

جامعة سعيدة، الدكتور مولاي الطاهر



كلية الحقوق والعلوم السياسية
قسم القانون الخاص

الحماية القانونية للمستهلك في مواجهة مخاطر الدفع الإلكتروني

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في العلوم السياسية
تخصص قانون أعمال

• تحت إشراف الأستاذ:

• سليمان جميل

• من إعداد الطالبة:

• باشي صارة

أعضاء لجنة المناقشة

رئيساً	جامعة سعيدة	أستاذ محاضر	لربي مكي
مشرفاً ومقرراً	جامعة سعيدة	أستاذ محاضر	سليمان جميل
عضواً	جامعة سعيدة	أستاذ محاضر	مغربي قويدر

السنة الجامعية: 2026/2025



جامعة سعيدة، الدكتور مولاي الطاهر



كلية الحقوق والعلوم السياسية
قسم القانون الخاص

الحماية القانونية للمستهلك في مواجهة مخاطر الدفع الإلكتروني

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في العلوم السياسية
تخصص قانون أعمال

• تحت إشراف الأستاذ:

• سليمان جميل

• من إعداد الطالبة:

• باشي صارة

أعضاء لجنة المناقشة

رئيساً	جامعة سعيدة	أستاذ محاضر	لربي مكي
مشرفاً ومقرراً	جامعة سعيدة	أستاذ محاضر	سليمان جميل
عضواً	جامعة سعيدة	أستاذ محاضر	مغربي قويدر

السنة الجامعية: 2026/2025

إِهْدَاء

إلى من جعلها الله جنّةً تحت أقدامها.. إلى سر وجودي ونور عيني.. إلى التي رافقتني منذ صغري وكانت لي والعُدد، ولم تملّ يوماً من كثرة دعواتها لي..

"أمي" الحبيبة

أهديكِ ثمرة جهدي هذا، فأنتِ البطلة الحقيقية وراء كل نجاح حققته، وبدون حبكِ وتضحياتكِ التي لا تُعد ولا تُحصى، ما كنتُ لأصل إلى هنا. لكِ في قلبي مكانة لا يملؤها أحد، وشكر لا توفيه الكلمات.

إلى من كان لي فخراً وذخراً، ومن بذل الغالي والنفيس لإنارة دربي..

"أبي" الحبيب

شكراً لك لأنك كنت السند المتين الذي لم يمل، ولأنك وفرت لي كل سبل النجاح والراحة، جزاك الله عني كل خير.

إلى كل من سكن قلبي، وأهداني تشجيعاً أو دعوةً بظهر الغيب.. أهديكم هذا النجاح.

باشي صارة

شكر وفلک

بقلبٍ يملؤه الامتتان، أقدم بجزيل الشكر والتقدير إلى الأستاذة الفاضلة والمشفرة القديرة:
سليمانى جميلة.

التي لم تبخل عليّ بتوجيهاتها السديدة، وصبرها الجميل، ونصائحها القيمة التي كانت
بمثابة المنارة التي أضاءت لي عتمة البحث. لقد كنت يا أستاذتي نعم القدوة في التواضع
والعلم، فلک منى كل معانى الاحترام والتقدير.

كما يمتد شكري إلى كل من ساندني من قريب أو بعيد، وإلى أعضاء لجنة المناقشة
الموقرين لقبولهم تقييم هذا العمل المتواضع.

باشى صارة

قائمة المختصرات:

د.ج.ج: دار الجامعة الجديدة.

ج.ر: الجريدة الرسمية.

م.ع.ب.د: المركز العربي للبحوث والدراسات.

م.ا.ح: مكتبة الآلات الحديثة.

د.ن.ع: دار النهضة العربية.

د.ف.ج: دار الفكر الجامعي.

د.م.ج: دار المطبوعات الجامعية.

د.ط: دون طبعة.

ط: طبعة.

ص: صفحة.

ق.إ.م.إ: قانون اجراءات مدنية وإدارية.

ق.إ.ج: قانون إجراءات جزائية.

مقدمة

يُعدّ الانتقال الجذري نحو الرقمنة الشاملة والتحول الرقمي المتسارع السمة الأبرز والعمود الفقري لكافة التحولات الاقتصادية والاجتماعية التي يشهدها العصر الراهن، حيث لم يعد الاعتماد على التقنيات الحديثة والأنظمة الذكية مجرد خيار ثانوي أو رفاهية تقنية، بل أضحت في الآونة الأخيرة ضرورة حتمية ومطلباً استراتيجياً لضمان كفاءة ومرونة الخدمات العامة والخاصة على حد سواء، بما يتماشى مع معايير الجودة العالمية. وفي قلب هذا التحول الرقمي المتسارع الذي مسّ عصب الحياة اليومية، برزت المنظومة المصرفية والمالية كأحد أكثر القطاعات حيوية وتأثراً بهذا التطور التقني الهائل، مفسحة المجال لظهور أجيال جديدة ومبتكرة من الخدمات المالية الرقمية التي تهدف في جوهرها إلى تجاوز كافة القيود التقليدية المرتبطة بالتعاملات الورقية والمادية البطيئة، والتي أصبحت لا تتماشى إطلاقاً مع سرعة وتيرة العصر الحالي المتسم بالتدفق اللحظي للمعلومات والأموال. وتتمحور هذه الدراسة الأكاديمية بشكل دقيق ومركز حول "نظام الدفع الإلكتروني" الذي لا يمكن حصره في مجرد آلة تقنية، بل يُعرف قانوناً واصطلاحاً بأنه منظومة متكاملة من الأدوات التقنية والإجراءات التنظيمية والأنظمة البرمجية المحمية التي تتيح نقل القيم المالية وتسوية كافة الالتزامات التعاقدية بين الأطراف عبر وسائط إلكترونية مشفرة، مما يؤدي حتماً إلى إلغاء الحاجة للتعامل المادي المباشر بالنقد ويوفر بيئة افتراضية آمنة للتبادل المالي تضمن السرعة والدقة والشفافية في آن واحد¹.

ويهدف البحث من خلال هذا الإطار المفاهيمي الواسع إلى تسليط الضوء على كيفية مواءمة النصوص التشريعية والمنظومة القانونية مع حجم المخاطر الرقمية والتهديدات السيبرانية المستحدثة التي باتت تواجه المستهلك في تعاملاته المالية اليومية، خاصة في ظل الطفرة التشريعية التي شهدتها الجزائر بصدور القانون رقم 18-05 المتعلق بالتجارة الإلكترونية²، والذي جاء كاستجابة

(1) محمد الأمين الخرشاوي، الآليات القانونية لحماية المستهلك في عقود التجارة الإلكترونية د.ف.ج، الإسكندرية، 2020، ص 45.

(2) القانون رقم 18-05، المؤرخ في 10 مايو 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادر بتاريخ 16 مايو 2018.

لتحديد القواعد الأساسية لهذا النوع من المعاملات الرقمية وتحديد التزامات الأطراف في الفضاء الافتراضي. كما يسعى البحث وبشكل معمق لتحليل الأطر والضوابط القانونية الجديدة التي استحدثها المشرع مؤخراً من خلال الأمر رقم 09-23 المتضمن قانون النقد والصرف، وهو النص الذي استهدف بشكل صريح تعزيز مستويات أمن المدفوعات وحماية الأنظمة المصرفية الوطنية من الاختراقات المتطورة، وتكريس حماية قانونية فاعلة لأرصدة الزبائن ضد المخاطر التقنية المتزايدة³.

وتنبثق أهمية هذا البحث من كونه يعالج موضوعاً حيوياً يمس جوهر "الثقة الرقمية" في النظام المالي الوطني؛ فمن الناحية النظرية يطمح البحث لإثراء المكتبة القانونية بضبط تكييف الجرائم المعلوماتية المعقدة التي تثير إشكالات فقهية وقضائية معاصرة، أما من الناحية العملية فيهدف البحث إلى تزويد المستهلك بالإطار القانوني الواضح الكفيل بحماية حقوقه وتبيان كافة المسارات الإجرائية والقضائية المتاحة لجبر أضراره في حالة التعرض لأي شكل من أشكال القرصنة أو الاحتيال المالي الإلكتروني، وصولاً إلى تكريس مبدأ الأمن التعاقدي الذي يضمن استقرار المعاملات الرقمية وحماية الطرف الضعيف من تغول المخاطر التقنية العابرة للحدود.

لقد استند اختيارنا لهذا الموضوع والتعمق في دراسته إلى جملة من المبررات المنطقية؛ فمن الناحية الموضوعية فرض التنامي الرهيب لظاهرة الإجرام المعلوماتي والاعتداءات المستحدثة على أرصدة المستهلكين ضرورة ملحة لتقييم مدى نجاعة النصوص الوطنية. أما من الناحية الذاتية، فقد دفعنا الشغف الأكاديمي والرغبة العميقة في التخصص في "قانون الأعمال الرقمي" إلى تقديم إسهام يحلل الثغرات القانونية في ظل توجه الدولة نحو تعميم الرقمنة المالية. وانطلاقاً من هذه المعطيات، تتبلور إشكالية البحث المحورية في التساؤل الجوهرية التالي:

(1) الأمر رقم 09-23، المؤرخ في 21 يونيو 2023، المتضمن قانون النقد والمصرفية، ج.ر، العدد 43، الصادر بتاريخ 27 يونيو 2023.

ما مدى فعالية الحماية القانونية المقررة للمستهلك من مخاطر الدفع الإلكتروني؟

وللإحاطة بجوانب هذه الإشكالية، نطرح مجموعة من التساؤلات الفرعية:

• كيف كيّف المشرع الجزائري الجرائم المرتبطة بالدفع الإلكتروني وما هي خصوصية إثباتها جنائياً؟

• ما هي حدود مسؤولية المؤسسات المالية والمصرفية في تعويض المستهلك عن الخروقات التقنية؟

• ما مدى نجاعة الآليات الوقائية والقضائية المقررة لضمان الأمن الرقمي للمستهلك؟

وللإجابة على هذه الإشكالية، اعتمدنا مجموعة من المناهج؛ حيث ارتكزنا على المنهج الوصفي لاستعراض الأطر النظرية، متبوعاً بالمنهج التحليلي لتحليل النصوص القانونية، مع الاستعانة بالمنهج المقارن للاستفادة من التجربة الفرنسية. وبالرغم من أهمية الموضوع، واجهنا صعوبات متباينة أهمها ندرة المراجع المتخصصة، بالإضافة إلى عقبة "السرية المصرفية" التي جعلت من الحصول على نماذج لأحكام قضائية أمراً معقداً. واستناداً لما تقدّم، اعتمدنا على خطة مقسمة إلى فصلين؛ حيث أفردنا الفصل الأول بعنوان "التكليف الجنائي لجرائم الدفع الإلكتروني"، وقسمناه بدوره إلى مبحثين؛ يتناول المبحث الأول: ماهية نظام الدفع الإلكتروني وتصنيف الجرائم المرتبطة به، في حين يركز المبحث الثاني على: البنيان القانوني للجريمة الرقمية وقواعد الإثبات الجنائي. بينما خصصنا الفصل الثاني لـ "النظام القانوني لحماية المستهلك في الدفع الإلكتروني"، والذي يندرج تحته مبحثان؛ ينصب المبحث الأول على: النظام القانوني لمساءلة الأطراف عن أضرار الدفع الإلكتروني، بينما يُعالج المبحث الثاني: القواعد الوقائية والتسوية القضائية لمنازعات الدفع.

الفصل الاول

التكليف الجنائي لجرائم الدفع الالكتروني

تعد عملية التحول الرقمي في المعاملات المالية من أبرز تحديات العصر الحديث، حيث أفرزت نظاماً مستحدثة للوفاء تتجاوز الأطر التقليدية للنقود الورقية، وهو ما يصطلح عليه بـ "الدفع الإلكتروني". بيد أن هذا التطور التقني، ورغم ما يحمله من مزايا اقتصادية، قد فتح آفاقاً جديدة لأنماط إجرامية مستحدثة تتخذ من الفضاء السيبراني مسرحاً لها، مما وضع المشرع والقاضي الجنائي أمام تحديات جسيمة تتعلق بمدى استيعاب النصوص التقليدية لهذه الجرائم. إن دراسة هذا الإطار لا تستقيم دون تأصيل مفاهيمي يحدد ماهية هذه الوسائل وأطراف العلاقة القانونية فيها، خاصة في ظل التحديات التي يفرضها التكييف الجنائي لإضفاء الحماية اللازمة على البيانات والأنظمة المعلوماتية، وتحديد الطبيعة القانونية للاعتداءات التي تطل الزمة المالية الرقمية.

وبناءً على ما تقدم، وللإحاطة بالجانب النظري والجنائي لهذه المعاملات، سنعتمد في دراستنا لهذا الفصل على التقسيم التالي:

المبحث الأول: ماهية نظام الدفع الإلكتروني وتصنيف الجرائم المرتبطة به.

المبحث الثاني: أركان الجريمة الرقمية وقواعد الإثبات الجنائي.

المبحث الأول: ماهية نظام الدفع الإلكتروني وتصنيف الجرائم المرتبطة به

تعتبر دراسة المنظومة القانونية للدفع الإلكتروني مدخلاً حتمياً لفهم الآليات الجنائية الكفيلة بحمايتها، إذ لا يمكن تكييف الاعتداءات التي تطال هذه المنظومة دون الإحاطة بمقوماتها الذاتية وخصائصها الفنية والقانونية التي تميزها عن وسائل الوفاء التقليدية كعلاقة عقدية وتقنية متكاملة. وعليه، يسعى هذا المبحث لتأصيل نظام الدفع الرقمي وتصنيف الاعتداءات التي تمس بسلامة بياناته، وذلك وفق التقسيم التالي:

المطلب الأول: المفهوم القانوني للدفع الإلكتروني وأطراف العلاقة.

المطلب الثاني: التصنيف القانوني لأبرز جرائم الدفع الإلكتروني.

