المركز الجامعي المقاوم الشيخ آمود بن مختار –إيليزي–

معهد الحقوق

مذكرة تخرج لنيل شهادة ماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية

بعنوان

جرائم النصب والاحتيال الالكتروني في التشريع الجزائري

من اعداد الطالبين:

–أبوبكر تيتاوي.

–الياس مالك قرادي

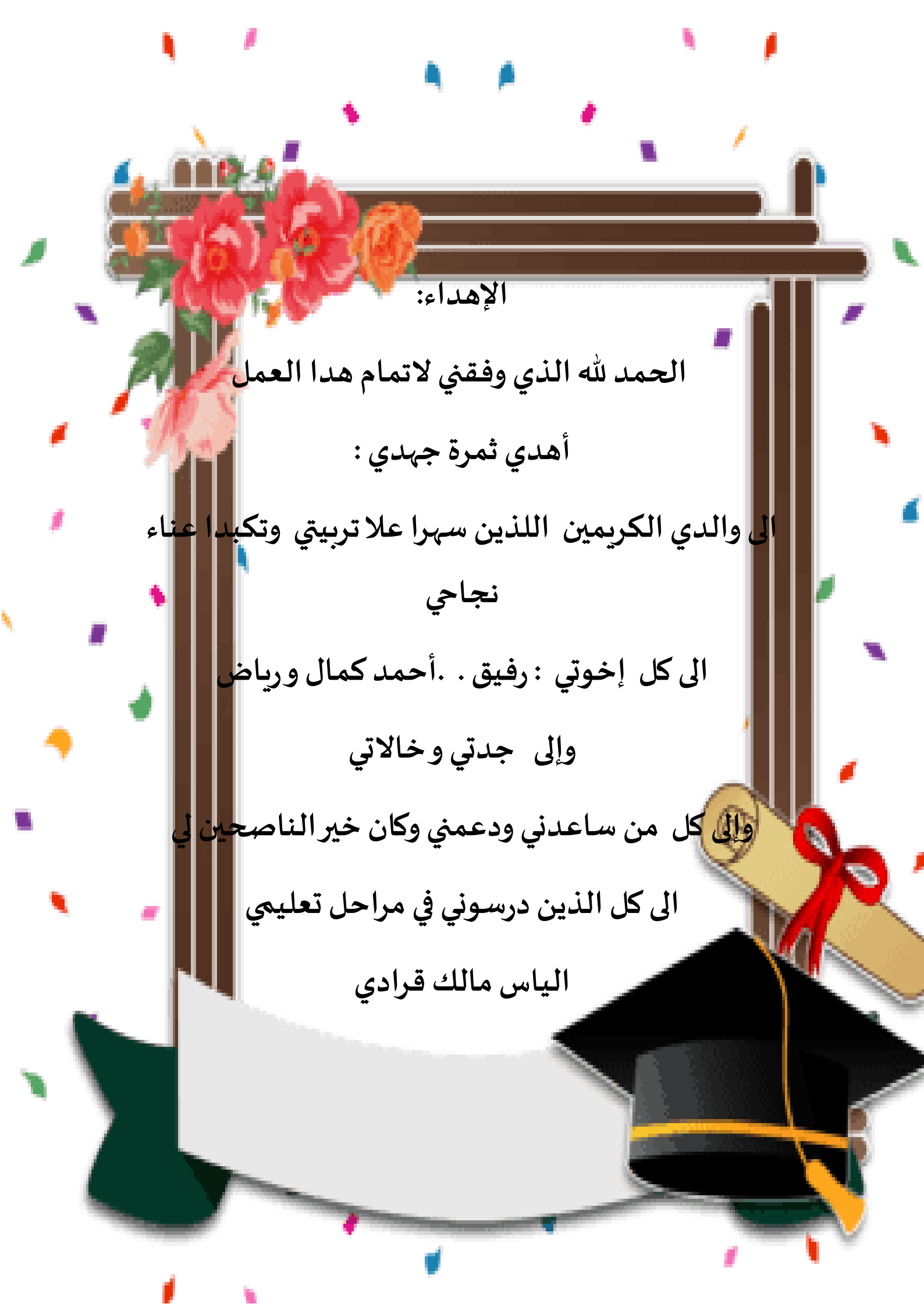
تحت اشراف الأستاذ:

د. عباس صادقي

وتتكون لجنة المناقشة من الأساتذة:

د. الطاهر عبدو علي	أستاذ محاضر أ	المركز الجامعي إيليزي	رئيسا
د. عباس صادقي	أستاذ محاضر أ	المركز الجامعي إيليزي	مشرفا ومقررا
د. مراد شروف	أستاذ محاضر ب	المركز الجامعي إيليزي	مناقشا

السنة الجامعية: 2025/2024



الإهداء:

الحمد لله الذي وفقني لاتمام هدا العمل

أهدي ثمرة جهدي :

الى والدي الكريمين اللذين سهرا علا تربيتي وتكبدا عناء نجاحي

الى كل إخوتي : رفيق . .أحمد كمال ورياض

وإلى جدتي وخالاتي

وإلى كل من ساعدني ودعمني وكان خير الناصحين لي

الى كل الذين درسوني في مراحل تعليمي

الياس مالك قرادي

إهداء

الى من غرس في قلبي حُبّ الطموح، وكان [illegible] الا يلين...

الى أبي، يا من علّمتني أنّ الإرادة تصنع المستحيل، فكنت النور الذي أضاء دربي بحكمته ونصائحه.

الى نبع الحنان، ومصدر الصبر، الى قلبٍ لا يشبهه قلب...

الى أمي، يا من كنتِ الدعاء الصادق ترفعني كلّما تعثرت، لن أبلغ قمة دون رضاكِ.

الى إخوتي الذين كانوا لي عونًا وسندًا، ومصدرَ قوةٍ في لحظات الضعف،

الى أخواتي، زهرة أيامي، و ضحكتكن كانت بلسمًا في أوقات التعب.

الى أصدقائي الذين شاركوني تفاصيل الرحلة، وكانوا كتفًا يُستند إليه، وحدٍ يشهم يزرع الأمل في أوقاتي الصعبة...

لكم جميعًا اهدي هذه الصفحات، فهي ثمرة صبركم و تشجيعكم ودعواتكم.

بوبكر تيتاوي

مقدمة

مقدمة:

يشهد العالم اليوم تطورًا تكنولوجيًا متسارعًا شمل مختلف نواحي الحياة، وفتح آفاقًا جديدة للتواصل والتعاملات الإلكترونية، مما أدى إلى بروز ظواهر جديدة ترتبط بهذا الفضاء الرقمي، من أبرزها جرائم النصب والاحتيال الإلكتروني التي أصبحت تشكل تهديدًا حقيقيًا لأمن الأفراد والمؤسسات على حد سواء.

فقد بات من السهل على الجناة استغلال الثغرات التقنية، وسلوك المستخدمين أحيانًا، لتنفيذ عملياتهم الاحتيالية بطرق يصعب اكتشافها أو إثباتها قانونيًا، مستفيدين من الطابع اللامادي والافتراضي لهذه الجرائم.

وأمام تنامي هذا النوع من السلوكيات الإجرامية، ظهرت الحاجة إلى دراسة هذا الموضوع، نظرًا لأهميته من الناحيتين القانونية والاجتماعية، خصوصًا مع تزايد استخدام الوسائط الإلكترونية في المعاملات اليومية، وتنامي حالات الاحتيال التي تطال الأفراد والمؤسسات، مما يتطلب وعيًا قانونيًا وتقنيًا مشتركًا لتقليص دائرة الخطر. ويكتسي الموضوع أهمية إضافية في كونه يتقاطع مع تحديات العصر الرقمي، من حيث الحماية الجنائية للمعاملات الإلكترونية، وضمان أمن المعلومات، وصيانة حقوق الضحايا.

وتهدف هذه الدراسة إلى تسليط الضوء على الإطار المفاهيمي والقانوني لجريمة النصب والاحتيال الإلكتروني، مع تحليل الأركان التي تقوم عليها، واستعراض أبرز أنواعها وخصائصها، إضافة إلى التطرق إلى العقوبات التي أقرها المشرع الجزائري لمواجهتها، سواء الأصلية أو التكميلية، ثم تقديم عرض شامل لأهم الوسائل المعتمدة للوقاية من هذه الجرائم، سواء كانت تقنية أو إدارية أو إعلامية أو قانونية، وذلك من أجل اقتراح تصور وقائي أكثر فعالية في التصدي لها.

وقد جاء اختيار هذا الموضوع نتيجة دوافع ذاتية تتعلق بالاهتمام الشخصي بالمجالات القانونية المتصلة بالتحول الرقمي، ورغبة في مواكبة التحديات التي يفرضها الواقع الافتراضي على البيئة القانونية، كما أن الطابع المستحدث لهذه الجرائم وما تطرحه من إشكالات قانونية مستجدة جعل من الموضوع ذا أهمية موضوعية تستدعي البحث والتمحيص.

ومع هذا، واجهت الدراسة بعض الصعوبات، أبرزها ندرة المراجع العربية المتخصصة في هذا المجال، وغموض بعض المفاهيم التقنية المستخدمة في النصوص القانونية، إلى جانب التحدي المرتبط بسرعة تطور أساليب الاحتيال التي يصعب حصرها.

وتسعى هذه الدراسة للإجابة عن الإشكالية التالية:

فيم تتمثل جرائم النصب والاحتيال الالكتروني في القانون الجزائري، وما هي أبرز الوسائل المعتمدة لمواجهتها والوقاية منها في ظل التحديات التي يطرحها الفضاء الرقمي؟

وقد تم اعتماد المنهج التحليلي من خلال دراسة النصوص القانونية ذات الصلة، والمنهج الوصفي لتقديم صورة شاملة عن الظاهرة، بالإضافة إلى توظيف بعض عناصر المقارنة مع تجارب أخرى قصد استكمال الرؤية وتحقيق توازن في المعالجة القانونية والعملية.

وقد تم تقسيم الدراسة الى **فصلين** كان عنوان **الأول:** مفهوم جرائم النصب والاحتيال الإلكتروني، أما **الثاني:** العقوبات المقررة لجرائم النصب والاحتيال الالكتروني وآليات الوقاية منها.

الفصل الأول

الفصل الأول

مفهوم جرائم النصب والاحتيال الالكتروني

لقد أفرز التطور التكنولوجي الهائل في العصر الرقمي أنماطًا جديدة من السلوك الإجرامي، تجاوزت في خطورتها وتعقيدها الحدود التقليدية للجرائم المعهودة، وكان من أبرزها جرائم النصب والاحتيال الإلكتروني. فقد باتت هذه الجرائم تتخذ من الفضاء السيبراني مسرحًا لعملياتها، مستغلة ما يتيحه هذا الفضاء من سهولة الوصول إلى الضحايا، والتخفي وراء هويات زائفة، وتعدد الوسائل والتقنيات الرقمية المستخدمة في ارتكاب الأفعال الإجرامية.

وتتسم جرائم النصب والاحتيال الإلكتروني بخصوصية تميزها عن الجرائم التقليدية، سواء من حيث طبيعة الوسائل المستعملة أو من حيث صعوبة كشف مرتكبيها وإثبات أركانها، مما يشكل تحديًا حقيقيًا أمام أجهزة إنفاذ القانون والقضاء. كما أن هذا النوع من الجرائم يطرح إشكالات قانونية وفقهية تتصل بتحديد ماهيتها، وأركانها، وتكييفها القانوني، وتمييزها عن الجرائم القريبة منها في المظهر، كجريمة التزوير أو الاختلاس.

وفي هذا السياق، يأتي هذا الفصل لتسليط الضوء على الإطار المفاهيمي لهذه الجرائم من خلال بيان تعريفها وأركانها، **(المبحث الأول)** وانواعها مع إبراز خصائصها الأساسية، **(المبحث الثاني)** وهو ما يعد تمهيدًا لازمًا لفهم الآليات القانونية والتقنية للوقاية منها ومعالجتها، والتي سيتناولها الفصل اللاحق.

المبحث الأول

تعريف جرائم الاحتيال الالكتروني وأركانها

يشكّل فهم ماهية جرائم النصب والاحتيال الإلكتروني مدخلًا أساسيًا لدراسة هذا النوع المستحدث من الجرائم. ويقتضي ذلك التمييز بين التعريفات اللغوية والاصطلاحية من جهة، وبين المقاربات الفقهية والقانونية من جهة أخرى **(المطلب الأول)**، مع التوقف عند أركان الجريمة المادية والمعنوية التي تُضفي عليها الصبغة الجنائية. **(المطلب الثاني)**.

المطلب الأول: تعريف جرائم النصب والاحتيال الالكتروني:

يُعد تحديد مفهوم جرائم النصب والاحتيال الإلكتروني خطوة جوهرية لفهم طبيعتها وتمييزها عن غيرها من الجرائم ذات الطابع المالي أو المعلوماتي. ويستوجب ذلك الوقوف أولًا عند التعريفين اللغوي والاصطلاحي لمصطلحي "النصب "و"الاحتيال"، **(الفرع الأول)** ثم الانتقال إلى استعراض التصورات الفقهية والقانونية التي أرست الإطار النظري لهذه الجريمة في سياقها التقليدي والإلكتروني **(الفرع الثاني)**.

الفرع الأول: التعريف اللغوي والاصطلاحي للنصب والاحتيال الالكتروني:

يتأسس التعريف اللغوي للنصب والاحتيال على دلالات ترتبط بالخداع والمكر والإيقاع بالآخرين بوسائل ملتوية. فـ"النصب" في اللغة يُشير إلى رفع الشيء وإظهاره، وقد جاء بمعنى الخداع والتلبيس بقصد الاستيلاء على مال الغير بغير حق[1].

أما "الاحتيال"، فجاء في لسان العرب على أنه الاحتيال والتحول والتحيُّل كل ذلك الحذق وجودة النظر والقدرة على دقة التصرف فالمحتال يتصف بالحذق وجودة النظر والدقة في التصرف والمهارة في استدراج الهدف[2]، وهو مأخوذ من الحيلة، ويُقصد به التوصل إلى شيءٍ معين بأسلوب خفيّ يتّسم بالمكر والخداع.[3]

---

[1] عبد العزيز بن عبد الرحمن الشمري، جريمة النصب والاحتيال، مجلة العدل، عدد 39، وزارة العدل السعودية، 2000، ص175.

[2] محمد بن مكرم بن منظور، لسان العرب، دار المعارف، بيروت، جزء 12، 1998، ص187.

[3] طنطاوي ابراهيم أحمد، المسؤولية الجنائية لجرائم النصب والاحتيال، شركة ناس للطباعة والنسر، القاهرة، 1998، ص10.

ومن ثم، فإن كلا المصطلحين يجتمعان في دلالتهما اللغوية على استخدام وسائل غير مشروعة للإضرار بالغير أو الاستيلاء على حقوقهم، وهو ما يشكّل الأساس اللغوي الذي بُني عليه التكييف القانوني لهذه الجرائم في صورتها الحديثة المرتبطة بالوسط الإلكتروني.

أما اصطلاحا فيعرف النصب، كما ورد في بعض التشريعات، ومنها القانون المصري، بأنه: "الاستيلاء على مال مملوك للغير بطريق احتيالي، بهدف تملّكه دون وجه حق". ويتّخذ هذا الاستيلاء صورة استخدام وسائل أو أساليب خادعة يكون من شأنها إقناع المجني عليه بتسليم ماله طواعية، نتيجة انخداعه بالمظاهر الكاذبة أو الوقائع المزيفة التي ينسجها الجاني[1].

ويُشير هذا التعريف إلى أن الجريمة لا تقتصر على مجرد انتزاع المال، بل ترتكز على عنصر جوهري يتمثل في "الحيلة" أو "الخداع"، والذي يُعدّ الأداة الرئيسية في تنفيذ الجريمة وتحقيق غايتها، وهي تملك مال الغير دون رضاه الحقيقي. وبهذا، يكون الجاني — الموصوف قانونًا بـ"النصّاب" أو "المحتال" — قد مارس سلوكًا احتياليًا أدى إلى إيقاع المجني عليه في وهم أو خداع حمله على التصرف بماله على نحو ما كان ليفعله لولا ذلك التأثير غير المشروع.

