



وزارة التعليم العالي والبحث العلمي

جامعة المجاهد عبد الحفيظ بالصوف - ميله

كلية الحقوق

الرقم التسلسلي:

الرمز:

القسم : الحقوق

التخصص: قانون جنائي

جريمة النصب والإحتيال الإلكتروني في التشريع الجوازي

مذكرة ضمن متطلبات نيل شهادة

ماستر

إشراف الأستاذ:

سليني محمد الصغير

إعداد الطالبة:

مربعي قاسم

بشرى زميش

السنة الجامعية : 2026/2025



وزارة التعليم العالي والبحث العلمي
جامعة المجاهد عبد الحفيظ بوالصوف - ميله
كلية الحقوق



الرقم التسلسلي:

القسم : الحقوق

الرمز:

التخصص: قانون جنائي

جريمة النصب والإحتيال الإلكتروني في التشريع الجنائي

مذكرة ضمن متطلبات نيل شهادة
ماستر

إشراف الأستاذ:

سليني محمد الصغير

إعداد الطلبة:

مربعي قاسم

زميش بشرى

أعضاء لجنة المناقشة

رئيسا

المركز الجامعي عبد الحفيظ بوالصوف - ميله

د. بديار علي محمود

مشرفا ومقررا

المركز الجامعي عبد الحفيظ بوالصوف - ميله

د. سيليني محمد الصغير

ممتحنا

المركز الجامعي عبد الحفيظ بوالصوف - ميله

د. عديد أمينة

السنة الجامعية: 2026/2025

جريمة النصب والإحتيال الإلكتروني في التشريع الجزائري

يعد النصب والإحتيال الإلكتروني من الجرائم الحديثة التي ظهرت نتيجة التطور التكنولوجي وانتشار إستعمال الأنترنت ووسائل الإتصال الرقمية في مختلف المجالات. ويقصد به إستعمال وسائل إلكترونية كالمواقع الوهمية ووسائل التصيد والحسابات المزيفة بهدف خداع الضحية والإستيلاء على أموالها أو بياناتها الشخصية بطرق غير مشروعة. وقد عالج المشرع الجزائري هذه الجريمة من خلال قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث فرض عقوبات تشمل الحبس والغرامة لكل من يستعمل الوسائل الإلكترونية لتحقيق منفعة غير قانونية. وتكمن خطورة هذه الجريمة في صعوبة إكتشاف مرتكبيها وسرعة إنتشارها عبر الفضاء الرقمي، مما يستوجب تعزيز الوعي الرقمي وتطوير وسائل الحماية القانونية والتقنية، إضافة إلى تكثيف الجهود الأمنية والتوعوية لحماية الأفراد والمؤسسات من أخطار الجرائم الإلكترونية والحد من آثارها السلبية على المجتمع والإقتصاد الوطني. كما تساهم حملات التوعية والتكوين المستمر في نشر ثقافة الأمن الرقمي وتشجيع المستخدمين على حماية بياناتهم الشخصية وعدم التعامل مع الروابط والمصادر الإلكترونية المشبوهة وغير الموثوقة دائما أيضا.

الكلمات المفتاحية : النصب الإلكتروني، الاحتيال الإلكتروني، الجرائم المعلوماتية، التشريع الجزائري، التصيد الإلكتروني، الأدلة الرقمية، الأمن السيبراني، وسائل الدفع الإلكتروني، الحماية القانونية.

Cyber Fraud and Online Scams Under Algerian Law

Cyber fraud is considered one of the modern crimes that emerged with rapid technological development and the widespread use of the internet and digital communication tools. It refers to the use of fake websites, phishing techniques, and fraudulent accounts to deceive victims and illegally obtain their money or personal information. Algerian law has addressed this issue through the Penal Code and laws related to the prevention of cybercrime, imposing penalties such as imprisonment and fines on offenders. The seriousness of this crime lies in how difficult it is to track down perpetrators and how quickly such crimes spread across digital platforms. This makes it necessary to strengthen digital awareness, improve legal and technical protection measures, and encourage users to be more cautious when dealing with suspicious online sources and electronic transactions.

Keywords : Cyber fraud, online scams, cybercrime, Algerian legislation, phishing, digital evidence, cybersecurity, electronic payments, legal protection.

الشكر واليقين

بسم الله الرحمن الرحيم

(ربي أوزعني أن أشكر نعمتك التي أنعمت علي وعلى والدي وأن أعمل صالحا ترضاه

وأدخلني برحمتك في عبادك الصالحين) النمل الآية 91.

نشكر الله عز وجل ونحمده كل الحمد على نعمه التي انعم بها علينا ووفقنا إلى

إنهاء هذا العمل المتواضع، ونتقدم بالشكر إلى كل من علمنا علما نافعا، كما

توجه بالشكر الجزيل المرفق بأسمى عبارات التقدير والاحترام والامتنان إلى

الأستاذ المشرف سليلي محمد الصغير على كل النصيح والتوجيه والإرشاد وإلى كل

من ساهم في انجاز هذا العمل من قريب ومن بعيد ولوبكلمة طيبة

أو بإتسامة صادقة.

الحمد لله

الحمد لله الذي بفضلہ اتممت عملي ووقفني في مشوار حياتي

إلى من قال فيهم الرحمان بعد بسم الله الرحمان الرحيم

﴿وقضى ربك ألا تعبدوا إلا إياه وبالوالدين إحسانا﴾

إليك يا أمي يا من علمتني العطاء دون انتظار المقابل، يامن زرعتي في قلبي أسمى معاني الأفاضل.

وإلى ذلك السرح العظيم الذي علمني الخلق الكريم والذي الغالي صاحب الفضل الكبير.

أحمدك لكم عملك المتواضع

مع تمنياتي لكم بالنجاح والتوفيق في كل شأن الحياة.

والسلام
عليكم

الأم

﴿فرحس بما أتاكم الله من فضله﴾

هذه اللحظة لا تورث ولا تشتري، لقد دفعت ثمنها عمري وشبابي، سهري، خوفي ودموعي هي
لهفة الوصول ودمعة الحزن، فرحة العمر هذه هي النهاية السعيدة لبدايات أعظم وأصبح حلمي
حقيقة أهدي تخرجي إلى من هم كل ما أملك، إلى العمود الثابت في عثرات أيامي، إلى من هم
في الحياة حياة إلى من بدلو جهد السنين من أجلي «أبي، أمي» ولجدي التي كانت أمي الثانية
التي تمننت أن تراني في أعلى المراتب لكنها قد فارقت الحياة رحمها الله كما أهدي تخرجي إلى
زوجي الذي كان سندي وقوتي وعمودي ومصدر الصبر وإخوتي الذين كانوا لي عوناً وسنداً
ومصدر قوتي في لحظات الضعف والفشل وإلى أخواتي زهرات أيامي الذين كانوا بلسماً
في أوقات الضعف (رفيق، سهام، حفيظ، سعاد، محمد، آسيا، إيمان) وإلى كل من وقفوا بجانبني
في السراء والضراء ولكل روح عانقتني بالحب والدعوات والمهارة في طريقي وإلى كل أصدقائي
الذين شاركوني تفاصيل الرحلة وكانوا كنفاً يستند إليهم، شكراً لكل أساتذتي الكرام الذين أناروا
دربي بالعلم والمعرفة، شكراً لكل من علمني كلمة أو مهارة راجية من الله أن يجعله
خطوة نحو مستقبل أفضل ونجاح دائم.

قائمة المحتويات

الصفحة	العنوان
	ملخص
	الشكر
	الإهداء
1	مقدمة
الفصل الأول: الإطار العام لجريمة النصب والاحتيال الإلكتروني	
13	المبحث الأول: المفاهيم والأسس العامة لجريمة النصب والاحتيال الإلكتروني
13	المطلب الأول: تعريف النصب والاحتيال الإلكتروني فقهيًا وقانونيًا
13	الفرع الأول: بدايات الاحتيال باستخدام وسائل الاتصال التقليدية
14	الفرع الثاني: ظهور الاحتيال الرقمي مع بدايات الإنترنت
16	الفرع الثالث: تطور الاحتيال الإلكتروني في بداية الألفية الجديدة
17	المطلب الثاني: المقصود بالنصب والإحتيال الإلكتروني
17	الفرع الأول: تعريف النصب و الإحتيال
20	المطلب الثاني: خصائص جريمة النصب والاحتيال الإلكتروني.
24	المطلب الثالث: تمييز جريمة النصب والاحتيال الإلكتروني عن الجرائم الإلكترونية الأخرى.
24	الفرع الأول : أهم أنواع الجرائم الإلكترونية
31	الفرع الثاني : الفرق بين جريمة النصب والاحتيال الإلكتروني والجرائم الإلكترونية الأخرى
34	المبحث الثاني: أركان ووسائل إرتكاب جريمة النصب والاحتيال الإلكتروني واثارها
35	المطلب الأول: وسائل ارتكاب جريمة النصب والاحتيال الإلكتروني
35	الفرع الأول: التصيد الإلكتروني (Phishing)
36	الفرع الثاني: إنشاء مواقع إلكترونية وهمية
37	الفرع الثالث: انتحال الهوية الرقمية

قائمة المحتويات

39	الفرع الرابع: البرمجيات الخبيثة(Malware)
40	الفرع الخامس: الهندسة الاجتماعية(Social Engineering)
41	المطلب الثاني : الآثار المترتبة على جريمة النصب والاحتيال الإلكتروني
42	الفرع الأول: الآثار النفسية والاجتماعية على الضحايا
43	الفرع الثاني: الآثار الاقتصادية لجريمة الاحتيال الإلكتروني
44	الفرع الثالث : تأثير الاحتيال الإلكتروني على الثقة في الدولة ومؤسساتها
45	خلاصة الفصل الأول
الفصل الثاني: الإطار القانوني وسبل مكافحة جريمة النصب والاحتيال الإلكتروني	
48	المبحث الأول: الأحكام القانونية المنظمة لجريمة الاحتيال الإلكتروني في التشريع الجزائري
48	المطلب الأول: النصوص التشريعية المتعلقة بجريمة النصب والاحتيال الإلكتروني
57	المطلب الثاني: إجراءات المتابعة القضائية لمرتكبي جريمة النصب و الاحتيال الإلكتروني
61	المبحث الثاني: سبل مكافحة جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري
61	المطلب الأول: التدابير الوقائية (التوعية، الأمن السيبراني، دور الإعلام)
64	المطلب الثاني: الإصلاحات القانونية والتقنية لمكافحة الجريمة (تشديد العقوبات، التعاون القضائي، الأدوات التقنية)
77	المطلب الثالث: الجهود الوطنية في مواجهة النصب والاحتيال الإلكتروني (الشرطة، القضاء، التعاون البنكي)
81	خلاصة الفصل الثاني
83	خاتمة
86	قائمة المراجع

مقدمة :

مقدمة :

في العصر الحالي، الذي يتميز بسرعة تطور التكنولوجيا وانتشار الإنترنت، أصبح العالم مكانًا مترابطًا بفضل تطور وسائل الاتصال الرقمية. هذه الثورة الرقمية غيرت الطريقة التي يعمل بها الأفراد، المؤسسات، والحكومات على حد سواء، وفتحت آفاقًا جديدة للنشاطات الاقتصادية، الاجتماعية، والتعليمية. ومع هذه التغيرات الكبيرة، ظهرت العديد من الفرص والتهديدات في الوقت ذاته، مما جعل التقنيات الحديثة أداة فعالة في يد المجرمين لتحقيق أهدافهم بطرق لم تكن ممكنة في السابق. ومن بين أبرز التحديات التي فرضها هذا التقدم التكنولوجي تبرز جريمة النصب والاحتيال الإلكتروني، باعتبارها أحد أخطر مظاهر الانحراف الإجرامي الرقمي التي تهدد الأفراد والمجتمعات على حد سواء.

تُعد جريمة النصب والاحتيال الإلكتروني من الجرائم المستحدثة، التي فرضها تطور شبكات المعلومات وأنظمة الحوسبة، حيث بات بإمكان الجناة استغلال الثغرات التقنية لتحقيق مكاسب غير مشروعة. ولم يعد هذا الفعل الإجرامي يقتصر على الخداع البسيط، بل اتخذ أشكالًا أكثر تعقيدًا وتنوعًا، تبدأ من الاحتيال على الحسابات البنكية، وتصل إلى التلاعب في المعاملات التجارية عبر الإنترنت، وانتهاك الخصوصية الرقمية للمستخدمين. ويتسم هذا النوع من الجرائم بالخطورة المضافة التي يمنحها الطابع العابر للحدود، مما يزيد من تعقيد آليات مكافحته ويحد من فعالية الإجراءات القانونية الوطنية في مواجهته.

خلال السنوات الأخيرة، شهدت هذه الظاهرة توسعًا ملحوظًا من حيث الانتشار والحجم، لتصبح من أبرز التحديات القانونية التي تواجهها مختلف الأنظمة القضائية في العالم. وفي السياق الجزائري، تزايدت حالات النصب والاحتيال الإلكتروني مع ازدياد الاعتماد على الوسائط الرقمية، في ظل تزايد استخدام الإنترنت والخدمات الإلكترونية. وقد أضحت من الضروري أن تواكب المنظومة التشريعية هذا التطور، بما يضمن الحماية الفعالة للمجتمع الرقمي الناشئ، ويعالج مواطن القصور في النصوص القانونية التقليدية.

ولا تنحصر آثار هذه الجريمة في الجانب المالي فحسب، بل تمتد إلى الجانب النفسي والاجتماعي، حيث يعاني الضحايا من انعدام الشعور بالأمان وفقدان الثقة في البيئة الرقمية. مثل هذه التداعيات تُقضي إلى

تقليص التفاعل الآمن مع الخدمات الإلكترونية، وقد تؤدي إلى عزوف الأفراد عن استخدام الوسائل التكنولوجية الحديثة، بما يشكل عائقاً أمام التنمية الاقتصادية والتحول الرقمي في المجتمع.

يمتاز النصب والاحتيال الإلكتروني بخاصية فنية دقيقة، تتمثل في استخدام وسائل إلكترونية متطورة يصعب تعقبها، كالمواقع المزيفة، وحسابات البريد الإلكتروني الاحتيالية، وتقنيات الهندسة الاجتماعية، ما يجعل إثباته أمام القضاء مسألة معقدة تتطلب خبرة قانونية وتقنية متكاملة. وإذا كانت الجرائم التقليدية تُركّب من عناصر مادية ومعنوية مرئية ومباشرة، فإن هذا النمط الإجرامي يستدعي فهماً دقيقاً للوسائل الرقمية المستخدمة، مع تحديد الأركان التي تقوم عليها الجريمة من حيث السلوك الاحتيالي، القصد الجنائي، والنتيجة الضارة.

أهمية الموضوع:

وتبرز أهمية هذه الجريمة في ظل الحاجة إلى تمييزها عن باقي الجرائم الإلكترونية، التي قد تتشابه معها في الوسيلة التكنولوجية لكنها تختلف من حيث الغرض والبنية القانونية. فالنصب والاحتيال الإلكتروني يتفرد باعتماده على الخداع المقنع، واستغلال الثقة، والتخفي وراء قناع رقمي يصعب اختراقه. هذه الخصوصية تفرض ضرورة بناء تصور تشريعي واضح ودقيق، يأخذ في الحسبان واقع الجريمة، وطبيعة الأدوات المستخدمة فيها، وحدود المسؤولية الجنائية.

ولا يكتمل التصدي لهذه الجريمة دون النظر إلى المسار الوقائي، القائم على نشر التوعية، وتعزيز الثقافة القانونية لدى مستخدمي الإنترنت، وتدعيم البنية التحتية للأمن السيبراني. كما يفرض الواقع التكنولوجي المعاصر تطوير آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، بالنظر إلى أن الجناة غالباً ما ينفذون أفعالهم من خارج النطاق الإقليمي للدولة، مستغلين هشاشة التشريعات أو ضعف التنسيق بين الدول.

تفرض هذه الظاهرة على المشرع الجزائري أن يعيد النظر في الإطار القانوني المنظم لها، من خلال سنّ قواعد خاصة تواكب طبيعة هذه الجريمة، وتضع آليات فعالة للملاحقة والردع، سواء من خلال تشديد العقوبات، أو تسهيل إجراءات إثبات الجريمة الرقمية، أو تحديث آليات التعاون القضائي على المستويين

الوطني والدولي. كما أن تطوير الكفاءات التقنية لدى الجهات القضائية والأمنية يُعد ضرورة حتمية لضمان الفعالية في مكافحة النصب والاحتيال الإلكتروني، وحماية المجتمع من مخاطره.

أهداف الموضوع:

- التعريف بجريمة النصب والاحتيال الإلكتروني.
- تمييز جريمة النصب والاحتيال الإلكتروني عن باقي الجرائم الإلكترونية.
- التعرف على مختلف الأساليب التي يتبعها الجناة للقيام بالنصب والاحتيال الإلكتروني.
- التعرف على القوانين والتشريعات الجزائية فيما يخص النصب والاحتيال الإلكتروني.
- اقتراح حلول ومقترحات تشريعية لتطوير آليات قانونية للمكافحة والوقاية من جريمة النصب والاحتيال الإلكتروني.

أسباب اختيار الموضوع:

تعود أسباب اختيار الموضوع أساسا لما يلي:

✓ أسباب موضوعية:

- **الانتشار الواسع لجريمة النصب والإحتيال الإلكتروني:** مع زيادة الاعتماد على الإنترنت في مختلف المجالات، أصبح النصب والاحتيال الإلكتروني يشكل تهديداً متزايداً على الأفراد والشركات في الجزائر.
- **تحديات التشريع الجزائري:** رغم وجود قوانين تخص مكافحة الجرائم الإلكترونية، إلا أن التشريع الجزائري لا يزال يواجه صعوبة في تقديم تعريفات قانونية دقيقة وكافية لهذه الجرائم.
- **زيادة الجرائم المرتكبة عبر الإنترنت:** إن النصب والاحتيال الإلكتروني في الجزائر يتزايد، ويستغل المجرمون الثغرات الأمنية في الأنظمة الرقمية لتحقيق مكاسب غير مشروعة.
- **عدم كفاية الآليات القانونية:** على الرغم من بعض التطورات في التشريع الجزائري، إلا أن هناك فجوات تشريعية في التعامل مع الجرائم الإلكترونية وتطبيق القوانين ذات الصلة.

✓ أسباب ذاتية:

- الاهتمام الشخصي بالتكنولوجيا الحديثة: كوننا أشخاص ملمين بالفضاء الرقمي و تواجد أحدنا في مجال العمل عبر الإنترنت، فإننا نتعامل يوميًا مع الأدوات الرقمية وأنظمة الدفع الإلكتروني، مما يجعلنا مدركين تمامًا للمخاطر التي قد تنشأ من استخدام هذه التقنيات بشكل غير قانوني. هذا الأمر دفعنا إلى دراسة آثار جريمة النصب والاحتيال الإلكتروني التي تهدد هذا المجال.
- الاهتمام بالذكاء الاصطناعي: في ظل تطور تقنيات الذكاء الاصطناعي، يمكن للمجرمين الاستفادة من هذه الأدوات في تنفيذ عمليات احتيالية معقدة. كنت أرغب في توضيح العلاقة بين التقنيات الحديثة وكيف يمكن للمجرمين استغلالها في ارتكاب الجرائم الإلكترونية، وخاصة النصب والاحتيال الإلكتروني.
- الرغبة في تعزيز الوعي القانوني: باعتباري شخصًا مهتمًا بالقانون، أرى أن هناك حاجة ماسة لتعزيز الوعي العام حول تأثير الجرائم الإلكترونية على الأفراد، وكيفية تحديد المسؤوليات القانونية لهذه الجرائم. لذلك، كان اختياري لهذا الموضوع نابغًا من رغبتي في المساهمة في نشر المعرفة القانونية المتعلقة بكيفية مكافحة النصب والاحتيال الإلكتروني في الجزائر.

صعوبات الموضوع:

- قلة المراجع المتاحة ومحدودية المصادر القانونية والفقهية المتعلقة بالنصب والاحتيال الإلكتروني في التشريع الجزائري.
- عدم توفر دراسات وأبحاث معمقة حول جريمة النصب والاحتيال الإلكتروني في الجزائر، حيث يعد هذا الموضوع حديثًا نسبيًا.
- غموض بعض النصوص القانونية المتعلقة بالجرائم الإلكترونية في الجزائر وعدم وضوح تطبيقها على جريمة النصب والاحتيال الإلكتروني.
- قصر الوقت المخصص لتحضير المذكرة، خاصة لموضوع حديث مثل النصب والاحتيال الإلكتروني في التشريع الجزائري.

الدراسات السابقة:

1- دراسة شهيرة بولحية ودنيا زاد سويح بعنوان: “الاحتيال الإلكتروني”، المنشورة بمجلة الدراسات القانونية والاقتصادية، المجلد 02، العدد 02، سنة 2019.

تناولت هذه الدراسة جريمة الاحتيال الإلكتروني باعتبارها من أبرز الجرائم المستحدثة الناتجة عن الانتشار الواسع لتكنولوجيات الإعلام والاتصال وشبكة الإنترنت، حيث ركزت الباحثتان على بيان العلاقة بين التطور الرقمي وظهور أنماط جديدة من الجرائم المعلوماتية تختلف عن الجرائم التقليدية من حيث الوسائل وطبيعة التنفيذ. كما أوضحت الدراسة أن الاحتيال الإلكتروني يعتمد أساسًا على أساليب الغش والخداع باستعمال الوسائط المعلوماتية والبيانات الإلكترونية بهدف الاستيلاء على أموال الغير بطريقة غير مشروعة.

كما أبرزت الدراسة الخصائص المميزة لهذا النوع من الجرائم، والمتمثلة في سهولة ارتكابها، وسرعة انتشارها عبر الحدود، وصعوبة اكتشاف مرتكبيها بسبب الطابع التقني الذي تتسم به البيئة الرقمية. وخلصت الدراسة إلى أن مكافحة الاحتيال الإلكتروني لا يمكن أن تتحقق فقط عبر النصوص القانونية، وإنما تستوجب أيضًا توفير حماية تقنية وتوعية رقمية للمستخدمين.

وتتقاطع هذه الدراسة مع موضوع بحثنا من حيث تناولها لجريمة الاحتيال الإلكتروني، غير أن دراستنا تنفرد بالتركيز بصورة أعمق على موقف المشرع الجزائري من جريمة النصب والاحتيال الإلكتروني وآليات مكافحتها في ظل تطور الوسائل الرقمية الحديثة.

2- دراسة حسن كليبي ونجمة الطيب بعنوان: “جريمة النصب الإلكتروني من منظور المشرع الجزائري”، المنشورة بمجلة المفكر، المجلد 20، العدد 01، سنة 2025.

ركزت هذه الدراسة على معالجة جريمة النصب الإلكتروني من الناحية القانونية في التشريع الجزائري، حيث تناول الباحثان مفهوم النصب الإلكتروني باعتباره صورة حديثة من صور الاحتيال المرتبط باستخدام التكنولوجيا الحديثة والفضاء الافتراضي. كما أوضحت الدراسة أن التطور التكنولوجي، رغم ما حققه من تسهيل للمعاملات اليومية، أفرز في المقابل بيئة خصبة لنشاط المجرمين الإلكترونيين وصعوبة تعقبهم.

كما قامت الدراسة بتحليل النصوص القانونية التي اعتمدها المشرع الجزائري لمواجهة هذا النوع من الجرائم، مع إبراز أركان الجريمة والعقوبات المقررة لها، إضافة إلى توضيح أهم الأساليب الاحتيالية المستعملة إلكترونياً، مثل انتحال الهوية والتلاعب بالمعلومات والخداع عبر الوسائط الرقمية. وقد توصل الباحثان إلى أن المشرع الجزائري حاول مسايرة التطور الرقمي من خلال تعديل قانون العقوبات وإدراج نصوص خاصة بالجرائم الإلكترونية، إلا أن التطور السريع لأساليب الاحتيال ما يزال يفرض تحديات عملية وقانونية مستمرة.

وتتشابه هذه الدراسة مع موضوع بحثنا بصورة كبيرة، إلا أن بحثنا يسعى إلى التوسع أكثر في دراسة صور الاحتيال الإلكتروني وبيان الجوانب الوقائية والإجرائية المتعلقة بمكافحته.

3- دراسة سامية العايب ومنال عرابة بعنوان: “ الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني ”، المنشورة بمجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 05، العدد 03، سنة 2021.

تناولت هذه الدراسة موضوع الحماية الجزائية للمستهلك الإلكتروني في مواجهة جرائم النصب الإلكتروني، خاصة في ظل التوسع الكبير للتجارة الإلكترونية واعتماد الأفراد على المعاملات الرقمية في إبرام العقود وشراء السلع والخدمات. وقد ركزت الدراسة على بيان مدى تعرض المستهلك الإلكتروني لمختلف صور الاحتيال والخداع عبر المنصات الإلكترونية بسبب ضعف الخبرة التقنية وصعوبة التحقق من مصداقية التعاملات الإلكترونية.

كما أوضحت الدراسة أن المشرع الجزائري حاول توفير حماية قانونية للمستهلك الإلكتروني من خلال إصدار القانون رقم 05-18 المتعلق بالتجارة الإلكترونية، غير أن البيئة الرقمية ما تزال بحاجة إلى رقابة أكثر فعالية وآليات قانونية وتقنية أكثر تطوراً للحد من الجرائم الإلكترونية. وانتهت الدراسة إلى أن الحماية الجزائية للمستهلك الإلكتروني لا تتحقق فقط بتشديد العقوبات، بل تتطلب أيضاً رفع مستوى الوعي الرقمي وتفعيل وسائل الرقابة الإلكترونية.

وتلتقي هذه الدراسة مع موضوع بحثنا في تناولها لجريمة النصب الإلكتروني، غير أن دراستنا تتناول الجريمة من زاوية أوسع تشمل مفهومها وأركانها وصورها المختلفة وسبل مكافحتها في التشريع الجزائري.

4- دراسة سفيان صوان بعنوان: “ الجريمة الإلكترونية في التشريع الجزائري: دراسة مقارنة ”، دار الهدى، الجزائر، سنة 2020.

تناولت هذه الدراسة موضوع الجريمة الإلكترونية بصفة عامة في التشريع الجزائري، حيث سعى الباحث إلى توضيح مفهوم الجرائم الإلكترونية وخصائصها وأهم صورها المستحدثة، مع مقارنة بعض النصوص القانونية الجزائرية بالتشريعات الأجنبية. كما ركزت الدراسة على الطبيعة الخاصة للجريمة الإلكترونية التي تختلف عن الجرائم التقليدية من حيث الوسيلة الإجرامية وصعوبة الإثبات والامتداد العابر للحدود.

كما تعرض الباحث لمختلف الجرائم الواقعة على الأنظمة المعلوماتية، وبين الصعوبات العملية التي تواجه سلطات الضبط والتحقيق في تعقب المجرمين الإلكترونيين، خاصة مع التطور المستمر للتقنيات الحديثة. وخلصت الدراسة إلى أن المشرع الجزائري حاول التكيف مع التطور الرقمي من خلال سن قوانين خاصة بالجرائم الإلكترونية، إلا أن التطبيق العملي ما يزال يواجه العديد من الإشكالات التقنية والقانونية.

وتتقاطع هذه الدراسة مع موضوع بحثنا من حيث تناول الجرائم الإلكترونية بصفة عامة، بينما تتميز دراستنا بالتركيز على جريمة النصب والاحتيال الإلكتروني باعتبارها من أخطر الجرائم المستحدثة في البيئة الرقمية.

5- دراسة أمال دبز بعنوان: “ جريمة النصب والاحتيال في مجال الأعمال ”، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة.

تناولت هذه الدراسة جريمة النصب والاحتيال في المجال الاقتصادي والتجاري، حيث ركزت الباحثة على تحليل الأركان القانونية للجريمة وبيان الوسائل الاحتمالية التي يعتمد عليها الجناة للإيقاع بالضحايا والاستيلاء على أموالهم. كما تناولت الدراسة آثار جرائم الاحتيال على المعاملات التجارية والثقة الاقتصادية داخل المجتمع.

وأوضحت الدراسة أن التطور الاقتصادي والتكنولوجي أدى إلى ظهور أشكال حديثة ومتطورة من جرائم الاحتيال، خاصة مع توسع استخدام الوسائط الرقمية في المعاملات المالية والتجارية، الأمر الذي فرض على التشريعات الحديثة ضرورة تطوير آليات المواجهة القانونية والوقائية لهذه الجرائم.

وتتشابه هذه الدراسة مع موضوع بحثنا في تناول جريمة الاحتيال، غير أن موضوع بحثنا يركز بصورة خاصة على النصب والاحتيال الإلكتروني باعتباره صورة حديثة مرتبطة باستخدام تكنولوجيا الإعلام والاتصال والفضاء الرقمي.

الإشكالية الرئيسية:

ساهم التقدم الهائل في تكنولوجيا المعلومات والاتصال، وانتشار استخدام الإنترنت، في ظهور أنماط جديدة من الجرائم، تُرتكب بوسائل إلكترونية، وبأساليب معقدة تعتمد على استغلال الثغرات التقنية وخداع الضحايا عبر الفضاء الرقمي. ومن بين أخطر هذه الجرائم المستحدثة تبرز جريمة النصب والاحتيال الإلكتروني، التي أصبحت تُهدد الأفراد والمؤسسات، وتُلحق أضرارًا جسيمة بالثقة العامة في المعاملات الإلكترونية.

