المجلة الجزائرية للسياسة والأمن
ISSN : 2800-1095

المجلد: 05 – العدد: 01 - جوان 2026
/ ص.ص 219-238

الآليات القانونية والتقنية لمكافحة الاحتيال عبروسائل الدفع الإلكتروني

Legal and technical mechanisms to combat fraud through electronic payment methods

حمزة بوميدونة
جامعة وهران 2 محمد بن احمد، (الجزائر)،
boumidouna.hamza@univ-oran2.dz

تاريخ الاستلام: 2026-06-07 **تاريخ القبول:** 2026-06-12 **تاريخ النشر:** 2026-07-10

الملخص باللغة العربية:

تتناول هذه الدراسة ظاهرة الاحتيال الإلكتروني التي أصبحت تشكل التحدي الأكبر لاستقرار النظام المالي الرقمي، حيث تسعى الدراسة إلى تقديم رؤية متكاملة تجمع بين الحلول التقنية الاستباقية والمواجهة القانونية الزجرية.

كما تبرز الدراسة أن مكافحة الاحتيال لا تتحقق بالتشريع وحده ولا بالتقنية وحدها، بل بوجود منظومة قانونية مرنة تدعم الابتكار التقني وتوفر حماية قانونية ناجزة للمتضررين.

الكلمات المفتاحية:. الاحتيال الإلكتروني- الدفع الرقمي- الأمن السيبراني- الجريمة المعلوماتية- الإثبات الرقمي.

Abstract:

This study addresses the phenomenon of electronic fraud, which has become the greatest challenge to the stability of the digital financial system. The study seeks to present an integrated vision that combines proactive technical solutions and injunctive legal confrontation.

The study also highlights that combating fraud is not achieved by legislation alone or technology alone, but rather by the presence of a flexible legal system that supports technical innovation and provides effective legal protection for those affected.

Keywords: electronic fraud - digital payment - cyber security - information crime - digital proof.

مقدمة:

أصبحت وسائل الدفع الإلكتروني هي العصب النابض للتبادل التجاري والخدماتي. وبالرغم من أن هذا التحول قد وفر كفاءة عالية وسرعة فائقة في نقل الأموال، إلا أنه فتح في المقابل ثغرات أمنية استغلها مرتكبو الجرائم المعلوماتية لتطوير أساليب احتيالية معقدة تتجاوز الحواجز التقليدية للرقابة، ومنه فإن الاحتيال عبر وسائل الدفع الإلكتروني لم يعد مجرد سرقة عابرة، بل أصبح جريمة منظمة تعتمد على الهندسة الاجتماعية والاختراقات البرمجية، مما يضع الثقة في النظام المالي على المحك.

وأمام هذا التهديد المتنامي، وجدت الدول نفسها أمام حتمية مزدوجة تفرض تبني أنظمة أمان استباقية تعتمد على الذكاء الاصطناعي والتشفير، والثانية قانونية، تهدف إلى سد الفراغ التشريعي وتوفير حماية قضائية ناجعة للمستهلك الرقمي ضد مخاطر لم تكن معهودة في القوانين الجنائية التقليدية تكمن في ضرورة حماية الثقة في المعاملات المالية الإلكترونية، خاصة مع تطور أساليب الهندسة الاجتماعية والاختراق التقني التي تتجاوز الحدود الجغرافية للدول، واستعراض دور تقنيات التشفير، التحقق المتعدد العوامل، والاعتماد المتزايد على الذكاء الاصطناعي في رصد العمليات المشبوهة وتحليل سلوك المستخدمين لمنع وقوع الاحتيال قبل اكتماله، إلى جانب تحليل مدى كفاية النصوص التشريعية الحالية (قوانين مكافحة الجرائم المعلوماتية) في تكييف

أفعال الاحتيال الحديثة، كما يناقش معضلة الإثبات الرقمي أمام القضاء وتحديد المسؤولية المدنية بين البنك والعميل في حال وقوع خسائر مالية.

تهدف الدراسة إلى وضع استراتيجية مزدوجة تضمن تحديث القوانين لتواكب الجريمة الرقمية، بالتوازي مع فرض معايير أمنية تقنية صارمة على مزودي خدمات الدفع لتقليل فرص الاختراق.

تتمثل الإشكالية المحورية لهذه الدراسة في التساؤل التالي:

إلى أي مدى استطاعت المنظومة التقنية والتشريعية المعاصرة إرساء توازن فعال بين تشجيع الابتكار في وسائل الدفع الرقمي، وبين توفير آليات حماية وردع كافية لمواجهة الأساليب المتطورة للاحتيال الإلكتروني؟

المبحث الأول: الإطار المفاهيمي للاحتيال الإلكتروني والآليات التقنية للوقاية منه

لا يمكن بناء إستراتيجية قانونية فعالة لمواجهة الاحتيال عبر وسائل الدفع الإلكتروني دون فهم دقيق لطبيعة هذه الجريمة في بيئتها الرقمية ،فالمجرم " المعلوماتي " لا يعتمد على العنف المادي، بل يستغل "الثغرات"؛ سواء كانت ثغرات برمجية في الأنظمة، أو ثغرات بشرية في سلوك المستخدمين.