المطلب الأول: المفهوم القانوني للدفع الإلكتروني وأطراف العلاقة

يتطلب الإلمام بالنظام القانوني للدفع الإلكتروني تحديد ماهيته القائمة على استبدال الوسائط المادية ببيانات رقمية مشفرة، مما أدى لبروز أدوات وفاء ذات طبيعة فنية وقانونية خاصة؛ كما يستوجب تحليل شبكة العلاقات التعاقدية التي تربط المستهلك الإلكتروني بالمؤسسات المصرفية والوسطاء. وعليه، سنقسم دراسة هذا المطلب إلى فرعين:

الفرع الأول: تحديد مفهوم الدفع الإلكتروني وخصائصه.

الفرع الثاني: تحليل أطراف العلاقة القانونية.

الفرع الأول: تحديد مفهوم الدفع الإلكتروني وخصائصه

تقتضي الإحاطة بمنظومة الدفع الإلكتروني ضبط خلفيتها المفاهيمية وتحديد ركائزها الفنية، تمييزاً لها عن أساليب الوفاء التقليدية؛ وعليه، سنعمل في هذا الفرع على تأصيل تعريفها فقهاً وتشريعياً، واستعراض عناصرها وأنواع أدواتها وصولاً لاستخلاص خصائصها المميزة، وذلك وفق الآتي:

أولاً: التعريف الفقهي والتشريعي للدفع الإلكتروني.

ثانياً: العناصر الأساسية لعملية الدفع الرقمي.

ثالثاً: أنواع أدوات الدفع الإلكتروني (البطاقات، المحافظ، التحويلات).

رابعاً: الخصائص القانونية المميزة لعملية الدفع الإلكتروني.

أولاً: التعريف الفقهي والتشريعي للدفع الإلكتروني

أ/- التعريف الفقهي للدفع الإلكتروني:

لم يتفق الفقه القانوني على وضع تعريف جامع ومانع لمصطلح الدفع الإلكتروني، ويعود ذلك بالدرجة الأولى إلى الطبيعة المتغيرة والمتطورة للوسائط التقنية، فضلاً عن تداخل الأبعاد الاقتصادية والتقنية والقانونية في هذه العملية؛ إذ يواجه الفقهاء تحدياً مستمراً في الإحاطة بكافة الجوانب الإجرائية التي تستحدثها التكنولوجيا المالية بصفة يومية، مما جعل المحاولات الفقهية تتأرجح بين الانغلاق على الوسيلة التقنية وبين الانفتاح على الآثار القانونية المترتبة عنها. ويعد هذا التباين والبحث عن مصطلح دقيق أمراً جوهرياً في الدراسات القانونية، لكونه يمثل القاعدة الأساسية التي يبنى عليها تحديد طبيعة المسؤولية وحقوق الأطراف المتعاقدة في الفضاء الرقمي، وهو ما يمكن استخلاصه من خلال تتبع أهم المقاربات الفقهية التي انقسمت إلى اتجاهين أساسيين:

1- الاتجاه الضيق (المقاربة التقنية): ركز أنصار هذا الاتجاه على الوسيلة المستخدمة في تنفيذ العملية، حيث عُرِفَ الدفع الإلكتروني بأنه مجرد استخدام للوسائط التكنولوجية الحديثة كالحاسب الآلي وشبكات الاتصال لتنفيذ عمليات نقل وتحويل الأموال. ويرى أصحاب هذا الرأي أن الدفع الإلكتروني هو مجرد عملية فنية يتم من خلالها تحويل الالتزام النقدي من صيغته المادية الورقية إلى صيغة رقمية مشفرة قابلة للتداول عبر الفضاء السيبراني.¹

غير أن هذا التعريف واجه انتقادات قانونية، كونه حصر العملية في جانبها الفني البحت، وأغفل الأبعاد التعاقدية والالتزامات المتبادلة، وكذا المسؤولية القانونية الناشئة عن هذا النظام تجاه أطراف العلاقة، غير أن هذا التعريف واجه انتقادات قانونية، كونه حصر العملية في جانبها الفني البحت، وأغفل الأبعاد التعاقدية والالتزامات المتبادلة، وكذا المسؤولية القانونية الناشئة عن هذا النظام تجاه أطراف العلاقة.

2) الاتجاه الواسع (المقاربة النظامية): ذهب هذا الاتجاه إلى أبعد من الجانب التقني، لينظر إلى الدفع الإلكتروني كمنظومة قانونية وتقنية متكاملة. ويُعرّف وفق هذا المنظور بأنه منظومة تعاقدية تهدف إلى تسوية المعاملات المالية الناتجة عن تبادل السلع والخدمات عبر بيئة رقمية، بحيث تحل القيم الرقمية محل النقود القانونية في الوفاء والإبراء. ويؤكد الفقهاء هنا على أن الدفع الإلكتروني يمثل نظاماً قانونياً تنشأ عنه التزامات متقابلة بين الدافع والمستفيد والمؤسسة المصرفية؛ مما يمنحه قوة إبرائية كاملة للذمة المالية، ويجعله وسيلة وفاء قانونية معترفاً بها²، وهو ما يكرس استقلالية هذه المنظومة عن القواعد التقليدية للوفاء، باعتبارها توفر حماية قانونية مزدوجة تضمن من جهة سرعة التداول المالي.

(1) عبد الصمد حوالف، النظام القانوني لوسائل الدفع في الجزائر: دراسة مقارنة، د.ط، د.ج.ح، الإسكندرية، 2017، ص 30.

(2) المرجع نفسه

ثانيا: التعريف التشريعي للدفع الإلكتروني: تباينت المسالك التشريعية في تعريف الدفع الإلكتروني؛ فبينما فضلت بعض التشريعات وضع تعريفات مستقلة، ذهبت أخرى إلى إدراجه ضمن القواعد العامة المنظمة للتجارة الإلكترونية:

أ) موقف المشرع الجزائري:

إن المشرع قد بنى مقاربة عملية ركزت على "وسيلة الدفع" كأداة جوهرية للعملية. وقد عرفتها المادة 2 من القانون 05-18 بأنها كل وسيلة تسمح لصاحبها بإجراء دفع عن بعد عبر منظومة إلكترونية². ويلاحظ أن المشرع الجزائري صاغ هذا التعريف بمرونة واسعة ليستوعب كافة التطورات التقنية الحالية والمستقبلية، سواء تعلق الأمر بالبطاقات البنكية، الهواتف الذكية، أو التحويلات المصرفية الرقمية. كما وضع ضابطاً قانونياً هاماً يتمثل في ضرورة إجراء هذه العمليات عبر مقدم خدمات دفع معتمد، وذلك لضمان الرقابة المالية وتحقيق الأمن المعلوماتي للمتعاملين.

ب) موقف التشريعات المقارنة والاتفاقيات الدولية: تميز التشريع الفرنسي في التقنين النقدي والمالي بدقة أكبر، حيث وضع قواعد واضحة لعمليات الدفع. كما نصت المادة L133-3³ منه على أن عملية الدفع هي فعل يتمثل في نقل أموال، بناءً على طلب الدافع أو المستفيد، وبشكل مستقل عن الالتزامات الأساسية القائمة بينهما. وتكمن أهمية هذا التعريف في تكريسه لمبدأ

(1) المادة 2، القانون رقم 05-18 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 مايو 2018=

(2) المرجع السابق، ص 30.

استقلال عملية الوفاء الإلكتروني عن العقد الأصلي. وقد عرف قانون "اليونيسترال" النموذجي التحويلات الإلكترونية بأنها سلسلة من العمليات تبدأ بأمر دفع يصدره المرسل بقصد وضع أموال تحت تصرف المستفيد، مما يعزز فكرة تسلسل الإجراءات التقنية والقانونية¹.

ثالثاً: أنواع وأدوات الدفع الإلكتروني (البطاقات، المحافظ، التحويلات): لا يمكن حصر أدوات الدفع الإلكتروني في قالب واحد، فهي تتطور بتطور التقنيات والجهات المصدرة لها، وهو ما جعلها المحرك الأساسي لانتشار التجارة الإلكترونية. و تقسيم أبرز هذه الأدوات من الناحية القانونية والتقنية إلى :

أ/- بطاقات الدفع الإلكتروني (Les Cartes de Paiement):

تعد الوسيلة الأكثر تداولاً في الواقع العملي، وهي عبارة عن أداة بلاستيكية ممغنطة أو مزودة بشريحة ذكية، تمنح حاملها الحق في السحب النقدي أو الوفاء بقيمة مشترياته. ومن خلال استقراء الواقع المصرفي، نجد أنها تنقسم من حيث طبيعتها الائتمانية إلى نوعين:

1)-بطاقات الحسم أو السحب الفوري (Debit Cards):

وهي المرتبطة مباشرة برصيد العميل في حسابه الجاري، حيث يتم خصم المبلغ فوراً بمجرد إعطاء أمر الدفع إلكترونياً، وفي حالة عدم كفاية الرصيد ترفض العملية تلقائياً من طرف النظام البنكي²، إذ تعتمد هذه الوسيلة على تقنية "الاستعلام اللحظي" التي تفرض على المؤسسة المصرفية التحقق من توافر المؤونة الكافية قبل إتمام القيد المحاسبي، مما يجعلها أداة وفاء آمنة تحد من مخاطر الائتمان وتمنع العميل من تجاوز سقف أرصده النقدية المتاحة فعلياً.

(1) قانون اليونيسترال النموذجي بشأن التحويلات الدولية، 1992، ص 11.

(2) شمة جاسم سيف الدين السليطي، الجوانب القانونية لوسائل الدفع الإلكترونية، مذكرة ماجستير، كلية القانون، جامعة قطر، 2021، ص 20.

2- بطاقات الائتمان (Credit Cards):

وهي التي تمنح العميل "خطأ ائتمانياً" (قرضاً قصير الأجل)، حيث يقوم البنك بالوفاء للمستفيد نيابة عن العميل، على أن يسدد الأخير المبالغ في مواعيد لاحقة. وتبرز أهميتها كأداة "وفاء وائتمان" في آن واحد، مما يسهل المعاملات التجارية الكبرى¹.

ب/- المحافظ الإلكترونية (E-Wallets):

تمثل جيلاً متطوراً من وسائل الوفاء، وهي تطبيقات برمجية على الأجهزة الذكية تسمح بتخزين بيانات البطاقات أو شحن أرصدة مسبقة الدفع. وتكمن الميزة القانونية للمحفظة في توفير "حماية إضافية" للمستهلك؛ إذ لا يضطر العميل للإفصاح عن بيانات حسابه الأصلي عند كل عملية، بل يكفي باستخدام بيانات المحفظة المشفرة، مما يقلل من مخاطر القرصنة².

ج/- التحويلات والعمليات المصرفية الإلكترونية (E-Transfers):

تتمثل في أوامر الدفع التي يصدرها العميل لمصرفه لنقل الأموال إلكترونياً (الصيرفة عبر الإنترنت). وتعتمد هذه الوسيلة على بروتوكولات تشفير معقدة لضمان سلامة نقل البيانات المالية. وقد نافست هذه الوسيلة "الشبكات الورقية" نظراً لسرعتها اللحظية، خاصة في المعاملات العابرة للحدود التي تتطلب أماناً عالياً وسرعة في التسوية³.

(1) المرجع نفسه ص ٢١.

(2) طارق محمد حمزة، النقود الإلكترونية كإحدى وسائل الدفع (تنظيمها القانوني والمسائل الناشئة عن استعمالها)، ط 1، منشورات زين الحقوقية، بيروت، 2011، ص 24.

(3) عطية سالم، بطاقات الدفع الإلكترونية وأهميتها في عصرنا الحديث، منشورات معهد الدراسات المصرفية، القاهرة، 1998، ص 121.

رابعاً: الخصائص القانونية المميزة لعملية الدفع الإلكتروني: تنفرد عملية الدفع الإلكتروني بمجموعة من الخصائص الذاتية التي تخرجها من إطار الوفاء التقليدي إلى فضاء "الرقمنة القانونية"، وهذه الخصائص ليست مجرد سمات فنية بل هي ركائز تؤثر في تكييف المسؤولية، ومن أبرزها:

أ/- السرعة والآنية (L'instantanéité):

تعد الميزة الأبرز، حيث يتم نقل القيم المادية في أجزاء من الثانية. وقانوناً، تقلب هذه الخاصية مفاهيم "زمن الوفاء"؛ ففي البيئة الرقمية، يعد الوفاء نهائياً بمجرد صدور التأكيد الإلكتروني، مما يقلص إمكانية الرجوع في العملية أو إلغائها، وهذا ما يفرض على البنوك التزامات أمنية صارمة لتدارك أي خطأ فوري.¹

ج/- الطابع العابر للحدود (Transnationalité):

تتميز هذه الوسائل بكسر الحواجز الجغرافية عبر شبكة الإنترنت. وهذا يطرح إشكالات في القانون الدولي الخاص حول "تنازع القوانين" وتحديد "مكان وقوع الجريمة"؛ إذ غالباً ما تنشبت أطراف العملية بين دول مختلفة، مما يتطلب حماية قانونية تتجاوز الحدود الوطنية لضبط الجناة دولياً²، وهذا ما يجعل من الفضاء السيبراني بيئة خصبة للمجرمين الذين يستغلون غياب التنسيق التشريعي بين الدول، مما يضع المشرع الجزائري أمام حتمية تفعيل اتفاقيات التسليم والمساعدة القضائية الدولية لضمان محاصرة الجريمة الإلكترونية في منابعها وأينما امتدت آثارها المادية.

(1) عبد الصمد حوالف، النظام القانوني لوسائل الدفع في الجزائر: دراسة مقارنة، د.ط، د.ج.ج، الإسكندرية، 2017، ص 35.

(2) ذكري عبد الرزاق محمد، النظام القانوني للبنوك الإلكترونية، د.ج.ج، الإسكندرية، 2010، ص 38.