إن الطبيعة غير المادية لهذا النوع من الجرائم، والسرعة التي يتم بها ارتكابها، إلى جانب صعوبة إثباتها وتعقيدات ملاحقة مرتكبيها، تجعل من مواجهتها القانونية تحديًا حقيقيًا للمنظومة القضائية والتشريعية. وتزداد هذه التحديات وضوحًا في البيئة الجزائرية، التي لا تزال في طور بناء منظومة قانونية متكاملة في مجال مكافحة الجريمة الإلكترونية، وخصوصًا الاحتيال الرقمي.

ولأن النصب والاحتيال الإلكتروني يُعد من الجرائم ذات الطبيعة الخاصة، فإن التصدي له يتطلب فهماً دقيقاً للأركان المكونة له، والأساليب المعتمدة في ارتكابه، وكذا الآليات القانونية والتنظيمية الكفيلة بمكافحته ضمن الإطار القانوني الجزائري، فتُعد الحاجة حالية ملحة لوضع موضوع النصب والاحتيال الإلكتروني موضع الدراسة والتحليل القانوني، قصد الإحاطة بجوانبه المختلفة، وتبسيط الضوء على أركانه، ووسائل ارتكابه، وتحديد موقعه ضمن التشريع الجزائري، والوقوف على الثغرات القانونية والعملية التي تعيق مكافحته، واقتراح ما يمكن من حلول لتعزيز فعالية التصدي له.

وعليه وبناء على ما سبق يمكن صياغة إشكالية البحث على النحو الآتي:

ما هي جريمة النصب والاحتيال الإلكتروني، وكيف تعامل التشريع الجزائري معها في ظل التطورات التكنولوجية؟

تساؤلات فرعية:

ولمعالجة ودراسة هذه الإشكالية لابد من الإجابة عن التساؤلات الفرعية التالية:

ما المقصود بجريمة النصب والاحتيال الإلكتروني؟

• ما هي الخصائص التي تميز هذه الجريمة عن باقي الجرائم الإلكترونية؟

- ما هي الأركان التي تقوم عليها جريمة النصب والاحتيال الإلكتروني؟
- ما هي الأساليب والوسائل الأكثر استخدامًا في تنفيذ هذه الجريمة؟
- كيف تعامل التشريع الجزائري مع هذا النوع من الجرائم؟
- ما هي العقوبات المقررة في القانون الجزائري لمكافحة النصب الإلكتروني؟
- ما مدى فعالية الإجراءات الوقائية والأمنية والقضائية في التصدي لهذه الجريمة؟
- هل توجد آليات محلية لتعزيز التعاون لمواجهة النصب والاحتيال الإلكتروني في الجزائر؟

✓ منهج الدراسة:

منهج الدراسة التي تم اتباعها تعتمد على المنهج الوصفي ، من خلال وصف جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري، وتحليل الأبعاد القانونية والفقهية المتعلقة بها. كما إعتدناه المنهج التحليلي من خلال تحليل النصوص القانونية المتاحة وتفسيرها، ووسائل تنفيذها وآثارها على الأفراد والمجتمع.

كذلك المنهج الاستنباطي، لتقديم الاستنتاجات حول فعالية التشريعات الجزائرية في التصدي لهذه الجرائم بناءً على الدراسات النظرية والتحليل القانوني.

خطة وهيكلية البحث:

تم تقسيم هذه الدراسة إلى فصلين رئيسيين، حيث تناولنا في الفصل الأول الإطار العام لجريمة النصب والاحتيال الإلكتروني، من خلال التطرق إلى مفهوم هذه الجريمة والأسس العامة التي تقوم عليها، إضافة إلى دراسة أركانها والوسائل المعتمدة في ارتكابها، وكذا الآثار المترتبة عنها، وذلك ضمن مبحثين متكاملين يعكسان مختلف الجوانب النظرية لهذا النوع من الجرائم.

أما الفصل الثاني فقد خصص لمعالجة جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري، حيث قمنا بتشخيص مختلف النصوص القانونية الوطنية ذات الصلة، ثم تحليلها وتحليل مدى فعاليتها في مواجهة هذه الجريمة، مع إجراء مقارنة مع بعض التشريعات الدولية، بهدف الوقوف على أوجه التشابه والاختلاف وتحديد مدى نجاعة الإطار القانوني الجزائري في هذا المجال.

وقد اختُتمت هذه الدراسة بخاتمة تضمنت أهم النتائج المتوصل إليها، إلى جانب جملة من الاقتراحات والتوصيات التي نراها مناسبة لتعزيز الحماية القانونية من جرائم النصب والاحتيال الإلكتروني.

الفصل الأول
الإطار المفاهيمي
لجريمة النصب
والاحتيال الإلكتروني

تعتبر جريمة النصب والاحتيال الإلكتروني من بين الجرائم المستحدثة التي فرضها التطور السريع للتكنولوجيا الرقمية ووسائل التواصل الحديثة، إذ أصبح من الممكن لأي شخص استخدام الشبكة الإلكترونية لتحقيق مكاسب غير مشروعة، مستغلًا الثغرات التي توفرها هذه الوسائل. ويمثل هذا النوع من الجرائم تهديدًا خطيرًا للأفراد والمجتمعات على حد سواء، حيث يُمكن أن يتسبب في خسائر مادية ونفسية كبيرة.

إنّ النصب والاحتيال الإلكتروني لا يقتصر على الأساليب التقليدية التي كانت تعتمد على الخداع والمكر، بل يتخذ أشكالًا متنوعة تتماشى مع التطور التكنولوجي السريع، وتؤثر على مجالات متعددة مثل التجارة الإلكترونية، والحسابات البنكية الرقمية، وعمليات التوظيف عبر الإنترنت، وغيرها من النشاطات التي تسهل الاتصال بين الأفراد والشركات عبر الفضاء الإلكتروني.

يهدف هذا الجزء إلى وضع الإطار العام لجريمة النصب والاحتيال الإلكتروني من خلال تحديد ماهية جريمة النصب و الإحتيال الإلكتروني (المبحث الأول) . كما سيتم التعرف على وسائل إرتكاب جريمة النصب و الإحتيال الإلكتروني و الآثار القانونية المترتبة عليها (المبحث الثاني) .

المبحث الأول: ماهية جريمة النصب والاحتيال الإلكتروني.

أفرز التطور المتسارع لتكنولوجيات الإعلام والاتصال واقعاً إجرامياً جديداً، أصبحت فيه الوسائط الرقمية بيئة خصبة لظهور أنماط حديثة من الجرائم، وفي مقدمتها جريمة النصب والاحتيال الإلكتروني التي تعد من أخطر الجرائم المعلوماتية المعاصرة لما تتسم به من تعقيد تقني واتساع في نطاق آثارها. فلم يعد الاحتيال مرتبطاً بالوسائل التقليدية القائمة على المواجهة المباشرة بين الجاني والضحية، بل انتقل إلى الفضاء الرقمي مستغلاً السرعة والانتشار وسهولة إخفاء الهوية التي توفرها الشبكات الإلكترونية.

وانطلاقاً من ذلك، يقتضي فهم هذه الجريمة الإحاطة بمفهومها وأسسها التاريخية والقانونية، وكذا إبراز خصائصها وتمييزها عن باقي الجرائم الإلكترونية المشابهة. وعليه، سيتم في هذا المبحث التطرق إلى ماهية جريمة النصب والاحتيال الإلكتروني من خلال دراسة نشأتها وتعريفها وخصائصها (المطلب الأول)، ثم بيان أوجه التمييز بينها وبين الجرائم الإلكترونية الأخرى.

المطلب الأول: نشأة جريمة النصب والاحتيال الإلكتروني.

إن جريمة النصب والاحتيال الإلكتروني لم تظهر بصورة مفاجئة، وإنما جاءت نتيجة تطور تدريجي رافق تطور وسائل الاتصال والتكنولوجيا الحديثة، حيث انتقلت أساليب الخداع من الوسائل التقليدية البسيطة إلى تقنيات رقمية معقدة تستغل البيئة الإلكترونية لتحقيق أغراض غير مشروعة. وقد ساهم انتشار الإنترنت والخدمات الرقمية في توسيع نطاق هذه الجريمة، وجعلها أكثر احترافية وتأثيراً على الأفراد والمؤسسات.

ولأجل الإحاطة بهذه الجريمة من جوانبها المختلفة، يتعين بدايةً تتبع نشأتها التاريخية ومراحل تطورها عبر وسائل الاتصال التقليدية والرقمية، ثم الوقوف على المقصود بالنصب والاحتيال الإلكتروني من خلال التعريفات اللغوية والفقهية والقانونية، إضافة إلى إبراز أهم الخصائص التي تميزها عن غيرها من الجرائم الحديثة.

الفرع الأول: بدايات الاحتيال باستخدام وسائل الاتصال التقليدية

قبل ظهور الإنترنت والتقنيات الرقمية الحديثة، عرف العالم صوراً أولية من الاحتيال المرتبط بوسائل الاتصال التقليدية، حيث استغل بعض الأفراد التقنيات الناشئة آنذاك لتحقيق مكاسب غير مشروعة بطرق تقوم على الخداع واستغلال الثغرات التقنية. وقد شكلت هذه الممارسات النواة الأولى لتطور الجريمة الإلكترونية بمفهومها الحديث، خاصة مع انتقال وسائل الاحتيال من الاحتكاك المباشر إلى استغلال أنظمة الاتصال عن بعد.

ومن هذا المنطلق، سيتم التطرق إلى أبرز المراحل الأولى التي شهدت استغلال وسائل الاتصال التقليدية كالتلغراف والهاتف في تنفيذ أفعال احتيالية، وبيان أثر ذلك في ظهور الأنماط الأولى للجرائم ذات الطابع التقني.

تُعد جريمة النصب من أقدم أشكال الجرائم التي رافقت الإنسان منذ بدء التبادل الاقتصادي، وقد ارتبطت بالتطورات الاجتماعية والتقنية. فمع اختراع التلغراف في القرن التاسع عشر، استُخدمت هذه الوسيلة لأول مرة في تنفيذ عمليات احتيال تحمل سمات الجرائم الإلكترونية. ففي سنة 1834، أقدم شقيقان فرنسيان على استغلال شبكة التلغراف الفرنسية لنقل معلومات مالية حول البورصة، قبل أن تصل هذه البيانات إلى المستثمرين، ما مكنهما من جني أرباح خيالية من خلال المضاربة في السوق¹، ويمكن اعتبار هذه الواقعة أول جريمة "اختراق معلومات" مسجلة في التاريخ.

ومع ظهور الهاتف، توسعت أساليب الخداع لتشمل تحويل المكالمات بطريقة غير قانونية واستغلال الثغرات في شبكات الاتصال، وهي ما تُعرف لاحقاً بقرصنة الهواتف أو "phreaking". هذه الممارسات تُظهر كيف أن المجرمين كانوا دائماً في سباق مع الزمن لتطويع التكنولوجيا الناشئة بما يخدم أغراضهم الإجرامية. ويذهب بعض الباحثين إلى أن هذه المرحلة كانت بمثابة انتقال من الخداع التقليدي، الذي يتطلب تواصلاً مباشراً مع الضحية، إلى نمط جديد من الجريمة يعتمد على استغلال أنظمة تقنية دون الحاجة إلى تفاعل بشري مباشر مع الضحية، إلى نمط جديد من الجريمة يعتمد على استغلال أنظمة تقنية دون الحاجة إلى تفاعل بشري مباشر، مما يمثل تحولاً نوعياً في مفهوم الاحتيال².

الفرع الثاني : ظهور الاحتيال الرقمي مع بدايات الإنترنت

أدى الانتشار الواسع لشبكة الإنترنت خلال تسعينيات القرن الماضي إلى تحول جذري في أساليب الاحتيال، حيث ظهرت ممارسات إجرامية جديدة تعتمد على البيئة الرقمية كوسيلة رئيسية للخداع والاستيلاء على المعلومات والأموال. وقد ساهم البريد الإلكتروني وغرف المحادثة والمنصات الإلكترونية الأولى في فتح المجال أمام المحتالين لتطوير أساليب أكثر تعقيداً وانتشاراً.

Apsimet, N., Smanova, A., & Utegenova, G. The Role of the Internet in the Evolution of Fraud. Bulletin of 1 (2024)., p. 248..L.N. Gumilyov ENU

Apsimet, N., Smanova, A., & Utegenova, G 2 نفس المرجع، ص 249 .

وعليه، سيتم في هذا الفرع إبراز بدايات الاحتيال الرقمي، خاصة من خلال ظهور التصيد الإلكتروني والبرمجيات الخبيثة، وبيان كيف ساهمت هذه الوسائل في تشكيل أولى صور النصب الإلكتروني المنظم.

مع بروز شبكة الإنترنت في تسعينيات القرن الماضي، وخصوصًا بعد تعميم استخدام البريد الإلكتروني، بدأت تظهر ممارسات احتيالية ذات طابع جديد كليًا. وتمثل التصيد الاحتيالي (Phishing) أبرز هذه الأنماط، حيث يستدرج المجرمون الضحايا من خلال رسائل بريد إلكتروني مزيفة تبدو وكأنها من مؤسسات موثوقة.

وقد سجل عام 1995 أول ظهور فعلي لمصطلح "phishing"، حين طُوّر برنامج "AOHell" لاختراق حسابات مستخدمي منصة America Online (AOL). استخدم البرنامج خوارزميات لتوليد أرقام بطاقات ائتمان عشوائية، وأتاح إرسال رسائل زائفة تطلب من المستخدمين تزويد المخترقين بمعلومات حساسة مثل كلمات السر¹.

وقد علّق مطور البرنامج، Koceilah Rekouche، في مذكراته قائلاً: "لقد بدأ التصيد كحيلة شبابية للتمرد الرقمي، لكنه سرعان ما تحول إلى آلية حقيقية للسرقة المنظمة"².

يُظهر هذا المثال كيف انتقل النصب الإلكتروني من الاستخدامات البسيطة إلى نماذج أكثر تنظيمًا، وكيف تطورت أدوات الجريمة لتصبح أكثر سهولة وانتشارًا، مما يتطلب من المشرع الجنائي مسايرة هذا التطور في أساليب الاحتيال. ومع نهاية التسعينيات، ظهرت كذلك البرمجيات الخبيثة مثل "حصان طروادة" و "Keyloggers" التي تُستخدم للتجسس على أنشطة المستخدمين وسرقة بيانات الدخول للحسابات البنكية والبريد الإلكتروني.

وتمثل هذه البرمجيات تطورًا خطيرًا لأنها تعمل بصمت وتنتقل عبر الروابط والمرفقات الإلكترونية بسهولة، مما جعلها من الأدوات الأساسية في ترسانة مجرمي الإنترنت.

¹ Rekouche, K. (2011). Early Phishing. ArXiv, p. 2

² نفس المرجع، ص3.

كما أن ظهور برامج المحادثة مثل ICQ و MSN Messenger ساهم في تسهيل عمليات الاحتيال من خلال إنشاء هويات مزيفة والتواصل مع الضحايا بصورة مباشرة، وهي ممارسات سبقت ظهور شبكات التواصل الاجتماعي ولكنها حملت معها نفس الديناميكية في استغلال الثقة بين الأطراف.

الفرع الثالث : تطور الاحتيال الإلكتروني في بداية الألفية الجديدة

شهدت بداية الألفية الثالثة تطوراً ملحوظاً في جرائم الاحتيال الإلكتروني، سواء من حيث الوسائل المستخدمة أو حجم الأضرار المترتبة عنها، إذ أصبحت الهجمات أكثر تنظيماً واحترافية، وتوسعت لتشمل المؤسسات المالية ومنصات الدفع الإلكتروني والمستخدمين عبر مختلف أنحاء العالم. كما ظهرت جماعات إجرامية متخصصة تستغل التطور التكنولوجي لتحقيق أرباح ضخمة بطرق غير مشروعة.

وفي هذا الإطار، سيتم تناول أبرز مظاهر تطور الاحتيال الإلكتروني خلال هذه المرحلة، مع بيان دور التطور التقني والعولمة الرقمية في تعقيد أساليب الجريمة وفرض تحديات جديدة على التشريعات الجنائية.

مع دخول الألفية الثالثة، شهدت جريمة النصب الإلكتروني طفرة كبيرة على مستوى التقنيات المستخدمة ونطاق الضحايا المستهدفين. أصبحت الهجمات أكثر تنظيماً وتنوعاً، ولم تعد تقتصر على البريد الإلكتروني فقط، بل شملت مواقع إلكترونية مزيفة، رسائل نصية، وحتى تطبيقات الهواتف المحمولة.

بدأ المحتالون في استهداف البنوك ومواقع الدفع الإلكتروني، حيث تعرض موقع E-Gold لهجوم في يونيو 2001، تبعه استهداف مباشر لمنصة PayPal من خلال تسجيل نطاقات شبيهة بموقع الشركة الأصلي لإرسال رسائل بريدية وهمية تطلب من المستخدمين تحديث بياناتهم المالية¹.

في الفترة بين مايو 2004 ومايو 2005، تم تسجيل خسائر قدرها 929 مليون دولار بسبب هجمات التصيد الاحتيالي في الولايات المتحدة فقط².

¹ IEEE I2CT 'Shete, N. L., Maddel, M. M., & Shaikh, Z., A Comparative Analysis of Cybersecurity Scams Conference، 2024، ص. 4.

² نفس المرجع، ص. 5.

كما ظهرت مجتمعات رقمية متخصصة في الجريمة المنظمة، مثل "ShadowCrew"، والتي وصفها مكتب التحقيقات الفيدرالي بأنها "أول منظمة إجرامية متخصصة في الجرائم الإلكترونية". كان هذا المجتمع الإلكتروني يعرض بيانات بطاقات ائتمان مسروقة، ويوفر منتديات لتبادل المعرفة في مجال القرصنة¹.

وقد ساهمت أيضًا وسائل الإعلام في نقل الوعي بهذه الظواهر الجديدة، حيث بدأت تقارير إخبارية وتحقيقات تلفزيونية في تسليط الضوء على ضحايا الاحتيال الإلكتروني، مما زاد من الضغط على الحكومات لتطوير تشريعات خاصة بالأمن السيبراني. وقد بادرت بعض الدول إلى إنشاء وحدات شرطة متخصصة في مكافحة الجريمة الإلكترونية، كما ظهرت اتفاقيات دولية كاتفاقية بودابست (2001) لمحاربة الجرائم الرقمية، والتي تضمنت توصيات واضحة بشأن جريمة الاحتيال الإلكتروني.

إلى جانب ذلك، بدأت منصات التجارة الإلكترونية والبنوك في اعتماد بروتوكولات تحقق ثنائية، وفرض قيود أمنية على المعاملات المالية عبر الإنترنت، في محاولة لتقليل الثغرات التي يستغلها المحتالون.

المطلب الثاني: المقصود بالنصب والاحتيال الإلكتروني

يُعد تحديد المقصود بجريمة النصب والاحتيال الإلكتروني خطوة أساسية لفهم طبيعتها القانونية وتمييزها عن غيرها من الجرائم المشابهة، خاصة وأن هذه الجريمة تجمع بين عناصر النصب التقليدي والوسائل التقنية الحديثة. لذلك، فإن ضبط مفهومها يقتضي العودة إلى المعاني اللغوية والفقهية لكل من النصب والاحتيال، ثم إسقاط هذه المفاهيم على البيئة الإلكترونية الحديثة.

ومن هذا المنطلق، سيتم التطرق في هذا المطلب إلى تعريف النصب والاحتيال في اللغة والاصطلاح والقانون، ثم بيان مفهوم النصب والاحتيال الإلكتروني وخصائصه الأساسية التي تمنحه طابعًا إجراميًا مميزًا.

الفرع الأول: تعريف النصب و الاحتيال

يشكل تعريف النصب والاحتيال الأساس الذي تُبنى عليه الدراسة القانونية لجريمة الاحتيال الإلكتروني، إذ لا يمكن فهم الطبيعة الحديثة لهذه الجريمة دون الإحاطة بالمفاهيم التقليدية المرتبطة بالخداع والتدليس والاستيلاء غير

¹ نفس المرجع، ص. 6.

المشروع على أموال الغير. وقد تناول الفقه والقانون هذه المفاهيم بتعريفات متعددة ركزت في مجملها على عنصر التضليل وإيقاع المجني عليه في الغلط لتحقيق منفعة غير مشروعة.

وعليه، سيتم في هذا الفرع التطرق إلى تعريف النصب والاحتيال من الناحية اللغوية والاصطلاحية والقانونية، ثم الانتقال إلى تحديد مفهوم النصب والاحتيال الإلكتروني باعتباره صورة حديثة لهذه الجريمة في البيئة الرقمية.

أولاً : تعريف النصب

لغة: هو الكذب، والخداع والاحتيال، سواء إقترن بجرم أخذ المال أم لا، ويطلق العرب كلمة النصب عن قريب من المخادعة والحيلة¹.

إصطلاحاً: يعرف النصب إصطلاحاً بأنه إستخدام الخداع والتضليل عمداً لإيهام شخص أو جهة بمعلومات زائفة، بهدف إقناعه بالتصرف بطريقة تؤدي إلى نقل أموال أو ممتلكات إليه دون وجه حق. بمعنى آخر، يعتبر النصب استخدام أساليب احتيالية تعتمد على الكذب والتزييف لتحقيق مكاسب غير مشروعة على حساب المجني عليه.

فالنصب يقوم على عنصر الإحتيال حيث نص قانون العقوبات الجزائري في المادة 372 على أن كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالإحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما بإستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو إعتقاد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار².

¹ أمال دبز، "جريمة النصب والاحتيال في مجال الأعمال"، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، ص. 5

² قانون العقوبات الجزائري، المادة 372، الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المعدل والمتمم.

ثانيا :تعريف الإحتيال

لغة: الإحتيال هو الحذق، وجودة النظر، والقدرة على دقة التصرف، والاحتيال والمحاولة: مطالبتك الشيء بالحيل، والحيل، والحيلة هي المكر والخديعة والكيد لكل فعل يقصد فاعله به خلاف مايقضيه ظاهره¹.

إصطلاحا: الاحتيال هو التلاعب بالحقيقة أو إستغلال المراكز القانونية، الإقتصادية أو الإجتماعية، من خلال وسائل غير مشروعة تؤدي إلى إيقاع المجني عليه في وهم أو إلزام غير مدروس، مما يدفعه إلى التصرف بطريقة تلحق به ضررا، وتحقق للجاني مكاسب غير مشروعة .ويشمل الاحتيال مختلف الأساليب دون الحاجة إلى اللجوء إلى القوة أو التهديد المباشر .

ثالثا : تعريف النصب والإحتيال الإلكتروني:

يمكن تعريف الاحتيال الإلكتروني بأنه: كل سلوك احتيالي يتم عبر شبكة الإنترنت أو باستخدام إحدى الوسائل التقنية الحديثة كالحواسيب، أو شبكات الاتصالات، أو التطبيقات الرقمية، يكون من شأنه خداع الضحية والاستيلاء على أمواله أو بياناته أو منفعته، سواء بشكل مباشر أو غير مباشر، وبغرض تحقيق مكاسب غير مشروعة من خلال الخداع أو التلاعب أو انتحال الصفة. وقد يأخذ هذا السلوك مظاهر متعددة، مثل إرسال رسائل إلكترونية مزيفة، إنشاء مواقع وهمية، أو استغلال تطبيقات المحمول أو وسائل التواصل الاجتماعي في عمليات مقنّعة تخفي النية الاحتيالية خلف واجهات مزيفة.

وبناءً على ذلك، فإن الاحتيال الإلكتروني لا يُعدّ مجرد امتداد رقمي للاحتيال التقليدي، بل هو جريمة نوعية مستقلة من حيث الوسائل المستخدمة، والآثار المترتبة عنها، والأطراف المستهدفة بها. ولذلك، فإن تجريم هذا الفعل يتطلب اجتهداً تشريعياً خاصاً يأخذ بعين الاعتبار الطابع التقني والبعد العابر للحدود لهذه الجريمة².

وبالرجوع إلى أدبيات الفقه القانوني، نجد أن الباحث أحمد محمد عبد الرؤوف المنيفي عرّف الاحتيال عبر الإنترنت

¹ شهيرة بولحية، دنيا زاد سويح، "الإحتيال الإلكتروني"، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس - بركة، العدد 04، ديسمبر 2019، ص. 38.

² القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

بأنه "استعمال خدمة أو برنامج من برامج الإنترنت للوصول إلى الضحايا وإجراء عمليات احتيالية عليهم، مثل استخدام البريد الإلكتروني أو مواقع الويب أو غرف الدردشة أو الرسائل الإلكترونية لطلب معلومات أو تنفيذ معاملات مزيفة"¹.

غير أن هذا التعريف، على أهميته، لا يعكس إلا جزءاً من الصورة الكاملة، إذ يغفل بعض الأبعاد النفسية والاجتماعية والتقنية التي باتت تشكل جزءاً لا يتجزأ من هذه الجريمة.

لذلك، ومن خلال استقراء للنصوص والدراسات، يمكننا تعريف جريمة النصب والاحتيال الإلكتروني بأنها كل سلوك مادي أو معنوي يصدر عن شخص طبيعي أو معنوي، يستخدم فيه إحدى الوسائل التقنية الحديثة، كالإنترنت أو شبكات الاتصالات أو البرامج أو التطبيقات، بقصد إيهام الغير بوجود أمر غير حقيقي أو إخفاء الحقيقة عنه، من أجل خداعه والاستيلاء على أمواله أو بياناته أو منفعته، سواء تم ذلك من داخل الإقليم الوطني أو من خارجه، وبما يشكل خرقاً لأحكام القانون ويؤدي إلى ضرر بالمجني عليه.

المطلب الثاني: خصائص جريمة النصب والاحتيال الإلكتروني.

تتميز جريمة النصب والاحتيال الإلكتروني بجملة من الخصائص التي تجعلها تختلف عن الجرائم التقليدية، سواء من حيث الوسائل المستخدمة أو طبيعة السلوك الإجرامي أو الآثار المترتبة عنها. فهي جريمة تعتمد على التكنولوجيا الحديثة، وتتسم بسرعة الانتشار وصعوبة الكشف، فضلاً عن طابعها العابر للحدود. ومن أجل الإحاطة بهذه الخصائص، سيتم في هذا الفرع دراسة أهم السمات التي تميز جريمة النصب والاحتيال الإلكتروني، وبيان أثرها على الجوانب القانونية والأمنية المرتبطة بمكافحة هذا النوع من الجرائم. تُعد جريمة النصب والاحتيال الإلكتروني من أبرز صور الجريمة المعلوماتية التي فرضها التطور التقني المعاصر، وقد تميزت بعدة خصائص جوهرية جعلتها محل اهتمام خاص من قبل الفقه والتشريع، وذلك بالنظر إلى طبيعتها التقنية المعقدة وآثارها الاجتماعية والاقتصادية الواسعة.

1 أحمد محمد عبد الرؤوف المنيفي، الاحتيال الإلكتروني وحكمه في الإسلام والقوانين المعاصرة، مكتبة نور، دون ذكر البلد، 2021، ص. 6.

أولا :الاعتماد الكامل على الوسائط الإلكترونية كوسيلة ارتكاب:

تُرتكب جريمة الاحتيال الإلكتروني من خلال استغلال البيئة الرقمية الحديثة، حيث يستخدم الفاعل الإنترنت، والبريد الإلكتروني، وتطبيقات الهواتف الذكية، ومنصات التواصل الاجتماعي، كأدوات رئيسية لتنفيذ أفعاله الإجرامية. وتُتيح هذه الوسائط الإلكترونية إمكانية الوصول إلى عدد غير محدود من الضحايا بسرعة فائقة، مع القدرة على إخفاء الهوية باستخدام تقنيات مثل الشبكات الخاصة الافتراضية (VPN) أو التصفح المجهول¹.

يُلاحظ أن هذا الاعتماد على الوسائل التقنية يخلق تحديات كبرى فيما يتعلق بالإثبات الجنائي، إذ يصبح من الصعب تتبع مصدر الجريمة أو تحديد هوية الجاني بدقة، وهو ما فرض على التشريعات تبني وسائل تحقيق خاصة مثل التحري الإلكتروني وتحليل الأدلة الرقمية.

ثانيا : جوهر الجريمة هو التدليس والخداع التقني:

يُشكل التدليس والخداع لب هذه الجريمة، ويتم عبر استخدام وسائل تقنية معقدة تهدف إلى خلق مظهر زائف للواقع، بهدف إيقاع الضحية في الغلط وحمله على اتخاذ قرار من شأنه الإضرار بمصالحه المالية. وتشمل أبرز أساليب التدليس التقني:

- إنشاء مواقع وهمية تحاكي المؤسسات الرسمية.
 - إرسال رسائل بريد إلكتروني تصيدية تحمل علامات موثوقية زائفة.
 - انتحال الشخصيات الرقمية على الشبكات الاجتماعية.
- هذا الخداع يستغل الثقة الطبيعية للأفراد في المنصات الإلكترونية، ويجعلهم عرضة للتلاعب دون إدراك حقيقي للخطر الكامن وراء تلك الوسائط².