في حين يمكننا تعريف الاحتيال اصطلاحا على أنه: "هو سلوك احتيالي قائم على ادعاء كاذب يدعمه الجاني بمظاهر خارجية مضلّلة، يُمارس بقصد خداع المجني عليه ودفعه طواعية إلى تسليم ماله، مما يُفضي في النهاية إلى استيلاء المحتال على مال الغير دون وجه حق."[2]

الاحتيال في الاصطلاح القانوني يُقصد به كل فعل ينطوي على الخداع والمكر، يُمارسه الجاني بقصد التأثير على إرادة المجني عليه وحمله على اتخاذ قرار لم يكن ليُقدم عليه لولا ذلك التأثير غير المشروع. ويتحقق الاحتيال عادة من خلال الكذب المقترن بوسائل خارجية توهم بالصدق، كاصطناع مستندات أو انتحال صفات أو تقديم معلومات مضللة[3]. والغرض من هذا السلوك الاحتيالي هو الاستيلاء على مال الغير دون وجه حق، تحت ستار قانوني

[1] طنطاوي ابراهيم أحمد، المرجع السابق، ص11.

[2] عبد العزيز بن عبد الرحمن الشمري، المرجع السابق، ص 178.

[3] عبيد علي، ناصر موفق، وآخرون، ماهية جريمة الاحتيال الإلكتروني، مجلة كلية القانون والعلوم السياسية، كلية الحقوق، جامعة تكريت، بغداد، العراق، المجلد 5، العدد 19، 2016، ص338.

أو واقعي زائف، مما يجعل من الجريمة عملاً مركبًا يقوم على الحيلة كسلوك مادي، وعلى نية التملك كسلوك معنوي.

الفرع الثاني: تعريف النصب والاحتيال في الفقه والقانون:

بعد الوقوف على المعنى اللغوي والاصطلاحي للنصب والاحتيال، أصبح من الضروري الانتقال إلى استعراض الكيفية التي تناول بها فقهاء القانون هذه الجريمة من حيث مضمونها وخصائصها، لا سيما في ظل تطور وسائل تنفيذها، خاصة عبر الفضاء الإلكتروني. كما تجدر الإشارة إلى أن التشريعات العربية، ومنها التشريع الجزائري، قد سعت إلى ضبط هذا النوع من السلوك الإجرامي بنصوص قانونية واضحة، تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجريمة ووسائل ارتكابها، وهو ما يُبرز أهمية التمييز بين التعريف الفقهي للجريمة وتعريفها القانوني الوضعي.

أولا: تعريف الفقه لجريمة النصب والاحتيال الالكتروني:

يرى فقهاء القانون أن جريمتي النصب والاحتيال تُعدّان من الجرائم الخطيرة التي تمس الذمة المالية للأفراد وتهدد الثقة في التعاملات المدنية والاقتصادية.

ويقصد بالنصب، وفقًا للطرح الفقهي، "كل فعل احتيالي يصدر عن الجاني بهدف الاستيلاء على مال مملوك للغير دون وجه حق، وذلك عن طريق استعمال وسائل تدليسية تتمثل في الكذب المقترن بمظاهر خارجية أو وقائع وهمية تُوهم المجني عليه بصدق ما يدعيه الجاني، مما يدفعه بمحض إرادته إلى تسليم المال[1]".

ويشترط في هذا السلوك الإجرامي أن يكون الغرض منه تملّك المال وليس مجرد حيازته المؤقتة، وهو ما يميز النصب عن بعض الجرائم الأخرى كخيانة الأمانة.

أما جريمة الاحتيال، فهي تتقاطع مع جريمة النصب في العديد من الجوانب، غير أنها تُركّز على الخداع كأسلوب رئيس، وتُعرّف بأنها: "سلوك ينطوي على استخدام وسائل غير

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، (جرائم ضد الأشخاص وجرائم ضد الأموال وبعض الجرائم الخاصة (الجزء الأول، دار هومة لطباعة والنشر والتوزيع، الجزائر، الطبعة 21، 2024، ص324.

مشروعة، كإخفاء الحقيقة أو تقديم بيانات كاذبة، بقصد خداع الغير وحمله على القيام بعمل أو الامتناع عن عمل، يترتب عليه إلحاق ضرر مادي أو معنوي بالمجني عليه وتحقيق منفعة للجاني أو للغير"[1].

وتُعد الحيلة والمناورة من أبرز خصائص هذه الجريمة، حيث تُمارَس بأساليب ذكية ومقنعة تضعف من قدرة الضحية على التحقق أو الشك.

وبهذا، فإن كلا الجريمتين تُعبران عن سلوك احتيالي منظم يهدف إلى الإضرار بحقوق الغير المالية عبر الخداع والتضليل، مع اختلاف نسبي في طبيعة الوسائل والنتائج المترتبة عن كل منهما.

ثانيا: التعريف القانوني لجريمتي النصب والاحتيال الالكتروني:

بعد الوقوف على المعنى اللغوي والاصطلاحي والفقهي لمفهومي النصب والاحتيال، يقتضي المنهج العلمي أن نتناول هذه الجريمة من الزاوية القانونية التي تجسّد موقف التشريعات الوضعية منها. ذلك أن تحديد المفهوم بدقة لا يكتمل إلا من خلال استعراض هذه الرؤى، لما لها من أثر في فهم الجريمة وتطبيق النصوص القانونية المتعلقة بها

وعليه تم تعريفها في القانون المصري على أنها تتحقق "متى توصل الجاني إلى الاستيلاء على مال مملوك للغير باستخدام طرق احتيالية، من بينها اتخاذ اسم كاذب أو صفة غير صحيحة، أو عن طريق إيهام المجني عليه بوجود مشروع وهمي، أو واقعة مزورة، أو إقناعه بتحقيق ربح خيالي".[2]

ويُفهم من هذا النص أن المشرع المصري قد ربط تمامًا بين قيام الجريمة ووجود وسيلة تدليسية يتّبعها الجاني بهدف التأثير على إرادة المجني عليه ودفعه إلى تسليم المال طواعية، معتقدًا في صحة الادعاءات المقدمة. فالخداع ليس مجرد عنصر شكلي، بل هو ركن جوهري

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

[2] بن الشيخ لحسين، مذكرة في القانون الجزائي الخاص، دار هومة، 2005، ص 187.

في بناء الجريمة، ويجب أن يكون هو السبب المباشر والدافع الحقيقي لتصرف المجني عليه، ما يجعل الركن المادي للجريمة يقوم على الفعل الاحتيالي المصحوب بالنية الإجرامية.

أما في القانون الفرنسي فعرفتها المادة 313-1 من قانون العقوبات الفرنسي على أن جريمة الاحتيال (Escroquerie) تُرتكب عندما يقوم الجاني بـ"خداع شخص طبيعي أو اعتباري، باستخدام اسم كاذب أو صفة غير صحيحة، أو عن طريق استغلال صفة حقيقية، أو باستخدام وسائل احتيالية، مما يدفع هذا الشخص إلى تسليم أموال أو ممتلكات أو تقديم خدمات، أو قبول التزام أو إبراء ذمة، مما يسبب له أو لطرف ثالث ضررًا"[1]. ويُعاقب على هذه الجريمة بالسجن لمدة تصل إلى خمس سنوات وغرامة تصل إلى 375,000 يورو.

في حين أن المشرع الجزائري، فقد سار في الاتجاه المصري، حيث نصت المادة 372 من قانون العقوبات على أن جريمة النصب تتحقق عندما يقوم الجاني بـ"الاستيلاء على مال الغير بواسطة التدليس، من خلال اتخاذ اسم كاذب أو صفة غير حقيقية، أو عن طريق إيهام الضحية بوجود مشروع زائف أو واقعة مختلقة"،[2] وهو ما يخلق انطباعًا زائفًا لدى الضحية يدفعه إلى التصرف في ماله تحت تأثير هذه الأكاذيب.

ويُشترط – كما في التشريع المصري – أن تكون هذه الوسائل الاحتيالية ذات أثر مباشر على إرادة المجني عليه، وأن تكون السبب الحاسم في إقناعه بالتخلي عن ماله، مما يعكس مدى اعتناء المشرّع الجزائري بركن الوسيلة التدليسية كعنصر قوام للجريمة.

في حين أن المشرع الفرنسي يُركّز على عنصر الخداع كركن أساسي في الجريمة، ويشترط أن يكون هذا الخداع هو الدافع المباشر لتصرف المجني عليه، سواء كان ذلك بتسليم المال أو تقديم خدمة أو قبول التزام، مما يبرز أهمية النية الإجرامية والوسائل الاحتيالية في تكوين الجريمة.

---

[1] بن الشيخ لحسين، المرجع السابق، ص 187.

[2] المادة 372 من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 يتضمن قانون العقوبات. (الجريدة الرسمية عدد 49 لسنة 1966) المعدل والمتمم بالقانون رقم 24-06 المؤرخ في 28 أبريل سنة 2024 (الجريدة الرسمية عدد 30 لسنة 2024)

من خلال استقراء مختلف التعاريف السابقة، يمكن استخلاص أن الاحتيال والنصب الإلكتروني يُعدان شكلاً من أشكال الخداع والاستغلال الذي يتم عبر شبكة الإنترنت، ويُنفذ من قبل أفراد ذوي خبرة عالية في مجال التقنيات الإلكترونية. يستغل هؤلاء المجرمون ثغرات الضحايا لإيقاعهم في فخ افتراضي محكم، بهدف الاستيلاء على أموالهم أو بياناتهم أو حتى ممتلكاتهم الخاصة، سعياً لتحقيق أرباح غير مشروعة بطرق سريعة. وغالباً ما تستند هذه الأفعال إلى انتحال الصفات واستغلال المناصب أو المراكز الحساسة التي يشغلها الضحايا، من أجل الوصول إلى معلومات ذات قيمة.

أما من الناحية القانونية، فإن المشرع الجزائري لم يضع تعريفاً مستقلاً لجريمة الاحتيال المعلوماتي، بل تناولها في إطار عام ضمن المادة 372 من قانون العقوبات، والتي تنص على تجريم كل من يستخدم طرقاً احتيالية كاستعمال أسماء وصفات كاذبة أو خلق آمال أو وقائع وهمية، من أجل الاستيلاء على أموال الغير أو بعض ممتلكاتهم، وهو ما يمكن أن يُسقط أيضاً على الأفعال الاحتيالية التي تُرتكب بواسطة التقنيات الحديثة.

ويُميز الفقه بين نوعين من الجرائم المعلوماتية ذات الصلة بالاحتيال[1]:

1. الجرائم المرتكبة بواسطة الكمبيوتر: حيث يُستخدم الجهاز كوسيلة لتنفيذ الجريمة، مثل الاستعمال غير المشروع لبطاقات الائتمان أو البطاقات الممغنطة.

2. الجرائم الواقعة على الكمبيوتر: حيث يكون الجهاز نفسه أو ما يحتويه من بيانات ومعلومات هو محل الاعتداء، ويشكل موضوعاً مباشراً للجريمة.[2]

وبناءً على ذلك، يُمكن تحديد العناصر التي تقوم عليها جريمة الاحتيال المعلوماتي كما يلي:

*الموضوع: يتمثل في البيانات والبرمجيات والمعلومات المُخزنة داخل النظام المعلوماتي.

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبيانات المعالجة الالكترونية، مؤتمر دولي، الطبعة 3، الإمارات العربية المتحدة، 2004، ص20.

[2] محمد عبد الله أبوبكر سلامة، جرائم الكمبيوتر والانترنت، منشأة المعارف، الاسكندرية، 2006، ص116.

*الدعامة: وهي النظام المعلوماتي ذاته، الذي يُستغل كبيئة لارتكاب الجريمة.

*الأداة: وتتمثل في استخدام الجهاز أو الشبكة كوسيلة لخرق النظام أو استخراج معلومات سرية، كأرقام البطاقات أو الحسابات[1].

ونظراً للتطور المتسارع في تكنولوجيا المعلومات، فقد أصبحت هذه الجرائم أكثر انتشاراً وخطورة، لما تسببه من خسائر اقتصادية كبيرة وتهديدات لسرية البيانات ومصالح الأفراد والمؤسسات، خاصة في ظل توسع التجارة الإلكترونية وانتشار منصات التواصل الاجتماعي.

ومن هنا يمكن تقديم تعريف جامع لجريمة الاحتيال المعلوماتي بأنها: "كل استخدام غير مشروع لوسائل إلكترونية أو معلوماتية، كالغش أو الخداع أو التلاعب بالبيانات الرقمية، بهدف الحصول على معلومات سرية أو منافع مالية أو اختراق الأنظمة الحاسوبية أو الشبكات الإلكترونية، مما يشكل انتهاكاً للقانون واعتداءً على حقوق ومصالح الغير، سواء في بيئة رقمية أو افتراضية"[2].

المطلب الثاني: أركان جريمة النصب والاحتيال الالكتروني:

تُعد جريمة النصب والاحتيال الإلكتروني من الجرائم المركبة التي لا تقوم إلا بتوافر مجموعة من الأركان الجوهرية التي تُشكل بنيتها القانونية، والتي لا يمكن مساءلة الفاعل عنها ما لم تتحقق مجتمعة. وكغيرها من الجرائم، تقوم جريمة الاحتيال المعلوماتي على ركنين أساسيين: الركن المادي الذي يتجسد في السلوك الإجرامي المتمثل في استعمال وسائل احتيالية عبر الوسائط الإلكترونية، والركن المعنوي الذي يتمثل في القصد الجنائي للفاعل، أي العلم والإرادة في ارتكاب الفعل غير المشروع بقصد تحقيق منفعة غير مستحقة أو الإضرار بالغير.

وسنتناول هذين الركنين بشيء من التفصيل في فرعين مستقلين، حيث نُخصص الفرع الأول لدراسة الركن المادي بما يشمله من أفعال وأساليب تقنية تُستخدم في تنفيذ الجريمة،

[1] Mohamed Chawki, Essai sur la notion de cybercriminalité, Institut Européen des Hautes Etudes Internationales IEHEI,France, juillet 2006, p23.

[2] نهال عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، القاهرة، 2008، ص 168.

بينما نُخصص الفرع الثاني لتحليل الركن المعنوي الذي يُمثل القصد الجنائي الواجب توافره لمساءلة الجاني عن فعله الإجرامي.

الفرع الأول: الركن المادي لجريمة النصب والاحتيال الالكتروني:

تقوم الجريمة عمومًا على ثلاثة عناصر أساسية ضمن الركن المادي، وهي: السلوك الإجرامي، النتيجة، والعلاقة السببية. وبما أن جريمة الاحتيال المعلوماتي تتداخل بين الاحتيال التقليدي والجريمة المعلوماتية، فإن دراستها تقتضي بيان مكونات الركن المادي لكل منهما.

أولا: السلوك الإجرامي (وسائل التدليس والاحتيال):

نصت المادة 372 من قانون العقوبات الجزائري على الأفعال التي تُشكّل السلوك الإجرامي في الاحتيال، والتي يمكن تلخيصها في:

الكذب: يتمثل في تقديم معلومات زائفة على أنها حقيقية، سواء شفويًا أو كتابيًا. على سبيل المثال، ادّعاء شخص امتلاكه لقدرات خارقة كالشفاء من الأمراض أو التنبؤ بالمستقبل لإقناع الضحايا، مما يدفعهم لتسليمه أموالًا أو ممتلكا[1].

المظاهر الخارجية المصاحبة للكذب: لا يكفي الكذب وحده لقيام الاحتيال، بل يجب أن يكون مدعومًا بوسائل أو أساليب ظاهرية توهم المجني عليه بمصداقيته، ومنها:

- ✓ الاستعانة بشخص آخر لتأكيد الرواية الاحتيالية.
- ✓ استخدام أوراق أو مستندات صحيحة أو مزورة.
- ✓ استغلال وسائل الإعلام والنشر لنشر معلومات مضللة.
- ✓ انتحال صفة صحيحة (كصفة موظف رسمي أو طبيب).
- ✓ أداء تمثيليات توهم بالمكانة أو السلطة.
- ✓ القيام بأعمال مادية تُوهم بوجود مشروع فعلي.
- ✓ استغلال وقائع ناقصة لإقناع الضحية. [2]

[1] فاطمة الزهراء رمضاني، علي بدراني، القصور التشريعي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، الجزائر، المجلد 07، العدد 02، 2022، ص 866.

[2] المرجع نفسه، ص 867.