د/- التقنية والاعتماد على التشفير (Cryptage):

لا وجود لدفع إلكتروني دون "وسيط تقني" ونظام أمان يعتمد على الخوارزميات. هذه الخاصية جعلت من "الالتزام بالأمن" التزاماً جوهرياً يقع على عاتق البنك. فسلامة المعاملة ترتبط بقوة "الجدار التقني"، حيث يصبح الرقم السري أو التوقيع الإلكتروني هو الحجة الوحيدة والقوية لإثبات صدور الإرادة بالدفع.¹

الفرع الثاني: تحليل أطراف العلاقة القانوني

لا تكتمل دراسة نظام الدفع الإلكتروني بالوقوف على جانبه التقني فحسب، بل يستوجب الأمر تحليل المراكز القانونية للأطراف الفاعلة في هذه العملية؛ حيث تتقاطع إرادة المستهلك كطرف ضعيف مع التزامات البنوك والوسطاء التقنيين وكذا دور التاجر الإلكتروني. وعليه، سنحاول في هذا الفرع تسليط الضوء على هذه الأدوار المتباينة، مع تمييز الطبيعة الخاصة للجرائم الناشئة عن هذه العلاقة مقارنة بالجرائم التقليدية، وذلك وفق الأجزاء التالية:

أولاً: المركز القانوني للمستهلك (الطرف الضعيف).

ثانياً: التزامات البنوك ومقدمي خدمات الدفع.

ثالثاً: دور التاجر الإلكتروني في عملية الدفع.

رابعاً: التمييز بين الجريمة الإلكترونية والجرائم التقليدية المشابهة.

(1) كوثر سعيد عدنان خالد، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2012، ص551.

أولاً: المركز القانوني للمستهلك في منظومة الدفع الإلكتروني: يقتضي البحث في الجرائم المرتبطة بالدفع الإلكتروني البدء بتحليل الركن الأساسي في هذه العلاقة وهو "المستهلك"؛ إذ أن تحديد مركزه القانوني هو الذي يرسم حدود المسؤولية الجنائية والمدنية. وتتجلى خصوصية هذا المركز في النقاط التالية:

أ/- مفهوم المستهلك الإلكتروني وخصائصه:

لا يختلف المستهلك الإلكتروني في جوهره عن المستهلك التقليدي من حيث الهدف النهائي وهو إشباع حاجاته الشخصية، إلا أنه يتميز بخصائص تجعل طبيعته القانونية أكثر تعقيداً؛ فهو الشخص الذي يتعاقد عبر "وسيط إلكتروني" بمعزل عن المعاينة المادية للسلعة، معتمداً كلياً على البيانات الرقمية التي يقدمها المورد. ويترب على هذا النوع من التعاقد "إبراء ذمته" تجاه الدائن من خلال استخدام وسائل الوفاء الحديثة، وهو ما يضعه في مواجهة مباشرة مع مخاطر تقنية لا يد له فيها¹.

ب/- مظاهر الضعف الفني والمعلوماتي للمستهلك:

يعتبر الفقه القانوني المستهلك الإلكتروني "طرفاً ضعيفاً" (Partie faible) بامتياز، وهذا الضعف ليس مادياً بالضرورة، بل هو "ضعف معرفي وتقني". فالمستهلك يجهل غالباً خوارزميات التشفير المعقدة، ولا يملك القدرة الفنية للتحقق من مدى أمان المنصات التي يودع فيها بيانات بطاقته البنكية. هذا التفاوت المعرفي بين "المهني" (البنك أو التاجر) والمستهلك يولد حالة من "التبعية التقنية"، حيث يضطر الأخير للثقة المطلقة في التدابير الأمنية التي يوفرها الطرف القوي في العقد، مما يجعله عرضة لمخاطر القصور الوظيفي للأداة أو القرصنة الإلكترونية².

(1) المرجع نفسه، ص 552.

(2) سيف الدين رخالي، مخاطر الدفع الإلكتروني على المستهلك الإلكتروني، مجلة البحوث والدراسات القانونية والسياسية، جامعة بومرداس، المجلد 02، العدد 11، 2021، ص 152.

ج/- مبررات الحماية القانونية المشددة (الأساس الجنائي):

إن إضفاء صفة "الطرف الضعيف" على المستهلك يترتب عليه نتائج قانونية جوهرية؛ أهمها تفسير الشك دائماً لمصلحة المستهلك في حالات النزاع حول عمليات الدفع، وافترض حسن نيته ما لم يثبت المهني عكس ذلك. كما تهدف الحماية القانونية إلى إعادة التوازن المفقود في "عقود الإذعان" الإلكترونية، حيث يوافق المستهلك على شروط معدة مسبقاً لا يملك حق نقاشها. ومن هذا المنطلق، تدخل المشرع الجزائري عبر القانون 18-05¹ ليس فقط لتنظيم العلاقة المدنية، بل لوضع قواعد جنائية وقائية تعتبر أي مساس ببيانات المستهلك .

ثانياً: المركز القانوني لمقدمي خدمات الدفع (البنوك): بناءً على التقسيم المنهجي المعتمد، يبرز البنك أو مؤسسة الدفع كطرف محوري وأقوى في منظومة الدفع الإلكتروني. ونظراً لمركزه الفني والمهني المتخصص، تقع على عاتقه جملة من الالتزامات القانونية التي تهدف لحماية العملية المالية وضمان استقرار المعاملات الرقمية، وتتمثل في:

أ/- الالتزام بضمان أمان وسلامة نظام الدفع:

يعد هذا الالتزام حجر الزاوية في العلاقة البنكية الرقمية؛ إذ يتعهد البنك بتوفير بنية تحتية محصنة تقنياً ضد أي اختراق. ويتسع نطاق هذا الالتزام ليشمل ضرورة اتخاذ كافة التدابير الوقائية لحماية الحامل من مخاطر ضياع أو سرقة البطاقة، حيث يلتزم المصرف بوقف العمل بالوسيلة فور إخطاره بواقعة فقدان، ويكون مسؤولاً عن أي تقصير في التحقق من شخصية الحامل أو إهمال في حفظ المعلومات السرية التي تؤدي لإلحاق ضرر بالذمة المالية للمستهلك².

(1) القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، 16 ماي 2018.

(2) سعاد مجايوي، ربيعة خلافي، التجربة الجزائرية لحماية المستهلك في مواجهة المخاطر المتعلقة بوسائل الدفع الإلكتروني، مجلة هيودوت للعلوم الإنسانية والاجتماعية، جامعة معسكر، المجلد 06، العدد 02، 2022، ص 877.

ب/- بالإعلام والتبصير (الطبيعة القانونية):

نظراً لافتقار المستهلك للخبرة الفنية، يفرض القانون على البنك "التزاماً ببذل عناية" في نقل المعلومات المتعلقة باستخدام الوسيلة ومخاطرها. ولا يقتصر هذا الدور على النصائح العامة، بل يمتد ليكون "التزاماً بتحقيق نتيجة" في بعض جوانبه، لاسيما في تخفيف عبء الإثبات عن المستهلك باعتباره الطرف الضعيف اقتصادياً معرفياً أمام نفوذ البنك المحترف. إن هذا الإعلام الوقائي يهدف لتبصير المستهلك بكافة الوسائل التي فرضها المشرع (كالوسم والبيانات الملحقة) لضمان وعيه الكامل بالتبعات القانونية لعملية الدفع¹.

ج/- الالتزام بتنفيذ أوامر الدفع والرقابة التقنية:

بمجرد صدور أمر الدفع، يلتزم البنك بتنفيذه بدقة وسرية مطلقة؛ فالبنك مسؤول عقدياً تجاه التاجر بوفاء قيمة الفواتير، وتجاه الحامل بضمان عدم تسريب بياناته. ومن الناحية الجنائية الحديثة، يتجاوز دور البنك مجرد التنفيذ ليلعب دور "الرقيب التقني" المطالب بمراقبة التدفقات المالية المشبوهة، حيث تقع على عاتقه مسؤولية التبليغ عن العمليات التي قد تشير لغسيل أموال أو احتيال ناتج عن استغلال وسائط دفع مسروقة².

ثالثاً: المركز القانوني والالتزامات المهنية للمورد الإلكتروني: يُمثل المورد الإلكتروني الطرف

المحترف والمستفيد في عملية الدفع، والذي يقع على عاتقه واجب تهيئة البيئة التعاقدية والتقنية المناسبة للمستهلك. ولا يقتصر دوره على تقديم السلعة، بل يمتد ليشمل مسؤوليات جوهرية لضمان سلامة التدفقات المالية:

(1) محمد عبد الله بوكار، محمد سلامة، حماية المستهلك الإلكتروني، مذكرة لنيل شهادة الماستر، تخصص قانون أعمال، كلية الحقوق و العلوم السياسية، قسم القانون الخاص، جامعة أدرار، 2017/2018، ص 46.

(2) المرجع نفسه، ص 47.

أ- الالتزام بالإعلام المسبق والشفافية التقنية:

باعتبار الحق في الإعلام أو ما يُطلق عليه "الالتزام بالتبصير" من الالتزامات الأساسية التي كرسها تشريعات التجارة الإلكترونية، يلتزم المورد بتزويد المستهلك بكافة المعلومات الجوهرية قبل الشروع في الدفع. ويتضمن ذلك تعريف المستهلك بهوية المورد، ومواصفات الخدمة، وكذا طبيعة الشروع في الدفع. ويتضمن ذلك تعريف المستهلك بهوية المورد، ومواصفات الخدمة، وكذا طبيعة وسيلة الدفع المستخدمة¹.

ب- الالتزام بضمان استمرارية العقد والحماية من الفسخ التعسفي:

تثور إشكالية قانونية حول مدى حق المورد أو البنك (وسيط) في فسخ العقد أو تعديله بإرادة منفردة. ويرى جانب من الفقه أن للمستهلك الحق في طلب التعويض إذا كان هناك تعسف في إلغاء الخدمة أو تعديل شروط الدفع دون إخطار مسبق، "فالل عقد شريعة المتعاقدين". كما يمتد هذا الالتزام ليشمل حالات القوة القاهرة ك وفاة الحامل؛ حيث تنعقد المسؤولية المدنية والتقصيرية في حال الاستمرار في عمليات الوفاء بعد تاريخ العلم بالوفاة، مما ينقص حقوق الورثة في التركة².

ج- الالتزام بحماية الخصوصية الرقمية ومنع تسريب البيانات:

يلتزم المورد باتخاذ كافة التدابير التقنية والمنطقية لحماية البيانات الشخصية والبنكية التي يحصل عليها أثناء عملية الدفع. ويُحظر عليه قانوناً استخدام هذه البيانات في غير الأغراض التي جمعت من أجلها أو تسريبها لأطراف ثالثة. إن أي تهاون في هذا الجانب لا يعد إخلالاً عقدياً فحسب، بل

(1) جمال أوجاني، النظام القانوني لبطاقة الائتمان، مذكرة لنيل شهادة الماستر، تخصص قانون أعمال، كلية الحقوق و العلوم السياسية، قسم القانون الخاص، قلمة، 2015/2016، ص 117.

(2) المرجع نفسه، ص 118.

يضعه تحت طائلة المساءلة الجنائية المتعلقة بـ "المساس بحرمة الحياة الخاصة" وإساءة استخدام البيانات المعلوماتية وفق ما نص عليه التشريع الجزائي، وهو ما يعزز دور المورد كحارس قانوني على أسرار العميل المالية¹.

رابعاً: التمييز بين الجريمة الإلكترونية والجرائم التقليدية المشابهة: تثير تقنية الدفع الإلكتروني مخاطر أمنية ناتجة عن طبيعة العمليات التي تُنفذ عبر الفضاء الرقمي، مما يفرض ضرورة التمييز بين الجريمة الإلكترونية والجرائم التقليدية المشابهة (كالسرقة والاحتيال الكلاسيكي)، نظراً للاختلاف الجوهرى في الوسائل والأبعاد:

أ/- من حيث طبيعة الجاني والوسيلة المستخدمة:

على خلاف المجرم التقليدي، فإن "الجاني المعلوماتي" غالباً ما يمتلك مهارات تقنية عالية وخبرة واسعة في اختراق الشبكات. فالجريمة هنا لا تعتمد على القوة العضلية، بل على "الذكاء البرمجي" واستغلال الثغرات في منصات الدفع للسطو على البيانات. هذا الاعتماد على "المعطى المعلوماتي" بدلاً من "الشيء المادي" هو ما يغير الركن المادي للجريمة ويجعل الوسيلة هي الأداة الوحيدة للتنفيذ².

ب/- من حيث النطاق المكاني والزمني:

تتميز الجريمة الإلكترونية بأنها عابرة للحدود وتُمارس في "فضاء رقمي مفتوح" دون قيود جغرافية. فبينما تتطلب السرقة التقليدية تواجد الجاني في مكان الجريمة، يمكن للمجرم المعلوماتي تنفيذ هجومه من قارة أخرى وفي أي وقت، مستخدماً أساليب معقدة كـ "أسلوب تفجير الموقع المستهدف"

(1) المرجع نفسه، ص119

(2) المادة 27، القانون رقم 18-05، المؤرخ في 2018/05/10، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، 2018/05/16.

أو الخداع التكنولوجي، مما يجعل تتبع الجاني وضبطه أصعب بكثير من الجرائم المادية¹. حيث تضع هذه السيولة المكانية سلطات التحقيق أمام تحدي "التنازع الدولي للاختصاص".

ج/- من حيث المساس بالخصوصية والبيانات الشخصية:

ترتبط الجريمة الإلكترونية بانتهاك "الحرمة الخاصة" للمستهلك؛ إذ أن الاعتداء يبدأ بانتهاك سرية البيانات المصرفية والمعطيات ذات الطابع الشخصي التي عرّفها المشرع الجزائري بأنها كل معلومة تسمح بالتعريف بالشخص مباشرة أو غير مباشرة. في الجرائم التقليدية، يكون الاعتداء غالباً على "المال" تسمح بالتعريف بالشخص مباشرة أو غير مباشرة. في الجرائم التقليدية، يكون الاعتداء غالباً على "المال" ككيان مادي، أما هنا فالمساس يطال الكيان الرقمي والخصوصية المالية للمستهلك قبل الوصول لمال ويترتب على هذا الاختراق ضررٌ معنوي جسيم يتمثل في استباحة البيانات الحساسة وتوظيفها في عمليات "الهندسة الاجتماعية" لاستدراج الضحايا².