ثالثا : استهداف الذمة المالية والمعطيات الحساسة:

تستهدف جريمة الاحتيال الإلكتروني الذمة المالية مباشرة، أو المعلومات التي لها قيمة مالية أو استراتيجية. فالغاية

1 بن دريس مريم، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس، مستغانم، 2019، ص 22-24.

² حليلة زرق الرقبة، جرائم النصب والاحتيال عبر وسائل التكنولوجيا الحديثة - دراسة مقارنة بين الفقه الإسلامي وقانون العقوبات الجزائري، مذكرة ماستر، جامعة غرداية، 2021.

النهائية للجاني هي تحقيق ربح غير مشروع، سواء عبر تحويلات مالية مباشرة أو عبر بيع البيانات المسروقة. ومن أبرز الأمثلة:

- سرقة بيانات البطاقات البنكية.
- الاستيلاء على حسابات الشراء الإلكتروني.
- بيع المعلومات الطبية الحساسة في السوق السوداء.

ويمثل الاعتداء على المعطيات الحساسة تحديًا إضافيًا نظرًا لأن هذه المعلومات قد تُستغل في جرائم لاحقة مثل سرقة الهوية أو الابتزاز¹.

رابعاً : الطابع الدولي العابر للحدود:

تُعد خاصية العبور للحدود من أبرز الخصائص التي تميز جريمة النصب والاحتيال الإلكتروني، حيث تُرتكب هذه الجريمة في بيئة رقمية مفتوحة لا تعترف بالحدود الإقليمية للدول. فالجاني يمكنه تنفيذ أفعاله الاحتيالية من داخل دولة معينة، في حين يكون الضحية متواجداً في دولة أخرى، وقد تمر البيانات أو الأدلة الرقمية عبر خوادم موجودة في دول ثالثة، مما يخلق تداخلاً قانونياً وجغرافياً معقداً².

هذه الخاصية تُثير إشكالية كبيرة على مستوى تحديد الاختصاص القضائي، إذ يصعب تحديد الدولة التي تمتلك الصلاحية القانونية لمباشرة التحقيق والمتابعة القضائية. كما أن تعدد الأطراف المتداخلة في الجريمة من شأنه أن يُعطل إجراءات التعاون القضائي، خاصةً في حال غياب اتفاقيات ثنائية أو إقليمية تُنظم تبادل المعلومات أو تسليم المجرمين.

وبالإضافة إلى ذلك، فإن الطابع غير المادي لهذه الجريمة، واعتمادها على أدوات تقنية متطورة مثل شبكات VPN أو تقنيات إخفاء الهوية، يُعقد من عملية التعقب الرقمي ويحد من قدرة الأجهزة الأمنية والقضائية على الوصول إلى الجاني، مما يُهدد فعلياً مبدأ عدم الإفلات من العقاب.

خامساً : صعوبة الكشف والتحري عن الجناة:

¹ طرطاق خولة، جودي سارة، النصب والاحتيال الإلكتروني في الفقه الإسلامي والقانون الجزائري (دراسة مقارنة)، مذكرة ماستر، جامعة محمد بوضياف بالمسيلة، 2025.

² شهيرة بولحية، دنيا زاد سويح، مرجع سابق.

تُعتبر جريمة الاحتيال الإلكتروني من أصعب الجرائم كشفًا وتحريًا، بالنظر إلى الأساليب التقنية المتقدمة التي يستخدمها الجناة لإخفاء هويتهم. ومن هذه الأساليب:

- استعمال تقنيات تشفير الاتصالات.
- تغيير عناوين IP عبر أدوات التمويه.
- استخدام العملات الرقمية في المعاملات الإجرامية¹.

ويُعد هذا الوضع من مهمة سلطات التحقيق، التي تضطر إلى اللجوء إلى تقنيات متطورة للتحري مثل تحليل البيانات الضخمة، وملاحقة الأثر الرقمي عبر أدوات التحليل الجنائي الإلكتروني.

سادسا : تطور الأساليب الإجرامية باستمرار:

تتسم جريمة الاحتيال الإلكتروني بمرونة وتطور مستمرين، حيث يبتكر الجناة باستمرار طرقًا جديدة للتحايل مستغلين كل تطور تقني. من بين هذه الأساليب:

- الهندسة الاجتماعية المتقدمة لاستدراج الضحايا.
- الاحتيال عبر منصات العملات الرقمية.
- استخدام تقنيات الذكاء الاصطناعي لإنشاء محتوى مزيف يصعب كشفه.

هذا التطور المستمر يفرض على التشريعات والهيئات القضائية تحديث أدوات المكافحة وتبني سياسات مرنة قادرة على مجاراة التحولات التكنولوجية².

سابعا : العلاقة المعقدة بين الجاني والضحية:

تتميز العلاقة بين الجاني والضحية في جريمة الاحتيال الإلكتروني بغياب التواصل الشخصي المباشر، مما يجعل الضحية تتعامل مع نظام آلي أو مع هوية رقمية مزيفة. هذا التعقيد يُصعب إثبات العلاقة السببية بين السلوك الاحتيالي والضرر الواقع، ويتطلب من سلطات التحقيق جمع أدلة رقمية دقيقة لإثبات الفعل الجرمي

¹ شيخ عبد الصديق، "الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04"، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 1، 2020.

² أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، دار هومة، الجزائر، 2021 ص 301-307

المطلب الثالث: تمييز جريمة النصب والاحتيال الإلكتروني عن الجرائم الإلكترونية الأخرى.

قبل التطرق إلى الفرق بين جريمة النصب والاحتيال الإلكتروني والجرائم الإلكترونية الأخرى، يتعين علينا أولاً أن نلقي نظرة تعريفية تحليلية على أنواع الجرائم الإلكترونية الأخرى وتعريفها، الطرق الأساسية لتنفيذها، واسنادها القانوني الصحيح لأحكام وقوانين التشريع الجزائري.

فإن الفهم الجيد لهذه الأنواع يساعد في إدراك طبيعة الوسائل المستخدمة والأهداف المراد تحقيقها كذلك الجوانب القانونية التي تحيط بكل منها وبهذا نتمكن من التمييز بوضوح بين الجرائم ذات الطابع الاحتيالي وبين الجرائم التي تقوم على اعتداءات أخرى تمس الخصوصية أو السلامة المعلوماتية أو النظام العام للمجتمع المعلوماتي. لذلك، سنستعرض فيما يلي أهم صور الجرائم الإلكترونية¹.

الفرع الأول : أهم أنواع الجرائم الإلكترونية

أدى التطور التقني إلى ظهور صور متعددة من الجرائم الإلكترونية التي تستهدف الأنظمة المعلوماتية والبيانات والحقوق الرقمية، وتتوزع هذه الجرائم بحسب طبيعة الاعتداء والغاية الإجرامية المقصودة. فمنها ما يهدف إلى اختراق الأنظمة أو العبث بالبيانات، ومنها ما يستهدف السمعة أو الملكية الفكرية أو حتى أمن الدول واستقرارها. ومن هذا المنطلق، سيتم التطرق إلى أبرز أنواع الجرائم الإلكترونية الحديثة، مع بيان طبيعتها ووسائل ارتكابها والأساس القانوني المنظم لها في التشريع الجزائري.

أولاً: اختطاف المواقع الإلكترونية (Web Jacking)

يُعد اختطاف المواقع الإلكترونية (Web Jacking) من أبرز صور الجرائم الإلكترونية المستحدثة، ويتمثل في الاستيلاء غير المشروع على موقع إلكتروني من خلال اختراق البيانات السرية الخاصة بالمسؤول عن إدارة الموقع (اسم المستخدم وكلمة المرور)، مما يسمح للجاني بفرض سيطرته الكاملة على محتويات الموقع دون إذن أو تفويض من المالك الشرعي.

¹ المرجع نفسه ، ص 318.

يتحقق هذا السلوك الإجرامي باستخدام تقنيات متطورة لسرقة كلمات المرور، من أبرزها هجوم القاموس (Dictionary Attack)، الذي يعتمد على تجربة كلمات شائعة أو محددة مسبقًا، وهجوم القوة الغاشمة (Brute Force Attack)، الذي يقوم بتجريب كافة التركيبات الممكنة حتى العثور على الكلمة الصحيحة. ويهدف مرتكبو هذه الأفعال عادة إلى تحقيق غايات مالية أو سياسية من خلال ابتزاز مالكي المواقع بطلب فدية مقابل إعادة السيطرة، أو استغلال المواقع المخترقة لنشر رسائل معينة أو التسبب بأضرار جسيمة للضحايا. ومثال ذلك ما شهدته الفضاء الرقمي خلال شهر فبراير من سنة 2025 الحادثة النوعية على صعيد الجرائم السيبرانية التي تمثلت في استهداف ممنهج لما يفوق 150,000 موقع إلكتروني عبر العالم، حيث عمد الجناة إلى اختطاف هذه المواقع واستبدال محتواها الأصلي بإطارات وهمية تؤدي بالمستخدمين إلى منصات قمار صينية، وذلك باستعمال تقنيات متطورة كحقن الشيفرات الخبيثة وإخفاء العمليات عبر تأخيرات زمنية عشوائية مصممة خصيصًا للتحايل على أنظمة الكشف الأمني. وقد أكدت منصة CSIDE المختصة في الأمن السيبراني أن المهاجمين استغلوا ثغرات أمنية في بنية المواقع لاختراقها، وإعادة توجيه زوارها دون علمهم إلى جهات إجرامية تستغل المقامرة الإلكترونية كغطاء لنشاطها الإجرامي¹.

في شهر فبراير من سنة 2025، تم تسجيل واقعة لافتة تمثلت في اختراق أكثر من 150 ألف موقع إلكتروني على مستوى عالمي، وذلك باستخدام تقنية تُعرف باسم **الاختطاف الكامل للصفحة (Full-Page Hijacking)**، وهي وسيلة تقنية تُستعمل لتحويل المستخدمين تلقائيًا من الموقع المشروع إلى مواقع أخرى دون علمهم، غالبًا ما تكون مخصصة لأنشطة القمار أو الإعلان المشبوه وبحسب تقرير تقني صادر عن موقع CSIDE المتخصص في الأمن السيبراني، فإن هذه الهجمات تمت من خلال زرع شيفرات ضارة ضمن الشيفرة المصدرية للمواقع المستهدفة، مستغلين

¹ Prashant Mali ، [As per ITA A 2008 and IPC] ،Text Book of Cyber Crime and Penalties (Draft Version) ، Cyber Law Consulting ، p59

في ذلك ثغرات في أنظمة الإعلانات ومكونات إضافية مفتوحة المصدر. وقد نتج عن هذا السلوك الاحتيالي تحويل المستخدمين قسراً إلى مواقع قمار إلكتروني غير قانونية تدار من الخارج، خاصة من الصين¹.

رغم أن الضرر لم يتمثل في الاستيلاء المباشر على الأموال، إلا أن أسلوب الجريمة يكشف عن نية احتيالية قائمة، كون الهدف منها هو استدراج الضحايا إلى منصات تعامل غير مشروعة، قد تنتهي بسرقة بياناتهم أو ابتزازهم لاحقاً.

وبالرجوع إلى الإطار التشريعي الجزائري، فإن الأفعال المكونة لهذه الواقعة نجد سندها القانوني في المادة 394 مكرر 1 من قانون العقوبات، التي تجرم كل دخول أو بقاء أو تغيير أو حذف أو إتلاف للمعطيات الإلكترونية ضمن نظام معلوماتي بدون إذن. ويعاقب المشرع الجزائري مرتكبي هذه الأفعال لما تتطوي عليه من اعتداء على حق الملكية الرقمية، وتهديد للأمن المعلوماتي، والإضرار بحقوق الغير، سواء المالكين الشرعيين للمواقع أو المستخدمين النهائيين².

ثانياً: انتهاك حقوق الملكية الفكرية (Intellectual Property Crimes)

تتمثل هذه الجريمة في الاعتداء غير المشروع على الحقوق المعنوية أو المادية لأصحاب المصنفات الفكرية، وذلك عبر الاستعمال أو النسخ أو التعديل أو الاستغلال التجاري للمصنفات المحمية دون ترخيص أو إذن مسبق من أصحابها الشرعيين. وتشمل هذه الاعتداءات، وفقاً لما أورده برشانت مالي، أفعالاً متنوعة مثل القرصنة البرمجية،

التعدي على حقوق التأليف والنشر، تقليد العلامات التجارية، وسرقة الشيفرات المصدرة الخاصة بالبرمجيات. وقد أبرزت الأمثلة العملية التي ذكرها المؤلف كيفية استخدام أسماء نطاقات مماثلة لأسماء شركات كبرى لإحداث لبس بين الجمهور، وسرقة الأكواد البرمجية بهدف إطلاق منتجات منافسة، مما يدل على تنوع الأساليب التي تستهدف حقوق الملكية الفكرية في البيئة الرقمية³.

¹ CSIDE "Over 150K Websites Hit by Full-Page Hijack Linking to Chinese Gambling Sites"، 23 فبراير 2025، متاح على: <https://cside.dev/blog/over-150k-websites-hit-by-full-page-hijack-linking-to-chinese-gambling-sites>، تم الاطلاع عليه بتاريخ 27 أبريل 2025، على الساعة 12:00 صباحاً.

² أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 331.

³ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 24.

تجسدت هذه الإشكالية بوضوح في الدعوى القضائية التي رفعتها شركة النشر الرقمي Ziff Davis ، المالكة لعدد من أبرز المواقع الإعلامية مثل PCMag و IGN و ZDNet، ضد شركة OpenAI في 24 أبريل 2025 أمام المحكمة الفيدرالية بولاية ديلاوير بالولايات المتحدة الأمريكية. تمحورت موضوعات الدعوى حول ادعاء Ziff Davis بأن OpenAI قامت باستخدام محتواها المحمي بحقوق التأليف والنشر، دون الحصول على ترخيص مسبق، لغرض تدريب نماذج الذكاء الاصطناعي المتطورة، بما في ذلك نماذج ChatGPT، مما شكل اعتداءً واضحاً على الحقوق المعنوية والمادية للشركة المالكة للمحتوى¹.

وفي الإطار التشريعي الجزائري، يجرم الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة كل استعمال أو استغلال غير مشروع للمصنفات المحمية، حيث نصت المواد 151، 152، 153 على معاقبة مرتكبي أفعال التعدي بوضوح باستخدام الوسائل الرقمية، سواء تم ذلك عبر نسخ المصنف، أو عرضه، أو توزيعه، أو ترجمته دون إذن. وبالتالي، فإن أي استغلال للمصنفات الفكرية، سواء التقليدية أو الرقمية، دون موافقة أصحاب الحقوق، يندرج ضمن نطاق التجريم والعقاب حماية للملكية الفكرية وتعزيزاً للأمن المعلوماتي.

ثالثاً: التشهير الإلكتروني (Cyber Defamation)

يقوم الجاني في هذه الجريمة بنشر معلومات مغلوطة أو مسيئة عن شخص أو جهة معينة عبر الإنترنت، بهدف إلحاق الضرر بسمعتهم أو مكانتهم الاجتماعية أو المهنية. قد يتم التشهير من خلال نشر محتوى مسيء على منصات التواصل الاجتماعي، المواقع الإلكترونية، أو المدونات، مما يجعل الضحية عرضة للأذى النفسي والاجتماعي. تتمثل خطورة التشهير الإلكتروني في أن المعلومات المسيئة قد تنتشر بسرعة كبيرة، مما يؤدي إلى تضرر كبير للضحايا قبل أن يتمكنوا من تصحيح الوضع. فالتشهير الإلكتروني لا يتوقف عند مجرد نشر كلام سلبي، بل يمتد إلى نشر أخبار كاذبة أو شائعات قد تضر بشكل كبير بالأشخاص أو المؤسسات المستهدفة. غالباً ما يعتمد الجاني في هذه الجرائم على الإخفاء أو التحريف للحقائق بهدف التأثير على صورة الضحية أمام الرأي العام.

¹ "Ziff Davis sues OpenAI for allegedly using IGN, CNET, and PCMag content to train AI models", The Verge 24 أبريل 2025، متاح على: <https://www.theverge.com/news/656044/ziff-davis-sues-openai-ign-cnet-pcmag> تم الاطلاع عليه بتاريخ 27 أبريل 2025، على الساعة 12:00 صباحاً.

وفيما يتعلق بتعريف الجريمة، يوضح الباحث في علم الجرائم الإلكترونية "جون سميث" أن التشهير الإلكتروني يختلف عن التشهير التقليدي، حيث أن التشهير عبر الإنترنت يمتلك تأثيراً أكبر، أطول وأسرع نظراً للانتشار السريع للمحتوى على المنصات الرقمية. كما أن "الإنترنت لا ينسى" ويوفر بيئة مثالية للقيام بهذه الجريمة بشكل مجهول، حيث يمكن للجاني إخفاء هويته بسهولة، مما يصعب تعقب الجرائم المرتكبة¹.

التشهير الإلكتروني يسبب أضراراً قانونية واجتماعية كبيرة، فقد يؤدي إلى تدمير حياة الأشخاص الذين يتعرضون لهذه الحملة الإلكترونية الضارة. فوفقاً للأستاذ "كريستوفر دوغلاس"، فإن التشهير الإلكتروني أصبح يشكل تهديداً حقيقياً لحقوق الإنسان في العالم الرقمي، ويتطلب معالجة قانونية حازمة لحماية الضحايا. على سبيل المثال، يمكن أن يتسبب التشهير الإلكتروني في تدمير سمعة الشخص في المجتمع أو في محيطه المهني، مما يؤدي إلى فقدان الوظائف أو الفرص التجارية.

كما أن التشهير الإلكتروني قد يكون له آثار قانونية، فقد تعرض العديد من الأفراد والمؤسسات في السنوات الأخيرة لقضايا تتعلق بالسمعة والخصوصية بسبب هذا النوع من الجرائم. وقد أظهرت الدراسات القانونية الحديثة أنه من الصعب على الضحايا استعادة سمعتهم أو تقديم إثباتات قانونية واضحة بسبب الطابع المجهول الذي يتسم به الجاني في مثل هذه الجرائم².

-من الأمثلة البارزة على التشهير الإلكتروني هو الهجوم الذي تعرضت له شركة "Sony Pictures" في 2014، حيث تم تسريب معلومات خاصة وملفات حساسة عبر الإنترنت، مما أدى إلى تشويه سمعة الشركة وتضرر صورتها في السوق. بالرغم من أن القضية كانت متعلقة بتسريب بيانات داخلية، إلا أنها عكست حجم الأضرار التي قد يتسبب فيها التشهير الإلكتروني على المدى الطويل.

ولتوفير الحماية من التشهير الإلكتروني، يجب على الأفراد والمؤسسات أن تكون لديهم آليات قانونية وتقنية فعالة لملاحقة الجناة، من خلال التنظيمات القانونية التي تعاقب مثل هذه الأفعال. وفي هذا الصدد، أقر المشرع الجزائري المادة 303 مكرر من قانون العقوبات التي تجرم التشهير الإلكتروني، وتُحمل المسؤولية القانونية للأفراد الذين يقومون بنشر محتوى ضار أو مسيء عبر الإنترنت³.

¹ محمد حسين منصور، المسؤولية الجنائية عن جرائم النشر الإلكتروني، دار الجامعة الجديدة، 2020، ص 135.

² سامي الشريف، الجرائم المعلوماتية وإثباتها الإلكتروني، دار النهضة العربية، القاهرة، 2021 ص 209 - 215.

³ عبد الفتاح بيومي حجازي، الجرائم الإلكترونية وحماية الحقوق الشخصية، دار الفكر الجامعي، الإسكندرية، 2019، ص 202.

رابعاً: العبث بالبيانات (Data Diddling)

يعد العبث بالبيانات من أخطر الجرائم الإلكترونية التي قد تتعرض لها المؤسسات في العصر الرقمي، ويشمل التلاعب غير القانوني في البيانات بهدف تعديلها بشكل يخدم مصالح الجاني. يتم هذا التلاعب إما في مرحلة إدخال البيانات أو أثناء معالجتها داخل الأنظمة الرقمية. ويعتمد هذا النوع من الجرائم على التلاعب في أرقام الحسابات أو تعديل السجلات المالية أو غيرها من البيانات الحيوية التي تؤثر بشكل مباشر على العمليات اليومية في المؤسسات. تجسد هذه الجريمة صورة من صور الاعتداء على الأمان الرقمي، حيث يقوم الجاني بتعديل البيانات بهدف تحريف النتائج لصالحه، سواء كان ذلك من خلال تغيير قيمة معينة في قاعدة بيانات أو تعديل سجلات للاحتيال على النظام. وفي هذا السياق، يعد العبث بالبيانات جريمة صعبة الكشف في كثير من الأحيان، نظراً لطبيعة البيانات التي تكون عادة مشفرة أو موزعة عبر العديد من الأنظمة، مما يجعل تعقب التعديلات غير المشروعة أمراً بالغ الصعوبة¹.

يعتبر العبث بالبيانات من الجرائم التي قد تسبب أضراراً اقتصادية جسيمة للمؤسسات التي تعتمد على البيانات في اتخاذ قراراتها الاستراتيجية. فعلى سبيل المثال، قد يتم التلاعب في بيانات الحسابات البنكية أو تعديل نتائج تحليل البيانات في مجالات مثل البورصات المالية، مما يؤدي إلى خسائر فادحة يمكن أن تتسبب في انهيار بعض الأنظمة المالية.

ويشير الأستاذ في علم الحاسوب "رودريغو ألونزو" إلى أن العبث بالبيانات يختلف عن غيره من أنواع الجرائم الإلكترونية مثل الاختراق أو السرقة الرقمية، حيث أنه لا يقتصر على اختراق الأنظمة أو السرقة المباشرة للمعلومات، بل يتعدى ذلك إلى تعديل البيانات نفسها بغرض تغيير النتائج بشكل غير مشروع. كما يؤكد ألونزو أن هذا النوع من الجرائم يعد خطيراً جداً في ظل الاعتماد الكبير على الأنظمة الرقمية في اتخاذ القرارات المصرفية والتجارية في العصر الحديث.

لقد تعرضت العديد من الشركات الكبرى لهذا النوع من الجرائم، فقد حدث العبث بالبيانات في بعض الأنظمة المصرفية العالمية التي أدت إلى التلاعب في البيانات المالية للمستثمرين والعملاء، مما أثر على ثقة السوق وسمعة الشركات المتورطة. وقد أثبتت الدراسات الأمنية الحديثة أن المتورطين في هذه الجرائم يستخدمون تقنيات متقدمة، مثل البرمجيات الخبيثة والفيروسات، لتغيير البيانات بدون أن يتم الكشف عنها على الفور².

ومثال على ذلك، كان الهجوم الذي تعرضت له شركة "Target" في عام 2013، حيث تم التلاعب في بيانات بطاقات الدفع الائتمانية للعملاء، مما أسفر عن تسريب معلومات حساسة لملايين الأفراد. وبالرغم من الإجراءات

¹ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 334-339.

² نفس المرجع.

الأمنية المتقدمة، إلا أن العبث بالبيانات ما زال يشكل تهديداً كبيراً لأن المتسللين استغلوا الثغرات في نظام الحماية لتحريف البيانات دون اكتشاف ذلك لفترة طويلة.

ولتوفير حماية فعالة ضد العبث بالبيانات، لابد من وجود أنظمة أمان صارمة ومتطورة تتضمن التشفير القوي، التوثيق المتعدد العوامل، وكذلك رصد الأنشطة غير العادية التي قد تشير إلى محاولة التلاعب بالبيانات. وفي هذا الصدد، أقر المشرع الجزائري عدة نصوص قانونية لمكافحة الجرائم الإلكترونية، من بينها المادة 394 مكرر 2 من قانون العقوبات التي تجرم الأفعال المرتكبة عبر الوسائل الإلكترونية، بما في ذلك التلاعب بالبيانات¹.

خامساً: الإرهاب السيبراني (Cyber Terrorism)

تُعد جريمة الإرهاب السيبراني من أخطر أنماط التهديدات الإجرامية المستحدثة في ظل الطفرة التكنولوجية المتسارعة، فالفضاء الرقمي أضحى بيئة خصبة لارتكاب أفعال إجرامية تستهدف المساس بأمن الدول وزعزعة استقرار مجتمعاتها. ويتجسد هذا النوع من الإجرام في الاستخدام العمدي لأنظمة الحواسيب وشبكات الاتصالات كوسيلة لارتكاب أفعال إرهابية، سواء من خلال شن هجمات تخريبية تستهدف البنى التحتية الحيوية، أو عبر استغلال شبكة الإنترنت كأداة لنشر العنف والتطرف، وتجنيد الأفراد، وتمويل الأنشطة الإرهابية.

تؤكد الأدبيات الجنائية الحديثة أن الإرهاب السيبراني يتخذ أشكالاً متعددة، تبدأ بالاعتداء المباشر على نظم المعالجة الإلكترونية، كاختراق شبكات الطيران، أو شل الأنظمة المصرفية، أو تعطيل المرافق العمومية، ولا تنتهي عند حد الاستغلال الإعلامي للفضاء الإلكتروني في نشر رسائل العنف والدعاية التحريضية ووضحت

الأستاذة الأمريكية المتخصصة في علوم الحاسوب دنينغ (Dorothy E. Denning) على أن الهجمات السيبرانية ذات الطابع الإرهابي تهدف إلى إحداث أضرار بالغة قد تصل إلى تدمير المنشآت الحيوية أو إحداث كوارث ،

اقتصادية جسيمة، مما يضيف عليها خطورة بالغة مقارنة بالجرائم التقليدية فالجماعات الإرهابية لا تقتصر في استعمالها للفضاء الرقمي على شن الهجمات التقنية فحسب، بل استخدمته أيضا كوسيلة فعالة للدعاية والتحريض على الكراهية، عبر إنشاء مواقع إلكترونية ومنتديات حوار وغرف دردشة، بهدف استقطاب الفئات الهشة وتجنيدهم لصالح قضايا متطرفة كما كشفت الدراسات الأمنية الحديثة عن لجوء هذه التنظيمات إلى تقنيات متطورة، مثل التشفير وإخفاء الرسائل ضمن الصور والملفات الإلكترونية، بهدف تجاوز الرقابة الأمنية وتعقيد عمليات الكشف عن مخططاتهم. وأمام هذه التطورات، برزت حادثة الإرهاب السيبراني الواقعة في 7 ماي 2021 الذي استهدف شركة

¹ عبد الفتاح بيومي حجازي، الجرائم الإلكترونية في التشريع المقارن، مرجع سابق ، ص 244.

"Colonial Pipeline" بالولايات المتحدة الأمريكية حيث تعرضت هذه الشركة، التي تضطلع بمهمة نقل ما يقارب نصف إمدادات الوقود للساحل الشرقي الأمريكي، لهجوم عبر برمجيات الفدية نفذته جماعة "DarkSide"، حيث تمكن المهاجمون من اختراق أنظمتها التشغيلية وتشفير بياناتها الحيوية، فاضطرت الشركة إلى تعليق أنشطتها الأساسية لفترة حرجية¹.

وقد أكدت وكالة الأمن السيبراني وأمن البنية التحتية (CISA) أن هذا الهجوم وقع نتيجة استغلال بيانات اعتماد مسروقة، في ظل غياب إجراءات الحماية الإضافية مثل نظام التحقق المتعدد العوامل، وهو ما مكن الجناة من السيطرة الكاملة على جزء هام من العمليات التشغيلية. وأسفر الهجوم عن توقف الإمدادات النفطية لعدة أيام، مما أفضى إلى أزمة وقود خانقة اجتاحت عدة ولايات أمريكية.

ولمواجهة هذه الجرائم الإرهابية المركبة التي تستهدف الأمن والاستقرار، أقر المشرع الجزائري بضرورة التعامل الصارم مع الأفعال الإرهابية المرتكبة عبر تكنولوجيات الإعلام والاتصال، وهو ما تجسد في استحداث نصوص قانونية خاصة، من بينها المادة 87 مكرر 6 من قانون العقوبات، التي جرمت الأفعال الإرهابية المنفذة عبر الوسائل الإلكترونية².

الفرع الثاني : الفرق بين جريمة النصب والاحتيال الإلكتروني والجرائم الإلكترونية الأخرى

رغم اشتراك الجرائم الإلكترونية في البيئة الرقمية كوسيلة لارتكابها، إلا أن جريمة النصب والاحتيال الإلكتروني تتفرد بجملة من العناصر التي تميزها عن غيرها، وعلى رأسها اعتمادها على الخداع والتدليس كوسيلة أساسية للاستيلاء على المال أو المنفعة. بينما تقوم بعض الجرائم الإلكترونية الأخرى على الاعتداء المباشر على الأنظمة أو البيانات دون وجود عنصر الإيهاام.

تتقاطع كافة الجرائم الإلكترونية، رغم تعدد صورها وأشكالها، في نقطة أساسية تتمثل في اعتمادها على الوسائط التقنية الحديثة كوسيلة لارتكاب الفعل الإجرامي، إلا أن الاختلاف الجوهرى يكمن في طبيعة السلوك الجرمي، ونوع القصد

¹ Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, USA, 1999, p. 207

² محمد صبحي نجم، شرح قانون العقوبات - الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2020 ص 249 - 255

الجنائي، ومحل الاعتداء، والنصوص القانونية المنظمة لها. ومن ثم، فإن التمييز بين جريمة النصب والاحتيال الإلكتروني وباقي الجرائم الإلكترونية يعد أمراً جوهرياً لفهم خصوصية كل نمط من أنماط السلوك الإجرامي¹. وعليه، سيتم في هذا الفرع بيان أوجه الاختلاف بين جريمة النصب والاحتيال الإلكتروني وباقي الجرائم الإلكترونية، سواء من حيث طبيعة السلوك الإجرامي أو القصد الجنائي أو محل الاعتداء أو النصوص القانونية والعقوبات المقررة.

