



الرقم التسلسلي:.....

مذكرة بعنوان:

جرائم النصب عبر الوسائط الرقمية في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون أعمال

إعداد الطالبة: إشراف الأستاذ:

• بن عمار فطيمة الزهرة / الدكتور / بوسنة زهر الدين

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
د. مدار توفيق	استاذ محاضر ب	جامعة الشاذلي بن جديد - الطارف	رئيسا
د. بوسنة زهر الدين	استاذ محاضر أ	جامعة الشاذلي بن جديد - الطارف	مشرفاً
د. سعدون بلقاسم	استاذ محاضر ب	جامعة الشاذلي بن جديد - الطارف	ممتحنا

السنة الجامعية: 2026/2025

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية



الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

الرقم التسلسلي:

مذكرة بعنوان:

جرائم النصب عبر الوسائط الرقمية في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون أعمال

إشراف الأستاذ:

إعداد الطالبة:

بن عمار فطيمة الزهرة / الدكتور / بوسنة زهر الدين

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
د. مدار توفيق	استاذ محاضر ب	جامعة الشاذلي بن جديد - الطارف	رئيسا
د. بوسنة زهر الدين	استاذ محاضر أ	جامعة الشاذلي بن جديد - الطارف	مشرفاً
د. سعدون بلقاسم	استاذ محاضر ب	جامعة الشاذلي بن جديد - الطارف	ممتحنا

السنة الجامعية: 2026/2025

وزارة التعليم العالي والبحث العلمي
جامعة الشاذلي بن جديد الطارف
كلية الحقوق والعلوم السياسية
قسم الحقوق



Minister de L'enseignement Supérieur
Et de La Recherche Scientifique
Université el tarf
Faculté de Droit et des Sciences Politiques
Département de Droit

القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد المنطقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): **بن عبد الحليم الزهرى**

الحامل لبطاقة التعريف الوطنية رقم: **11.987.084.1015.25.0006**

الصادرة بتاريخ: **25 / 11 / 2016**

عن دائرة: **الطالب**

المسجل بقسم: **لكليات الحقوق والعلوم السياسية والمكلف بإتجاز مذكرة تخرج ماستر**

عنوانها: **حسب النظام التعليمي والأكاديمي المعمول به في**
السرعة الجزائرية

أصرح بشرفي أنني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية
والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: **11 / 11 / 2016**

إمضاء المعني

شكر وعرفان

الحمد لله العليّ القدير الذي وفّقني بفضلِهِ وكرمه لتذليل الصعاب وإتمام هذا البحث، والصلاة

والسلام على أشرف المرسلين

أتقدم بخالص شكري وعظيم امتناني إلى الأستاذ الفاضل والقدير

الدكتور / الأستاذ: بوستة زهرالدين

والذي غمرني بنبل أخلاقه وسديد نصحه، فكان لعلمه الوافر، وتوجيهاته القيمة، ومتابعته المستمرة

الأثر البالغ في إتمام هذا العمل وتصويب مساره.

فجزاه الله عني وعن العلم والطلبة خير الجزاء، وأدام عليه الصحة والعافية .

كما يمتد شكري الخالص إلى جميع أساتذتي الأفاضل في الكلية الذين أناروا طريقي بالعلم والمعرفة

طوال مسيرتي الدراسية، ولم يخلوا عليّ بنصح أو توجيه .

وأخيراً، أتوجه بالشكر والتقدير إلى كل من مدّ لي يد العون والمساعدة من قريب أو من بعيد لإنجاز

هذا العمل المتواضع.

إهداء

إلى من أحمل اسمه بكل فخر، إلى روحك الطاهرة التي تسكن وجداني... أبي الغالي (رحمك الله وأسكنك فسيح جناته)

كنت أتمنى أن تكون بجانبني اليوم لتشهد ثمرة غرسك وتفرح بتخرجي، لكنني أهدي إليك هذا النجاح ليكون بَرًا بك، ودعاءً موصولاً لك بالرحمة والمغفرة. نم قرير العين، فابنتك لم تخذل ظنك قط

إلى منبع الحنان، وسر النجاح، ودعائي المستجاب في كل صلاة... أُمِّي الحبيبة (حفظك الله ورعاك وأطال في عمرك) إلى من سهرت الليالي، وقاسمتني التعب والقلق، وكانت كلماتها لي بلسماً ودافعاً للاستمرار والتفوق.

إليك يا جنتي أهدي هذا التخرج، فلولا دعواتك ورضائك ما بلغت هذا المقام. أدامك الله تاجاً فوق رأسي .

إلى سندي وعزوتي، ومن بهم تكتمل فرحتي... إخوتي وأخواتي الأعزاء شكراً لأنكم كنتم دائماً السند والدافع والقلوب الدافئة التي ألتجئ إليها في كل حين.

أهديكم هذا النجاح امتناناً لوجودكم ودعمكم المستمر في حياتي

إلى كل هؤلاء... أهدي ثمرة جهدي ونجاحي.

مقدمة

شهدت الألفية الثالثة طفرة تكنولوجية هائلة وثورة معلوماتية غير مسبقة، أعادت بصورة جذرية تشكيل الأنماط السلوكية، والمعاملاتية، والاقتصادية في المجتمعات المعاصرة. ولم يكن المجتمع الجزائري بمعزل عن هذا التحول الرقمي المتسارع؛ إذ عرفت البيئة القانونية والاقتصادية الوطنية قفزة نوعية نحو ما يُعرف بـ "عصرنة المعاملات"، وتجلّى ذلك بوضوح في تبني الإستراتيجيات الوطنية للرقمنة، والتي توجت بصدور القانون رقم 18-05 المتعلق بالتجارة الإلكترونية¹، وتعميم استخدام وسائل الدفع الإلكتروني عبر البنى التحتية النقدية كـ (البطاقة الذهبية) الخاصة ببريد الجزائر، وبطاقات بنوك النقد الآلي المقاصية

غير أن هذا الفضاء الافتراضي الرحب، بقدر ما وفر من تسهيلات اقتصادية لا حصر لها، واختصار للوقت والجهد، وتنشيط للحركة التجارية، بقدر ما شكل في المقابل "بيئة خصبة ونموذجية" لولادة أنماط مستحدثة وسلوكات منحرفة من الإجرام المعلوماتي. وعلى رأس هذه السلوكيات تأتي جرائم النصب والاحتيال الرقمي؛ وهي الجرائم التي تجاوزت الأساليب التقليدية الكلاسيكية القائمة على الحيلة اللفظية والمواجهة المادية بين الجاني والضحية، لتنتقل إلى أساليب سيبرانية تعتمد على الذكاء التقني، التمويه الرقمي، والهندسة. حيث أصبح الجاني يختبئ خلف شاشات الحواسيب وعبر خوارزميات معقدة، مستغلاً قلة الوعي التكنولوجي لدى فئات واسعة من المستهلكين والمواطنين، مما يسهل سلب أموالهم ومدخراتهم بلمسة زر واحدة.

ثانياً: أهمية الموضوع

- تكمن في رصد ومواكبة مدى مرونة وقدرة المنظومة القانونية الجزائرية
- بشقيها الموضوعي والإجرائي على مسايرة هذه المستجدات التقنية المتلاحقة. فالأبحاث القانونية مدعوة اليوم وأكثر من أي وقت مضى لبيان مدى كفاية النصوص الكلاسيكية (مثل المادة 372 من قانون العقوبات الخاصة بالنصب التقليدي)².

¹ - القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية جريدة رسمية عدد 28 المؤرخة في 16 ماي 2018.

² - الأمر رقم 66-156 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، جريدة رسمية عدد 49 المؤرخة في 11 جوان 1966.

- مدى قدرتها على استيعاب السلوكيات الإجرامية المعاصرة، وإثراء المكتبة القانونية بقراءات تحليلية للنصوص القانونية الخاصة مثل القانون 09 - 04، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها³.

تتجلى في حماية المنظومة الاقتصادية والمالية الوطنية من الهزات التي قد تسببها موجات الاحتيال، ودعم الائتمان التجاري الرقمي الذي يعد عصب الاقتصاد الحديث. إن صون أموال الأفراد والمؤسسات من الاستنزاف الرقمي يسهم مباشرة في بناء ثقة مجتمعية صلبة في أنظمة الدفع الإلكتروني، وهو الشرط الأساسي والركيزة الأولى للتحويل نحو اقتصاد رقمي آمن، ومستدام، وجاذب للاستثمار.

ثالثاً: أهداف البحث:

تسعى هذه الدراسة من خلال الغوص في تفاصيل الآليات التشريعية إلى تحقيق جملة من الأهداف أبرزها:

- تفكيك العناصر التكوينية والأركان القانونية، للصور المستحدثة للاحتيال الرقمي في التشريع الجزائي، وتحديد مكامن الاختلاف بين الجريمة المعلوماتية والجريمة التقليدية من حيث الوسيلة، والمحل، والنتيجة الإجرامية.

- تبيان الثغرات القانونية ومواطن القصور التشريعي، سواء في النصوص العقابية الموضوعية من حيث عدم استيعابها لبعض الأنماط الإجرامية الذكية، أو في النصوص الإجرائية التي قد تقف عاجزة أمام الطبيعة الافتراضية للجريمة (كسرعة اختفاء الدليل الرقمي وصعوبة ضبطه).

- تحليل وتقييم فاعلية آليات التحري الرقمي والمؤسساتيين خلال تسليط الضوء على دور الضبطية القضائية المتخصصة، والمصالح الأمنية السبرانية، والهيئات الوطنية المستحدثة لمكافحة هذه الجرائم،

³- القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر في 16 أوت 2009.

والوقوف على مدى نجاعة الصلاحيات الممنوحة لهم قانوناً (كالتفتيش الإلكتروني، واعتراض المراسلات)

- تقديم رؤية استشرافية وتوصيات تشريعية، إذ تسهم في سد الفراغات القانونية، وتطوير آليات مكافحة بما يتلاءم مع المعايير والاتفاقيات الدولية ذات الصلة بالجريمة العابرة للحدود.

رابعاً: الإشكالية:

بناءً على التنازع القائم بين جمود النص القانوني وحركية التطور التكنولوجي، تبلور الإشكالية الرئيسية لهذه الدراسة في التساؤل الجوهرى التالي:

مدى كفاية القواعد المؤطرة لجريمة النصب من خلال التشريع الوطني في تقرير عقوبات رادعة؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية لتفكيك البحث:

1/ كيف تتجسد الصور المستحدثة للاحتيال الرقمي (كالهوية الرقمية المزيفة، المواقع الوهمية، وتصيد البيانات البنكية في ظل التشريع الجزائري الحالي؟ وما هي خصوصية أركانها المادية والمعنوية التي تميزها عن الجريمة التقليدية؟

2/ هل المنظومة العقابية والتدابير الردعية المقررة حالياً للأشخاص الطبيعيين (المحتالين) والأشخاص المعنويين (كالشركات والمصارف المقصرة في الحماية) كافية لتحقيق الردع العام والخاص وكبح جماح الجناة؟

3/ ما مدى نجاعة آليات التحري الرقمي والمؤسساتي في مواجهة العقوبات التقنية والقانونية (مثل مشكلة الاختصاص القضائي، وصعوبة إثبات الدليل الرقمي، وعقبة الجرائم العابرة للحدود التي تُرتكب من خارج الإقليم الوطني)؟

خامساً: منهج البحث المعتمد:

لأجل الإحاطة الشاملة بأبعاد هذه الإشكالية والإجابة عن التساؤلات المطروحة، تم الاعتماد في هذه الدراسة على **المنهج الوصفي و المنهج التحليلي**، باعتباره المنهج الأكثر ملائمة للدراسات القانونية التطبيقية.

ويتحقق ذلك من خلال استعراض، وتفكيك، وتحليل النصوص القانونية التي تنظم وتجرم السلوك الإلكتروني في التشريع الجزائري، وعلى رأسها القواعد العامة في قانون العقوبات وقانون الإجراءات الجزائية، مروراً بالنصوص الخاصة كالقانون رقم **09-04** المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والقانون رقم المتعلق بالتجارة الإلكترونية. ويهدف هذا التحليل إلى تقييم الجودة التشريعية لهذه النصوص، ومعرفة مدى فاعليتها الإجرائية والموضوعية عند التطبيق القضائي في المحاكم الجزائية لمواجهة هذا الخطر الداهم.

سادساً: خطة الدراسة :

تأسيساً على ما تقدم، وللإجابة على الإشكالية المطروحة، تم تقسيم هذا البحث إلى فصلين أساسيين:

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري (ويتناول ماهية الجريمة، وصورها المستحدثة، وأركانها القانونية).

الفصل الثاني: الآليات الإجرائية والمؤسسية لمكافحة الاحتيال الرقمي ومعوقات ضبطه (ويتناول طرق التحري والبحث، وجمع الأدلة الرقمية، ومدى فاعلية العقوبات المقررة قانوناً)

الفصل الأول:

الإطار النظري لجرائم الاحتيال الرقمي

في التشريع الجزائري

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

يُشكل التحول المتسارع نحو الرقمنة والاعتماد المتزايد على تكنولوجيات الإعلام والاتصال في المعاملات اليومية بالجزائر، بيئة خصبة لظهور أنماط إجرامية مستحدثة تتجاوز القواعد التقليدية للذمة المالية، حيث لم تعد الاعتداءات تتطلب مواجهة مادية أو وسائل ملموسة، بل أصبحت تُدار عبر شاشات رقمية واستراتيجيات تلاعب نفسي معقدة تقع تحت مظلة الهندسة الاجتماعية. ويسعى هذا الفصل إلى تقديم دراسة تحليلية وتأصيلية لأبرز ثلاثة مظاهر للإجرام المعلوماتي المالي؛ حيث نناقش جريمة النصب الإلكتروني عبر المنصات والمواقع مبيناً الخصوصية الإجرائية التي تفصلها عن النصب الكلاسيكي الوارد في المادة 372 من قانون العقوبات.

