تكييف الأفعال المرتكَبة في الفضاء الرقمي ضمن النصوص العقابية المنظِّمة لجريمة النصب التقليدية مع إضافة نصوصٍ خاصةٍ تتعلق بالاعتداء على أنظمة المعالجة الآلية للمعطيات. ومن جهةٍ أخرى، تمّ تحديث قانون الإجراءات الجزائية بإدخال تقنياتٍ حديثةٍ للتحري وجمع الأدلة الرقمية. كما لم يُهمل المشرّع البُعدَ الوقائي، فأرسى آلياتٍ تقنيةً وإداريةً وقانونيةً تهدف إلى الحدّ من انتشار هذه الجريمة قبل وقوعها.

وبناءً على ما تقدّم، فإنّ دراسة هذا الفصل تكتسي أهميةً بالغة، إذ تجمع بين تحليل النصوص القانونية المنظِّمة للمتابعة الجزائية والعقوبات المقرّرة من جهة، واستعراض الوسائل التقنية والإدارية والقانونية للوقاية من جهةٍ أخرى. وسنتناول ذلك من خلال مبحثَين: نخصّص الأول للأحكام الإجرائية لمتابعة جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري، ونتناول في الثاني وسائل الوقاية من هذه الجريمة.

المبحث الأول: الأحكام الإجرائية لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

تُعدّ الأحكام الإجرائية في جريمة النصب والاحتيال الإلكتروني الإطارَ العملي الذي تترجم من خلاله النصوص الموضوعية إلى تطبيقٍ فعلي أمام جهات التحري والتحقيق والحكم. فالقواعد الإجرائية هي التي تَكفل ملاحقة الجاني، وضمان حقوق الضحية، وتحقيق التوازن بين فعالية الردع وحماية الحريات الفردية.

وقد فرضت الطبيعة المستحدثة لهذه الجريمة، التي تتم في فضاء افتراضي عابرا للحدود، تحديات جسيمة على المنظومة الاجرائية التقليدية والقواعد الكلاسيكية للاختصاص ولوسائل التحري، ولإثبات الجريمة لم تعد قادرة وحدها على استيعاب خصوصيات الاجرام الرقمي، لذا نجد المشرع الجزائري نظم جملة من النصوص أبرزها القانون رقم **09-04** المؤرّخ في 5 أوت 2009، **المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**[1]، فضلًا عن التعديلات التي أُدخلت على قانون الإجراءات الجزائية بموجب القانون رقم **06-22**، والمتعلقة بأساليب التحرّي الخاصة كاعتراض المراسلات والتسرّب.

ولأجل تناول هذا المبحث بشكلٍ متكامل، خصص المطلب الأول لدراسة المتابعة الجزائية لهذه الجريمة، ، فيما تناول المطلب الثاني العقوبات المقرّرة لها، أصلية كانت أم تكميلية.

المطلب الأول: المتابعة الجزائية لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

تُعدّ المتابعة الجزائية لجريمة النصب والاحتيال الإلكتروني إحدى أهمّ الآليات القانونية التي اعتمدها المشرّع الجزائري لمواجهة هذا النوع من الجرائم المستحدثة، التي أصبحت تُرتكب عبر الوسائط الرقمية وشبكات الاتصال.

[1]- **القانون رقم 09-04 المؤرّخ في 5 أوت 2009**، المتضمّن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، الجريدة الرسمية للجمهورية الجزائرية، العدد 47 الصادر بتاريخ 16 أوت 2009.

ونظرًا لغياب نصّ خاصّ يُعرّف الجريمة الإلكترونية بشكلٍ مستقل، فقد تمّ تكييف جريمة النصب الإلكتروني ضمن أحكام المواد من 372 إلى 379 من قانون العقوبات الجزائري، مع الاستناد إلى القواعد العامة في قانون الإجراءات الجزائية[1]، إلى جانب الأحكام الخاصة الواردة في القانون رقم 09-04 المتعلّق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وتتمثّل المتابعة الجزائية في مجموعة الإجراءات التي تباشرها السلطات المختصّة، بدءًا من تحريك الدعوى العمومية، مرورًا بالتحقيق وجمع الأدلة، وصولًا إلى المحاكمة وإصدار الحكم، وذلك بهدف حماية الأموال العامة والخاصة وردع مرتكبي هذه الجرائم.

الفرع الأول: الأساس القانوني وإجراءات تحريك الدعوى العمومية في جريمة النصب والاحتيال الإلكتروني

تُعدّ مرحلة تحريك الدعوى العمومية الحلقةَ المفصلية في المسار الإجرائي الجزائي، إذ تُمثّل نقطة الانتقال بمقتضاها الجريمةُ من حيّز الواقعة المادية المُجرَّدة إلى حيّز المتابعة الجزائية الرسمية المُنتجة لآثارها القانونية.

وتكتسي هذه المرحلة في جريمة النصب والاحتيال الإلكتروني أهميةً مضاعفة بحكم الطبيعة التقنية والمعقّدة لهذه الجريمة الجزائية، التي تجعل من عنصر السرعة في المبادرة بالإجراءات شرطًا جوهريًا لإنجاح المتابعة وضمان حفظ الأدلة الرقمية قبل اندثارها أو تعرّضها للعبث[2].

أولًا: الأساس القانوني لتحريك الدعوى العمومية

يستند تحريك الدعوى العمومية في جريمة النصب والاحتيال الإلكتروني إلى منظومةٍ قانونيةٍ متكاملةٍ يتقاطع فيها التشريع الموضوعي مع التشريع الإجرائي. فعلى الصعيد

[1]–أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص**،_الجزء الثاني، دار هومة، الجزائر، الطبعة الأخيرة، ص 130

[2]–عبد الفتاح بيومي حجازي، **الجرائم المعلوماتية في التشريع المقارن**، دار الفكر الجامعي، الإسكندرية، 2008، ص 185.

الموضوعي، تُشكّل المادة 372 من قانون العقوبات الجزائري المرجعَ الأساسي للتجريم، إذ تُعاقب كلَّ من توصّل إلى تسلُّم أموال الغير أو منقولاتهم أو سندات تتضمّن تصرّفًا في الأموال باستعمال طرقٍ احتيالية تَخدع الضحية وتدفعها إلى التسليم بإرادتها المعيبة[1].

وتُكمَّل هذه المادة بأحكام المواد 394 مكرر وما بعدها من القانون نفسه، التي أُدرجت بموجب القانون رقم 04-15 المؤرّخ في 10 نوفمبر 2004 المعدّل والمتمّم لقانون العقوبات، والتي جرّمت الاعتداء على أنظمة المعالجة الآلية للمعطيات، فيكون النصب الإلكتروني في حالة الاقتران بفعل اختراق أو تلاعب بالنظام المعلوماتي خاضعًا لتكييفٍ مُركّب يجمع بين التجريمَين.

أمّا على الصعيد الإجرائي، فقد كرّس الأمر رقم 66-155 المتضمّن قانون الإجراءات الجزائية مبدأَ احتكار النيابة العامة لسلطة تحريك الدعوى العمومية ومباشرتها باعتبارها الجهة الممثّلة للمجتمع وحامية النظام العام[2].

وتُمارَس هذه السلطة عمليًا من قِبَل وكيل الجمهورية لدى المحكمة المختصّة إقليميًا، وفقًا لأحكام المادتَين 29 و36 من القانون المذكور. وتتعزّز هذه الأحكام العامة بنصوصٍ خاصة وردت في القانون رقم 09-04 المؤرّخ في 5 أوت 2009 المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3]، الذي أرسى أساليبَ تحرٍّ مستحدثةً تتلاءم مع خصوصية البيئة الرقمية، كاعتراض المراسلات الإلكترونية وتفتيش الأنظمة المعلوماتية.

ثانيًا: مصادر تحريك الدعوى العمومية

---

[1]-**الأمر رقم 66-156** المؤرّخ في 8 يونيو 1966 المتضمّن **قانون العقوبات**، المعدّل والمتمّم، **المادة 372**.

[2]-**الأمر رقم 66-155** المؤرّخ في 8 يونيو 1966 المتضمّن **قانون الإجراءات الجزائية**، المعدّل والمتمّم، **المادتان 29 و36**.

[3]-**القانون رقم 09-04** المؤرّخ في 5 أوت 2009 المتضمّن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

لا يستلزم تحريك الدعوى العمومية في جريمة النصب الإلكتروني توافرَ شكوى مسبقة من المجني عليه، إذ تُصنَّف ضمن جرائم الحق العام التي تتولّى النيابة العامة تحريكها تلقائيًا متى توافرت لديها قرائنُ كافية على وقوعها. غير أنّ مصادر العلم بالجريمة تتعدّد وتتنوّع، ويمكن إجمالها فيما يلي:

1. **شكوى الضحية المتضرّرة:**

تُعدّ المصدرَ الأكثر شيوعًا في الجرائم الماسّة بالذمّة المالية، إذ يَتقدّم المجني عليه بشكواه أمام النيابة العامة أو ضباط الشرطة القضائية، مُرفقةً بكلّ ما يتوفّر لديه من قرائن وأدلة رقمية، كرسائل البريد الإلكتروني المُستلمة من الجاني، ولقطات شاشةٍ للمحادثات والمواقع المُزيَّفة، وكشوف الحسابات البنكية المُثبتة للتحويلات المشبوهة، وأرقام الهواتف وحسابات التواصل الاجتماعي المُستعمَلة في الإيقاع به[1].

2. **البلاغ الصادر عن مصالح الضبطية القضائية:**

ويتجسّد ذلك حين تَعلم هذه المصالح بوقوع الجريمة عن طريق التحرّيات الميدانية أو الاستخبارية، أو بناءً على معلوماتٍ ترِدها من المصالح المتخصّصة في مكافحة الجريمة الإلكترونية، أو من المؤسّسات المالية التي ترصد عبر أنظمتها الذكية عملياتٍ مشبوهةً ذات نمطٍ احتياليٍّ متكرّر، كالتحويلات المتزامنة لمبالغ صغيرة من حسابات متعدّدة إلى وجهةٍ واحدة[2].

3. **الإخطار من الهيئات المتخصّصة:**

وفي مقدّمتها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المُنشَأة بموجب المرسوم الرئاسي رقم 15-261 المؤرّخ في 8 أكتوبر 2015[3]، والتي تختصّ برصد الجرائم المعلوماتية وجمع الأدلّة الرقمية وتنسيق

---

[1]– عبد رحمان خلفي، **الإجراءات الجزائية**،، الطبعة الثامنة، دار بلقيس الجزائر ،2025ص180

[2]– خوري عمر، "**سلطات الشرطة القضائية في مواجهة الجريمة المتلبس بها**" ،المجلة الجزائرية العلوم القانونية والسياسية، المجلد 51 رقم 3ص28

[3]–**المرسوم الرئاسي رقم 15-261** المؤرّخ في 8 أكتوبر 2015 المتضمّن **إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وسيرها**، الجريدة الرسمية، العدد 54.

التعاون الدولي مع نظيراتها الأجنبية. وتُحيل هذه الهيئة المعلوماتِ التي تَتلقّاها إلى النيابة العامة لاتخاذ الإجراءات القانونية المناسبة.

4. الاكتشاف العَرَضي للجريمة:

قد تُكشف جريمة النصب الإلكتروني بمناسبة التحقيق في جريمةٍ أخرى مرتبطة بها، كجريمة تبييض الأموال أو تمويل الإرهاب أو الاتجار في المؤثرات العقلية عبر الإنترنت، حيث تُسفر عمليات تتبّع التدفّقات المالية أو تحليل الأجهزة المحجوزة في إطار قضيةٍ معيّنة عن وقائع نصبٍ إلكتروني سابقة لم تُكشف بعد[1].

5. الإخطار التلقائي من مقدّمي الخدمات:

فرضت المادة 10 من القانون 09-04 على مقدّمي خدمات الإنترنت ومتعهّدي الاتصالات التزامًا قانونيًا بتبليغ السلطات المختصّة فورًا بكلّ ما يَصل إلى علمهم من معلوماتٍ تتعلّق بأفعالٍ يُحتمل أن تُشكّل جرائمَ معلوماتية، تحت طائلة المسؤولية الجزائية والمدنية[2]. ويُعدّ هذا الالتزام أحدَ أهم آليات الكشف المبكّر عن الجرائم الإلكترونية[3].