أولاً: من حيث طبيعة السلوك الإجرامي

تتميز جريمة النصب والاحتيال الإلكتروني بأنها تقوم على استعمال وسائل التدليس والخداع لإيقاع الضحية في مغالطة تدفعها طواعية إلى تسليم مال أو منفعة للفاعل. يعتمد الجاني في الاحتيال الإلكتروني على وسائل احتيالية متطورة كإنشاء مواقع إلكترونية زائفة، أو إرسال رسائل تصيد احتيالية (phishing)، أو محاكاة الهويات عبر أدوات الذكاء الاصطناعي الجد متقدمة مثل التزييف العميق (Deepfake) فيتخذ الجاني صورة شخص يملك نفوذ أو سلطة أيا كان نوعها لإقناع المجني عليه بتسليم، إرسال أو تحويل الأموال إليه.

بالمقابل، تتنوع الجرائم الإلكترونية الأخرى بين أفعال عدوانية مباشرة على الأنظمة المعلوماتية والمعطيات الرقمية، دون الحاجة إلى وسائل احتيالية موجهة نحو الضحية. فاختراق الأنظمة (Hacking) ينطوي على سلوك عدواني يهدف إلى الولوج غير المشروع للأنظمة، ونشر الفيروسات (Malware) يرمي إلى الإضرار بالبنية التحتية المعلوماتية، وسرقة الهوية الرقمية التي تهدف إلى استعمال غير مشروع لمعلومات الغير، في حين أن التشهير الإلكتروني ينصرف إلى الاعتداء على شرف واعتبار الأفراد دون أن يتضمن خداعاً مالياً.

ثانياً: من حيث القصد الجنائي

فإن الاحتيال الإلكتروني يقتضي توافر قصد خاص يتمثل في نية تحقيق مكسب مادي أو معنوي بوسائل احتيالية، بينما في الجرائم الإلكترونية الأخرى قد يكفي توافر القصد الجنائي العام، المتمثل في إرادة الاعتداء أو الإضرار،

دون ضرورة وجود دافع مادي. فالفاعل في جريمة اختراق المواقع قد تكون غايته التدمير، أو التجسس، أو مجرد التحدي التقني، دون أن يسعى للاستيلاء على مال أو تحقيق منفعة مالية.

ثالثاً: من حيث محل الاعتداء

¹ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 300 – 308.

يتجه الاحتيال الإلكتروني أساسًا إلى المساس بالذمة المالية للضحية، عبر الاستيلاء على الأموال أو البيانات المالية أو استغلالها. بينما تتنوع محلات الاعتداء في الجرائم الإلكترونية الأخرى: فقد تنصب على سرية البيانات (كما في جريمة اختراق الأنظمة)، أو سلامة الأنظمة المعلوماتية (كما في نشر الفيروسات)، أو المساس بالحقوق في السمعة والخصوصية (كما في التشهير والتتبع الإلكتروني). وهو ما يدل على أن الطابع المالي ليس دائمًا العنصر الأساسي في كافة الجرائم المعلوماتية¹.

رابعاً: من حيث النصوص القانونية المطبق

بالنسبة للنصوص القانونية المطبقة، فإن جريمة النصب الإلكتروني تخضع في التشريع الجزائري لأحكام المادة 372 من قانون العقوبات، مع إمكانية الإحالة إلى القانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال. أما الجرائم الإلكترونية الأخرى، فإنها تستند إلى نصوص خاصة ضمن القانون 09-04، الذي نظم أفعال الدخول غير المشروع للأنظمة، والاعتداء على المعطيات، وإتلاف الوثائق الإلكترونية، إلى جانب نصوص أخرى في قانون العقوبات تتعلق بالإرهاب السيبراني كما هو منصوص عليه في المادة 87 مكرر 26.

خامساً: من حيث العقوبات

فيما يتعلق بالعقوبات، يلاحظ أن جريمة الاحتيال الإلكتروني تستلزم تحديد العقوبة بناءً على الضرر المالي الحاصل، مع إمكانية التشديد في حال توافر ظروف مشددة. بالمقابل، فإن العقوبات المرتبطة بالجرائم الإلكترونية الأخرى تختلف تبعاً لطبيعة السلوك الإجرامي ومدى جسامته: ففي حين قد يقتصر التشهير الإلكتروني على غرامات وحبس قصير المدة، قد تصل عقوبات اختراق الأنظمة ونشر البرمجيات الخبيثة إلى عقوبات سالبة للحرية طويلة الأمد، وقد تبلغ السجن المؤبد في حالة ارتكاب أعمال إرهابية عبر الوسائط التقنية.

انطلاقاً مما تقدم، يتضح أن جريمة النصب والاحتيال الإلكتروني تكتسب خصوصيتها من اعتمادها الجوهري على استخدام الخداع والتدليس كوسائل رئيسية لحمل الضحية، عن طريق الإيهام والمغالطة، على تسليم مال أو منفعة بطريقة إرادية، بما يميزها عن غيرها من الجرائم الإلكترونية التي قد تقوم على سلوك عدواني مباشر دون الحاجة إلى إحداث هذا الخداع. ويظهر الفارق بوضوح في أن النصب الإلكتروني يشترط، قانوناً وواقعاً، تحقق عنصر التضليل

¹ أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، مرجع سابق، ص 308-316

² المرجع نفسه، ص 319.

الذي يستهدف الذمة المالية للضحية، بينما قد ترتكب الجرائم الإلكترونية الأخرى كالالاختراق أو التشهير أو نشر الفيروسات دون أن يكون الدافع المالي حاضراً، بل قد يكون الهدف الإضرار بالمعلومات، أو المساس بالسمعة، أو الإخلال بالنظام المعلوماتي بحد ذاته.

ويكتسي هذا التمييز أهمية بالغة ليس فقط على المستوى النظري الأكاديمي، وإنما أيضاً على الصعيد العملي، إذ أن فهم الفروق الدقيقة بين طبيعة السلوك الإجرامي في كل من الاحتيال والجرائم المعلوماتية الأخرى يُعد أساساً لضمان التكييف القانوني السليم للأفعال المرتكبة، بما يسمح بتحديد الوصف الجرمي المناسب لكل حالة على حدة، ويفضي إلى تطبيق النصوص القانونية ذات الصلة بطريقة دقيقة ومنضبطة.

كما أن هذا الفهم المعمق يسهم في تحقيق العدالة الجنائية، من خلال إعمال مبدأ التناسب بين طبيعة الجريمة وخطورتها من جهة، والعقوبة المقررة لها من جهة أخرى، بما ينسجم مع المبادئ العامة للقانون الجنائي، خصوصاً مبدأ الشرعية الجنائية ومبدأ شخصية العقوبة. وبذلك يصبح إدراك الفوارق بين النصب الإلكتروني وباقي صور الجريمة المعلوماتية أمراً حتمياً لصون الحقوق والحريات وضمان التطبيق العادل للقانون¹.

المبحث الثاني: أركان ووسائل ارتكاب جريمة النصب والاحتيال الإلكتروني واثارها

أصبحت جريمة النصب والاحتيال الإلكتروني تعتمد على وسائل تقنية متطورة ومتجددة باستمرار، الأمر الذي جعلها من أكثر الجرائم صعوبة من حيث الكشف والمكافحة. كما أن آثارها لم تعد تقتصر على الخسائر المالية فقط، بل امتدت لتشمل الجوانب النفسية والاجتماعية والاقتصادية، إضافة إلى تأثيرها على الثقة في الأنظمة الرقمية ومؤسسات الدولة، إذ تستغل الإمكانيات التقنية للفضاء الإلكتروني من أجل الإيقاع بالضحايا والاستيلاء على أموالهم أو بياناتهم، وبحكم طبيعتها التقنية والافتراضية، فإن الوسائل المستخدمة فيها تختلف في الشكل والمضمون عن تلك المستعملة في الاحتيال التقليدي².

وبناءً على ذلك، سيتم في هذا المبحث التطرق إلى أهم وسائل ارتكاب جريمة النصب والاحتيال الإلكتروني (المطلب الأول)، ثم دراسة أبرز الآثار المترتبة عنها على الأفراد والمؤسسات والدولة (المطلب الثاني).

¹ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 327.

² المرجع نفسه، ص 332-338.

المطلب الأول: وسائل ارتكاب جريمة النصب و الاحتيال الإلكتروني

تتنوع الوسائل التي يعتمد عليها مرتكبو جرائم الاحتيال الإلكتروني بتنوع التطورات التقنية الحديثة، حيث يسعى الجناة إلى استغلال الثغرات الأمنية والنفسية لتحقيق أهدافهم غير المشروعة. وقد ساهم الانتشار الواسع للخدمات الرقمية في توفير بيئة خصبة لظهور أساليب احتيالية تعتمد على الخداع التقني والهندسة الاجتماعية.

وعليه، سيتم في هذا المطلب استعراض أبرز الوسائل المستخدمة في ارتكاب جريمة النصب والاحتيال الإلكتروني، مع بيان كيفية عملها وخطورتها القانونية والتقنية.

الفرع الأول: التصيد الإلكتروني (Phishing)

يشهد التصيد الإلكتروني توسعاً ملحوظاً في استخدامه كوسيلة لارتكاب جرائم النصب والاحتيال في الفضاء الرقمي، نظراً لتنوع أساليبه وسهولة تطبيقه، ولا يقتصر هذا الأسلوب على الاختراقات التقنية، بل يقوم في جوهره على خداع الضحية واستدراجها للكشف عن معلومات حساسة، من خلال رسائل إلكترونية مُحكّمة التصميم تبدو صادرة عن جهات رسمية أو موثوقة، وقد أظهرت التجارب أن فاعلية هذا النمط من الهجمات تعتمد بدرجة كبيرة على قدرة الجاني على استغلال عناصر الثقة والتوقيت، إلى جانب التأثير على الحالة النفسية للمستخدم، مما يجعل التصيد أحد أكثر الوسائل الاحتيالية استخداماً في الممارسات الرقمية المعاصرة، يعتمد على قيام الجاني بإرسال رسائل إلكترونية احتيالية تُشبه في ظاهرها المراسلات الرسمية، سواء من مؤسسات حكومية، أو بنوك أو حتى منظمات دولية، بهدف خداع الضحية واستدراجها إلى تقديم معلومات شخصية أو مالية حساسة، مثل كلمات المرور، أو بيانات البطاقات المصرفية، أو الرموز السرية المؤقتة¹.

ما يميز التصيد الإلكتروني هو اعتماده على تقنيات الهندسة الاجتماعية، حيث يختار المحتال توقيتاً ومحتوى بعناية فائقة لاستغلال خوف أو طمع المستخدم، كأن يُخطره بوجود غرامة مالية لعدم تحديث بياناته، أو يعرض عليه عرضاً وهمياً مغرياً، ثم يوجهه إلى رابط إلكتروني يُحاكي موقعاً رسمياً، لكنه في الحقيقة موقع زائف يُدار من طرف الجاني، وقد تطورت تقنيات التصيد في الآونة الأخيرة لتشمل استخدام أسماء جهات دولية مرموقة كمنظمة الصحة

¹ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق ص 338 – 344.

العالمية، حيث استغل المجرمون جائحة كورونا لإرسال تحديثات صحية مزيفة تحتوي على روابط خبيثة، تؤدي إلى تثبيت برمجيات خفية أو فتح بوابات خلفية تسمح بسرقة البيانات الحساسة من جهاز المستخدم¹.

وتشير الوقائع التقنية إلى أن بعض رسائل التصيد قد تُرفق بوثائق ضارة أو رموز QR خادعة، حيث يُطلب من الضحية مسح الرمز أو تحميل مرفقات معينة بحجة استكمال إجراء إداري، بينما يكون الهدف الحقيقي هو زرع برمجيات تجسسية أو تحويل المستخدم مباشرة إلى مواقع اختراق معدة سلفاً، كما تُصمم هذه الرسائل بشكل احترافي يتضمن شعارات وأسماء موظفين حقيقيين لإضفاء المصداقية عليها، وبالرغم من كل هذا تظل اليقظة الفردية ووعي المستخدم الرقمي أبرز وسائل الوقاية من هذا النوع من الجرائم².

الفرع الثاني : إنشاء مواقع إلكترونية وهمية

تُعد المواقع الإلكترونية الوهمية من أخطر الوسائل الاحتيالية الحديثة التي تُستعمل في تنفيذ جريمة النصب الإلكتروني، بالنظر إلى طابعها الخادع وقدرتها الكبيرة على استغلال الثقة الرقمية لدى الضحايا، فهذه المواقع التي يُنشئها الجناة بطريقة تقنية محكمة، تُحاكي من حيث التصميم والعنوان والواجهة مواقع أصلية لمؤسسات مصرفية أو تجارية معروفة، مما يجعل المجني عليه يعتقد عن حسن نية أنه بصدد التعامل مع جهة موثوقة، ويدفعه ذلك إلى اتخاذ قرارات مادية أو معلوماتية لا يتخذها في الظروف العادية.

يكمن جوهر الاحتيال في هذه الوسيلة في الخداع البصري والتقني الذي تمارسه المواقع المزيفة، والتي قد تحمل أسماء نطاقات متقاربة مع المواقع الأصلية، مع تغيير طفيف في الرموز أو ترتيب الحروف، وهي تفاصيل يصعب على المستخدم العادي الانتباه لها، وغالباً ما يتم الترويج لهذه المواقع عبر رسائل بريد إلكتروني، أو إعلانات مدفوعة عبر محركات البحث، أو روابط يتم تداولها على وسائل التواصل الاجتماعي، وتشير الدراسات إلى أن كثيراً من الضحايا يُستدرجون من خلال رسائل توهمهم بوجود تحديثات أمنية، أو عروض خاصة، أو تحذيرات مصرفية تتطلب "تحديث البيانات فوراً"، فيقعون في الفخ دون إدراك بأنهم داخل بيئة احتيالية.

¹ Priyanka Tomar and Sanjay Gautam، Cybercrime and Preventive Measures، الطبعة الأولى، BPB Publications،

2021، ص 25.

² المرجع نفسه، ص 26.

وقد أشار عبد الفتاح حجازي إلى خطورة هذه المواقع قائلاً: "المواقع الإلكترونية الاحتيالية تُعد وسيلة مباشرة للتغريب بالضحية، حيث يتم إعدادها خصيصاً لاستدراجه إلى الإدلاء ببياناته السرية في ظل انخداعه بالشكل الخارجي للموقع"، هذا الاقتباس يُبرز أن الجريمة هنا ليست فقط تقنية، بل تقوم على توجيه إرادة المجني عليه نحو الخداع، من خلال وسائل ظاهرها الثقة وباطنها التضليل¹.

ومن الناحية القانونية، فإن التشريع الجزائري لا ينص صراحة على المواقع المزيفة كوسيلة مستقلة للنصب، إلا أن المادة 372 من قانون العقوبات التي تُجرّم "استخدام طرق احتيالية لإيهام المجني عليه بوجود مشروع كاذب" تصلح لتكييف هذا السلوك، طالما أن الموقع صُمم واشتُهر بهدف خداع المجني عليه وحمله على تسليم مال أو بيانات، ويرى بعض الباحثين أن هذه الأفعال تدخل في نطاق "الحيلة المؤثرة في الإرادة"، وهي أحد الأركان الكلاسيكية لجريمة النصب².

وعند إسقاط هذه الأفعال على شروط الجريمة، نجد أن الموقع الوهمي يُمثل السلوك الاحتيالي، بينما يُعد تسليم المال أو إدخال البيانات هو النتيجة الجرمية، أما العلاقة السببية فتتجلى في أن الضحية لم يكن ليُقدم على هذا الفعل لولا انخداعه بالموقع، وبالتالي فإن أركان الجريمة تامة من منظور قانوني، حتى وإن تم التنفيذ عبر وسيط إلكتروني.

من جهة أخرى، فإن القضاء يجد نفسه أمام تحدٍ في إثبات هذا النوع من النصب، نظراً لأن الجاني قد يكون غير معروف، أو يُخفي هويته باستخدام أدوات مثل الشبكات الافتراضية (VPN)، أو أسماء نطاقات مسجلة باسم جهات أجنبية، لذا فإن المحقق أو القاضي بحاجة إلى أدلة رقمية متقدمة، مثل تتبع عنوان IP، وتحليل توقيات الدخول، ومطابقة النشاط الرقمي مع نتائج التحقيق الجنائي الرقمي.

الفرع الثالث : انتحال الهوية الرقمية

انتحال الهوية الرقمية من الوسائل الاحتيالية التي تُستخدم بشكل متزايد في الجرائم الإلكترونية، بالنظر إلى بساطة تنفيذها وفعالية نتائجها، إذ يتمكن الجاني من خلال معلومات حقيقية تعود للغير، من تجاوز نظم الحماية الرقمية

¹ عبد الفتاح بيومي حجازي، المرجع سابق، ص. 254.

² سفيان صوان، الجريمة الإلكترونية في التشريع الجزائري: دراسة مقارنة، دار الهدى، الجزائر، 2020، ص. 189.

بسهولة نسبية، دون الحاجة إلى تقنيات اختراق معقدة، وتبرز خطورة هذه الوسيلة في أنها توفر للمحتال مظهرًا قانونيًا زائفًا يسمح له بالتواصل مع الضحايا أو المؤسسات من موقع سلطة أو ثقة، مما يسهل استدراجهم لتنفيذ أوامر أو إفشاء بيانات، كما أن هذا النوع من الانتحال لا يقتصر على الأفراد، بل يشمل كذلك تقمص صفات كيانات اعتبارية، كالبنوك أو الهيئات الرسمية، مما يعزز من طابع الخداع ويعقد من عمليات التتبع والإثبات، ولهذا، فإن هذه الممارسة تمثل تهديدًا مباشرًا لمنظومة الأمن الرقمي، وتتطلب تكييفًا قانونيًا دقيقًا يراعي تطور أساليب الجريمة الإلكترونية¹.

وفي هذا السياق، يؤكد بعض الفقهاء أن انتحال الهوية ليس مجرد استغلال لبيانات الغير فحسب، بل هو اعتداء صريح على شخصية قانونية مستقلة، لما يترتب عنه من ضرر مادي ومعنوي، وقد يصل الأمر إلى تحميل الضحية مسؤولية تصرفات لم تصدر عنه مطلقًا، كما أن استغلال هوية الغير بشكل رقمي يُعد وفقًا للتشريعات الحديثة صورة من صور "التزوير المعلوماتي"، وذلك لقيام الجاني بتقديم بيانات غير صحيحة على أنها حقيقية، مما يؤدي إلى إضفاء مظهر مشروع على عمل غير قانوني².

وفي حالات أخرى، يلجأ المحتال إلى تقمص صفة مسؤول أو موظف مصرفي بهدف استدراج الضحية للكشف عن معلومات سرية، أو الضغط عليه لإجراء تحويلات مالية مستعجلة، وهو ما يُعرف بتقنية الاحتيال عبر التمثيل المؤسساتي الزائف، حيث تكون هوية الجاني بالكامل مستعارة، مدعومة أحيانًا بمواقع إلكترونية مقلدة أو شعارات رسمية مزيفة، وتُظهر الإحصائيات الحديثة أن هذا النوع من الانتحال قد أصبح من أكثر الوسائل فعالية في الإيقاع بالضحايا، خصوصًا في ظل غياب الوعي الرقمي الكافي لدى الكثير من المستخدمين.

ويمثل هذا النوع من الانتحال تحديًا حقيقيًا على مستوى الإثبات، إذ غالبًا ما يختفي الجاني وراء أدوات تمويه رقمية يصعب تتبعها بالوسائل التقليدية، كما أن الحدود غير الواضحة بين البيانات العامة والبيانات الخاصة على الإنترنت تخلق بيئة خصبة لاستغلال الثغرات، خاصة في ظل ضعف ثقافة الحماية الرقمية لدى الأفراد والمؤسسات على حد سواء، ومن الجوانب الجديرة بالانتباه أن بعض الجناة لا يكتفون بانتحال الهوية لهدف مباشر، بل يستخدمونها كمرحلة أولى ضمن سلسلة من الأفعال الاحتيالية، ما يجعل هذا الأسلوب أكثر خطورة من حيث الأثر التراكمي

¹ عبد القادر بن عبد الله آل معبر، جريمة الانتحال الإلكتروني: دراسة مقارنة بين الفقه الإسلامي والنظام السعودي، المجلة الدولية للبحوث القانونية، العدد 9، ص. 1020.

² عبد القادر بن عبد الله آل معبر، نفس المرجع، ص. 1027.

للجريمة، وبناءً على ذلك فإن معالجة هذا التهديد لا تقتصر على الجانب القانوني فقط، بل تتطلب أيضاً جهوداً تقنية وقضائية متكاملة، تأخذ بعين الاعتبار أن الجريمة هنا تستهدف الثقة الرقمية كمبدأً أساسياً في المعاملات الحديثة¹.

ومن صور انتحال الهوية التي شهدت تطوراً لافتاً في السنوات الأخيرة، اعتماد بعض الجناة على تقنيات التزييف العميق (Deepfake)، التي تتيح إنشاء صور أو مقاطع صوتية ومرئية تبدو حقيقية تماماً، لكنها في الواقع مكوّنة بواسطة الذكاء الاصطناعي، وتكمن خطورة هذه الوسيلة في أنها تمنح الانتحال بُعداً بصرياً أو صوتياً يُعزز من قابلية التصديق، مما يزيد من فعالية الاحتيال ويعقّد من عملية كشفه، فقد أصبح بالإمكان إنتاج فيديو مزيف لشخصيات عامة أو موظفين رسميين، تُستعمل لإقناع الضحية بإجراء تحويلات أو الإفصاح عن معلومات سرية، ضمن سيناريو مُحكم يصعب التشكيك فيه للوهلة الأولى، واستعمال هذه التقنية ضمن سياق النصب الإلكتروني يمثل تطوراً نوعياً في الوسائل الاحتيالية، ويضع المشرّع والمؤسسات القضائية أمام تحديات جديدة تتعلق بكيفية إثبات هوية الجاني، وتمييز المحتوى الحقيقي من الملفق.

الفرع الرابع : البرمجيات الخبيثة (Malware)

بات استغلال البرمجيات الخبيثة في تنفيذ عمليات النصب والاحتيال الإلكتروني يمثل واقعاً ملموساً، لا مجرد احتمال نظري هذه البرمجيات، التي تُطوّر خصيصاً لتنفيذ تعليمات غير مشروعة داخل بنية النظام، باتت تُوظف بذكاء ضمن خطط احتيالية معقّدة تستهدف سرية البيانات وسلامة المعاملات الرقمية، ولا تقف خطورتها عند الجانب التقني فحسب بل تمتد إلى قدرتها على تقويض الثقة في الوسائط الإلكترونية².

تُعَدّ البرمجيات الخبيثة من أعقد الوسائل الاحتيالية التي تُستعمل، كونها تتيح للجاني التسلل إلى أنظمة معلوماتية واستغلالها في تحقيق مكاسب غير مشروعة، وتقوم هذه البرمجيات في الغالب على مبدأ تنفيذ تعليمات ضارة داخل

نظام التشغيل، دون علم الضحية، ما يحقق عنصر المباغته ويصعّب عملية الكشف المبكر، وتتنوع من حيث وظائفها وأهدافها، فمنها ما يُستخدم في سرقة المعطيات البنكية، ومنها ما يُستخدم في تعطيل النظام، أو فتح أبواب خلفية للسيطرة على الجهاز عن بُعد وما يُميز هذه البرامج عن غيرها من الوسائل التقليدية هو أنها لا تُظهر أي سلوك مباشر يُثير الشك، بل تُبرمج لتعمل في الخلفية، وقد تمرّ عبر جدران الحماية دون أن تُكتشف، خاصةً إن تم تغليفها أو تشفيرها، ويشير "سيكورسكي" و"هونيج" إلى أن البرمجيات الخبيثة في الغالب تُصمم بطريقة تجعل تحليلها واكتشاف

¹ عبد القادر بن عبد الله آل معبر، مرجع سابق، ص. 1030.

² Legal rules for preventing and combating cyber crimes in Algerian legislation مجلة العلوم الإنسانية – جامعة قسنطينة 1

سلوكها أمراً معقداً، حيث يتم استخدام تقنيات مثل إخفاء السلاسل النصية وتغليف الملفات التنفيذية لمنع فحصها الساكن¹.

ومن بين أكثر البرمجيات استخداماً في جرائم الاحتيال، نجد أحصنة طروادة (Trojans) التي تُرسل عادة في مرفقات البريد الإلكتروني، متخفية تحت غطاء مستند أو ملف مشروع، لكنها بمجرد تفعيلها تتيح للمهاجم إمكانية تسجيل ضغطات لوحة المفاتيح أو الوصول إلى الحسابات البنكية للضحية، وهو ما يُسهّل سحب الأموال أو تغيير بيانات الدخول، كما تستعمل الديدان (Worms) في نشر البرمجيات الخبيثة تلقائياً داخل شبكة داخلية، مما يُضاعف من حجم الخطر عند استهداف مؤسسات أو بنوك².

الفرع الخامس: الهندسة الاجتماعية (Social Engineering)

قد لا تحتاج بعض أساليب النصب والاحتيال الإلكتروني إلى كسر الشيفرات أو اختراق الأنظمة، بل يكفي فيها فهم سلوك الضحية، ومعرفة اللحظة المناسبة للضغط النفسي. من هنا، برزت "الهندسة الاجتماعية" كأداة لا تقل خطورة عن البرامج الخبيثة، بل ربما تفوقها أثراً، لأنها تستهدف الحلقة الأضعف في سلسلة الأمن المعلوماتي للإنسان.

تقوم هذه التقنية الاحتيالية على توظيف المهارات الاجتماعية لإقناع الضحية بالتصرف من تلقاء نفسها بما يخدم مصلحة الجاني، لا يُطلب منها سوى أن تصدق، أن تثق، أن تفتح الباب، وهذا ما يجعل الهندسة الاجتماعية خطرة وفعالة في آن واحد، خاصة عندما تُدمج مع معطيات يتم جمعها بهدوء عبر الفضاء الرقمي، دون أي خرق فني.

إنّ جوهر الهندسة الاجتماعية يقوم على التلاعب العاطفي والنفسي، حيث يعتمد الجاني إلى تقمص شخصية ذات سلطة أو مصداقية، كموظف بنك أو تقني صيانة، ليكسب ثقة الضحية ويوجّهها نحو تنفيذ السلوك المطلوب، مثل الكشف عن رموز الدخول أو تحويل الأموال. وقد أشار المؤلف "هادنيغي" إلى أن هذه الوسيلة لا تحتاج إلى مهارات

¹ 'Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software'، Michael Sikorski and Andrew Honig، No Starch Press، 2012، ص. 11.

² نفس المرجع، ص 12.

تقنية بقدر ما تتطلب فهماً دقيقاً لنفسية الإنسان وكيفية التأثير عليه، معتبراً أن الهندسة الاجتماعية هي "فن التلاعب بالبشر لدفعهم إلى اتخاذ قرارات قد لا تكون في صالحهم"¹.

وتزداد خطورة هذا الأسلوب عندما يُوظف في بيئة رقمية مفتوحة، كوسائل التواصل الاجتماعي أو البريد الإلكتروني، حيث يُمكن للجاني أن يجمع معلومات كثيرة عن الضحية دون علمها، ثم يستخدمها لاحقاً في حيك سيناريو مُقنع، وكثيراً ما تبدأ الهجمات بمحاولات بسيطة لجمع بيانات أولية تُستخدم لاحقاً في بناء عملية احتيال مركبة. ويشبه "هادنيغي" هذه التقنية بـ"الاختراق النفسي"، إذ يتم تجاوز الحواجز الأمنية من خلال الإنسان نفسه، لا عبر الجهاز أو النظام².

ومن خلال تحليلنا لهذا الأسلوب، يتبين أنه لا يركز فقط على الخداع، بل على قدرة الجاني على تصميم موقف نفسي معقد، يجعل الضحية تستشعر التهديد أو الاستعجال، مما يقلل من قدرتها على اتخاذ قرار عقلاني، كما أن الجريمة هنا تتحول إلى "سلوك مزدوج"، حيث يشترك فيها الجاني بمكر، والضحية عن غير قصد، في تنفيذ الفعل المجرّم.

فيتضح أن الهندسة الاجتماعية تمثل تهديداً حقيقياً للأمن المعلوماتي، وتُعد وسيلة فعالة في تنفيذ النصب الإلكتروني، لما تتميز به من صعوبة التتبع وسرعة التأثير، وهو ما يفرض على المشرّع والفاعلين الأمنيين مراجعة استراتيجيات المواجهة، ليس فقط عبر الحماية التقنية، بل كذلك من خلال التكوين والتحسيس المستمر للمواطنين والمؤسسات.