ومنه، يهدف هذا المحور إلى محاولة تفكيك ظاهرة الاحتيال الإلكتروني من خلال ضبط مفاهيمها الحديثة وتمييزها عن الأشكال التقليدية للاحتيال، مع تسليط الضوء

على أخطر الأساليب الشائعة مثل "التصيد الاحتيالي" و "الهندسة الاجتماعية" التي تلاعبت بعقول المستخدمين قبل أن تتلاعب بأرصدتهم.[1]

كما يسعى هذا المحور إلى استعراض "الخط الدفاعي الأول"؛ وهو المنظومة التقنية، من خلال البحث عن مدى فاعلية أدوات التحقق الحديثة، بدءا من البصمات الحيوية وصولا إلى الدور المحوري للذكاء الاصطناعي في التنبؤ بالعمليات المشبوهة وتحليل أنماط السلوك في أجزاء من الثانية، وذلك لضمان بيئة دفع رقمية تتسم بالموثوقية والاستدامة

المطلب الأول: ماهية الاحتيال عبروسائل الدفع الإلكتروني وصوره الحديثة

سنتطرق في هذا المطلب الى تعريف الاحتيال في البيئة الرقمية وتمييزه عن الاحتيال التقليدي من خلال استعراض صور الاحتيال الحديث .

أولا : تعريف الاحتيال في البيئة الرقمية وتمييزه عن التقليدي:

يعرف الاحتيال الإلكتروني بأنه استخدام الوسائل التقنية والشبكات المعلوماتية للاستيلاء على أموال الغير أو بياناتهم المالية بطرق تدليسية، ويختلف عن الاحتيال التقليدي في عدة نقاط جوهرية:

- يتم الاحتيال عن بُعد دون اتصال جسدي بين الجاني والضحية.[2]
- يمكن تنفيذ عملية احتيال واحدة تستهدف آلاف الضحايا في أجزاء من الثانية.

[1] Les Principes de Base de la Protection du Consommateur dans le Commerce Électronique, guide pour les commerçants et des conseils pour les consommateurs, sont offerts par voie électronique sur le Web.

[2] محمد دباس الحميد، ماركة إبراهيم نينو: **حماية أنظمة المعلومات**، دار الحامد للنشر والتوزيع، عمان 2007، ص 34.

- غالبا ما يكون الجاني في دولة والضحية في دولة أخرى، مما يعقد الملاحقة.

ومنه، فقد تحول الاحتيال في البيئة الرقمية من مجرد فعل مادي بسيط يعتمد على الحيلة اللفظية إلى جريمة فنية معقدة تستهدف سلامة المعطيات والأنظمة الآلية. وفي ظل التشريع الجزائري، لم يعد هذا النوع من الإجرام خاضع حصرا للنصوص التقليدية الواردة في قانون العقوبات، بل أوجد المشرع منظومة قانونية متكاملة تتلاءم وخطورة الوسائل المستخدمة في سلب أموال المستخدمين عبر وسائط الدفع الإلكتروني.

إن تعريف الاحتيال الرقمي في الجزائر يستند أساساً إلى مفهوم "المساس بأنظمة المعالجة الآلية للمعطيات"، وهو ما كرسه القانون رقم 04-15 المعدل والمتمم لقانون العقوبات. فالمحتال هنا لا يستهدف الضحية بشكل مباشر دائماً، بل غالباً ما يوجه نشاطه الإجرامي نحو البيانات البنكية أو الأوامر البرمجية التي تدير عمليات الدفع. ويُمكن استخلاص تعريف قانوني دقيق للاحتيال الإلكتروني في المنظومة الجزائرية بأنه كل فعل عمدي يتضمن الدخول أو البقاء غير المشروع في نظام للمعالجة الآلية للمعطيات المالية، أو إدخال أو تغيير أو حذف للمعطيات، بقصد الاستيلاء على مال الغير أو تحقيق منافع مالية غير مشروعة.