ثالثًا: الإجراءات العملية لتحريك الدعوى العمومية

تَمرّ عملية تحريك الدعوى العمومية في جريمة النصب والاحتيال الإلكتروني بسلسلةٍ من الإجراءات المتعاقبة التي تستلزم دقّةً قانونية وكفاءةً تقنية عالية، نظرًا لخصوصية الدليل الرقمي وقابليته السريعة للتغيّر أو الإتلاف[3]. ويمكن استعراض هذه الإجراءات في المراحل التالية:

1. مرحلة تلقّي الشكوى أو البلاغ وتحرير المحضر:

تتلقّى النيابة العامة أو ضباط الشرطة القضائية الشكوى أو البلاغ، ويُحرَّر بشأنها محضرٌ رسميٌّ يتضمّن البيانات الكاملة للمشتكي، وعرضًا تفصيليًا للوقائع، مع تحديد الوسيلة الإلكترونية المُستعملة (موقع إلكتروني، بريد إلكتروني، تطبيق

---

[1]–أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص**، الجزء الثاني، دار هومة، الجزائر، الطبعة 19،2021، ص 130.

[2]–**القانون رقم 09-04**، المرجع السابق، **المادة 10**.

[3]–عبد الله أوهايبية، **شرح قانون الإجراءات الجزائية، الجزء الأول**، الطبعة الثانية، دار هومة، الجزائر 2018 ،ص71

محادثة، منصة تواصل اجتماعي)، والتاريخ والساعة الدقيقَين لارتكاب الفعل، وقيمة الضرر المالي، وأرقام الحسابات والمحافظ الإلكترونية المُستهدَفة. وتُرفق بالمحضر كافّةُ المستندات الرقمية المتاحة لدى الضحية، مع الحرص على حفظها بأكثر من نسخةٍ احتياطية.

2. **مرحلة التحرّيات الأولية:**

يتولّى ضباط الشرطة القضائية، ولا سيما المنتمون إلى المصلحة المركزية لمكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال التابعة للمديرية العامة للأمن الوطني، إجراء التحرّيات الأولية. وتشمل هذه التحرّيات تحديدَ عنوان بروتوكول الإنترنت (IP) المُستعمَل في ارتكاب الجريمة، والتنسيق مع مزوّد الخدمة المعني للحصول على بيانات المُشترك، والاستفسار من المؤسسات البنكية ومُتعهّدي خدمات الدفع الإلكتروني حول وجهات التحويلات وأصحاب الحسابات المُتلقّية، فضلًا عن استخدام أدوات التحليل الرقمي لرسم خريطةٍ شاملة للنشاط الإجرامي[1].

3. **مرحلة جمع الأدلّة الرقمية وتأمينها:**

تُعدّ هذه المرحلة من أدقّ مراحل التحرّي وأشدّها حساسية، إذ تستوجب احترام بروتوكولاتٍ علميةٍ صارمة في حجز الأجهزة وتحليلها، حفاظًا على سلامة الدليل وقابليته للاحتجاج به أمام القضاء. وقد سمح المشرّع الجزائري للضبطية القضائية، بموجب المادتَين 5 و6 من القانون 09-04[2]، باللجوء إلى أساليب التحرّي الخاصة كالمراقبة الإلكترونية للاتّصالات وتفتيش الأنظمة المعلوماتية وحجز المعطيات، شريطة الحصول على إذنٍ مسبقٍ مكتوب من وكيل الجمهورية أو قاضي التحقيق المختصّ[3].

---

[1]– امال قارة، **الحماية الجزائية المعلوماتية في التشريع الجزائري** ، دار هومة ،الجزائر، 2006 ،ص42.

[2]–**القانون رقم 09-04**، المرجع السابق، **المادتان 5 و6.**

[3]–عبد الله اوهايبية ، **المرجع السابق** ،ص181

كما يُلزَم المحقّقون باتّباع تقنيات «التحليل الجنائي الرقمي» (Digital Forensics) التي تضمن سلسلة الحيازة (Chain of Custody) وعدم العبث بالدليل، وذلك بإنشاء نسخةٍ مطابقة (Bit–by–bit Image) من القرص الصلب قبل أيّ فحص [1].

4. مرحلة عرض الملف على وكيل الجمهورية:

بعد استكمال التحرّيات الأولية، يُحال الملف على وكيل الجمهورية المختصّ إقليميًّا، الذي يتمتّع بسلطةٍ تقديريةٍ واسعةٍ في تكييف الوقائع وتقدير مدى كفاية الأدلّة.فإمّا أن يَأمر بحفظ الملف لانعدام الأدلة الكافية أو لعدم قابلية الواقعة للمتابعة قانونًا، أو يُحرّك الدعوى العمومية مباشرةً عن طريق التكليف المباشر بالحضور أمام محكمة الجنح، أو يَطلب فتحَ تحقيقٍ قضائي متى كانت الوقائع تكتسي طابعًا جنائيًا أو تستلزم تحقيقًا مُعمَّقًا لكشف ملابساتها وتحديد جميع المتورّطين فيها[2].

5. مرحلة التحقيق القضائي:

يَفتح قاضي التحقيق التحقيقَ القضائي ويُباشر إجراءاتٍ خاصةً تتلاءم مع طبيعة الجريمة الإلكترونية، فيُصدر أوامرَ بالضبط والإحضار الوطني والدولي عبر النشرات الحمراء للمنظمة الدولية للشرطة الجنائية (الإنتربول)، ويَستعين بخبراء معتمدين في المعلوماتية لإجراء الخبرة التقنية على الأجهزة المحجوزة وتحليل المراسلات المُعترَضة، ويُوجّه إنابات قضائيةً دوليةً إلى الدول التي يُحتمل تواجد الجاني أو الخوادم بها، وذلك في إطار الاتفاقيات الثنائية والمتعدّدة الأطراف للتعاون القضائي الدولي[3]. كما يَأمر بالاستماع إلى الضحايا والشهود، ويُجري المواجهات بينهم وبين المتّهمين عند الاقتضاء[4].

6. مرحلة الإحالة على جهة الحكم:

---

[1]–عبد العزيز سعد، **الجرائم الواقعة على أنظمة المعالجة الالية للمعطيات**، دار هومة ،الجزائر ،2019، ص،131

[2]–عبد الله اوهايبية ، **المرجع السابق** ،ص98.

[3]–عبد الفتاح بيومي حجازي، **المرجع السابق**، ص 193.

[4]–عبد العزيز سعد، **المرجع نفسه**، ص132،

متى توافرت الأدلة الكافية على ارتكاب المتّهم للجريمة المنسوبة إليه، يُصدر قاضي التحقيق أمرًا بإحالته على الجهة القضائية المختصّة (محكمة الجنح أو محكمة الجنايات بحسب التكييف القانوني)، التي تَفصل في الدعوى وفقًا للقواعد العامة للإجراءات الجزائية، مع مراعاة خصوصية الدليل الرقمي في مرحلتَي الإثبات والمناقشة، وحقّ الدفاع في الاستعانة بخبراء تقنيين لمناقشة الخبرة المنجزة.

رابعًا: الضمانات الإجرائية أثناء تحريك الدعوى

حرص المشرّع الجزائري، رغم خصوصية الجريمة الإلكترونية ودواعي السرعة في التحرّي، على إحاطة إجراءات تحريك الدعوى بجملةٍ من الضمانات التي تكفل احترام الحقوق والحرّيات الفردية، تجنّبًا لأيّ تعسّف في استعمال الصلاحيات الواسعة المُخوَّلة للضبطية القضائية وقضاة التحقيق[1].

وتتجلّى أبرز هذه الضمانات في اشتراط الحصول على إذنٍ قضائيٍّ مُسبَّقٍ ومكتوبٍ قبل اللجوء إلى أساليب التحرّي الخاصة، وتحديد مدّة المراقبة الإلكترونية بأربعة (4) أشهر قابلة للتجديد ضمن الشروط المنصوص عليها في المادة 4 من القانون 09-04[2]، وقد قيد اللجوء الى هذه الأساليب بحالات الجرائم الماسة بامن الدولة وبعض الجرائم الالكترونية المحددة قانونا على سبيل الحصر، مع ضرورة اخطار الشخص المعني بالإجراءات المتخذة في حقه فور اتاحة ذلك، ضمانا لاحترام مبدأ الوجهية وصونا لحقوق الدفاع.

كما تظلّ القواعد العامة لقانون الإجراءات الجزائية واجبةَ التطبيق، ولا سيما ما يتعلق بحقوق الموقوف للنظر، وحقّه في الاستعانة بمحامٍ منذ بدء الإجراءات، وعرضه على الطبيب عند الاقتضاء، وإعلام عائلته بمكان تواجده، وذلك تجسيدًا للموازنة الدقيقة بين فعالية الردع الجنائي وصون الحقوق الأساسية للإنسان.

الفرع الثاني: الاختصاص في جريمة النصب والاحتيال الإلكتروني

[1] – أحسن بوسقيعة، **المرجع السابق**، ص 150 –151.

[2] –**القانون رقم04–09** المؤرخ في 5اوت2009.

يُحدَّد الاختصاص القضائي في جريمة النصب الإلكتروني في الأصل وفق القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية الجزائري، ولا سيّما المادة 37 التي تُقرّر أنّ الاختصاص ينعقد للجهة القضائية التي وقع في دائرة اختصاصها الجريمة، أو التي يقيم فيها المتّهم، أو التي تمّ القبض عليه فيها[3]. ويُعدّ هذا المبدأ من القواعد الأساسية في التنظيم القضائي، إذ يهدف إلى تحقيق التوازن بين سهولة ملاحقة الجاني وضمان حسن سير العدالة.

غير أنّ تطبيق هذا المبدأ التقليدي يواجه صعوباتٍ كبيرةً عند تعلّق الأمر بالجرائم الإلكترونية، وعلى رأسها جريمة النصب الإلكتروني، وذلك بسبب الطبيعة الخاصة لهذا النوع من الجرائم التي لا ترتبط بمكانٍ ماديٍّ واحد، بل تتمّ في فضاءٍ رقميٍّ عابرٍ للحدود. فالفعل الإجرامي قد يبدأ في دولةٍ معيّنة، بينما تتحقّق النتيجة في دولةٍ أخرى، وقد تمرّ البيانات عبر عدّة دولٍ وأنظمةٍ معلوماتيةٍ مختلفة، ممّا يجعل تحديد مكان ارتكاب الجريمة أمرًا معقّدًا وغير ثابت [1].

وانطلاقًا من هذه الخصوصية، أصبح مفهوم الاختصاص القضائي في الجرائم الإلكترونية أكثرَ مرونةً واتساعًا، حيث لم يعد يقتصر فقط على مكان ارتكاب الفعل المادي، بل أصبح يشمل عدّة معايير بديلة تهدف إلى تسهيل المتابعة الجزائية وضمان عدم إفلات الجناة من العقاب [2].

فمن بين أهمّ المعايير: مكان وقوع النتيجة الإجرامية، أي المكان الذي تحقّق فيه الضرر المالي للضحية. ففي جريمة النصب الإلكتروني، قد يقوم الجاني بتنفيذ فعل الاحتيال من مكانٍ بعيد، بينما يتمّ سحب الأموال أو تحويلها من حساب الضحية في دولةٍ أو منطقةٍ أخرى. وفي هذه الحالة، يُعتبر مكان تحقّق الضرر المالي أحدَ أهمّ معايير تحديد الاختصاص القضائي، باعتباره المكان الذي ظهرت فيه آثار الجريمة بشكلٍ فعلي [3].

---

[1] – شهيرة بولحية و دنيا زاد سويح،"_**الاحتيال الالكتروني" مجلة الدراسات القانونية والاقتصادية** ،المركز الجامعي بريكة، المجلد 2،العدد2 ، 2019 ص ص37–38

[2] – عبدالقادر عدو، **المبادئ العامة في قانون الإجراءات الجزائية الجزائري**، دار هومة الجزائر،2018،ص180.

[3] – فضيلة عاقلي،**الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، كتاب اعمال مؤتمر الجرائم الالكترونية المنعقد في طرابلس ،لبنان ، يومي 24–2017/03/25 ص215.