د/- من حيث الأثر الاقتصادي والسياسة الجنائية:

تتجاوز آثار هذه الجرائم الضرر الفردي لتشمل النظام العام؛ حيث تساهم الصفقات غير الآمنة في تزايد "التهرب الضريبي" لصعوبة رقابة التدفقات المالية الرقمية من قبل الجهات الحكومية. ومن ناحية أخرى، تؤدي هذه الجرائم إلى "أزمة ثقة" في المنظومة المصرفية، مما دفع السياسة الجنائية الحديثة لتشديد العقوبات التكميلية كغلق المواقع والمصادرة الرقمية، وهي عقوبات تختلف عن تلك المعهودة في القانون الجنائي التقليدي³.

(1) الصمد حوالف، النظام القانوني لوسائل الدفع في الجزائر: دراسة مقارنة، د.ط، د.ج.ج، الإسكندرية، 2017، ص 323.

(2) سامية مساعد، حماية البيانات الشخصية للمستهلك من مخاطر الدفع الإلكتروني، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 15، العدد 01، 2022، ص 1395.

(3) محمد رمضان، الإنترنت كوسيلة للتهرب من الضريبة أو تجنبها، مجلة البحوث المالية والضريبية، العدد 18، لسنة 2003، ص 163.

المطلب الثاني: التصنيف القانوني لأبرز جرائم الدفع الإلكتروني

بمجرد استجماع أركان العلاقة القانونية في منظومة الدفع الإلكتروني وتحديد مراكز أطرافها، تبرز إلى الواجهة حزمة من التهديدات الأمنية التي تستهدف هذا النظام في مفاصله الحيوية؛ فبقدر ما وفرت هذه الوسائل من سرعة ومرونة، بقدر ما أنتجت بيئة خصبة لظهور أنماط إجرامية مستحدثة تتجاوز في خطورتها وتعقيدها الجرائم التقليدية.

وعليه، وللإحاطة بمختلف هذه الصور الجرمية وتكييفها قانوناً في ظل التشريع الجزائري، سنعمد إلى دراسة هذا المطلب من خلال تقسيم المادة العلمية إلى فرعين أساسيين:

الفرع الأول: الجرائم الواقعة على البيانات والأنظمة المعلوماتية للدفع.

الفرع الثاني: الجرائم الماسة بالمعاملات المالية الإلكترونية وإشكالات التكييف.

الفرع الأول: الجرائم الواقعة على البيانات والأنظمة المعلوماتية للدفع

تعد البيانات الرقمية للمستهلك والأنظمة البرمجية التي تُدار من خلالها عمليات الدفع الهدف الرئيسي للهجمات السيبرانية الحديثة؛ حيث يسعى الجناة بشتى الوسائل التقنية إلى اختراق هذه الحصون الرقمية للاستيلاء على الهوية المالية للمستخدم أو تعطيل المنظومة البنكية بشكل كامل. ومن أجل الإحاطة بهذه الاعتداءات وتكييفها قانوناً، سنعمد إلى دراسة هذا الفرع كالتالي:

أولاً: جريمة التصيد الإلكتروني وسرقة الهوية المالية.

ثانياً: جريمة اعتراض البيانات والتنصت الإلكتروني.

ثالثاً: جريمة تزوير وتزييف وسائل الدفع الإلكتروني.

رابعاً: جرائم اختراق وتعطيل قواعد بيانات الأنظمة البنكية.

أولاً: جريمة التصيد (Phishing) وسرقة الهوية المالية: تعد جريمة التصيد الإلكتروني وسرقة الهوية المدخل الرئيسي لأغلب الجرائم المالية الرقمية؛ فهي عملية تضليلية تهدف إلى استدراج الضحية للكشف عن بياناتها السرية، ثم استخدام تلك البيانات لانتحال شخصيتها وتجريدها من أصولها المالية. ومن أجل الإحاطة بهذه الجريمة، سنقوم بتحليل أركانها و تكييفها في التشريع الجزائري وفق الآتي:

أ/-الركن الشرعي للجريمة (التكييف القانوني):

تجد هذه الجريمة أساسها في منظومة التشريع الجزائري عبر تضافر عدة نصوص عقابية؛ حيث لم يضع المشرع نصاً خاصاً بمسمى "التصيد"، بل كيف أفعاله ضمن نصوص قانون العقوبات المعدل والمتمم. وتبرز المادة 394 مكرر¹ كحجر زاوية في التجريم، لكونها تعاقب على الدخول أو البقاء غير المشروع في منظومة معالجة آلية للمعطيات، وهو ما ينطبق على "الوصول" لبيانات المستهلك عبر الروابط المزيفة. كما يمكن تكييف الفعل وفق المادة 372² المتعلقة بجريمة النصب، نظراً لاعتماد التصيد على "الاحتيال" وانتحال صفة البنك لإيقاع الضحية في الغلط. ويتم هذا البنيان القانوني القانون رقم 09-04³ لاسيما في مواده التي تجرم حيازة أو استخدام بيانات الهوية الرقمية للغير دون وجه حق⁴.

(1) المادة 394 مكرر، الأمر رقم 66-156، المؤرخ في 08/06/1966، المتضمن قانون العقوبات، المعدل والمتمم.

(2) المادة 372، القانون نفسه.

(3) القانون رقم 09-04، المؤرخ في 05/08/2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(4) بوزيدي مريم، الآليات القانونية لحماية المستهلك عبر الإنترنت، مذكرة لنيل شهادة الماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة سعيدة، 2024، ص 28.

ب/-الركن المادي للجريمة:

يتمثل السلوك الإجرامي هنا في نشاط إيجابي يتخذ صوراً تقنية، تبدأ بإرسال رسائل وهمية تتضمن "روابط ملغومة" تحاكي الواجهات الرسمية للبنوك. ويتحقق الركن المادي بمجرد استجابة الضحية وإدخال بياناته (الرقم السري، رقم البطاقة)، وهنا تتحول الجريمة من محاولة تصيد إلى "سرقة هوية مكتملة". وتتمثل سرقة الهوية الرقمية في الاستيلاء على بيانات تحديد الهوية الخاصة بالغير واستخدامها بدون رضا صاحبها من أجل ارتكاب جرائم أخرى. وتكتمل النتيجة الإجرامية بحدوث الضرر المالي للمستهلك أو بمجرد سيطرة الجاني على "الذاتية الرقمية" للضحية، مما يمنحه سلطة التصرف في أمواله¹.

ج/-الركن المعنوي للجريمة:

تُصنف هذه الجريمة ضمن الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة "القصد الجنائي" القائم على تلازم عنصري العلم والإرادة؛ إذ يجب أن يحيط علم الجاني إحاطة تامة بكافة العناصر الواقعية والقانونية المكونة للجريمة، لا سيما إدراكه بأن الموقع الإلكتروني الذي أنشأه هو موقع زائف يهدف إلى التغرير بالجمهور، وأن إرادته قد انصرفت صراحةً وبوعي كامل نحو اختراق خصوصية المستهلك والاعتداء على بياناته الرقمية بطريقة غير مشروعة (القصد العام). ولا يكتفي القانون الجزائي لقيام هذه الجريمة بمجرد العلم، بل يستلزم بالضرورة توافر "نية الإضرار" والوصول لنتيجة إجرامية محددة، وهو ما يعرف بـ "القصد الجنائي الخاص" الذي يتجسد في نية الاستيلاء على أموال الغير أو التلاعب ببياناتهم البنكية لتحقيق ربح غير مشروع².

(1) المرجع نفسه، ص31

(2) الشيخ أمال، الجوانب الموضوعية والإجرائية للجريمة المعلوماتية في التشريع الجزائري، دار الجامعة الجديدة، الجزائر، 2021، ص 114

ثانياً: جريمة اعتراض البيانات والتنصت الإلكتروني: تعد جريمة اعتراض البيانات من أخطر الاعتداءات التقنية التي تمس سرية تدفقات الدفع الإلكتروني؛ حيث لا يستهدف الجاني هنا "خداع" المستهلك كما في جريمة التصيد، بل يعتمد على "الاختراق الصامت" لقنوات الاتصال بين المستهلك والبنك للاستيلاء على المعلومات أثناء عبورها في الفضاء السيبراني. وسنفصل في أركان هذه الجريمة وفقاً للآتي:

أ/- الركن الشرعي للجريمة (التكليف القانوني):

لقد أفرد المشرع الجزائري نصوصاً صريحة لمواجهة أفعال الاعتراض والتنصت الرقمي، ضماناً لحزمة المعطيات وسرية المراسلات الإلكترونية. وتعد المادة 394 مكرر 1¹ من قانون العقوبات النص المرجعي الأساسي، حيث تجرم فعل "الاعتراض" الذي يتم بوسائل تقنية للمعطيات أثناء نقلها غير العمومي داخل نظام معلوماتي أو انطلاقاً منه أو إليه. كما عزز القانون رقم 09-204 الحماية الإجرائية والموضوعية ضد محاولات "التقاط" التدفقات الرقمية دون وجه حق. وبالإضافة لذلك، نجد سنداً قانونياً في القانون 18-305³ المتعلق بالتجارة الإلكترونية، الذي يلزم المورد بضمان سرية البيانات، مما يجعل أي اعتراض لهذه المعطيات خرقاً للمنظومة الأمنية المحمية قانوناً. وهو ما يعكس توجهاً تشريعياً صارماً يهدف إلى بسط الرقابة الجنائية على الفضاءات الافتراضية الخاصة، للحيلولة دون تحويل أدوات الاتصال الحديثة إلى وسائل للتجسس المالي أو المعلوماتي. كما أن هذا الحظر يتجاوز مجرد حماية المحتوى الرقمي ليصل إلى ضمان استمرارية الثقة في البنية التحتية للمعاملات الإلكترونية.

(1) المادة 394 مكرر 1، الأمر رقم 66-156، المؤرخ في 08/06/1966، المتضمن قانون العقوبات، المعدل والمتمم.

(2) القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(3) القانون رقم 18-05، المؤرخ في 10/05/2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، 2018/05/16.

ب/-الركن المادي للجريمة:

يتحقق الركن المادي في هذه الجريمة من خلال "السلوك الإيجابي" المتمثل في عملية الالتقاط التقني للبيانات؛ حيث يتم ذلك باستخدام برامج متخصصة (مثل برامج Sniffers) تقوم بالتنصت على حزم البيانات (Packets) المتداولة عبر الشبكة أثناء عملية الدفع، لاستخلاص أرقام البطاقات ورموز التحقق. ولا يشترط في الركن المادي هنا أن يقوم الجاني بتغيير البيانات أو حذفها، بل يكفي مجرد "الاطلاع غير المشروع" أو اعتراض مسارها لتحقيق الجريمة. وتكتمل النتيجة الإجرامية بمجرد نجاح الجاني في وضع يده على المعطيات البنكية أثناء انتقالها من جهاز المستهلك إلى خادم البنك، وهو ما يُعرف قانوناً بالاعتداء على سلامة النقل الرقمي¹.

ج/-الركن المعنوي للجريمة:

تعتبر جريمة اعتراض البيانات جريمة عمدية، تتطلب توافر القصد الجنائي بعنصريه: القصد العام الذي يتمثل في اتجاه إرادة الجاني إلى استخدام أدوات تقنية لاعتراض مسار البيانات مع علمه المسبق بأنها بيانات خاصة ولا يحق له الاطلاع عليها. أما القصد الخاص، فيتمثل في "نية الاستيلاء" على تلك البيانات لاستغلالها لاحقاً في عمليات سحب مالي أو بيعها في "الشبكة المظلمة" (Dark Web). فالجرم هنا لا يعترض البيانات بدافع الفضول التقني، بل بنية إجرامية تهدف إلى الإضرار بالذمة المالية للمستهلك وزعزعة الثقة في أنظمة الدفع الإلكتروني ككل³، وهو ما يجعل من هذا السلوك اعتداءً مزدوجاً يمس بجرمة الحياة الخاصة من جهة، ويقوض دعائم الاستقرار المالي والموثوقية الرقمية التي يسعى المشرع لحمايتها من جهة أخرى².

(1) جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، د.ن.ع، القاهرة، 1992، ص 44.

(2) خالد ممدوح إبراهيم، جرائم نظام الدفع الإلكتروني، د.ف.ج، الإسكندرية، مصر، 2008، ص 201.

ثالثاً: جريمة تزوير أو تزيف وسائل الدفع الإلكتروني: تعتبر جريمة تزوير وسائل الدفع الإلكتروني، ولا سيما البطاقات البنكية، من الجرائم التقنية المعقدة التي تتطلب مهارة فائقة في التقليد أو المحاكاة الرقمية؛ فهي لا تستهدف مجرد الاستيلاء على البيانات، بل تهدف إلى خلق "سند دفع وهمي" يحمل كافة خصائص السند الصحيح لإيهام نظام الدفع بمشروعية العملية المالية. ويتعدى هذا التزوير مجرد المحاكاة المادية لشكل البطاقة، ليصل إلى اختراق وتزيف الخصائص البرمجية والشفيرات الأمنية المدججة، مما يجعل من الصعب على الأنظمة الآلية العادية اكتشاف الفارق بين الوسيلة الأصلية والنسخة المزورة. وسنتناول أركان هذه الجريمة وتفصيلاتها القانونية وفق الآتي:

أ/- الركن الشرعي للجريمة (التكليف القانوني):

لقد خص المشرع الجزائري جرائم التزوير في المحررات والوثائق الإلكترونية بحماية خاصة، معتبراً إياها اعتداءً صارخاً على الثقة العامة. وتعد المادة 394 مكرر 2¹ من قانون العقوبات النص العام المطبق على التزوير المعلوماتي، كونها تعاقب على إدخال معطيات في نظام معالجة آلية أو تغييرها أو شطبها بطريقة غير مشروعة. كما يمتد التكليف القانوني ليشمل القواعد العامة للتزوير في الأوراق النقدية والسندات المالية المنصوص عليها في المواد 197²، حيث يُكيف القضاء تزوير البطاقة البنكية على أنه تزوير في سند مالي ذو قوة إبرائية. ويأتي القانون 05-18³ المتعلق بالتجارة الإلكترونية ليشدد العقوبات في حال تعلق التزوير بوسيلة دفع معتمدة، نظراً للأثر الاقتصادي السلبي على المنظومة البنكية، وهو ما يعكس توجهاً تشريعياً يهدف إلى سد الثغرات أمام تطور الأساليب الإجرامية تسعى إلى إحداث تغيير في الحقيقة الرقمية المخزنة لغرض الاستيلاء على الائتمان المالي.