المطلب الثاني : الآثار المترتبة على جريمة النصب والاحتيال الإلكتروني

تشكل جريمة النصب والاحتيال الإلكتروني تهديداً كبيراً على الأمان الشخصي والاقتصادي للأفراد والمجتمعات في العصر الرقمي، فمع تزايد الاعتماد على الإنترنت في مجالات الحياة اليومية من تواصل، تجارة، وخدمات مصرفية، أصبحت هذه الجريمة لا تقتصر في تأثيرها على الضحايا المباشرين فقط، بل تمتد لتؤثر على النظام الاقتصادي بشكل عام، ولهذا من المهم التطرق لتأثيرها الواسع لفهم خطورة هذه الجريمة تحديدها.

¹ Christopher Hadnagy، *Social Engineering: The Art of Human Hacking*، Wiley Publishing، 2011، ص. 10.

² نفس المرجع، ص 12.

الفرع الأول : الآثار النفسية والاجتماعية على الضحايا

لا تقتصر خطورة جريمة الاحتيال الإلكتروني على الأضرار المادية التي تلحق بالضحية، بل تمتد لتشمل آثارًا نفسية واجتماعية عميقة قد تستمر لفترات طويلة بعد وقوع الجريمة. فالضحية لا تفقد أموالها أو بياناتها فحسب، وإنما تفقد كذلك شعورها بالأمان والثقة في البيئة الرقمية، الأمر الذي ينعكس سلبًا على استقرارها النفسي وعلاقاتها الاجتماعية.

ومن هذا المنطلق، سيتم التطرق في هذا الفرع إلى أبرز الانعكاسات النفسية والاجتماعية التي تُخلفها جريمة الاحتيال الإلكتروني على الضحايا، مع بيان أثرها على الثقة الرقمية والسلوك الاجتماعي للأفراد داخل المجتمع المعلوماتي. إن الأثر النفسي الذي تخلفه جريمة الاحتيال الإلكتروني لا يقل خطورة عن الآثار التي تخلفها الجرائم التقليدية كالسرقة أو النصب الواقعي، بل يتفوق عليها في بعض الحالات من حيث شدة الصدمة التي يعيشها الضحية، حيث إن الوقوع ضحية لجريمة رقمية لا يشكل فقط خسارة مالية، بل يفقد الفرد شعوره بالأمان الرقمي ويجعله عرضة للقلق المستمر والاضطرابات النفسية¹.

وقد أظهرت دراسات متعددة أن الضحايا يعانون من أعراض مختلفة، أبرزها القلق المعمم، اضطرابات النوم، الاكتئاب، والشعور بالخزي والإذلال، خاصة حين يُحملون أنفسهم مسؤولية ما جرى من خلال جلد الذات والاعتقاد أنهم كانوا سُدجًا أو غافلين، ويؤكد الباحثان "باتن" و"كروس" أن الكثير من الضحايا يمرّون بحالة من الإنكار أولًا، ثم الغضب، فالانطواء، ما يؤشر على وجود ضرر نفسي حقيقي شبيه بما يُعرف في علم النفس بصدمة ما بعد الجريمة². وعلى الصعيد الاجتماعي، ينعكس هذا الضرر في ما يُسمّى بـ"الانغلاق الرقمي"، إذ يختار كثير من الضحايا الانسحاب من التعامل مع الإنترنت أو التوقف عن استخدام الخدمات الإلكترونية، لا سيما تلك المتعلقة بالمعاملات المالية أو تقديم البيانات الشخصية، ويؤدي هذا السلوك إلى عزل الأفراد عن المجتمع الرقمي المتطور، ويزيد من الهوة بين الفئات المتمكنة تقنيًا وتلك المتخوفة من استخدام التكنولوجيا³.

وتتفاقم هذه الظاهرة في الدول النامية التي لا توفر آليات مؤسساتية فعالة لدعم الضحايا نفسيًا أو قانونيًا، مما يترك الفرد في مواجهة مباشرة مع الآثار النفسية والاجتماعية من دون سند، ويؤدي إلى تفشي ظاهرة عدم التبليغ عن

¹ Mark Button and Cassandra Cross 'Cyber Frauds, Scams and their Victims', Routledge, 2017, P. 83

² Mark Button and Cassandra Cross P 84

³ Mark Button and Cassandra Cross P.88

الجريمة الإلكترونية، كما أن غياب أنظمة الحماية يعمق من مشاعر الخوف، ويعزز من انعدام الثقة في الوسائل الرقمية ككل، ما يعيق مسار التنمية التكنولوجية في الدولة¹.

الفرع الثاني : الآثار الاقتصادية لجريمة الاحتيال الإلكتروني

تمثل جريمة الاحتيال الإلكتروني أحد أبرز التهديدات الاقتصادية في العصر الرقمي، لما تُحدثه من خسائر مالية مباشرة وغير مباشرة تمس الأفراد والمؤسسات وحتى الاقتصاد الوطني ككل. فالتوسع المتزايد في استخدام المعاملات الإلكترونية والخدمات الرقمية جعل الأنظمة المالية والتجارية أكثر عرضة للهجمات الاحتيالية وما يترتب عنها من أعباء اقتصادية متصاعدة.

وعليه، سيتم في هذا الفرع دراسة أهم الآثار الاقتصادية الناجمة عن جرائم الاحتيال الإلكتروني، سواء على مستوى الأفراد من خلال الخسائر المالية المباشرة، أو على مستوى المؤسسات والدولة من خلال تكاليف الحماية وتراجع الثقة في الاقتصاد الرقمي.

لا تقف آثار الاحتيال الإلكتروني عند الجانب النفسي، بل تمتد لتشمل تأثيرات مالية واقتصادية بالغة الخطورة، سواء على الأفراد أو على المؤسسات والدولة، فعلى مستوى الأفراد، يتسبب هذا النوع من الجرائم في خسائر مالية مباشرة تتمثل في سرقة الحسابات، اختراق بطاقات الائتمان، أو تحويل الأموال دون علم الضحية، كما قد يُجبر الضحايا على تحمل تكاليف إضافية مثل الاستعانة بخبراء تقنيين لاستعادة الحسابات، أو تكاليف قانونية لملاحقة الجناة². وتزداد المعاناة لدى الأفراد العاملين في قطاعات غير مؤمنة رقمياً أو الذين يستخدمون هواتفهم الذكية في المعاملات اليومية، حيث يُشكّلون فريسة سهلة للمحتالين، بل وتؤدي بعض هذه الحالات إلى إفلاس فردي أو تعطل مشاريع تجارية صغيرة، لا سيما في البيئات الريفية أو الاقتصادية المحدودة.

أما على صعيد المؤسسات، فالأمر أكثر تعقيداً، حيث إن جريمة واحدة قد تُكلف الشركة ليس فقط أموالاً طائلة بل سمعتها أيضاً، ويضطر كثير من الشركات إلى تخصيص ميزانيات ضخمة للأمن السيبراني، بما يشمل تطوير الأنظمة، تدريب العاملين، والاشتراك في خدمات مراقبة وحماية متقدمة، وتُعدّ هذه المصاريف عبئاً إضافياً، خصوصاً على المؤسسات الصغيرة والمتوسطة التي لا تملك أساساً موارد كبيرة³.

¹ "On the Issue of Cyber Fraud" ، N. Krasovskaya and A.A. Gulyaev ، Vestnik Udmurtskogo Universiteta ، 2022 ، P134.

² "A Review of Online Scams and Financial Frauds in the Digital Age" ، Amos Kipngetich ، مجلة GSC Advanced ،

Research and Reviews ، 2025 ، p. 7

³ Ibid.، p. 09. ، Amos Kipngetich

وعلى مستوى الدولة، يؤدي انتشار الاحتيال الإلكتروني إلى تأثيرات مباشرة على الاقتصاد الوطني، من خلال خفض حجم الاستثمارات الرقمية، وتراجع الثقة في المعاملات الإلكترونية، وانخفاض استخدام المنصات الحكومية فكل هجوم إلكتروني ناجح، خاصة إذا استهدف مؤسسة رسمية أو بنكية، يحدث صدمة في السوق الرقمية، ويثير موجة من الشك والخوف تؤدي إلى عزوف المواطنين عن استخدام الوسائل الرقمية¹.

وقد أشارت تقارير اقتصادية دولية إلى أن العالم يخسر سنوياً ما يتجاوز 6 تريليونات دولار بسبب الجرائم الإلكترونية، وهي خسائر تمس كل الأطراف الأفراد، الشركات، والدول. كما أن هذه الجرائم تُعرق نمو قطاع التجارة الإلكترونية، وتبطئ من سير المشاريع الحكومية في الرقمنة الشاملة، ما يؤدي في نهاية المطاف إلى تأخير مسار التنمية الاقتصادية.

الفرع الثالث : تأثير الاحتيال الإلكتروني على الثقة في الدولة ومؤسساتها

تُعتبر الثقة في مؤسسات الدولة أحد أهم مؤشرات الشرعية السياسية والإدارية، وهي عنصر حساس يتأثر سريعاً عند كل خرق أمني أو قانوني، وفي حالة الاحتيال الإلكتروني يكون تآكل هذه الثقة أكثر حدة، لا سيما حينما تتورط منصات رسمية أو يتم استغلال ضعف الأنظمة الحكومية لتنفيذ الهجمات.

وفي هذا الإطار، سيتم التطرق إلى مدى تأثير جريمة الاحتيال الإلكتروني على ثقة الأفراد في الدولة ومؤسساتها، مع بيان انعكاسات ذلك على استخدام الخدمات الرقمية والصورة السيادية للدولة في البيئة المعلوماتية الحديثة.

حين يُخدع المواطن من خلال منصة حكومية مزيفة أو يتم الاحتيال عليه تحت غطاء مؤسسة رسمية، تنتزع ثقته في الدولة ومؤسساتها، ويبدأ في التشكيك في قدرتها على حمايته. وقد لا يميز المواطن العادي بين الجهة الحقيقية والجهة المزيفة، لكنه بالتأكيد يُحمّل الدولة مسؤولية التقصير في الحماية أو في الرقابة على الفضاء الإلكتروني.

كما أن غياب الاستجابة الفورية أو ضعف المتابعة القانونية يزيد من هذه الهوة، ويجعل المواطن يشعر بأنه متروك لمصيره في عالم رقمي خطير، ما يحدث فجوة عميقة بين الدولة والمجتمع. ويؤثر ذلك مباشرة في التفاعل مع المنصات الرقمية الحكومية، حيث يُفضّل الكثيرون العودة إلى الطرق التقليدية لتفادي المخاطر.

على المستوى الدولي، يُشكل فشل الدولة في التصدي للجرائم الإلكترونية نقطة ضعف تؤثر على صورتها السيادية، وتُضعف من قدرتها على اجتذاب الاستثمارات أو الدخول في شراكات تقنية، كما قد تصنّف في تقارير الشفافية أو الحوكمة على أنها بيئة محفوفة بالمخاطر الرقمية، ما يقلص من فرص النمو الاقتصادي والتكنولوجي على المدى الطويل².

¹ Rick D. Howard، Cyber Fraud: Tactics, Techniques, and Procedures، CRC Press، 2009، P. 125.

² عبد الفتاح بيومي حجازي، الجرائم الإلكترونية وأثرها على الأمن المجتمعي، مرجع سابق، ص 289.

ملخص الفصل :

تُعد جريمة النصب والاحتيال الإلكتروني من الجرائم المستحدثة التي فرضها التطور المتسارع للتكنولوجيا الرقمية، حيث أصبحت الشبكة المعلوماتية وسيلة فعالة تُستغل في ارتكاب أفعال احتيالية تهدف إلى الاستيلاء غير المشروع على أموال أو بيانات الغير. وقد أدى انتشار المعاملات الإلكترونية وتوسع استخدام الإنترنت إلى تنامي هذه الظاهرة، مما جعلها تشكل تهديدًا حقيقيًا للأفراد والمؤسسات على حد سواء، سواء من حيث حجم الخسائر أو من حيث صعوبة الكشف والمتابعة.

وقد تناول هذا الفصل الإطار المفاهيمي لجريمة النصب والاحتيال الإلكتروني من خلال التطرق إلى ماهيتها ونشأتها وتطورها، حيث تبين أنها امتداد للجريمة التقليدية لكنها تختلف عنها من حيث الوسائل والأساليب المعتمدة، إذ تعتمد على تقنيات حديثة كالنصيد الإلكتروني، والمواقع الوهمية، وانتحال الهوية الرقمية، والبرمجيات الخبيثة، والهندسة الاجتماعية. كما أظهر التطور التاريخي لهذه الجريمة أنها تطورت من أشكال بسيطة من الخداع عبر وسائل الاتصال التقليدية إلى جرائم رقمية منظمة وعابرة للحدود.

كما تم التمييز بين جريمة النصب والاحتيال الإلكتروني وباقي الجرائم الإلكترونية الأخرى، حيث يتضح أن الاحتيال يقوم أساسًا على عنصر التدليس والخداع بهدف الاستيلاء على المال أو المنفعة، بينما تركز الجرائم الإلكترونية الأخرى على أفعال اعتداء مباشرة على الأنظمة أو البيانات أو السمعة دون ضرورة وجود خداع مالي. ويُبرز هذا التمييز أهمية التكيف القانوني الصحيح للأفعال الإجرامية لضمان تطبيق النصوص المناسبة لكل حالة.

وفيما يتعلق بوسائل ارتكاب هذه الجريمة، فقد تبين أنها متعددة ومتطورة باستمرار، وتشمل النصيد الإلكتروني، المواقع المزيفة، انتحال الهوية الرقمية، البرمجيات الخبيثة، والهندسة الاجتماعية، وهي وسائل تعتمد في مجملها على استغلال الثقة الرقمية للمستخدم وإيقاعه في الغلط. كما أن هذه الجريمة تتسم بطابعها العابر للحدود، وصعوبة كشف مرتكبيها، وسرعة تطورها المستمر.

أما على مستوى الآثار، فقد خلص الفصل إلى أن جريمة النصب والاحتيال الإلكتروني لا تقتصر على إحداث أضرار مالية فحسب، بل تمتد آثارها إلى الجوانب النفسية والاجتماعية للضحايا، إضافة إلى تأثيراتها الاقتصادية الواسعة على الأفراد والمؤسسات والدولة، فضلاً عن إضعاف الثقة في المعاملات الرقمية ومؤسسات الدولة، وهو ما يبرز خطورة هذه الجريمة وضرورة تعزيز آليات مكافحتها القانونية والتقنية.

الفصل الثاني

الإطار القانوني لجريمة

النصب والاحتيال

الإلكتروني

بما أن الاحتيال الإلكتروني إحدى الجرائم المستحدثة التي أفرزتها التكنولوجيا المعاصرة، حيث أسهم في تسهيل المعاملات وتبادل المعلومات بشكل سريع وفعال، فإن الحماية من هذه الجريمة تكون هي الأخرى بإستخدام التقنيات التكنولوجية الحديثة والتدابير الوقائية وتوفير الأمن المعلوماتي يعتبر وسيلة فعالة في التصدي له، لأنه يبحث في إستراتيجيات توفير الحماية للمعلومة الإلكترونية من المخاطر التي تهددها ومن الإعتداء عليها بالإعتماد على الوسائل والإجراءات اللازم توفيرها لضمان الحماية الداخلية والخارجية للمعلومة، لهذا سعى المشرع الجزائري إلى مواكبة هذه التحولات من خلال إدراج نصوص قانونية تجرم الأفعال المرتبطة بالاحتيال عبر الوسائط الإلكترونية، خاصة ضمن قانون العقوبات والقوانين المكملة له، مثل قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويقصد بالنصب والاحتيال الإلكتروني كل سلوك إجرامي يستعمل الوسائل الرقمية كشبكة أنترنت أو البريد الإلكتروني أو الهواتف التقنية، بهدف خداع الضحية والإستيلاء على الأموال أو بياناتها بطرق إحتيالية

وعليه يتعين دراسة هذا الفصل في بحثين، حيث نتطرق إلى النظام القانوني المنظمة لجريمة النصب والاحتيال الإلكتروني في المبحث الأول، سبل مكافحة جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري في المبحث الثاني.

المبحث الأول: النظام القانوني المنظمة لجريمة النصب والاحتيال الإلكتروني

أفرز التطور التكنولوجي وانتشار وسائل الاتصال الحديثة أنماطًا إجرامية جديدة، من بينها جريمة النصب والاحتيال الإلكتروني التي أصبحت تشكل خطرًا حقيقيًا على المعاملات المالية والبيانات الشخصية للأفراد. ونظرًا لخصوصية هذه الجريمة، فقد تدخل المشرع الجزائري من خلال مجموعة من النصوص القانونية والإجراءات القضائية لمحاولة تنظيمها ومواجهتها. وعليه، يقتضي الأمر دراسة الأركان القانونية التي تقوم عليها هذه الجريمة، إلى جانب بيان إجراءات المتابعة القضائية المتعلقة بها.

المطلب الأول: أركان جريمة النصب والاحتيال الإلكتروني

تقوم جريمة النصب والاحتيال الإلكتروني، كغيرها من الجرائم، على مجموعة من الأركان القانونية التي لا يمكن تصور قيام الجريمة دون توافرها. غير أن خصوصية البيئة الرقمية أضفت على هذه الأركان طابعًا تقنيًا معقدًا، سواء من حيث الوسائل المستعملة أو طريقة تنفيذ الفعل الإجرامي. لذلك، يستوجب الأمر دراسة الركن الشرعي، ثم الركن المادي، وأخيرًا الركن المعنوي باعتبارها الأساس القانوني لقيام المسؤولية الجزائية.

الفرع الأول : الركن الشرعي

يُعد الركن الشرعي حجر الأساس في التجريم والعقاب، إذ لا يمكن مساءلة أي شخص جزائيًا ما لم يوجد نص قانوني يجرم الفعل المرتكب ويحدد العقوبة المقررة له، تجسيدًا لمبدأ الشرعية الجنائية. ومع تطور الجرائم الإلكترونية، برزت إشكالية مدى كفاية النصوص التقليدية لاستيعاب صور النصب والاحتيال المرتكبة عبر الوسائط الرقمية، وهو ما يقتضي دراسة الأساس القانوني الذي اعتمد عليه المشرع الجزائري في تجريم هذا النوع من الأفعال

الركن الشرعي لجريمة النصب والاحتيال الإلكتروني في التشريع الجزائري يقصد به النصوص القانونية التي تجرم الأفعال المرتبطة باستخدام الوسائل الإلكترونية في ارتكاب جريمة النصب والاحتيال، يُعتبر الركن الشرعي العنصر الأساسي الذي يحدد الجريمة، ويشمل النصوص التي تحدد الأفعال المحظورة والعقوبات المقررة.

في التشريع الجزائري جريمة النصب والاحتيال تُعاقب عليها المادة 372 من قانون العقوبات الجزائري، التي تنص على معاقبة الأشخاص الذين يتوصلون إلى استلام أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات باستخدام وسائل احتيالية، مثل استعمال أسماء أو صفات كاذبة أو سلطة خيالية، أو اعتماد مالي خيالي، أو إحداث الأمل في وقوع حادث أو واقع وهمي، وتشمل العقوبات الحبس من سنة إلى خمس

سنوات وغرامة مالية تتراوح من 500 إلى 20,000 دينار، مع إمكانية الوصول إلى عشر سنوات حبس في حال تعلق الأمر بإصدار أسهم أو سندات مالية¹.

ورغم أن النصب والاحتيال الإلكتروني لم يُحدد بشكل صريح في التشريع الجزائري، فإن الأفعال المرتكبة باستخدام الوسائل الإلكترونية في تنفيذ جريمة النصب تُعتبر ضمن الأفعال المجرمة وفقاً للمادة 372 من قانون العقوبات، حيث يُمكن تطبيق نفس المبادئ على الأفعال التي يتم تنفيذها عبر الإنترنت باستخدام التقنيات الحديثة مثل انتحال الهوية الرقمية، أو المواقع الإلكترونية المقلدة، أو البرمجيات الخبيثة.

الركن الشرعي لجريمة النصب والاحتيال الإلكتروني يتحدد بشكل أساسي من خلال استخدام الوسائل الإلكترونية أو التقنيات الحديثة لتنفيذ الجريمة تشمل هذه الوسائل الإنترنت والأجهزة الرقمية التي يتم استغلالها في تنفيذ أفعال احتيالية على الإنترنت، سواء كان ذلك عبر انتحال الهوية الرقمية أو المواقع الإلكترونية المقلدة أو حتى البرمجيات الخبيثة². ولتوقيع العقوبة على مرتكبي هذه الجرائم يعتمد الأمر بشكل أساسي على المادة 372 من قانون العقوبات الجزائري، التي تجرم الاستيلاء على مال أو حق الغير باستخدام الوسائل الاحتيالية، وتشمل هذه المادة أيضاً جميع الوسائل الرقمية التي تُستخدم في تنفيذ الأفعال الاحتيالية، وبالتالي يتم محاكمة الجاني مرتكب هذه الجريمة وفقاً لنفس المبادئ القانونية التي تحكم النصب التقليدي.

من الجدير بالذكر أنه رغم غياب نص قانوني صريح يحدد النصب والاحتيال الإلكتروني بشكل مفصل في قانون العقوبات الجزائري، إلا أن الأفعال المرتكبة باستخدام الوسائل الإلكترونية يمكن معاقبتها تحت نفس الفقرة التي تتناول النصب التقليدي، بالإضافة إلى ذلك هناك قانون التجارة الإلكترونية و قانون حماية البيانات الشخصية اللذان يُجرمان الأفعال التي تشمل التلاعب بالبيانات أو الاحتيال عبر الإنترنت.

¹ قانون العقوبات الجزائري، المادة 372.

² القانون رقم 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولتعزيز القاعدة القانونية الأساسية "لا جريمة ولا عقوبة إلا بنص"، يُفهم أن الركن الشرعي لجريمة النصب والاحتيال الإلكتروني يجب أن يعتمد على نص قانوني محدد يجرم هذا النوع من الجرائم، وعليه يتم محاكمة مرتكبي هذه الجرائم باستخدام قانون العقوبات، بالإضافة إلى قانون التجارة الإلكترونية و قانون حماية البيانات الشخصية¹.

الفرع الثاني : الركن المادي

لا يكفي لقيام جريمة النصب والاحتيال الإلكتروني وجود نص قانوني يجرم الفعل، بل يجب أن يصدر عن الجاني سلوك مادي ملموس يؤدي إلى نتيجة إجرامية يترتب عنها ضرر بالمجني عليه. ويكتسي الركن المادي في الجرائم الإلكترونية خصوصية واضحة، بالنظر إلى اعتماد الجاني على الوسائل التقنية والرقمية في تنفيذ نشاطه الإجرامي، الأمر الذي يفرض تحليل عناصر هذا الركن من سلوك إجرامي ونتيجة جرمية وعلاقة سببية.

يُعدّ الركن المادي أحد العناصر الجوهرية التي لا غنى عنها في قيام جريمة النصب والاحتيال الإلكتروني، حيث يُعبّر عن الفعل الخارجي الذي ارتكبه الجاني، والذي يمثلّ السلوك الجرمي في صورته الظاهرة ولما كانت الجرائم الإلكترونية تتميز بوسائلها الرقمية غير التقليدية، فإن فهم الركن المادي في هذا السياق يقتضي التوسّع في تفسير مكوناته، ويتكوّن الركن المادي من ثلاث عناصر أساسية مترابطة: السلوك الإجرامي، النتيجة الجرمية، والعلاقة السببية بين الفعل والنتيجة².

أولاً : السلوك الإجرامي

السلوك الإجرامي هو الفعل أو الامتناع الذي يصدر عن الجاني ويكون مخالفاً للقانون، ويتحقق من خلاله النشاط الخارجي الذي يُرتكب به الفعل المجرّم في جريمة النصب والاحتيال الإلكتروني، يتمثل السلوك في استخدام وسائل رقمية لخداع المجني عليه وحمله على تسليم مال أو منفعة، وتتميز هذه الوسائل بالتنوع والتطور مما يزيد من صعوبة مواجهتها بالطرق القانونية التقليدية، وتتخذ الأفعال الاحتيالية في السياق الإلكتروني صوراً مختلفة منها:

¹ الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المعدل والمتمم .

² الوسيط في شرح قانون العقوبات - القسم العام، دار النهضة العربية، القاهرة.

- إرسال رسائل إلكترونية زائفة توهم الضحية بأنها مرسله من جهات رسمية أو مؤسسات مصرفية.
- إنشاء مواقع إلكترونية مزيفة تحاكي المواقع الأصلية وتطلب من المستخدمين إدخال بياناتهم الشخصية أو البنكية.
- انتحال صفة موظف أو مسؤول حكومي عبر الهاتف أو البريد الإلكتروني.
- استخدام تطبيقات وهمية أو رموز QR خادعة تؤدي إلى تحميل برمجيات خبيثة¹.

وقد لاحظ الفقه أن الجاني في هذه الجرائم يعتمد بشكل كبير على "الهندسة الاجتماعية"، وهي مجموعة من التقنيات النفسية التي تهدف إلى استغلال ثقة المجني عليه من خلال التأثير على قراراته، يُستغل في ذلك جهل الضحية بالتقنيات الرقمية، أو طمعه في عروض مغرية، أو خوفه من فقدان بياناته أو ماله، وهنا تظهر براعة الجاني في خلق سيناريو احتيالي مقنع يحمل الضحية على اتخاذ قرار يصب في مصلحته.

ومن الناحية القانونية يجب أن يتصف هذا السلوك بالاحتيال، أي أن يكون قائماً على الكذب والمراوغة، وليس على مجرد إغفال أو صمت، فالاحتيال يُفترض فيه أن يكون سلوكاً إيجابياً مقصوداً يهدف إلى الخداع كما يشترط أن يكون هذا الفعل مؤثراً بشكل جوهري على إرادة المجني عليه، بحيث لو علم بالحقيقة لما أقدم على التصرف الذي كلفه خسارة مالية أو معنوية².

وتُجمع الدراسات على أن السلوك الإجرامي في هذا النوع من الجرائم غالباً ما يكون مركباً من عدة أفعال متتابعة، تبدأ بإعداد البيئة الاحتيالية (مثل الموقع أو التطبيق)، ثم تنفيذ الخداع (كالرسالة أو المكالمات)، وأخيراً انتظار التفاعل من المجني عليه، هذا التسلسل في التنفيذ يزيد من تعقيد الجريمة ويجعل من الصعب رصدها مبكراً أو إثباتها قضائياً³.

كما أن السلوك الاحتيالي في البيئة الرقمية قد يتخذ طابعاً مستمراً أو دورياً، إذ يكرر الجاني نفس الأسلوب الاحتيالي على عدد من الضحايا بهدف تحقيق ربح مستمر، وقد تكون الأداة المستخدمة واحدة أو تختلف حسب نوع الضحية المستهدفة، فبعض الجناة يتخصصون في الاحتيال عبر العملات الرقمية، بينما يركز آخرون على اختراق البريد

¹ عبد الله سليمان، شرح قانون العقوبات - القسم العام، ديوان المطبوعات الجامعية، الجزائر، ص 143.

² صرا ندية، جريمة النصب والاحتيال عبر مواقع التواصل الإلكتروني، مذكرة ماستر، جامعة غرداية، 2023، ص. 10.

³ صرا ندية، جريمة النصب والاحتيال عبر مواقع التواصل الإلكتروني، مرجع سابق، ص. 11.

الإلكتروني أو تطبيقات الدفع، من الأمثلة العملية الشائعة: رسائل البريد التي تطلب من المستخدم تحديث بياناته المصرفية لأسباب أمنية، أو رسائل فورية تدّعي ربح جائزة وتطلب معلومات شخصية، أو اتصالات هاتفية مزيفة من موظفي بنوك وهميين، كل هذه الأساليب تعتمد على بث الذعر أو الطمع في ذهن المجني عليه، ما يدفعه إلى اتخاذ قرارات غير عقلانية.

ولأن القانون الجزائري لا ينص صراحة على كل وسيلة من هذه الوسائل، فإن قضاة الموضوع يضطرون إلى التكييف الواسع انطلاقاً من المفهوم العام للنصب الوارد في قانون العقوبات، وهو ما يجعل الاجتهاد القضائي يحتل مكانة هامة في مواجهة هذه الجرائم، من خلال توسيع مفهوم الوسائل الاحتيالية لتشمل الأشكال الحديثة¹.

ثانياً : النتيجة الجرمية

تُعدّ النتيجة الجرمية من بين العناصر المحورية في الركن المادي، إذ أنها تُجسّد الضرر الفعلي الذي ترتب عن السلوك الاحتيالي، وتتحقق هذه النتيجة عندما يُسلم المجني عليه مالا أو يُفصح عن معلومات سرية بناءً على اعتقاده الخاطئ الذي نتج عن الحيلة أو الوسيلة الاحتيالية المستعملة، ولا يشترط أن يكون الضرر كبيراً أو ذا قيمة مادية مرتفعة، بل يكفي أن يكون له أثر واقعي، حتى وإن كان بسيطاً، كأن يتم اختراق حساب إلكتروني، أو سرقة مبلغ مالي زهيد، أو الحصول على صورة شخصية تُستخدم لاحقاً في الابتزاز.

وفي هذا الإطار، تختلف النتيجة الجرمية بين جريمة وأخرى حسب وسيلة الاحتيال المعتمدة، ومدى تجاوب المجني عليه، فمثلاً إذا تم خداع الضحية عبر رسالة توهي بأنها من مؤسسة بنكية ونتج عن ذلك تسليمه لرقمه السري، فإن هذه النتيجة تعد قائمة حتى وإن لم يتم سحب المال فوراً، لأن التصرف في حد ذاته تم تحت تأثير الخداع.