ويتمثل هذا الركن في جريمة النصب والاحتيال الالكتروني في قيام الجاني باستخدام وسائل إلكترونية أو رقمية بهدف خداع المجني عليه واستغلال جهله أو ثقته. ومن أبرز هذه الوسائل: الرسائل الاحتيالية عبر البريد الإلكتروني Phishing المواقع الإلكترونية الوهمية، الحسابات المزورة على شبكات التواصل الاجتماعي، أو التطبيقات المزيفة. وغالبًا ما تتضمن هذه الوسائل ادعاءات كاذبة مثل الفوز بجائزة، أو ضرورة تحديث معلومات بنكية، أو طلب مساعدة مالية مستعجلة.[1]

ثانيا: النتيجة الإجرامية:

تتمثل النتيجة الإجرامية في جريمة الاحتيال بقيام المجني عليه بتسليم مال أو منقول للجاني، بناءً على اقتناعه بصحة الوقائع الكاذبة التي عرضها هذا الأخير، سواء كانت هذه الوقائع في شكل أقوال كاذبة، أو سلوكيات مصطنعة تدعمها مظاهر خارجية توحي بالصدق. ويُعدّ عنصر التسليم جوهريًا لتمييز جريمة الاحتيال والنصب عن غيرها من الجرائم التي تمس الذمة المالية، وعلى رأسها جريمة السرقة، إذ أن التسليم في الاحتيال والنصب يتم بموافقة المجني عليه، وإن كانت هذه الموافقة قائمة على غش وخداع أفقداه الإدراك والتمييز السليم.[2] أما في السرقة، فإن الاستيلاء على المال يتم خلسة أو باستخدام القوة، دون علم أو رضا من المجني عليه.

وتكمن خطورة هذه النتيجة في أن الجاني لا يستخدم العنف المادي بل يعتمد على وسائل نفسية ومعنوية، مما يجعل الضحية يتصرف بإرادته تحت تأثير الخداع. وهو ما يجعل القانون يتعامل مع هذه النتيجة بكثير من الجدية، نظرا لما تسببه من مساس مباشر بمصالح الأفراد الاقتصادية وبالثقة في التعاملات المدنية والمالية.[3]

ثالثا: العلاقة السببية:

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص ص 120 121.

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

[3] المرجع نفسه، ص64.

تُعد العلاقة السببية أحد الأركان الأساسية في الركن المادي لجريمة الاحتيال، إذ يُشترط لقيام هذه العلاقة أن يكون تسليم المال أو المنقول نتيجة مباشرة ومترتبة على الأفعال الاحتيالية التي ارتكبها الجاني[1]. ويقصد بالعلاقة السببية أن تكون الأفعال الاحتيالية هي التي دفعت المجني عليه إلى اتخاذ قرار التسليم، أي أن هذا التسليم لم يكن ليحدث لولا تلك الأفعال أو الوسائل الخادعة.

ولكي تتحقق هذه العلاقة، يجب توافر ثلاثة شروط رئيسية:[2]

أ- أن يكون التسليم قد تم بفعل الوسائل الاحتيالية:

يجب أن تكون الوسائل المستعملة من قبل الجاني – سواء كانت أقوالًا كاذبة أو مظاهر خادعة أو وثائق مزيفة – هي التي أنتجت الأثر المباشر في نفس المجني عليه، وأقنعته بصحة المزاعم المقدمة، مما دفعه إلى تسليم المال أو المنقول.

ب- أن يكون المجني عليه جاهلًا بالحقيقة:

فلو كان الضحية على علم بالحقيقة، أو كان متحفظًا في قراره، فإن عنصر العلاقة السببية ينهار، ولا تتحقق الجريمة في شكلها الكامل. إذ يجب أن يكون الجهل بالحقيقة ناتجًا عن الاحتيال، لا عن إهمال من المجني عليه أو تفريط منه في التحقق.

ج -أن **تكون الأفعال الاحتيالية السبب المباشر لاتخاذ قرار التسليم:**

أي أن يكون هناك ترابط زمني ومنطقي بين الفعل الاحتيالي وقرار التسليم. فإذا تدخل سبب أجنبي أو مؤثر خارجي آخر، فإن العلاقة السببية تنقطع، ولا يمكن مساءلة الجاني عن النتيجة التي لم تترتب مباشرة عن فعله.

في سياق الجرائم المعلوماتية، تتجلى هذه العلاقة عندما يقع المجني عليه ضحية للخداع الرقمي، كأن يستجيب لرسالة إلكترونية توهمه بربح جائزة ويقوم بتحويل مبلغ مالي أو

[1] مجموعة مؤلفين، جرائم الاحتيال والإجرام المنظم، الطبعة ،01 جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2008، ص 13.

[2] أسامة حمدان الرقب، المرجع السابق، ص 53.

تقديم بياناته البنكية. فإذا ثبت أن قرار المجني عليه بالتسليم لم يكن ليقع لولا الأفعال الاحتيالية التي مارسها الجاني باستخدام وسائل رقمية، فإن العلاقة السببية تُعد متحققة، وتقوم بذلك أركان الجريمة بكاملها[1].

وتجدر الإشارة إلى أن إثبات الركن المادي في النصب الإلكتروني قد يكون أكثر تعقيدًا من النصب التقليدي، نظراً لغياب التفاعل المادي المباشر بين الجاني والضحية، ولجوء الجناة إلى أدوات رقمية يصعب تتبعها. ولهذا فإن مهمة القاضي الجنائي تتطلب دقة كبيرة في تحليل الأدلة الإلكترونية وربط الوقائع ببعضها لإثبات أن الوسيلة الاحتيالية كانت السبب الحقيقي الذي دفع المجني عليه إلى التسليم[2].

الفرع الثاني: الركن المعنوي:

لكي تُعتبر الجريمة قائمة في القانون، لا يكفي توافر الركنين الشرعي والمادي فقط، بل لا بد من وجود صلة تربط بين الجاني والفعل الإجرامي الذي ارتكبه، وتتمثل هذه الصلة في الركن المعنوي. وبما أن جريمة الاحتيال المعلوماتي تُعد من الجرائم العمدية، فإن تحقق هذا الركن يستلزم توفر عنصرين أساسيين: العِلم بالفعل غير المشروع والإرادة في ارتكابه بقصد تحقيق نتيجة معينة.

***العلم بعملية الاحتيال:**

لكي تتحقق جريمة الاحتيال، يجب أن يكون الجاني مدركًا تمامًا بأنه يمارس سلوكًا ينطوي على الكذب والخداع. فعلى سبيل المثال، إذا قام الجاني بالتصرف في منقول لا يملكه مع علمه بذلك، فإن هذا الوعي يُثبت قيام الركن المعنوي للجريمة، لعلمه بأن أفعاله تنطوي على مخالفة قانونية واضحة[3].

---

[1] حسين الدعدي، "أركان الجريمة المعلوماتية في النظام السعودي"، تم الاطلاع عليه بتاريخ 11-04-2025، الساعة 02:22، متوفر على الموقع الإلكتروني: https://lawfirm-hd.com.

[2] علي إبراهيم بن دراج، محاضرات في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط،2021، ص 15.

[3] أسامة حمدان الرقب، المرجع السابق، ص 69.

وعلى العكس من ذلك، إذا لم يكن الجاني على علم بأن تصرفه غير قانوني ولم يستخدم وسائل خداع لتضليل الغير، فإن العنصر المعنوي للجريمة ينتفي، ولا يمكن مساءلته جنائيًا عن الاحتيال.

*** العلم بالجريمة المعلوماتية:**

لا يكفي أن يقوم الشخص بفعل ما في مجال تقنيات المعلومات حتى يُتهم بارتكاب جريمة معلوماتية، بل يجب أن تتوافر لديه نية ارتكاب ذلك الفعل، أي أن يكون على علم بأن ما يقوم به يُعد مخالفة للقانون، وأن يكون قادرًا على تنفيذه عمدًا[1].

وتتحقق النية الإجرامية فقط عندما يعلم الفاعل بأن سلوكه مجرم قانونًا. أما إذا دخل شخص إلى نظام معلوماتي لأغراض مسموح بها – كالتصفح – ونتيجة جهله بالتقنيات ارتكب خطأ أدى إلى إلحاق ضرر بشخص طبيعي أو معنوي، فإن المسؤولية في هذه الحالة تكون عن خطأ غير مقصود، ولا تُكيّف الجريمة على أنها عمدية.[2]

[1] حسين الدعدي، المرجع السابق، نفس تاريخ الاطلاع والتوقيت.

[2] المرجع نفسه.

المبحث الثاني

أنواع جرائم النصب والاحتيال الالكتروني وخصائصها

تُعد جرائم الاحتيال والنصب الإلكتروني من أبرز التحديات التي فرضها التطور التكنولوجي، نظرًا لتنوع أساليبها وسرعة انتشارها. فقد اتخذت هذه الجرائم أشكالًا متعددة تستهدف الأفراد والمؤسسات عبر الوسائط الرقمية. ويكتسي التعرف على أنواعها **(المطلب الأول)**، وخصائصها **(المطلب الثاني)** أهمية بالغة لفهم طبيعتها القانونية وأساليب مكافحتها. وعليه، يُعنى هذا المبحث ببيان التصنيفات المختلفة لهذه الجرائم وسماتها المميزة.

المطلب الأول: أنواع جرائم الاحتيال والنصب الالكتروني:

تمثل جرائم الاحتيال والنصب الإلكتروني أحد أبرز أنماط الجرائم المستحدثة التي أفرزها التطور الرقمي، حيث أضحت تعتمد على وسائل تقنية متطورة لارتكاب أفعال إجرامية تهدف إلى الاستيلاء على أموال الغير أو بياناتهم بطرق احتيالية. وبفعل تنوع أساليبها وتعدد صورها، بات من الضروري التطرق إلى أبرز أنواع هذه الجرائم، لفهم طبيعتها القانونية وتحديد سبل التصدي لها.

الفرع الأول: الاحتيال الإلكتروني القائم على وسائل الاتصال الرقمية:

هذا النوع يعتمد على استخدام وسائل الاتصال الحديثة لاستدراج الضحية وإقناعه بمعلومات زائفة تؤدي به إلى تسليم مال أو بيانات شخصية. وتتنوع أساليبه كما يلي:

أولا: الاحتيال والنصب عبر البريد الإلكتروني (Phishing):

يُعد هذا النوع من الاحتيال الإلكتروني من أكثر الأساليب شيوعًا وخطورة، حيث يعتمد على خداع الضحية نفسيًا وتقنيًا معًا. يقوم الجاني بإرسال رسالة بريد إلكتروني تبدو حقيقية

تمامًا، من حيث الشعار، التصميم، وحتى عنوان البريد الإلكتروني،[1] بحيث توحي بأنها واردة من جهة موثوقة مثل:

- بنك محلي أو دولي،
- موقع تسوّق إلكتروني معروف،
- هيئة حكومية،
- أو حتى مزوّد خدمات الإنترنت أو البريد الإلكتروني.

غالبًا ما تتضمن رسائل الاحتيال عبر البريد الإلكتروني عناصر تثير القلق أو تدفع إلى اتخاذ قرار سريع دون تفكير. ومن أبرز الأساليب المستعملة في هذه الرسائل: التحذير من إغلاق الحساب البنكي خلال فترة زمنية قصيرة (مثلاً 24 ساعة) في حال عدم تحديث البيانات، أو إشعار بوجود تحويل مالي بانتظار التأكيد، أو حتى إبلاغ الضحية بأنه فاز بجائزة كبيرة تتطلب "تفعيلًا" عبر رابط معين.[2] هذه العبارات المصاغة بعناية تهدف إلى دفع الضحية نحو اتخاذ رد فعل سريع دون التحقق من مصدر الرسالة.

عادة ما تتضمن هذه الرسائل رابطًا يبدو في ظاهره شرعيًا ويحاكي عناوين المواقع الأصلية بدقة، مثل: www.yourbank.com، لكنه في الواقع رابط مزيف يقود إلى موقع إلكتروني مصمم بعناية ليطابق الموقع الرسمي للمؤسسة المستهدفة. يُعد هذا الموقع أداة أساسية في الاحتيال، إذ يُستخدم لجمع المعلومات الحساسة من الضحية.[3]

بمجرد أن يقوم المستخدم بإدخال بياناته الشخصية أو المصرفية – مثل رقم الحساب، كلمة المرور، أو رمز التحقق – تُرسَل هذه المعلومات مباشرة إلى المحتال. بعد ذلك، يستغل الجاني هذه البيانات بطرق متعددة، كأن يقوم بسحب الأموال من

[1] مقال الكتروني بعنوان التسوق في الجزائر منظمة تحذر من الاحتيال، في مجلة الحرة، على الموقع https://www.maghrebvoices.com/algeria/2022/12/20/تم الاطلاع عليه بتاريخ 2025/04/16، بتوقيت: 6:09.

[2] مقال الكتروني بعنوان أنواع الاحتيال الالكتروني في المملكة، في مجلة law firm ، . في الموقع https://etqanlawfirm-sa.com/ تم الاطلاع عليه بتاريخ 2024/04/16، بتوقيت: 6:58.

[3] المرجع نفسه.

الحساب المصرفي، أو بيع المعلومات على السوق السوداء الرقمية، أو حتى استخدام الحساب في أنشطة إجرامية أخرى مثل غسل الأموال أو شراء منتجات وخدمات بطرق احتيالية.[1]

هذه العملية الخادعة تمثل تهديدًا حقيقيًا لأمن الأفراد الرقمي، وتبرز الحاجة إلى توعية مستمرة حول كيفية التحقق من الرسائل الإلكترونية المشبوهة.

ثانيا: الاحتيال عبر الرسائل النصية أو تطبيقات الدردشة:

يُعد هذا النوع من الاحتيال من أكثر الأساليب شيوعًا وانتشارًا بسبب سهولة الوصول إلى الأفراد عبر هواتفهم المحمولة. يتلقى الضحية رسالة نصية قصيرة (SMS) أو إشعارًا عبر تطبيقات التراسل الفوري مثل "واتساب"، "فايبر" أو "ماسنجر"، يتضمن مضمونًا مثيرًا أو مقلقًا، مثل الفوز بجائزة مالية مغرية أو وجود خلل في الحساب البنكي يتطلب تدخلاً عاجلًا.[2] وتحت ضغط الاستعجال، يُطلب من الضحية إما الاتصال برقم معين يُدار من طرف الجاني، أو النقر على رابط يؤدي إلى موقع مشبوه.

في كثير من الحالات، يؤدي النقر على الرابط إلى تحميل برمجيات خبيثة (malware) على جهاز المستخدم، تمكن الجاني من مراقبة نشاطه أو سرقة بياناته. وفي حالات أخرى، يُطلب من الضحية إدخال معلومات حساسة مثل أرقام بطاقات الائتمان أو كلمات المرور، والتي تُستخدم لاحقًا في تنفيذ عمليات مالية غير مشروعة[3].

في القانون الجزائري، يُمكن تكييف هذا السلوك في إطار جريمة الاحتيال الإلكتروني المنصوص عليها في المادة 394 مكرر من قانون العقوبات، والتي تجرّم

---

[1] مقال الكتروني بعنوان التسوق في الجزائر منظمة تحذر من الاحتيال ، المرجع السابق.

[2] مقال الكتروني بعنوان بطرق الاحتيال والوقاية منها، على الموقع: https://www.kuveytturk.com.tr/ar/d"gita'-banking/security/avoiding-scams-and-frauds تاريخ الاطلاع: 2025/04/17، بتوقيت 3:00.

[3] نسيم رمضان، عمليات الاحتيال الالكتروني، صحيفة الشرق الأوسط الالكترونية، تاريخ تحرير المقال 2024، على الموقع https://aawsat.com/% تم الاطلاع عليها بتاريخ: 2025/04/17، بتوقيت 4:56.

كل من يستخدم الوسائل التقنية لخداع الغير من أجل الحصول على منافع مالية غير مشروعة[1].

ثالثا: انتحال الهوية على مواقع التواصل الاجتماعي:

تُعد جريمة انتحال الهوية واحدة من الجرائم الإلكترونية المتطورة التي تستغل الانتشار الواسع لمواقع التواصل الاجتماعي. في هذا السياق، يقوم الجاني بإنشاء حساب مزيف ينتحل فيه صفة شخص معروف (مثل شخصية عامة أو قريب للضحية) أو مؤسسة رسمية (مثل بنك، شركة توظيف، جمعية خيرية).[2] يستخدم هذا الحساب للتواصل مع الضحية في محاولة لاكتساب ثقته، ثم يبدأ في طلب مبالغ مالية لأغراض وهمية (مثل مساعدة طارئة، دفع رسوم، استثمار مربح...) أو للحصول على معلومات سرية يمكن استغلالها لاحقًا.