(1) المادة 394 مكرر 1، الأمر رقم 66-156، المؤرخ في 08/06/1966، المتضمن قانون العقوبات، المعدل والمتمم.

(2) القانون رقم 09-04، المؤرخ في 05/08/2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(3) القانون رقم 18-05، المؤرخ في 10/05/2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16/05/2018.

ب/-الركن المادي للجريمة:

يتحقق الركن المادي عبر سلوك إيجابي يتمثل في "تغيير الحقيقة" في وسيلة الدفع؛ حيث يأخذ التزوير عدة صور، منها "التزوير المادي" باصطناع بطاقة مشابهة تماماً للأصلية (Clonage)، أو "التزوير المعنوي" بالتلاعب في البيانات المشفرة داخل الشريحة لتغيير هوية صاحبها أو رصيدها المالي، كما يشمل الركن المادي استخدام أجهزة القارئات (Skimming) لاستنساخ البيانات وتفريغها في بطاقات بيضاء فارغة. وتكتمل النتيجة الإجرامية بمجرد إحداث هذا التغيير وجعل الوسيلة صالحة للاستعمال كأداة وفاء حقيقية، ولا يشترط وقوع الضرر المادي فعلاً لتحقيق الجريمة، بل يكفي احتمال وقوعه نتيجة وجود الوسيلة المزورة في التداول¹.

ج/-الركن المعنوي للجريمة:

تعد هذه الجريمة عمدية بامتياز، تقوم على القصد الجنائي العام والخاص؛ القصد العام يتمثل في علم الجاني بأن فعله (تعديل أو اصطناع البيانات) يغير الحقيقة في سند مالي محمي قانوناً، وأن إرادته تتجه بحرية للقيام بهذا الفعل مع علمه التام بعدم مشروعيته. أما القصد الخاص، فيتمثل في "نية استعمال" الوسيلة المزورة؛ فالجاني لا يزور البطاقة لمجرد العبث التقني، بل يهدف لاستعمالها كأداة وفاء للحصول على سلع أو سحب مبالغ نقدية بغير حق. وقد استقر الفقه والقضاء على أن سوء النية يُفترض بمجرد ثبوت قيام الشخص بعملية التعديل غير المصرح بها على البيانات البنكية للغير².

(1) طارق إبراهيم الدسوقي، ثورة المعلومات والجريمة المعلوماتية، د.ج.ج، الإسكندرية، 2011، ص 215.

(2) مدحت رمضان، جرائم الاعتداء على الأشخاص والأموال في تكنولوجيا المعلومات، د.ن.ع، القاهرة، 2000، ص 98.

رابعاً: جرائم اختراق وسرقة قواعد بيانات البنوك: تعد قواعد البيانات البنكية بمثابة "الحصون الرقمية" السيادية التي تحتزن أدق المعلومات الحساسة المتعلقة بدمم المستهلكين المالية وكافة تفاصيل عملياتهم المصرفية ؛ ولا يتوقف التكليف القانوني لهذه الجريمة عند حدود "الدخول" غير المصرح به فحسب، بل يمتد ليشمل كافة صور السيطرة على البيانات أو تعطيلها أو تخريبها، وسنفصل في ماهية هذه الأركان وفقاً للآتي

أ/-الركن الشرعي للجريمة (التكليف القانوني):

أفرد المشرع الجزائري منظومة عقابية صارمة لحماية أنظمة المعالجة الآلية للمعطيات، خاصة تلك التابعة للمؤسسات المالية. وتعد المادة 394 مكرر¹ من قانون العقوبات النص المرجعي الاول، حيث تجرم الدخول أو البقاء غير المشروع في المنظومة، وتشدد العقوبة إذا نتج عن ذلك حذف أو تغيير تجرم الدخول أو البقاء غير المشروع في المنظومة، وتشدد العقوبة إذا نتج عن ذلك حذف أو تغيير في المعطيات. ويأتي القانون 09-04² المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ليصنف الاعتداء على المنظومات المعلوماتية الوطنية (ومنها البنكية) ضمن الجرائم التي تستوجب إجراءات تحقيق خاصة نظراً لخطورتها البالغة على الأمن الاقتصادي الوطني .

ب/-الركن المادي للجريمة:

يتمثل السلوك الإجرامي هنا في تخطي الحواجز الأمنية للبنك (Firewalls) باستخدام برمجيات اختراق معقدة أو استغلال ثغرات النظام. ويتحقق الركن المادي بمجرد نجاح الجاني في النفاذ إلى قاعدة البيانات والاستيلاء على المعطيات المخزنة، سواء كانت بيانات تعريفية أو أرقام حسابات

(1) المادة 394 مكرر2، الأمر رقم 66-156، المؤرخ في 08 جوان 1996، المتضمن قانون العقوبات، المعدل والمتمم .

(2) القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولا يشترط وقوع فعل السرقة المادية للأموال فعلاً، بل تكتمل الجريمة بمجرد "المساس بسلامة المنظومة". وتتخذ النتيجة الإجرامية صوراً متعددة، منها "تسريب البيانات" للعموم، أو "تشفيرها" لابتزاز البنك (Ransomware)، أو حتى "المحو الكلي" للسجلات المالية لإخفاء أثر عمليات إجرامية أخرى، مما يزعزع ثقة المستهلكين في أمان الدفع الإلكتروني¹.

ج/-الركن المعنوي للجريمة:

تعتبر جريمة اختراق قواعد البيانات جريمة عمدية تتطلب قصداً جنائياً خاصاً؛ فالقصد العام يتمثل في علم الجاني التام بأن النظام الذي يخترقه محمي بإجراءات أمنية مملوكة للغير، واتجاه إرادته لتجاوز هذه العقوبات التقنية دون تصريح قانوني. أما القصد الخاص، فيتمثل في "نية الإضرار بالبنك" أو "نية الاستيلاء على الأسرار المصرفية" للمتاجرة بها أو استغلالها. وقد اعتبر الفقه والقضاء الجزائري أن استخدام أدوات اختراق احترافية (مثل هجمات Brute-force) يعد دليلاً قاطعاً على سوء النية والرغبة الأكيدة في تحقيق نتيجة إجرامية ضارة بالمنظومة البنكية، وهو ما ينقل الفعل من مجرد دخول غير مشروع إلى اعتداء جسيم يستهدف تقويض النظام العام للمعلوماتي للمؤسسات المالية، الأمر الذي يستوجب تكييفاً عقابياً يراعي حجم الضرر على الاقتصاد الرقمي، وحجم الانتهاك الذي يطال خصوصية المودعين وسرية حساباتهم التي كفل القانون حمايتها بطرق وقانونية².

الفرع الثاني : الجرائم الماسة بالمعاملات المالية الإلكترونية

إذا كانت الاعتداءات السابقة قد ركزت على اختراق الأنظمة والبيانات، فإن هناك طائفة أخرى من الجرائم تستهدف جوهر العملية المالية وموثوقية التبادل التجاري الإلكتروني؛ حيث تمتد هذه الجرائم لتشمل الاحتيال في تنفيذ الالتزامات أو شل قدرة الأنظمة على تقديم خدماتها.

(1) ممدوح عبد الحميد عبد المطلب، الجريمة المعلوماتية، د.ن.ع، القاهرة، 2001، ص 85.

(2) بوزيدي مريم، الآليات القانونية لحماية المستهلك عبر الإنترنت، مذكرة ماستر، تخصص قانون أعمال، جامعة سعيدة، 2024، ص 18.

ولإحاطة بهذا الجانب وتفصيل صوره الجرمية، سنعمد إلى تقسيم هذا الفرع وفقاً للفقرات

التالية:

أولاً: جريمة الاحتيال في المعاملات المالية وعدم تسليم السلع.

ثانياً: جرائم الحرمان من الخدمة (DDoS) وأثرها على عمليات الدفع.

ثالثاً: جريمة الإكراه والتهديد الإلكتروني للحصول على بيانات الدفع.

رابعاً: إشكالات التكييف القانوني وتحديد الصفة الجرمية للمعاملات المالية الرقمية.

أولاً: جريمة الاحتيال في المعاملات (عدم تسليم السلعة المدفوعة): تعتبر جريمة

الاحتيال في المعاملات الإلكترونية من أكثر الصور الإجرامية شيوعاً في ظل تنامي التجارة الرقمية؛ حيث يتم استغلال آليات الدفع الإلكتروني كأداة لإتمام عمليات تعاقدية زائفة. وتكمن خطورة هذه الجريمة في وقوعها بعد تنفيذ المستهلك لالتزامه المالي كاملاً، مما يجعله في مواجهة مباشرة مع ضياع ماله دون الحصول على المقابل السلعي أو الخدمي الموعود به.

أ/-الركن الشرعي وجدلية التكييف القانوني:

يستمد هذا الفعل صفته الجرمية من تضافر نصوص قانونية متكاملة في التشريع الجزائري

تهدف لحماية المستهلك من التدليس؛ حيث تُعد المادة 372 من قانون العقوبات¹ حجر الزاوية

في تجريم النصب، إذ يكيف القضاء "عرض سلع وهمية" أو "إخفاء انعدام نية التسليم" كطرق

(1) المادة 372، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

احتياالية لإيهام الضحية بوجود مشروع كاذب. كما عزز القانون 18-05¹ المتعلق بالتجارة الإلكترونية هذه الحماية من خلال إرساء التزامات صارمة على عاتق المورد الإلكتروني، معتبراً الإخلال العمدي بالتسليم بعد استلام الثمن إلكترونياً صورة من صور الاحتيال الموصوف الذي يمس الثقة الرقمية والائتمان المالي .

ب/-التجليات المادية للسلوك الإجرامي والنتيجة:

يتحقق الركن المادي في هذه الجريمة عبر سلوك إيجابي مركب يبدأ بخلق مظهر كاذب لمنصة تجارية توحي بالمصداقية، لإغراء المستهلك بالتعاقد والدفع الرقمي. فالاحتيال هنا يتجسد في استخدام الجاني لأساليب تدليسية تجعل المستهلك يثق في العملية، ليقوم بتحويل الأموال عبر بطاقته البنكية، ليجد نفسه لاحقاً ضحية لعدم تنفيذ الالتزام. وتكتمل النتيجة الإجرامية بمجرد انتقال القيمة المالية من حساب الضحية إلى ذمة الجاني، مما يحقق ضرراً مالياً حالاً ومباشراً؛ فالعبرة بوقوع "الاستيلاء غير المشروع" الذي يتجاوز مجرد التأخر المدني في التسليم ليدخل في حيز التجريم الجنائي².

ج/-القصد الجنائي وعناصر الركن المعنوي:

باعتبارها جريمة عمدية، فإن الركن المعنوي فيها يقوم على انصراف إرادة الجاني إلى إيقاع الغلط لدى المستهلك مع علمه التام بأن العملية وهمية. ولا يكتفي القانون بالقصد العام، بل يشترط "نية التملك النهائي" للمال المقبوض بغير حق؛ ويستنبط القضاء الجزائري سوء النية هذا من قرائن مادية قوية،

(1) القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 ماي 2018.

(2) محمد الأمين بن خدة، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2012، ص 156.

كقطع الاتصال بالضحية أو إغلاق الحسابات الإلكترونية فور استلام التحويل المالي، مما يؤكد أن الجاني لم يكن يهدف منذ البداية لإتمام المعاملة بل لاستنزاف الرصيد المالي للمستهلك بطرق تدليسية مبيتة، وهذا ما يحول الإخلال العقدي من مجرد نزاع مدني حول تنفيذ الالتزام إلى جريمة نصب مكتملة الأركان، تعكس خطورة إجرامية تهدف لزعزعة استقرار الثقة في الفضاء السيبراني البنكي¹.

ثانياً: جرائم الحرمان من الخدمة (DDoS) الموجهة لأنظمة الدفع: تعد هجمات الحرمان من الخدمة الموزعة من أكثر الاعتداءات السيبرانية تعقيداً وخطورة في البيئة الرقمية؛ حيث لا يستهدف الجاني فيها سرقة بيانات المستهلك بشكل مباشر في الغالب، وإنما يهدف إلى إخراج نظام الدفع الإلكتروني عن الخدمة وشله تماماً عن العمل. ويترتب على هذه الجريمة التقنية خسائر مالية فادحة للمؤسسات والزبائن نتيجة التوقف المفاجئ للمعاملات، مما يزعزع استقرار المنظومة البنكية ويضرب موثوقيتها. وسنفصل في أركانها الجنائية وتكليفها في التشريع الجزائري وفق الآتي:.

أ/-الركن الشرعي وتكليف فعل العرقلة المعلوماتية:

لقد وضع المشرع الجزائري نصوصاً صريحة تحرم الأفعال التي تؤدي إلى تعطيل الأنظمة المعلوماتية، حمايةً للاستمرارية الرقمية للمرافق المالية؛ حيث تُعد المادة 394 مكرر 1² من قانون العقوبات والتي تعاقب على عرقلة سير نظام معالجة آلية للمعطيات، إذ يعتبر المشرع أن كل فعل تقني يؤدي إلى إبطاء النظام أو منعه من أداء وظائفه الطبيعية هو جريمة قائمة بذاتها. كما عززت التعديلات القانونية هذه الحماية، بالتوازي مع ما أقره

(1) بوزيدي مريم، الآليات القانونية لحماية المستهلك عبر الإنترنت، مذكرة ماستر، تخصص قانون أعمال، جامعة سعيدة، 2024

(2) المادة 394 مكرر 1، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

القانون 09-04¹ المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام، والذي وفر الآليات الإجرائية لملاحقة مرتكبي هذه الهجمات.