ثم ننتقل لتفكيك جريمة التصيد الاحتيالي وانتحال الهوية الرقمية والوقوف على أساليبها التقنية في تزوير الواجهات البنكية وموقع بريد الجزائر في ظل أحكام حماية المنظومات المعلوماتية (المواد 394 مكرر وما بعدها)، وصولاً إلى تحليل إلى جريمة الاحتيال المالي عبر أنظمة الدفع الإلكتروني وبطاقات الائتمان لبحث آليات قرصنة البطاقة الذهبية وبطاقات (CIB) وتجاوز التحقق الثنائي لتطبيق "بريدي موب"، بهدف رسم صورة قانونية متكاملة لمدى كفاية النص الجزائي الجزائري في مجابهة هذه الطفرة الإجرامية.

المبحث الأول: جريمة النصب الإلكتروني التقليدي :

يُشكل النصب الإلكتروني عبر المواقع والمنصات الرقمية الامتداد التقني لجريمة النصب الكلاسيكية. ورغم اشتراك الصورتين في الغاية النهائية وهي "الاستيلاء على ثروة الغير بدون وجه حق"، إلا أن البيئة الافتراضية تمنح الجريمة المستحدثة أبعاداً وآليات تنفيذ معقدة تفصلها عن القواعد التقليدية. وسنحاول من خلال هذا المبحث تبيان المفهوم القانوني والصور التطبيقية لهذه الجريمة)

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

المطلب الأول: مفهوم الجريمة وصورها :

إن دراسة جريمة النصب الإلكتروني تقتضي بدايةً تحديد مفهومها القانوني وتمييزها عن صور النصب التقليدية التي عرفت التشريعات الجنائية منذ زمن طويل، وذلك بالنظر إلى خصوصية البيئة الرقمية التي تُرتكب فيها هذه الجريمة واختلاف الوسائل المستخدمة في تنفيذها. فمع التطور المتسارع لتكنولوجيات الإعلام والاتصال وانتشار استخدام شبكة الإنترنت في مختلف المعاملات التجارية والمالية، ظهرت أساليب احتيالية جديدة استغل من خلالها الجناة الوسائط الإلكترونية للإيقاع بالضحايا والاستيلاء على أموالهم بطرق يصعب اكتشافها أو تتبع مرتكبيها.

ويكتسي تحديد مفهوم النصب الإلكتروني أهمية بالغة من الناحية القانونية، لأنه يسمح ببيان العناصر المكونة له وتمييزه عن الجرائم المشابهة كخيانة الأمانة والسرقة الإلكترونية والدخول غير المشروع إلى الأنظمة المعلوماتية. كما أن فهم هذه الجريمة يساهم في تحديد مدى كفاية النصوص القانونية القائمة لمواجهتها، خاصة في ظل التطور المستمر للأساليب الإجرامية الرقمية التي تتجاوز في كثير من الأحيان الحدود الجغرافية للدول

الفرع الأول: تعريف النصب الإلكتروني وتمييزه عن النصب التقليدي :

من خلال هذه النقطة سوف نتعرض للتعريف التشريعي و التعريف الفقهي لجريمة النصب الإلكتروني ، مع التركيز على موقف المشرع الجزائري من زاوية تعديلات قانون العقوبات المختلفة.

أولاً: تعريف النصب الإلكتروني التشريعي:

بالنسبة للمنظور التشريعي، فالملاحظ أن المشرع الجزائري لم يفرد -حتى الآن- نصاً خاصاً جامعاً لتعريف النصب الإلكتروني بشكل مستقل في قانون العقوبات، بل ترك الأمر للقواعد العامة مع محاولة إسقاطها إجرائياً وموضوعياً من خلال القوانين المكملة مثل القانون

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

رقم 18-05 المتعلق بالتجارة الإلكترونية والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹

ثانياً: تعريف النصب الإلكتروني فقها:

يمكن تعريف النصب الإلكتروني بأنه: "كل سلوك إجرامي عمدي يعتمد على استخدام تكنولوجيات الإعلام والاتصال، يهدف إلى خداع الضحية وإيقاعه في الغلط، عن طريق مظاهر احتيالية رقمية مصطنعة، لحمله على تسليم أموال أو منقولات تقع تحت حيازته الشرعية لنقلها إلى الذمة المالية للجاني أو لغيره"²

ثانياً: تمييز النصب الإلكتروني عن النصب التقليدي :

تنص المادة 372 من قانون العقوبات الجزائري على أنه: "كل من التمس أموالاً أو ثروات... واستعمل أسماء أو صفات كاذبة أو مخادعة... أو استعمل طرقاً احتيالية لإيهام بوجود مشروعات كاذبة... يعاقب بالحبس"³. وعند مقارنة هذا النص الكلاسيكي بالظاهرة الرقمية نجد فوارق جوهرية:

1. **طبيعة الوسيلة الإجرامية:** في النصب التقليدي، يعتمد الجاني على وسائل مادية ملموسة (تقديم وثائق ورقية مزورة، الاستعانة بشخص آخر لتأييد الأكاذيب "المظهر الخارجي المادي"، المقابلة الشخصية وجهاً لوجه). أما في النصب الإلكتروني، فإن الوسيلة افتراضية بحتة، حيث يتم استبدال المظهر المادي بمظهر رقمي (شاشات عرض، أكواد، واجهات مواقع مصممة باحترافية، حسابات مستعارة على منصات التواصل الاجتماعي)⁴

¹ - بوقرة أمين، "جرم النصب الإلكتروني في ظل القانون رقم 18-05 المتعلق بالتجارة الإلكترونية"، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 14، العدد 02، 2022، ص 234.

² - جلال ثروت، نظم القسم الخاص في قانون العقوبات: الجرائم الواقعة على الأموال، دار الجامعة الجديدة، الإسكندرية، 2019، ص 184.

³ - المادة 372 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات الجزائري، المعدل والمتمم.

⁴ - أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص: الجرائم الواقعة على الأموال والملكية، دار هومة، الجزائر، طبعة 2021، ص 105.

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

2. **المواجهة المادية والاتصال:** يتطلب النصب التقليدي -غالباً- وجود الجاني والضحية في مكان مادي واحد أو تواصل ملموس. بينما يتميز النصب الإلكتروني بغياب المواجهة المادية تماماً، فالجاني قد يكون في ولاية تمنراست والضحية في ولاية عنابة، أو قد يكون الجاني خارج الحدود الوطنية بالكامل، مما يسهل عليه الإفلات من الرقابة الأمنية الوجيهة¹
3. **حجم الأثر وامتداد الجريمة:** النصب التقليدي هو جريمة "فردية الأثر" في الغالب، حيث يستهدف النصاب ضحية واحدة أو عدداً محدوداً في كل عملية. بينما يتميز النصب عبر المنصات بالقدرة على استهداف آلاف الضحايا في ذات اللحظة الزمنية عبر منشور واحد ممول، مما يضاعف العائد الإجرامي والضرر المجتمعي²

الفرع الثاني: صورها التطبيقية :

أفرزت الممارسة اليومية في المجتمع الجزائري أنماطاً متكررة من النصب الإلكتروني، استغلت الفراغ التنظيمي لبعض الأنشطة الافتراضية وغياب الثقافة القانونية الرقمية لدى شريحة واسعة من المستهلكين:

1- مواقع ومنصات التسوق الوهمية:

تتمثل هذه الصورة في قيام الجاني بإنشاء موقع ويب ذو مظهر احترافي، أو صفحة تجارية على منصات التواصل الاجتماعي (فايسبوك و انستغرام) مستغلاً غياب الرقابة الصارمة على إنشاء الصفحات. يتم من خلالها عرض سلع (هواتف ذكية، ملابس، أجهزة كهرومنزلية) بأسعار منخفضة جداً مقارنة بأسعار السوق لجذب الضحايا³

¹ - بن خليفة فريد، الآليات الإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 1، 2021، ص 142 .

² - جميل عبد الباقي الصغير، المنظومة القانونية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2017، ص 92.

³ - المادة 12 من القانون رقم 05-18 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية.

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

بالنسبة لآلية الخداع، يُطلب من الضحية دفع تسبيق مالي عبر تحويل رصيد "بريدي موب" أو إرسال وصل تحويل الحساب الجاري (CCP) كشرط لشحن السلعة. وبمجرد استلام الجاني للأموال وتحقق النتيجة، يتم حظر الضحية وتصفية الصفحة أو تغيير اسمها، ليجد المستهلك نفسه أمام شبح افتراضي لا وجود له على أرض الواقع¹.

2- الإعلانات التجارية الكاذبة والخدمات الوهمية: لا تقتصر الجريمة على بيع السلع، بل تمتد إلى الخدمات. ومن أبرز مظاهرها في الجزائر:

- عقود العمل الوهمية بالخارج: نشر إعلانات منسوبة لوكالات سياحية أو شركات توظيف وهمية تزعم توفير تأشيرات وعقود عمل في دول أوروبية أو خليجية، ويُطلب من الضحايا دفع مبالغ مالية معتبرة تحت غطاء "رسوم الملف الإداري"²

- مسابقات الربح السريع والجوائز الكاذبة: إرسال رسائل عبر تكنولوجيا الاتصال (فايبر و واتساب) أو نشر منشورات تزعم فوز الضحية بجائزة مالية ضخمة من مؤسسة وطنية (مثل بريد الجزائر أو متعاملي الهاتف النقال)، ويُشترط للحصول عليها إرسال بطاقات تعبئة أو دفع رسوم ضريبية مسبقة، وهو ما يعد أسلوباً احتيالياً رقمياً مكتملاً³

¹ - هلاي أسامة، "الحماية الجنائية للمستهلك الإلكتروني عبر شبكات التواصل الاجتماعي في الجزائر"، مجلة الفكر العقاري، جامعة قسنطينة 2، المجلد 09، العدد 01، 2023، ص 410 .

² - عبد الله سليمان: دروس في القانون الجنائي الجزائري: القسم الخاص، ديوان المطبوعات الجامعية، الجزائر، 2018، ص 215 .

³ - عمارة عيسى، "آليات ضبط الجريمة السيبرانية في التشريع الجزائري"، مجلة البحوث القانونية والسياسية، جامعة المدية، العدد 12، 2022، ص 89

المطلب الثاني: الأركان القانونية للجريمة:

تخضع جريمة النصب الإلكتروني، في ظل غياب نص تشريعي مستقل ينظمها بصورة شاملة، للقواعد العامة المقررة لجريمة النصب المنصوص عليها في قانون العقوبات، مع مراعاة خصوصية الوسائل الرقمية المستخدمة في ارتكابها. ويقتضي قيام هذه الجريمة توافر مجموعة من الأركان القانونية التي تمنحها وصفها الإجرامي وتسمح بمتابعة مرتكبها جزائياً.

وتتمثل هذه الأركان أساساً في الركن المادي الذي يجسد السلوك الإجرامي والنتيجة المترتبة عنه والعلاقة السببية بينهما، والركن المعنوي الذي يعبر عن الإرادة الإجرامية للجاني واتجاه قصده إلى تحقيق النتيجة غير المشروعة. وتكتسي دراسة هذه الأركان أهمية بالغة، إذ لا يكفي مجرد وقوع ضرر أو خسارة مالية للضحية لقيام الجريمة، بل يجب إثبات جميع العناصر التي تتطلبها القانون حتى يمكن إسناد المسؤولية الجزائية إلى الفاعل. وعليه، سيتم التطرق إلى الركن المادي لجريمة النصب الإلكتروني، ثم بيان الركن المعنوي باعتباره الأساس الذي يميز بين الفعل العمدى المجرم والسلوك الخالي من القصد الجنائي.

الفرع الأول: الركن المادي :

لا يقوم الركن المادي للجريمة إلا بتوافر ثلاثة عناصر متلازمة، إذا سقط أحدها انتفت الجريمة بمفهومها الجزائي:

1- السلوك الإجرامي (استخدام الوسيلة الرقمية الاحتيالية): يمثل السلوك الإجرامي النشاط الإيجابي الذي يباشره الجاني لإيقاع الضحية في الغلط. وفي النصب الإلكتروني، يتمثل هذا السلوك في صياغة الأكاذيب وتدعيمها بمظاهر رقمية تخدع البصر والعقل.

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

يرى الفقه أن مجرد الكذب الإلكتروني (الادعاء المجرد في رسالة إلكترونية) لا يكفي وحده لقيام النصب، بل يجب أن يقترن بـ "أعمال خارجية رقمية" تُضفي عليه ثقة ومصادقية¹. ومن أمثلة ذلك: دمج صور سلع حقيقية مسروقة من مواقع أخرى، وضع تقييمات وتعليقات وهمية لحسابات يصطنعها الجاني نفسه لإيهام الضحية بجديّة الموقع، أو استخدام شعارات وعلامات تجارية مسجلة ومحمية دون إذن أصحابها².

2- النتيجة الإجرامية (تسليم المال أو المنقول): (المقصود بالنتيجة هنا هو الأثر المادي الناجم عن السلوك الاحتيالي، وهو قيام الضحية بـ "تسليم" ماله وتجرّد نفسه من حيازته طواعيةً تحت تأثير الغلط.

بالنسبة للخصوصية الرقمية في بيئة النصب الإلكتروني، يأخذ التسليم طابعاً مختلطاً؛ فقد يكون تسليمًا مادياً تقليدياً (عندما يلتقي الضحية بوكيل وهمي أو موزع ويسلمه النقود يداً بيد بناءً على اتفاق افتراضي)، أو تسليمًا رقمياً بحتاً (عن طريق تحويل الأموال إلكترونياً من حساب إلى حساب عبر تطبيقات الدفع الفوري، أو إرسال أرقام السيرال لبطاقات التعبئة والنقد)³. ويشترط أن يكون المال المسلم ذو قيمة مادية أو معنوية قابلة للتقويم المالي.