ومن جهةٍ أخرى، يمكن أن يمتدّ الاختصاص أيضًا إلى مكان تواجد الخوادم أو الأنظمة المعلوماتية المستخدمة في تنفيذ الجريمة، حيث تعتمد العديد من عمليات النصب الإلكتروني على مواقع إلكترونيةٍ أو خوادم رقميةٍ يتمّ عبرها تمرير البيانات وتخزينها ومعالجتها[2] وفي هذه الحالة، فإنّ مكان وجود هذه الخوادم قد يُعتمد كعنصرٍ مكمّلٍ لتحديد الاختصاص القضائي، خاصةً في الحالات التي يصعب فيها تحديد مكان الجاني أو الضحية بدقّة [1]

ويُلاحَظ أنّ هذا التعدّد في معايير الاختصاص يعكس محاولة المشرّع والفقه القضائي التكيّفَ مع الطبيعة المعقّدة للجرائم الإلكترونية، التي لا تخضع للحدود الجغرافية التقليدية، بل تتجاوزها عبر الشبكات الرقمية المفتوحة. وقد أقرّ المشرّع الجزائري في المادة 15 من القانون 09-04 صلاحيةَ الجهات القضائية الجزائرية بالنظر في الجرائم الإلكترونية المرتكبة خارج التراب الوطني متى كانت تستهدف مؤسساتٍ جزائريةً أو مواطنين جزائريين [2].

كما أنّ هذا التوسّع في الاختصاص القضائي يهدف بالأساس إلى ضمان فعّالية المتابعة الجزائية، من خلال تفادي حالات الإفلات من العقاب التي قد تنشأ نتيجة صعوبة تحديد المكان الدقيق للجريمة. فلو تمّ التمسّك الصارم بالمعايير التقليدية فقط، لأصبح من السهل على مرتكبي جرائم النصب الإلكتروني استغلالُ الطبيعة العابرة للحدود للتهرّب من الملاحقة القضائية، وهو ما يتعارض مع أهداف العدالة الجنائية [3].

الفرع الثالث: وسائل الإثبات في جريمة النصب الإلكتروني وصعوباته

تُعدّ مرحلة الإثبات في جريمة النصب الإلكتروني المرحلةَ الفاصلةَ في المسار الإجرائي، بل يمكن اعتبارها العنصرَ الحاسمَ في نجاح أو فشل الدعوى العمومية، فمهما كانت الجريمة واضحةً في وقوعها، فإنّ عدم القدرة على إثباتها بدليلٍ يقيني يُفضي حتمًا إلى البراءة احترامًا لقرينة الأصل في الإنسان البراءة.

---

[1] – عبد القادر عدو، **المرجع السابق** ،ص200.

[2] – **المادة 15 من القانون09-04**.

[3]– العايب سامية وعرابة منال، "**الحماية الجزائية للمستهلك من جريمة النصب الالكتروني**" مجلة هيرودوت للعلوم الإنسانية والاجتماعية ،المجلد 5،العدد 3، 2021،ص229

ونظرًا لما تتسم به الأدلّة الرقمية من خصائص فريدة، فقد فرضت هذه الجريمة على المشرّع والقاضي على حدٍّ سواء إعادة النظر في كثيرٍ من المسلَّمات التقليدية في نظرية الإثبات الجزائي.

أولًا: الإطار القانوني لوسائل الإثبات :

أدرك المشرّع الجزائري خصوصية الدليل الرقمي، فسمح باستخدام وسائلَ تقنيةٍ حديثةٍ في جمع الأدلة وإثبات الجرائم، وذلك من خلال ما نصّت عليه المواد 65 مكرّر 12 وما بعدها من قانون الإجراءات الجزائية[1]والتي تُجيز للسلطات القضائية والأمنية اللجوءَ إلى وسائل خاصة في التحرّي، من بينها اعتراض المراسلات الإلكترونية، وتسجيل المكالمات الهاتفية، والمراقبة التقنية للوسائط الرقمية، وذلك وفق ضوابط قانونية تهدف إلى تحقيق التوازن بين فعالية التحقيق واحترام الحقوق والحريات الفردية[2].

ويُكمَّل هذا الإطار بأحكام القانون 09-04 الذي خصّ الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقواعد إجرائية مرنة، تتيح حفظ المعطيات المخزَّنة لدى مزوّدي الخدمات لمدة سنة كاملة، وإلزامهم بتقديمها للسلطات المختصّة عند الطلب، بما يُسهّل عمليةَ تتبّع المسار الرقمي للجريمة.

ثانيًا: أنواع الأدلّة الرقمية المعتمَدة

تتنوّع الأدلّة الرقمية المعتمَدة في إثبات جريمة النصب الإلكتروني، ويمكن تصنيفها في طوائف عدّة:

1. اعتراض المراسلات الإلكترونية:

حيث يسمح للجهات المختصّة بالاطلاع على الرسائل المتبادلة بين الجاني والضحية أو بين الجناة أنفسهم، سواء عبر البريد الإلكتروني أو تطبيقات التواصل

[1] – **الأمر 66-155** المتضمّن **قانون الإجراءات الجزائية**، المعدّل والمتمّم **بالقانون 06-22**، المواد 65 مكرّر 12.

[2]– عبد القادر عدو، مرجع سابق ، ص202

الاجتماعي. وتكتسي هذه الوسيلة أهميةً كبيرةً لأنها قد تكشف عن نية الجاني، وخطّة تنفيذ الجريمة، والأساليب الاحتيالية المستعملة في الإيقاع بالضحايا [1].

2. تسجيل المكالمات والاتصالات الهاتفية:

ويُعدّ وسيلةً فعّالةً في كشف الجرائم الإلكترونية، خاصةً تلك التي يتمّ فيها استدراج الضحايا أو تقديم وعودٍ وهميةٍ عبر الهاتف. إذ يمكن من خلال هذه التسجيلات إثباتُ وجود علاقةٍ مباشرةٍ بين الجاني والضحية، وتحديد أسلوب الاحتيال المستخدم [2].

3. المراقبة التقنية للوسائط الرقمية:

وتُعدّ من أكثر الوسائل تطوّرًا، حيث تشمل تتبّعَ الأنشطة الإلكترونية للجاني، وتحليل حركة البيانات، ومراقبة الحسابات الإلكترونية والمواقع المستعمَلة في تنفيذ الجريمة[3].

4. البيانات البنكية والتحويلات المالية الإلكترونية:

وتُعتبر من أقوى الأدلة في هذا النوع من الجرائم، لأنها تُظهر حركة الأموال وتحدّد مصدرها وجهتها، ممّا يساعد على تتبّع الأموال المستولى عليها وربطها بالجاني[4]

5. عناوين بروتوكول الإنترنت (IP) وسجلّات الاتصال (Logs):

حيث يُستخدم هذا العنوان لتحديد الجهاز أو الشبكة التي تمّ من خلالها تنفيذ الفعل الإجرامي. وعلى الرغم من إمكانية إخفاء أو تغيير هذا العنوان عبر وسائل

---

[1]– اشرف قنديل عبد القادر، **الاثبات الجنائي في الجريمة الالكترونية** ، دار الجامعة الجديدة، الإسكندرية ، 2015،ص123

[2]– محمد الأمين البشري ، **التحقيق في الجرائم المستحدثة** ،الطبعة 1، اكاديمية نايف العربية للعلوم الأمنية ، السعودية ،2004ص23

[3]– نبيلة هبة هروال، **الوانب الإجرائية لجرائم الانترنت**، في مجلة جمع الاستدلالات، دراسة مقارنة دار الفكر الجامعي، الإسكندرية ،2013، ص 273

[4] – شايب محمد،" **اليات الحماية من الغش في وسائل الدفع الالكتروني**"، مجلة نماء للاقتصاد والتجارة ،جامعة جيجل، المجلد1،العدد2، 2017، ص8

تقنية، إلا أنه يظلّ عنصرًا مهمًّا في عملية التحقيق الرقمي، خاصةً عند دمجه مع باقي الأدلة التقنية الأخرى[1].

6. الأدلة المستخرجة من الأجهزة الإلكترونية:

مثل الحواسيب والهواتف الذكية والأجهزة اللوحية، حيث يمكن من خلال تحليل هذه الأجهزة الوصولُ إلى ملفّاتٍ ومحادثاتٍ وصورٍ أو تطبيقاتٍ تُثبت علاقة الجاني بالجريمة، شريطة احترام إجراءات الحجز والخبرة القضائية لضمان سلامة الدليل[2].

ثالثًا: صعوبات الإثبات في جريمة النصب الإلكتروني

على الرغم من تعدّد وسائل الإثبات وتطوّرها، فإنّ إثبات جريمة النصب الإلكتروني يصطدم بجملةٍ من الصعوبات النوعية التي تنفرد بها هذه الجريمة عن سائر الجرائم التقليدية. وتتوزّع هذه الصعوبات على ثلاثة مستويات: تقني، وقانوني، وقضائي.

1. الصعوبات ذات الطابع التقني :

تنبثق هذه الصعوبات أساسًا من الطبيعة غير المادية للدليل الرقمي. فالدليل الرقمي ليس له وجود فيزيائي ملموس، بل هو عبارة عن نبضاتٍ كهربائيةٍ ومعطياتٍ ثنائيةٍ مخزّنةٍ على وسائط إلكترونية، يمكن نسخها أو حذفها أو تعديلها في ثوانٍ معدودة دون أن يترك ذلك أثرًا ظاهرًا. وهذا ما يجعل سلامته الفعلية موضعَ شكٍّ دائمٍ ما لم تُتّبع بروتوكولات صارمة في الجمع والحفظ والتحليل.[3]

ومن أبرز هذه الصعوبات أيضًا: استخدام تقنيات إخفاء الهوية كالشبكات الافتراضية الخاصة (VPN) وشبكة (TOR) وعناوين IP المتغيّرة، فضلًا عن انتشار العملات المشفّرة (Cryptocurrencies) كالبيتكوين، التي تُتيح إجراءَ معاملاتٍ ماليةٍ مجهولةِ الهوية يصعب

---

[1] – عائشة بن قارة مصطفى، **حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن** دار الجامعة الجديدة 2010،ص31

[2] – أحسن بوسقيعة ، **المرجع السابق**،ص ص150–151.

[3] – عبد الفتاح بيومي حجازي، **الدليل الرقمي وحجيته في الإثبات الجنائي**، دار الفكر الجامعي، الإسكندرية، 2019، ص 112–118.

تتبّعها بالأساليب التقليدية. كما أنّ كثيرًا من الجناة يلجؤون إلى تشفير محتويات أجهزتهم بكلمات مرور قويّة، ممّا يُعطّل عملية الخبرة التقنية ولو تمّ حجز الجهاز ماديًّا[1].

ويُضاف إلى ذلك سرعةُ تَلاشي بعض الأدلة الرقمية، كملفّات السجلّات (Logs) التي تُحذف تلقائيًّا بعد فتراتٍ قصيرة، أو رسائل التطبيقات المشفّرة كـ«تيليغرام» و«سيغنال» التي تتضمّن خاصية الحذف الذاتي، ممّا يستوجب سرعةً قصوى في التدخّل قد لا تتلاءم مع البطء الإجرائي المعتاد[2].

2. الصعوبات ذات الطابع القانوني :

تتعلّق هذه الصعوبات بمدى حجّية الدليل الرقمي أمام القضاء، وبكيفية التوفيق بين فعّالية التحرّي وحماية الحقوق الأساسية للمتّهم. فالأصل في القانون الجزائي الجزائري هو حرية الإثبات وفقًا لنصّ المادة 212 من قانون الإجراءات الجزائية، إلا أنّ تطبيق هذا المبدأ على الدليل الرقمي يَطرح إشكالياتٍ جدّيةً تتعلق بمصداقية الدليل وسلامة سلسلة حيازته[3]

(Chain of Custody) .

كما تَطرح وسائل التحرّي الخاصة، كاعتراض المراسلات والمراقبة الإلكترونية، إشكالية التعارض مع الحق في الحياة الخاصة وسرّية المراسلات المكفولَين دستوريًّا. ولئن كان المشرّع قد أحاط هذه الوسائل بضمانات إجرائية صارمة، فإنّ كلّ خرقٍ لهذه الضمانات يُفضي إلى بطلان الدليل المستمدّ منها وعدم الاحتجاج به[4].

ومن الإشكاليات القانونية المهمّة أيضًا: عدمُ وجود قواعد إثباتٍ خاصةٍ بالدليل الرقمي في التشريع الجزائري، إذ ما زال القاضي يُطبّق القو اعد العامة المعدّة أصلًا للأدلة المادية

---

[1] –منشاوي محمد عبد الله **جرائم الانترنت من منظور شرعي وقانوني**،، منشور في الموقع، https://mwada.com ، اطلع عليه في 23–04–2026.