ما يزيد من خطورة هذا النوع من الاحتيال هو أن الجاني قد يستخدم صورًا ومعلومات حقيقية عن الشخص المنتحَل لتحقيق مصداقية أكبر، وهو ما يؤدي إلى وقوع الضحية في الفخ بسهولة.[3]

وفقًا للتشريع الجزائري، فإن انتحال الهوية الرقمية يُعد جريمة منصوصًا عليها في المادة 67 من قانون الوقاية من الجرائم المعلوماتية ومكافحتها، والتي تُجرّم الاستعمال غير المشروع لهوية الغير عبر الوسائط الإلكترونية، خاصة إذا كان ذلك بقصد الإضرار أو الاحتيال[4].

[1] الامر: رقم 66-156 المتضمن قانون العقوبات، المرجع السابق.

[2] محمد مهدي عجمي، جريمة الانتحال الشخصية في مواقع التواصل الاجتماعي، مجلة النشر العلمي، العدد 130، 2022، ص 191.

[3] نسيم رمضان، المرجع السابق.

[4] الامر رقم 66-156، المتضمن قانون العقوبات، المرجع السابق.

كلا النوعين يُظهران كيف أن التطور التكنولوجي قد وفر للمحتالين أدوات جديدة لارتكاب أفعالهم الإجرامية بطرق خفية يصعب كشفها دون خبرة رقمية وتحقيق تقني معمق، مما يفرض على المشرّع والقضاء تعزيز آليات الردع والوقاية في هذا المجال.

الفرع الثاني: الاحتيال الإلكتروني القائم على استغلال الأنظمة والمواقع

هذا النوع أكثر تعقيدًا من حيث الأسلوب، ويعتمد على استغلال تقنيات في اختراق الأنظمة أو تصميم منصات إلكترونية وهمية لخداع الضحايا، ومن أبرز أنواعه:

أولا: المواقع والتطبيقات الوهمية

في هذا النوع من الاحتيال، يقوم الجاني بتصميم موقع إلكتروني أو تطبيق ذكي يُشبه إلى حدّ كبير موقعًا معروفًا وموثوقًا، كأن يكون موقع بنك، متجر إلكتروني، أو حتى منصة خدمات حكومية. ويحرص المحتال على تقليد كل تفاصيل الواجهة الأصلية، بما في ذلك الشعارات والعناوين والألوان، مما يُعطي الانطباع بأنه موقع رسمي وشرعي.[1]

يتم الترويج لهذا الموقع أو التطبيق المزيف عبر وسائل التواصل الاجتماعي، الرسائل النصية، الإعلانات المدفوعة، أو البريد الإلكتروني. وعند زيارة الضحية لهذا الموقع، يُطلب منه إدخال بياناته البنكية أو إتمام عملية شراء. بعد تنفيذ العملية، يكتشف الضحية أن الأموال قد سُحبت دون أن يحصل على أي منتج أو خدمة.[2]

في القانون الجزائري، يُعد هذا الفعل من صور "النصب المعلوماتي"، ويُمكن تكييفه ضمن المادة 394 مكرر من قانون العقوبات، التي تُعاقب كل من استخدم وسيلة إلكترونية لخداع الغير بهدف تحقيق ربح غير مشروع. كما يندرج ضمن جرائم "انتحال المواقع" أو "استعمال علامات مضلّلة"، والتي تتطلب رقابة رقمية صارمة وتعاونًا دوليًا لتفكيكها.[3]

---

[1] مقال الكتروني بعنوان التسوق في الجزائر منظمة تحذر من الاحتيال ، المرجع السابق.

[2] المرجع نفسه.

[3] الامر رقم 66-156 المتضمن قانون العقوبات، المرجع السابق.

ثانيا: اختراق الأنظمة البنكية أو حسابات الدفع الإلكتروني:

هذا النوع من الجرائم يعتمد على خبرة تقنية عالية، وغالبًا ما يُرتكب من طرف أفراد أو شبكات متخصصة في الهجمات السيبرانية. يستهدف الجناة قواعد بيانات البنوك أو أنظمة الدفع الإلكتروني (مثل Western Union،PayPal ، أو التطبيقات البنكية)، ويستغلون ثغرات أمنية لاقتحامها وسرقة بيانات العملاء وتحويل الأموال بشكل غير شرعي إلى حسابات وهمية أو خارجية.[1]ومثل هذه الهجمات تكون معقدة من حيث التنفيذ والتتبع، وغالبًا ما تستهدف ليس فقط الأفراد، بل المؤسسات المالية والاقتصادية، ما يُسبب خسائر جسيمة ويُهدد الأمن المالي.

وفقًا للتشريع الجزائري، يمكن اعتبار هذه الجريمة ضمن "جرائم الوصول غير المشروع إلى نظم المعلومات"، والتي يُعاقب عليها في القانون 18-04 المؤرخ في 10 مايو 2018، والمتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها، لاسيما في مواده من 10 إلى 13 التي تُجرّم كل من يتعدى أو يُخترق نظم المعلومات المحمية.[2]

ثالثا: برامج خبيثة (Malware) وبرمجيات الفدية (Ransomware):

تُعد هذه البرامج أحد أخطر أدوات الجريمة الإلكترونية، حيث يقوم الجاني بإرسال ملف خبيث عبر البريد الإلكتروني، أو ضمن رابط، أو من خلال موقع إلكتروني مزيف، وبمجرد فتحه أو تحميله، يتم تثبيت البرنامج تلقائيًا على جهاز الضحية دون علمه.[3]

---

[1]شايب محمد، آليات الحماية من الغش في وسائل الدفع الالكتروني، مجلة نماء للاقتصاد والتجارة، جامعة جيجل،المجلد 1، العدد 2، 2017، ص 8.

[2]القانون رقم 18-04 المؤرخ في 10 مايو 2018، والمتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها، الجريدة الرسمية الجمهورية الجزائرية عدد 5، الصادرة بتاريخ: 16 أوت 2018.

[3]رؤى حمود، مقال بعنوان فيروس الفدية: المهاجم الأخطر للمؤسسات في العصر الرقمي، 2021، مجلة مجموعة ريناد المجد لتقنية المعلومات، على الموقع https://www.rmg-sa.com/%/تاريخ الاطلاع 2025/04/17، بتوقيت 8:21.

تتنوع أهداف هذه البرامج بين سرقة البيانات (مثل كلمات السر، ملفات العمل، الصور الشخصية...)، مراقبة نشاط المستخدم، أو تشفير الملفات كليًا ومطالبة الضحية بدفع مبلغ مالي (فدية) مقابل استعادتها، وهو ما يُعرف بـ برمجيات الفدية Ransomware[1].

ويُمكن أن تُصيب هذه الهجمات الأفراد، المؤسسات، الشركات، بل وحتى البنى التحتية الرقمية في الدولة، مما يجعلها جريمة ذات طابع خطير قد تدخل ضمن نطاق الجرائم الموجهة ضد أمن الدولة الرقمي.

قانونيًا في الجزائر، تُجرّم المادة 16 من القانون 18-04 نشر أو استخدام البرامج الخبيثة التي تهدف إلى إلحاق الضرر بالمعلومات أو النظام، وتُشدَّد العقوبة إذا استهدف الفعل جهة رسمية أو اقتصادية حساسة.[2]

تُبرز هذه الأنواع الثلاثة من الجرائم التحديات المتزايدة التي تفرضها التكنولوجيا على أنظمة العدالة والأمن، ما يستدعي تحديثًا دائمًا للترسانة القانونية وتطويرًا مستمرًا للمهارات الفنية لدى الجهات المختصة.

المطلب الثاني: خصائص جرائم النصب والاحتيال وتمييزها عما يشابهها:

تتميّز جريمة الاحتيال والنصب الإلكتروني بخصائص تجعلها مختلفة عن الجرائم التقليدية، سواء من حيث الوسائل المستعملة أو طبيعة ارتكابها. فهي تُرتكب عبر بيئة رقمية معقّدة يصعب تتبعها، وتتسم بالخفاء والسرعة والقدرة على تجاوز الحدود الجغرافية. كما تعتمد على مهارات تقنية متقدمة، مما يضفي عليها طابعًا خاصًا يستدعي دراسة معمقة لتمييزها عن غيرها من الجرائم.

الفرع الأول: خصائص جرائم النصب والاحتيال الالكتروني:

تتميز جريمة الاحتيال والنصب الإلكتروني عبر شبكة المعلومات الدولية بجملة من الخصائص التقنية والقانونية التي تميزها عن الجرائم التقليدية، ويمكن إبراز أبرزها كما يلي:

[1] رؤى حمود، المرجع السابق.

[2] القانون رقم 04-18 المتضمن الوقاية من من الجرائم المعلوماتية والوقاية منها، المرجع السابق.

أولا. البيئة الرقمية الإلكترونية:

أبرز ما يميز جريمة الاحتيال الإلكتروني هو وقوعها ضمن بيئة افتراضية تعتمد على الحواسيب وشبكات الإنترنت، حيث تُرتكب باستخدام إشارات إلكترونية غير مرئية تنتقل بين الأنظمة المعلوماتية. وتعتمد هذه الجريمة بشكل أساسي على استغلال الثغرات ونقاط الضعف في البنية التحتية الرقمية وتكنولوجيا المعلومات[1].

ثانيا: صعوبة الاكتشاف وبساطتها النظرية:

تستغرق عمليات الاحتيال الإلكتروني عادة وقتاً طويلاً قبل اكتشافها، وغالبًا لا يُكشف عنها إلا عبر عمليات تدقيق تقنية دقيقة أو تبليغ عرضي من الضحايا. وعلى الرغم من خطورتها، إلا أنها تُعد بسيطة من الناحية النظرية، حيث يمكن لفرد واحد يمتلك مهارات تقنية متقدمة أن ينفّذ هذه الجريمة بسهولة من خلال تتبّع الثغرات الإلكترونية واستغلالها لخداع ضحيته.[2]

ثالثا: التخفي وسرعة التنفيذ:

تتسم هذه الجريمة بطابعها الخفي، إذ قد تُرتكب في حضور الضحية دون أن يدرك ذلك، كأن يتصفح موقعًا مزيفًا أو يفتح رابطًا خبيثًا دون علمه. ويعتمد المحتال الإلكتروني على خبراته التقنية العالية لإتمام عملية النصب بدقة وسرعة، باستخدام وسائل متقدمة مثل الفيروسات، وسرقة البيانات البنكية، والتجسس، وتشفير الملفات مقابل فدية[3].

رابعا: الطابع العابر للحدود:

---

[1] عرب يونس، موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، الجزء الأول، اتحاد المصارف العربية، 2002، ص 234.

[2] منشاوي محمد عبد الله، جرائم الانترنيت من منظور شرعي وقانوني، مكة المكرمة، 2002، ص123.

بحث منشور على الرابط: http://www.khayma.com/education-technology/Study33.htm

[3] إبراهيم حسني عبد السميع، الجرائم المستحدثة عن طريق الانترنت، القاهرة، دار النهضة العربية. 2011، ص ص 133 .134

بفعل الطابع العالمي لشبكات المعلومات، لم تعد هناك حدود جغرافية تشكّل عائقًا أمام ارتكاب الجريمة الإلكترونية. فبإمكان الجاني تنفيذ عمليته من دولة ما بينما يكون الضحية في دولة أخرى، مما يجعل جريمة الاحتيال الإلكتروني تتصف بالعالمية وتُحدث آثارًا متزامنة في مناطق متعددة من العالم[1].

إلى جانب خصائصها العامة، تنفرد جريمة الاحتيال والنصب الإلكتروني بعدة سمات تجعلها من أكثر الجرائم الرقمية تعقيدًا، من أبرزها:

أولا: الاعتماد الكامل على الحاسوب وشبكة الإنترنت:

يُعد الحاسب الآلي الأداة الأساسية لارتكاب هذه الجريمة، حيث يتم من خلاله الدخول إلى شبكة المعلومات الدولية وتنفيذ عمليات الاحتيال بمختلف صورها، وهو ما يجعل الجريمة مرتبطة عضوياً بالتكنولوجيا ولا تُمارس إلا من خلال وسيط إلكتروني[2].

ثانيا: استهداف مؤسسات حساسة وذات طابع مالي:

غالبًا ما تُوجّه عمليات الاحتيال الإلكتروني إلى جهات ذات طابع مالي واقتصادي كالبنوك، والمؤسسات الصناعية، والمتاجر الإلكترونية، نظرًا لقيمتها المادية وسهولة استهدافها إلكترونيًا. وهذا ما دفع العديد من هذه المؤسسات إلى تطوير نظم أمن إلكتروني متقدمة للحد من الخسائر المحتملة[3].

ثالثا: احتراف مرتكبي الجريمة في مجال الحوسبة:

يرتكب هذه الجرائم عادة أشخاص يتمتعون بكفاءة عالية في مجال البرمجة وهندسة الشبكات ونظم الحماية، حيث يمتلكون المعرفة التي تمكّنهم من التسلل إلى

---

[1] الصغير جميل عبد الباقي، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، القاهرة، دار النهضة العربية، 2001، ص123.

[2] الخن محمد طارق، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، مصر، الطبعة الأولى، 2011، ص 68.

[3] المرجع نفسه، ص17.

الأنظمة والتلاعب بالبيانات دون أن يُكشف أمرهم بسهولة. وغالبًا ما تبدأ التحقيقات الأمنية في مثل هذه الجرائم بالبحث بين خبراء الحاسوب[1].

رابعا: التحكم في المعلومات واستغلالها:

غالبًا ما يكون مرتكبو الاحتيال الإلكتروني ممن يملكون حق الوصول إلى البيانات، سواء أثناء إدخالها أو معالجتها أو تخزينها. ويستغلون هذا الامتياز في تنفيذ عملياتهم الاحتيالية، وتحقيق مكاسب غير مشروعة من خلال التلاعب بالمعلومات أو تحويل الأموال بشكل غير قانوني[2].

الفرع الثاني: تمييز جرائم النصب والاحتيال الالكتروني عما يشابهها من الجرائم الأخرى:

تتشابه جريمة الاحتيال عبر شبكة المعلومات الدولية مع جريمة الاحتيال التقليدية في العديد من الجوانب، حيث تعتمد كلتاهما على وسائل الغش والخداع. كما أن الهدف في كلا الجريمتين هو الاستيلاء على أموال الغير بنية التملُّك وحرمان صاحب المال منها، وتعتمد الجريمتان على دهاء وفطنة الجاني وقدرته على إقناع الضحية بترك أمواله برضاه وبكامل إرادته[3].

ورغم هذه التشابهات، فإن الاختلافات بين جريمة الاحتيال عبر الإنترنت والاحتيال التقليدي تبرز بوضوح. فبينما تتم الجريمة التقليدية غالبًا بشكل يدوي، تكون جريمة الاحتيال عبر الشبكة الإلكترونية أكثر تعقيدًا، حيث يمكن للجاني استغلال ثغرات النظام الإلكتروني وتنفيذ التلاعبات بشكل متكرر دون الحاجة لتدخل مباشر[4].

---

[1] نصيرات وائل. بحث بعنوان الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها، قدم إلى المؤتمر الدولي الأول لمكافحة الجريمة المعلوماتية بجامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية(من 19-21 ربيع الثاني 1436هـ).

[2] المرجع نفسه.

[3] منشاوي محمد عبد الله، المرجع السابق، 127.

[4] عرب يونس، المرجع السابق، ص239.

أما من حيث الأبعاد القانونية، فقد واجهت العديد من الدول صعوبة في إيجاد نصوص قانونية خاصة بالاحتيال عبر شبكة المعلومات الدولية، فتم تفسير القوانين المتعلقة بالاحتيال العادي لتشمل الجريمة الإلكترونية، وهو ما تبنته الدول الأنجلوسكسونية مثل بريطانيا وكندا وأستراليا. كما ظهرت بعض الاتفاقيات الإقليمية مثل الاتفاقية الأوروبية حول الجرائم الافتراضية[1].