ويتجلى البعد لهذا التعريف في اعتراف المشرع الجزائري بالدليل الرقمي كحجة قانونية، حيث أقر بموجب القانون المدني المادة 323 مكرر 1 حجية الكتابة الإلكترونية شريطة إمكانية تحديد هوية صاحبها وضمان سلامتها، هذا التطور التشريعي سمح بتكييف أفعال مثل "التصيد الاحتيالي" و"تزوير البطاقات البنكية" مثل الذهبية و CIB كجرائم معلوماتية قائمة بذاتها، تخرج عن النطاق الضيق لمادة النصب التقليدية

لتشمل عقوبات مشددة نظراً لخطورة استخدام تكنولوجيا الإعلام والاتصال في تهديد الاستقرار المالي للأفراد والمؤسسات.[1]

علاوة على ذلك، فإن قانون التجارة الإلكترونية رقم 18-05 جاء ليعزز هذا التعريف من خلال وضع إطار قانوني لحماية المستهلك الإلكتروني، معتبراأن أي تلاعب ببيانات الدفع أو انتحال صفة المواقع التجارية الرسمية يمثل خرقصريح للأمان الرقمي يستوجب المساءلة الجزائية والمدنية، وبذلك، فإن الاحتيال في التشريع الجزائري الحديث بات يعرف بطبيعته "التقنية"، حيث لا يكتمل الركن المادي للجريمة إلا بالتدخل غير المشروع في سيرورة البيانات الرقمية التي تمثل القيمة المالية المسلوبة.

ثانيا : **استعراض صور الاحتيال الحديثة:**

تتنوع صور الاحتيال عبر وسائل الدفع الإلكتروني في البيئة الرقمية الجزائرية، متخذةً أشكالاً هجينة تدمج بين الذكاء التقني والتلاعب النفسي، وهو ما جعل المشرع الجزائري يواجه تحدي مستمر في ملاحقة هذه الأنماط المتغيرة التي تتجاوز مفهوم "الحيلة" التقليدي:

1- **التصيد الاحتيالي:** هيرسال رسائل بريدية أو نصية زائفة تحاكي جهات موثوقة (بنوك، شركات دفع) لاستدراج المستخدم لإدخال بياناته السرية، حيث يتم تصميم واجهات إلكترونية أو روابط وهمية تتطابق تماما مع المواقع الرسمية للبنوك أو منصات الدفع. وبمجرد قيام المستخدم بإدخال بيانات بطاقته، يتم الاستيلاء عليها واستخدامها في عمليات شراء أو تحويلات غير مشروعة. هذه الصورة تقع تحت طائلة المادة 394 مكرر وما يليها من قانون العقوبات الجزائري، المتعلقة بالدخول غير المشروع لأنظمة

[1]FredericHuet : La fiscalité du commerce électronique, Paris, Litec, 2000.

المعالجة الآلية للمعطيات، حيث يُعد مجرد "اعتراض" البيانات البنكية أو استيقافها جريمة مكتملة الأركان، حتى قبل البدء في سحب الأموال.[1]

2- **الهندسة الاجتماعية:** تتصدر الهندسة الاجتماعية واجهة هذه الصور، وهي أسلوب لا يستهدف ثغرات النظام المعلوماتي بقدر ما يستهدف "الثغرة البشرية"، فالمحتال هنا يقوم بإيهام الضحية بأنه يمثل جهة رسمية، كأن ينتحل صفة موظف في مؤسسة "بريد الجزائر" أو مؤسسة بنكية، ويطلب بيانات حساسة مثل الرقم السري لبطاقة "الذهبية" أو رمز التحقق OTP بحجة تحديث البيانات أو تقديم جائزة وهمية، هذا النوع من الاحتيال يكيف قانونا في الجزائر كجناية "انتحال صفة" مقترنة بالنصب الإلكتروني، كون الجاني استعمل وسائل معلوماتية لتضليل الضحية والحصول على أمواله.

3- **اختراق الحسابات الرقمية:** كما تبرز صورة تزوير وسائل الدفع وإساءة استعمالها، والتي تشمل استنساخ بيانات البطاقات المغناطيسية أو استخدام بيانات البطاقات المسروقة في عمليات دفع إلكترونية عبر مواقع دولية. وفي ظل القانون 18-05 المتعلق بالتجارة الإلكترونية، أصبح المشرع الجزائري ينظر بصرامة إلى أي استخدام غير مصرح به لبيانات الهوية الرقمية للغير، معتبراً أن أمن المعاملات المالية جزء لا يتجزأ من الأمن السيبراني الوطني. وبذلك، فإن صور الاحتيال المعاصر لم تعد تقتصر على سرقة الرصيد، بل امتدت لتشمل "سرقة الهوية الرقمية" واستغلالها كأداة لتنفيذ جرائم مالية عابرة للحدود، مما يجعل من الدليل الرقمي المستخلص من هذه العمليات المحور الأساسي في أي ملاحقة قضائية.[2]

---

[1] Le rapport de la banque d'Algérie de l'année 2005, Chapitre 06 : Modernisation de l'infrastructure du système bancaire, p 120.

[2] نادر عبد العزيز شافي: **المصارف والنقود الإلكترونية**، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2011.