ب/-الركن المادي ومظاهر الاعتداء على التوافر الرقمي:

يتمثل السلوك الإجرامي في إغراق خادم نظام الدفع بطلبات وهمية تتجاوز قدرته الاستيعابية، مما يؤدي لتعطيله وحرمان المستهلكين من إتمام معاملاتهم. وتتحقق الجريمة بمجرد الاعتداء على التوافر الرقمي للنظام، مما يشكل إهداراً لمبدأ استمرارية المرفق الرقمي وزعزعة للأمان المالي الافتراضي، وهو ما يترتب خسائر مادية مباشرة ناتجة عن انهيار المنظومة التقنية في مواجهة هذه الهجمات المنظمة².

ج/-الركن المعنوي وتوافر القصد التخريبي:

تعتبر هذه الجريمة عمدية تتطلب قصداً عاماً يتمثل في إرادة شل النظام رغم العلم بنتائجه، وقصداً خاصاً ينصرف لنية الإضرار بالمنشأة المالية أو ابتزازها. ويُستخلص سوء النية من الطبيعة التنظيمية للهجوم، مما ينفي عنه صفة الخطأ العفوي ويؤكد القصد الإجرامي المبيت الذي يستهدف زعزعة استقرار أنظمة الدفع الرقمي³.

ثالثاً: جريمة الإكراه أو التهديد للحصول على بيانات الدفع: تعد جريمة الإكراه الإلكتروني من الجرائم

المركبة التي تجمع بين الاعتداء على حرية الشخص والاعتداء على ذمته المالية في آن واحد؛ ففي بيئة الدفع الرقمي، قد يلجأ الجاني إلى استخدام التهديد بتشويه السمعة أو تسريب بيانات خاصة (الابتزاز) مقابل الحصول على أرقام البطاقات البنكية أو الرموز السرية للمستهلك، مما يجعل إرادة الضحية في الكشف عن بياناته معيبة وفاقدة للاختيار، وهو ما ينسف مبدأ الأمان في التعاملات المالية، إذ لا يقتصر أثر هذا الإكراه على الضرر

(1) القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(2) نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، د.ن.ع.د.ط، القاهرة، 1994، ص 102.

(3) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة آلاي، القاهرة، 1992، ص 180.

المادي المباشر فحسب، بل يمتد لزعزعة استقرار المنظومة الائتمانية ككل من خلال تقويض عامل "الثقة المفترضة" في الوسائط الرقمية. وسنفصل في أركان هذه الجريمة وتكييفها القانوني وفقاً للآتي:

أ/-الركن الشرعي وتعدد نصوص التجريم:

لقد وضع المشرع الجزائري نصوصاً عقابية صارمة لمواجهة أفعال التهديد والابتزاز، سواء وقعت في الفضاء المادي أو الافتراضي؛ حيث يعد النص العام الوارد في المادة 370 من قانون العقوبات¹ حجر الزاوية، والتي تعاقب كل من حصل على أموال أو أوراق أو توقيعات عن طريق التهديد بالكشف عن أمور شائنة، وهو النص الذي يطبق بوضوح على حالات الابتزاز الإلكتروني. كما تتقاطع هذه الحماية مع المادة 394 مكرر 2² من قانون العقوبات المتعلقة بالاعتداء على سلامة المعطيات، حيث يُكيف التهديد الذي يتبعه دخول للنظام باستخدام بيانات منتزعة بالإكراه كجريمة معلوماتية مشددة. وقد تعززت هذه المنظومة بالقانون رقم 04-15 المعدل لقانون العقوبات³، الذي شدد العقوبات عند استخدام الوسائل الإلكترونية لتهديد الأشخاص، معتبراً إيها ظرفاً يسهل الجريمة ويضاعف من أثرها، مما يعكس رغبة المشرع في بسط حماية جنائية شاملة تحسن "الإرادة التعاقدية" للمستهلك من أي ضغط خارجي قد يسلبها حريتها في الاختيار أو يعبث بسلامة ذمتها المالية الرقمية، وهو ما يبرر إدراج هذه الأفعال ضمن الجرائم الماسة بالثقة الائتمانية، بالنظر إلى أن الابتزاز الرقمي لا يقتصر أثره على ترويع الضحية فحسب، بل يمتد لتقويض أسس الأمان في التعاملات المالية الإلكترونية عبر زعزعة موثوقية الهوية الرقمية و التزامات قانونية.

(1) المادة 370، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

(2) المادة 394 مكرر2، القانون نفسه .

(3) القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

ب/-الركن المادي ومظاهر الإكراه الرقمي:

يتحقق الركن المادي في هذه الجريمة بسلوك إيجابي يتمثل في ممارسة "التهديد" الموجه للمستهلك، ويتخذ هذا السلوك طابعاً معنوياً في الغالب عبر الفضاء السيبراني من خلال التلويح بنشر أسرار خاصة مقابل الحصول على بيانات الدفع الحساسة. فالسلوك الإجرامي يقوم على مطالبة الضحية بالكشف عن بياناته المالية تحت طائلة تنفيذ وعيد معين، مما يدفع الضحية للرضوخ قسراً خوفاً من الضرر الموعود به. وتكتمل النتيجة الإجرامية بمجرد "تسليم البيانات" أو القيام بالتحويل المالي تحت تأثير الرهبة؛ ولا يشترط وقوع الضرر المادي الفعلي بالمال في هذه المرحلة، بل تكتمل الجريمة قانوناً بمجرد سلب إرادة الضحية وإجباره على إفشاء أسرار المصرفية تحت توطأ الضغط القانوني¹.

ج/-الركن المعنوي وتوافر نية الابتزاز:

إن الركن المعنوي فيها يقوم على انصراف إرادة الجاني إلى بث الرعب في نفس المستهلك مع علمه التام بأن فعله غير قانوني ويشكل اعتداءً على الخصوصية. ويهدف القصد العام هنا إلى إجبار الضحية على القيام بفعل الكشف عن البيانات الذي لم يكن ليقوم به اختيارياً. وبالإضافة لذلك، يشترط توافر قصد جنائي خاص يتمثل في "نية الابتزاز وتحقيق نفع مالي غير مشروع"؛ فالفاعل لا يهدف لمجرد التخويف، بل يسعى للوصول لمدخرات الضحية أو استخدام بياناتها في عمليات شراء مجهولة. ويستنبط الفقه سوء النية من خلال التصميم المسبق لرسائل الابتزاز واستهدافها المباشر للبيانات البنكية، مما يؤكد غرض الجاني في الثراء غير المشروع على حساب أمن المستهلك².

(1) خالد ممدوح إبراهيم، جرائم نظام الدفع الإلكتروني، د.ف.ج، الإسكندرية، 2008، ص 210.

(2) محمد الأمين بن خدة، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2012، ص 168.

رابعاً: الإشكالات القانونية في تحديد الصفة الجرمية: تثير جرائم الدفع الإلكتروني إشكالات معقدة عند إسقاط النصوص التقليدية على السلوكيات الحديثة؛ حيث يعجز التكييف القانوني غالباً عن الإحاطة بطبيعتها العابرة للحدود. إن تحديد الصفة الجرمية لهذه الأفعال يتطلب دقة عالية في التمييز بين الإخلال التقني والجريمة الجنائية، وهو ما سنفصله في النقاط الآتية:

أ/- إشكالية التكييف بين النصوص التقليدية والمستحدثة:

تتجلى أولى الإشكالات في صعوبة تحديد النص الواجب التطبيق، خاصة في ظل غياب تعريفات حصرية لبعض الأفعال مثل "التصيد" أو "الحرمان من الخدمة" في صلب قانون العقوبات. إن محاولة تكييف أفعال الدفع الإلكتروني وفقاً للنصوص التقليدية، كجريمة النصب أو السرقة، غالباً ما يصطدم بمبدأ "شرعية الجرائم والعقوبات"؛ نظراً لأن الركن المادي في الجريمة الرقمية لا يعتمد على الاختلاس المادي، بل يتم عبر نبضات إلكترونية ومعالجات آلية للمعطيات.¹ وعليه، يقع القاضي في حيرة بين استخدام المواد 394 مكرر² المتعلقة بالجرائم المعلوماتية، وبين النصوص الكلاسيكية.

ب/- صعوبة إثبات الركن المعنوي وتحديد القصد:

يمثل الركن المعنوي عقبة كأداء في تحديد الصفة الجرمية؛ ففي بيئة تقنية معقدة، يصعب التمييز أحياناً بين "سوء النية الإجرامي" وبين "الأخطاء البرمجية" أو حتى "إهمال المستهلك". إن إثبات القصد الجنائي الخاص لدى المحتال يتطلب خبرة فنية دقيقة لفك شفرة السلوك؛ إذ أن مجرد الوصول إلى النظام قد لا يكون كافياً لإسباغ الصفة الجرمية ما لم يقترن بنية الإضرار أو التملك.³

(1) محمد الأمين بن خدة، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2012، ص 210.

(2) المادة 394 مكرر، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

(3) جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، د.ن.ع، القاهرة، 1992، ص 162.

المبحث الثاني: البنيان القانوني للجريمة الرقمية وقواعد الإثبات الجنائي

تعتبر الجرائم المرتبطة بالدفع الإلكتروني من التحديات الجسيمة التي تواجه المنظومة الجنائية الحديثة، إذ تفرض طبيعتها الافتراضية ضرورة إعادة قراءة الأركان العامة للجريمة وفق منظور تقني يستوعب الوسائل المستحدثة في الاعتداء على الذمة المالية للمستهلك. ولا تقتصر الإشكالية على تحديد العناصر المكونة للجريمة فحسب، بل تمتد لتشمل الجانب الإجرائي المتعلق بصعوبة إثبات الدليل الرقمي وتحديد المسؤولية الجنائية في ظل تداخل أدوار الفاعلين والوسطاء الماليين.

ومن هذا المنطلق، يهدف هذا المبحث إلى تشريح البنيان القانوني لهذه الجرائم وتبيان آليات ملاحقتها وإثباتها؛ وعليه ستم معالجة هذا المبحث من خلال المطلبين التاليين:

المطلب الأول: الأركان العامة والخاصة للجرائم الماسة بالدفع الإلكتروني.

المطلب الثاني: آليات إثبات الجريمة الإلكترونية وتحديد المسؤولية الجنائية.

المطلب الأول: الأركان العامة والخاصة لجرائم الماسة بالدفع الإلكتروني

يتوقف قيام جريمة الدفع الإلكتروني على استجماع عناصرها القانونية المتمثلة في الركنين المادي والمعنوي مع مراعاة خصوصية البيئة الرقمية في تكييف السلوك والنتيجة؛ وهو ما سنعالجه عبر تقسيم هذا المطلب إلى فرعين على النحو الآتي:

الفرع الأول: الركن المادي للجريمة الرقمية وعلاقة السببية.

الفرع الثاني الركن المعنوي والاختصاص القضائي.

الفرع الأول: الركن المادي للجريمة الرقمية وعلاقة السببية

يتمثل الركن المادي في النشاط التقني الخارجي الذي يمس سلامة أنظمة الدفع أو بياناتها، وما يترتب عليه من نتائج وإشكالات في إثبات الرابطة السببية ومظاهر الشروع؛ حيث لا قيام للجريمة دون سلوك ملموس في الفضاء الرقمي يغير من المراكز القانونية لأطراف المعاملة المالية.

ولإحاطة بعناصر هذا الركن، سنقوم بتقسيم هذا الفرع إلى الفقرات التالية:

أولاً: الأفعال المكونة للاعتداء على نظام الدفع أو بياناته.

ثانياً: النتيجة الإجرامية في جرائم الدفع الإلكتروني.

ثالثاً: علاقة السببية وإشكالية الإثبات التقني.

رابعاً: صور الشروع في اعتداءات الدفع الرقمي.

أولاً: الأفعال المكونة للاعتداء على نظام الدفع أو بياناته: لا يمكن تصور قيام الركن المادي في جرائم الدفع الإلكتروني دون وجود نشاط إيجابي خارجي ملموس يأتيه الجاني، وهذا النشاط يتميز بطابع فني وتقني دقيق يستهدف المنظومة المعلوماتية التي تُدار من خلالها العمليات المالية. وقد حصر المشرع الجزائي صور هذا السلوك في المواد 394 مكرر¹ من قانون العقوبات، وهي الأفعال التي تشكل في مجملها "الاعتداء الرقمي" المباشر على ركيزة الثقة في التعاملات المصرفية، مما يجعل من الركن المادي في هذه الجرائم ركيزة أساسية لترتيب المسؤولية الجنائية المشددة نظراً لجساسة الضرر المترتب عنها؛ وسنفصل في هذه الأفعال وفق الآتي:

(1) المادة 394 مكرر، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

أ/- فعل الدخول أو البقاء غير المصرح به (الاختراق):

يعد الدخول غير المشروع (Accès non autorisé) حكر الزاوية في الركن المادي لهذه الجرائم، ويقصد به تمكن الجاني من كسر الحواجز الأمنية للولوج إلى "قلب" النظام المعلوماتي الخاص بالبنك أو منصة الدفع الإلكتروني. ولا يشترط القانون وسيلة محددة لهذا الدخول، فقد يتم عبر استغلال ثغرة برمجية، أو استخدام برامج التجسس لسرقة كلمات المرور الخاصة بالمستهلكين. والتوسع في تحليل هذا الفعل يقودنا حتماً إلى صورة "البقاء غير المشروع"؛ فإذا كان الجاني قد وُلج إلى نظام الدفع بطريقة مشروعة في البداية (كموظف بنكي أو تقني مخول له الدخول) ثم استمر في التواجد داخل قاعدة بيانات الزبائن بعد انتهاء صلاحية دخوله أو خارج حدود مهامه الوظيفية بقصد التلاعب، فإن فعل "البقاء" هنا يشكل ركناً مادياً مكتملاً للجريمة، كونه ينتهك حرمة النظام المعلوماتي الخاص بالمعاملات المالية¹.