[2] – عبد الفتاح بيومي ، **المرجع السابق** ،ص114.

[3] – عائشة قارة مصطفى، **المرجع السابق** ،ص201.

[4] –عبد الحميد سفيان ،"**أساليب التحري الخاصة بقانون الإجراءات** "مجلة صوت القانون،العدد9، جامعة خميس مليانة، 2023 ، ص209–210.

التقليدية، ممّا يخلق فجوةً تشريعيةً تستدعي تدخّلًا عاجلًا لسنّ نظامٍ متكاملٍ للإثبات الرقمي يُحدّد شروط القبول والحجّية ودرجة الإقناع[1].

3. الصعوبات ذات الطابع القضائي والمؤسّسي :

تتجلّى هذه الصعوبات في ضعف التكوين التقني لدى القضاة وأعضاء النيابة العامة وضباط الشرطة القضائية، إذ يتطلّب التعامل مع الجريمة الإلكترونية إلمامًا واسعًا بالمفاهيم التقنية، وهو

ما لا تَكفله البرامج التكوينية الحالية بشكلٍ كافٍ. وقد أَدّى هذا الضعف إلى الاعتماد المفرط على الخبراء، ممّا قد يُضعف الدور التحكيمي للقاضي[2].

كما تتميّز هذه الجرائم بالطابع العابر للحدود، ممّا يفرض اللجوءَ المتواصل إلى آلية الإنابة القضائية الدولية، التي تُعدّ في الواقع العملي إجراءً بطيئًا ومُكلفًا، تتعطّل من خلاله العديد من الملفّات لسنواتٍ طويلة، خصوصًا حين يتعلّق الأمر بدولٍ غير مرتبطة باتفاقيات تعاون قضائي مع الجزائر[3].

ويُضاف إلى ذلك نقصُ الإمكانيات المادية والتقنية لدى المخابر الجنائية والوحدات المتخصّصة، التي تجد نفسها في كثيرٍ من الأحيان غيرَ قادرةٍ على تحليل أحدث الأجهزة أو فكّ تشفير البيانات المعقّدة، ممّا يُؤثّر مباشرةً على نجاح المتابعات.

4. آفاق تجاوز هذه الصعوبات :

لمعالجة هذه الإشكاليات، يَتعيّن تبنّي مقاربةٍ متعدّدة الأبعاد تشمل: تحديث التشريع لتكريس قواعد خاصة بالدليل الرقمي، وتعزيز التكوين المتخصّص للقضاة وضباط الشرطة القضائية، وإحداث مخابر وطنية متطوّرة للتحقيق الرقمي، وتفعيل الانضمام إلى الاتفاقيات

---

1 ــ عائشة قارة مصطفى **المرجع السابق**، ص 232.

2 – عبد القادرعدو، **الاثبات في الجرائم الالكترونية بين النص القانوني والتطبيق القضائي**، دار الجامعة الجديدة، الجزائر، 2020 ص ص 201-202.

3 – عبد الفتاح بيومب حجازي، **المرجع السابق**، ص185-193.

الدولية كاتفاقية بودابست لمكافحة الجرائم الإلكترونية لسنة 2001، وتعزيز التعاون مع شركات التكنولوجيا الكبرى لتسهيل الوصول إلى المعطيات المخزّنة[1].

وفي ضوء ما سبق، يمكن القول إنّ وسائل الإثبات في جريمة النصب الإلكتروني أصبحت تشكّل حجرَ الزاوية في المتابعة الجزائية، نظرًا لكونها الوسيلةَ الأساسيةَ لكشف الحقيقة في ظلّ صعوبة الاعتماد على الأدلة التقليدية في البيئة الرقمية، ممّا يجعل من تطوير الخبرة التقنية والتشريعية ضرورةً ملحّةً لمواكبة تطوّر هذا النوع من الجرائم[2].

المطلب الثاني: العقوبات المقرّرة لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

لم يكتفِ المشرّع الجزائري بتجريم أفعال النصب والاحتيال الإلكتروني وتحديد الإجراءات الخاصة بمتابعتها، بل أرفق ذلك بمنظومةٍ عقابيةٍ متدرّجةٍ تجمع بين العقوبات الأصلية والعقوبات التكميلية، بهدف تحقيق الأثر الردعي العام والخاص، وحماية الاقتصاد الوطني والمعاملات الرقمية.

الفرع الأول: العقوبات الأصلية

بالنسبة لهذه العقوبات ميز المشرع بين تلك المفروضة على الشخص الطبيعي كفاعل أصلي للجريمة أو شريكا فيها ، والعقوبات المفروضة على الشخص المعنوي اذا ارتكبت الجريمة باسمه ولحسابه وهي كما يلي.

أولًا: العقوبات المقرّرة للشخص الطبيعي :

[1] – عبد القادر قادة ، **المرجع السابق** ،ص204-205.

[2] – احسن بوسقيعة، **المرجع السابق**، ص329.

تتمثّل الجزاءات المقرّرة لجريمة النصب والاحتيال في حقّ الشخص الطبيعي في عقوباتٍ مختلفة، من بينها الحبس والغرامة، حيث يُجرِّم قانون العقوبات الجزائري هذه الأفعال ضمن المواد 372 إلى 379[1]، وقد حدّد العقوبات التي يمكن أن تُسلَّط على الفاعل.

1. **عقوبة الحبس:** تُعدّ من أهمّ العقوبات التي تُطبَّق على الشخص الطبيعي في جريمتَي النصب والاحتيال، إذ تتراوح مدّتها بين سنةٍ وخمس سنواتٍ وفق ظروف كلّ قضية. وتختلف هذه المدد تبعًا لخطورة الفعل ووجود ظروفٍ مخفّفةٍ أو مشدّدة. فإذا ارتُكبت الجريمة باستعمال محرّراتٍ مزوَّرة02.24، أو كانت الضحية في وضعية ضعفٍ مثل كبار السنّ أو ذوي الاحتياجات الخاصة، فإنّ القاضي قد يلجأ إلى تشديد العقوبة. كما أنّ صور النصب التي تتمّ عبر الوسائل الرقمية قد تكون عقوباتها أكثرَ صرامةً نظرًا لخطورة هذا النوع من الجرائم.
2. **الغرامة المالية:** تُفرض على مرتكب الجريمة وتتراوح قيمتها بين 100.000 دج و500.000 دج، حسب جسامة الفعل وحجم الضرر. ويأخذ القاضي بعين الاعتبار قيمةَ الأموال التي تمّ الاستيلاء عليها بطريقةٍ غير مشروعة، إضافةً إلى طبيعة الضحية وأسلوب الاحتيال المستخدم. وفي الحالات التي يتسبّب فيها الجاني في خسائر مالية كبيرة لعدّة أشخاص، يمكن أن ترتفع قيمة الغرامة لتصل إلى 1.000.000 دج، خصوصًا إذا ارتُكبت الجريمة ضدّ أكثر من ثلاثة أشخاص.

ثانيًا: العقوبات المقرّرة للشخص المعنوي

يمكن أن يُسأل الشخص المعنوي، كالشركات والمؤسسات، جزائيًّا عن الأفعال الإجرامية التي تُرتكب لفائدته من قِبَل ممثّليه أو موظّفيه. ووفقًا للمادة 18 مكرّر من القانون 15/04،[2] يتحمّل الشخص المعنوي المسؤوليةَ الجزائيةَ إذا ارتُكبت جريمة النصب أو

[1]– **الأمر رقم 66–156** المؤرّخ في 8 يونيو **1966** المتضمّن **قانون العقوبات** (الجريدة الرسمية عدد 49 لسنة 1966)، المعدّل والمتمّم.

[2]– **المادة372من الامر رقم 66–156** المتضمن **قانون العقوبات**، المعدل والمتمم.

الاحتيال لحسابه[1]، ويشمل ذلك الجرائم التي يتمّ ارتكابها من طرف العاملين أو المسؤولين داخل المؤسسة.

وفي حالة ثبوت مسؤولية الشخص المعنوي، تُفرض غرامة مالية تعادل خمسة أضعاف الحدّ الأقصى للغرامة المقرّرة للشخص الطبيعي، فقد يصل مبلغها إلى 2.500.000 دج[2]. وقد تتّخذ الجهات القضائية إجراءات إضافية مثل غلق المؤسسة لمدةٍ معيّنة أو فرض عقوبات تؤثّر على نشاطها.

ثالثًا: عقوبة الاتفاق الجنائي

يُقصد بالاتفاق الجنائي، وفقًا للمادة 394 مكرّر 5 من قانون العقوبات، وجود تنسيقٍ بين عدّة أشخاصٍ بهدف تنفيذ جريمةٍ محدّدة[3]. ويُعتبر هذا الاتفاق جريمةً قائمةً بذاتها حتى في حال عدم تنفيذ الفعل الإجرامي المادة 394 مكرر5 وهو الشروع في الجريمة وفي حال ثبوته، تُطبَّق نفس العقوبة التي كانت ستُفرض لو تمّ تنفيذ الجريمة، وإذا شمل الاتفاق عدّة جرائم تُطبَّق أشدّ العقوبات.

رابعًا: الاختصاص المكاني واستخدام الوسائل التقنية

وفقًا للمادة 37 من قانون الإجراءات الجزائية، تختصّ الجهات القضائية المحلية باتخاذ الإجراءات القانونية إذا وقعت الجريمة ضمن نطاقها الإقليمي. غير أنه في حالات النصب أو الاحتيال المرتكَبة عبر الإنترنت، يمكن إحالة القضية إلى المحكمة التي تقع في دائرة اختصاصها مكان إقامة الضحية أو مكان وقوع الجريمة.

---

[1]–حسن بن شيخ، **مذكّرات القانون الجزائي الخاص، الجرائم ضدّ الأشخاص والجرائم ضدّ الأموال**، دار هومة للطباعة والنشر والتوزيع، 2012، ص 237.

[2]–فرحاوي عبد العزيز، **«المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري»**، مجلة الآداب والعلوم الاجتماعية، جامعة سطيف 2، ، العدد 2، 2019، ص 85.

[3] – **المادة 394 مكرّر 5 من الأمر 66–156** المتضمّن **قانون العقوبات** المعدّل والمتمّم.

ويُجيز قانون الإجراءات الجزائية، في المواد 65 مكرّر 3 و65 مكرّر 5، استعمالَ وسائل تقنية مثل اعتراض المراسلات وتسجيل الاتصالات كوسيلةٍ لجمع الأدلة في الجرائم الاقتصادية. ويُعدّ اللجوء إلى هذه الوسائل التكنولوجية خطوةً متقدّمةً في مكافحة الجرائم الحديثة[1].

الفرع الثاني: العقوبات التكميلية

إلى جانب الجزاءات الأصلية، أقرّ المشرّع الجزائري مجموعةً من العقوبات التكميلية التي ترمي إلى تعزيز الردع والتقليل من الآثار الناتجة عن الجرائم، وتُعدّ هذه التدابير جزءًا من السياسة الجنائية الحديثة لما توفّره من حمايةٍ إضافيةٍ للمجتمع والضحايا.

أولًا: المصادرة

تُعتبر المصادرة من أبرز العقوبات التكميلية، لا سيّما في الجرائم ذات الطابع المادي أو الرقمي مثل النصب والاحتيال[2]. وتشمل حجزَ جميع الوسائل والتجهيزات والبرامج التي استُعملت أو كانت مهيّأة للاستعمال في تنفيذ الجريمة. غير أنّ تطبيقها ليس مطلقًا، إذ يراعي المشرّع حقوق الغير حسن النية.

ثانيًا: غلق المواقع أو أماكن الاستغلال

ينصّ قانون العقوبات على إمكانية إغلاق المواقع الإلكترونية أو المحلّات التجارية التي استُخدمت في ارتكاب الجريمة، مثل مقاهي الإنترنت أو المراكز التقنية[3]. ويشترط لتطبيق هذا الإجراء ثبوتُ علم مالك المكان أو المسؤول القانوني بوقوع الجريمة.

---

[1]–العايب سامية وعرابة منال، «**الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني**»، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 1، العدد 9، الصفحات 200–205.