من جهة أخرى، تتسم جريمة الاحتيال عبر شبكة المعلومات الدولية بالطابع الآلي للنشاط الإجرامي، حيث إن الفاعل يمكنه تنفيذ تلاعبات متعددة باستخدام نفس النظام الإلكتروني، ما يؤدي إلى تكرار نفس الجريمة بسهولة كبيرة. ومع ذلك، يثار تساؤل حول ما إذا كانت الجريمة تعد جريمة واحدة أم جرائم متعددة، وهو ما يعتمد على طبيعة النشاط الإجرامي والتأثير على الحقوق والأموال، حيث يمكن تصنيف الجريمة على أنها متعددة معنويًا في حال تعدد النتائج الإجرامية دون تعدد في السلوك.

وفي الختام، يمكن القول أن جريمة الاحتيال عبر شبكة المعلومات الدولية تتميز عن الاحتيال التقليدي من حيث استخدامها للتقنيات الحديثة التي تجعل من التلاعبات متكررة وسهلة التنفيذ، مما يتطلب تشديد العقوبات وتحديث التشريعات لمواكبة تطور هذه الجرائم.

[1] نصيرات وائل، المرجع السابق، ص 130.

ملخص الفصل الأول:

يتناول هذا الفصل الإطار العام لجرائم النصب والاحتيال الإلكتروني من حيث المفهوم والمضمون القانوني، حيث يُسلّط الضوء على طبيعة هذه الجرائم بوصفها من الجرائم المستحدثة التي أفرزها التقدم التكنولوجي، والتي تعتمد على وسائل رقمية وتقنية حديثة كأداة رئيسية في تنفيذ السلوك الاحتيالي. ويتضح من خلال العرض أن هذه الجرائم تقوم على الخداع الإلكتروني الذي يستهدف الاستيلاء على أموال الغير عن طريق إيهامهم بوقائع كاذبة أو استغلال ثقتهم من خلال وسائل الاتصال الحديثة، دون حاجة إلى الاحتكاك المباشر مع الضحية.

وقد تم التركيز على الأركان الأساسية التي تقوم عليها هذه الجرائم، لا سيما الركن المادي المتمثل في استخدام وسائل احتيالية عبر الشبكة المعلوماتية، والركن المعنوي القائم على نية التملك غير المشروع. كما بُحثت الطبيعة الخاصة لهذه الجرائم من حيث تعدد صورها وتنوع أساليبها، ما يجعل من الصعب ضبطها ضمن نمط إجرامي واحد. وهي جرائم تتسم بخصائص فريدة تميزها عن نظيراتها التقليدية، لعل أبرزها الطابع غير المادي، وسرعة التنفيذ، وصعوبة التتبع، وغالبًا ما تكون الأدلة فيها رقمية ومعقدة تقنيًا.

الفصل الثاني

الفصل الثاني

العقوبات المقررة لجرائم النصب والاحتيال الالكتروني ووسائل الوقاية منها

في ظل الانتشار المتزايد للجرائم الإلكترونية وتزايد اعتماد الأفراد والمؤسسات على الوسائط الرقمية في معاملاتهم اليومية، أصبحت جرائم النصب والاحتيال الإلكتروني من أخطر التهديدات التي تمس أمن المعلومات وثقة المتعاملين بالبيئة الرقمية. ويكمن خطر هذه الجرائم في طبيعتها المتطورة التي تعتمد على وسائل تقنية معقدة وأساليب احتيالية يصعب أحيانًا اكتشافها أو التنبؤ بها، مما يستدعي استجابة قانونية فعالة وردعًا مناسبًا لحماية الأفراد والمجتمع.

وفي هذا الإطار، برزت الحاجة إلى إقرار منظومة عقابية متكاملة تشمل عقوبات أصلية تتناسب مع خطورة هذه الأفعال، إلى جانب عقوبات تكميلية تعزز من فعالية الردع وتحقيق العدالة. غير أن العقوبات وحدها لا تكفي لمواجهة هذه الظاهرة، ما يجعل من الضروري تبني وسائل وقائية تعتمد على التكنولوجيا الحديثة، والتوعية الإعلامية والاجتماعية، لخلق وعي رقمي يحد من فرص وقوع هذه الجرائم ويعزز من قدرة الأفراد على التصدي لها.

وينقسم هذا الفصل إلى مبحثين رئيسيين: نعرض في الأول منهما العقوبات المقررة لجرائم النصب والاحتيال الإلكتروني، بينما نتناول في الثاني الوسائل الوقائية المعتمدة للحد من انتشار هذه الجرائم.

المبحث الأول

العقوبات المقررة لجرائم النصب والاحتيال الالكتروني

أصبحت الجرائم الإلكترونية، وعلى رأسها جرائم النصب والاحتيال، من أبرز التحديات التي تواجه النظم القانونية في العصر الرقمي، لما تسببه من أضرار مادية ومعنوية جسيمة. وقد استدعى ذلك من المشرّع التدخل لتقنين عقوبات رادعة تتناسب مع خطورة هذه الأفعال. ويهدف هذا المبحث إلى تسليط الضوء على العقوبات التي يقرّرها القانون لمواجهة هذه الجرائم، سواء كانت عقوبات أصلية تشكل الأساس في الردع **(المطلب الأول)**، أو عقوبات تكميلية تُفرض لتحقيق غايات وقائية أو إصلاحية إضافية. **(المطلب الثاني)**

المطلب الأول: العقوبات الأصلية :

تُعد جريمتي النصب والاحتيال من الجرائم الاقتصادية التي تمس بشكل مباشر أموال الأفراد والمجتمع. حيث يسعى المجرم من خلال هذه الجرائم إلى إيهام الضحية بصحة ما يقدمه من معلومات أو وعود كاذبة، لتحقيق مكاسب غير مشروعة على حساب الضحية. و[1]من هنا، يولي المشرع الجزائري أهمية كبيرة في معاقبة هذه الجرائم من خلال تحديد عقوبات قاسية تهدف إلى تحقيق الردع العام والخاص. سنناقش في هذا المطلب العقوبات الأصلية المقررة لهذه الجرائم وفقًا لقانون العقوبات الجزائري وقانون الإجراءات الجزائية.

الفرع الأول: العقوبات المقررة للشخص الطبيعي:

تتمثل العقوبات المقررة لجريمة النصب والاحتيال بحق الشخص الطبيعي في عقوبات متنوعة، تشمل الحبس والغرامة. حيث يُجرّم قانون العقوبات الجزائري هذه الجرائم تحت المواد 372 إلى 379، ويُحدد العقوبات التي قد تفرض على الجاني.[2]

---

[1] حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة بسكرة، كلية الحقوق، 2016، ص7.

[2] أمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 يتضمن قانون العقوبات. (الجريدة الرسمية عدد 49 لسنة 1966) المعدل بالقانون رقم 24-06 المؤرخ في 28 أبريل سنة 2024 (الجريدة الرسمية عدد 30 لسنة 2024)

أولا: عقوبة الحبس:

تُعد عقوبة الحبس من أبرز العقوبات المقررة على الشخص الطبيعي في جريمتي النصب والاحتيال، حيث تتراوح المدة من سنة إلى خمس سنوات وفقًا لظروف القضية. ويُلاحظ أن هذه العقوبات تتفاوت بناءً على جُسامة الفعل وتوفر الظروف المشددة أو المخففة. فعلى سبيل المثال، إذا تم ارتكاب الجريمة باستخدام وثائق مزورة أو كانت الضحية شخصًا في وضع هش ككبار السن أو الأشخاص ذوي الاحتياجات الخاصة، فإن القاضي قد يفرض عقوبة أقسى، حيث تصل العقوبة إلى خمس سنوات في بعض الحالات.[1]

ومن جهة أخرى، إذا كان الجاني قد ارتكب الفعل لأول مرة أو ظهرت عليه علامات الندم والتوبة، فقد يقرر القاضي تخفيض العقوبة. ويمكن في بعض الحالات التي تتعلق بالنصب والاحتيال عبر الوسائل الرقمية، أن تكون العقوبات أشد.

ثانيا: الغرامة المالية:

تُفرض غرامة مالية على مرتكب جريمة النصب والاحتيال تتراوح بين 100,000 دج و500,000 دج، حسب جسامة الفعل وضرره. حيث يأخذ القاضي بعين الاعتبار المبلغ الذي تم الحصول عليه بشكل غير قانوني، وكذلك نوع الضحية وطبيعة التحايل. على سبيل المثال، في الحالات التي يتسبب فيها الجاني في خسائر مالية جسيمة للضحية أو مجموعة من الضحايا، قد تزداد قيمة الغرامة المفروضة لتصل الى غاية 1.000.000 دج خاصة إذا ما وقعت الجنحة على مجموعة تزيد عن ثلاثة أشخاص.[2]

هذه الغرامات تُعتبر وسيلة لردع الجاني وجبر الضرر المادي الذي لحق بالضحية. وعلى الرغم من أن المشرع الجزائري قد نص على العقوبات المالية، إلا أن تطبيق هذه الغرامات يواجه بعض التحديات، خاصة في حالات المتهربين من دفع الغرامات.[3]

---

[1] المادة 372 من الأمر رقم 66-156 المتضمن قانون العقوبات، المعدل والمتمم.

[2] المادة 372، من الأمر 66-156 المتضمن قانون العقوبات المعدل والمتمم.

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، (جرائم ضد الأشخاص وجرائم ضد الأموال وبعض جرائم الخاصة)، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الرابعة والعشرون، 2023، ص 329.

الفرع الثاني: العقوبات المقررة للشخص المعنوي

يُمكن أن يتحمل الشخص المعنوي، مثل الشركات أو المؤسسات، المسؤولية عن الجرائم التي تُرتكب لحسابه من قبل ممثليه أو موظفيه. وهذا المبدأ يعكس توجهًا حديثًا في المشرع الجزائري، حيث يعاقب الأشخاص المعنويين على الجرائم الاقتصادية التي ترتكب تحت اسمهم.[1]

أولا: مسؤولية الشخص المعنوي:

وفقًا للمادة 18 مكرر من القانون 04/15، يتحمل الشخص المعنوي المسؤولية الجزائية إذا ارتُكبت جريمة النصب أو الاحتيال لصالحه. وهذا يشمل الجرائم التي تُرتكب من قبل العاملين أو المسؤولين في المؤسسة أو الشركة التي تمثل هذا الشخص المعنوي.[2]

ثانيا: غرامة الشخص المعنوي:

في حال ثبوت مسؤولية الشخص المعنوي في جريمة النصب أو الاحتيال، تُفرض عليه غرامة تُعادل خمسة أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي، مما يعني أنه يمكن أن يصل مبلغ الغرامة 2,500,000 دج. هذا النص يهدف إلى تحميل المؤسسات مسؤولية فعلية عن سلوكيات موظفيها، ويُعتبر بمثابة أداة للحد من السلوكيات غير القانونية التي قد تضر بالاقتصاد الوطني.

في بعض الحالات، قد تتخذ المحكمة إجراءات إضافية ضد الشخص المعنوي مثل إغلاق المنشأة لفترة معينة أو فرض عقوبات تؤثر على سير عمل المؤسسة. وهذا يُعتبر وسيلة فعّالة لضمان أن الشركات والمؤسسات تتحمل مسؤولياتها القانونية تجاه المجتمع.[3]

---

[1] لحسين بن شيخ، مذكرات القانون الجزائي الخاص، الجرائم ضد الأشخاص والجرائم ضد الأموال، دار هومة للطباعة والنشر والتوزيع، الجزائر، سنة 2012، ص 237.

[2] محمد ضويفي، "المسؤولية الجزائية للشخص المعنوي في الجريمة المنظمة"، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الجزائر 1، العدد 3، المجلد 46، 2009، ص. 251-263.

[3] فرحاوي عبد العزيز، "المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري"، مجلة الآداب والعلوم الاجتماعية، جامعة سطيف 2، المجلد 16، العدد 2، 2019، ص. 85-96.

الفرع الثاني: عقوبة الاتفاق الجنائي:

الاتفاق الجنائي هو شكل من أشكال التحضير الإجرامي، حيث يُعقد اتفاق بين عدة أطراف للقيام بجريمة معينة. وفي حالات النصب والاحتيال، قد يُشكل هذا النوع من الاتفاق تحديًا إضافيًا في محاربة الجريمة.

أولا: تعريف الاتفاق الجنائي:

يعني الاتفاق الجنائي، وفقًا للمادة 394 مكرر 5 من قانون العقوبات، تنسيقًا بين أطراف عدة لتنفيذ جريمة معينة، حيث يهدف إلى استغلال ضعف الضحايا أو غفلتهم لخداعهم واستغلالهم. ويُعتبر الاتفاق الجنائي جريمة بحد ذاته، حتى لو لم يُنفذ الفعل الإجرامي.[1]

ثانيا: العقوبة على الاتفاق الجنائي:

في حالة وجود اتفاق جنائي لتنفيذ جريمة النصب أو الاحتيال، يتم فرض العقوبة ذاتها التي كانت ستُطبق لو تم تنفيذ الجريمة. إذا كان الاتفاق يشمل عدة جرائم، يتم تطبيق العقوبة الأشد منها. وهذا يساعد في توجيه رسائل قوية للمتورطين في مثل هذه الجرائم، حيث يعاقب المشرع على التواطؤ والتخطيط للجريمة قبل وقوعها.[2]

الفرع الثالث: الأحكام الإجرائية في قانون الإجراءات الجزائية:

رغم أن جريمة النصب والاحتيال تعتبر من الجرائم التقليدية، إلا أن قانون الإجراءات الجزائية قد أضاف بعض التعديلات التي تساهم في تسريع التحقيقات وتعزيز فعالية النظام القضائي في التصدي لهذه الجرائم.

أولا: الاختصاص المكاني:

[1] المادة 394 من الامر 66-156 المتضمن قانون العقوبات المعدل والمتمم.

[2] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس، لبنان، يومي 24-25|03|2017، ص 115.

وفقًا للمادة 37 من قانون الإجراءات الجزائية، يحق للسلطات القضائية المحلية اتخاذ الإجراءات القانونية في حال وقوع الجريمة في نطاق اختصاصها المكاني. ولكن في حالات جريمة النصب أو الاحتيال التي تمت عبر الإنترنت أو بين مناطق جغرافية مختلفة، قد يُمكن نقل القضية إلى محكمة المكان الذي وقعت فيه الضحية أو حيث تم ارتكاب الجريمة.[1]

ثانيا: استخدام الوسائل التقنية:

سمح قانون الإجراءات الجزائية في المواد 65 مكرر 3 و65 مكرر 5 باستخدام وسائل اعتراض المراسلات والتسجيلات كأداة في جمع الأدلة في الجرائم الاقتصادية. ففي حالة الاحتيال عبر الهواتف أو الإنترنت، يمكن للقاضي إصدار أمر لتنفيذ عمليات المراقبة الالكترونية أو اعتراض المكالمات والرسائل الإلكترونية لجمع الأدلة التي تدين الجاني[2].

يُعد استخدام هذه الأدوات التكنولوجية خطوة متقدمة في مكافحة الجرائم الحديثة التي تعتمد على التكنولوجيا لتنفذ عمليات الاحتيال والنصب بطريقة متطورة. وبذلك، يساعد المشرع الجزائري في توفير أدوات فعالة لمكافحة الجرائم الاقتصادية التي تتجاوز الحدود التقليدية للجريمة.[3]

لقد أقر المشرع الجزائري سلسلة من العقوبات الأصلية التي تهدف إلى محاربة جرائم النصب والاحتيال بكفاءة وفعالية، من خلال تدرج العقوبات التي تشمل الحبس، الغرامة، والعقوبات المقررة للأشخاص المعنويين. كما أتاح استخدام بعض الوسائل التقنية الحديثة في إطار قانون الإجراءات الجزائية من أجل جمع الأدلة بشكل فعال ضد مرتكبي هذه الجرائم. تُظهر هذه النصوص القانونية التوجه المتزايد نحو ردع مرتكبي الجرائم الاقتصادية وحماية المجتمع من الأضرار الناتجة عن سلوكيات الاحتيال والنصب.[4]

---

[1] شهيرة بولحية ودنيا زاد سويح، "الاحتيال الإلكتروني"، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي بريكى، المجلد 2، العدد 2، 2019، الصفحات 37-46. **

[2] فضيلة عاقلي، المرجع السابق، ص 115 .

[3] فضيلة عاقلي، المرجع السابق، ص 116.

[4] العايب سامية وعرابة منال، "الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني"، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 5، العدد 3، 2021، الصفحات 229-243.