المطلب الثاني: التدابير التقنية والأمنية لضمان سلامة عمليات الدفع

تنتقل المواجهة هنا من "رد الفعل" إلى "الاستباق"، حيث تلعب التقنية دور الدرع الواقي من خلال:

أولا : أنظمة التحقق من الهوية:

- البصمة الحيوية: استخدام الخصائص البيولوجية الفريدة (بصمة الوجه، العين، الأصبع) التي يصعب تزويرها مقارنة بكلمات المرور التقليدية.
- التحقق المتعدد العوامل:نظام يتطلب أكثر من دليل لإثبات الهوية؛ غالباً ما يجمع بين "شيء تعرفه" (كلمة المرور) و"شيء تملكه" (رمز يصل للهاتف أو توكن رقمي).

ثانيا : دور تقنيات التشفير والذكاء الاصطناعي:

- **التشفير:** نعني بالتشفير تحويل البيانات المالية إلى رموز غير مفهومة أثناء انتقالها عبر الشبكة، بحيث لا يمكن قراءتها حتى لو تم اعتراضها.

الذكاء الاصطناعي ورصد العمليات المشبوهة:

- يعمل الذكاء الاصطناعي عبر خوارزميات تعلم الآلة لتحليل سلوك المستخدم التاريخي.

- إذا تمت محاولة دفع بمبلغ ضخم من موقع جغرافي غريب وفي وقت غير معتاد، يقوم النظام فورا بـ"تجميد" العملية وطلب تحقق إضافي، وهو ما يسمى بأنظمة كشف الاحتيال في الوقت الفعلي.[1]

تنتقل المواجهة في البيئة الرقمية من "الردع القانوني" اللاحق للفعل إلى "التحصين التقني" الاستباقي، حيث تمثل التدابير الأمنية الحديثة حائط الصد الأول الذي يحول دون نفاذ المحتال إلى المنظومة المالية. وفي ظل الاعتماد المتزايد على بطاقة "الذهبية" وخدمات الدفع عبر الهاتف المحمول في الجزائر، أصبحت هذه التدابير ضرورة تقنية تفرضها المعايير الأمنية الدولية والمحلية لضمان سلامة المعاملات.

تتصدر أنظمة التحقق المتعدد العواملهذه التدابير، وهي آلية أمنية تتجاوز الاعتماد التقليدي على كلمة المرور "التي يمكن سرقتها أو تخمينها". تعتمد هذه التقنية على مبدأ "تعدد الأدلة"، حيث يُطلب من المستخدم تقديم عنصرين أو أكثر لإثبات هويته، غالباما يجمع بين ما يعرفه المستخدم رقم التعريف السري وما يملكه (رمز مؤقت OTP يصل عبر رسالة نصية)، هذا النظام يقلص فرص النجاح في عمليات "التصيد الاحتيالي"، فحتى لو استولى المحتال على بيانات البطاقة، فإنه سيصطدم بجدار الرمز المؤقت الذي لا يملكه إلا صاحب الحساب الفعلي.

وعلى صعيد آخر، برزت البصمات الحيوية كأداة لا تقبل التزوير، حيث يتم ربط الوصول إلى التطبيقات البنكية أو الموافقة على الدفع بخصائص بيولوجية فريدة مثل بصمة الإصبع أو التعرف على الوجه،هذه التقنية تمنح "الهوية الرقمية" حصانة ذاتية،

[1]Djamel B: Réforme bancaire en Algérie, site: www.algerie-monde.com/actualite/article495.html

كونها ترتبط مادي ابشخص المستخدم، مما يغلق الباب أمام محاولات "اختراق الحسابات" الناتجة عن تسريب كلمات المرور التقليدية.[1]

أما العقل المدبر لهذه المنظومة الوقائية، فهو الذكاء الاصطناعي الذي يعمل في كواليس عمليات الدفع من خلال خوارزميات "تعلم الآلة"، تقوم الأنظمة البنكية بتحليل "السلوك المعتاد" لكل مستخدم مثل الموقع الجغرافي، توقيت العمليات، وحجم المبالغ المتداولة، وبمجرد رصد أي حركة "شاذة" لا تتوافق مع النمط السلوكي للمستخدم، كأن تتم محاولة دفع من دولة أخرى في وقت متأخر وبمبلغ غير مألوف، يقوم النظام آليا بتجميد العملية وطلب تحقق إضافي.

هذا النوع من الرصد اللحظي يحول دون وقوع الخسارة المالية قبل اكتمالها، محققا بذلك مفهوم "الأمن السيبراني الوقائي" الذي يتكامل مع النصوص القانونية لضمان بيئة دفع رقمية آمنة وموثوقة.

ومنه نخلص إلى أن التقنية هي "خط الدفاع الأول"، ولكنها تظل غير كافية أمام بعض أساليب الخداع النفسي، وهنا تبرز الحاجة الملحّة لاستكمال منظومة الحماية.