[2]–**المادة 394 مكرّر 6: «مع الاحتفاظ بحقوق الغير حسن النية، يُحكم بمصادرة الأجهزة والبرامج والوسائل المستعملة، مع غلق المواقع التي تكون محلًّا لجريمةٍ من الجرائم المعاقَب عليها وفقًا لهذا القسم، وكذلك غلق المحلّ أو مكان الاستغلال إذا كانت الجريمة قد ارتُكبت بعلم مالكها».**

[3]–فضيلة عاقلي، «**الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**»، أعمال المؤتمر الدولي حول الجرائم الإلكترونية، طرابلس – لبنان، 24–25 مارس، ص 116.

ثالثًا: الظروف المشدّدة

قد تحيط بجريمة النصب أو الاحتيال بعض الملابسات التي تزيد من خطورتها، مثل قيام الجاني بمحو أو إتلاف البيانات، أو استهداف منشآت ذات طابعٍ حسّاس كالمؤسسات ذات الصلة بالأمن الوطني. وتؤدّي هذه الظروف إلى تغليظ العقوبة سواء من حيث مدّتها أو طبيعتها.

رابعًا: قانون البريد والاتصالات الإلكترونية

يتضمّن هذا القانون عقوبات خاصة تُطبَّق على العاملين في قطاع الاتصالات في حال ثبوت تورّطهم في جرائم النصب أو الاحتيال[1]. ومن أبرز هذه العقوبات إنهاء مهام الموظف المعني وسحب الترخيص الممنوح له أو للمؤسسة.

خامسًا: قانون التأمينات

يفرض قانون التأمينات الجزائري مجموعةً من العقوبات التأديبية والتنظيمية على الشركات والوسطاء المعتمَدين عند ثبوت تورّطهم في التلاعب بالبطاقات الإلكترونية[2]، وتشمل التوقيف المؤقت أو النهائي عن النشاط، وفرض غرامات إدارية.

سادسًا: الهيئات المتخصّصة

تُسهم عدّة أجهزةٍ تقنيةٍ وقضائيةٍ في تنفيذ العقوبات التكميلية أو اقتراح تدابيرَ موازية، من بينها الهيئة الوطنية للوقاية من الجرائم السيبرانية والوحدات المختصّة في الجرائم الاقتصادية هي جهاز وطني متخصص انشأه المشرع الجزائري بموجب القانون ،يهدف ،الى الوقاية من الجرائم السيبيرانية ومكافحتها، من خلال تنسيق عمليات التحري والبحث و جمع المعلومات التقنية المتعلقة بالجرائم المرتكبة عبر أنظمة الاعلام والاتصال ،مع تقديم

[1]–**القانون 18-04** المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية ،العدد27 سنة 2018.

[2]–هواري عياش، **مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية**، المعهد الوطني للأدلة الجنائية وعلم الإجرام، الملتقى الوطني حول الجؤيمة المعلوماتية، كلية الحقوق، جامعة بسكرة ، نوفمبر2016، ص 16.

المساعدة التقنية والقضائية للجهات المختصة ،وتقوم هذه الجهات بتقديم الدعم الفني والقانوني، ويمكنها التوصية باتخاذ إجراءات احترازية مثل حجب المواقع الإلكترونية[1].

المبحث الثاني: وسائل الوقاية من جريمة النصب والاحتيال الإلكتروني

إذا كانت السياسة الجنائية الحديثة قد رسّخت مبدأ أنّ «الوقاية خيرٌ من العلاج»، فإنّ هذا المبدأ يكتسي أهميةً مضاعفةً في مجال الجرائم الإلكترونية، حيث يكون الضرر الناتج عنها يَصعُب إصلاحه أو استرجاع ما فُقد بفعله، خصوصًا حين يتعلّق الأمر بأموالٍ حُوّلت إلى حساباتٍ خارجيةٍ أو تمّ تبييضها عبر العملات المشفّرة. ومن هنا، فإنّ الاكتفاء بالردع البَعدي لم يعد كافيًا، بل يجب أن يقترن بمنظومةٍ وقائيةٍ استباقيةٍ تَحُول دون وقوع الجريمة من الأصل.

المطلب الأول: الوسائل التقنية

وتقوم هذه المنظومة الوقائية على ثلاث ركائز متكاملة: ركيزة تقنية تَستند إلى أحدث الحلول التكنولوجية كالتشفير وبروتوكولات الأمان والتوقيع الإلكتروني، وركيزة إدارية تتجسّد في السياسات المؤسّسية وضوابط أمن المعلومات، وركيزة قانونية وإعلامية تَجمع بين إصدار التشريعات الملائمة ونشر الوعي الرقمي بين أفراد المجتمع. ولا يمكن لأيٍّ من هذه الركائز أن تُحقّق نتائجَ فعّالةً بمعزلٍ عن الأخريَين، إذ يتوقّف نجاح المنظومة الوقائية على مدى تكاملها وانسجامها[2].

وعليه، سيتمّ التطرّق في هذا المبحث إلى أهمّ وسائل الوقاية من جريمة النصب والاحتيال الإلكتروني، من خلال عرض الوسائل التقنية في المطلب الأول، ثم الوسائل الإدارية والقانونية والإعلامية في المطلب الثاني.

الفرع الأول: الوسائل التقنية لحماية المستهلك في البيئة الرقمية

[1]– فضيلة عاقلي، **المرجع السابق**، ص113.

[2]– يمينة حوحو، **المرجع السابق**، ص243.

أصبحت حماية المستهلك في البيئة الرقمية من المسائل الأساسية التي أفرزها تطوّر الاقتصاد الرقمي. وقد سعت المؤسسات إلى اعتماد مجموعةٍ من الآليات التقنية التي تهدف إلى تأمين البيانات وصون خصوصية المستخدمين[1]، ومن أبرز هذه الوسائل ما يلي:

1. بروتوكول طبقة المنافذ الآمنة (SSL):

يُعتبر من أهمّ التقنيات المستعمَلة لتأمين نقل البيانات عبر شبكة الإنترنت. ويقوم بتشفير المعلومات المتبادَلة بين المستخدم والموقع، ممّا يمنع المتسلّلين من الاطلاع عليها أو التلاعب بها. وغالبًا ما يُستدلّ على استخدامه بوجود رمز القفل أو عبارة «HTTPS» في شريط العنوان[2].

2. بروتوكول المعاملات المالية الآمنة (SET):

ظهر سنة 1997 بهدف حماية العمليات المالية. ويعتمد على شهاداتٍ رقميةٍ تُصدرها البنوك، ويتكامل مع تطبيقات المحافظ الإلكترونية للتحقّق من هوية حامل البطاقة[3].

3. التشفير الإلكتروني:

يتمثّل في تحويل البيانات من شكلها العادي إلى صيغةٍ غير مفهومةٍ إلا للأطراف المصرَّح لها، باستخدام خوارزميات معقّدة[4]. وينقسم إلى نوعَين: التشفير المتماثل الذي يعتمد على مفتاحٍ واحد، والتشفير غير المتماثل الذي يقوم على مفتاحَين (عام وخاص).

4. البصمة الرقمية (Hashing):

[1]–عزّ الدين غبش، **حماية المستهلك الإلكتروني في ظلّ الجرائم السيبرانية**، المجلة الدولية للتحوّلات القانونية والسياسية، المجلد 1، العدد 1، 2022، ص 104.

[2]– حوحو يمينة ،**عقد البيع الالكتروني في القانون الجزائري**، الطبعة الأولى، دار بلقيس، الجزائر 2016 ص209.

[3]– عز الدين غبش **المرجع السابق** ص 105.

[4]عبان عميروش ،**"النظام القانوني للتشفير كألية للتصديق الالكتروني في التشريع الجزائري و التشريعات المقارنة"**، مجلة البحوث والدراسات القانونية والسياسية، جامعة محمد بو ضياف مسيلة،2022 ، ص 88.

تعتمد على إنتاج قيمةٍ رقميةٍ فريدةٍ تمثّل ملفًّا أو رسالةً معيّنة، وتُستخدم للتأكّد من سلامة البيانات وعدم تعرّضها للتغيير أثناء الإرسال. ومن أشهر خوارزمياتها[1] (SHA-256).

5. **التوقيع الإلكتروني:** يُعتبر بمثابة ختمٍ رقميٍّ يُثبت هوية المُرسِل ويضمن عدم تعديل الوثيقة بعد توقيعها، حيث يتمّ استعمال المفتاح الخاص للتوقيع، في حين يُستخدم المفتاح العام للتحقّق من صحّته.

6. **الشهادة الرقمية(Digital_certificate):** مستندٌ إلكترونيٌّ يَصدر عن جهةٍ موثوقةٍ تُعرف بسلطة التصديق، ويُستخدم لإثبات هوية الأطراف في التعاملات الإلكترونية.

7. **الجدران النارية (Firewalls):** تُعدّ من أهمّ وسائل حماية الشبكات، حيث تُراقب حركة البيانات الواردة والصادرة، وتمنع أيّ محاولات دخولٍ غير مصرَّح بها[2].

8. **استخدام الوسائط الوسيطة مثل PayPal:** توفّر طبقةَ حمايةٍ إضافيةٍ بين المستهلك والبائع، إذ لا يتمّ الكشف المباشر عن البيانات البنكية[3].

المطلب الثاني: الوسائل الإدارية والقانونية والإعلامية

تعد الوسائل الإدارية والقانونية والإعلامية من اهم الاليات المعتمدة في مواجهة الجرائم الالكترونية والحد من اثارها، اذ تسهم كل وسيلة منها في تحقيق جانب معين من الحماية والوقاية.

الفرع الأول: الوسائل الإدارية لحماية أمن المعلومات

تضطلع الإدارة العليا بدورٍ أساسي في تعزيز أمن المعلومات داخل المؤسسات، من خلال تبنّي سياسات رقابية واعتماد تدابير تنظيمية[4].

---

[1] – عز الدين غبش ،**المرجع السابق**، ص 102.

[2] – حوحو يمينة، **المرجع السابق** ، ص 106

[3] – عز الدين غبش، **المرجع السابق** ،ص107.

[4]–جمل عبد اللطيف وطارش عبد الغني، «**الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري**»، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة الأغواط، المجلد 9، العدد 1، 2025، ص 1381.

وتتمثّل أبرز الآليات الإدارية الوقائية فيما يلي:

1. إعداد سياسة واضحة لأمن المعلومات:

يقصد بها وضع قواعد وتعليمات تنظم كيفية حماية المعلومات داخل المؤسسة، مع توعية الموظفين بواجباتهم الأمنية لتقليل الأخطاء والمخاطر، و تتضمّن تحديد المبادئ العامة ومعايير الحماية الأساسية، ممّا يساهم في رفع وعي الموظفين[1].

2. حماية الأجهزة ومراكز البيانات:

تتمثل في تأمين أماكن حفظ الأجهزة والخوادم ومنع دخول غير المصرح لهم، باستعمال وسائل حماية كالبطاقات الأمنية أو البصمة البيومترية[2]. .

3. تنظيم تأمين قواعد البيانات:

يقوم على تحديد صلاحيات كل موظف داخل النظام المعلوماتي، بحيث لا يتمكن من الوصول إلا إلى البيانات المرتبطة بعمله. باعتماد هيكلٍ تنظيميٍّ واضحٍ يتمّ من خلاله توزيع المهام وتحديد صلاحيات كلّ موظف.

4. الإدارة الآمنة لوسائط التخزين والنسخ الاحتياطي:

تعني حماية وسائط التخزين المختلفة مع القيام بنسخ احتياطية دورية للبيانات لتفادي ضياعها أو تلفها. أي تأمين وسائط التخزين الخارجية، مع برمجة عمليات نسخٍ احتياطيٍّ دورية[3].

5. تنظيم مغادرة الموظفين والمتابعة الداخلية:

[1]–جمل عبد اللطيف وطارش عبد الغني، 2025، مرجع سابق، ص 1382.

[2]–يمينة حوحو،مرجع سابق ، ص 107.

[3]–علي عبد القادر القهوجي، "**الحماية الجنائية للبيانات المعالجة إلكترونيًّا**"، مرجع سابق، ص 10.

يقصد به سحب صلاحيات الموظف فور مغادرته المؤسسة ومتابعة استخدام الأنظمة بشكل مستمر لمنع أي استغلال غير مشروع ، من خلال إلزام الموظف بتسليم جميع الوسائل التي بحوزته وسحب صلاحياته فورًا.