3- العلاقة السببية: يجب أن يثبت القضاء وجود رابطة سببية مباشرة ومتصلة بين الوسيلة الرقمية الاحتيالية التي استخدمها الجاني وبين فعل التسليم الصادر عن الضحية⁴ بمعنى آخر: يجب أن يثبت أن الضحية ما كان ليسلم أمواله أو مدخراته للجاني لولا انخداعه بالموقع الوهمي أو الإعلان المضلل والمظاهر الرقمية المصاحبة له. فإذا كان التسليم قد تم لسبب آخر مستقل

¹ - طاهري حسين، المرشد في القانون الجنائي الخاص، دار الهدى، عين مليلة، الجزائر، 2020، ص 167.

² - محمد الأمين الخضري، الجرائم المعلوماتية المستحدثة وآليات مكافحتها، دار الفكر الجامعي، الإسكندرية، 2021، ص 201.

³ - سليمان مريم، الحماية الجزائية للمستهلك عبر وسائل الدفع الإلكتروني في التشريع الجزائري، رسالة ماجستير في القانون الجنائي، جامعة تلمسان، 2023، ص 64.

⁴ - أحسن بوسقيعة، المرجع السابق، ص 109.

(كالهرج أو الشفقة أو بناءً على علاقة صداقة سابقة)، انتفت الجريمة بوصفها نصباً إلكترونياً¹

الفرع الثاني: الركن غير المادي (المعنوي):

يعتبر الركن المعنوي من الأركان الأساسية لقيام جريمة النصب الإلكتروني، باعتبارها من الجرائم العمدية التي تتطلب توافر إرادة إجرامية واعية وموجهة نحو تحقيق نتيجة غير مشروعة. فلا يكفي لقيام الجريمة مجرد استعمال الوسائل الرقمية أو وقوع الضرر على الضحية، بل يجب أن يثبت أن الجاني قد تصرف عن علم وإرادة بقصد خداع الضحية والاستيلاء على ماله.

ويتخذ القصد الجنائي في هذه الجريمة صورتين متكاملتين، تتمثل الأولى في القصد الجنائي العام القائم على عنصري العلم والإرادة، حيث يكون الجاني عالماً بعدم مشروعية أفعاله ومريداً لارتكابها، أما الثانية فتتمثل في القصد الجنائي الخاص الذي ينصرف إلى نية تملك مال الغير والاستفادة منه بصفة نهائية. ومن ثم فإن انتفاء أحد هذين العنصرين يؤدي إلى انتفاء الركن المعنوي، وبالتالي عدم قيام جريمة النصب الإلكتروني بصورتها القانونية الكاملة.

حيث تعتبر جريمة النصب الإلكتروني من الجرائم العمدية التي لا يتصور ارتكابها نتيجة إهمال أو خطأ غير مقصود؛ لذا يجب توافر القصد الجنائي بشقيه العام الخاص:

1- القصد الجنائي العام (العلم والإرادة):

- **العلم:** يجب أن يكون الجاني عالماً علماً يقينياً وبصيراً بنقاط متعددة؛ أولها أن الموقع أو الصفحة التي أنشأها وهمية ولا وجود لها تجارياً، وأن الإعلانات التي ينشرها كاذبة

¹ - جلال ثروت، المرجع السابق، ص 190 .

ومضللة، وأن سلوكه هذا غير مشروع ويقع تحت طائلة التجريم القانوني¹. كما يجب أن يعلم بأن هذا السلوك من شأنه إيقاع الضحية في الغلط وحمله على تسليم ماله.

• **الإرادة:** يجب أن تتجه إرادة الفاعل الحرة والمدركة إلى ارتكاب السلوك الإجرامي بجميع عناصره. أي أن تتجه إرادته إلى تصميم الموقع الخادع، وإلى نشر الإعلان المضلل، وإلى استقبال الأموال الناتجة عن هذا الخداع². فإذا انتفت الإرادة (كأن يكون الشخص واقعاً تحت إكراه مادي أو معنوي، أو مجرد تقني قام بتصميم الموقع بناءً على طلب زبون دون علمه بنواياه الاحتيالية)، انتفى الركن المعنوي في حقه.

2- **القصد الجنائي الخاص (نية التملك):** لا يكفي القانون بالقصد العام لقيام جريمة النصب الإلكتروني، بل يشترط انصراف نية الجاني إلى تحقيق هدف محدد وهو "نية التملك وحرمان صاحب المال منه نهائياً"³.

• معيار التمييز: يجب أن تتوجه نية المحتال إلى إدخال الأموال المستلمة من الضحية ضمن ذمته المالية حيازةً وتملكاً، والتصرف فيها تصرف المالك، وليس مجرد حيازتها مؤقتة أو على سبيل عارية الاستعمال أو بقصد المزاح. فثبوت نية سلب مال الغير واستغلاله هو المحرك الأساسي لإضفاء الوصف الجزائي على السلوك الرقمي⁴.

المبحث الثاني: جريمة التصيد الاحتيالي وانتحال الهوية الرقمية

إذا كان النصب الإلكتروني عبر المنصات يعتمد على الخداع التجاري والخدمي الظاهري، فإن جريمة التصيد الاحتيالي وانتحال الهوية الرقمية تمثل جيلاً أكثر خطورة وتعقيداً من الإجرام المعلوماتي. فهي لا تستهدف إقناع الضحية بمجدية مشروع وهمي فحسب، بل

¹ - مصطفى طاهر، جرائم الإنترنت وتحديات القانون الجنائي، دار النهضة العربية، القاهرة، 2018، ص 133.

² - بوقرة أمين، المرجع السابق، ص 239.

³ - عبد الله سليمان، المرجع السابق، ص 220.

⁴ - بن خليفة فريد، المرجع السابق، ص 150.

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

تعتمد على "الهندسة الاجتماعية" والتلاعب الفني لسرقة المفاتيح الأمنية والبيانات الحساسة للضحايا وتقمص هوياتهم الافتراضية للاستيلاء على أموالهم أو تشويه سمعتهم. وسنناقش هذا المبحث من خلال تبيان ماهية الجريمة وأساليبها التقنية

المطلب الأول: ماهية الجريمة وأساليبها التقنية

أفرز التطور المتسارع لتكنولوجيات الإعلام والاتصال أنماطاً إجرامية جديدة استغلت البيئة الرقمية كوسيلة للاعتداء على الأموال والحقوق، ومن أبرزها جريمة الاحتيال أو النصب الإلكتروني. وتكتسي دراسة هذه الجريمة أهمية خاصة بالنظر إلى تزايد انتشار المعاملات الإلكترونية واعتماد الأفراد على الإنترنت في مختلف أوجه الحياة اليومية. ويقتضي فهم هذه الجريمة تحديد مفهومها القانوني وخصائصها التي تميزها عن الجرائم التقليدية المشابهة، لاسيما جريمة النصب المنصوص عليها في قانون العقوبات.

كما يتطلب الأمر الوقوف على أهم الأساليب التقنية التي يعتمد عليها الجناة لتنفيذ مخططاتهم الاحتيالية، والتي تتنوع بين إنشاء مواقع وهمية واستعمال الحسابات المزيفة ورسائل التصيد الإلكتروني وغيرها من الوسائل المستحدثة. ومن ثم فإن الإحاطة بماهية الجريمة وصورها التقنية تمثل خطوة أساسية لفهم آليات مكافحتها والحد من آثارها السلبية على الأفراد والمجتمع.

الفرع الأول: تعريف التصيد الاحتيالي وسرقة الهوية الرقمية

أولاً: تعريف التصيد الاحتيالي

يُعرف التصيد الاحتيالي فقهيًا وتقنيًا بأنه: "وسيلة إجرامية تكنولوجية تقوم على خداع الضحايا عبر إرسال رسائل أو روابط إلكترونية مفبركة تحاكي وتطابق تماماً قنوات

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

اتصال تابعة لمؤسسات موثوقة (كالبنوك، أو هيئات البريد، أو شبكات التواصل)، لحث المستهدفين على إدخال بياناتهم السرية كأرقام الحسابات، وكلمات المرور، ورموز الأمان"¹

ولم يضع المشرع الجزائري مصطلحاً خاصاً بـ "التصيد الاحتيالي" في قانون العقوبات، ولكنه عاقب على الآثار التقنية المترتبة عنه بموجب أحكام تعديل قانون العقوبات (المواد 394 مكرر وما بعدها) المتعلقة بالمساس بالمنظومات المعلوماتية والدخول غير المصرح به²

ثانياً: سرقة وانتحال الهوية الرقمية

الهوية الرقمية هي مجموعة البيانات والمعطيات الإلكترونية التي تميز شخصاً معيناً في الفضاء الافتراضي (مثل: الاسم الرقمي، البريد الإلكتروني، الحساب البنكي، أو الحساب على مواقع التواصل). ويقصد بانتحالها: "قيام الجاني بالاستيلاء على هذه المعطيات الخاصة بغيره، واستخدامها دون رضاه لإيهام الآخرين بأنه هو صاحب الهوية الحقيقي، وذلك لتحقيق مآرب إجرامية مادية أو معنوية"³

وقد استوعب المشرع الجزائري خطورة هذا السلوك جزئياً في التعديلات الكلاسيكية الخاصة بانتحال الصفة والأسماء، فضلاً عن حماية المعطيات ذات الطابع الشخصي بموجب القانون رقم 07-18، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي⁴

¹ - د. محمد الأمين الخضري، المرجع السابق، ص 245.

² - انظر: المواد 394 مكرر إلى 394 مكرر 7 من الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري (المستحدثة بموجب القانون رقم 04-15 وتعديلاته)

³ - مصطفى طاهر، المرجع السابق، ص 178.

⁴ - القانون رقم 07-18 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، المؤرخة في 10 جوان 2018.

الفرع الثاني: أساليبها التقنية :

تتعدد الأساليب التقنية التي يعتمد عليها مرتكبو جرائم التصيد الاحتيالي الإلكتروني بهدف الحصول على البيانات الشخصية أو المصرفية للضحايا بطرق غير مشروعة، مستغلين الثقة التي يوليها الأفراد للمؤسسات الرسمية والخدمات الرقمية. وتتميز هذه الأساليب بالتطور المستمر لمواكبة التطور التكنولوجي ووسائل الحماية المستحدثة، مما يزيد من صعوبة اكتشافها من قبل المستخدم العادي. ومن أكثر هذه الأساليب شيوعاً إنشاء صفحات إلكترونية مزيفة تحاكي المواقع الرسمية للبنوك والمؤسسات المالية، وإرسال روابط خبيثة عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي.

بالإضافة إلى انتحال صفة هيئات رسمية أو شركات معروفة لإضفاء المصداقية على الرسائل الاحتيالية. وتهدف جميع هذه الوسائل إلى دفع الضحية إلى الإفصاح عن معلوماته السرية أو القيام بعمليات مالية يستفيد منها الجاني بصورة غير مشروعة. لذلك أصبحت معرفة هذه الأساليب التقنية أمراً ضرورياً لفهم طبيعة الجريمة وآليات مكافحتها.

1. **تزوير الواجهات البنكية وتطبيقات الدفع الفوري:** تعتبر هذه الصورة الأكثر انتشاراً وإضراراً بالمنظومة المصرفية في الجزائر مؤخراً.

• **آلية التنفيذ:** يقوم الجاني بتصميم واجهة ويب نسخاً وتفاصيل وتصميم الموقع الرسمي لمؤسسة "بريد الجزائر" (مثل واجهة خدمة ECCP أو أو البنوك الوطنية (كبنك التنمية المحلية BDL أو القرض الشعبي الجزائري (CPA). يتم بعد ذلك إرسال رابط هذه الواجهة المزورة إلى الضحايا عبر رسائل نصية (SMS) قصيرة مضللة، تزعم أن "حسابك البنكي مهدد بالتجميد، يرجى تحديث بياناتك فوراً عبر الرابط التالي"¹.

¹ - سليمان مريم ، المرجع السابق، ص 88.

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

وبمجرد دخول الضحية وإدخاله لاسم المستخدم وكلمة السر، يلتقطها الجاني في قاعدة بياناته الخاصة ويياشر سلب الأموال¹

2. الروابط الخبيثة المدججة والهندسة الاجتماعية: يعتمد المحتالون على استغلال المناسبات الوطنية أو الأزمات الاقتصادية لنشر روابط تندرج تحت مفهوم التصيد. مثل نشر روابط تزعم تقديم "منحة البطالة بقيمة مضاعفة"، أو "تسجيلات سكنات عدل بامتيازات خاصة"، أو "مساعداً مالية من صندوق الزكاة". تحوي هذه الروابط برمجيات خبيثة تقوم بمجرد الضغط عليها باختراق متصفح الضحية وسحب ملفات تعريف الارتباط (Cookies) وكلمات المرور المحفوظة في جهازه²

3. انتحال صفة وموقع هيئات رسمية أو مؤسسات تجارية: يتمثل هذا الأسلوب في إنشاء حسابات أو بريد إلكتروني يحمل اسماً مشابهاً جداً لبريد مؤسسات رسمية على سبيل المثال، مراسلة شركات أو مؤسسات اقتصادية جزائرية ببريد إلكتروني منتحل لصفة "مديرية الضرائب" أو "الجمارك الجزائرية"، لمطالبتهم بإرسال كشوفات مالية أو وثائق سرية تحت طائلة العقوبات الإدارية، ليتم استغلال تلك الوثائق في عمليات ابتزاز أو احتيال واسعة النطاق³

المطلب الثاني: الأركان القانونية للجريمة

تقتضي دراسة جريمة التصيد الاحتيالي وانتحال الهوية الرقمية الوقوف على أركانها القانونية التي يقوم عليها التجريم والعقاب، وذلك بالنظر إلى طبيعتها الخاصة التي تجمع بين الوسائل التقنية الحديثة وأساليب الخداع التقليدية. فهذه الجريمة لا تتحقق بمجرد استخدام الوسائط الإلكترونية، وإنما تستلزم توافر عناصر مادية ومعنوية محددة يقتضيها القانون الجنائي.