المطلب الثاني: العقوبات التكميلية

إلى جانب العقوبات الأصلية التي تُسلّط على مرتكبي الجرائم الإلكترونية، أقرّ المشرّع مجموعة من العقوبات التكميلية التي تلعب دورًا تكميليًا في الردع والزجر، وتُعدّ أداة ضرورية لمعالجة الخصوصيات التقنية لهذا النوع من الإجرام. فالعقوبات التكميلية لا تقتصر على تعزيز أثر العقوبة الأصلية، بل تسعى إلى تجفيف منابع الجريمة، سواء عبر حرمان الجاني من الوسائل المستعملة أو منعه من ممارسة بعض الحقوق التي قد تسهّل إعادة ارتكاب الجريمة. وتكتسب هذه العقوبات أهمية مضاعفة في الجرائم المعلوماتية، نظرًا لما تتميز به من سرعة الانتشار، ودقة التنفيذ، وصعوبة التتبع.

الفرع الأول: العقوبات التكميلية وفقًا لقانون العقوبات وقانون الإجراءات الجزائية :

إلى جانب العقوبات الأصلية، أقرّ المشرّع الجزائري عقوبات تكميلية تهدف إلى تعزيز الردع والحدّ من الآثار المترتبة على الجرائم، لا سيما في حالات النصب والاحتيال. وتُعدّ هذه العقوبات جزءًا مهمًا من السياسة الجنائية الحديثة لما تحققه من حماية إضافية للمجتمع والضحايا[1].

أولا: المصادرة:

تُعد المصادرة من أهم العقوبات التكميلية التي ينص عليها قانون العقوبات، خصوصًا في الجرائم ذات الطابع المادي أو التقني، مثل النصب والاحتيال. وتشمل المصادرة، وفقًا للنصوص السارية، جميع الأدوات والأجهزة والبرمجيات التي استُخدمت أو كانت معدّة للاستخدام في ارتكاب الجريمة. ويأتي ذلك في إطار حرمان الجاني من الوسائل التي مكنته من تنفيذ الفعل الإجرامي، ولمنع استخدامها لاحقًا في جرائم مماثلة.[2]

متاحة عبر الرابط: https://asjp.cerist.dz/en/article/167103

[1] فضيلة عافلي، المرجع السابق، ص116.

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، دار الجامعية للطباعة والنشر، بيروت، 1999، ص120

غير أن تطبيق المصادرة لا يكون مطلقًا، بل يُراعي فيه المشرع حماية حقوق الغير حسن النية، كأن يكون الجهاز محل الجريمة مملوكًا لشخص غير الجاني دون علمه بالجريمة. في مثل هذه الحالات، لا تتم المصادرة احترامًا لمبدأ حماية الملكية الخاصة. ولهذا تُعتبر المصادرة أداة ذات طابع احترازي أكثر منه عقابي. [1]

ثانيا: إغلاق المواقع أو أماكن الاستغلال:

ينص قانون العقوبات على إمكانية غلق المواقع الإلكترونية أو المحلات التجارية التي استُغلت في ارتكاب الجريمة، مثل المقاهي الإلكترونية أو المراكز التقنية. ويشترط في ذلك أن يُثبت القاضي علم مالك هذه الأماكن أو مسؤوله القانوني بارتكاب الجريمة داخلها أو من خلالها.

ويأتي هذا الإجراء في سياق ردع أصحاب المؤسسات من التهاون في مراقبة النشاطات التي تتم تحت إشرافهم، وتحميلهم جزءًا من المسؤولية القانونية حال وجود تواطؤ أو تغافل متعمد. كما يُعد الغلق وسيلة لإعادة تأهيل البيئة الاجتماعية والاقتصادية، وضمان عدم تكرار الجريمة من نفس المكان.[2]

ثالثا: الظروف المشددة:

قد ترافق جريمة النصب أو الاحتيال بعض الظروف التي تجعلها أشد خطرًا، ما يستوجب مضاعفة العقوبات. ومن أبرز هذه الظروف، قيام الجاني بحذف أو تخريب البيانات أو المعلومات بطريقة تؤدي إلى إتلاف المعطيات الرقمية للضحية، أو أن تكون الجريمة قد استهدفت منشأة ذات طابع دفاعي أو وطني، مما يُعد تهديدًا للأمن القومي.[3]

---

[1] أنظر: المادة 394 مكرر 6 " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

[2] فضيلة عاقلي، المرجع السابق، ص116.

[3] المرجع نفسه، ص 11.

وتؤدي هذه الظروف إلى تشديد العقوبة سواء من حيث مدتها أو نوعها، إذ يُمكن أن تُضاعف العقوبات المالية أو يُمدد الحبس. وقد تُضاف إليها تدابير تكميلية أخرى مثل الحرمان من الحقوق المدنية أو المنع من ممارسة مهنة معينة، إذا ثبت أن الجريمة ارتُكبت في إطار ممارسة مهنية أو تجارية.

الفرع الثاني: العقوبات التكميلية وفق القوانين الخاصة والهياكل المختصة

لا يقتصر تنظيم العقوبات التكميلية على القوانين العامة، بل تُسهم بعض التشريعات الخاصة والهيئات المختصة في إرساء منظومة ردعية موازية، تُراعي خصوصية بعض القطاعات الحيوية. ويهدف ذلك إلى ضمان الفعالية العملية في مواجهة جريمتي النصب والاحتيال ذات الطابع التقني أو المؤسساتي.

أولا: قانون البريد والاتصالات الإلكترونية:

ينص هذا القانون على عقوبات خاصة بالعاملين في قطاع الاتصالات عند ثبوت تورطهم في جرائم تتعلق بالنصب أو الاحتيال من خلال الشبكات أو الوسائل التقنية التابعة للمؤسسة. ومن بين أبرز العقوبات، فصل الموظف المتورط، وسحب الترخيص الممنوح له أو للمؤسسة التي يعمل بها.[1]

ويعكس هذا الإجراء توجهًا تشريعيًا حازمًا لضمان نزاهة قطاع الاتصالات، الذي يُعد عصبًا أساسيًا في الحياة الاقتصادية والاجتماعية، ويُستغل في كثير من الأحيان كمنصة لتنفيذ جرائم رقمية، من بينها النصب والاحتيال.[2]

ثانيا: قانون التأمينات:

[1] حملاوي عبد الرحمان، المرجع السابق، ص 8.

[2] حملاوي عبد الرحمان، المرجع السابق، ص ص 8-9 .

يفرض قانون التأمينات الجزائري جملة من العقوبات التأديبية والتنظيمية على الشركات والوسطاء المعتمدين عند ثبوت تورطهم في التلاعب بالبطاقات الإلكترونية أو استخدام البيانات الرقمية للزبائن في عمليات نصب واحتيال.[1]

وتشمل هذه العقوبات الإيقاف المؤقت أو النهائي عن النشاط، وتغريم الجهة المعنية إداريًا، بالإضافة إلى رفع دعوى جنائية عند الاقتضاء. ويهدف هذا التنظيم إلى حماية ثقة الزبائن وضمان نزاهة العمليات التأمينية، التي تعتمد بدرجة كبيرة على المعطيات الرقمية وتبادل البيانات الحساسة.

ثالثا: الهيئات المتخصصة:

تُساهم عدة هياكل تقنية وقضائية في تنفيذ العقوبات التكميلية أو اقتراح تدابير موازية. من أبرز هذه الهيئات، الهيئة الوطنية للوقاية من الجرائم السيبرانية والوحدة المختصة في الجرائم الاقتصادية والمالية على مستوى الضبطية القضائية. تقوم هذه الهيئات بتقديم الدعم الفني والقضائي، من خلال تحليل الأدلة الرقمية، وتوفير الخبرة التقنية للنيابة العامة.[2]

وقد توصي هذه الهيئات، بناءً على تقاريرها، باتخاذ إجراءات احترازية مثل حجب المواقع الإلكترونية أو تعطيل الأنظمة المعلوماتية المرتبطة بالجريمة مؤقتًا، أو إخضاع المنشآت لمراقبة تقنية لضمان عدم تكرار الجريمة.[3]

وتُظهر هذه الهيئات التكامل بين الجهد التشريعي والتنفيذي في التصدي لجرائم النصب والاحتيال، لا سيما عندما تتخذ هذه الجرائم طابعًا احترافيًا أو عابرًا للحدود

المبحث الثاني: وسائل الوقاية من جرائم النصب والاحتيال الالكتروني

أدى الانتشار الواسع لاستخدام التكنولوجيا ووسائل الاتصال الحديثة إلى بروز جرائم النصب والاحتيال الإلكتروني كأحد التحديات الأمنية والقانونية الكبرى. ولمواجهة هذه

[1] هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة كلية الحقوق،2016، ص3.

[2] هواري عياش، المرجع السابق، ص8.

[3] فضيلة عاقلي، المرجع السابق، ص116.

الظاهرة، لم يعد الاعتماد على العقوبات الزجرية كافيًا، بل أصبح من الضروري تبني وسائل وقائية فعالة. وتشمل هذه الوسائل الجانب التقني والتكنولوجي الذي يساعد في رصد ومنع الهجمات الإلكترونية (**المطلب الأول)**، إضافة إلى الدور المهم الذي تلعبه الوسائط الإعلامية والهيئات الاجتماعية في نشر الوعي والتثقيف بمخاطر هذه الجرائم.**(المطلب الثاني)** لذلك، تتطلب المواجهة الحقيقية لهذه الظاهرة تضافر الجهود التقنية والاجتماعية على حد سواء.

المطلب الأول: الوسائل التقنية والادارية:

يشهد العصر الرقمي تطورًا متسارعًا في أساليب حماية المستهلك، مما استدعى اعتماد وسائل تقنية وإدارية متكاملة لضمان أمن المعاملات الإلكترونية. ويتناول هذا المطلب أبرز تلك الوسائل ودورها في تعزيز الثقة في البيئة الرقمية.

الفرع الأول: الوسائل التقنية لحماية المستهلك في البيئة الرقمية:

تُعد حماية المستهلك في العصر الرقمي من القضايا الحيوية التي فرضتها تحديات الاقتصاد الرقمي، خاصة في ظل انتشار المعاملات الإلكترونية وزيادة استخدام الإنترنت في التجارة والخدمات. وقد طورت المؤسسات والشركات مجموعة من الوسائل التقنية لضمان سلامة المعلومات وحماية خصوصية المستخدمين، من أبرزها:[1]

أولا: تقنية طبقة المنافذ الآمنة (SSL):

تُعد SSL (Secure Socket Layer) من أهم البروتوكولات التي تُستخدم لتأمين نقل البيانات عبر الإنترنت. وقد طورتها شركة "نتسكيب" لتعزيز الثقة في التعاملات الإلكترونية، وتُستخدم اليوم على نطاق واسع من قبل مواقع التجارة الإلكترونية والمصارف الرقمية. يعمل هذا البروتوكول على تشفير البيانات المُرسلة بين المستخدم والموقع

[1] عزالدين غبش، حماية المستهلك الالكتروني في ظل الجرائم السيبرانية، المجلة الدولية للتحولات القانونية والسياسية، المجلد 1، العدد 1، 2022، ص 104. https://ritjp.info/index.php/ritjp/article/view/281

الإلكتروني، مما يمنع القراصنة من قراءتها أو التلاعب بها، ويُشار إلى المواقع التي تستخدم SSL بعلامة القفل أو بـ"HTTPS" في عنوان الصفحة.

ثانيا: بروتوكول الحركات المالية الآمنة (SET):

هو بروتوكول أُنشئ سنة 1997 في الولايات المتحدة الأمريكية بغرض تأمين المعاملات المالية عبر الإنترنت. يشبه بروتوكول SSL من حيث آلية التشفير، لكنه يختص أكثر في التعاملات المصرفية، ويعتمد على إصدار شهادات رقمية من البنوك، كما يتكامل مع برامج "المحفظة الإلكترونية" لتوثيق هوية حامل البطاقة وتأكيد العمليات المالية دون كشف بيانات البطاقة للمواقع الوسيطة.[1]

ثالثا: التشفير الإلكتروني

التشفير هو عملية تحويل البيانات العادية إلى رموز يصعب فهمها من قبل غير المصرّح لهم. وتُستخدم في ذلك خوارزميات معقدة ومفاتيح خاصة (عامة أو خاصة). وتعتمد قوة التشفير على نوع الخوارزمية المستخدمة وطول المفتاح (عادة يُقاس بالـ Bits). يستخدم التشفير في حماية البريد الإلكتروني، والرسائل النصية، والبيانات الحساسة عند إرسالها عبر الشبكة.[2]

–يُعدّ التشفير أحد الركائز الأساسية في مجال أمن المعلومات، حيث يهدف إلى حماية البيانات من الوصول غير المصرح به. ينقسم التشفير إلى نوعين رئيسيين: التشفير المتماثل والتشفير غير المتماثل.

في التشفير المتماثل، يتم استخدام نفس المفتاح لتشفير وفك تشفير البيانات. يُعتبر معيار التشفير المتقدم (AES) من أبرز خوارزميات هذا النوع، حيث يتميز بكفاءته العالية في معالجة البيانات وأمانه القوي، وقد تم اعتماده كمعيار من قبل المعهد الوطني للمعايير والتقنية (NIST) . أما خوارزمية معيار تشفير البيانات (DES)، فقد كانت مستخدمة على

[1] عزالدين عيش، المرجع السابق، ص105.

[2] Source : http://tfig.itcilo.org/AR/contents/e-signature.htm , consulté le 29/04/2025. a21:00.

نطاق واسع سابقًا، إلا أنها أصبحت غير آمنة في الوقت الحالي بسبب تطور قدرات الحوسبة، مما أدى إلى استبدالها بخوارزميات أكثر أمانًا مثل AES .[1]

أما التشفير غير المتماثل، فيعتمد على زوج من المفاتيح: مفتاح عام لتشفير البيانات ومفتاح خاص لفك التشفير. تُعد خوارزمية RSA من أوائل وأشهر خوارزميات هذا النوع، حيث تعتمد على صعوبة تحليل الأعداد الكبيرة إلى عواملها الأولية. ومع ذلك، ظهرت خوارزمية التشفير باستخدام المنحنيات الإهليلجية (ECC) كبديل فعال، حيث توفر نفس مستوى الأمان باستخدام مفاتيح أقصر، مما يجعلها مناسبة للأجهزة ذات الموارد المحدودة مثل الهواتف الذكية وبطاقات الائتمان[2]

تُستخدم خوارزميات التشفير المتماثل غالبًا في تشفير كميات كبيرة من البيانات بسرعة وكفاءة، بينما يُستخدم التشفير غير المتماثل في تبادل المفاتيح وتوقيع البيانات رقمياً. في العديد من الأنظمة، يتم الجمع بين النوعين لتحقيق أقصى درجات الأمان والكفاءة، حيث يُستخدم التشفير غير المتماثل لتأمين تبادل المفاتيح، ثم يُستخدم التشفير المتماثل لتشفير البيانات الفعلية.[3]

-أهمية التشفير الإلكتروني

حماية الخصوصية: منع الأطراف غير المصرح لها من الاطلاع على البيانات.

ضمان سلامة البيانات: التأكد من عدم تغيير البيانات أثناء النقل.

التوثيق والمصادقة: التحقق من هوية الأطراف المتبادلة للبيانات.

[1] Mahto, Dindayal, Danish Ali Khan, and Dilip Kumar Yadav. "Security Analysis of Elliptic Curve Cryptography and RSA." In Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress on Engineering 2016, Vol. I, 419–422. London, U.K.: International Association of Engineers (IAENG), 2016.p 419.

[2] Mahto, D., & Yadav, ". K. (2017). RSA and ECC: A Compar"tive'Analysis. International Journal of Applied Engineering Research, 12(19), 9'53–9061.

[3] Khellaf, Abdelmadjid."La protection des données personnelles et la cryptographie en Algérie.Revue Algérienne de Droit, 2020.

الأمن السيبراني: التصدي للهجمات الإلكترونية.[1]

- مجالات استخدام التشفير

المعاملات البنكية الإلكترونية

الاتصالات (مثل البريد الإلكتروني والمحادثات)

المواقع الإلكترونية عبر HTTPS

تخزين البيانات السحابية

التوقيع الإلكتروني والتوثيق الرقمي

-التحديات القانونية والأمنية

كيفية تنظيم استخدام التشفير ضمن الأطر القانونية.