المبحث الثاني: المواجهة القانونية للاحتيال الإلكتروني وتوزيع المسؤولية عن مخاطر

استعرضنا في المحور الأول الدرع التقني الذي يسعى لمنع وقوع الجريمة، وعليه سنحاول دراسة نطاق "المواجهة القانونية" التي تبدأ حينما تخفق التدابير الأمنية أو يتم تجاوزها، فالقانون لا يقف مكتوف الأيدي أمام التطور التقني لأساليب الاحتيال، بل

[1] حوالف عبد الصمد: النظام القانوني لوسائل الدفع الإلكتروني، أطروحة دكتوراه غير منشورة، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2015/2014.

يسعى جاهدا لتكييف هذه الأفعال المستحدثة ضمن قوالب جنائية تضمن إنزال العقاب الرادع على الجناة، مع مراعاة الخصوصية الفنية لـ "الدليل الرقمي" الذي يمثل التحدي الأكبر أمام القضاء في إثبات الجريمة ونسبتها لفاعلها.[1]

بيد أن المعضلة لا تتوقف عند الجانب الجزائي فحسب، بل تمتد لتشمل الجانب المدني الذي يمس جوهر الثقة المالية، فبمجرد وقوع الخسارة المالية نتيجة عملية احتيالية، يثور نزاع قانوني معقد حول "توزيع المسؤولية"، هل يتحمل البنك أو مزود خدمة الدفع تبعات الاختراق باعتباره المسؤول عن تأمين المنظومة؟ أم تقع المسؤولية على عاتق العميل الذي ربما فرط في بياناته السرية بدافع الإهمال أو الوقوع في فخ الهندسة الاجتماعية؟

سيتناول هذا المحور بالتحليل الدقيق آليات الملاحقة القضائية في التشريع الجزائري، مع تسليط الضوء على المعايير التي يعتمد عليها القضاء لتحديد "المسؤولية التقنية" و"المسؤولية البشرية"، وصولا إلى صياغة رؤية قانونية تضمن حماية حقوق المتضررين دون إثقال كاهل المؤسسات المالية بالتزامات تفوق طاقتها التقنية، بما يحقق التوازن المنشود في اقتصاد رقمي آمن.

المطلب الأول: النظام القانوني لمكافحة جرائم الاحتيال الالكتروني

أولا: تطور النظام القانوني لمكافحة جرائم الاحتيال الالكتروني

يشكل النظام القانوني لمكافحة الاحتيال الإلكتروني في الجزائر "ترسانة تشريعية" متطورة، انتقلت من مرحلة استعارة النصوص التقليدية إلى مرحلة

[1] هداية بوعزة: النظام القانوني للدفع الإلكتروني - دراسة مقارنة - أطروحة دكتوراه غير منشورة، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2019/2018.

التخصص الرقمي المحض. هذا النظام لا يعمل بمعزل عن الواقع التقني، بل ينسج قواعده من طبيعة "البيانات" باعتبارها أموالامعنوية تستحق الحماية الجنائية ذاتها التي يحظى بها المال المادي.[1]

يتجلى هذا النظام في هيكل ثلاثي الأبعاد، يبدأ بـ التجريم الصارم، حيث لم يعد المشرع يكتفي بوصف "النصب"، بل توسع في المادة 394 مكرر 1 من قانون العقوبات لتجريم مجرد "البقاء" أو "الدخول" غير المصرح به إلى المنظومة البنكية. هذا التوجه التشريعي يعكس فلسفة وقائية، فالقانون الجزائري يعاقب على "اختراق النظام" كجريمة خطر، حتى قبل أن يمتد يد المحتال إلى الرصيد المالي، معتبرا أن مجرد التلاعب بالمعطيات هو اعتداء صارخ على الثقة الرقمية التي تقوم عليها الدولة.

أما البعد الثاني، فيتمثل في آليات التحقيق والتحري الرقمي التي أرسى قواعدها القانون رقم 09-04، إن هذا النظام القانوني استحدث ما يمكن تسميته بـ "الشرطة التقنية"، ومنحها صلاحيات مراقبة الاتصالات واعتراض المعطيات المعلوماتية في الوقت الحقيقي بإذن من القضاء. هذا التطور الإجرائي جاء ليعالج معضلة "الحدود الجغرافية"، حيث سمح المشرع بالتعاون الدولي لملاحقة الجناة الذين يتخذون من السيرفرات الخارجية ملاذ لتنفيذ عمليات احتيال تستهدف المواطنين داخل الجزائر، مما يجعل النظام القانوني نظامعابر للحدود بطبعه.[2]