¹ - هلال أسامة، المرجع السابق، ص 512 .

² - عمارة عيسى، المرجع السابق، ص 102 .

³ - جميل عبد الباقي الصغير، المنظومة القانونية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2017، ص 119 .

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

ويتمثل الركن المادي في الأفعال والسلوكيات الاحتيالية التي تستهدف الحصول على البيانات أو الأموال بطرق غير مشروعة، بينما يتمثل الركن المعنوي في توافر القصد الجنائي لدى الجاني وعلمه بعدم مشروعية أفعاله واتجاه إرادته إلى تحقيق النتيجة الإجرامية. ومن ثم فإن توافر هذين الركنين يعد شرطاً أساسياً لقيام المسؤولية الجزائية وإسناد الجريمة إلى مرتكبها.

الفرع الأول: الركن المادي :

يتخذ الركن المادي في هذه الجريمة سلوكاً مركباً يمر بعدة مراحل فنية تشكل في مجموعها النشاط الإجرامي المحظور:

1- فعل التصميم والقرصنة (السلوك التحضيري والتنفيذي):

يبدأ الركن المادي بنشاط إيجابي يتمثل في اصطناع وتزوير الأدوات الرقمية؛ أي قيام الجاني ببرمجة وتصميم "الواجهة التطابقية المزورة" أو تشفير الروابط الخبيثة. ورغم أن هذا الفعل قد يبدو عملاً تحضيرياً، إلا أن التشريع الجزائري يعتبره سلوكاً مجرمًا بحد ذاته إذا ثبت استخدامه للوصول إلى أنظمة المعالجة الآلية للمعطيات طبقاً للمادة 394 مكرر 2 من قانون العقوبات (توفير برامج أو وسائل مصممة لارتكاب الجرائم المعلوماتية)¹.

2- عرض وتوجيه أداة الخداع (طرح الفخ السيبراني):

وهو إرسال الروابط أو الواجهات المزورة إلى الضحايا عبر قنوات الوسائط الرقمية (البريد، منصات التواصل، الرسائل النصية). هذا الفعل يمثل السلوك المادي المباشر للخداع، ويحل محل "الأكاذيب المدعومة بمظاهر خارجية" في جريمة نصب التقليديّة².

¹ - المادة 394 مكرر 2 من قانون العقوبات الجزائري

² - بن خليفة فريد، المرجع السابق، ص 189 .

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

3- النتيجة المادية: تتحقق النتيجة الإجرامية بمجرد وقوع البيانات السرية للضحية في يد الجاني.

التكليف القانوني الجزائري: لا يشترط لقيام جريمة التصيد أن يترتب عليها سحب الأموال فوراً؛ بل إن مجرد حصول الجاني على "المعطيات الشخصية والبنكية" للضحية بشكل غير مشروع يمثل نتيجة إجرامية كاملة تكيف على أنها "جريمة الدخول البقاء غير المشروع في منظومة معالجة آلية للمعطيات" المعاقب عليها بالمادة 394 مكرر، وكذا انتهاك أحكام القانون 07-18 المتعلق بالمعطيات الشخصية¹

الفرع الثاني: الركن غير المادي/المعنوي

تعد هذه الجريمة من الجرائم العمدية القائمة على سبق الإصرار الفني؛ إذ لا يمكن لتقنيات التصيد والقرصنة أن تحدث نتيجة خطأ مادي أو إهمال، وعليه يتكون الركن المعنوي من قصد جنائي عام وخاص:

4- القصد الجنائي العام :

• العلم: يجب أن يكون الجاني على علم ويقين تامين بأن الواجهة التي صممها كاذبة ومزورة، وأن البريد أو الحساب الذي ينتحله ليس ملكاً له ولا يملك صفة قانونية لتمثيله². كما يجب أن يعلم بأن اختراقه لخصوصية بيانات الضحية واستدراجها هو فعل مجرم قانوناً بموجب التشريع الجزائري والأحكام الحمائية للأنظمة المعلوماتية³.

¹ - أحسن بوسقيعة، المرجع السابق، ص 160 .

² - طاهري حسين، المرجع السابق، ص 204 .

³ - جلال ثروت، المرجع السابق ، ص 240 .

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

• **الإرادة:** انصراف إرادة الفاعل الحرة والواعية إلى توجيه هذا السلوك التقني الخبيث نحو الضحايا. أي أنه أرسل الروابط وصمم الواجهات بمحض إرادته وبدون أي ضغط أو إكراه مادي أو معنوي خارجي¹

5- القصد الجنائي الخاص (نية الإضرار بالضحية واستغلال هويته

يتطلب التكيف السليم للجريمة ثبوت القصد الخاص، وهو انصراف نية الجاني الداخلية إلى "استخدام البيانات المسروقة للإضرار بالضحية أو تحقيق كسب غير مشروع.

• مظاهر القصد الخاص: تتجلى نية الجاني في استخدام المعطيات البنكية المستولى عليها لسحب الأرصدة، أو استخدام الحساب الشخصي المخترق (الهوية الرقمية المنتهكة) لمراسلة أصدقاء الضحية وابتزازهم مالياً باسمه، أو تشويه سمعته الاجتماعية أو التجارية. وثبوت هذه النية التدميرية أو الاستغلالية هو ما يمنح الجريمة صبغتها الجنائية الشديدة الخطورة.²

المبحث الثالث: جريمة الاحتيال المالي عبر أنظمة الدفع الإلكتروني وبطاقات الائتمان

تمثل أنظمة الدفع الإلكتروني وبطاقات الائتمان والنقد الشريان النابض للتجارة الإلكترونية والتحول الاقتصادي الرقمي. ورغم التسهيلات والمزايا التي تقدمها هذه الأنظمة في الجزائر، إلا أنها أصبحت هدفاً رئيساً لمنظمات وشبكات الاحتيال المالي. فالجاني هنا لا يستهدف استدراج الضحية بالطرق التقليدية فحسب، بل يوجه نشاطه الإجرامي مباشرة نحو المعطيات البنكية والنبضات الإلكترونية المخزنة في الأنظمة المعلوماتية المصرفية لسلب

¹ - بوقرة أمين، المرجع السابق، ص 145.

² - عبد الله سليمان، المرجع السابق، ص 267.

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

الأرصدة وتحويلها بأساليب تقنية معقدة. وسنتناول هذا المبحث من خلال دراسة الإطار المفاهيمي للجريمة ومظاهرها)

المطلب الأول: الإطار المفاهيمي للجريمة ومظاهرها:

يتطلب فحص هذه الجريمة ضبط دلالاتها الاصطلاحية في الشقين القانوني والتقني، ثم رصد تحليلاتها وصورها التطبيقية الأكثر شيوعاً في البيئة المصرفية والبريدية الجزائرية، حيث تعد من الجرائم الإلكترونية المستحدثة التي أفرزها التطور المتسارع لتكنولوجيات الإعلام والاتصال وتوسع استخدام الخدمات المصرفية والبريدية عبر الإنترنت.

ويقتضي الإحاطة بما تحدد مفهومها القانوني والتقني وبيان خصائصها التي تميزها عن الجرائم التقليدية الماسة بالأموال والبيانات. كما تبرز أهمية دراسة هذه الجريمة بالنظر إلى ما تشكله من تهديد لأمن المعاملات الإلكترونية وثقة الأفراد في الخدمات الرقمية. وقد ساهم الانتشار الواسع للتطبيقات البنكية والبريدية في ظهور صور متعددة لهذه الجريمة تستهدف الحسابات الشخصية والبيانات السرية للمستخدمين. لذلك يقتضي الأمر الوقوف على أهم مظاهرها التطبيقية وأساليب ارتكابها في البيئة المصرفية والبريدية الجزائرية لفهم أبعادها القانونية والعملية.

الفرع الأول: تعريف الاحتيال على المعطيات البنكية الرقمية:

لابد من التطرق لكل من التطرق للتعريفين التشريعي و الفقهي للاحتيال عن طريق المعطيات البنكية الرقمية.

أولاً: التعريف التشريعي:

وقد واكب المشرع الجزائري هذا النمط الإجرامي عبر استحداث آليات حماية جزائية متطورة؛ فلم يعد يعتمد على الوصف الكلاسيكي لجريمة السرقة أو النصب، بل دمج هذه

السلوكيات تحت مظلة جرائم المساس بأنظمة المعالجة الآلية للمعطيات (المواد 394 مكرر وما بعدها من قانون العقوبات)، نظراً لأن الاعتداء يقع على "نظام معلوماتي بنكي" يحوي بيانات مالية¹. كما عزز هذه الحماية من خلال أحكام القانون رقم 05-18 المتعلق بالتجارة الإلكترونية، والذي ألزم في مادته 27 بتأمين المعاملات والبيانات الحساسة للمستهلكين.

ثانياً: التعريف الفقهي:

يمكن تعريف الاحتيال على المعطيات البنكية الرقمية بأنه: "كل تلاعب غير مشروع، أو ولوج غير مصرح به، أو استخدام غير مأذون فيه لبيانات ومعطيات بطاقات الدفع الإلكتروني أو الحسابات المصرفية المرقمنة، يترتب عليه إجراء تحويلات مالية أو سحبات نقدية من أرصدة الضحايا دون علمهم أو رضاهم، بهدف تحقيق كسب مالي غير مشروع للجاني أو لغيره"²

¹ - انظر: المادة 394 مكرر 1 من الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري، المعدل والمتمم

² - جميل عبد الباقي الصغير ، المرجع السابق، ص 74 .

الفرع الثاني: صورها التطبيقية في الجزائر :

عرف الواقع الجزائري طفرة في المعاملات المالية الإلكترونية، قابلتها طفرة موازية في صور الاحتيال المالي الرقمي، ومن أبرزها:

1. قرصنة البطاقة الذهبية وبطاقات بنوك النقد الآلي (CIB)

تتمثل هذه الصورة في استيلاء الجاني على "المعطيات الثلاثية الحساسة" المطبوعة على جسم البطاقة النقدية للضحية، والتي تشمل: (الرقم التسلسلي المكون من 16 رقماً، تاريخ نهاية الصلاحية، ورمز الأمان الخلفي المكون من 3 أرقام)¹.

أما آلية الاستغلال، فبمجرد حصول المحتال على هذه المعطيات (سواء عبر تصوير البطاقة مادياً بغفلة من صاحبها، أو عبر واجهات التصيد)، يقوم باستخدامها في منصات الشراء الإلكتروني غير المحمية، أو في شحن الأرصدة الهاتفية، أو دفع فواتير الخدمات عبر الإنترنت دون الحاجة لحيازة البطاقة مادياً².

2. اختراق وتجاوز نظام التحقق الثنائي عبر تطبيق "بريدي موب"

يعتبر تطبيق "بريدي موب" التابع لمؤسسة بريد الجزائر من أكثر التطبيقات استهدافاً بالاحتيال المالي في الوقت الحالي.

فالخداع، يقوم المحتال بإقناع الضحية (عبر الهندسة الاجتماعية) بإرسال رمز التفعيل المؤقت الذي يصل إلى هاتف الضحية عبر رسالة نصية قصيرة، بحجة تأكيد معاملة بيع أو تقديم منحة وهمية³. وبمجرد حصول المحتال على هذا الرمز، يقوم بتفعيل التطبيق على هاتفه

¹ - سليمان مريم، المرجع السابق، ص 95 .

² - هلاي أسامة، المرجع السابق، ص 519 .

³ - بوقرة أمين، المرجع السابق، ص 177 .

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

الشخصي، مما يمنحه ولاءً كاملاً وصلاحيّة مطلقة لإجراء تحويلات مالية فصيطة من حساب الضحية البريدي إلى حسابات أخرى وسيطة، مفرغاً رصيد الضحية في ثوانٍ معدودة.¹

المطلب الثاني: الأركان القانونية للجريمة:

بما أن الاحتيال المالي عبر الوسائط الرقمية ينطوي على اعتداء مزدوج يمس "الذمة المالية للضحية" من جهة، و"سلامة المنظومة المعلوماتية المصرفية" من جهة أخرى، فإن تفكيك بنيانه القانوني يتطلب فحص أركانه المادية والمعنوية بدقة.

الفرع الأول: الركن المادي :

يتخذ الركن المادي لهذه الجريمة طابعاً فنياً بحيثاً ينبثق من طبيعة البيئة التي تُرتكب فيها، ويتكون من العناصر التالية:

1- السلوك الإجرامي:

يتمثل السلوك المادي في ارتكاب أحد الأفعال المحظورة المنصوص عليها في المادة 394 مكرر 1 من قانون العقوبات، وهي²:

- إدخال معطيات كاذبة: قيام الجاني بإدخال بيانات بطاقة مسروقة أو كود تفعيل مخترق في المنظومة المصرفية الإلكترونية لإيهام النظام بأنه صاحب الحساب الشرعي.

- تعديل أو تغيير المعطيات: التلاعب البرمجي بالقيم الرقمية للأرصدة، أو تعديل رقم الهاتف المرتبط بالحساب البريدي لكي تصل رسائل التحقق إلى هاتف المحتال بدلاً من هاتف الضحية الأصلي.

¹ - عمارة عيسى، "المرجع السابق"، ص 115

² - المادة 394 مكرر 1 من قانون العقوبات الجزائري .