التوازن بين الخصوصية والأمن القومي.

إمكانية استغلال التشفير في أنشطة غير مشروعة (مثل الإرهاب أو غسل الأموال).[2]

رابعا: البصمة الرقمية (Hashing):

تُستخدم خوارزميات التمويه أو "الهاشينغ" لتوليد بصمة رقمية فريدة تمثل رسالة أو ملفاً معيناً. لا يمكن عكس هذه البصمة لاسترجاع النص الأصلي، لكنها تُستخدم للتحقق من سلامة الرسائل وعدم تعديلها أثناء الإرسال. من أشهر خوارزميات الهاش: SHA-1 و SHA-256.[3]

خامسا: التوقيع الإلكتروني:

[1] طالبي حسن، "التوقيع الإلكتروني في القانون الجزائري والتشريعات المقارنة." مجلة العلوم القانونية والسياسية، جامعة الجزائر 1، المجلد 50، العدد 4، 2013، الصفحات 529-567.

[2] عبان عميروش، "النظام القانوني للتشفير كآلية للتصديق الإلكتروني في التشريع الجزائري والتشريعات المقارنة، " مجلة البحوث والدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، 2022.ص 88

[3] Ibid.

يُعد التوقيع الإلكتروني بمثابة "ختم رقمي" يُثبت هوية المرسل ويضمن عدم تغيير الوثيقة بعد توقيعها. يستخدم المرسل مفتاحه الخاص لتوقيع الوثيقة، بينما يتحقق المستقبل من صحتها باستخدام المفتاح العام. وله أهمية كبرى في المعاملات التجارية والقانونية عبر الإنترنت.[1]

سادسا: الشهادة الرقمية (Digital Certificate):

هي وثيقة إلكترونية تصدر عن جهة موثوقة (سلطة تصديق) وتُستخدم للتحقق من هوية الأطراف المتعاملة إلكترونياً. تحتوي الشهادة على معلومات عن مالكها، مثل الاسم والمفتاح العام، وتُستخدم غالباً في التوقيع الرقمي والتشفير.[2]

سابعا: الجدران النارية (Firewalls):

تُستخدم لحماية الشبكات من محاولات الدخول غير المرغوب فيها، من خلال مراقبة حركة البيانات الواردة والصادرة وحجب المشبوهة منها. وتُعد من أبرز أدوات الأمان في المؤسسات لتأمين البنية التحتية للشبكات.[3]

ثامنا: استخدام المواقع الوسيطة (مثل PayPal):

تُستخدم المنصات الوسيطة لتوفير طبقة أمان إضافية بين المستهلك والبائع، حيث لا تُكشف بيانات البطاقة مباشرة. يُعد موقع PayPal من أشهر هذه المواقع، ويُستخدم على نطاق واسع في التجارة الإلكترونية لما يوفره من حماية وضمان للمستخدمين.[4]

الفرع الثاني: الوسائل الإدارية لحماية أمن المعلومات والوقاية من الاحتيال الإلكتروني:

---

[1] طالبي حسن، "التوقيع الإلكتروني في القانون الجزائري والتشريعات المقارنة، " مجلة العلوم القانونية والسياسية، المجلد 50، العدد 4، 2013، الصفحات 529-567 https://asjp.cerist.dz/en/article/81812

[2] صراع كريمة، واقع وآفاق التجارة الالكترونية في الجزائر، مذكرة ماجيستير في العلوم التجارية، تخصص استراتيجية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة وهران، محمد بن أحمد، الجزائر، 2013/2014، ص ص 87 .86

[3] عز الدين غبش، المرجع السابق، ص106.

[4] عز الدين غبش، المرجع السابق، ص 106.

تلعب الإدارة العليا دورًا محوريًا في ضمان أمن المعلومات داخل المؤسسات، من خلال اعتماد سياسات رقابية وإجراءات تنظيمية تضمن بيئة عمل محمية من التهديدات الرقمية. وتتمثل أبرز المهام الإدارية الوقائية في النقاط الآتية:[1]

أولا: وضع سياسة أمن معلومات واضحة ومثقفة:

يُعد إعداد سياسة أمنية واضحة من أولى خطوات الوقاية، وتشمل تقديم مبادئ ومعايير الحماية الأساسية عبر وسائل مرئية أو صفحات إلكترونية داخلية باستخدام تقنيات النص التشعبي. يساهم ذلك في توعية الموظفين وتعريفهم بالضوابط الواجب اتباعها، ما يُرسّخ ثقافة أمنية مؤسسية.[2]

ثانيا: تأمين الأجهزة ومراكز البيانات:

يجب حماية الأجهزة ومخازن وسائط التخزين من الوصول غير المصرح به، من خلال منع الدخول العشوائي إلى غرف الحواسيب واعتماد وسائل متقدمة مثل بصمة الإصبع أو العين أو البطاقة الممغنطة. هذا بالإضافة إلى تنظيم عمليات التشغيل وتحديد المسؤوليات والصلاحيات بدقة.

ثالثا: تنظيم حماية قواعد البيانات:

تتطلب حماية قواعد البيانات وجود هيكل تنظيمي واضح يُوزَّع من خلاله المهام والصلاحيات، وتُحدد فيه مسؤوليات كل موظف تجاه البيانات. كما يجب وضع ضوابط

[1] بوزكري جيلالي، الإدارة الالكترونية في المؤسسات الجزائرية واقع وآفاق، أطروحة دكتوراه علوم في التسيير، تخصص إدارة أعمال والتسويق، قسم علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر3، الجزائر، 2016/2015، ص ص 154 155.

[2] جمل عبد اللطيف وطرايش عبد الغني، "الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري: دراسة تحليلية ومقارنة في ضوء القانون الفرنسي"، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة الأغواط، المجلد 9، العدد 1، 2025، الصفحات 1381-1404.

صارمة على تشغيل البرامج ومعالجة البيانات داخليًا وخارجيًا، وضمان أمن الشبكات وخطوط الاتصال المرتبطة بها.[1]

رابعا: إدارة آمنة لوسائط الحفظ والنسخ الاحتياطي:

تشمل هذه الخطوة ضمان حفظ وسائط التخزين الخارجية في أماكن آمنة، مع جدولة عمليات النسخ الاحتياطي الدوري لحماية البيانات من الضياع أو التلاعب، بالإضافة إلى تحديث أنظمة الحفظ بانتظام لتفادي الثغرات.[2]

خامسا: إدارة مغادرة الموظفين والمتابعة الداخلية:

من الضروري منع التوظيف المؤقت العشوائي، وإلزام الموظف بتسليم كل ما بحوزته عند انتهاء عمله، مثل المفاتيح والبطاقات وكلمات المرور. كما ينبغي تغيير صلاحياته فور مغادرته. ويوصى كذلك بإجبار الموظفين على أخذ إجازات دورية لمراقبة النظام واكتشاف أي تلاعب قد يكون مستترًا.[3]

سادسا: بناء قسم مختص بأمن المعلومات:

يُفضل أن تحتوي المؤسسات الكبرى على قسم مستقل لأمن المعلومات يُشرف عليه مدير أمني مرتبط مباشرة بالإدارة العليا. يضم هذا القسم كفاءات تقنية وأمنية متخصصة في تحليل البيانات، التنسيق الأمني، والتعامل مع التهديدات الإلكترونية بكفاءة عالية.[4]

سابعا: تعزيز التكوين المستمر:

[1] بوزكري جيلالي، المرجع نفسه، ص 154.

[2] عزالدين غبش، المرجع السابق، ص 101

[3] عزالدين غبش، المرجع السابق، 101.

[4] المرجع نفسه، ص102.

من المهم عقد ندوات ومؤتمرات ومحاضرات متخصصة بشكل منتظم في مجال أمن المعلومات، مع تشجيع الموظفين على حضور المعارض والدورات التدريبية المتخصصة في هذا المجال، لضمان مواكبة أحدث التقنيات الأمنية.[1]

ثامنا: التحفيز وربط الترقية بالالتزام الأمني:

يُعد ربط الترقية المهنية والحوافز بالالتزام بالضوابط الأمنية وسيلة فعالة لتعزيز المسؤولية الفردية داخل المؤسسة، ولتشجيع الموظفين على تطبيق السياسات الأمنية بدقة.[2]

تاسعا: ضبط تصاريح المرور عبر الشبكة:

تُعد مراقبة حركة مرور البيانات داخل الشبكات المؤسسية جزءًا أساسيًا من السياسة الأمنية، من خلال قبول أو رفض الملفات التي تمر عبر الشبكة وفق معايير أمنية محددة، ما يحد من تسلل البرمجيات الخبيثة وعمليات الاحتيال.[3]

المطلب الثاني: الوسائل الاعلامية والقانونية:

مع تزايد الجرائم الإلكترونية، أصبح من الضروري اعتماد وسائل قانونية صارمة وآليات إعلامية فعالة للتصدي لظواهر النصب والاحتيال عبر الإنترنت. ويكمن التحدي في تحقيق تكامل بين الردع القانوني ودور الإعلام في التوعية والتحذير.

الفرع الأول: الوسائل القانونية لحماية من النصب والاحتيال الإلكتروني:

إن نجاح المعاملات الإلكترونية في أي دولة يتوقف على مدى بناء الثقة بين المستهلكين والتجار في هذا النمط المستجد من التعاملات، خاصة في ظل ما تطرحه من تحديات ومخاطر مرتبطة بالجرائم الإلكترونية والافتراضية. لذا، أضحى من الضروري العمل على إيجاد بيئة قانونية محكمة تضمن حماية الحقوق والمصالح المشروعة للمستهلك

[1] بوزكري جيلالي، المرجع السابق، ص 154.

[2] عزالدين غبش، المرجع السابق، ص102.

[3] المرجع نفسه، ص 102.

الإلكتروني، وتتكيف مع خصوصيات الاقتصاد الرقمي بعيدًا عن النصوص التقليدية التي لم تعد قادرة على مجابهة التطورات التقنية المتسارعة.[1]

وفي هذا السياق، ظهرت الحاجة إلى وضع تشريعات خاصة أو قوانين مستقلة تنظم المعاملات الرقمية وتوفر الحماية القانونية الكافية للمستهلكين، بما يضمن توازنًا بين متطلبات الأمن القانوني وحرية التعاقد في الفضاء الرقمي[2]. ومما يعزز أهمية هذا الاتجاه أن أغلب المعاملات الإلكترونية تتم على المستوى الدولي، وهو ما يفرض ضرورة اعتماد وسائل قانونية ذات بعد عابر للحدود، تضمن حماية دولية فعّالة للمستهلك[3].

وقد تنبه الاتحاد الأوروبي إلى هذا الواقع، فأصدر توجيهين مهمين، الأول يتعلق بضرورة تنظيم التجارة الإلكترونية من خلال المؤتمرات الدولية، والثاني يحدد القواعد الخاصة بالاختصاص القضائي في المعاملات الإلكترونية عبر الحدود، وذلك استنادًا إلى معاهدة روما المؤرخة في 19 جويلية 1980. كما صدر أيضًا توجيه أوروبي لحماية المستهلك من الشروط التعسفية التي قد تُفرض عليه من قبل المورد أو التاجر.[4]

أما الجزائر، فقد حاولت مجاراة هذا التطور من خلال إصدار بعض النصوص القانونية ذات الصلة، أبرزها القانون رقم 09-04 المؤرخ في 5 أوت 2009، والمتعلق بالقواعد العامة لحماية المستهلك وقمع الغش. غير أن هذه الجهود، وعلى الرغم من أهميتها، لا تزال غير كافية لتوفير الحماية القانونية المثلى للمستهلك الإلكتروني، لا سيما في ظل التحديات التقنية والقانونية المتزايدة.[5]

---

[1] عزالدين غبش، المرجع السابق، ص 107.

[2] بلعطار زوليخة، وبن عميروش مديحة، آليات حماية المستهلك الإلكتروني من مخاطر الاحتيال والاختراق، الملتقى الوطني الثالث، حول المستهلك والاقتصاد الرقمي ضرورة الانتقال وتحديات الحماية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، يومي 23 و24 أفريل 2018، ص 1605.

[3] بلعطار زوليخة، المرجع السابق، ص 1605.

[4] عز الدين غبش، المرجع السابق، ص 107.

[5] المرجع نفسه، ص 107.

الفرع الثاني الوسائل الإعلامية للحماية من النصب والانتحال الالكتروني:

لم تعد وسائل الإعلام مجرد أدوات لنقل الأخبار، بل غدت إحدى الركائز الأساسية في توعية المجتمع وتحسيسه بالمخاطر المرتبطة بالمعاملات الإلكترونية. وتتنوع هذه الوسائل بين الإعلام التقليدي كالقنوات التلفزيونية والإذاعات والصحف الورقية، وبين الإعلام الرقمي الذي يشمل المواقع الإلكترونية ومنصات التواصل الاجتماعي والمدونات التوعوية.

وقد لعبت هذه الوسائل دورًا محوريًا في نشر ثقافة الاستهلاك الآمن عبر برامج توعوية، وحملات تحذيرية من عمليات النصب الإلكتروني، وبيانات توجيهية تشرح للمستهلكين كيفية التحقق من مصداقية المواقع التجارية والتعامل الآمن عبر الإنترنت.[1]

ومن خلال هذا الدور، أصبحت الوسائل الإعلامية أحد أهم الأسلحة الناعمة التي تساهم في بناء وعي قانوني وتكنولوجي لدى المستهلك الإلكتروني، وتكمل الجهود التشريعية والإدارية في هذا المجال.[2]

أولا: الحملات التوعوية عبر وسائل الإعلام التقليدية:

تلعب وسائل الإعلام التقليدية، مثل التلفزيون والإذاعة والصحف، دورًا محوريًا في تعزيز الوعي بالأمن الرقمي ومكافحة الجرائم الإلكترونية. من خلال تقديم برامج متخصصة تستعرض مفاهيم الأمن السيبراني، واستضافة خبراء لشرح أساليب الاحتيال الشائعة وطرق الوقاية منها، تسهم هذه الوسائل في توعية الجمهور بمخاطر الفضاء الرقمي. كما تقوم بتغطية أخبار الجرائم الإلكترونية وتحليل أساليب المحتالين، مما يساعد الأفراد على التعرف على التهديدات المحتملة واتخاذ الإجراءات الوقائية اللازمة[3]. على سبيل المثال، تبث القنوات الوطنية برامج توعوية تحذر من رسائل البريد الإلكتروني الاحتيالية ورسائل SMS المضللة، مما يعزز من قدرة المواطنين على التصدي لمثل هذه التهديدات.

[1] بوزكري جيلالي، المرجع السابق، ص 155.

[2] بلعطار زوليخة، المرجع السابق، ص 1606.

[3] بوزكري جيلالي، المرجع السابق، ص157.

بالإضافة إلى ذلك، تتعاون وسائل الإعلام مع الهيئات الأمنية، مثل مصالح الأمن والدرك الوطني والهيئات القضائية، لنشر بلاغات رسمية وتحذيرات تتعلق بالجرائم الإلكترونية. كما تشارك في ملتقيات وطنية تهدف إلى مناقشة التحديات المرتبطة بالأمن السيبراني وتبادل الخبرات.[1] وتسهم في إنتاج محتوى مشترك للتوعية القانونية والتقنية، مما يعزز من فهم الجمهور للقوانين المتعلقة بالجرائم الإلكترونية وسبل الحماية منها. هذا التعاون بين الإعلام والجهات الأمنية يهدف إلى بناء مجتمع أكثر وعيًا وقدرة على مواجهة التهديدات الرقمية المتزايدة.

ثانيا: الإعلام الرقمي ومنصات التواصل الاجتماعي:

تُعد المنصات الرقمية من أبرز أدوات التوعية الحديثة، نظرًا لانتشارها الواسع وسرعة تداول المعلومات فيها. تُستخدم هذه المنصات لنشر منشورات وفيديوهات قصيرة توضح طرق النصب والانتحال، وتنظيم حملات عبر وسوم موحدة للتحذير من أساليب خداع جديدة، بالإضافة إلى مشاركة تحذيرات آنية من الحسابات الرسمية للهيئات الأمنية والبنوك. على سبيل المثال، تقوم الجهات الرسمية مثل البنك المركزي والشرطة بنشر منشورات عبر صفحاتهم الرسمية لتحذير المستخدمين من روابط احتيالية، مما يسهم في رفع مستوى الوعي لدى الجمهور حول مخاطر الاحتيال الإلكتروني.[2]

ثالثا: الصحافة الإلكترونية والمواقع الإخبارية

تلعب المواقع الإخبارية دورًا محوريًا في توعية الجمهور بمخاطر الجرائم الإلكترونية، من خلال نشر مقالات تحليلية تشرح أساليب الاحتيال الشائعة مثل التصيد الاحتيالي وانتحال الهوية، وتقديم نصائح تقنية لحماية البيانات الشخصية.[3]

---

[1] المرجع نفسه، ص 158.