6. إنشاء وحدةٍ متخصّصة في أمن المعلومات:

تتمثل في تخصيص قسم أو فريق مختص يتولى مراقبة الأنظمة المعلوماتية والتصدي للمخاطر والهجمات الإلكترونية. و يُفضَّل أن تتوفّر المؤسسات الكبرى على قسمٍ مستقلٍّ يُعنى بأمن المعلومات[1].

7. دعم التكوين المستمر:

يقصد به تدريب الموظفين بصفة دورية على أساليب الحماية الحديثة وكيفية التعامل الآمن مع المعلومات والأنظمة الرقمية. من خلال تنظيم ندواتٍ ودوراتٍ تدريبيةٍ متخصّصة[2]..

8. التحفيز وربط الترقية في المؤسسات بالالتزام الأمني:

يعتمد على تشجيع الموظفين على احترام قواعد الأمن المعلوماتي من خلال المكافآت أو ربط الترقية بمدى الالتزام بالتعليمات الأمنية.

ربطُ الحوافز المهنية بمدى احترام الموظفين لقواعد الأمانة، ويقصد بها اعتماد سياسة داخلية تقوم على تشجيع الموظفين على احترام قواعد الامن المعلوماتي والالتزام بالإجراءات الوقائية المعتمدة داخل المؤسسة[3]..

9. مراقبة حركة البيانات داخل الشبكة:

تتمثل في متابعة انتقال البيانات داخل الشبكات المعلوماتية للكشف المبكر عن أي نشاط مشبوه أو محاولة اختراق، مما يساعد على حماية المعلومات ومنع تسربها أو التلاعب بها.

---

[1]– علي عبد القادر القهوجي، **المرجع السابق**، ص 10.

[2]–جمل عبد اللطيف وطارش عبد الغني، مرجع سابق، ص 1382.

[3]–جمل عبد اللطيف وطارش عبد الغني، المرجع نفسه، ص 1383.

ضبطُ مرور الملفات وفق معايير محدّدة، ممّا يساهم في منع تسرّب البرمجيات الخبيثة ومنع قرصنة الملفات.[1]

الفرع الثاني: الوسائل القانونية

إنّ نجاح المعاملات الإلكترونية يرتبط بمدى توفّر الثقة بين المستهلكين والمتعاملين، خاصةً في ظلّ المخاطر المرتبطة بالفضاء الرقمي لذلك، أصبح من الضروري توفير إطارٍ قانوني متكاملٍ يَضمن حماية الحقوق والمصالح المشروعة للمستهلك الإلكتروني.

وفي هذا السياق، أصدر الاتحاد الأوروبي توجيهات تنظّم التجارة الإلكترونية وتحدّد قواعد الاختصاص القضائي. أمّا في الجزائر، فقد سعى المشرّع إلى مواكبة هذه التطوّرات من خلال إصدار القانون رقم 09-04 المتعلّق بمكافحة الجرائم المعلوماتية، والقانون رقم 09-03 المؤرّخ في 25 فبراير 2009 المتعلّق بحماية المستهلك وقمع الغش، وقانون التجارة الإلكترونية رقم 18-05. غير أنّ هذه الجهود لا تزال بحاجةٍ إلى تعزيزٍ وتطويرٍ لمواجهة التحدّيات المتزايدة[2]..

الفرع الثالث: الوسائل الإعلامية

لم تَعد وسائل الإعلام تَقتصر على نقل الأخبار، بل أصبحت دعامةً أساسيةً في نشر الوعي المجتمعي وتنبيه الأفراد إلى المخاطر المرتبطة بالمعاملات الرقمية[3]. وقد تنوّعت هذه الوسائل بين الإعلام التقليدي كالتلفزيون والإذاعة والصحف، والإعلام الحديث الذي يشمل المواقع الإلكترونية وشبكات التواصل الاجتماعي.

أولًا: الحملات التوعوية عبر وسائل الإعلام التقليدية

---

[1]– علي عبد القادر القهوجي، **المرجع السابق**، ص 10.

[2]–بلعطار زوليخة وبن عميروش مديحة، «**آليات حماية المستهلك الإلكتروني من مخاطر الاحتيال والاختراق**»، الملتقى الوطني الثالث، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر،12-05- 2018، 1606.

[3]– خبزاوي مراد ،" **الاعلام الأمني الرقمي كممارسة امنية استباقية** "، مجلة البحوث و الدراسات العلمية، جامعة لمدية ، مجلد 18، العدد 1، 2024، ص810.

تؤدّي وسائل الإعلام التقليدية دورًا بارزًا في نشر الوعي بالأمن الرقمي ومكافحة الجرائم الإلكترونية، من خلال برامج متخصّصة تستعرض مفاهيم الأمن السيبراني، واستضافة مختصّين لشرح أساليب الاحتيال الشائعة. ومن بين الأمثلة، بثّ برامج تحذيرية حول رسائل البريد الإلكتروني الاحتيالية والرسائل النصية المضلّلة[1].

ثانيًا: الإعلام الرقمي ومنصّات التواصل الاجتماعي

تُعدّ المنصّات الرقمية من أبرز أدوات التوعية الحديثة نظرًا لسرعة انتشار المعلومات عبرها حيث تُستغلّ هذه الوسائل في نشر محتوياتٍ توعويةٍ مثل المنشورات والفيديوهات القصيرة[2].

ثالثًا: الصحافة الإلكترونية والمواقع الإخبارية

تلعب المواقع الإخبارية دورًا مهمًّا في توعية الأفراد بمخاطر الجرائم الإلكترونية، من خلال نشر مقالات تحليلية تشرح أساليب الاحتيال وتعتمد هذه المنصّات على عرض الحالات الواقعية كأسلوبٍ توعوي مؤثّر، يجعل المتلقّي أكثر إدراكًا لخطورة هذه الجرائم[3].

كما تقدّم هذه المواقع إرشاداتٍ عمليةً دقيقةً تساعد المستخدمين على اكتشاف المواقع المزيّفة، من خلال التركيز على علاماتٍ تحذيريةٍ مثل التحقّق من عنوان الموقع، والتأكّد من وجود بروتوكول الأمان (HTTPS)، وملاحظة الأخطاء اللغوية أو التصميم غير الاحترافي[4].

رابعًا: التعاون بين الإعلام والجهات الأمنية

شَهدت العلاقة بين وسائل الإعلام والجهات الأمنية تطوّرًا ملحوظًا في مواجهة الجرائم الإلكترونية، حيث يتمّ التنسيق لنشر تحذيرات رسمية وتنبيهات موجَّهة للمواطنين، ويتجلّى

---

[1]– بلعطار زليخة وبن عميروش مديحة ، **المرجع نفسه** ، ص1606.

[2]– خبزاوي مراد ، **المرجع السابق**، ص 813.

[3]– شيرين بحري ،"**دور الاعلام الرقمي في تعزيز الامن السيبيراني**"،المجلة العلمية للبحوث والعلاقات العامة، جامعة القاهرة، العدد 25، 2024، ص55.

[4] – حوحو يمينة ، **المرجع السابق**، ص 114.

هذا التعاون أيضًا في المشاركة في الندوات والملتقيات المتخصّصة في الأمن السيبراني، التي تجمع بين الخبراء والباحثين والممارسين في المجالين القانوني والتقني[1].

خامسًا: المحتوى التعليمي عبر الإنترنت

تُسهم المنصّات الرقمية بشكلٍ كبيرٍ في نشر المعرفة المتعلّقة بمخاطر الاحتيال الإلكتروني، من خلال تقديم محتوى تعليميٍّ مبسَّطٍ يساعد المستخدمين على فهم أساليب الاحتيال مثل التصيّد الإلكتروني وانتحال الهوية[2].

ومن أهمّ الإرشادات في هذا الإطار: تفعيل خاصية التحقّق الثنائي(Two-Factor Authentication)، واستخدام كلمات مرورٍ قويةٍ ومعقّدة، والحذر عند التعامل مع الروابط والملفّات المجهولة المصدر، وتحديث كلمات المرور بشكلٍ دوري. وتُسهم هذه الجهود التوعوية في بناء ثقافةٍ رقميةٍ وقائيةٍ تقوم على مبدأ «المستخدم هو خط الدفاع الأوّل»[3].

[1] – خبزاوي مراد ،**المرجع السابق**، ص 819.

[2] – خديجة بغدادي،"**الاعلام الامني ودوره في نشر ثقافة الوعي الأمني المجتمعي**"، مجلة العلوم الاجتماعية، جامعة البليدة،مجلد1، العدد4، يونيو ،2018، ص442.

[3] – عز الدين غبش، **المرجع السابق**، ص102.

خلاصة الفصل:

يتّضح من خلال ما تمّ تناوله في هذا الفصل أنّ المشرّع الجزائري قد سعى إلى إحاطة جريمة النصب والاحتيال الالكتروني بإطارٍ قانوني وإجرائي يهدف إلى تحقيق الفعّالية في المتابعة الجزائية، من خلال تجريمها ضمن أحكام قانون العقوبات، وتفعيل دور النيابة العامة في تحريك الدعوى العمومية وتنويع مصادرها بين الشكوى الفردية والإخطار المؤسّسة والتحرّي الاستباقي، إلى جانب توسيع قواعد الاختصاص القضائي بما يتماشى مع الطبيعة العابرة للحدود لهذا النوع من الجرائم. كما تمّ إقرار وسائل إثباتٍ حديثةٍ تقوم على الأدلة الرقمية والتقنيات الإلكترونية، وإن كانت ما زالت تَصطدم بصعوباتٍ تقنيةٍ وقانونيةٍ وقضائيةٍ تستوجب تدخّلًا تشريعيًّا عاجلًا.

ومن جهةٍ أخرى، لم يَقتصر تدخّل المشرّع على الجانب الردعي فحسب، بل امتدّ ليشمل الجانب الوقائي من خلال تبنّي مجموعةٍ من الوسائل التقنية والإدارية والقانونية والإعلامية التي تهدف إلى الحدّ من انتشار هذه الجريمة، وهو ما يعكس توجّهه نحو سياسةٍ جنائيةٍ شاملةٍ تجمع بين الوقاية والردع.

ومع ذلك، فإنّ فعّالية هذه المنظومة تبقى مرهونةً بمدى تطوّر الوسائل التقنية المتاحة، وتكامل الجهود بين مختلف الأجهزة المختصّة، إضافةً إلى تعزيز التعاون الدولي في مواجهة الجرائم الإلكترونية العابرة للحدود. لذلك، يبقى تطوير الإطار القانوني وتدعيم الخبرة التقنية ضرورةً ملحّةً لمواكبة التطوّر المستمرّ في هذا المجال.

الخاتمة

الخاتمة :

في ختام هذه الدراسة المتعلقة بجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري، يتبين أن هذا الموضوع من أهم المواضيع القانونية الحديثة التي فرضت نفسها بقوة في ظل التطور التكنولوجي المتسارع واعتماد الأفراد والمؤسسات بشكل متزايد على الوسائل الإلكترونية في مختلف المعاملات اليومية.

فقد أدى هذا التطور إلى ظهور أنماط جديدة من الجرائم التي تستهدف الأموال والمعلومات الشخصية بطرق احتيالية دقيقة ومعقدة، و جعل هذه الجريمة تشكل تهديد حقيقي للأمن المالي والرقمي على حد سواء , و جريمة النصب والاحتيال الإلكتروني تتميز بخصوصية تجعلها مختلفة عن الجرائم التقليدية، سواء من حيث الوسائل المستعملة في ارتكابها أو من حيث صعوبة اكتشافها وإثباتها، إضافة إلى كونها غالبا ما تتم عبر فضاء إلكتروني واسع وعابر للحدود و يزيد من تعقيد مكافحتها.

وهذا ما دفع المشرع الجزائري إلى محاولة مواكبة هذا التطور من خلال سن نصوص قانونية , تهدف إلى تجريم هذه الأفعال ووضع آليات قانونية للحد منها غير أن فعالية هذه النصوص تبقى محل نقاش في ظل استمرار انتشار هذه الجرائم وتطور أساليب ارتكابها .