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

- حذف المعطيات: إلغاء أو محو القيود الحسابية أو سجلات العمليات التتبع الرقمية لإخفاء معالم سحب الأموال وعرقلة جهود الضبطية القضائية¹

2- النتيجة الإجرامية :

تتحقق النتيجة الإجرامية في الشق المالي بمجرد حدوث التغير في السجلات الرقمية للبنك أو بريد الجزائر، والذي يترتب عليه انتقال القيمة المالية (الرصيد) من ذمة الضحية المالية إلى ذمة الجاني أو الحساب الوسيط². ولا يشترط أن يقوم الجاني بسحب الأموال كاشمن الصراف الآلي لقيام الجريمة؛ بل إن مجرد تحويل الرقم المالي في البيئة الافتراضية بشكل غير مشروع يمثل نتيجة إجرامية كاملة³

3- العلاقة السببية.

يجب أن يثبت القضاء بصورة يقينية أن سلب الرصيد المالي أو التحويل غير المشروع كان نتيجة مباشرة لعملية الاختراق، أو التعديل، أو استخدام بيانات الدفع المقرصنة إلكترونياً. فإذا ثبت أن النقص في الحساب تم نتيجة خطأ تقني في خوادم البنك أو عطل في النظام البريدي دون تدخل إجرامي من طرف ثالث، انتفت الجريمة لانتهاء الرابطة السببية⁴.

¹ - أحسن بوسقيعة، المرجع السابق، ص 172 .

² - محمد الأمين الخضري، المرجع السابق، ص 310

³ - بن خليفة فريد، المرجع السابق، ص 210 .

⁴ - مصطفى طاهر، المرجع السابق، ص 212 .

الفرع الثاني: الركن غير المادي/المعنوي :

تندرج هذه الجريمة ضمن طائفة الجرائم العمدية المقصودة، ويتخذ ركنها المعنوي صورة قصد جنائي عام وخاص ينبغي على النيابة العامة إثبات توافره في حق المتهم:

1- القصد الجنائي العام :

يجب أن يكون المتهم عالماً علماً يقينياً وبصيراً بأن البيانات البنكية أو أرقام البطاقات التي يستخدمها ليست ملكاً له، وأنه لا يحمل إذناً شرعياً أو تفويضاً من صاحبها لاستعمالها¹. كما يجب أن يعلم بأن ولوجه إلى تطبيق الدفع (بريدي موب) أو إدخاله لمعطيات الغير في النظام هو فعل مجرم قانوناً ويمس بسلامة أنظمة المعالجة الآلية المصرفية المحمية جزائرياً².

انصراف إرادة الجاني الحرة والواعية إلى ارتكاب السلوك التقني المحظور؛ أي أنه قام بإدخال الأرقام السرية، أو تفعيل التطبيق، أو إجراء عملية التحويل المالي بمحض إرادته وتصميمه، دون أن يكون واقعاً تحت تأثير خطأ مادي (كغلط غير مقصود في كتابة أرقام حساب مشابه) أو إكراه³.

2- القصد الجنائي الخاص :

لا يكفي القانون بالقصد العام لقيام هذه الجريمة، بل يشترط توافر قصد خاص يتمثل في " انصراف نية الجاني الداخلية إلى تحقيق إثراء غير مشروع وسلب القيمة المالية للضحية نهائياً"⁴.

¹ - طاهري حسين، المرجع السابق، ص 230 .

² - جلال ثروت، المرجع السابق، ص 285

³ - بوقرة أمين، المرجع السابق ص 182

⁴ - عبد الله سليمان، المرجع السابق، ص 294 .

الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري

- أهمية القصد الخاص: هذا العنصر يفرق بين الباحث الأمني الذي قد يدخل إلى النظام المالي لإثبات وجود ثغرة أمنية دون نية الاستيلاء على الأموال، وبين المحتال الرقمي الذي يتلاعب بالنظام بنية تحويل الأرصدة لحسابه الخاص وحرمان صاحبها الشرعي منها وتملكها تملكاً تاماً¹.

¹ - بن خليفة فريد، المرجع السابق، ص 218.

خلاصة الفصل الأول :

تأسيساً على ما تم تحليله، نخلص إلى أن الجريمة المالية الإلكترونية في الجزائر قد تحولت من سلوكيات فردية معزولة إلى ظاهرة تقنية منظمة تتطور بالتوازي مع الأنظمة المصرفية. ورغم محاولات القضاء إسقاط القواعد العامة وقوانين التجارة الإلكترونية 05-18 وحماية المعطيات الشخصية 07-18 عليها، إلا أن الممارسة أثبتت وجود قصور تشريعي جوهري؛ يتمثل في غياب نصوص خاصة تُعرّف النصب الإلكتروني والتصيد بشكل مستقل، وعجز معيار المظهر الخارجي المادي عن استيعاب تعقيدات الواجهات البرمجية والصفحات الممولة، ناهيك عن تحول فعل تسليم المال إلى طابع رقمي فوري ضاعف من حجم الضرر الجنائي.

وبناءً على ذلك، نوصي المشرع الجزائري بالإسراع في أفراد فصل خاص يُجرّم الاحتيال المعلوماتي وانتحال الهوية الرقمية بعقوبات مشددة، مع إلزام المؤسسات البريدية والمصرفية بتطوير جدران حماية ديناميكية تحظر الحسابات الوسيطة المستخدمة في تبييض الأموال المقرصنة. فضلاً عن ذلك، يجب تكثيف الحملات التوعوية للمستهلك الجزائري ضد أساليب الهندسة الاجتماعية وسرقة الرموز، باعتبار وعي الضحية هو خط الدفاع الأول والأساسي في مواجهة الفخاخ السيبرانية.

الفصل الثاني

الآليات القانونية والإجرائية ومدى

كفايتها لتحقيق الردع

تمثل جرائم الاحتيال الرقمي أحد أبرز التحديات القانونية التي فرضها التطور التكنولوجي المتسارع وانتشار استخدام وسائل الاتصال الحديثة في مختلف المعاملات المالية والتجارية. فقد أفرزت البيئة الرقمية أنماطاً إجرامية مستحدثة تعتمد على استغلال الثغرات التقنية والنفسية للإيقاع بالضحايا والاستيلاء على أموالهم أو بياناتهم الشخصية. وأمام تنامي هذه الجرائم وتزايد آثارها السلبية على الأفراد والمؤسسات، تدخل المشرع الجزائري بوضع مجموعة من النصوص القانونية والآليات الإجرائية الرامية إلى الوقاية منها ومكافحتها. وعليه، يقتضي هذا الفصل دراسة الإطار القانوني والإجرائي لجرائم الاحتيال الرقمي، من خلال تحليل السياسة العقابية المقررة لها، وآليات البحث والتحري المعتمدة في كشفها وإثباتها، وكذا الوقوف على أبرز الصعوبات التي تواجه الجهات المختصة في ملاحقة مرتكبيها وتطبيق النصوص القانونية المتعلقة بها.

المبحث الأول: السياسة العقابية الموضوعية ومدى تحقيقها للردع:

إن مواجهة جرائم الاحتيال والنصب الرقمي لا تتوقف عند حدود التكييف القانوني السليم لصورها وأركانها، بل تتوقف بالدرجة الأولى على مدى قوة وحزم "السياسة العقابية" التي ينتهجها المشرع في مواجهة الجناة. فالجزء الجنائي هو الأداة الإستراتيجية لتحقيق الردع العام (زجر المجتمع ومنع المحاكاة الإجرامية) والردع الخاص (إصلاح الجاني ومنعه من العود). وسنحاول من خلال هذا المبحث تحليل العقوبات الموضوعية المقررة للأشخاص الطبيعيين وفائدتها الردعية مع رصد ظروف التشديد) **المطلب الأول**، ثم فحص المسؤولية الجزائية والردعية للشخص المعنوي كالمُنصّات الرقمية والشركات) **المطلب الثاني**

المطلب الأول: العقوبات المقررة للأشخاص الطبيعيين وفائدتها الردعية:

يتدرج المشرع الجزائري في معاقبة الشخص الطبيعي الذي يرتكب جرائم الاحتيال الرقمي بين العقوبات الأصلية والتكميلية المشتقة من قواعد قانون العقوبات والقوانين الخاصة، تليها ظروف تشديد ترتبط بجسامة الفعل وطبيعة الضحية.

الفرع الأول: العقوبات الأصلية والتكميلية في ظل قانون العقوبات والقانون 09-04:

لابد من التطرق للعقوبات الأصلية و العقوبات التكميلية.

أولاً: العقوبات الأصلية:

تتأرجح العقوبات الأصلية المسلطة على الجاني الطبيعي بحسب النص القانوني المعتمد في المتابعة القضائية:

1. عقوبة النصب (المادة 372 من قانون العقوبات): (إذا تم تكييف الفعل على أنه نصب تقليدي بوسيلة إلكترونية، يعاقب الجاني بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة مالية من 20.000 دج إلى 100.000 دج¹
2. عقوبة المساس بأنظمة المعالجة الآلية للمعطيات (المواد 394 مكرر وما بعدها): (إذا توبع الجاني بجرمة الاحتيال المالي أو التصيد عبر الدخول أو التعديل في الأنظمة البنكية، فإن المادة 394 مكرر 1 تعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 3.000.000 دج². أما إذا ترتب على هذا الاحتيال مساس بأنظمة الدولة أو الهيئات الحيوية، فقد ترتفع العقوبة إلى الحبس لمدة أطول.
3. عقوبات القانون 04-09: يعزز هذا القانون العقوبات إذا ارتبط الاحتيال الرقمي بقرصنة منظومة اتصالات كاملة، أو تجميع بيانات حساسة، وتتراوح عقوباته بالحبس لمدة تصل إلى خمس سنوات وغرامات مالية مشددة تتناسب مع الطابع التكنولوجي للجريمة.

ثانياً: العقوبات التكميلية:

- نظراً للطبيعة الفنية للجريمة، أدرك المشرع أن العقوبة البدنية (الحبس) لا تكفي؛ لذا أقر عقوبات تكميلية إلزامية وجوازية (المادة 9 من قانون العقوبات والمادة 394 مكرر 5)³
- المصادرة: مصادرة كافة الأجهزة والوسائل الإلكترونية، الحواسيب، الهواتف، والبرمجيات المستخدمة في عملية الاحتيال، وكذا مصادرة الأموال والعائدات النقدية الناشئة عن الجريمة والمودعة في الحسابات البريدية أو البنكية للجنة.
 - غلق المواقع والمنصات: غلق الموقع الإلكتروني أو الصفحة الافتراضية أو الخادم الذي أديرت منه العملية الاحتيالية غلقاً نهائياً أو مؤقتاً.
 - الحرمان من الحقوق والإقامة: الحرمان من الحقوق الوطنية والمدنية، أو الحظر من الإقامة، والمنع من ممارسة النشاط المهني أو التجاري المرتبط بتكنولوجيات الإعلام والاتصال⁴

¹ - المادة 372 من قانون العقوبات الجزائري، المعدل والمتمم

² - المادة 394 مكرر 1 من قانون العقوبات الجزائري (المستحدثة بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004.

³ - أحسن بوسقيعة، المرجع السابق، ص 315.

⁴ - بن خليفة فريد، المرجع السابق، ص 245

الفرع الثاني: ظروف التشديد ومدى ملائمتها لخطورة الجريمة

أقر المشرع الجزائري تشديد العقوبات الأصلية إذا وافقت الجريمة ظروفًا تعكس خطورة إجرامية كامنة في شخص الجاني أو طبيعة الضحية، ومن أبرزها:

1. **حالة العود:** طبقاً للقواعد العامة في قانون العقوبات، إذا عاد الجاني لارتكاب ذات الجريمة الرقمية أو جريمة مماثلة قبل انقضاء مدد رد الاعتبار، تضاعف العقوبة سالبة الحرية والغرامة المالية لكسر شوكتة الإجرامية¹

2. **استهداف الفئات الهشة:** يُعد من قبيل ظروف التشديد استغلال المحتال لضعف الضحية (ككبار السن المتقاعدين، أو الأميين رقمياً، أو ذوي الاحتياجات الخاصة) الذين يسهل استدراجهم للحصول على ال OTP الخاص ببطاقتهم الذهبية. هنا ترفع المحاكم العقوبة إلى حدها الأقصى²

3. **استغلال الأزمات والوظيفة:** إذا ارتكبت الجريمة في أوقات الأزمات (كالترويج لإعانات وهمية أثناء جائحة أو كوارث)، أو إذا ارتكبتها شخص يسهل له عمله الاطلاع على المعطيات (كموظف في بريد الجزائر أو بنك وطني)، فإن الصفة الوظيفية تشكل ظرف تشديد جنائي صريح³

تقييم الفقه وملائمة العقوبة: يرى الفقه الجزائري أن هذه السياسة العقابية ما زالت "قاصرة"؛ فمعظم جرائم الاحتيال المالي الرقمي تُكيف كـ "جنح" لا تتعدى عقوبتها خمس سنوات، بينما الأرباح المحققة تتجاوز الملايين، مما يجعل العقوبة غير رادعة بالقدر الكافي، ويدعو للمطالبة برفع هذه الجرائم إلى مصاف "الجنايات" إذا مسّت بالأمن المالي القومي⁴

المطلب الثاني: المسؤولية الجزائية للشخص المعنوي

لا يقتصر الإجرام الرقمي على الأفراد؛ بل كثيراً ما تختبئ شبكات الاحتيال وراء واجهات شركات توصيل وهمية، أو وكالات تسويق رقمي، أو منصات تجارة إلكترونية غير مرخصة، وهو ما استدعى بسط المسؤولية الجزائية على الشخص المعنوي.

¹ - عبد الله سليمان، المرجع السابق، ص 180.