ب/- فعل عرقلة سير النظام والاعتداء المباشر على المعطيات:

تأخذ العرقلة طابعاً تعطيلاً يهدف إلى شل حركة نظام الدفع الإلكتروني، وهو فعل يستهدف "الخدمة" قبل أن يستهدف "المال" بذاته. ويتحقق ذلك من خلال إرسال البيانات الوهمية التي تفوق طاقة استيعاب خوادم البنك (Servers)، مما يؤدي إلى إبطاء النظام أو منعه من العمل بشكل طبيعي، وهو ما عاقب عليه المشرع الجزائري في المادة 394 مكرر¹ 2 تحت مسمى "العرقلة بطريق الغش المادي". وتبرز خطورة هذا الفعل في كونه غالباً ما يستخدم كغطاء إجرامي لإلهاء الفريق التقني بالبنك عن عمليات سحب أموال تتم في الخلفية، مما يجعل العرقلة فعلاً مكتملاً لجرائم الاستيلاء³.

(1) محمد الأمين بن خدة، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2012، ص 142.

(2) المادة 394 مكرر¹، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

(3) خالد ممدوح إبراهيم، جرائم نظام الدفع الإلكتروني، د.ف.ج، الإسكندرية، مصر، 2008، ص 198.

وهي إضافة رصيد مالي لحساب بنكي لم يقابل ببدل نقدي حقيقي. إن هذا الاعتداء الثلاثي على البيانات هو الذي يحقق النتيجة الجرمية المباشرة، وقد شدد المشرع العقوبة عليه في المادة 394 مكرر 2¹ لتصل إلى الحبس لمدة خمس سنوات، نظراً لما يلحقه من مساس بالثقة العامة والائتمان المالي الوطني.²

ثانياً: النتيجة الإجرامية (الضرر المالي أو الأمني): تعتبر النتيجة الإجرامية الأثر الخارجي المترتب على السلوك الإجرامي، وهي الركن الذي يكتمل به الكيان المادي للجريمة؛ وفي مجال جرائم الدفع الإلكتروني، لا تخرج هذه النتيجة عن كونها اعتداءً مادياً أو معنوياً يلحق بنظام المعالجة الآلية أو بالحقوق المالية والخصوصية الرقمية للمستهلك والبنك على حد سواء. وتتجلى النتيجة المالية كغاية أكثر شيوعاً في هذه الجرائم، حيث تتحقق بمجرد حدوث "نقل غير مشروع للقيم المالية" من حساب الضحية إلى حساب الجاني. ويذهب الفقه القانوني في هذا الصدد إلى أن النتيجة الإجرامية لا تشترط بالضرورة حيازة الجاني للمال حيازة مادية ملموسة، بل يكفي مجرد "القيد الحسابي الإلكتروني" الذي يثبت خروج المال من ذمة الضحية، وهو ما يقوض الثقة في نظام الدفع ككل³، وقد جعل المشرع الجزائري الاعتداء على الأموال عبر الوسائط الإلكترونية ظرفاً مشدداً، بالنظر إلى سرعة تحويل هذه المبالغ وصعوبة استردادها مقارنة بالسرققات التقليدية⁴.

(1) المادة 394 مكرر 2، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

(2) محمد الأمين بن خدة، المرجع السابق، ص 148.

(3) هلاي عبد الله أحمد، "جرائم الكمبيوتر والإنترنت"، د.ن.ع، القاهرة، 2011، ص 142.

(4) طاهري حسين، الحماية الجنائية للتجارة الإلكترونية في القانون الجزائري، مجلة المفكر، جامعة بسكرة، العدد 04، 2009، ص 92.

ثالثاً: الرابطة السببية وإشكالية الإثبات التقني: لا يكفي لقيام الركن المادي في جرائم الدفع الإلكتروني وجود سلوك إجرامي ونتيجة ضارة فحسب، بل يجب أن تتوافر "رابطة سببية" (Lien de causalité) تجمع بينهما، بحيث يكون السلوك التقني الذي أتاح للجاني هو السبب المباشر والمنتج في حدوث النتيجة الإجرامية، سواء كانت استيلاءً على أرصدة مالية أو تخريباً للمعطيات. وتثير هذه الرابطة إشكالات قانونية وفنية واسعة في الفضاء السيبراني نظراً لغياب التماس المادي المباشر بين الجاني والضحية، وتدخل عوامل تقنية وسيطة قد تقطع هذه السلسلة؛ فعلى الرغم من تطبيق القواعد العامة لإثبات السببية، إلا أن الفقه الجنائي الحديث يميل في مجال الدفع الإلكتروني إلى تبني نظرية "السبب الملائم". فلكي يسأل الجاني عن ضياع أموال المستهلك، يجب إثبات أن اختراقه أو إرساله لروابط التصيد هو الذي أدى، وفق السير العادي للأمر، إلى النتيجة الضارة¹.

وتتجلى خصوصية إثبات هذه الرابطة في ضرورة الربط الفني بين "الفعل التقني" و "الضرر المالي"؛ حيث يعتمد القضاء على ما يُعرف بـ "تتبع الأثر الرقمي". فالمعاينات الفنية تهدف إلى كشف الرابط المنطقي بين الثغرة التي استغلها الجاني (ككود برمجي خبيث) وبين لحظة خروج الأموال من حساب الضحية. ويتحقق هذا الإثبات من خلال مطابقة "البصمة الرقمية" للجاني مع سجلات النظام البنكي، بحيث يُستخلص تقنياً أن الفعل المرتكب لم يكن مجرد عامل ثانوي، بل كان هو "السبب المنتج" الذي أدى مباشرة لتعطيل آليات الحماية وتدمير العملية المالية غير المشروعة. إن هذا الترابط الفني هو الذي يسمح للقاضي الجنائي بالتيقن من أن الضرر المالي للمستهلك لم يكن نتيجة خلل برمجياً عارضاً في نظام البنك، بل نتيجة مباشرة لنشاط الجاني الإجرامي².

(1) جميل عبد الباقي الصغير، "قانون العقوبات - القسم العام"، د.ن.ع، القاهرة، 2011، ص 245.

(2) بوشقيف آمال، الحماية الجنائية للمستهلك عبر شبكة الإنترنت، أطروحة دكتوراة في الحقوق، جامعة جيلالي لباس - سيدي بلعباس، 2017، ص 165.

قد وقع بسبب قوة قاهرة أو خطأ جسيم من الضحية استغرق فعل الجاني بالكامل، فهنا فقط تنعدم الرابطة. ومع ذلك، غالباً ما يتخذ الجاني من "ضعف الوعي التقني للمستهلك" أداة لتنفيذ مأربه، وفي هذه الحالة لا ينفي خطأ الضحية مسؤولية الجاني، بل يُعتبر مجرد ظرف مساعد ساهم في وقوع الفعل. إن خصوصية السببية هنا تكمن في كونها "سببية افتراضية" يتم تتبع خيوطها عبر السجلات الإلكترونية، وهو ما استوجب الاعتماد على المعاينة الإلكترونية كوسيلة لإثبات الاتصال المباشر بين الفعل والنتيجة وفقاً للقانون 09-04¹.

رابعاً: الشروع في جرائم الدفع الإلكتروني والنصب المعلوماتي: تطرح مسألة في جرائم الدفع الإلكتروني تحديات قانونية وتقنية فريدة؛ حيث يثير تحديد "لحظة البدء في التنفيذ" إشكالات معقدة في البيئة الرقمية. فبموجب المادة 30 من قانون العقوبات الجزائري²، يتحقق الشروع بكل فعل لا ينقصه إلا العدول الإرادي أو تحقق النتيجة الإجرامية؛ كما تبرز معضلة التمييز بين "الأعمال التحضيرية" غير المعاقب عليها، وبين "البدء في التنفيذ" الذي يستوجب العقاب. فمحاولة اختراق أنظمة الدفع تضعنا أمام تساؤل جوهري حول كنه الأفعال المادية؛ إذ يذهب الاتجاه الفقهي السائد إلى أن البدء في التنفيذ يتحقق، أو بمجرد إطلاق الروابط المزيفة في جرائم "التصيد الاحتيالي"، كون السلوك قد خرج هنا من حيز الإعداد المكثبي إلى حيز التنفيذ المباشر الذي يستهدف سلب المعطيات المالية، حتى لو لم يرقم الضحية بإدخال بياناته فعلياً³.

(1) القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47.

(2) المادة 30، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

(3) بوشقيف آمال، الحماية الجنائية للمستهلك عبر شبكة الإنترنت، أطروحة دكتوراة في الحقوق، جامعة جيلالي ليايس - سيدي بلعباس، 2017، ص 170.

أما بخصوص معايير الشروع في جرائم النصب الإلكتروني، فإن الأمر يتخذ صبغة خاصة ترتبط بالوسائل الاحتيالية الرقمية؛ إذ يتحقق البدء في التنفيذ بمجرد صدور أفعال خارجية ملموسة تهدف إلى إيقاع المستهلك في الغلط. ويشمل ذلك البدء في استخدام برمجيات تزوير المواقع (Spoofing) أو إرسال رسائل تتضمن إغراءات مالية وهمية لحث الضحية على كشف بيانات بطاقته البنكية. فالمشروع الجزائري، ومن خلال القواعد العامة للنصب المطبقة في الفضاء الرقمي، يعتبر أن وضع "الخديعة الإلكترونية" موضع التنفيذ يخرج بالفعل من دائرة التحضير إلى دائرة الشروع المعاقب عليه، طالما أن الجاني قد استنفد وسائله الفنية للإيقاع بالضحية، ولم يحل دون وقوع النتيجة إلا يقظة المستهلك أو تدخل الأنظمة الأمنية للبنك. وتبرز الصعوبة هنا في التمييز بين مجرد "تطوير" البرنامج الاحتيالي كعمل تحضير، وبين "بنه" عبر الشبكة كبدء في التنفيذ يمثل تهديداً مباشراً وحالاً للذمة المالية¹.

وفيما يتعلق بالنتيجة الإجرامية في الشروع، فإن المشروع الجزائري قد ساوى في العقوبة بين الجريمة التامة والشروع فيها في أغلب الجرائم المعلوماتية نظراً لخطورتها العالية على الائتمان المالي، ولأن الضرر في البيئة الرقمية قد يقع بمجرد البدء في التنفيذ. ويشترط لقيام الشروع قانوناً عدم وجود "عدول اختياري"؛ فإذا توقف الجاني عن إتمام عملية الاختراق بمحض إرادته وقبل الوصول للمال نتيجة صحوة ضمير أو تراجع ذاتي، فإنه قد يفلت من العقاب، إلا إذا شكل فعله الأول جريمة مستقلة وقائمة بذاتها كالمساس العمدي بالمعطيات أو الدخول غير المصرح به للنظام²، مما يضمن تكييفاً قانونياً سليماً يتلاءم مع الطبيعة الافتراضية للجريمة ويحقق الردع المطلوب لحماية المستهلك الإلكتروني.

(1) عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت، د.ف.ج، الإسكندرية، مصر، 2007، ص 192.

(2) بوشقيف آمال، المرجع السابق، ص 174.

الفرع الثاني: الركن المعنوي والاختصاص القضائي

لا يكفي الركن المادي لقيام جريمة الدفع الإلكتروني بل يجب اقترانه بركن معنوي يجسد نية الجاني، وما يتبع ذلك من إشكالات في تحديد المحكمة المختصة وقانونها؛ و هي كالتالي:

*أولاً: القصد الجنائي العام في الجرائم الإلكترونية.

*ثانياً: القصد الجنائي الخاص ونية الاستيلاء.

*ثالثاً: مكان وقوع الجريمة في الفضاء السيبراني.

*رابعاً: تحديد القانون الواجب التطبيق.

أولاً: القصد الجنائي العام في الجرائم الإلكترونية: يُعد القصد العام المحرك الأساسي للمسؤولية الجنائية في جرائم الدفع الإلكتروني، حيث لا يكفي لوقوعها مجرد الخطأ المادي، بل يجب أن تتجه نية الجاني بوعي وإدراك نحو خرق النظم المعلوماتية. ويقوم هذا القصد على ركنين جوهريين متلازمين هما العلم والإرادة، وهو ما سنفصله فيما يلي:

أ/- عنصر العلم في القصد الجنائي العام

يقوم عنصر "العلم" كركيزة أولى له على إدراك الجاني إدراكاً يقينياً وشاملاً بأن نظام الدفع الذي يلج إليه أو المعطيات التي يتلاعب بها هي ملكية خاصة لغيره، مع علمه التام بأن فعله يشكل اعتداءً غير مصرح به قانوناً. ويترتب على ذلك انتفاء الركن المعنوي في حال ثبت أن الدخول لنظام الدفع كان وليد خطأ تقني غير مقصود لم يقصد الجاني استغلالها، إذ أن الجهل بتوفر الصفة غير المشروعة للسلوك يرفع المسؤولية الجنائية لعدم إحاطة العلم بعناصر الجريمة¹.

(1) المادة 394 مكرر، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

ب/- عنصر الإرادة وتوجيه السلوك الإجرامي:

أما عنصر "الإرادة"، فيقصد به انصراف نية الجاني الجازمة نحو تحقيق السلوك الإجرامي بمحض اختياره وحريته، وذلك من خلال توجيه نشاطه التقني لانتهاك حرمة الأنظمة المعلوماتية البنكية. وقد جسد المشرع الجزائري هذا العنصر من خلال اشتراط صبغة "العمد" أو "الغش" في نصوص قانون العقوبات، مؤكداً على ضرورة وجود رغبة واعية في إحداث النتيجة الإجرامية، وهو ما يخرج الأفعال الناتجة عن الإهمال أو الرعونة التقنية من دائرة التجريم العمدي لجرائم الدفع الإلكتروني¹.