وبناء على ما سبق فإن دراسة هذا الموضوع سمحت بالوقوف على مختلف الجوانب القانونية لجريمة النصب والاحتيال الإلكتروني، من حيث مفهومها وأركانها وكذا الإطار التشريعي المخصص لمكافحتها في الجزائر , و أبرزت هذه الدراسة الحاجة المستمرة إلى تطوير المنظومة القانونية وتعزيز آليات الرقابة والتعاون الأمني والقضائي، بما يضمن حماية أفضل للأفراد والمعاملات الإلكترونية، ويواكب التحولات الرقمية المتسارعة التي يشهدها العالم اليوم.

النتائج :

الخاتمة :

توصلت هذه الدراسة إلى أن جريمة النصب والاحتيال الإلكتروني من أخطر الجرائم المستحدثة في العصر الرقمي، نظرا لاعتمادها على وسائل تكنولوجية متطورة يصعب في كثير من الأحيان تتبعها أو كشف مرتكبيها، مما يجعلها أكثر تعقيد مقارنة بجريمة النصب التقليدية , و تبين أن هذه الجريمة تتسم بمرونة في الأساليب وتنوع في الصور الأمر الذي يسمح بتجددها المستمر وتوسع نطاقها الجغرافي عبر الفضاء الإلكتروني.

و خلصت الدراسة إلى أن المشرع الجزائري قد سعى إلى مواكبة هذا النوع من الجرائم من خلال سن نصوص قانونية في قانون العقوبات والقوانين الخاصة بمكافحة الجرائم المعلوماتية، غير أن هذه النصوص رغم أهميتها لا تزال بحاجة إلى مزيد من التطوير والتحديث لمواكبة التطور السريع في أساليب الاحتيال الإلكتروني , إضافة إلى ذلك تبين أن الصعوبات العملية في الإثبات والتحري تشكل عائقا أمام فعالية المتابعة القضائية.

أظهرت الدراسة أن مكافحة جريمة النصب والاحتيال الإلكتروني لا تقتصر فقط على الجانب التشريعي، بل تتطلب أيضا تعزيز التعاون الأمني والقضائي وتكثيف التوعية الرقمية لدى المستخدمين، إلى جانب تطوير الخبرات التقنية للجهات المختصة و يساهم في الحد من انتشار هذه الجريمة وتقليل آثارها على الأفراد والمجتمع.

لم يَقتصر تدخّل المشرّع على الجانب الردعي فحسب، بل امتدّ ليشمل الجانب الوقائي من خلال تبنّي مجموعةٍ من الوسائل التقنية والإدارية والقانونية والإعلامية التي تهدف إلى الحدّ من انتشار هذه الجريمة

وكما توصلنا إلى أن فعّالية هذه المنظومة تبقى مرهونةً بمدى تطوّر الوسائل التقنية المتاحة، وتكامل الجهود بين مختلف الأجهزة المختصّة، إضافةً إلى تعزيز التعاون الدولي في مواجهة الجرائم الإلكترونية العابرة للحدود،

الخاتمة :

المقترحات.

في ضوء ما توصلت إليه الدراسة من نتائج يمكن تقديم مجموعة من الاقتراحات , التي من شأنها تعزيز الحماية القانونية والحد من جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري.

أولا : التحديث التشريعي وسد الفراغات القانونية :

-إدراج صور الإحتيال الحديثة، حيث يجب ألا يقتصر النص القانوني على تجريم الفعل العام، بل يتعداه لتجريم الأساليب الرقمية الناشئة صراحةً، مثل: الاحتيال عبر تقنيات الذكاء الاصطناعي والتزييف العميق(Deepfakes) ، والهندسة الاجتماعية، وسرقة الهويات الرقمية لغرض النصب، والتصيد الاحتيالي .(Phishing) .

-سد الفراغ القانوني المتعلق باستغلال العملات الرقمية والمشفرة كقنوات لتهريب الأموال الناتجة عن النصب الإلكتروني، ووضع أطر تنظيمية تُلزم منصات التداول (إن وُجدت) بالشفافية وتحديد الهوية .

ثانيا : تعزيز القدرات التقنية وتفعيل التعاون الدولي .

-إنشاء دوائر قضائية متخصصة حصرياً في الجرائم السيبرانية، تضم قضاة تحقيق ووكلاء جمهورية ملمين بالبرمجة والشبكات .

-دعم الأجهزة الأمنية (الشرطة والدرك الوطني) بمختبرات متطورة قادرة على استرجاع البيانات المشفرة وتتبع البصمات الرقمية (IP tracking) حتى في حال استخدام شبكات .VPN .

-تفعيل أكبر للاتفاقيات الدولية (مثل اتفاقية بودابست للجريمة الإلكترونية)، وتسهيل آليات تسليم المجرمين واسترداد الأموال المنهوبة بالتنسيق مع "الإنتربول."

ثالثا : الحوكمة الرقمية والتوعية المجتمعية :

-إلزام البنوك والمؤسسات المالية بتطوير أنظمة إنذار مبكر تعتمد على الذكاء الاصطناعي لرصد المعاملات المالية المشبوهة أو التحويلات الضخمة المفاجئة، وتسهيل إجراءات تجميد الحسابات المصرفية محل الشبهة فوراً .

-إطلاق حملات تحسيسية وطنية مستمرة تشترك فيها وسائل الإعلام، وزارة التعليم العالي، ووزارة البريد والمواصلات السلكية واللاسلكية، لتعليم المواطنين قواعد "النظافة الرقمية" (مثل عدم مشاركة رموز OTP أو كلمات المرور

-تطوير تطبيقات ومواقع رسمية سهلة الاستخدام تتيح للضحايا التبليغ عن محاولات النصب فور حدوثها، مما يسمح للجهات المختصة بحظر المواقع أو الحسابات الاحتيالية قبل اتساع رقعة الضحايا.

قائمة المصادر والمراجع

قائمة المصادر و المراجع :

أولا- قائمة المصادر

النصوص التشريعية

- **القوانين والأوامر**

1. **الأمر رقم 66-156 المؤرخ في 8 يونيو 1966**، المتضمن **قانون العقوبات**، الجريدة الرسمية عدد 49، المعدل بالقانون رقم 24-06 المؤرخ في 28 أبريل 2024، الجريدة الرسمية عدد 30.
2. **القانون رقم 04-15 المؤرخ في 10 نوفمبر** 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر، العدد 71، الصادرة في 10 نوفمبر 2004.
3. **القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.
4. **القانون 18-04 المؤرخ في 10 ماي 2018**، المحدد **للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية**، الجريدة الرسمية، العدد27 سنة 2018.
5. **Code pénal français** – dernière modification le 01 janvier 2021 – Document généré le 12 février 2021.

- **النصوص التنظيمية**

6. **المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015** المتضمن **إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وسيرها**، الجريدة الرسمية، العدد 54.

ثانيا- قائمة المراجع

- **الكتب**

7. إبراهيم حسني عبد السميع، **الجرائم المستحدثة عن طريق الإنترنت**، دار النهضة العربية، القاهرة، .
8. أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص، الجزء الأول**، دار هومة، الجزائر، الطبعة الثانية عشرة، 2023.
9. _____، **الوجيز في القانون الجزائي الخاص**، الجزء الثاني، دار هومة، الجزائر، الطبعة 19، 2021.
10. أحمد الخمليشي، **القانون الجنائي الخاص، الجزء الثاني**، مكتبة المعارف، ط2، 1986.
11. أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006.
12. أحمد عمرة حسبو، **حماية الحريات في مواجهة نظم المعلومات**، دار النهضة العربية، القاهرة، 2006.
13. أحمد محمود مصطفى، **جرائم الحاسبات الآلية في التشريع المصري**، دار النهضة العربية، القاهرة، 2010.
14. أسامة أحمد المناعسة، **جرائم الحاسب الآلي والإنترنت**، دار وائل للنشر، 2001.
15. أسامة حمدان الرقب، **جرائم النصب والاحتيال: الأساليب والمظاهر والعلاج**، دار يافا، عمان ، د س ن .
16. أسامة سمير حسين، **الاحتيال الإلكتروني الوجه القبيح للتكنولوجيا**، الجنادرية للنشر، عمان، 2006.
17. أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة، 1994.
18. اشرف قنديل عبد القادر، **الاثبات الجنائي في الجريمة الالكترونية** ، دار الجامعة الجديدة، الإسكندرية ، 2015.
19. أمال قارة، **الحماية الجزائية المعلوماتية في التشريع الجزائري** ، دار هومة ،الجزائر، 2006 .

20. _____، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة، الجزائر، 2007.

21. أمير فرج يوسف، **جرائم المعلومات على شبكة الإنترنت**، دار المطبوعات الجامعية، الإسكندرية، 2009.

22. حسن بن شيخ، **مذكرات القانون الجزائي الخاص، الجرائم ضد الأشخاص والجرائم ضد الأموال**، دار هومة للطباعة والنشر والتوزيع، 2012.

23. حسن طاهر داوود، **جرائم نظم المعلومات**، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.

24. حوحو يمينة ،**عقد البيع الالكتروني في القانون الجزائري**، الطبعة الأولى، دار بلقيس، الجزائر 2016 ص209.

25. خالد عباد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة، عمان، 2000.

26. خالد محمد المهيري، **جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية**، معهد القانون الدولي، دبي.

27. خالد مصطفى فهمي، **النظام القانوني للتوقيع الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2007.

28. د الغافري، **السياسة الجنائية في مواجهة جرائم الإنترنت**، دار النهضة العربية، القاهرة، 2009 .

29. رياض فتح الله بصلة، **جرائم بطاقات الائتمان**، دار الشروق، القاهرة، 1995.

30. سامح محمد عبد الحكيم، **الحماية الجنائية لبطاقات الائتمان**، دار النهضة العربية، القاهرة، 2003.

31. الشحات إبراهيم منصور، **الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية**، دار النهضة العربية، القاهرة، 2002.

32. الصغير جميل عبد الباقي، **الإنترنت والقانون الجنائي**، دار النهضة العربية، القاهرة، 2001.

33. طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي والنظام القانوني للحماية المعلوماتية،** دار الجامعة الجديدة، 2009.

34. طنطاوي إبراهيم أحمد، **المسؤولية الجنائية لجرائم النصب والاحتيال،** د د ن ، القاهرة، 1998.

35. عائشة بن قارة مصطفى، **حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن** ، دار الجامعة الجديدة، 2010.

36. عبد العزيز سعد، **إجراءات ممارسة الدعوى الجزائية،** دار هومة، الجزائر، 2008.

37. _____، **الجرائم الواقعة على أنظمة المعالجة الالية للمعطيات،** دار هومة ،الجزائر ،2019.

38. عبد الفتاح بيومي حجازي، **الجرائم المعلوماتية في التشريع المقارن،** دار الفكر الجامعي، الإسكندرية، 2008.

39. _____، **الدليل الرقمي وحجيته في الإثبات الجنائي،** دار الفكر الجامعي، الإسكندرية، 2019.

40. عبد القادر عدو، **المبادئ العامة في قانون الإجراءات الجزائية الجزائري،** دار هومة الجزائر،2018.

41. _____، **الاثبات الجرائم الالكترونية بين النص القانوني والتطبيق القضائي،** دار الجامعة الجديدة، الجزائر، 2020 .

42. عبد الله أوهايبية، **شرح قانون الإجراءات الجزائية، الجزء الأول،** الطبعة الثانية، دار هومة، الجزائر ً2018 .

43. عبد رحمان خلفي، **الإجراءات الجزائية،** دار بلقيس الجزائر، الطبعة الثامنة،2025.

44. عرب يونس، **موسوعة القانون وتقنية المعلومات، الجزء الأول،** اتحاد المصارف العربية، 2002.

45. _____، **موسوعة جرائم الكمبيوتر والإنترنت،** اتحاد المصارف العربية، 2002.

46. علي عبد القادر القهوجي، **الحماية الجنائية للبيانات المعالجة إلكترونيا**، الطبعة 3،الإمارات العربية المتحدة، 2004.

47. _____، **جرائم الاعتداء على الإنسان والمال**، منشورات الحلبي، 2002.

48. _____، **قانون العقوبات – القسم الخاص، منشورات الحلبي الحقوقية**، بيروت، الطبعة الثانية، 2002.

49. محمد عوض ، **جرائم الأشخاص والأموال**، دار المطبوعات الجامعية، الإسكندرية، 2002.

50. محمد الأمين البشري ، **التحقيق في الجرائم المستحدثة** ،الطبعة 1، اكاديمية نايف العربية للعلوم الأمنية ، السعودية ،2004.