² - بوقرة أمين، المرجع السابق، ص 248.

³ - طاهري حسين، المرجع السابق، ص 285.

⁴ - د. محمد الأمين الخضري، المرجع السابق، ص 412.

الفرع الأول: شروط قيام مسؤولية الشركات والمنصات الرقمية :

أقر المشرع الجزائري مبدأ المسؤولية الجزائية للشخص المعنوي بموجب المادة 18 مكرر من قانون العقوبات، ولكي تقوم هذه المسؤولية في جرائم الاحتيال الرقمي، يشترط توافر شروط تلازمية.

1. ارتكاب الجريمة لحساب الشخص المعنوي: أي أن يعود العائد المالي أو المنفعة الاقتصادية الناتجة عن النصب والاحتيال الرقمي إلى خزانة الشركة أو المنصة، وليس إلى الحساب الشخصي للموظف بمفرده¹

2. وقوع الفعل من ممثل أو عضو شرعي: يجب أن تُرتكب الجريمة بواسطة أحد الأشخاص الذين يملكون سلطة الإدارة، أو التمثيل، أو الرقابة داخل الشركة (كالمدير التنفيذي، أو الشريك المؤسس، أو المسؤول التقني عن المنصة الافتراضية)²

3. ثبوت الخطأ التنفيذي أو الرقابي: أن يثبت القضاء أن الشركة غضت الطرف عن عمليات الاحتيال التي تتم عبر خوادمها، أو قصرت تقنياً في حماية معطيات زبائنها ولم تتخذ تدابير الحماية والأمان الإلزامية المنصوص عليها في القانون 18-05 المتعلق بالتجارة الإلكترونية³

الفرع الثاني: تدابير العقاب المقررة للشخص المعنوي.

إذا ثبتت مسؤولية الشركة أو المنصة الرقمية، تطبق بحقها عقوبات وتدابير رادعة تتناسب مع طبيعتها القانونية والاعتبارية وفقاً للمادة 18 مكرر 1 وما بعدها من قانون العقوبات

1. الغرامات المالية المشددة: تُعاقب الشركة بغرامة مالية تتراوح بين خمس (5) إلى عشر (10) مرات من قيمة الغرامة المقررة للشخص الطبيعي في ذات الجريمة، وهو ما قد يصل إلى مئات الملايين من الدينار الجزائري، مما يشكل ضربة مالية قاضية لبنيتها الاقتصادية⁴

¹ - أحسن بوسقيعة ، المرجع السابق، ص 89

² - جلال ثروت، المرجع السابق، ص 340

³ - انظر: المادة 41 من القانون رقم 18-05 .

⁴ - سليمان مريم، المرجع السابق، ص 142.

2. المصادرة العينية والبرمجية: مصادرة كافة الأصول المالية للشركة الناشئة عن الاحتيال، ومصادرة العلامة التجارية الرقمية، وحجب النطاق الخاص بالموقع الإلكتروني ومصادرة الخوادم التابعة له¹
3. المنع من النشاط والحل: تشمل هذه التدابير منع الشركة من ممارسة نشاطها التجاري أو التقني بشكل مؤقت، أو المنع من المشاركة في الصفقات العمومية للدولة. وفي الحالات الخطيرة التي تؤسس فيها الشركة أساساً كغطاء لشبكة نصب سيرانية، يقضي القضاء بـ "حل الشخص المعنوي" نهائياً وشطب سجله التجاري²

المبحث الثاني: الفعالية الإجرائية لآليات البحث والتحري الرقمي

بما أن جرائم الاحتيال الرقمي تتميز بالتطير وسرعة الاختفاء عبر الخوادم الافتراضية، فإن القواعد الإجرائية التقليدية في البحث والتحري والتقصي أصبحت عاجزة عن ضبط أدلتها الرقمية وملاحقة مرتكبيها. هذا الواقع دفع المشرع الجزائري إلى تحديث ترسانته الإجرائية عبر تبني "آليات تحري رقمية خاصة" تستهدف رصد النبضات الإلكترونية وتتبع الأثر السيبراني، بالتوازي مع تفعيل دور مؤسساتي أمني متخصص. وسنناقش هذا المبحث من خلال تبيان أساليب التحري الرقمية الخاصة وحجيتها في الإثبات) **المطلب الأول** ثم استعراض الدور المؤسساتي للأجهزة الأمنية والهيئات المتخصصة **المطلب الثاني**.

المطلب الأول: أساليب التحري الرقمية الخاصة وحجيتها في الإثبات.

استحدث المشرع الجزائري أساليب إجرائية استثنائية بموجب القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلى جانب تعديلات قانون الإجراءات الجزائية، وذلك لمواجهة خصوصية الجرائم الرقمية التي يصعب كشفها بالوسائل التقليدية. ومن أهم هذه الأساليب: اعتراض المراسلات الإلكترونية، والتقاط البيانات المعلوماتية، والتفتيش والحجز الإلكتروني، والمراقبة التقنية للأنظمة المعلوماتية. وقد منح المشرع لهذه الإجراءات طابعاً قانونياً

¹ - عمارة عيسى، المرجع السابق، ص 104.

² - بن خليفة فريد، المرجع السابق، ص 270.

خاصاً يوازن بين فعالية التحري وحماية الحقوق والحريات الفردية. كما اشترط إخضاعها لإذن قضائي ورقابة قضائية لضمان مشروعيتها. وتكتسب الأدلة الرقمية المستخلصة من هذه الإجراءات حجية في الإثبات متى تم جمعها وفق الضوابط القانونية والتقنية التي تكفل سلامتها وعدم التلاعب بها.

الفرع الأول: أساليب التحري :

منح القانون لضباط الضبطية القضائية المؤهلين صلاحيات واسعة للتحري الفني تحت الإشراف المباشر للجهات القضائية (وكيل الجمهورية أو قاضي التحقيق)، وتتمثل أبرز هذه الأساليب في:

1. **التفتيش الإلكتروني وضبط المعطيات:** يتجاوز التفتيش هنا المفهوم المادي (المساكن والشركات) إلى تفتيش "المنظومات المعلوماتية وحوامل البيانات" (الهواتف، الأقراص الصلبة، السيرفرات). ووفقاً للمادة 11 من القانون 04-09، يجوز للضبطية القضائية تفتيش أي نظام معلوماتي أو جزء منه يُعتقد أن المعطيات المخزنة داخله تفيد في كشف حقيقة الاحتيال البنكي، مع صلاحية حجز الحوامل الإلكترونية أو نسخ المعطيات ومصادرتها رقمياً.
2. **اعتراض المراسلات والاتصالات وتسجيلها:** بالنظر إلى أن المحتالين يعتمدون على تطبيقات المحادثة الفورية والبريد الإلكتروني لاستدراج الضحايا، أتاحت المادة 4 من القانون 04-09 للجهة القضائية المختصة إصدار إذن بـ "الاعتراض والمراقبة الفورية للاتصالات"¹. ويشمل ذلك مراقبة التدفق الرقمي، وتسجيل محتوى المحادثات الإلكترونية، والتعرف على حركة البيانات لتحديد الهوية الرقمية للجاني وموقعه الجغرافي عبر بروتوكول الإنترنت².
3. **اختراق المنظومات والمعالجة الآلية عن بُعد:** تعد من أدق الآليات المستحدثّة؛ حيث تتيح للضبطية القضائية - في ظروف مشددة وبإذن قضائي مسبق - الولوج عن بُعد (عبر برمجيات مرخصة) إلى

¹ - المادة 4 من القانون رقم 04-09، المصدر نفسه .

² - بن خليفة فريد، المرجع السابق، ص 312.

النظام المعلوماتي الذي يستخدمه المحتال دون علمه، لغرض تتبع مسار الأموال المسروقة عبر تطبيق "بريدي موب" أو رصد واجهات التصيد الاحتيالي قبل قيام الجاني بمحوها¹.

الفرع الثاني: حجية الدليل الرقمي المستمد منها وشروط قبوله قضائياً.

يواجه القضاء الجزائري تحدياً كبيراً في تقييم "الدليل الرقمي" (كالمستخرجات التقنية، صور الشاشة للتحويلات، سجلات الخوادم) نظراً لسهولة تعديله أو فبركته بالذكاء الاصطناعي، ولذا يخضع قبول هذا الدليل لشروط صارمة:

1. **مشروعية الدليل الرقمي:** يشترط صراحةً أن يكون الدليل قد استُخرج بناءً على الإجراءات القانونية الصحيحة (وجود إذن قضائي مكتوب ومسبب بالتفتيش أو الاعتراض). وكل دليل رقمي يتم الحصول عليه عبر اختراق غير قانوني من طرف الضبطية يُعد باطلاً ولا يُعتد به بناءً على قاعدة "ما بُني على باطل فهو باطل"².
2. **سلامة واستمرارية الدليل:** يجب إثبات أن المعطيات الرقمية المضبوطة لم تعرض للتعديل أو التحريف منذ لحظة ضبطها وحجزها في الفضاء الافتراضي حتى عرضها على المحكمة. ويتطلب ذلك الاستعانة بـ "الهاش التقني" كبصمة رقمية تضمن عدم التلاعب بالملفات³.
3. **الحجية القانونية المقيدة:** أقر المشرع الجزائري الحجية القانونية للمستند الإلكتروني بموجب القانون رقم 04-15 المتعلق بالتوقيع الإلكتروني والمعاملات الإلكترونية، حيث أصبحت للوثيقة الرقمية نفس حجية الوثيقة الورقية بشرط إمكانية التحقق من هوية مصدرها وسلامتها⁴. ومع ذلك، يخضع الدليل الرقمي في المواد الجزائية لمبدأ "الاقتناع الشخصي للقاضي" (المادة 212 من قانون الإجراءات الجزائية)، فللقاضي كامل السلطة في تقدير القوة الإقناعية للتقرير الفني⁵.

¹ - مصطفى طاهر، المرجع السابق، ص 345.

² - أحسن بوسقيعة، التحقيق القضائي، دار هومة، الجزائر، طبعة 2020، ص 198.

³ - محمد الأمين الحضري، المرجع السابق، ص 480.

⁴ - القانون رقم 04-15 المؤرخ في 1 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع الإلكتروني والمعاملات الإلكترونية، الجريدة الرسمية، العدد 06، المؤرخة في 10 فيفري 2015.

⁵ - طاهري حسين، المرشد في قانون الإجراءات الجزائية الجزائري، دار الهدى، عين مليلة، الجزائر، 2021، ص 220.

المطلب الثاني: الدور المؤسسي للأجهزة الأمنية والهيئات المتخصصة.

لم يكتفِ المشرع الجزائري بتحديث النصوص الإجرائية، بل عمل على إنشاء وتطوير أجهزة أمنية وهيئات متخصصة تمتلك الخبرة التقنية اللازمة لمواجهة الجرائم السيبرانية. ومن أبرز هذه الجهات المصالح المختصة التابعة للأمن الوطني والدرك الوطني، والتي تضم فرقاً متخصصة في مكافحة الجرائم المعلوماتية وتتولى تتبع مرتكبيها وجمع الأدلة الرقمية.

كما أنشئت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنسيق مكافحتها، بهدف تعزيز التعاون بين مختلف المتدخلين في هذا المجال. وتضطلع هذه الأجهزة بمهام الرصد والتحليل والتدخل السريع عند وقوع الهجمات الإلكترونية. ويسهم التنسيق بينها وبين الجهات القضائية في تعزيز فعالية المتابعة والتحقيق. كما يشكل التكوين المستمر للعناصر المختصة عاملاً أساسياً لمواكبة التطور المتسارع للوسائل الإجرامية الرقمية.

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

أنشئت هذه الهيئة بموجب القانون 09-04 (المواد 12 وما بعدها) وضُبطت صلاحياتها بموجب المرسوم الرئاسي رقم 15-261.¹ وتعتبر هذه الهيئة بمثابة سلطة تنسيقية وعملية عليا موضوعة لدى وزير العدل، وتلعب دوراً محورياً يتركز في:

1. **تجميع وتحليل البيانات:** تعمل الهيئة كمركز وطني لتجميع المعلومات والتقارير المتعلقة بالاحتيال الرقمي والتصيد، وتتبع مسارات الهجمات السيبرانية التي تستهدف المنظومات البنكية الوطنية²
2. **المساعدة التقنية للقضاء:** تتولى الهيئة تقديم الدعم الفني المباشر للجهات القضائية ومساعدة ضباط الضبطية القضائية في تتبع وإجراء التحريات المعقدة التي تتطلب كفاءات برمجية عالية، أو تتطلب تنسيقاً دولياً لطلب بيانات من خوادم تقع خارج التراب الوطني¹

¹ - المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها العدل و المتمم ، الجريدة الرسمية، العدد 53، المؤرخة في 08 أكتوبر 2015

² - عمارة عيسى ، المرجع السابق، ص 138 .

3. إطلاق الإنذارات الوقائية: تملك الهيئة صلاحية رصد المواقع الحاملة لواجهات التصيد وإخطار الجهات المعنية (مثل سلطة ضبط البريد والاتصالات الإلكترونية) لحجبها فوراً لحماية المواطنين²

الفرع الثاني: الفرق الجنائية الرقمية المتخصصة

تتوزع المهام الميدانية للضبطية القضائية الرقمية بين جهازي الأمن والدرك الوطني عبر خلايا ومصالح متخصصة عُهد إليها بالاتصال المباشر مع بلاغات الضحايا:

1. المصلحة المركزية لمكافحة الجرائم السيبرانية بالأمن الوطني: وتتبعها فرق مكافحة الجريمة المعلوماتية على مستوى أمن الولايات. تمتلك هذه الفرق مختبرات جنائية رقمية لتحليل الهواتف المحمولة المقرصنة، وفحص العمليات المشبوهة عبر تطبيق "بريدي موب"، واستصدار مذكرات التوقيف بناءً على مسح البصمات الرقمية والمواقع الجغرافية للجنة³

2. مصلحة مكافحة الإجرام السيبراني للدرك الوطني: وتضم مهندسين وتقنيين متخصصين يعملون في إطار المعهد الوطني للأدلة الجنائية وعلم الإجرام. وتتميز هذه المصالح بقدرتها العالية على تتبع الشبكي، وتحليل البرمجيات الخبيثة المستخدمة في التصيد الاحتيالي، وتقديم تقارير خبرة رقمية متكاملة يعتمد عليها⁴ 56 ليها قضاة الموضوع في إدانة المحتالين صراحة.