[1] الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية المحررة في القاهرة بتاريخ 21 ديسمبر 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-251 المؤرخ في 13 ذي القعدة 1435 الموافق لـ 08 سبتمبر 2014، **الجريدة الرسمية** عدد 56.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009، **جريدة رسمية** عدد 47 لسنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وفي البعد الثالث، نجد نظام الإثبات الفني، حيث أحدث المشرع ثورة في قواعد الإثبات الكلاسيكية. فبموجب المادة 323 مكرر 1 من القانون المدني، أصبحت البصمة الإلكترونية، والتوقيع الرقمي، وسجلات الدخول أدلة كاملة الحجية أمام القضاء، ولم يعد ينظر إلى الدليل الرقمي باعتباره "قرينة" بسيطة، بل أصبح "دليل مادي" متى ثبتت نسبته لصاحبه وصحة ظروف تخزينه. هذا النظام القانوني المتكامل يهدف في نهاية المطاف إلى خلق بيئة تشريعية "مرنة"، قادرة على مطاردة المحتال في الفضاء السيبراني بالسرعة ذاتها التي ينفذ بها جريمته، مما يوفر غطاء قانونيا يبعث الطمأنينة في نفوس المستخدمين والمستثمرين على حد سواء.[1]

ثانيا : ازدواجية المنظومة العقابية

تتجسد المواجهة القانونية لظاهرة الاحتيال الإلكتروني في التشريع الجزائري من خلال منظومة عقابية مزدوجة، تجمع بين النصوص العامة لقانون العقوبات والنصوص الخاصة الواردة في القوانين المستحدثة لضبط الفضاء الرقمي. فالمشرع الجزائري لم يعد ينظر إلى الاحتيال عبر وسائل الدفع كجريمة "نصب" بسيطة، بل صنفها ضمن الجرائم التقنية التي تستوجب تكييفاً جنائياً دقيقاً يستوعب خطورة الاعتداء على أنظمة المعالجة الآلية للمعطيات المالية.

يستند التكييف الجنائي لهذه الأفعال أساسا إلى المواد 394 مكرر وما يليها من قانون العقوبات بموجب التعديل رقم 04-15 و 24-06، حيث جرم المشرع كل دخول أو بقاء غير مشروع في نظام المعالجة الآلية للمعطيات، وتزداد العقوبة صرامة إذا نتج عن هذا الدخول تخريب المعطيات أو حذفها أو تعديلها، وهي الحالة التي تنطبق على اختراق

[1] إبراهيم أحمد سعيد زمزمي: القانون الواجب التطبيق في منازعات عقود التجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه غير منشورة، جامعة عين شمس، كلية الحقوق، قسم الدراسات العليا، مصر، 2015.

الحسابات البنكية وتغيير وجهة الأموال. وتصل العقوبات في هذه الحالات إلى الحبس لمدة خمس سنوات وغرامات مالية معتبرة، وتُضاعف العقوبة إذا استهدفت الجريمة المؤسسات الوطنية أو الأنظمة المالية الحيوية، مما يعكس نية المشرع في توفير حماية "فوق عادية" لوسائل الدفع الرقمي.[1]

وعلى صعيد إجرائي، يبرز القانون رقم 09-04 الذي يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كإطار ينظم عملية "الملاحقة القضائية"؛ حيث منح الضبطية القضائية والهيئة الوطنية المعنية صلاحيات واسعة في التفتيش الإلكتروني واعتراض المراسلات الرقمية بإذن قضائي، غير أن التحدي الأكبر يظل في "خصوصية الإثبات الرقمي"، فالدليل في هذه الجرائم هو دليل "افتراضي" قابل للمحو أو التعديل، وهو ما دفع القضاء الجزائري إلى التشدد في معايير قبول الأدلة الرقمية، مشترطا ضمان سلامتها من لحظة الضبط إلى حين عرضها في الجلسة، استنادا إلى المادة 323 مكرر 1 من القانون المدني التي أقرت الحجية القانونية للكتابة الإلكترونية بنفس رتبة الكتابة الورقية، متى استوفت شروط الموثوقية.

أما في شق المسؤولية المدنية، فإن الفصل في النزاعات بين البنك والعميل عند وقوع الاحتيال يستند إلى قواعد المسؤولية العقدية وقانون التجارة الإلكترونية 18-05[2]، فالأصل أن البنك، بصفته مزودا للخدمة، يقع عليه "التزام ببذل عناية مشددة" لتأمين حسابات زبائنه، ويتحمل المسؤولية في حال ثبت وجود ثغرة تقنية في نظامه المعلوماتي، وفي المقابل، يقر القضاء الجزائري بإعفاء البنك من المسؤولية إذا ثبت وقوع "خطأ

[1] القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فيفري 2015، **الجريدة الرسمية** عدد 6 لسنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[2] القانون رقم 18-05 المؤرخ في 24 شعبان 1439 الموافق لـ 10 ماي 2018، **الجريدة الرسمية** عدد 28 لسنة 2018، يتعلق بالتجارة الإلكترونية.