51. محمد طارق رمضان، **جريمة الاحتيال عبر الإنترنت**، دار الحامد، الأردن، 2011.

52. محمد عبد الله أبو بكر سلامة، **جرائم الكمبيوتر والإنترنت**، منشأة المعارف، الإسكندرية، 2006.

53. محمد عبيد الكعيبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، 2009.

54. محمود نجيب حسني، **شرح قانون العقوبات القسم الخاص**، دار النهضة العربية، القاهرة، 1988.

55. الفريق طاهر جليل الحبوش، **جرائم الاحتيال: الأساليب والوقاية والمكافحة**، أكاديمية نايف، الرياض، 2001.

56. نائلة قرة عادل محمد فريد، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي الخقوقية، بيروت، 2005.

57. هيثم حمود الشلبي، **إدارة مخاطر الاحتيال في قطاع الاتصالات**، دار صفاء، عمان، 2009.

- **المقالات**

58. جمل عبد اللطيف وطارش عبد الغني، «**الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري**»، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة الأغواط، المجلد 9، العدد 1، 2025.

59. خبزاوي مراد ،" **الاعلام الأمني الرقمي كممارسة امنية استباقية** "، مجلة البحوث و الدراسات العلمية، جامعة لمدية ، مجلد 18، العدد 1، 2024.

60. خديجة بغدادي،"**الاعلام الامني ودوره في نشر ثقافة الوعي الأمني المجتمعي**"، مجلة العلوم الاجتماعية، جامعة البليدة،مجلد1، العدد4، يونيو ،2018.

61. خوري عمر، "**سلطات الشرطة القضائية في مواجهة الجريمة المتلبس بها**" ،المجلة الجزائرية العلوم القانونية والسياسية المجلد 51 رقم 3.

62. شايب محمد، **اليات الحماية من الغش في وسائل الدفع الالكتروني**، مجلة نماء للاقتصاد والتجارة ،جامعة جيجل، المجلد1،العدد2، 2017.

63. شهيرة بولحية و دنيا زاد سويح، "**الاحتيال الالكتروني "مجلة الدراسات القانونية والاقتصادية**، المركز الجامعي بريكي، المجلد 2،العدد2 ، 2019 .

64. شيرين بحري ،"**دور الاعلام الرقمي في تعزيز الامن السيبيراني**"،المجلة العلمية للبحوث والعلاقات العامة، جامعة القاهرة، العدد 25، 2024.

65. العايب سامية وعرابة منال، "**الحماية الجزائية للمستهلك من جريمة النصب الالكتروني**" مجلة هيرودوت للعلوم الإنسانية والاجتماعية ،المجلد 5،العدد 3، 2021.

66. عبان عميروش ،"**النظام القانوني للتشفير كألية للتصديق الالكتروني في التشريع الجزائري و التشريعات المقارنة**"، مجلة البحوث والدراسات القانونية والسياسية، جامعة محمد بو ضياف مسيلة،2022 .

67. عبد الحميد سفيان ،"**أساليب التحري الخاصة بقانون الإجراءات** "مجلة صوت القانون،العدد9، جامعة خميس مليانة، 2023 .

68. عبد العزيز بن عبد الرحمن الشمري، "**جريمة النصب والاحتيال**"، مجلة العدل، عدد 39، وزارة العدل السعودية، 2000.

69. عبيد علي ناصر موفق وآخرون، "**ماهية جريمة الاحتيال الإلكتروني**"، مجلة كلية القانون والعلوم السياسية، جامعة تكريت، بغداد، د س ن .

70. عزّ الدين غبش، **حماية المستهلك الإلكتروني في ظل الجرائم السيبرانية**، المجلة الدولية للتحولات القانونية والسياسية، المجلد 1، العدد 1، 2022 .

71. فاطمة الزهراء رمضاني، "**القصور التشريعي في مجال الجريمة المعلوماتية**"، مجلة الأستاذ الباحث، جامعة المسيلة، المجلد 07، العدد 02، 2022.

72. فرحاوي عبد العزيز، **«المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري»**، مجلة الآداب والعلوم الاجتماعية، جامعة سطيف 2، ، العدد 2، 2019.

73. مهدي رضا، **الجرائم السبيرانية وأليات مكافحتها في التشريع الجائري** ، المجلد 06، العدد 2 ، 2021.

74. منشاوي محمد عبد الله، **جرائم الانترنت من منظور شرعي وقانوني**، منشور في الموقع. https://mwada.com

75. نبيلة هبة هروال، **الوانب الإجرائية لجرائم الانترنت**، في مجلة جمع الاستدلالات، دراسة مقارنة دار الفكر الجامعي، الإسكندرية ،2013.

- **الرسائل والمذكرات الجامعية**

76. حمزة بن عقون، "**السلوك الإجرامي للمجرم المعلوماتي**"، رسالة ماجستير، منشورة في الدار الإفريقية للكتاب، الجزائر، 2024.

- **الملتقيات والمؤتمرات العلمية**

77. بلعطار زوليخة وبن عميروش مديحة، **«آليات حماية المستهلك الإلكتروني من مخاطر الاحتيال والاختراق»**، الملتقى الوطني الثالث **المستهلك والاقتصاد الرقمي ضرورة الانتقال وتحديات الحماية**، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، 14-15 نوفمبر 2017.

78. فضيلة عاقلي، «**الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**»، أعمال المؤتمر الدولي حول **الجرائم الإلكترونية**، طرابلس – لبنان، 24-25 مارس2017.

79. النصيرات وائل، "**الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها**"، بحث مقدم إلى المؤتمر الدولي الأول **لمكافحة الجريمة المعلوماتية**، جامعة الإمام محمد بن سعود الإسلامية، الرياض، نوفمبر 2015.

80. هواري عياش، **مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية**، المعهد الوطني للأدلة الجنائية وعلم الإجرام، الملتقى الوطني حول الجريمة المعلوماتية جامعة بسكرة، كلية الحقوق، 12 نوفمبر 2016.

ملخص دراسة :

الملخص :

شهد العالم في العقود الأخيرة تطوراً هائلاً في تكنولوجيا الإعلام والاتصال أفرز أنماطاً إجرامية مستحدثة تستغل الفضاء الرقمي، وفي مقدمتها جريمة النصب والاحتيال الإلكتروني التي باتت تشكل خطراً كبيراً لاعتمادها على وسائل تقنية متطورة وأساليب خادعة عابرة للحدود تهدف للاستيلاء على أموال وبيانات الغير؛ ومن هذا المنطلق تتمحور هذه الدراسة حول إشكالية رئيسية تبحث في كيفية تنظيم المشرع الجزائري لهذه الجريمة وضبط آليات مكافحتها، حيث تم الاعتماد على المنهجين الوصفي والتحليلي لتأصيل المفاهيم وتفكيك النصوص التشريعية ذات الصلة، وقد خضعت المذكرة لتقسيم ثنائي تناول الفصل الأول منه الإطار العام للجريمة من حيث صورها الرقمية المتعددة وأركانها القانونية (الشرعي، المادي، والمعنوي)، بينما خُصص الفصل الثاني لبحث آليات الردع والوقاية من خلال استعراض الإجراءات الخاصة بالملاحقة القضائية، وجمع الأدلة الرقمية، وتحديد العقوبات المقررة، وصولاً إلى الوسائل التقنية والإدارية المعتمدة لحماية المجتمع؛ وقد خلصت الدراسة إلى جملة من النتائج أبرزها تميز هذا السلوك الإجرامي بالمرونة العالية وصعوبة الإثبات، مع تبني المشرع الجزائري لسياسة جنائية تدمج بين القواعد العامة لقانون العقوبات والقوانين الخاصة بحماية أنظمة المعالجة الآلية للمطيات، مؤكدة على ضرورة تعزيز التعاون الدولي لمواجهة الطبيعة العابرة للحدود لهذه .

الكلمات المفتاحية **: النصب والاحتيال الإلكتروني ، الجرائم المعلوماتية ، الأدلة الرقمية ، المشرع الجزائري، الجريمة العابرة للحدود**

Abstract

In recent decades, the world has witnessed a tremendous advancement in information and communication technology, which has given rise to novel criminal patterns exploiting the digital sphere—foremost among which is electronic fraud. This crime poses a significant threat due to its reliance on sophisticated technical means and deceptive, cross-border methods aimed at misappropriating third-party funds and data. Consequently, this study centers around a core problematic that examines how the Algerian legislator has regulated this crime and established mechanisms to combat it. Utilizing descriptive and analytical methodologies, the research contextualizes the underlying concepts and deconstructs relevant legislative texts. The thesis adopts a balanced two-chapter structure: the first chapter delineates the general framework of the crime, examining its diverse digital forms and legal constituent elements (legal, material, and moral); the second chapter explores deterrence and prevention mechanisms by reviewing judicial prosecution procedures, digital evidence collection, prescribed penalties, as well as the technical and administrative measures adopted to safeguard society. Ultimately, the study concludes with several key findings, notably the high flexibility and evidentiary challenges characterizing this criminal behavior, alongside the Algerian legislator's

ملخص دراسة :

فهرس المحتويات	
الموضوع	الصفحة
شكر وعرفان	
اهداء	
مقدمة	8/1
الفصل الأول : الإطار العام لجريمة النصب والاحتيال الالكتروني	9-46
المبحث الأول : مفهوم جريمة النصب والاحتيال الالكتروني	10
المطلب الأول : تعريف جريمة النصب والاحتيال الالكتروني وخصائصه .	11
الفرع الأول : التعريف القانوني لجريمة النصب والاحتيال الإلكتروني.	12
الفرع الثاني : خصائص جريمة النصب والاحتيال الإلكتروني .	16
الفرع الثالث : تمييز جرائم النصب والاحتيال الإلكتروني عما يشابهها من الجرائم الأخرى .	19
المطلب الثاني : أنواع جريمة النصب والاحتيال الإلكتروني	20
الفرع الأول : النصب والاحتيال عبر وسائل الاتصال الإلكتروني	21
الفرع الثاني : النصب والاحتيال عبر المنصات الرقمية والمعاملات المالية الإلكترونية	24
المبحث الثاني: أركان جريمة النصب و الاحتيال الإلكتروني	27
المطلب الأول : الركن الشرعي	28
الفرع الأول : مبدأ الشرعية الجنائية وتطبيقه على جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري	29
الفرع الثاني : نطاق التجريم والعقاب في جريمة النصب والاحتيال الإلكتروني وفق المادتين 372 و394 مكرر	32
المطلب الثاني: الركن المادي	35
الفرع الأول : السلوك الإجرامي المكوّن لجريمة النصب والاحتيال	36
الفرع الثاني : النتيجة الإجرامية وعلاقة السببية	38

المطلب الثالث: الركن المعنوي	**41**
الفرع الأول: القصد الجنائي العام في جريمة النصب والاحتيال الإلكتروني	**42**
الفرع الثاني: القصد الجنائي الخاص	**44**
الفصل الثاني: آليات الردع و الوقاية من جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري	**47-76**
المبحث الاول: الأحكام الإجرائية لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري	**49**
المطلب الأول: المتابعة الجزائية لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري	**50**
الفرع الأول : الأساس القانوني وإجراءات تحريك الدعوى العمومية في جريمة النصب والاحتيال الإلكتروني	**50**
الفرع الثاني : الاختصاص في جريمة النصب والاحتيال الإلكتروني	**56**
الفرع الثالث: وسائل الإثبات في جريمة النصب الإلكتروني وصعوباته	**58**
المطلب الثاني: العقوبات المقرّرة لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري	**64**
الفرع الأول : العقوبات الأصلية	**64**
الفرع الثاني : العقوبات التكميلية	**66**
المبحث الثاني : وسائل الوقاية من جريمة النصب والاحتيال الإلكتروني .	**68**
المطلب الأول : الوسائل التقنية	**68**
الفرع الأول : الوسائل التقنية لحماية المستهلك في البيئة الرقمية	**69**
المطلب الثاني: الوسائل الإدارية والقانونية والإعلامية	**70**
الفرع الأول : الوسائل الإدارية لحماية أمن المعلومات	**71**
الفرع الثاني : الوسائل القانونية	**73**
الفرع الثالث: الوسائل الإعلامية	**73**
خاتمة	**77**
قائمة المراجع	

فهرس المحتويات:

ملخص الدراسة	
فهرس المحتويات	