المبحث الثالث: معوقات ملاحقة جرائم الاحتيال الرقمي وتطبيقها قضائياً

رغم الترسنة القانونية الموضوعية والإجرائية التي استحدثتها المشرع الجزائري، ورغم الجهود المبذولة من قبل الأجهزة الأمنية المتخصصة، إلا أن الواقع التطبيقي يشير إلى وجود فجوة عميقة بين نصوص التشريع ومعدلات الإدانة الفعلية للمحتالين رقمياً. وتعود هذه الفجوة إلى طبيعة الجريمة الافتراضية العابرة للحدود والمتطورة تقنياً، والتي تتصادم مع آليات تقليدية أو عوائق لوجستية وفنية تحول دون الكشف عن الجناة أو استرداد الأموال المسلوقة. وسنناقش في هذا المبحث هذه العراقيل

¹ - هلاي أسامة، المرجع السابق، ص 602 .

² - بن خليفة فريد، المرجع السابق، ص 350 .

³ - بوقرة أمين ، المرجع السابق، ص 211 .

⁴ - سليمان مريم ، المرجع السابق، ص 119.

بتفصيل من خلال استعراض الصعوبات الفنية والإجرائية العابرة للحدود) **المطلب الأول** ثم الصعوبات المؤسساتية والبشرية ونقص الوعي القانوني وثقافة التبليغ) **المطلب الثاني**.

المطلب الأول: الصعوبات الفنية والإجرائية العابرة للحدود

تمثل البنية التقنية المعقدة لشبكة الإنترنت وتطور وسائل الإخفاء الرقمي أحد أبرز التحديات التي تواجه أجهزة التحري والتحقيق في الجرائم السيبرانية. فالجناة يعتمدون على تقنيات متطورة كالشبكات الافتراضية الخاصة (VPN) والخوادم الوسيطة وبرامج التشفير لإخفاء هوياتهم ومواقعهم الحقيقية، مما يصعب عملية تتبعهم. كما أن الطابع العابر للحدود لهذه الجرائم يؤدي غالباً إلى تشتت الأدلة الرقمية بين عدة دول تخضع لأنظمة قانونية مختلفة. ويترتب على ذلك بطء إجراءات التعاون القضائي الدولي والحصول على المعلومات اللازمة للتحقيق. إضافة إلى ذلك، فإن سرعة محو البيانات أو تعديلها تشكل عائقاً أمام جمع الأدلة وحفظها. لذلك تفرض هذه التحديات ضرورة تعزيز التعاون الدولي وتطوير الوسائل التقنية والقانونية لمكافحة الجرائم الرقمية بفعالية.

الفرع الأول: العقوبات الفنية :

تتمثل أبرز الصعوبات الفنية التي تصطدم بها مصالح الأمن والدرك الوطني في الجزائر فيما يلي:

1. **استخدام تقنيات التمويه الجغرافي:** يعتمد محتالو الفضاء السيبراني على شبكات افتراضية خاصة لتغيير عناوين بروتوكول الإنترنت الخاصة بهم. فعندما يقوم المحتال باختراق حساب "بريدي موب" لضحية في الجزائر، تظهر بيانات النظام أن الدخول تم من دولة كندا أو هولندا مثلاً، مما يضلل المحققين ويمنعهم من تحديد مكان الجاني الفعلي¹.
2. **برمجيات التشفير المعقدة وتطهير البيانات:** يستخدم المحترفون برمجيات لتشفير تواصلهم، فضلاً عن استخدام أدوات مسح ذاتي وتطهير دوري لملفات الارتباط وسجلات الأحداث على الأجهزة

¹ - محمد الأمين الحضري، المرجع السابق، ص 510 .

والروابط المستخدمة في التصيد بمجرد انتهاء العملية، مما يجعل استرجاع الأدلة الرقمية من الأجهزة المحجوزة أمراً بالغ الصعوبة حتى بالنسبة للمختبرات الجنائية المتقدمة¹.

3. الهويات الافتراضية المستعارة والشرائح مجهولة الهوية: يرتكب الكثير من الجناة جرائمهم باستخدام حسابات "فيسبوك" أو "تلغرام" منشأة بمعلومات وهمية تماماً، أو مستندة إلى شرائح هاتفية مصنفة في الجزائر ضمن خانة "الشرائح المجهولة" أو المسجلة بأسماء أشخاص طبيعيين تم نسخ بطاقات هوياتهم الوطنية دون علمهم أثناء عمليات تجارية بسيطة².

الفرع الثاني: العقوبات الإجرائية (الاختصاص القضائي الدولي العابر للحدود، وقصور الاتفاقيات).

تتضاعف الأزمة عندما تكتسي الجريمة طابعاً دولياً، وتتجلى العوائق الإجرائية في نقطتين رئيسيتين:

1. تنازع الاختصاص القضائي الدولي: تتميز جريمة الاحتيال الرقمي بأنها قد تُرتكب من جاني مقيم في دولة (أ)، مستخدماً خوادم مستضافة في دولة (ب)، لإيقاع ضحية مقيم في الجزائر (دولة ج). هذا التشتت يطرح إشكالاً عويصاً حول المحكمة المختصة إقليمياً ودولياً بملاحقة الجاني، خاصة إذا كانت تشريعات بعض الدول لا تجرم السلوك بذات الجسامة التي ينص عليها القانون الجزائري³.

2. بطء وصعوبة إجراءات الإنابات القضائية الدولية: إذا ثبت أن موقع التصيد الاحتيالي مستضاف على خادم تابع لشركة أمريكية أو أوروبية، فإن الضبطية القضائية الجزائرية لا تملك صلاحية تفتيش هذا السيرفر أو إجبار الشركة على تقديم بيانات صاحبه إلا عبر "إنابة قضائية دولية" تمر بالقنوات الدبلوماسية الرسمية وتستغرق هذه الإجراءات أشهراً طويلة أو سنوات، وهي مدة كافية جداً للمحتال لكي يمحو أثره الرقمي تماماً ويغلق الحسابات الوسيطة⁴.

3. قصور الاتفاقيات الأمنية المشتركة: رغم انضمام الجزائر لبعض الاتفاقيات، إلا أن غياب اتفاقيات ثنائية متخصصة ومباشرة في تسليم المجرمين المعلوماتيين أو التبادل الفوري للمقترفين مع

¹ - مصطفى طاهر، المرجع السابق، ص 412.

² - بوقرة أمين، المرجع السابق، ص 189.

³ - جميل عبد الباقي الصغير، المرجع السابق، ص 298.

⁴ - بن خليفة فريد، المرجع السابق، ص 415.

بعض الدول التي تعد ملاذاً آمناً لقرصنة المال الرقمي، يحول دون تتبع خيوط شبكات النصب المنظمة¹

المطلب الثاني: الصعوبات المؤسسية والبشرية ونقص الوعي القانوني

لا تقتصر التحديات التي تواجه مكافحة الجرائم الإلكترونية على الجوانب التقنية فقط، بل تمتد إلى عوامل مؤسسية وبشرية تؤثر في فعالية المواجهة القانونية. فقلة الكفاءات المتخصصة في مجال التحريات الرقمية وتحليل الأدلة الإلكترونية تشكل عائقاً أمام سرعة وكفاءة التحقيقات. كما تعاني بعض الجهات من محدودية الإمكانيات المادية والتجهيزات التقنية اللازمة لمواكبة التطور المستمر لأساليب الجريمة الإلكترونية.

ومن جهة أخرى، يساهم ضعف الوعي القانوني والرقمي لدى المواطنين في زيادة عدد الضحايا وتردد بعضهم في التبليغ عن الجرائم خوفاً من فقدان الثقة أو لجهلهم بالإجراءات القانونية المتاحة. ويؤثر هذا الأمر سلباً على كشف الجرائم وملاحقة مرتكبيها. لذلك تبرز أهمية تعزيز التكوين المتخصص ونشر الثقافة القانونية والرقمية بين مختلف فئات المجتمع.

الفرع الأول: الصعوبات المؤسسية والبشرية (نقص التكوين التقني لرجال القضاء، وضعف التجهيز اللوجستي)

تواجه المنظومة القضائية والأمنية تحديات داخلية ترتبط بمواكبة التسارع التكنولوجي:

1. فجوة التكوين التقني لدى رجال القضاء: تفتقر نسبة معتبرة من قضاة الموضوع (قضاة الحكم والنيابة) إلى تكوين تخصصي معمق في هندسة الشبكات وتكنولوجيا المعلومات. ويترتب على ذلك صعوبة في استيعاب التقارير الفنية المعقدة المحالة إليهم من مصالح الأمن والدرك، أو التردد في تكييف الأدلة الرقمية، مما يؤدي أحياناً إلى إفلات الجناة من العقاب أو إصدار أحكام لا تتناسب مع الخطورة التقنية للفعل²

¹ - عمارة عيسى، المرجع السابق، ص 160.

² - طاهري حسين، المرجع السابق، ص 310.

2. الضغط على الهياكل المركزية والمتخصصة: رغم كفاءة "الهيئة الوطنية للوقاية من جرائم تكنولوجيايات الإعلام والاتصال"، إلا أن تمركز صلاحياتها وخبرائها الفنيين في العاصمة، وضخامة عدد القضايا المحالة إليها من كافة المحاكم والمجالس القضائية عبر الوطن، يخلق نوعاً من التراكم والتأخر في إصدار تقارير الخبرة الرقمية الحاسمة في الدعاوى الاستعجالية للاحتيال المالي¹.
3. ضعف التجهيز اللوجستي والمادي لبعض الفروع: تتطلب عمليات تتبع العمليات المالية المشفرة ومراقبة الشبكات برمجيات أصلية باهظة الثمن وأجهزة خادمة ذات قدرات معالجة فائقة وإن عدم تعميم هذه الإمكانيات اللوجستية على كافة الفرق المحلية لأمن الولايات والكتائب الإقليمية للدرك الوطني يحد من فاعلية التدخل السريع².

الفرع الثاني: نقص وعي الضحايا وثقافة التبليغ وعلاقتها بإفلات الجناة

يمثل سلوك الضحية حجر الزاوية في إنجاح أو إفشال المقاربة الأمنية لمكافحة الاحتيال، ويعاني الواقع الجزائري من أزمة وعي رقمي تتلخص في المظاهر الآتية:

1. ثقافة التأخر أو الامتناع عن التبليغ: يرفض قطاع واسع من ضحايا النصب الإلكتروني والتصيد الاحتيالي التوجه إلى مراكز الأمن أو وكلاء الجمهورية لتقيد شكاوى رسمية. ويعود ذلك إلى شعورهم بالخرج الاجتماعي والخلل من وقوعهم ضحايا لخداع بسيط (مثل تقديم ال OTP)، أو بسبب صغر حجم المبلغ المالي المسلوب مقارنة بالإجراءات القضائية، مما يشجع المحتال على الاستمرار وتوسيع شبكة ضحاياه³.
2. محو الأدلة الرقمية من طرف الضحية: بمجرد اكتشاف الضحية لعملية الاحتيال (كسحب رصيده من بريدي موب)، يقوم بدافع الغضب أو الخوف بحظر المحتال ومسح المحادثات ورسائل النصية أو الرابط الخبيث من هاتفه. هذا التصرف العفوي يؤدي إلى تدمير "المسرح الافتراضي للجريمة" ويحرم المحققين الجنائيين من التقاط الخيوط التقنية الأولى اللازمة للتعرف على الجاني⁴.

¹ - هلاي أسامة، المرجع السابق، ص 712.

² - سليمان مريم، المرجع السابق، ص 165.

³ - بوقرة أمين، المرجع السابق، ص 198.

⁴ - أحسن بوسقيعة، المرجع السابق، ص 215.

3. الأمية الرقمية الاستهلاكية: إن الانتشار الواسع لوسائل الدفع الإلكتروني (البطاقة الذهبية) في الجزائر لم ترافقه حملات توعية مؤسساتية مكافئة تشرح للمواطن البسيط خطورة مشاركة معطيات بطاقته أو الرموز السرية، مما يجعل الضحايا يسهمون -بخطأهم غير العمدى- في تسهيل الركن المادي للجريمة وإفلات الجاني من الرصد المباشر¹

خلاصة الفصل الثاني:

من خلال دراسة مختلف الجوانب القانونية والإجرائية لجرائم الاحتيال الرقمي، يتضح أن المشرع الجزائري سعى إلى توفير حماية جنائية فعالة للأموال والمعطيات الإلكترونية عبر مجموعة من النصوص العقابية والآليات الإجرائية المتخصصة. كما أظهر البحث أهمية الدور الذي تضطلع به الأجهزة الأمنية والهيئات المختصة في كشف هذه الجرائم وملاحقة مرتكبيها، خاصة في ظل التطور المستمر لأساليب الاحتيال الإلكتروني.