ويشير بعض الباحثين إلى أن الجرائم الإلكترونية تتطلب إعادة تصور لمفهوم "الضرر"، نظراً لأن بعض النتائج تكون غير مادية لكنها تؤدي إلى خسارة حقيقية، من ذلك مثلاً سرقة بيانات بيومترية لا يمكن تغييرها مثل بصمات الأصابع أو ملامح الوجه، أو التلاعب بهوية رقمية ترتبط بمعاملات مالية مستقبلية، تُعتبر النتيجة في هذه الحالة متحققة حتى وإن لم تُصرف الأموال فعلياً، طالما أن المجني عليه قد تم الإيقاع به وقام بتصرف لم يكن ليقوم به لولا

¹ محمد صبحي نجم، شرح قانون العقوبات - الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2020، ص 143 - 136.

الوسيلة الاحتيالية، وفي هذا الإطار فإن القانون الجزائري يعتمد على معيار "التصرف الإرادي المعيب"، أي أن المجني عليه تصرف طوعية، لكنه كان ضحية احتيال جعله غير مدرك للطبيعة الحقيقية للفعل الذي أقدم عليه¹.

ومن الناحية الإجرائية فإن إثبات النتيجة الجرمية في الجرائم الإلكترونية يعتمد على وسائل مختلفة منها:

- تحليل بيانات الاتصال بين الجاني والضحية.
- فحص الأدلة الرقمية مثل الرسائل الإلكترونية وسجلات الدخول.
- الاستعانة بخبراء التقنية لتحديد مصدر الفعل.
- مقارنة أقوال الضحية مع التسلسل الزمني للوقائع.

كل ذلك يهدف إلى التأكد من أن الفعل الاحتيالي هو الذي أدى مباشرة إلى الضرر، وأن المجني عليه لم يكن متواطئاً أو مهملاً إلى درجة تقطع العلاقة السببية.

ثالثاً : العلاقة السببية

العلاقة السببية تمثل الصلة المنطقية بين السلوك الاحتيالي والنتيجة التي ترتبت عليه، فبدون هذه العلاقة لا يمكن تحميل الجاني المسؤولية، حتى وإن ثبت قيامه بفعل معين، وتظهر أهمية العلاقة السببية بشكل خاص في الجرائم التي تتم عن بعد، والتي قد يتداخل فيها أكثر من عامل يؤدي إلى الضرر.

تقوم العلاقة السببية عندما يتبين أن الوسيلة الاحتيالية كانت العامل الحاسم الذي دفع المجني عليه إلى اتخاذ القرار محل الجريمة، سواء أكان تسليمًا لمال أو كشفًا لمعلومة أو تحميلاً لتطبيق خبيث، وكفي أن يكون هذا العامل "مرجحاً" لتصرف المجني عليه، حتى وإن وُجدت عوامل أخرى، ويمكن تناول العلاقة السببية من زاويتين:

- السببية المباشرة: وهي عندما يكون الفعل الاحتيالي واضحاً ومتصلاً زمنياً بالفعل الذي قامت به الضحية.
- والسببية غير المباشرة: وهي عندما يتخلل بين الفعل والنتيجة عوامل أخرى، لكنها لا تقطع العلاقة طالما أن الحيلة كانت هي الدافع الرئيسي.

وقد ذهب الفقه الجنائي إلى اعتبار العلاقة السببية في هذا النوع من الجرائم "سلسلة من التأثيرات العقلانية"، تربط بين السلوك التدليسي والضرر اللاحق، ولا تُقطع إلا بوجود سبب أجنبي طارئ أو تدخل مباشر من الضحية يخرج

¹ صرا ندية، المرجع السابق، ص. 11.

عن المألوف، أما عن مدى مسؤولية الضحية في حال مساهمته في النتيجة بسبب الإهمال أو الجهل كأن يقوم بإدخال بياناته السرية رغم تحذيرات البنك، فذلك لا يُعفي الجاني من المسؤولية لكن قد يُؤخذ سلوك الضحية كعنصر لتخفيف العقوبة، أو كسبب لرفض التعويض في بعض الحالات المدنية¹.

العلاقة السببية تظل من النقاط الأكثر تعقيداً في إثبات الجريمة الإلكترونية، وتتطلب تكاملاً بين الفهم القانوني والتحليل التقني، وهو ما يدعو إلى تعزيز التكوين المتخصص لدى القضاة وأعوان الضبط القضائي في هذا المجال².

الفرع الثالث : الركن المعنوي

إلى جانب الركنين الشرعي والمادي، يتطلب قيام جريمة النصب والاحتيال الإلكتروني توافر الركن المعنوي، باعتبار أن هذه الجريمة من الجرائم العمدية التي تقوم على الإرادة الواعية والنية الإجرامية. فالجاني لا يرتكب فعله بطريق الخطأ، وإنما يتجه قصده نحو خداع الضحية وتحقيق منفعة غير مشروعة باستعمال وسائل تقنية متنوعة، وهو ما يقتضي الوقوف على عناصر القصد الجنائي وصعوبات إثباته في البيئة الرقمية.

إثبات المسؤولية الجنائية في جرائم النصب والاحتيال الإلكتروني لا يكتمل بمجرد تحقق السلوك والنتيجة، بل يتطلب وجود إرادة إجرامية واضحة تُعبّر عن قصد جنائي وإع، فالجاني في هذا النوع من الجرائم لا يتصرف عن طريق الخطأ أو الإهمال، وإنما يتجه فعله عمداً نحو استخدام وسائل تدليسية لتحقيق منفعة غير مشروعة على حساب الضحية، ويبرز الركن المعنوي هنا كعنصر أساسي يميز بين التصرف الإجرامي المتعمد وبين السلوك العفوي أو غير المقصود، خاصة في سياق رقمي يتيح للجاني تخطيط أفعاله بدقة وتنفيذها بسرية وبأساليب تقنية متقنة.

أولاً : عناصر الركن المعنوي

1. القصد الجنائي العام:

الاحتيال الإلكتروني يختلف من حيث طبيعته التقنية عن الاحتيال التقليدي، لكنه يشترك معه في كونه جريمة عمدية تقوم على نية إجرامية واضحة، فالجاني يتخذ من الوسائل التكنولوجية وسيلة لتنفيذ مشروعه الإجرامي، مستغلاً

¹ عبد الفتاح بيومي حجازي، الجرائم الإلكترونية والإنترنت: دراسة قانونية مقارنة، دار الفكر الجامعي، الإسكندرية، 2011، ص. 273.

² المرجع نفسه، ص 280.

خصائص العالم الرقمي كسهولة التنكر وانتشار المعلومات وسرعة الوصول إلى الضحايا، هذه الخصائص لا تُلغي ضرورة القصد بل تجعل إثباته أكثر أهمية وتعقيداً¹.

القصد الجنائي كما عرّفه أحمد فتحي سرور هو "اتجاه الإرادة إلى ارتكاب الجريمة مع العلم بعناصرها القانونية" هذا التعريف يتلاءم مع خصوصية الجريمة الإلكترونية، إذ أن الجاني لا يقتصر دوره على تنفيذ فعل فني بل يتعداه إلى توجيه هذا الفعل لخداع الغير واستغلالهم.

تظهر النية الإجرامية في عدة صور: جمع معلومات الضحية، مراقبة نشاطها الرقمي، تصميم خطة تقنية دقيقة للإيقاع بها وغيرها، كل خطوة من هذه الخطوات تُظهر أن الجاني يتصرف بإرادة مدبرة، وتُعد محاولات التغطية بعد الفعل مثل حذف الحسابات أو تشفير البيانات دلالة على علم الجاني بعدم مشروعية ما قام به، هذه الإرادة لا تُفترض بل تُستنبط من الوقائع والقرائن، كتنكرار المحاولة، دقة الأسلوب، ونوعية الأدوات المستخدمة. فكلما كان الفعل أكثر تعقيداً، كانت الإرادة أوضح.

يتكوّن الركن المعنوي من عنصرين مترابطين هما: العلم، والإرادة، العلم يعني أن الجاني كان مدركاً لطبيعة الوسيلة التي يستعملها، وأنه يعلم بأنها غير مشروعة وتهدف إلى خداع الضحية، وقد يُثبت هذا العلم من خلال استخدام أدوات تقنية لا يلجأ إليها المستخدم العادي إلا لهدف احتيالي مثل استخدام برامج انتحال الهوية، أو إنشاء مواقع إلكترونية مزيفة².

أما الإرادة، فهي توجه الجاني لفعل معين رغم إدراكه بعدم قانونيته، الإرادة تتجلى في التصميم على تنفيذ الفعل رغم معرفته المسبقة بعواقبه، ويُستدل عليها من طبيعة التنفيذ: إرسال روابط خادعة، التواصل المُخادع، اختلاق وقائع وهمية، كلها مؤشرات تدل على وجود إرادة حرة ومتعمدة³.

هذا التفاعل بين العلم والإرادة يُنتج القصد الجنائي الكامل، والذي يُعد جوهر الركن المعنوي في النصب الإلكتروني، ويمنع الخلط بين الفعل العمدى والفعل الناتج عن إهمال أو جهل.

¹ أحمد فتحي سرور، الوسيط في قانون العقوبات: القسم العام، كتاب، دار النهضة العربية، القاهرة، 2008، ص 228.

² وليد عبد الحي الشرفات، الجرائم الإلكترونية: دراسة مقارنة، كتاب، دار الثقافة للنشر والتوزيع، عمان، 2020، ص 199.

³ محمد عبد الفتاح عبد الباقي، جرائم الحاسوب والإنترنت في القانون المقارن، كتاب، دار النهضة العربية، القاهرة، 2017، ص 142.

2. القصد الجنائي الخاص:

في بعض الحالات لا يكفي وجود القصد العام بل يجب إثبات وجود قصد خاص، يتمثل في نية الجاني تحقيق نتيجة معينة، مثل الاستيلاء على مبلغ مالي محدد أو استغلال ثغرة مالية أو فنية معينة يظهر هذا القصد، من خلال سلوك الجاني المتكرر والممنهج أو من خلال طبيعة الضحايا الذين تم استهدافهم، أو الوسائل المستخدمة التي تطلبت تجهيزاً وتحليلاً مسبقاً.

وكما كانت الغاية محددة كتحويل أموال أو سحب بيانات بنكية، كلما أمكن إثبات القصد الخاص بوضوح، وبالتالي فإن التمييز بين القصد العام والخاص يساعد في تحديد مدى خطورة الجريمة وشكل التكييف القانوني الأنسب لها¹.

ثانيا : صعوبة إثبات الركن المعنوي تقنياً:

إثبات القصد الجنائي في الجرائم الرقمية لا يتم غالباً عبر الاعتراف المباشر، بل بالاعتماد على أدلة غير مباشرة، هذه الأدلة تتضمن فحص الأدوات الإلكترونية التي استخدمها الجاني وتحليل سجل نشاطه، وتفسير سلوكه الرقمي مثلاً: استخدام برامج التمويه، حذف الرسائل بعد الإرسال، أو تشفير البيانات، تُعد قرائن تقنية تُدل على أن الجاني كان يعلم بما يفعل ويسعى إلى إخفاء فعله، كما يُستفاد من طبيعة المحتوى المرسل، سواء احتوائه عبارات مضللة، تقديم هوية مزيفة وغيرها هذه القرائن التراكمية تُشكل قاعدة إثبات قوية لتوافر الركن المعنوي، وبالتالي فإن القاضي الرقمي المعاصر لا يكتفي بالعناصر التقليدية بل يعتمد على خبرة فنية وتحليل معمق لطبيعة الجريمة الإلكترونية، مما يُتيح بناء قناعة سليمة عن توافر النية الإجرامية².

1- تمييز القصد عن الخطأ غير العمدى:

التمييز بين القصد والخطأ أمر دقيق لكنه ضروري. الخطأ غير العمدى قد يحدث في حالات مثل الجهل بالإجراءات التقنية، أو الوقوع في شرك الفعل الاحتيالي بسبب نقص المعرفة الرقمية، بينما القصد الإجرامي يتطلب وعياً كاملاً بالسلوك ورغبة واضحة في تحقيق نتيجة ضارة للغير، عندما يُرسل الجاني رسالة مُخادعة، ثم يتابعها بمطالبة معلومات

¹ أحسن بوسقيعة - الوجيز في القانون الجزائري العام.

² نفس المرجع السابق.

مالية فذلك يُعد فعلاً مقصوداً، أما من يضغط على رابط غير آمن بسبب جهل، فذلك لا يُشكّل جريمة ما لم يُثبت أنه كرّر الفعل رغم التنبيه أو استغل المعلومة لاحقاً¹.

شدد المشرع الجزائري في المادة 394 مكرر على "الغش"، وهو ما يعني أن الخطأ أو الإهمال لا يكفيان بل يجب أن يكون هناك تدليس ناتج عن إرادة حرة تهدف إلى الإضرار، ما يجعل القصد العنصر الفاصل بين السلوك الجرمي والسلوك غير المجرّم.

2 - انعكاس الركن المعنوي في التشريع الجزائري:

نصوص القانون الجزائري تظهر بوضوح أن الركن المعنوي ليس عنصراً شكلياً بل جوهرياً، استخدام لفظ "الغش" في المواد العقابية المتعلقة بالاحتيال الرقمي يدل على أن المشرّع يشترط قيام نية تدليسية واعية، وليس مجرد وجود وسيلة احتيالية.

كما أن القضاء الجزائري من خلال التطبيقات الحديثة، بدأ يعتمد على الأدلة الرقمية والفرائن الفنية لاستنباط نية الجاني، خصوصاً عندما يكون التنفيذ معقداً وذا طابع خفي، التقرير الفني وتتبع السلوك وتحليل الضحية، كلها وسائل قانونية معتبرة لإثبات القصد الجنائي، ولذلك فإن الركن المعنوي أصبح أداة قانونية قوية لتفكيك الجريمة الإلكترونية وفهمها، وهو ما يجعل من دراسته عنصراً محورياً في فهم النصب الرقمي وتكييفه الصحيح.

المطلب الثاني : إجراءات المتابعة القضائية لمرتكبي جريمة النصب و الاحتيال الإلكتروني

إن مكافحة جريمة النصب والاحتيال الإلكتروني لا تتوقف عند مرحلة التجريم فقط، بل تمتد إلى الجانب الإجرائي المتعلق بتحريك الدعوى العمومية ومباشرة التحقيق والمتابعة القضائية. ونظراً للطابع التقني لهذه الجرائم وصعوبة اكتشافها، فقد أقر المشرع الجزائري مجموعة من الإجراءات والآليات القانونية التي تهدف إلى تسهيل التبليغ عنها وضمان فعالية المتابعة القضائية.

¹ محمد جباوي منير وبولشين خليل، خصوصية أركان الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعرييج، 2023، ص 35.

تُعد الشكوى وسيلة أساسية لتحريك الدعوى العمومية في بعض الجرائم، وتكتسي أهمية أكبر حين يتعلق الأمر بالجرائم الإلكترونية، وعلى رأسها جريمة النصب والاحتيال الإلكتروني، لما تتميز به من طابع خفي ووسائل فنية يصعب كشفها تلقائياً. وقد أدرك المشرع الجزائري هذا الطابع، فأقر آليات قانونية وإجرائية لحماية المتضررين وتفعيل الحق في التبليغ .

سنتناول من خلال هذا المطلب إلى تحريك الدعوى العمومية بتقديم شكوى (الفرع الأول) ، ثم الجهات المختصة باستقبال الشكاوى الرقمية (الفرع الثاني) ، صعوبات تحريك الدعوى العمومية في جرائم النصب و الاحتيال الإلكتروني (الفرع الثالث) .

الفرع الأول: تحريك الدعوى العمومية بتقديم شكوى

تُعتبر الشكوى من أهم الوسائل القانونية التي تساهم في كشف الجرائم الإلكترونية وتحريك الدعوى العمومية بشأنها، خاصة وأن العديد من جرائم النصب والاحتيال الإلكتروني تتم في الخفاء ولا تصل إلى علم السلطات إلا من خلال تبليغ الضحية. لذلك، تبرز أهمية دراسة مفهوم الشكوى وشروطها القانونية في إطار الجرائم المعلوماتية. تنص المادة 1 من قانون الإجراءات الجزائية على أن "الدعوى العمومية لتطبيق العقوبات تُحرّك وتباشر من طرف النيابة العامة أو من طرف الموظفين المؤهلين لذلك قانوناً"¹.

ما يعني أن تحريكها يكون في الأصل تلقائياً، غير أن هناك استثناءات يفرض فيها القانون ضرورة وجود شكوى لتحريكها، حمايةً لخصوصية المجني عليه أو لتفادي الملاحقة دون رغبة المتضرر.

¹ قانون الإجراءات الجزائية، الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المعدل والمتمم، المادة 1.

في هذا السياق، تُعد جريمة النصب الإلكتروني من الجرائم التي، رغم أنها ليست محصورة ضمن الجرائم التي يشترط فيها القانون الشكوى لتحريك الدعوى، إلا أن كشفها في كثير من الحالات لا يتم إلا من خلال مبادرة الضحية بالتبليغ أو الشكوى.

أولاً : مفهوم الشكوى

الشكوى هي الإجراء الذي يقوم به المجني عليه بإبلاغ السلطات المختصة عن وقوع جريمة، مطالباً بتحريك الدعوى العمومية. وقد كرس المشرع هذا الحق في المادة 72 من قانون الإجراءات الجزائية التي تنص على: "لكل شخص يعتبر نفسه متضرراً من جريمة أن يُقدم شكوى إلى الضبطية القضائية أو إلى النيابة العامة أو إلى قاضي التحقيق"¹.

ثانياً : الشروط القانونية للشكوى

ويشترط في الشكوى أن:

- تصدر عن صاحب الصفة، أي المتضرر من الجريمة شخصياً أو من يمثله قانوناً.
- تكون موجهة إلى جهة مختصة إقليمياً (وكيل الجمهورية أو فرقة الشرطة القضائية).
- تُقدم مرفقة بالقرائن المتوفرة، لاسيما في الجرائم الإلكترونية، مثل المراسلات الرقمية، كشوف المعاملات، صور الحسابات الوهمية، إلخ.

الفقه يرى أن الشكوى لا تُعد فقط وسيلة قانونية، بل أداة لتفعيل الرقابة الاجتماعية، خاصة في الجرائم المستحدثة².

¹ نفس المرجع، المادة 72.

² عبد الحميد بوشوشة، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2019، ص 140.

الفرع الثاني : الجهات المختصة باستقبال الشكاوى الرقمية

أدى تزايد الجرائم المرتكبة عبر الفضاء الرقمي إلى ضرورة توفير جهات متخصصة تتولى استقبال الشكاوى الإلكترونية ومعالجتها، سواء عبر المنصات الرقمية أو من خلال المصالح الأمنية والقضائية المختصة. وقد سعت السلطات الجزائرية إلى تطوير آليات التبليغ بما يتماشى مع خصوصية الجريمة الإلكترونية وطبيعتها التقنية. نظرًا لطبيعة الجريمة الإلكترونية، أصبحت السلطات العمومية في الجزائر تعتمد على منصات إلكترونية للتبليغ، حيث خصصت وزارة الداخلية بالتنسيق مع المديرية العامة للأمن الوطني فضاءً إلكترونيًا لتلقي شكاوى الجرائم السيبرانية، مرفقًا بإرشادات توجيهية¹.

ويُسمح كذلك للضحية بالتوجه مباشرة إلى مركز الشرطة أو الدرك الوطني المختص، أو إلى وكيل الجمهورية لإيداع الشكاوى بالطريقة التقليدية.

الفرع الثالث : صعوبات تحريك الدعوى العمومية في جرائم النصب و الاحتيال الإلكتروني

رغم الجهود التشريعية والإجرائية المبذولة لمواجهة جرائم النصب والاحتيال الإلكتروني، إلا أن تحريك الدعوى العمومية بشأنها ما يزال يواجه عدة صعوبات عملية وتقنية، ترتبط أساسًا بطبيعة الدليل الرقمي والطابع العابر للحدود لهذه الجرائم، إضافة إلى محدودية الوعي القانوني لدى بعض الضحايا.

تواجه عملية تحريك الدعوى في هذا النوع من الجرائم عدة عراقيل، من أبرزها:

- صعوبة الإثبات الرقمي: إذ يستوجب الأمر فحصًا تقنيًا للأجهزة أو البيانات، وهو ما قد يتجاوز قدرات المواطن العادي.
- امتداد بعض الجرائم إلى الخارج: مما يجعل تنفيذ التحقيقات مرهونًا بالتعاون القضائي الدولي.
- غياب الوعي القانوني لدى فئات واسعة من المواطنين، خاصة كبار السن أو ذوي المستوى التعليمي المحدود، مما يؤدي إلى التأخر في التبليغ أو التخوف منه.

¹ المديرية العامة للأمن الوطني، دليل مكافحة الجرائم السيبرانية، الجزائر، 2022، ص 33.

ورغم هذه الصعوبات، يبقى تقديم الشكوى أداة فعالة لتحريك الدعوى ومباشرة المتابعة القضائية، شريطة دعمها بالعناصر التقنية الكافية لتسهيل العمل التحقيقي والخبري¹.

المبحث الثاني: سبل مكافحة جريمة النصب والاحتيال الإلكتروني في التشريع الجزائري

أمام التزايد المستمر لجرائم النصب والاحتيال الإلكتروني، أصبح من الضروري اعتماد سياسة جنائية متكاملة لا تقتصر على العقاب فقط، وإنما تشمل كذلك الوقاية والتوعية وتعزيز وسائل الحماية التقنية والقانونية. ولهذا عملت الجزائر على تطوير مجموعة من الآليات الوقائية والمؤسسية لمواجهة هذا النوع من الإجرام المستحدث.

المطلب الأول: التدابير الوقائية

تُعد التدابير الوقائية من أهم الوسائل الحديثة في مكافحة الجريمة الإلكترونية، إذ تهدف إلى الحد من فرص وقوع الجريمة قبل حدوثها، من خلال تعزيز الوعي المجتمعي وتطوير أنظمة الحماية الرقمية. وتكتسي هذه التدابير أهمية خاصة في مجال النصب والاحتيال الإلكتروني بالنظر إلى سرعة تطور أساليبه ووسائله التقنية.

تُدرج التدابير الوقائية ضمن آليات السياسة الجنائية الوقائية التي تهدف إلى تقليص فرص ارتكاب الجرائم عبر الوسائل التقنية والرقمية، ومن بينها جريمة النصب والاحتيال الإلكتروني. ويظهر التركيز على هذه التدابير نتيجة التحول البنوي في طبيعة الإجرام، الذي لم يعد يقتصر على الأساليب التقليدية، بل بات يستند إلى وسائل معقدة تستغل ثغرات الوعي المعلوماتي وهشاشة البيئة الرقمية. ويمكن تصنيف التدابير الوقائية إلى ثلاث فروع رئيسية: التوعية (الفرع الأول) ، الأمن السيبراني (الفرع الثاني) ، ودور الإعلام (الفرع الثالث)².

الفرع الأول : التوعية

تؤدي التوعية دورًا محوريًا في الوقاية من جرائم النصب والاحتيال الإلكتروني، باعتبار أن ضعف الثقافة الرقمية وقلة الوعي بأساليب الاحتيال الحديثة من أهم الأسباب التي تجعل الأفراد عرضة للاستغلال الإلكتروني. لذلك، أصبحت حملات التحسيس والتثقيف الرقمي من الوسائل الأساسية للحد من هذه الجرائم.

تُعتبر التوعية من بين أهم الوسائل الوقائية غير التشريعية، وتستهدف رفع المستوى المعرفي للمواطن حول مخاطر الجريمة الإلكترونية. وقد أشارت الدراسات السوسيولوجية إلى أن قابلية بعض الأفراد ليكونوا ضحايا للنصب ترجع إلى ضعف إدراكهم لطبيعة التهديدات الرقمية التي تُمارَس عليهم بطرق غير مباشرة

¹ أحسن بوسقيعة – الوجيز في القانون الجزائري الخاص

² موقع القيادة العامة للأمن الوطني الجزائري.

وتشمل أدوات التوعية الوسائط الورقية والرقمية المستخدمة في الحملات التحسيسية، كالمطويات والملصقات والإعلانات السمعية البصرية التي يتم بثها في المؤسسات التربوية والجامعات. كما تم إدراج موضوعات الأمن المعلوماتي ضمن برامج التعليم العالي لبعض الشعب التقنية والقانونية، وهو ما يساهم في ترسيخ الوعي الوقائي لدى فئة الطلبة. ويضاف إلى ذلك إشراك مراكز التكوين المهني في تقديم حصص تطبيقية حول الأمن المعلوماتي ضمن التكوينات التقنية¹.

ترتبط فعالية التوعية بانتظام حملات التحسيس وتوسيع دائرة المستهدفين بها. إذ تبين أن فئات عمرية مثل كبار السن والمراهقين هم الأكثر عرضة لعمليات الاحتيال الإلكتروني، مما يستدعي ضبط مضامين التوعية وفق الفئة المستهدفة من حيث اللغة المستعملة، الوسيط المعتمد، والمدة الزمنية للبرنامج التحشيسي.

تُشهم القطاعات البنكية من جانبها في رفع منسوب الحذر لدى زبائنها، إذ تعتمد تقنيات التحذير الفوري عبر الرسائل النصية والتنبيهات الرقمية، وتنتشر توصيات أمنية بخصوص تجنب مشاركة المعلومات المصرفية. كما توفر بعض المؤسسات المالية تطبيقات للتحقق الآلي من صحة المواقع التي تقدم خدمات تحويل الأموال أو الدفع الإلكتروني. تشير الإحصائيات الحديثة إلى أن حملات التوعية التي نُفذت في الجزائر خلال السنوات الأخيرة أدت إلى تقليص عدد الشكاوى المسجلة لدى مصالح الأمن بنسبة معتبرة، خاصة تلك المتعلقة بالنصب عبر الإنترنت. كما رصدت الجهات المختصة تحسناً ملحوظاً في استجابة المواطنين للتحذيرات الصادرة عبر القنوات الرسمية.

الفرع الثاني : الأمن السيبراني

يشكل الأمن السيبراني خط الدفاع الأول في مواجهة الجرائم الإلكترونية، إذ يهدف إلى حماية الأنظمة المعلوماتية والبيانات الرقمية من الاختراق والاستغلال غير المشروع. ومع تنامي أساليب النصب الإلكتروني، أصبح تعزيز الحماية التقنية ضرورة حتمية لضمان أمن الأفراد والمؤسسات داخل الفضاء الرقمي.

يُقصد بالأمن السيبراني مجموع الإجراءات والآليات التي تهدف إلى تأمين الأنظمة المعلوماتية من الهجمات والاختراقات التي قد تؤدي إلى استغلال بيانات الأفراد والمؤسسات. ويتمثل الجانب التقني من هذا الأمن في استخدام أدوات الكشف

¹ لموشي جهيدة، "دور الضحية في حدوث جريمة النصب والاحتيال - مقارنة سوسيولوجية"، مجلة العلوم الاجتماعية والإنسانية، العدد 15،

عن التسلل، التشفير، والحماية من البرمجيات الخبيثة، بينما يشمل الجانب التنظيمي وضع سياسات أمنية داخلية تضمن سلامة المعطيات¹.

أنشأت الجزائر المركز الوطني للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بموجب مرسوم تنفيذي، باعتباره هيئة وطنية متخصصة تُعنى بمتابعة المخاطر السيبرانية، وإنشاء آليات استجابة مبكرة، والتنسيق مع مصالح الأمن الوطني والدرك الوطني. ويدعم هذا المركز بنية البيانات الحكومية من خلال إصدار تقارير دورية تُرفع إلى الوزارات المعنية.

يتوفر الأمن الوطني والدرك الوطني على فرق بحث وتحليل جنائي رقمي، مُجهزة بمخابر رقمية لفحص الأدلة وتفرغ المحتويات الإلكترونية، بالإضافة إلى خبراء في تعقب الأثر الرقمي والاتصال المشفر. وتعتمد هذه الفرق في تحقيقاتها على بروتوكولات قانونية لضمان مشروعية الدليل الإلكتروني، من حيث الاسترجاع والحفظ والتوثيق.

أدرجت الجهات القضائية أيضاً وحدات دعم تقني في بعض المحاكم الابتدائية الكبرى، تقوم بالتنسيق مع مصالح الشرطة القضائية وممثلي النيابة العامة في تحليل المعطيات المحجوزة خلال التحقيقات. وتم التوقيع على اتفاقيات تعاون تقني بين وزارة العدل وبعض المؤسسات الجامعية لتأهيل الموارد البشرية العاملة في هذا المجال.

يشمل الأمن السيبراني أيضاً البعد التشريعي، إذ تم سن القانون 18-04 المؤرخ في 10 ماي 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، والذي نص على التزامات متعلقة بإعلام الشخص المعني، وحماية البيانات من الوصول غير المصرح به، كما نص على إنشاء سلطة وطنية لحماية المعطيات الشخصية².

كما تم إدراج مادة الحماية السيبرانية ضمن محتويات التكوين القاعدي لوكلاء الشرطة، والدرك، وبعض وحدات الجيش الوطني الشعبي، مع تحديث المقررات التكوينية سنوياً وفق المعايير المعتمدة من قبل المنظمات الدولية المختصة في الأمن الرقمي.