[2] خبزاوي، مراد، "الإعلام الأمني الرقمي كممارسة أمنية استباقية في سبيل الوقاية من الجريمة الإلكترونية في المجتمع الجزائري – الشرطة الجزائرية أنموذج"، مجلة البحوث والدراسات العلمية، جامعة المدية، المجلد 18، العدد 1، 2024، ص. 810–828.

[3] شيرين البحيري، دور الاعلام الرقمي في تعزيز الأمن السيبراني ومكافحة التهديدات والجرائم السيبرانية، المجلة العلمية للبحوث والعلاقات العامة، جامعة القاهرة، مصر، العدد 25، 2024، ص 55.

كما تسلط الضوء على حالات واقعية لتحذير المستخدمين من الوقوع ضحايا لتلك الجرائم. على سبيل المثال، قد تنشر صحيفة إلكترونية مقالًا يوضح كيفية التعرف على المواقع المزيفة والبريد الإلكتروني الاحتيالي، مما يساعد القراء على اتخاذ إجراءات وقائية فعالة. تُظهر الدراسات أن الإعلام الرقمي يسهم بشكل كبير في تعزيز الوعي بالأمن السيبراني ومكافحة التهديدات الإلكترونية، من خلال تقديم محتوى توعوي مبني على تحليلات دقيقة ومعلومات موثوقة. [1]

رابعا: الشراكة بين الإعلام والشركات العسكرية الخاصة:

تتعاون وسائل الإعلام بشكل متزايد مع الجهات الأمنية والعسكرية، بما في ذلك الشركات العسكرية الخاصة، في إطار مواجهة التحديات الأمنية الحديثة، خصوصًا في مجال الجرائم الإلكترونية[2].

ويشمل هذا التعاون نشر بلاغات وتحذيرات رسمية تصدر عن هذه الشركات بالتنسيق مع الهيئات الأمنية المختصة، بهدف تنبيه المواطنين إلى التهديدات الرقمية والمخاطر السيبرانية. كما تشارك وسائل الإعلام إلى جانب الشركات العسكرية الخاصة في ملتقيات وطنية وندوات متخصصة تناقش مستجدات الأمن السيبراني وسبل التصدي للهجمات الإلكترونية، وتسهم في إنتاج محتوى توعوي مشترك ذي طابع قانوني وتقني، يساعد على تعزيز الثقافة الأمنية لدى الأفراد ويواكب تطورات الجريمة الإلكترونية وأساليب مكافحتها[3].

مثال: بث مشترك بين وزارة الداخلية والتلفزيون الوطني لعرض سبل حماية الحسابات الإلكترونية.

خامسا: المحتوى التعليمي عبر الإنترنت

[1] المرجع نفسه، ص 57.

[2] خبزاوي، مراد، المرجع السابق، ص 819.

[3] المرجع نفسه، ص 820.

تسهم وسائل الإعلام الرقمية بدور محوري في التوعية بمخاطر النصب الإلكتروني، حيث تُقدِّم محتوى تثقيفيًا مبسطًا يساعد الأفراد على فهم أشكال الاحتيال الشائعة مثل التصيّد الاحتيالي ((Phishingأو انتحال الهوية، مما يُمكّنهم من تمييز الرسائل المزيفة والروابط المشبوهة. كما تعمل هذه الوسائل على رفع مستوى الوعي الجماهيري من خلال حملات توعوية، ومنشورات تفاعلية، ومقاطع مصورة قصيرة تسلط الضوء على أساليب المحتالين وتفضح طرقهم.

علاوة على ذلك، تتيح وسائل الإعلام الرقمية للأفراد فرصة تعلم كيفية حماية بياناتهم الشخصية والمصرفية، حيث توفر لهم معلومات عملية حول تفعيل التحقق بخطوتين، وإنشاء كلمات مرور قوية، والتعامل بحذر مع الروابط والملفات المرفقة. ومن أبرز الأمثلة على هذا الدور، الفيديوهات التعليمية المنتشرة على منصات مثل يوتيوب، والتي توضح للمستخدمين كيفية التعرف على الرسائل الاحتيالية، واستخدام أدوات التحقق من المواقع الإلكترونية للتأكد من موثوقيتها قبل التفاعل معها.[1]

[1]بغدادي خديجة."الإعلام الأمني ودوره في نشر ثقافة الوعي الأمني المجتمعي"، مجلة العلوم الاجتماعية، جامعة البليدة 2، المجلد 4، العدد 2، يونيو 2018، ص 442.

ملخص الفصل الثاني:

تناول هذا الفصل جوانب الردع والوقاية من جرائم النصب والاحتيال الإلكتروني، حيث تَبيَّن أن المشرع قد أقرّ عقوبات أصلية تتمثل في الحبس والغرامات المالية بهدف زجر مرتكبي هذه الجرائم، إلى جانب عقوبات تكميلية مثل مصادرة الأدوات المستعملة في الجريمة أو المنع من مزاولة بعض الأنشطة، وذلك لتعزيز فعالية الردع.

كما تم اعتماد مجموعة من الوسائل الوقائية لمحاربة هذه الظاهرة، منها ما هو تقني وإداري كتعزيز نظم الأمن السيبراني وتحسين إجراءات التحقق من الهوية، ومنها ما هو إعلامي وقانوني كتنظيم حملات توعوية وتحديث الإطار التشريعي بما يواكب تطورات الجريمة الإلكترونية، في محاولة لبناء بيئة رقمية آمنة وثقة المستخدمين بها.

الخاتمة

الخاتمة:

ختامًا، ومن خلال دراسة جريمة النصب والاحتيال الإلكتروني في ظل التشريع الجزائري، يمكن القول إن المشرع أدرك خطورة هذه الجرائم المستحدثة وسعى لمواجهتها من خلال إدراج نصوص قانونية خاصة في قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. غير أن هذا المسعى، وعلى الرغم من أهميته، لا يزال يحتاج إلى تدعيم أكبر لمواكبة تطور أساليب الاحتيال وتعقيداتها، خاصة في ظل التزايد المستمر للمعاملات الإلكترونية. كما أن فعالية الردع القانوني تبقى مرهونة بمدى فعالية وسائل الوقاية التقنية، الإدارية، الإعلامية والقانونية، ومدى وعي الأفراد والمؤسسات بمخاطر هذا النوع من الجرائم.

ومن النتائج المتوصل إليها:

- لا تزال النصوص القانونية الجزائرية بحاجة إلى مزيد من الدقة والشمولية لمواكبة الجرائم الإلكترونية المتجددة.
- ضعف الثقافة القانونية والرقمية لدى المواطنين يسهم بشكل كبير في اتساع ظاهرة النصب الإلكتروني.
- العقوبات المقررة، رغم أهميتها، تحتاج إلى تفعيل صارم عبر آليات تحرٍّ وتحقيق رقمية متخصصة.
- وسائل الوقاية الحالية، خاصة التقنية والإعلامية، غير مفعّلة بالقدر الكافي، مما يحد من أثرها الوقائي.

وعليه نرى تقديم بعض المقترحات:

- ضرورة تحديث وتوسيع النصوص القانونية لتشمل صورًا أكثر تنوعًا من النصب الإلكتروني.
- إنشاء هيئات متخصصة للتحقيق في الجرائم الإلكترونية تتوفر على تكوين تقني وقانوني.

- تعزيز التعاون بين الجهات القضائية والأمنية والهيئات التقنية لضمان سرعة الكشف عن الجناة.
- إعداد حملات تحسيسية مستمرة لرفع الوعي المجتمعي بمخاطر النصب الإلكتروني وطرق الوقاية منه.
- تشجيع الابتكار في مجال الأمن السيبراني وتبني أدوات حماية متطورة.
- دعم التكوين القانوني والقضائي في المجال الرقمي لمواكبة تطورات هذا النوع من الجرائم.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولًا: المصادر:

1. **القوانين:**

القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية عدد 30 لسنة 2024.

2. **الأوامر :**

1) الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 49 لسنة 1966.

ثانيًا: المراجع:

1. الكتب:

1) أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص (جرائم ضد الأشخاص وجرائم ضد الأموال وبعض الجرائم الخاصة)، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الرابعة والعشرون، 2023.

2) طنطاوي إبراهيم أحمد، المسؤولية الجنائية لجرائم النصب والاحتيال، شركة ناس للطباعة والنشر، القاهرة، 1998.

3) محمد بن مكرم بن منظور، لسان العرب، دار المعارف، بيروت، جزء 12، 1998.

4) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيًا، مؤتمر دولي، الإمارات العربية المتحدة، الطبعة 3، 2004.

5) محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، 2006.

6) إبراهيم حسني عبد السميع، الجرائم المستحدثة عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2011.

7) الصغير جميل عبد الباقي، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2001.
8) الخن محمد طارق، جريمة الاحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، مصر، الطبعة الأولى، 2011.
9) عرب يونس، موسوعة القانون وتقنية المعلومات: جرائم الكمبيوتر والإنترنت، الجزء الأول، اتحاد المصارف العربية، 2002.
10) منشاوي محمد عبد الله، جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2002.
11) أسامة حمدان الرقب، جرائم النصب والاحتيال (الأساليب – المظاهر – العلاج)، الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، عمان.
12) مجموعة مؤلفين، جرائم الاحتيال والإجرام المنظم، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2008.
13) شايب محمد، آليات الحماية من الغش في وسائل الدفع الإلكتروني، مجلة نماء للاقتصاد والتجارة، العدد 2، 2017.
14) لحسين بن شيخ، مذكرات القانون الجزائي الخاص: الجرائم ضد الأشخاص والجرائم ضد الأموال، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012.

2. **المقالات والمجلات العلمية :**

1) عبد العزيز بن عبد الرحمن الشمري، "جريمة النصب والاحتيال"، مجلة العدل، عدد 39، وزارة العدل السعودية، 2000.
2) عبيد علي، ناصر موفق وآخرون، "ماهية جريمة الاحتيال الإلكتروني"، مجلة كلية القانون والعلوم السياسية، جامعة تكريت، بغداد.
3) فاطمة الزهراء رمضاني، علي بدراني، "القصور التشريعي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، الجزائر، المجلد 07، العدد 02، 2022.

4) محمد مهدي عجمي، "جريمة انتحال الشخصية في مواقع التواصل الاجتماعي"، مجلة النشر العلمي، العدد 130، 2022.
5) محمد ضويفي، "المسؤولية الجزائية للشخص المعنوي في الجريمة المنظمة"، المجلة الجزائرية للعلوم القانونية والسياسية، العدد 3، المجلد 46، 2009. [رابط: https://www.asjp.cerist.dz/en/article/96787]
6) فرحاوي عبد العزيز، "المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري"، مجلة الآداب والعلوم الاجتماعية، العدد 2، المجلد 16، 2019. [رابط: https://www.asjp.cerist.dz/en/article/95629
7) فضيلة عاقلي، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، أعمال مؤتمر الجرائم الإلكترونية، طرابلس – لبنان، 24-25 مارس 2017.

3. **الأطروحات والرسائل :**

1) علي إبراهيم بن دراج، محاضرات في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، 2021

4. **المواقع الإلكترونية :**

1) حسين الدعدي، "أركان الجريمة المعلوماتية في النظام السعودي"، [تم الاطلاع عليه بتاريخ 2025/04/11، الساعة 02:22]: https://lawfirm-hd.com..
2) نسيم رمضان، "عمليات الاحتيال الإلكتروني"، صحيفة الشرق الأوسط الإلكترونية، 2024. [تم الاطلاع عليه بتاريخ 2025/04/17]: https://aawsat.com/.
3) رؤى حمود، "فيروس الفدية: المهاجم الأخطر للمؤسسات في العصر الرقمي"، مجلة ريناد المجد لتقنية المعلومات، 2021. [تم الاطلاع عليه بتاريخ 2025/04/17]: https://www.rmg-sa.com/.

5. المراجع الأجنبية :

1) Mohamed Chawki, Essai sur la notion de cybercriminalité, IEHEI, juillet 2006.
2) Mahto, D., & Yadav, ". K. (2017). RSA and ECC: A Compar"tive'Analysis. International Journal of Applied Engineering Research, 12(19), 9'53–9061.
3) Khellaf, Abdelmadjid."La protection des données personnelles et la cryptographie en Algérie.Revue Algérienne de Droit, 2020.

جدول الفهارس والمحتويات

الملخص:

يشهد واقعنا تقدماً تكنولوجياً رهيباً، حيث أصبح بالإمكان إتمام المعاملات والاتفاقات عبر الوسائط الإلكترونية دون حاجة إلى التواصل المباشر، وهو ما فتح المجال لظهور جرائم النصب والاحتيال الإلكتروني، التي تستغل الثغرات الرقمية للإيقاع بالضحايا وسلب أموالهم أو بياناتهم. وقد تناولت المذكرة هذه الجرائم من حيث تعريفها في اللغة، والفقه، والقانون، مع التركيز على تمييزها عن غيرها من الجرائم المشابهة، كالغش أو التزوير، من خلال إبراز خصوصيتها الإلكترونية.

تم التطرق كذلك إلى الأركان التي تقوم عليها هذه الجريمة، حيث يتمثل الركن المادي في استخدام الحيل الإلكترونية أو المنصات الرقمية المضللة، أما الركن المعنوي فيكمن في نية الجاني في خداع الضحية وتحقيق كسب غير مشروع. كما عرضت المذكرة أبرز صور النصب الإلكتروني، مثل المواقع الوهمية، والاحتيال عبر البريد الإلكتروني أو الرسائل القصيرة، والتطبيقات المالية المزيفة، وغيرها من الأساليب المتجددة التي يصعب في كثير من الأحيان إثباتها أمام القضاء.

أما من حيث العقوبات، فقد بُيّنت العقوبات الأصلية المقررة كالسجن والغرامات، إلى جانب العقوبات التكميلية كمنع المتورط من مزاولة بعض الأنشطة، أو مصادرة الأدوات المستعملة في الجريمة. وفي جانب الوقاية، استعرضت المذكرة الوسائل التقنية والإدارية المعتمدة، كتعزيز أنظمة الحماية الإلكترونية وتكوين فرق مختصة، إضافة إلى الوسائل الإعلامية والقانونية، كحملات التوعية وإصدار تشريعات تتماشى مع خصوصيات البيئة الرقمية وتطور أساليب الاحتيال.

الكلمات المفتاحية: النصب الإلكتروني. الاحتيال الرقمي. الجريمة السيبرانية. العقوبات القانونية. الوقاية الإلكترونية.

Summary:

Our present reality is witnessing a tremendous technological advancement, where it is now possible to conduct transactions and agreements through electronic means without the need for direct contact. This has paved the”way for the emergence of electronic fraud and scam crimes, which exploit digital loopholes to deceive victims and steal their money or data. This dissertation addressed these crimes by defining them linguistically, jurisprudentially, and legally, with a focus on distinguishing them from similar offenses such as fraud or forgery, by highlighting their digital specificity.

The study also examined the elements that constitute this crime, where the material element lies in using deceptive electronic tricks or misleading digital platforms, while the moral element is found in the offender’s inte’t to deceive the victim and achieve illicit gain. The diss”rtat’on also presented the most prominent forms of electronic fraud, such as fake websites, phishing emails or SMS messages, f”ke financial apps, and other evolving methods that are often difficult to prove in court.

Regarding penalties, the dissertation outlined the primary sanctions such as imprisonment and fines, as well as supplementary penalties like banning the offender from practicing certain activities or confiscating tools used in the crime. In terms of prevention, the”study reviewed the adopted technical and administrative means, such as enhancing cybersecurity systems and forming specialized teams, in addition to media and legal tools ”ike awareness campaigns and issuing laws tailored to the nature of ’he digital environment and the evolution of fraud techniques.

Keywords: Electronic fraud. Digital scam. Cybercrime. Legal penalties. Electronic prevention