غير أن فعالية هذه المنظومة لا تزال تواجه عدة تحديات تقنية وقانونية ومؤسسية، أبرزها صعوبة تحديد هوية الجناة، والطابع العابر للحدود للجريمة، ونقص الوعي الرقمي لدى بعض المستخدمين. ومن ثم فإن تعزيز مكافحة جرائم الاحتيال الرقمي يقتضي تطوير التشريعات القائمة، وتدعيم التعاون الدولي، وتكثيف برامج التوعية والتكوين المتخصص بما يضمن تحقيق حماية أكثر فعالية للأفراد والمؤسسات في البيئة الرقمية.

¹ - هلاي أسامة، المرجع السابق، ص 720.

خاتمة

أثرت التحولات الاقتصادية و التكنولوجيا الحديثة و استخدام الوسائط الرقمية عبر الوسائط الرقمية التي تمثل تهديدًا للأشخاص الطبيعية و المعنوية. حيث تشكل هذه الدراسة التحليلية للنصوص ، نقطة انطلاق لتطوير القاعدة القانونية المتعلقة بمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، بما يسمح تطوير القواعد الإجرائية للتصدي لهذا النوع من الجرائم. كما سلطنا الضوء على دور القضاء في مراحل التحري والبحث وجمع الأدلة الرقمية بما يتلاءم مع طبيعة الجريمة الإلكترونية ومتطلبات إثباتها.

وقد خلصت الدراسة كذلك إلى أن الجانب الوقائي في جرائم النصب عبر الوسائط الرقمية تمثل جانباً لا يقل أهمية عن الجانب الردعي. كما أن التركيز على الوعي بخطورة التعاملات الرقمية . و بناءً على ما تقدم، يمكننا صياغة زبدة النتائج العلمية التي تم التوصل إليها، مشفوعة بجملة من المقترحات و الاقتراحات الاستشرافية التي نلخصها فيما يلي:

- عدم كفاية النصوص القانونية ،ثبت يقيناً أن المادة 372 من قانون العقوبات باتت عاجزة -بمفردها- عن استيعاب جريمة النصب الإلكتروني، نظراً للشروط المادية الصارمة التي تتطلبها الصياغة الكلاسيكية للنص (مثل وجود مظهر خارجي ملموس ومواجهة مادية)، وهو ما لا يتوافق مع طبيعة السلوك الإجرامي الافتراضي القائم على الخداع البرمجي غير المرئي.

- توصل القضاء و الفقه لكوّن الاعتداء المباشر على الحسابات المالية وتطبيقات الدفع (كقرصنة رموز OTP لبريدي موب) لا يكفي كنصب مجرد، بل ينصرف التكييف القانوني السليم نحو "جرائم المساس بأنظمة المعالجة الآلية للمعطيات البنكية" (المادة 394 مكرر وما بعدها)، نظراً لكون محل الاعتداء هو خوادم وأنظمة رقمية محمية.

- عدم كفاية القواعد الردعية للشخص الطبيعي.

- عدم كفاية القواعد المؤطرة للجريمة في بعدها الدولي بالنظر إلى بطء وتوثيق إجراءات الإنابات القضائية الدولية والمساعدة القانونية المتبادلة.

و بناء على ما سبق نقترح مايلي :

- **فعلى الصعيد التشريعي** ، لابد من الإسراع في تعديل عميق على قانون العقوبات يفرد فرعاً خاصاً ومستقلاً تحت مسمى "النصب المعلوماتي والتصيد الاحتيالي"، يضبط تعريفاتها الفنية ويقر لها عقوبات مشددة ترقى إلى مصاف الجنايات إذا ارتكبت ضمن جماعة إجرامية منظمة أو استهدفت الاقتصاد الوطني. و كذلك العمل على سد الفراغ القانوني المتعلق بـ "انتحال الهوية الرقمية"، بتجريم فعل تقمص حسابات الغير أو صياغة واجهات تطابقية خادعة كفعل مجرم بحد ذاته، دون اشتراط تحقق النتيجة المالية فوراً.
- **أما على المستوى الإجرائي والتقني** ، منح النيابة العامة والضبطية القضائية صلاحية التجميد الإجرائي الفوري والتحفيز للحسابات البريدية والبنكية المشبوهة بمجرد تلقي البلاغ الإلكتروني الموثق، لقطع الطريق أمام سحب الأموال وضمان استرداد حقوق الضحايا قبل تهريبها.
- **على الصعيد الاحترازي** ، تكثيف الحملات الوطنية التوعوية بالمخاطر في البيئة الرقمية ، لترسيخ "الأمن السيبراني الذاتي" لدى المواطن.

المصادر والمراجع

أولاً: قائمة المصادر:

1 / القوانين :

- 1- القانون رقم **09-04** المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر في 16 أوت 2009.
- 2- القانون رقم **15-04** المؤرخ في 1 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع الإلكتروني والمعاملات الإلكترونية، الجريدة الرسمية، العدد 06، المؤرخة في 10 فيفري 2015 .
- 3- القانون رقم **18-05**، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية جريدة رسمية عدد 28 المؤرخة في 16 ماي 2018 .
- 4 - القانون رقم **18-07** المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، المؤرخة في 10 جوان 2018 .

2 / الأمر :

- ¹ - الأمر رقم **66-156** المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، جريدة رسمية عدد 49 المؤرخة في 11 جوان 1966.

3/ المراسيم :

- 1- المرسوم الرئاسي رقم **15-261** المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها المعدل و المتمم ، الجريدة الرسمية، العدد 53، المؤرخة في 08 أكتوبر 2015

ثانياً:المراجع

1/ الكتب

- 1- أحسن بوسقيعة، التحقيق القضائي، دار هومة، الجزائر، 2020 .
- 2- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص: الجرائم الواقعة على الأموال والملكية، دار هومة، الجزائر، طبعة 2021
- 3- جلال ثروت، نظم القسم الخاص في قانون العقوبات: الجرائم الواقعة على الأموال، دار الجامعة الجديدة، الإسكندرية، 2019

- 4- جميل عبد الباقي الصغير، المنظومة القانونية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2017
- 5- طاهري حسين، المرشد في القانون الجنائي الخاص، دار الهدى، عين مليلة، الجزائر، 2020
- 6 - طاهري حسين، المرشد في قانون الإجراءات الجزائية الجزائري، دار الهدى، عين مليلة، الجزائر، 2021
- 7- عبد الله سليمان: دروس في القانون الجنائي الجزائري: القسم الخاص، ديوان المطبوعات الجامعية، الجزائر، 2018
- 8- محمد الأمين الخصري، الجرائم المعلوماتية المستحدثة وآليات مكافحتها، دار الفكر الجامعي، الإسكندرية، 2021 .
- 9- مصطفى طاهر، جرائم الإنترنت وتحديات القانون الجنائي، دار النهضة العربية، القاهرة، 2018.

2/ المقالات

- 1- بوقرة أمين، "جرم النصب الإلكتروني في ظل القانون رقم 18-05 المتعلق بالتجارة الإلكترونية"، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 14، العدد 02، 2022
- 2- هلاي أسامة، "الحماية الجنائية للمستهلك الإلكتروني عبر شبكات التواصل الاجتماعي في الجزائر"، مجلة الفكر العقاري، جامعة قسنطينة 2، المجلد 09، العدد 01، 2023

3/ الرسائل الجامعية:

أ/ أطروحات:

- 1- بن خليفة فريد، الآليات الإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 1، 2021

ب/ رسائل و مذكرات:

- 1- سليمان مريم، الحماية الجزائية للمستهلك عبر وسائل الدفع الإلكتروني في التشريع الجزائري، رسالة ماجستير في القانون الجنائي، جامعة تلمسان، 2023

فهرس المحتويات

العنوان	الصفحة
شكر و تقدير	
الإهداء	
مقدمة	أ - د
الفصل الأول: الإطار النظري لجرائم الاحتيال الرقمي في التشريع الجزائري	
تمهيد	06
المبحث الأول: جريمة النصب الإلكتروني التقليدي	06
المطلب الأول: مفهوم الجريمة وصورها التطبيقية	07
الفرع الأول: تعريف النصب الإلكتروني وتمييزه عن النصب التقليدي	07
الفرع الثاني: صورها التطبيقية	09
المطلب الثاني: الأركان القانونية للجريمة	11
الفرع الأول: الركن المادي	11
الفرع الثاني: الركن غير المادي/المعنوي	13
المبحث الثاني: جريمة التصيد الاحتيالي وانتحال الهوية الرقمية	14
المطلب الأول: ماهية الجريمة وأساليبها التقنية	15
الفرع الأول: تعريف التصيد الاحتيالي وسرقة الهوية الرقمية	15
الفرع الثاني: أساليبها التقنية	17
المطلب الثاني: الأركان القانونية للجريمة	18
الفرع الأول: الركن المادي	19
الفرع الثاني: الركن غير المادي/المعنوي	20
المبحث الثالث: جريمة الاحتيال المالي عبر أنظمة الدفع الإلكتروني وبطاقات الائتمان	21
المطلب الأول: الإطار المفاهيمي للجريمة ومظاهرها	22
الفرع الأول: تعريف الاحتيال على المعطيات البنكية الرقمية	22
الفرع الثاني: صورها التطبيقية في الجزائر	24

25	المطلب الثاني: الأركان القانونية للجريمة
25	الفرع الأول: الركن المادي
27	الفرع الثاني: الركن غير المادي/المعنوي
29	خلاصة الفصل الأول
الفصل الثاني الآليات القانونية والإجرائية ومدى كفايتها لتحقيق الردع	
32	المبحث الأول: السياسة العقابية الموضوعية ومدى تحقيقها للردع
32	المطلب الأول: العقوبات المقررة للأشخاص الطبيعيين وفائدتها الردعية
32	الفرع الأول: العقوبات الأصلية والتكميلية في قانون العقوبات والقانون 04-09
34	الفرع الثاني: ظروف التشديد ومدى ملاءمتها لخطورة الجريمة
34	المطلب الثاني: المسؤولية الجزائية والردعية للشخص المعنوي
35	الفرع الأول: شروط قيام مسؤولية الشركات والمنصات الرقمية
35	الفرع الثاني: تدابير العقاب المقررة للشخص المعنوي
36	المبحث الثاني: الفعالية الإجرائية لآليات البحث والتحري الرقمي
36	المطلب الأول: أساليب التحري الرقمية الخاصة وحجيتها في الإثبات
37	الفرع الأول: أساليب التحري
38	الفرع الثاني: حجية الدليل الرقمي المستمد منها وشروط قبوله قضائياً
39	المطلب الثاني: الدور المؤسسي للأجهزة الأمنية والهيئات المتخصصة
39	الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها
40	الفرع الثاني: الفرق الجنائية الرقمية المتخصصة
40	المبحث الثالث: معوقات ملاحقة جرائم الاحتيال الرقمي وتطبيقها قضائياً
41	المطلب الأول: الصعوبات الفنية والإجرائية العابرة للحدود
41	الفرع الأول: العقوبات الفنية
42	الفرع الثاني: العقوبات الإجرائية

43	المطلب الثاني: الصعوبات المؤسسية والبشرية ونقص الوعي القانوني
43	الفرع الأول: الصعوبات المؤسسية والبشرية
44	الفرع الثاني: نقص وعي الضحايا وثقافة التبليغ وعلاقتها بإفلات الجناة
45	خلاصة الفصل الثاني
47	خاتمة
قائمة المصادر والمراجع	
الفهرس	
ملخص	

ملخص

ملخص

تتناول هذه المذكرة موضوع جرائم النصب والاحتيال عبر الوسائط الرقمية في التشريع الجزائري، باعتبارها من الجرائم المستحدثة التي نتجت عن التطور المتسارع لتكنولوجيات الإعلام والاتصال وانتشار المعاملات الإلكترونية. وتهدف الدراسة إلى تحديد مفهوم هذه الجرائم وبيان خصائصها وصورها المختلفة، مع توضيح أركانها القانونية وتمييزها عن جريمة النصب التقليدية. كما تعرض الإطار التشريعي الذي اعتمدته المشرع الجزائري لمكافحة هذه الجرائم من خلال أحكام قانون العقوبات والقوانين الخاصة ذات الصلة.

وتتناول كذلك وسائل التحري الرقمية وأساليب الإثبات الإلكترونية المعتمدة في الكشف عن هذه الجرائم وملاحقة مرتكبيها. كما تبرز دور الأجهزة الأمنية والهيئات المختصة في الوقاية منها ومكافحتها. وتناقش الدراسة أهم التحديات التقنية والقانونية والمؤسسية التي تواجه جهود المكافحة، خاصة في ظل الطابع العابر للحدود للفضاء الرقمي. وقد خلصت إلى ضرورة تعزيز المنظومة القانونية وتطوير القدرات التقنية والبشرية وتكثيف التعاون الدولي لمواجهة هذه الجرائم بفعالية أكبر.

الكلمات المفتاحية:

جرائم النصب الرقمي، الاحتيال الإلكتروني، الوسائط الرقمية، الجريمة السيبرانية،

Abstract

This dissertation addresses the issue of fraud and scam crimes committed through digital media in Algerian legislation, as one of the emerging forms of crime resulting from the rapid development of information and communication technologies and the widespread use of electronic transactions. The study aims to define these crimes, identify their characteristics and various forms, and explain their legal elements while distinguishing them from traditional fraud offenses. It also examines the legislative framework adopted by the Algerian legislator to combat such crimes through the provisions of the Penal Code and related special laws. Furthermore, the study discusses digital investigation methods and electronic evidence procedures used to detect these crimes and prosecute their perpetrators. It highlights the role of security agencies and specialized institutions in preventing and combating cybercrime. In addition, the research analyzes the main technical, legal, and institutional challenges facing efforts to combat these

offenses, particularly due to their cross-border nature in the digital environment. The study concludes that strengthening the legal framework, developing technical and human capacities, and enhancing international cooperation are essential to effectively address these crimes.

Keywords:

Digital Fraud Crimes, Online Fraud, Digital Media, Cybercrime,.