جسيم" من جانب العميل، كإفشاء الرقم السري لبطاقة "الذهبية" لأطراف خارجية أو الاستجابة لروابط تصيد واضحة، معتبراأن إهمال المستخدم يقطع رابطة السببية بين التقصير التقني للبنك والضرر الواقع، مما يجعل توزيع المسؤولية عملية دقيقة تخضع للسلطة التقديرية للقاضي بناءً على الخبرة التقنية المودعة في ملف الدعوى.

المطلب الثاني: المسؤولية المدنية وآليات حماية المتضررين من الاحتيال

أولا : الطبيعة القانونية لجر ائم الاحتيال الالكتروني

تنتقل إشكالية الاحتيال الإلكتروني من أروقة المحاكم الجنائية إلى ساحة القانون المدني بمجرد وقوع الضرر المالي، حيث تبرز معضلة "جبر الضرر" وتحديد الطرف الذي يتحمل التكلفة النهائية للجريمة. وفي ظل التشريع الجزائري، تعد المسؤولية المدنية في هذا المجال مسؤولية ذات طبيعة خاصة، تتجاوز القواعد العامة لتقوم على موازنة دقيقة بين التزامات البنك (كمحترف تقني) وحقوق العميل كمستهلك رقمي.

تستند مسؤولية المؤسسات المصرفية ومزودي خدمات الدفع في الجزائر إلى الالتزام بضمان أمن الأنظمة المعلوماتية، وهو التزام "بتحقيق نتيجة" في أغلب التوجهات القضائية الحديثة، فبموجب القانون 18-05 المتعلق بالتجارة الإلكترونية والقواعد المنظمة للعمل المصرفي، يقع على عاتق البنك أو "بريد الجزائر" عبء إثبات أن منظومته التقنية كانت محصنة بما يكفي وأن الاختراق لم يحدث نتيجة ثغرة في خوادمه. فالبنك هو "حارس" المعطيات والمنفذ التقني للعملية، وأي خلل في نظام التحقق أو تأخر في حظر البطاقة المسروقة بعد التبليغ عنها يرتّب مسؤوليته المدنية الكاملة، مما يلزمه برد المبالغ المسلوبة مع التعويض عن الأضرار اللاحقة بالعميل.[1]

ثانيا : نفي الخطأ و آليات حماية المتضررين

[1] حميزي سيد أحمد: تحديث وسائل الدفع كعنصر لتأهيل النظام المصرفي الجزائري، رسالة ماجستير، جامعة الجزائر، 2003، ص 121.

يبرز دور "الخطأ الجسيم للعميل" كأهم دفع قانوني لإعفاء البنوك من المسؤولية. فالمشرع والقضاء الجزائري يشددان على ضرورة وعي المستخدم، فإذا ثبت أن العميل قد سلم أرقامه السرية طواعية لمحتال عبر رابط مشبوه، أو أهمل في الحفاظ على هاتفه المرتبط بخدمة الدفع، فإن هذه الأفعال تكيف كخطأ الضحية الذي يقطع رابطة السببية بين التقصير التقني والضرر، هنا، تتحول المسؤولية من عاتق المؤسسة إلى عاتق الفرد، استنادا إلى مبدأ أن "الإهمال الفاحش لا يستحق الحماية"، وهو ما يجعل قضايا الهندسة الاجتماعية من أعقد النزاعات المدنية التي تتطلب خبرة فنية للفصل فيها.[1]

أما عن آليات حماية المتضررين، فقد سعى النظام القانوني الجزائري إلى تبسيط سبل الانتصاف، من خلال إقرار "حق الاسترداد" في حالات معينة، وتفعيل دور الهيئات الرقابية لمراقبة مدى التزام البنوك بمعايير الأمن السيبراني، كما تبرز أهمية التأمين على المخاطر الرقمية كآلية حديثة بدأت تلوح في الأفق لتوفير شبكة أمان مالي للمتضررين، بحيث يتم تعويض الضحية دون الدخول في نزاعات قضائية طويلة الأمد حول تحديد المخطئ. وبذلك، فإن المسؤولية المدنية في مواجهة الاحتيال الإلكتروني بالجزائر لم تعد مجرد عقاب للمخطئ، بل أصبحت أداة لتوزيع المخاطر الرقمية بما يضمن استمرارية الثقة في النظام المالي الرقمي الوطني.

الخاتمة:

من خلال دراسةالآليات القانونية والتقنية لمكافحة الاحتيال عبر وسائل الدفع الإلكتروني، نخلص إلى أن العلاقة بين التكنولوجيا والقانون في هذا المجال

[1] المرسوم الرئاسي رقم 19-172 المؤرخ في 3 شوال 1440 الموافق لـ 6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر عدد 37 مؤرخة في 06 جوان 2019.