الفرع الثالث : دور الإعلام

¹ حسن كليبي، نجمة الطبيب، "جريمة النصب الإلكتروني من منظور المشرع الجزائري"، مجلة المفكر، المجلد 20، العدد 01، 2025، ص. 64.

² القانون رقم 18-07 المؤرخ في 10 يونيو 2018، يتضمن إنشاء السلطة الوطنية لحماية المعطيات الشخصية، وواجبات حماية البيانات المتعلقة بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

يلعب الإعلام دوراً هاماً في مكافحة الجريمة الإلكترونية من خلال نشر الوعي القانوني والرقمي، وتبسيط الضوء على أساليب الاحتيال المستحدثة، بما يساهم في حماية المجتمع من مخاطر النصب الإلكتروني. كما يساهم الإعلام في تعزيز الثقافة الوقائية وتوجيه المواطنين نحو سبل الحماية القانونية والتقنية.

يمثل الإعلام أحد الأدوات المعتمدة في دعم الوقاية من الجريمة، من خلال مساهمته في نشر المعلومات ذات الصلة، ورفع الوعي الجماعي بأشكال النصب الإلكتروني. يتخذ هذا الدور طابعاً توعوياً حين يتعلق الأمر بتحليل الأساليب المستعملة في الاحتيال الرقمي، وعرض وقائع حقيقية لأشخاص تعرضوا للنصب الإلكتروني، وشرح تدابير الحماية الممكنة¹.

ساهمت بعض البرامج الإذاعية والتلفزيونية في تغطية موضوع الاحتيال الرقمي عبر تخصيص فقرات دورية بالتنسيق مع مصالح الأمن المختصة، كما نُظمت مؤائد مستديرة جمعت بين إعلاميين، مختصين في الإعلام الآلي، وممثلين عن الهيئات القضائية لشرح كيفية التصدي للجريمة الرقمية.

في موازاة ذلك، بدأت بعض الهيئات الرقابية، على غرار الهيئة الوطنية للوقاية من الجرائم المعلوماتية، إصدار دلائل للصحفيين تحتوي على مفردات دقيقة وتعريفات قانونية للجريمة الرقمية، مرفقة بأمثلة واقعية وأرقام خط النجدة الإلكتروني. وتم إدراج وحدات حول السلامة المعلوماتية في بعض مراكز تكوين الصحفيين².

المطلب الثاني: الإصلاحات القانونية والتقنية لمكافحة الجريمة (تشديد العقوبات، التعاون القضائي، الأدوات التقنية)
شهدت الجزائر خلال السنوات الأخيرة ارتفاعاً ملحوظاً في وتيرة الجرائم الإلكترونية، وعلى رأسها جريمة النصب والاحتيال الإلكتروني، وهو ما تطلب استجابة تشريعية وتقنية ومؤسسية عاجلة وفعالة.

وقد أدرك المشرع أن هذه الظاهرة لا يمكن مجابهتها بنفس الآليات التقليدية المخصصة للجرائم العادية، بل تتطلب إصلاحات نوعية تمس التشريع، الإجراء، والوسائل المعتمدة في التحري والإثبات.

في هذا الإطار، انطلقت الدولة الجزائرية في تنفيذ مسار إصلاحي متكامل، شمل تشديد العقوبات عند استخدام الوسائل الإلكترونية، وتحديث آليات التعاون القضائي داخلياً وخارجياً، بالإضافة إلى إدماج الأدوات التقنية الحديثة في المنظومة الأمنية والقضائية.

¹ سامية العايب، مثال عرابية، مرجع سابق ص. 230.

² حياة هراكي، "واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية"، مجلة التغيير الاجتماعي، جامعة بسكرة، المجلد الثامن، العدد 02، 2023، ص 41.

أولاً : تشديد العقوبات في حالة استعمال الوسائل الإلكترونية في ارتكاب الجريمة

أدرك المشرع الجزائري أن الاكتفاء بالنصوص العقابية الكلاسيكية لم يعد مجدياً أمام التطور النوعي لوسائل ارتكاب الجريمة، خاصة بعد أن أصبحت الوسائل التكنولوجية أداة رئيسية في الاحتيال والنصب، سواء من خلال المواقع المزيفة أو رسائل البريد الاحتيالي أو تطبيقات الدفع المزورة¹.

لذلك، جاء القانون رقم 15-20 المؤرخ في 30 ديسمبر 2015، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، ليحدث نقطة تحول في السياسة العقابية، حيث أقر ولأول مرة أن استعمال تكنولوجيا المعلومات والاتصال في ارتكاب جريمة يُعد ظرفاً مشدداً للعقوبة الأصلية².

وقد شمل هذا التعديل العديد من الجرائم من بينها النصب، التزوير، انتحال الهوية، الابتزاز، الدخول غير المشروع إلى نظم الإعلام الآلي. حيث ارتفعت العقوبة القصوى في حالات ارتكاب الجريمة عبر وسائط إلكترونية، أو عند استهداف مؤسسات أو مصالح عمومية، لتصل إلى عشر سنوات سجناً نافذاً، وهذا التوجه التشريعي يعكس تغييراً نوعياً في فلسفة التجريم والردع، حيث أصبح القانون ينظر إلى الجريمة الإلكترونية لا فقط من زاوية النتيجة، بل أيضاً من حيث طريقة التنفيذ، معتبراً الوسائل الإلكترونية عاملاً مضاعفاً للخطر الجنائي.

ولم يقتصر التشديد على الفاعل الرئيسي فحسب، بل شمل أيضاً الشريك، والمشارك، والوسيط الرقمي، حيث تم تجريم حيازة أدوات إلكترونية مُصممة خصيصاً لاختراق الأنظمة أو النصب على الغير، حتى ولو لم تُستعمل بعد، وهو ما يُعزز الطابع الوقائي للنص القانوني.

إضافة لذلك، أدرج المشرع الجزائري جرائم تحريض الفُصّر عبر الوسائط الإلكترونية، ونشر المحتويات المضللة، ضمن الأفعال المعاقب عليها، مما يؤكد شمولية هذا القانون في تغطية مختلف صور النصب والاحتيال المرتكبة عبر التكنولوجيا.

ثانياً: دعم التعاون القضائي الوطني والدولي في مكافحة الجريمة الإلكترونية

¹ القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، 2009

² قانون رقم 15-20 المؤرخ في 30 ديسمبر 2015، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، 2015.

تتميز الجرائم المعلوماتية عموماً، وجريمة النصب الإلكتروني خصوصاً، بكونها جرائم عابرة للحدود. فقد يكون الجاني في بلد، والضحية في بلد آخر، والوسيلة المستعملة (موقع إلكتروني - بريد - خوادم تخزين) في دولة ثالثة. هذه الطبيعة المركبة فرضت على السلطات الجزائرية تطوير آليات تعاون قضائي فعالة¹.

وفي هذا السياق، تشير الدراسات الأكاديمية إلى أن الجزائر انخرطت تدريجياً في آليات التعاون القضائي الرقمي، من خلال تفعيل الاتفاقيات الثنائية لتسليم المجرمين، والإنابات القضائية الدولية، وتعزيز آليات الاتصال القضائي عبر منصات إلكترونية².

فعلى الصعيد الداخلي، تم إنشاء وحدات مختصة على مستوى النيابة العامة مكلفة بمتابعة قضايا الجريمة السيبرانية، تتولى التنسيق بين مختلف الأجهزة الأمنية والقضائية، وتجميع المعلومات التقنية، والقيام بالتحقيقات اللازمة في إطار التعاون المحلي.

أما على المستوى الدولي، فتلجأ الجزائر إلى آليات المساعدة القانونية المتبادلة، خصوصاً في القضايا المعقدة التي يكون فيها مصدر الجريمة خارج التراب الوطني. ويشمل ذلك التعاون مع شركات الاتصالات الدولية ومزودي خدمات الإنترنت، لاسترجاع البيانات أو تحديد الهويات الرقمية، وهو ما سمح في العديد من الحالات بكشف شبكات نصب دولية.

كما تسترشد الجزائر بمضامين اتفاقية بودابست بشأن الجرائم السيبرانية، رغم عدم المصادقة الرسمية عليها، وتحرص على الانخراط العملي في المبادئ المنصوص عليها فيها، خاصة فيما يتعلق بتبادل المعلومات وحماية الأدلة الرقمية³.

ثانياً : تحديث الأدوات التقنية للكشف والتحري ومواكبة التحقيقات الرقمية

إدراكاً منها بأن النصوص القانونية مهما كانت صرامتها تبقى غير كافية إذا لم تُدعم بإمكانيات تقنية حديثة، سعت الجزائر إلى تعزيز قدرات الضبطية القضائية من حيث الوسائل الرقمية والبشرية.

¹ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 327.

² طارق ميهوب، "التعاون القضائي الدولي في مكافحة الجريمة السيبرانية"، مجلة الدراسات القانونية المعاصرة، جامعة باقنة، العدد 8، 2023، ص. 45.

³ Council of Europe, Convention on Cybercrime (Budapest Convention)، متاح على: www.coe.int، اطلع عليه بتاريخ: 5

ماي 2026.

وفي هذا الصدد، يوضح الباحثون أن التكوين المتخصص لفرق مكافحة الجرائم الإلكترونية أصبح ركيزة مركزية في السياسة الأمنية الجزائرية، حيث تم إدماج وحدات مكونة في تحليل البيانات الرقمية، تقنيات التتبع الرقمي، استرجاع الملفات المحذوفة، وتحديد المواقع الإلكترونية المشبوهة¹.

وتم تجهيز المخابر الأمنية ببرمجيات متقدمة لتحليل الأجهزة الإلكترونية، واختراق البيانات المحمية لغرض الإثبات الجنائي، إلى جانب استحداث نظام مركزي للأرشفة الرقمية للأدلة وتشغيلها. من جهة أخرى، تم إطلاق شراكات بين القطاعين العام والخاص، تسمح بالاستفادة من خبرات شركات التكنولوجيا والأمن السيبراني في مجال حماية الأنظمة، وتحليل الثغرات، وتكوين الخبراء المحليين.

أما في القطاع البنكي، فقد أصدر بنك الجزائر تعليمات صارمة لجميع المؤسسات المالية، تلزمها باعتماد معايير دولية لحماية المعاملات الرقمية، وتطبيق بروتوكولات تحقق معتمدة، والربط الفوري مع قاعدة بيانات مركزية لرصد أي محاولة احتيال أو تسلل للنظام البنكي وذلك لتقليص نسبة الاختراقات الرقمية، وتحسين زمن الاستجابة للحوادث، بفضل وجود نظام تحذير مبكر داخلي، وآليات تبليغ مؤتمنة للمخاطر².

ثالثا : النصوص التشريعية المتعلقة بجريمة النصب والاحتيال الإلكتروني

مع تزايد الاعتماد على الوسائط الرقمية في الحياة اليومية، أصبحت الجريمة الإلكترونية، وخاصة جريمة النصب والاحتيال عبر الإنترنت، واحدة من التحديات الكبرى التي تواجه الأنظمة القانونية الحديثة. فقد أصبحت هذه الجريمة لا تتطلب وجوداً مادياً للجاني، بل يمكن ارتكابها عن بُعد، باستخدام تطبيقات رقمية أو منصات وهمية، ما يجعلها أكثر خطورة وصعوبة في الملاحقة. في هذا السياق، تحرّك المشرع الجزائري على مراحل لمواكبة هذا التطور، حيث بدأ بمحاولات تكييف النصب الإلكتروني في إطار النصوص العامة، ثم انتقل إلى سنّ مواد عقابية خاصة، وأخيراً إلى وضع قوانين مستقلة ذات طبيعة تقنية وتنظيمية.

¹ عبد الحكيم بوشخي، التحقيق الجنائي في الجرائم الإلكترونية، دار هومة، الجزائر، 2021، ص. 122.

² بنك الجزائر، "التعليمية رقم 22/01 بشأن تأمين نظم الدفع الإلكتروني"، تاريخ الاطلاع: 24 أبريل 2026

ويُعَدُّ هذا التدرج في التقنين ضروريًا لفهم كيفية تعامل التشريع الوطني مع جريمة ذات طبيعة هجينة، تجمع بين عناصر النصب الكلاسيكي وآليات الفعل المعلوماتي، ما يفرض معالجة خاصة تستند إلى وعي قانوني بتطورات التكنولوجيا.

1- التكييف القانوني التقليدي لجريمة النصب والاحتيال الإلكتروني

قبل إدراج نصوص قانونية خاصة بالجرائم المعلوماتية وبالاخص جريمة النصب والاحتيال الإلكتروني، كان القضاء الجزائري يضطر إلى تكييف الأفعال الاحتيالية التي تتم عبر الوسائل الإلكترونية وفق المادة 372 من قانون العقوبات، التي تنص على تجريم النصب في حال استعمال طرق احتيالية، أو انتحال اسم أو صفة كاذبة بقصد الاستيلاء على مال الغير¹.

لكن النصب والاحتيال الإلكتروني، في كثير من حالاته، لا يتطلب انتحال صفة ولا يحتك بالضحية بشكل مباشر، بل يتم عبر مواقع إلكترونية مزيفة، أو تطبيقات دفع احتيالية، أو حتى رسائل بريد إلكتروني وهمية، ما يجعل انطباق مفاهيم المادة 372 محدودًا في بعض السياقات، فالنصب عبر واجهات إلكترونية لا يترك في الغالب أثرًا ماديًا أو بصمة واضحة، الأمر الذي يصعب إثبات نية التدليس أو القصد الاحتيالي بالطريقة التقليدية.

من ناحية أخرى، فإن الركن المادي في النصب الإلكتروني غالبًا ما يتم عبر وسيلة رقمية، كالإعلان عن منتج غير موجود، أو إرسال روابط كاذبة تدّعي تقديم خدمة معينة. وفي هذه الحالة، لا يكون العنصر المادي فعلاً ملموسًا كالتصرف أو اللقاء، بل يكون نقرة زر أو إدخال بيانات بنكية في موقع خادع. هذا التحول في طبيعة الوسائل يفرض على القاضي الجزائري أن يتعامل مع مفاهيم جديدة كـ"التزوير الرقمي"، و"الهوية المعلوماتية"، و"الانتحال الافتراضي"².

¹ الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

² عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، ص 69.

وبالرغم من هذه الإشكاليات، ظل التكييف وفق المادة 372 ممكناً في بعض الحالات، خاصةً إذا اقترن الفعل بواقعة كاذبة واضحة، مثل انتحال صفة وكالة رسمية أو شخصية اعتبارية معروفة، شريطة أن تكون الوسيلة الاحتيالية قابلة للإثبات قانونياً¹.

ومع ذلك، فإن الاعتماد الحصري على هذه المادة يبقى قاصراً، ويحتاج إلى دعم بنصوص حديثة تراعي الطبيعة الخاصة للجريمة.

2- التعديلات التشريعية الخاصة (الاستجابة الجزئية الأولى)

في خطوة أولى لمواجهة النصب المعلوماتي، أقر المشرع الجزائري تعديلاً مهماً بموجب الأمر رقم 06-23 المؤرخ في 20 أوت 2006، حيث أدرج فصل خاص تحت عنوان "الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات"، شمل المواد من 394 مكرر 1 إلى 394 مكرر 4، وقد جاء هذا التعديل استجابة لحاجة ملحة لتجريم أفعال لم تكن مغطاة بشكل صريح في المنظومة القانونية السابقة².

تضمنت هذه المواد ما يلي:

- **394 مكرر 1:** يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها، هذا النص يُشكل الأساس القانوني لملاحقة محاولات اختراق البريد الإلكتروني أو النظام البنكي بهدف التلاعب أو التهيئة لجريمة نصب.
- **394 مكرر 2:** تُوسّع هذه المادة نطاق التجريم لتشمل كل من يعترض أو يحوّر أو يستخدم البيانات الرقمية المملوكة للغير. وقد صيغت لتغطي التصرفات التي يتم بها سحب الأموال، أو استخدام بطاقات ائتمان عن طريق الاحتيال، وهو ما يُعد الشكل الأكثر شيوعاً للنصب الإلكتروني.

¹ سامية العايب ومنال عرابية، "الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني"، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، العدد 03، 2021، ص 229-243.

² الأمر رقم 06-23 المؤرخ في 20 أوت 2006، الجريدة الرسمية العدد 47، ص. 4.

• **394 مكرر3:** تُشدد العقوبات عند ارتكاب الفعل ضمن جماعة إجرامية أو عند العود، وهو ما يعكس وعي

المشرع بخطورة الشبكات المنظمة التي تنشط في الاحتيال الرقمي.

• **394 مكرر4:** تنص على مسؤولية الشخص المعنوي، مما يفتح الباب أمام ملاحقة الشركات والمنصات

التجارية الوهمية التي تُستعمل كواجهة للاحتيال، أو تلك التي تمتنع عمدًا عن تأمين بيانات المستخدمين¹.

من الواضح أن هذا التعديل أوجد أساسًا قانونيًا خاصًا لملاحقة صور النصب والاحتيال التي تتم عبر أنظمة رقمية، وأدخل مفاهيم جديدة في القانون الجنائي الجزائري، كالولوج غير المشروع، وتحويل البيانات، والنوايا الاحتيالية الرقمية، وعالج المشرع أيضًا نقطة كانت غائبة في النصوص التقليدية، وهي أن الجريمة قد تقع دون أن يستلم الجاني شيئًا ماديًا، بل يكفي الشروع أو الإعداد أو الدخول الاحتيالي بحد ذاته، وهو تصور حديث للجريمة يعكس تحولًا نوعيًا في فلسفة العقاب.

- القانون رقم 04-09 المؤرخ في 5 أوت 2009 - نحو تغطية شاملة للبيئة الرقمية

أدرك المشرع الجزائري أن تعديل قانون العقوبات لا يكفي وحده، فقام بإصدار القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها. هذا القانون جاء ليؤسس منظومة شاملة للوقاية من الجريمة المعلوماتية، وليس فقط معاقبتها².

ومن أهم ما نص عليه:

- تعريف نظام المعالجة الآلية للمعطيات بأنه كل بنية رقمية تقوم بمعالجة البيانات إلكترونيًا، سواء كانت مستقلة أو مرتبطة بشبكة. وقد توسّع هذا التعريف ليشمل الحواسيب، الخوادم، وحتى التطبيقات السحابية
- التأكيد على أن الاعتداء على هذا النظام يعتبر فعلاً مجرمًا بمجرد الشروع فيه، ولو لم تتحقق النتيجة، مثل إرسال فيروسات أو برمجيات خبيثة بهدف الاختراق.

¹ القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات"، المادة 394 مكرر 1.

² إيمان، بيدادي، "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية"، مجلة آفاق للبحوث والدراسات، العدد 04، 2019، ص.

- تفعيل آليات وقائية من خلال التعاون بين الجهات الأمنية، والتزامات قانونية على مزودي الخدمات، لا سيما فيما يتعلق بحماية سرية البيانات والاحتفاظ بسجلات الاتصالات الرقمية.

ويُلاحظ أن هذا القانون أرسى مبدأ التجريم الاحتياطي، أي منع الجريمة قبل وقوعها، عن طريق تشديد الرقابة على الفضاء الرقمي، وتفعيل آليات التبليغ، وهو ما يُعتبر خطوة متقدمة في مجال السياسة الجنائية الوقائية.

- القانون رقم 05-18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية

يُعتبر القانون رقم 05-18 بشأن التجارة الإلكترونية من القوانين الحديثة التي كرسها المشرع الجزائري لمواكبة التوسع في الاقتصاد الرقمي، وضبط العلاقة بين المستهلك والمورد داخل الفضاء الافتراضي. وقد جاء هذا القانون في وقت تتزايد فيه عمليات النصب والاحتيال عبر المنصات التجارية الرقمية، ما دفع إلى تبني قواعد حمائية توازن بين حرية التعاقد الإلكتروني ومبدأ الأمن القانوني

نصت المادة 16 من هذا القانون على ضرورة إعلام المستهلك بجميع البيانات المتعلقة بالخدمة أو المنتج، كالسعر ووسائل الدفع ومدة التسليم، وهو ما يُعدّ عنصراً جوهرياً لضمان الشفافية والحد من مظاهر التضليل التي قد تُستعمل وسيلةً للاحتيال¹.

أما المادة 18، فقد وضعت قيداً قانونياً صريحاً يمنع المورد من المطالبة بأي مقابل إذا لم يتم تنفيذ العقد، مما يوفر حماية فعلية للمستهلك الإلكتروني من حيث الالتزامات المالية².

وعند تحليل هذه المقتضيات في ضوء التطبيقات العملية، يتضح أن المشرع الجزائري تجاوز البُعد التنظيمي للعقد الرقمي، واتجه نحو تكريس ملامح الحماية القانونية المسبقة واللاحقة معاً. فالمستهلك، في الواقع، لا يمتلك القدرة التقنية للتحقق من صدقية كل منصة إلكترونية، مما يجعله عرضة للتغريب وسوء النية من بعض الموردين.

¹ القانون رقم 05-18 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، المادة 16.

² المادة 18، نفس المرجع.

وتُظهر الدراسات الحديثة أن العلاقة التعاقدية في بيئة التجارة الإلكترونية تتطلب إعادة صياغة تقليدية لمفهوم "الرضا الحر"، بحيث لم يعد كافيًا التعبير عن القبول إلكترونيًا، بل ينبغي أن يكون مسبوقًا بإعلام موثوق، وإطار قانوني واضح يحمي الإرادة من التلاعب، خاصة في غياب اللقاء المادي بين الطرفين¹.

هذا الفهم الحديث للعلاقة التعاقدية هو ما حاول القانون 05-18 تبنيه ضمنيًا، ليمنح المستهلك الإلكتروني إطارًا قانونيًا لا يقل حماية عن نظيره التقليدي، بل قد يكون أشد ضرورة بالنظر لطبيعة المخاطر الرقمية المستحدثة.

2- الإطار الإجرائي والاختصاص القضائي في الجرائم الإلكترونية

تُعد الجرائم الإلكترونية من بين الجرائم المستحدثة التي فرضت نفسها على المنظومة القانونية التقليدية، خاصة في بعدها الإجرائي، نظرًا لطبيعتها اللامادية، وسرعة تنفيذها، وامتدادها العابر للحدود، وهو ما أفرز تحديات حقيقية

أمام أجهزة التحري والتحقيق والنيابة، تتعلق بتحريك الدعوى العمومية، وتحديد المحكمة المختصة، وتنظيم عمل الجهات المتدخلة.

واستجابة لهذه الإشكالات، تدخل المشرع الجزائري بتعديلات على قانون الإجراءات الجزائية من خلال القانون 14-06، حيث تم توسيع قواعد الاختصاص المحلي، لا سيما في المادة 329، التي أتاحت للمحاكم النظر في قضايا الجرائم المعلوماتية حتى وإن كانت الأفعال أو نتائجها واقعة خارج دائرة الاختصاص الجغرافي التقليدي، ويعتبر هذا التعديل منطقيًا بالنظر إلى طبيعة هذه الجرائم التي غالبًا ما يتم تنفيذها عن بُعد، أو انطلاقًا من خارج الإقليم الوطني، بينما يقع أثرها داخل الدولة².

كما تم إسناد صلاحيات التحقيق والمتابعة إلى القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الذي أنشئ خصيصًا لهذا النوع من الجرائم، حيث يتمتع هذا القطب باختصاص وطني

¹ حمزة، هبة. "الآليات القانونية لحماية المستهلك الإلكتروني وفق القانون رقم 05/18 المتعلق بالتجارة الإلكترونية"، مجلة القانون الدولي والتنمية، المجلد 8، العدد 1، 2020، ص. 197.

² القانون رقم 15-02 المؤرخ في 23 يوليو 2015، المتضمن تعديل وتنظيم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 40، لسنة 2015.

شامل، ويمكن لوكيل الجمهورية التابع له مباشرة الدعوى العمومية دون التقيد بالإقليم الترابي ومن جهة أخرى، أقر المشرع في المادة 98 مكرر 3 من نفس القانون إمكانية طلب النائب العام لهذا القطب استرداد ملف أي قضية من قضايا الجرائم الإلكترونية من الجهات المحلية، إذا تبين أن موضوعها يدخل ضمن اختصاصه النوعي، مما يُمكن من توحيد الإجراءات وتقادي تضارب القرارات القضائية¹.

كما يُلاحظ أن المشرع حاول تكييف الإجراءات الجنائية مع البيئة الرقمية من خلال السماح بتقنيات تفتيش خاصة، وحجز المعطيات المخزنة في الوسائط الإلكترونية، والتصريح باستخدام برامج تتبع البيانات، غير أن هذه الترتيبات تصطدم في الواقع بصعوبات تطبيقية أبرزها محدودية التكوين التقني لأعوان الضبط، ونقص الموارد البشرية المؤهلة، إضافة إلى الضعف في البنية التكنولوجية لبعض الجهات القضائية².

3- التعدد النصي وتحديات التكييف جريمة النصب و الاحتيال الإلكتروني في التشريع الجزائري

يمثل التعدد النصي في التشريع الجزائري إحدى أبرز الإشكاليات عند تكييف جريمة النصب والاحتيال الإلكتروني، حيث تتداخل النصوص العامة والخاصة مما يصعب على القاضي تحديد القاعدة القانونية الواجبة التطبيق فالمادة 372 من قانون العقوبات تجرم النصب الكلاسيكي، بينما المواد من 394 مكرر إلى 394 مكرر 7، التي أُدرجت بموجب القانون 04-15، تنظم أفعالاً مرتبطة بالجرائم المعلوماتية من قبيل الدخول غير المشروع إلى الأنظمة وتزوير البيانات الرقمية، وهذا التداخل في النصوص يؤدي إلى تفاوت في تكييف نفس الوقائع من جهة قضائية لأخرى، إذ تعتبر بعض المحاكم أن الفعل يدخل في إطار النصب التقليدي، بينما تراه جهات أخرى جريمة معلوماتية خاضعة لنصوص خاصة. ويرجع ذلك جزئياً إلى غياب معيار واضح للفصل بين الجريمتين، خاصة عندما تستعمل الحيلة عبر وسائط إلكترونية كالمواقع المزيفة أو انتحال الهوية الرقمية³.

¹ بوسماط، حبيب. "جريمة النصب باستعمال الوسائل المعلوماتية"، مذكرة ماستر، جامعة عبد الحميد بن باديس مستغانم، 2019، ص. 85.

² المرجع السابق، ص. 86.

³ سويسبي فتيحة، "التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها"، مداخلة في ندوة بحثية من تنظيم مركز البحوث القانونية والقضائية، وزارة العدل الجزائرية، 18 جانفي 2022، ص 6-7.

تُبرز الدراسات الحديثة أن الوسائل التقنية المستخدمة في النصب الإلكتروني تختلف جوهرياً عن الوسائل التقليدية، ما يجعل إخضاعها لنص المادة 372 أمراً غير دقيق قانوناً، فهذه الأفعال ترتكب عبر بيئة رقمية لا تركز على الحضور المادي للجاني، بل على التحكم في المعلومات واستغلال ثغرات تقنية، وهذا ما يُدخل الركن المادي للجريمة في منطقة رمادية يصعب ضبطها ضمن مفاهيم القانون التقليدي¹.

تُعد إشكالات الإثبات من أبرز العوائق المرتبطة بتكييف النصب الإلكتروني، حيث يُلاحظ اعتماد الجناة على أدوات تموية رقمية معقدة، مثل استخدام هويات مزيفة، واستضافة المواقع خارج الجزائر، وتشفير البيانات. هذه الخصائص تجعل إثبات الركن المادي أو القصد الاحتيالي مرهوناً بتقنيات تحقيق رقمية متخصصة قد لا تكون متوفرة أو مألوفة لجميع الجهات القضائية².

فمن خلال ماسبق وبعض البحوث القانونية يتأكد بضرورة تدخل تشريعي جزائري صريح ينص على جريمة النصب الإلكتروني باعتبارها جريمة مستقلة، مع تحديد عناصرها ومجال تطبيقها، وتفايدي التضارب بين النصوص، ومثل هذا التدخل من شأنه أن يُسهّل عملية التكييف ويوحّد المعاملة الجزائية، خصوصاً في ظل تسارع وتيرة استخدام الوسائل الإلكترونية في المعاملات المالية والاجتماعية.

رابعا : العقوبات المقررة لجريمة النصب والاحتيال الإلكتروني في قانون العقوبات الجزائري

ينص قانون العقوبات الجزائري على مجموعة من العقوبات التي تطل مرتكب جريمة النصب والاحتيال، والتي تختلف باختلاف نوعها بين أصلية، تكميلية، وإضافية. وتُظهر هذه العقوبات مدى جدية المشرع في التصدي لهذا النوع من الجرائم، خصوصاً في السياق الإلكتروني الذي اتسع فيه مجال ارتكاب الأفعال الاحتيالية، مما يستدعي جزاءً رادعاً ومتكيفاً مع خطورة هذه الأفعال.

¹ شاين نوال، "الجريمة الإلكترونية في التشريع الجزائري - ماهيتها، موضوعها، خصائصها، ومظاهر تحدياتها"، مجلة سوسيوولوجيا، العدد 10، 2022، ص 202.

² سويسبي فتحة ، المرجع السابق، ص 8.