هي علاقة "سباق مستمر، فبقدر ما تتقدم تقنيات الدفع وتسهل حياة الأفراد، بقدر ما تبتكر العصابات الإجرامية أساليب احتيالية معقدة تتجاوز الحدود التقليدية للدول، ومن أهم النتائج:

- الحماية القانونية وحدها تظل عاجزة ما لم تكن مدعومة بمنظومة تقنية استباقية تعتمد على التشفير القوي والذكاء الاصطناعي لرصد التهديدات قبل وقوعها.

- لا تزال الجريمة المعلوماتية تفرض تحديات جسيمة أمام القضاء، نظراً لسهولة محو الدليل الرقمي أو تزييفه، مما يتطلب تخصص دقيق من جهات التحقيق والمحاكم.

- تحميل البنك أو مزود الخدمة المسؤولية الكاملة قد يحد من الابتكار، بينما تحميل العميل المسؤولية كاملة يزعزع الثقة في النظام المالي، ولذا فإن التوجه الحديث يميل نحو "المسؤولية المشتركة" بناءً على معايير العناية الواجبة.

ومن أهم التوصيات المقترحة:

- ضرورة مراجعة قوانين مكافحة الجرائم المعلوماتية بصفة دورية لتشمل صور الاحتيال الناشئة مثل "التزييف العميق"في انتحال الهويات المالية.

- تفعيل الاتفاقيات الدولية لملاحقة المجرمين السيبرانيين، نظراً للطبيعة العابرة للحدود لجرائم الدفع الإلكتروني.

- الاستثمار في نشر الثقافة التقنية للمستخدمين، حيث يظل "العنصر البشري" هو الحلقة الأضعف التي يستهدفها المحتالون عبر الهندسة الاجتماعية.

- فرض معايير أمنية تقنية صارمةمثل بروتوكولات على كافة شركات الوساطة المالية الناشئة قبل منحها تراخيص العمل.

قائمة المصادر والمراجع:

- النصوص القانونية:

- القانون رقم 00-03 الملغى المؤرخ في 5 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، جريدة رسمية عدد 48 لسنة 2000.
- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية عدد 71 لسنة 2004، المتمم لقانون العقوبات.
- القانون رقم 08-01 المؤرخ في 23 يناير 2008 المتمم للقانون رقم 83-11 المؤرخ في 02 جويلية 1983 والمتعلق بالتأمينات الاجتماعية، جريدة رسمية عدد 04 لسنة 2008.
- القانون رقم 09-04 المؤرخ في 5 أوت 2009، جريدة رسمية عدد 47 لسنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فيفري 2015، الجريدة الرسمية عدد 6 لسنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.
- القانون رقم 18-05 المؤرخ في 24 شعبان 1439 الموافق لـ 10 ماي 2018، الجريدة الرسمية عدد 28 لسنة 2018، يتعلق بالتجارة الإلكترونية.
- المرسوم الرئاسي رقم 19-172 المؤرخ في 3 شوال 1440 الموافق لـ 6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر عدد 37 مؤرخة في 06 جوان 2019.

- الكتب:

- نادر عبد العزيز شافي: المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2011.

- محمد دباس الحميد، ماركة إبراهيم نينو: حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان 2007.

- حسن طاهر داوود: الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة فهد الوطنية، الرياض.207933098

- الاتفاقيات:

- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية المحررة في القاهرة بتاريخ 21 ديسمبر 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-251 المؤرخ في 13 ذي القعدة 1435 الموافق لـ 08 سبتمبر 2014، الجريدة الرسمية عدد 56.

- المذكرات الجامعية:

- حوالف عبد الصمد: النظام القانوني لوسائل الدفع الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2015/2014.

- هداية بوعزة: النظام القانوني للدفع الإلكتروني - دراسة مقارنة - أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2019/2018.

- إبراهيم أحمد سعيد زمزمي: القانون الواجب التطبيق في منازعات عقود التجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، كلية الحقوق، قسم الدراسات العليا، مصر، 2015.

- حميزي سيد أحمد: تحديث وسائل الدفع كعنصر لتأهيل النظام المصرفي الجزائري، رسالة ماجستير، جامعة الجزائر، 2003.

- المو اقع الإلكترونية:

-www.algerie-monde.com/actualite/article495.html

https://journals.nauss.edu.sa/index.php/AJSS/article/view/1920/1209

المراجع الأجنبية:

- Djamel B: Réforme bancaire en Algérie, site: www.algerie-monde.com/actualite/article495.html
- Le rapport de la banque d'Algérie de l'année 2005, Chapitre 06: Modernisation de l'infrastructure du système bancaire, p 120.
- FredericHuet : La fiscalité du commerce électronique, Paris, Litec, 2000.
- Les Principes de Base de la Protection du Consommateur dans le Commerce Électronique, guide pour les commerçants et des conseils pour les consommateurs, sont offerts par voie électronique sur le Web.