1- العقوبات الأصلية

تُعد العقوبات الأصلية من أهم الوسائل الجزائية التي يعتمد عليها المشرع لمواجهة جريمة النصب والاحتيال، خاصة إذا تعلّق الأمر بوقائع احتيالية موجّهة إلى جمهور واسع عبر الإنترنت. فقد نصت المادة 2/372 من قانون العقوبات على إمكانية تشديد العقوبة الأصلية إذا وُجد ظرف مشدد يتمثل في كون الجريمة قد وُجّهت إلى الجمهور بغرض إصدار أسهم أو سندات أو أدوات مالية، أو إنشاء شركات صناعية أو تجارية، إذ ترفع العقوبة إلى السجن لمدة تصل إلى عشر سنوات وغرامة تصل إلى 200.000 دج¹.

تعتبر هذه العقوبات تعبيرًا عن توجه تشريعي يقوم على فكرة الردع العام والخاص، ويهدف إلى حماية النظام الاقتصادي والاجتماعي من اختراقات رقمية قد تؤدي إلى خسائر فادحة سواء للأفراد أو للدولة. وفي هذا السياق، فإن العقوبات الأصلية تتناسب طرديًا مع جسامة الضرر الذي قد ينجم عن أفعال النصب والاحتيال، خاصة في ظل توسع منصات التواصل الاجتماعي، وانتشار تطبيقات الدفع الإلكتروني.

علاوة على ذلك، فإن المشرع الجزائري أخذ بعين الاعتبار حالات التعدد المعنوي للجرائم، حيث تُرتكب عدة أفعال احتيالية باستخدام وسيلة واحدة أو سلسلة مترابطة من الأفعال. وفي مثل هذه الحالات، فإن القاضي يملك صلاحية ضم العقوبات أو تشديدها حسب ما تقتضيه خطورة الفعل وتكراره.

2- العقوبات التكميلية

لم يكتف المشرع بالعقوبات الأصلية، بل أقرّ أيضًا بعقوبات تكميلية تهدف إلى تضيق نطاق النشاط الإجرامي المستقبلي للجاني. ومن بين أبرز هذه العقوبات تلك المقررة في المواد 372 و 382 من قانون العقوبات

¹ المادة 53 مكررة، 4 القانون رقم 22-06 المؤرخ 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006. يعدل ويتمم الأمر رقم 155-66 المؤرخ في 18 صفر 1386 الموافق 8 جران 1966 والمتضمن قانون الاجراءات الجزائية، جريدة رسمية رقم 84/2006.

فقد نصت المادة 372، فقرة 3 من قانون العقوبات على أن القاضي يمكنه أن يحكم على الجاني بعقوبات إضافية ذات طابع تقييدي أو حرمان، تمس بعض الحقوق المدنية أو السياسية، كلما ثبت أن الفعل المرتكب ينطوي على درجة من الخطورة تستدعي مثل هذه التدابير¹.

ومنح القانون للقضاء سلطة تقرير هذه العقوبات، وفق تقديره الشخصي للوقائع، خاصة إذا كان الجاني قد استغل مركزاً وظيفياً، أو مهنة ترتبط بالثقة العامة، أو لجأ إلى وسائل تدليس متقنة للإيقاع بالضحايا. وتشمل هذه العقوبات الحرمان من الحقوق الواردة في المادة 14 من قانون العقوبات، سواء بصفة كلية أو جزئية، ومن بينها:

- الإقصاء من الوظائف العامة والمناصب العليا داخل أجهزة الدولة أو الهيئات السياسية.
- سحب الحقوق الانتخابية والمدنية، كمنع الترشح أو التصويت أو حمل الأوسمة الرسمية.
- المنع من ممارسة المهام القضائية والمساعدة القانونية، كأن يُمنع من الشهادة، أو أداء مهام الخبرة أو الدفاع، باستثناء الحالات التي يكون فيها شاهداً استدلالياً فقط.
- سحب الأهلية القانونية للوصاية أو النيابة الشرعية، خصوصاً إذا لم يكن الجاني ولياً طبيعياً على أبنائه.
- الحرمان من التدريس أو النشاط التربوي، سواء داخل المؤسسات التعليمية أو الإدارية، أو حتى الإشراف البيداغوجي في المدارس أو مراكز التكوين.

وفي هذا السياق، تنص المادة 382 مكرر من قانون العقوبات على تشديد العقوبة على مرتكبي النصب في حال تكرار الجريمة أو إذا تم ارتكابها باستعمال وسائل التدليس التي توهم الضحية بوجود صفة قانونية، وظيفية، أو اجتماعية غير حقيقية، سواء تم ذلك باسم الجاني نفسه أو بصفة مستعارة أو بواسطة الغير².

¹ عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري - القسم الخاص، دار هومة للطباعة والنشر، الجزائر، 1989، ص 32.
² الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المادة 382 مكرر..

المطلب الثالث: الجهود الوطنية في مواجهة النصب والاحتيال الإلكتروني

سعت الجزائر إلى تبني مجموعة من الجهود الأمنية والقضائية والتقنية لمواجهة جرائم النصب والاحتيال الإلكتروني، وذلك في إطار سياسة وطنية تهدف إلى التكيف مع التطور السريع للإجرام الرقمي. وقد شملت هذه الجهود عدة قطاعات ومؤسسات تعمل بشكل تكاملي للحد من خطورة هذه الجرائم.

لمواجهة تحدي بروز أساليب نصب واحتيال الكتروني جديدة مستحدثة يتطلب مقاربة أمنية وقضائية جديدة ، حيث سارعت الدولة الجزائرية إلى تعبئة أجهزتها، إلى جانب الفاعلين في القطاع المالي والمصرفي، من أجل وضع آليات ردع ووقاية تتماشى مع طابع الجريمة المعلوماتية. ويُلاحظ أن هذه الجهود الوطنية توزعت على ثلاثة فروع رئيسية الشرطة (الفرع الأول) ، القضاء (الفرع الثاني) ، والمؤسسات البنكية (الفرع الثالث) .

الفرع الأول : جهود الشرطة في مكافحة النصب والاحتيال الإلكتروني

تُعتبر المصالح الأمنية من أبرز الجهات المكلفة بمواجهة الجرائم الإلكترونية، حيث تعمل على رصد الأفعال الإجرامية وتتبع مرتكبيها باستعمال وسائل تقنية حديثة. وقد أولت الشرطة الجزائرية أهمية متزايدة لمكافحة النصب الإلكتروني من خلال إنشاء فرق متخصصة وتطوير وسائل التحري الرقمي.

تعد الشرطة الجزائرية ممثلة في المديرية العامة للأمن الوطني، أول جبهة أمامية في مواجهة الجرائم الإلكترونية عموماً، وجريمة النصب والاحتيال الإلكتروني على وجه الخصوص. وقد عرفت المنظومة الأمنية تحديثاً تدريجياً منذ مطلع الألفية، من خلال إنشاء فرق متخصصة في مكافحة الجرائم السيبرانية داخل مصالح الشرطة القضائية.

وقد أنيط بهذه الفرق دور مزدوج: أولاً، رصد وتتبع الجرائم الإلكترونية من خلال التقنيات الحديثة لتحليل عناوين الIP، والولوج المشروع إلى الأجهزة المصابة أو المختزقة. وثانياً، استقبال شكاوى المواطنين والضحايا عبر منصات إلكترونية مخصصة، مثل منصة التبليغ التابعة لموقع المديرية العامة للأمن الوطني¹.

¹ عبد الحكيم بوشیخي، الجريمة الإلكترونية والشرطة العلمية، دار هومة، الجزائر، 2021، ص. 115.

يُضاف إلى ذلك اعتماد الشرطة على تقنيات " التحقيق المفتوح المصدر " OSINT، التي تسمح بجمع المعلومات من الفضاء العام للإنترنت، وتحليل نشاطات المستخدمين المشتبه فيهم، مما يُمكن من تفكيك الشبكات الإجرامية حتى في غياب شكوى مباشرة من الضحية.

وتجدر الإشارة إلى أن تطور مهارات أعوان الشرطة في مجال التحليل الرقمي جاء نتيجة برامج تكوين وتدريب متخصصة على المستوى الوطني والدولي، بالتنسيق مع هيئات مثل الإنتربول ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، كما أن الشرطة الجزائرية بدأت تعتمد على التعاون المؤسساتي الداخلي، مثل التنسيق بين الأمن الوطني والدرك الوطني، وبين الشرطة والمصالح المختصة بالبريد والمواصلات، لوقف عمليات الاحتيال التي تمر عبر بوابات الدفع أو تحويل الأموال.

والأهم من ذلك، هو أن الجهود الأمنية لم تقتصر على الملاحقة فقط، بل شملت أيضًا البعد الوقائي، من خلال حملات التوعية الموجهة إلى فئة الشباب خاصة، عبر مواقع التواصل الاجتماعي، والإذاعة والتلفزيون العموميين، حيث حذرت السلطات من أساليب التحايل الشائعة، مثل الرسائل الوهمية، صفحات البيع الزائف، أو المواقع المزورة.

الفرع الثاني : دور القضاء في التصدي لمرتكبي الجريمة

يضطلع القضاء بدور أساسي في مكافحة جرائم النصب والاحتيال الإلكتروني، من خلال تكييف الأفعال الإجرامية وتطبيق النصوص القانونية المناسبة عليها، إضافة إلى ضمان حماية حقوق الضحايا وتحقيق الردع القانوني للجناة في إطار احترام قواعد المحاكمة العادلة.

يشكل القضاء الحلقة الأهم في مسار مكافحة الجريمة الإلكترونية، من حيث تكييف الوقائع، إثبات الأفعال، إصدار الأحكام، وتنفيذ العقوبات. وقد عرفت المنظومة القضائية الجزائرية تطورًا واضحًا في هذا المجال، لا سيما بعد صدور الأمر رقم 04-09 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹.

هذا النص التشريعي الهام جاء ليغطي فراغًا قانونيًا كان واضحًا، إذ لم تكن النصوص التقليدية مثل قانون العقوبات كافية لتجريم أفعال النصب الإلكتروني بشكل واضح، خصوصًا حين يتعلق الأمر بالتحايل على أنظمة إلكترونية أو انتحال هوية رقمية.

¹ الأمر رقم 04-09 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 50، 2009.

ومن التطبيقات القضائية التي أثبتت فعالية القضاء في هذا المجال، اعتماد المحاكم على الخبرة التقنية بشكل رسمي، حيث يتم تعيين خبراء معتمدين في مجال الإعلام الآلي لتحليل الأجهزة، المواقع، المعاملات الرقمية، والرسائل الإلكترونية.

كما أن الإثبات الإلكتروني بدأ يفرض نفسه بقوة في ساحة القضاء، حيث تقبل المحاكم، وفقاً لقواعد قانون الإجراءات الجزائية، نسخاً إلكترونية من رسائل، إيصالات إلكترونية، أو سجلات رقمية كأدلة إذا كانت محفوظة بطريقة موثوقة وغير قابلة للتزوير. وقد ظهرت قرارات قضائية تتبنى هذا التوجه، ما يعكس مرونة الجهاز القضائي وتطوره في التعامل مع معطيات العصر الرقمي.

على مستوى النيابة العامة، يلاحظ أن وكلاء الجمهورية باتوا أكثر اطلاعاً على خصائص الجريمة الرقمية، من خلال مساهمتهم في فتح تحقيقات استناداً إلى بلاغات إلكترونية، أو تقارير من خلية الاستعلام المالي أو وحدات التحري، مما ساهم في سرعة المتابعة القضائية وتقليص زمن الاستجابة¹. وتجدر الإشارة إلى أن التعاون القضائي الدولي أخذ حيزاً مهماً في بعض القضايا المعقدة التي يكون فيها الفاعل خارج التراب الوطني، أو حين يتم استخدام مواقع أجنبية كوسيلة للنصب على المواطنين الجزائريين.

الفرع الثالث : مساهمة القطاع البنكي في الحد من الجريمة

نظراً لارتباط جرائم النصب الإلكتروني غالباً بالمعاملات المالية والتحويلات الرقمية، أصبح القطاع البنكي شريكاً أساسياً في جهود مكافحة، من خلال تطوير أنظمة الحماية الإلكترونية وتعزيز إجراءات الرقابة والتوعية الموجهة للزبائن فمن الضروري إشراك هذا القطاع الحيوي في منظومة المكافحة. ويمكن حصر مساهمات القطاع البنكي في الجزائر في ثلاث مستويات:

أولاً : الحماية التقنية

أصبحت البنوك الجزائرية، وخاصة العمومية منها، تعتمد على أنظمة معلوماتية محمية بواسطة تقنيات التشفير المتقدمة. كما تم إدماج أنظمة المصادقة الثنائية (مثل إرسال رمز سري للهاتف) في عمليات الدفع الإلكتروني، تقادياً لأي استعمال غير مشروع لحسابات الزبائن².

¹ أحسن بوسقيعة – مرجع سابق ، ص 106

² رابح علاوي، الأمن السيبراني في المؤسسات المصرفية، دار الكتاب الحديث، الجزائر، 2022، ص. 88.

وتقوم المؤسسات المصرفية، بتوجيه من بنك الجزائر، بتحديث دوري لخوادمها وقواعد بياناتها، وتحليل محاولات الدخول غير المصرح بها، وتطبيق إجراءات عزل فوري للحسابات المشكوك في اختراقها.

ثانيا : التبليغ والرقابة

بموجب تعليمات تنظيمية صادرة عن بنك الجزائر، تُلزم البنوك بإعلام السلطات المختصة فوراً بأي عملية مشبوهة أو نشاط مالي غير معتاد، خاصة في المعاملات الإلكترونية العابرة للحدود أو التي لا تتطابق مع الملف الشخصي للزبون¹.

كما تقوم البنوك بتطبيق مبدأ "اعرف زبونك" KYC، الذي يقتضي جمع بيانات دقيقة عن الهوية، مصدر الدخل، وطبيعة النشاط المالي، كشرط أساسي لفتح الحساب أو تفعيله إلكترونياً.

ثالثا : التوعية والتحسيس

أطلقت عدة بنوك جزائرية حملات توعية عبر رسائل نصية قصيرة، وعلى مواقعها الإلكترونية، تحذر فيها الزبائن من مخاطر إفشاء المعلومات البنكية، والضغط على الروابط المشبوهة، واستعمال شبكات Wi-Fi العامة عند القيام بمعاملات إلكترونية².

وقد ساهمت هذه الحملات، المدعومة من بنك الجزائر، في تعزيز الثقافة الرقمية البنكية لدى المواطن، ما انعكس إيجاباً على تقليص عدد الضحايا من جهة، وتحسين سمعة القطاع المصرفي من جهة أخرى.

¹ بنك الجزائر، "التعليمية رقم 22/05 بشأن مكافحة الجرائم المالية"، www.bank-of-algeria.dz، تاريخ الاطلاع: 20 افريل 2026.

² الموقع الرسمي للمديرية العامة للأمن الوطني www.algeriepolice.dz : تاريخ الاطلاع: 3 ماي 2026.

ملخص الفصل الثاني:

يتناول هذا الفصل جريمة النصب والاحتيال الإلكتروني من زاويتين أساسيتين: الإطار القانوني وآليات المكافحة. فقد أبرز أن هذه الجريمة ظهرت نتيجة التطور الرقمي واعتماد المعاملات الحديثة على الوسائط الإلكترونية، مما جعلها أكثر تعقيداً وخطورة بسبب اعتمادها على الخداع عبر تقنيات رقمية مثل التصيد الإلكتروني، المواقع المزيفة، وانتحال الهوية.

ومن الناحية القانونية، أوضح الفصل أن المشرع الجزائري لم يفرد نصاً خاصاً بالنصب الإلكتروني، بل اعتمد على المادة 372 من قانون العقوبات لتجريم أفعال الاحتيال التقليدي، مع إمكانية تطبيقها على الجرائم الإلكترونية، إلى جانب نصوص مكملة في قانون تكنولوجيات الإعلام والاتصال، وحماية المعطيات الشخصية، والتجارة الإلكترونية. وهذا التداخل بين النصوص خلق نوعاً من الصعوبة في التكييف القانوني.

كما بين الفصل أن الجريمة تقوم على أركانها الثلاثة: ركن شرعي يستند إلى النصوص القانونية، وركن مادي يتمثل في السلوك الاحتيالي الرقمي وما يترتب عنه من ضرر وعلاقة سببية، وركن معنوي يقوم على القصد الجنائي الذي يصعب إثباته في البيئة الرقمية بسبب استخدام وسائل تمويه وإخفاء متطورة.

وعلى مستوى الإجراءات، فإن تحريك الدعوى العمومية غالباً ما يرتبط بشكوى من الضحية، نظراً لكون الجريمة تُرتكب في فضاء رقمي يصعب اكتشافه تلقائياً، كما تواجه الجهات القضائية تحديات كبيرة تتعلق بإثبات الأدلة الرقمية وتتبع الجناة خاصة في حال وجود عناصر خارج الإقليم الوطني.

أما في جانب المكافحة، فقد اعتمدت الجزائر على مقاربة متعددة الأبعاد تشمل الوقاية عبر التوعية الرقمية، وتعزيز الأمن السيبراني، وتفعيل دور الإعلام، إضافة إلى جهود الشرطة المتخصصة والقضاء والقطاع البنكي. كما تم تدعيم المنظومة القانونية بعقوبات مشددة، وتوسيع التعاون القضائي الداخلي والدولي، وتحديث الأدوات التقنية للتحقيق.

ويخلص الفصل إلى أن مواجهة هذا النوع من الجرائم لا يمكن أن تعتمد على القانون فقط، بل تتطلب تكاملاً بين التشريع، والوسائل التقنية، والوعي المجتمعي، لضمان فعالية الحماية من الاحتيال الإلكتروني.

خاتمة:

خاتمة :

جريمة النصب والإحتيال من الجرائم الموصوفة المتعلقة بالتعدي على الأموال، ويتضح أنها من أخطر صور الإجرام الحديث، حيث نظمها المشرع إلى جانب العديد من الجرائم كالسرقة وخيانة الأمانة وإصدار الشيك بدون رصيد، نظرا لإرتباطها بالتطور التكنولوجي وسهولة إرتكابها عبر الفضاء الرقمي، مما يصعب من عملية كشفها وتتبع مرتكبيها. وقد سعى المشرع الجزائري إلى مواكبة هذه التحولات من خلال سن نصوص قانونية تجرم مختلف صور الإحتيال الإلكتروني وتقر عقوبات دارة خاصة في إطار قانون العقوبات والقوانين الخاصة بمكافحة الجرائم المعلوماتية، أو رغم الجهود التشريعية المبذولة إلا أن فعالية مكافحة هذه الجريمة تبقى مرهونة بمدى تطوير الوسائل التقنية والبشرية وتعزيز التعاون الدولي ونشر الوعي الرقمي لدى الأفراد والمؤسسات بإعتباره خط دفاع أولي للوقاية من الوقوع في مثل هذه الجرائم، وعليه فإن التصدي لجريمة النصب والإحتيال الإلكتروني لا يقتصر فقط على الجانب القانوني، بل يتطلب مقاربة شاملة تجمع بين التشريع الفعال والتوعية المجتمعية، بما يضمن حماية المعاملات الإلكترونية وتعزيز الثقة في البيئة الرقمية داخل الجزائر.

ومن خلال دراستنا لموضوعها نستنتج أن:

- جريمة النصب والإحتيال لا يمكن أن تقوم إلا بتوفر كافة الشروط والأركان فإذا غاب ركن لا يجوز أن تحرك الدعوى العمومية خاصة مايتعلق بالعلاقة السببية.
- الإحتيال هو الوسيلة الأساسية في النصب لأن المحتال يكون على دراية تامة بأموال الضحية وطريقة الوصول 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 إتساع ظاهرة النصب والإحتيال الإلكتروني.

وعليه نرى تقديم بعض المقترحات:

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

- إعداد حملات تحسيسية بطرق حديثة فعالة غير كلاسيكية كالإستعانة بمشاهير مواقع التواصل الإجتماعي وناس ذات صوت مسموع في مختلف المنصات لرفع الوعي المجتمعي بمخاطر النصب والإحتيال الإلكتروني وطرق الوقاية منه.
- نرجوا من المشرع إعادة النظر في المادة 372 من قانون العقوبات، وهذا بتقسيم الجرائم المتعلقة بالأموال كل جريمة يخصص لها مادة منفردة.

قائمة المصادر

والمراجع:

قائمة المصادر والمراجع

أولاً: المصادر

1- النصوص القانونية

الأوامر

- الأمر رقم 66-155 (ملغى) المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم 2025.
- الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم .
- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات .
- الأمر رقم 06-23 المؤرخ في 20 أوت 2006، الجريدة الرسمية، العدد 47 .

القوانين

- القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .
- القانون رقم 15-02 المؤرخ في 23 يوليو 2015، المتضمن تعديل وتنظيم قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 40، 2015.
- القانون رقم 15-20 (ملغى) المؤرخ في 30 ديسمبر 2015، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، 2015 .
- القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 27 .
- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية .

ثانيًا: المراجع

أ- الكتب العربية

- أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الثاني، دار هومة، الجزائر، 2021 .
- أحمد فتحي سرور، الوسيط في قانون العقوبات: القسم العام، دار النهضة العربية، القاهرة، 2008 .
- أحمد محمد عبد الرؤوف المنيفي، الاحتيال الإلكتروني وحكمه في الإسلام والقوانين المعاصرة، مكتبة نور، 2021 .
- رابح علاوي، الأمن السيبراني في المؤسسات المصرفية، دار الكتاب الحديث، الجزائر، 2022 .
- سامي الشريف، الجرائم المعلوماتية وإثباتها الإلكتروني، دار النهضة العربية، القاهرة، 2021 .
- سفيان صوان، الجريمة الإلكترونية في التشريع الجزائري: دراسة مقارنة، دار الهدى، الجزائر، 2020 .
- عبد الحميد بوشوشة، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2019 .
- عبد الحكيم بوشيخي، الجريمة الإلكترونية والشرطة العلمية، دار هومة، الجزائر، 2021 .
- عبد الحكيم بوشيخي، التحقيق الجنائي في الجرائم الإلكترونية، دار هومة، الجزائر، 2021 .
- عبد الله سليمان، شرح قانون العقوبات - القسم العام، ديوان المطبوعات الجامعية، الجزائر .
- عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري - القسم الخاص، دار هومة للطباعة والنشر، الجزائر، 1989 .
- عبد الفتاح بيومي حجازي، الجرائم الإلكترونية والإنترنت: دراسة قانونية مقارنة، دار الفكر الجامعي، الإسكندرية، 2011 .
- عبد الفتاح بيومي حجازي، الجرائم الإلكترونية وحماية الحقوق الشخصية، دار الفكر الجامعي، الإسكندرية، 2019 .
- محمد حسين منصور، المسؤولية الجنائية عن جرائم النشر الإلكتروني، دار الجامعة الجديدة، 2020 .
- محمد صبحي نجم، شرح قانون العقوبات - الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2020 .

- محمد عبد الفتاح عبد الباقي، جرائم الحاسوب والإنترنت في القانون المقارن، دار النهضة العربية، القاهرة، 2017 .
- وليد عبد الحي الشرفات، الجرائم الإلكترونية: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2020 .

ب- الكتب الأجنبية

- Christopher Hadnagy, Social Engineering: The Art of Human Hacking, Wiley Publishing, 2011.
- Dorothy E. Denning, Information Warfare and Security, Addison-Wesley, USA, 1999.
- Mark Button and Cassandra Cross, Cyber Frauds, Scams and their Victims, Routledge, 2017.
- Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012.
- Prashant Mali, Text Book of Cyber Crime and Penalties [As per ITA A 2008 and IPC], Draft Version, Cyber Law Consulting.
- Priyanka Tomar and Sanjay Gautam, Cybercrime and Preventive Measures, BPB Publications, 2021.
- Rick D. Howard, Cyber Fraud: Tactics, Techniques, and Procedures, CRC Press, 2009.

ثالثاً: الأطروحات والمذكرات الجامعية

- أمال دبز، جريمة النصب والاحتيال في مجال الأعمال، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة .

- بن دريس مريم، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس، مستغانم، 2019 .
- بوسماط حبيب، جريمة النصب باستعمال الوسائل المعلوماتية، مذكرة ماستر، جامعة عبد الحميد بن باديس، مستغانم، 2019 .
- حليلة زرق الرقبة، جرائم النصب والاحتيال عبر وسائل التكنولوجيا الحديثة: دراسة مقارنة بين الفقه الإسلامي وقانون العقوبات الجزائري، مذكرة ماستر، جامعة غرداية، 2021 .
- طرطاق خولة، جودي سارة، النصب والاحتيال الإلكتروني في الفقه الإسلامي والقانون الجزائري: دراسة مقارنة، مذكرة ماستر، جامعة محمد بوضياف، المسيلة، 2025 .
- صرا ندية، جريمة النصب والاحتيال عبر مواقع التواصل الإلكتروني، مذكرة ماستر، جامعة غرداية، 2023 .
- محمد جباوي منير وبولشين خليل، خصوصية أركان الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2023 .

رابعاً: المقالات العلمية

- “A Review of Online Scams and Financial Frauds in the Digital Age”, Amos Kipngetich, مجلة GSC Advanced Research and Reviews، 2025 .
- Apsimet, N., Smanova, A., & Utegenova, G., “The Role of the Internet in the Evolution of Fraud”, Bulletin of L.N. Gumilyov ENU، 2024 .
- حسن كليبي، نجمة الطبيب، “جريمة النصب الإلكتروني من منظور المشرع الجزائري”، مجلة المفكر، المجلد 20، العدد 01، 2025 .
- حياة هراكي، “واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية”، مجلة التغيير الاجتماعي، جامعة بسكرة، المجلد 08، العدد 02، 2023 .
- حمزة هبة، “الآليات القانونية لحماية المستهلك الإلكتروني وفق القانون رقم 18-05 المتعلق بالتجارة الإلكترونية”، مجلة القانون الدولي والتنمية، المجلد 08، العدد 01، 2020 .

- إيمان ببيادي، "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية"، مجلة آفاق للبحوث والدراسات، العدد 04، 2019 .
- شيخ عبد الصديق، "الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04"، مجلة معالم للدراسات القانونية والسياسية، المجلد 04، العدد 01، 2020 .
- شاين نوال، "الجريمة الإلكترونية في التشريع الجزائري - ماهيتها، موضوعها، خصائصها، ومظاهر تحدياتها"، مجلة سوسيولوجيا، العدد 10، 2022 .
- شهيرة بولحية، دنيا زاد سويح، "الاحتيال الإلكتروني"، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس بريكة، العدد 04، ديسمبر 2019 .
- سامية العايب، منال عرابة، "الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني"، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، العدد 03، 2021 .
- طارق ميهوب، "التعاون القضائي الدولي في مكافحة الجريمة السيبرانية"، مجلة الدراسات القانونية المعاصرة، جامعة باتنة، العدد 08، 2023 .
- عبد القادر بن عبد الله آل معبر، "جريمة الانتحال الإلكتروني: دراسة مقارنة بين الفقه الإسلامي والنظام السعودي"، المجلة الدولية للبحوث القانونية، العدد 09 .
- لموشي جهيدة، "دور الضحية في حدوث جريمة النصب والاحتيال - مقارنة سوسيولوجية"، مجلة العلوم الاجتماعية والإنسانية، العدد 15، 2025 .
- Vestnik ،N. Krasovskaya and A.A. Gulyaev, "On the Issue of Cyber Fraud" Udmurtskogo Universiteta ، 2022 .
- ArXiv ،Rekouche, K., "Early Phishing" ، 2011 .
- Shete, N. L., Maddel, M. M., & Shaikh, Z., "A Comparative Analysis of Cybersecurity Scams" ، IEEE I2CT Conference ، 2024 .
- Legal rules for preventing and combating cyber crimes in Algerian legislation ، مجلة العلوم الإنسانية، جامعة قسنطينة 1 .

خامسًا: المداخلات العلمية

- سويسسي فتيحة، “التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها”، مداخلات مقدمة ضمن ندوة بحثية من تنظيم مركز البحوث القانونية والقضائية، وزارة العدل الجزائرية، 18 جانفي 2022 .

سادسًا: المواقع الإلكترونية

- بنك الجزائر، “التعليمية رقم 22/01 بشأن تأمين نظم الدفع الإلكتروني”، الموقع الرسمي لبنك الجزائر، تاريخ الاطلاع: 24 أفريل 2026 .
- بنك الجزائر، “التعليمية رقم 22/05 بشأن مكافحة الجرائم المالية”، الموقع الرسمي لبنك الجزائر، تاريخ الاطلاع: 20 أفريل 2026 .
- Council of Europe, Convention on Cybercrime (Budapest Convention)، الموقع الرسمي لمجلس أوروبا، تاريخ الاطلاع: 05 ماي 2026 .
- CSIDE، “Over 150K Websites Hit by Full-Page Hijack Linking to Chinese Gambling Sites”، منشور بتاريخ 23 فيفري 2025، تاريخ الاطلاع: 27 أفريل 2025 .
- The Verge، “Ziff Davis sues OpenAI for allegedly using IGN, CNET, and PCMag content to train AI models”، منشور بتاريخ 24 أفريل 2025، تاريخ الاطلاع: 27 أفريل 2025 .
- الموقع الرسمي للمديرية العامة للأمن الوطني الجزائرية، تاريخ الاطلاع: 03 ماي 2026.