ثانياً: القصد الجنائي الخاص ونية الاستيلاء: بالإضافة للقصد العام، يستلزم القضاء في جرائم الدفع الإلكتروني توافر "قصد جنائي خاص" يحدد الغاية النهائية من السلوك، وتتجلى أهمية هذا القصد بشكل صارخ في جريمة الاستيلاء على بيانات البطاقات البنكية. ففي هذه الصورة الإجرامية، لا يكفي القانون بإثبات علم الجاني بمكانة البيانات، بل يجب إثبات "نية التملك والاستيلاء" (Animus furandi) على الأرصدة المالية المرتبطة بتلك البيانات. إن إثبات القصد الخاص هنا هو الذي يميز بين "المخترق الهاوي" الذي يسعى لمجرد إثبات قدراته التقنية، وبين "المجرم المعلوماتي" الذي يستهدف المساس بالحقوق المالية للآخرين².

ويعتمد إثبات هذا القصد الخاص في البيئة الرقمية على مجموعة من القرائن المادية التي يستخلصها القاضي من فحوى السلوك الإجرامي؛ فقيام الجاني بتخزين بيانات البطاقات البنكية في ملفات مشفرة، أو محاولة بيعها في "الإنترنت المظلم" (Dark Web)، أو البدء في تجريب

(1) المادة 394 مكرر 2، نفس القانون.

(2) بوشقيف آمال، الحماية الجنائية للمستهلك عبر شبكة الإنترنت، أطروحة دكتوراة في الحقوق، قسم القانون، كلية الحقوق والعلوم السياسية، جامعة جيلالي لباس، سيدي بلعباس، الجزائر، 2017، ص 182.

صلاحيتها عبر عمليات شرائية صغيرة، كلها أدلة مادية تقطع بوجود "نية الاستيلاء". وقد شدد المشرع الجزائري العقوبات في حال اقتران الدخول غير المشروع بنية تخريب المعطيات أو الحصول على مبالغ مالية، معتبراً أن الضرر الواقع على المستهلك في هذه الحالة لا يمس ماله فحسب، بل يمس الثقة العامة في المنظومة الرقمية للدولة، وهو ما يبرز الأهمية القصوى لضبط القصد الخاص في توقيع العقوبة وتقدير جسامة الفعل الإجرامي¹.

ثالثاً: تحديد مكان وقوع الجريمة في الفضاء السيبراني: تطرح جرائم الدفع الإلكتروني إشكالية تحديد الحيز المكاني نظراً لطبيعتها العابرة للحدود، حيث يتلاشى المفهوم التقليدي للجغرافيا في ظل إمكانية توزيع الفعل والنتيجة والخادم بين دول مختلفة. ولحسم الاختصاص، برزت عدة اتجاهات فقهية أهمها "نظرية الوحدة" التي تعتبر الجريمة واقعة في كل مكان تحقق فيه جزء من ركنها المادي، سواء كان مكان الفعل أو مكان النتيجة أو حتى مكان مرور البيانات عبر الوسطاء التقنيين، وذلك بهدف سد الثغرات القانونية التي قد يستغلها المجرمون للإفلات من العقاب ومنع تنازع الاختصاص القضائي الدولي².

كما يبرز معيار "محل وجود نظام المعالجة الآلية" كأداة فعالة لحماية البنية التحتية المالية الوطنية، حيث تنعقد السيادة القضائية للدولة التي يقع فيها نظام البنك المستهدف بالقرصنة. وقد تبنى المشرع الجزائري توجهاً مرناً بموجب القواعد الخاصة بالوقاية من الإجرام المعلوماتي ومكافحته، إذ يمتد اختصاصه ليشمل كل فعل يقع أحد أركانه في الجزائر أو يمس مصالحها الحيوية، مسنداً ذلك

(1) خالد ممدوح إبراهيم، جرائم الكمبيوتر والإنترنت، د.ف.ج، الإسكندرية، مصر، 2009، ص 230.

(2) المادة 588 مكرر، الأمر رقم 66-155، المؤرخ في 08 جوان 1966، المتضمن ق.إ.ج، المعدل والمتمم.

لقطب جزائي وطني متخصص يمتد اختصاصه عبر كامل التراب الوطني لملاحقة هذه الجرائم بغض النظر عن مكان تواجد الجاني الفعلي¹، وهو ما يعكس رغبة المشرع في تجاوز العقوبات الإقليمية التقليدية من خلال منح هذا القطب صلاحيات إجرائية واسعة تمكنه من اختراق حواجز "الافتراضية" التي يتحصن خلفها المجرم المعلوماتي.

رابعاً: تحديد القانون الجنائي الواجب التطبيق (مبدأ الإقليمية): تعتبر مسألة تنازع القوانين من حيث المكان من أعقد الإشكالات التي تواجه القاضي الجنائي عند النظر في جرائم الدفع الإلكتروني؛ فبمجرد تحديد مكان وقوع الجريمة، و هو ما يجعلنا نقول القانون الواجب التطبيق هو قانون الدولة التي انطلق منها السلوك الإجرامي، أم قانون الدولة التي تحقق فيها الضرر المالي للمستهلك إن الأصل في التشريعات الجنائية هو "مبدأ إقليمية القوانين"، إلا أن الطبيعة الافتراضية لهذه الجرائم استوجبت البحث عن قواعد أكثر مرونة تضمن عدم إفلات الجاني من العقاب؛ وسنفصل في ذلك وفق الآتي:

أ/-إعمال مبدأ الإقليمية في الفضاء السيبراني:

يقضي مبدأ الإقليمية بخضوع كافة الجرائم المرتكبة فوق إقليم الدولة لقانونها الوطني، وبما أن جرائم الدفع الإلكتروني تقع عبر شبكة دولية، فقد توسع الفقه في تفسير "الإقليم" ليشمل الإقليم الافتراضي التابع للدولة، والمتمثل في الخوادم والنطاقات الوطنية. فمتى ثبت أن النشاط الإجرامي قد مس سلامة نظام دفع إلكتروني داخل الجزائر، فإن القانون الجنائي الجزائري يكون هو الواجب التطبيق حتماً، بغض النظر عن جنسية الفاعل أو مكان تواجده المادي².

(1) هشام محمد رستم، قانون العقوبات و مخاطر تقنية المعلومات، م.أ.م، سيوط، مصر 1994، ص 180

(2) خالد ممدوح إبراهيم، جرائم الكمبيوتر والإنترنت، د.ف.ج، الإسكندرية، مصر، 2009، ص 275.

ب/- الاستثناءات الواردة على مبدأ الإقليمية (المنازعات الدولية):

نظراً لهروب المجرمين المعلوماتيين خلف الحدود الرقمية، تبنت التشريعات الحديثة، ومنها التشريع الجزائري، مبادئ تكميلية لمبدأ الإقليمية؛ مثل "مبدأ الشخصية" (تطبيق القانون على الجزائري الذي يرتكب جريمة في الخارج) و"مبدأ العالمية" في حالات محددة. وتبرز أهمية هذه المبادئ في سد الثغرات القانونية؛ فإذا قام شخص بمهاجمة نظام بنكي جزائري من دولة لا تجرم هذا الفعل، فإن القضاء الجزائري يملك سلطة تطبيق قانونه الوطني بناءً على "مبدأ حماية المصلحة الوطنية"¹

ج/- موقف المشرع الجزائري وتعديلات قانون العقوبات:

أكد المشرع الجزائري على اختصاص القانون الوطني في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال نصوص صريحة في قانون الإجراءات الجزائية والقانون 09-2004. وقد تعزز هذا التوجه في التعديلات التشريعية الأخيرة بموجب القانون 24-2006، الذي رفع من سقف العقوبات لتشمل صوراً مستحدثة من الجرائم المالية الرقمية، مؤكداً على سريان القانون الجزائري على كل فعل يمس بالمنظومة البنكية الوطنية حتى لو تم ارتكابه عبر وسائط تقنية خارج الحدود الجغرافية. إن هذا "التمدد القانوني" يهدف في جوهره إلى خلق بيئة دفع إلكتروني آمنة ومحمية بقوة القانون ضد الهجمات السيبرانية أياً كان مصدرها التقني أو الجغرافي .

(1) المرجع نفسه، ص276.

(2) القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47.

(3) القانون رقم 24-06، المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات ج.ر، العدد 30، الصادرة بتاريخ 29 أبريل 2024.

المطلب الثاني: آليات إثبات الجريمة الإلكترونية وتحديد المسؤولية الجنائية

تستوجب الطبيعة الافتراضية لجرائم الدفع الإلكتروني وجود نظام إثبات يتلاءم وخصوصيتها الرقمية، مع ضرورة تحديد نطاق المسؤولية الجنائية للأطراف المتدخلة في عملية الوفاء؛ ولإحاطة بهذا الموضوع، سنحاول دراسة الآليات التقنية والقانونية المعتمدة في الإثبات وكيفية إسناد المسؤولية الجنائية، وذلك وفق التقسيم الآتي:

الفرع الأول: الطبيعة الخاصة للدليل الإلكتروني وحجته في الإثبات.

الفرع الثاني: المسؤولية الجنائية للأشخاص الطبيعية والمعنوية في جرائم الدفع الرقمي.

الفرع الأول: الطبيعة الخاصة للدليل الإلكتروني وحجته

تتميز جرائم الدفع الإلكتروني بكونها مخلفات رقمية لا تترك وراءها آثاراً مادية ملموسة بالمعنى التقليدي، مما يستوجب الاعتماد على نوع مستحدث من الأدلة يستمد قوته من الوسائط التقنية. ونظراً لسرعة محو هذه الأدلة وسهولة التلاعب بها، كان لزاماً البحث في ماهيتها وشروط قبولها قانوناً؛ وعليه، و سنفصل في هذا الفرع في كل من :

أولاً: مفهوم الدليل الرقمي وأنواعه (السجلات، البصمات)

ثانياً: شروط قبول وحجية الدليل الإلكتروني في الإثبات

ثالثاً: سلامة سلسلة حفظ الدليل الرقمي وعدم التلاعب به

رابعاً: دور الخبرة الفنية في كشف الجريمة وضبط الأثر الرقمي

أولاً: مفهوم الدليل الرقمي وأنواعه (السجلات، البصمات): يمثل الدليل الرقمي (Prevue numérique) حجر الزاوية في منظومة الإثبات الخاصة بجرائم الدفع الإلكتروني، وهو يختلف جوهرياً عن الأدلة المادية التقليدية بكونه كياناً غير ملموس، يعتمد في وجوده على نبضات إلكترونية ومجالات مغناطيسية مخزنة داخل وسائط تقنية. ونظراً لأن الاعتداء على أنظمة الدفع يتم في فضاء افتراضي، فإن الأثر الذي يتركه الجاني غالباً ما يكون مجرد بيانات برمجية تستلزم أدوات فنية دقيقة لاستخراجها وتفسيرها؛ وسنفصل في ماهية هذا الدليل وأنواعه وفق المعايير التالية:

أ/-تعريف الدليل الرقمي وخصائصه:

يمكن تعريف الدليل الرقمي من منظور قانوني وفني بأنه كل معلومة لها قوة استدلالية، تكون مخزنة أو منقولة في شكل رقمي، ومستخلصة من أجهزة الحاسوب أو شبكات الاتصال، بحيث يمكن استخدامها لإثبات أو نفي نية ارتكاب جريمة تمس أنظمة المعالجة الآلية للمعطيات المالية، تكمن خصوصية هذا الدليل في كونه عابراً للحدود، وسهل المحو أو التعديل دون ترك أثر مرئي، مما يجعل حجته مرتبطة بمدى سلامة الوسيط التقني والتدابير الأمنية المحيطة به ¹. اعترف المشرع الجزائري ضمناً بالدليل الرقمي، حيث نصت المادة 323 مكرر 1 ² من القانون المدني على أن الكتابة الإلكترونية تتمتع بنفس حجية الكتابة الورقية، متى أمكن تحديد هوية من أصدرها وكانت محفوظة في ظروف تضمن سلامتها. وهذا الاعتراف التشريعي يمتد ليشمل كافة الأدلة المستخلصة من وسائط الدفع الإلكتروني متى توفرت فيها الشروط الفنية اللازمة والقوة الاستدلالية المقنعة للقاضي الجنائي .

(1) ياسر اللامي، المسؤولية الجنائية والمدنية في جرائم الدفع الإلكتروني، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، مصر، العدد 35، ص 192.

(2) المادة 323 مكرر 1، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005.

(3) المرجع السابق، ص 195

ب/-أنواع الأدلة الرقمية في جرائم الدفع الإلكتروني:

تتعدد صور الأدلة الرقمية التي يتم الاعتماد عليها لكشف التلاعبات المالية، ومن أبرزها:

(1) السجلات الإلكترونية: وهي الملفات التي تدون آلياً كل نشاط تم على نظام الدفع، كوقت الدخول، رقم المستخدم، والعمليات المنفذة؛ وتعتبر هذه السجلات بمثابة "الصندوق الأسود" الذي يكشف حركة الجاني داخل المنصة البنكية وتعد أدلة مادية تربط الجاني بمسرح الجريمة الافتراضي¹، حيث تكمن أهميتها الإجرائية في استحالة تعديلها أو محوها دون ترك أثر رقمي مواز. مما يمنحها حجية قانونية في مواجهة محاولات التنصل من المسؤولية.

(٢) الروابط المزيفة ومواقع التصيد: في جرائم الاحتيال عبر الإنترنت، يعد الرابط الإلكتروني المزور الذي استخدمه الجاني دليلاً مادياً رقمياً يثبت استخدام طرق احتيالية لسلب بيانات بطاقة الدفع الخاصة بالمستهلك، حيث يمثل الوسيلة المادية لإيقاع الضحية في الغلط، ويأخذ هذا الدليل أهميته من كونه يجسد "المناورات التدليسي" في ثوبها الرقمي، مما يسهل على القاضي تكييف الفعل كجريمة نصب إلكتروني مكتملة الأركان، خاصة عند إثبات الارتباط التقني بين ذلك الرابط وبين الخادم الذي يتحكم فيه الجاني لاستقبال البيانات المسلوقة، وهو ما يعزز من فاعلية الملاحقة القضائية عبر تتبع البصمات الرقمية التي يتركها الجاني خلفه أثناء عملية الاستدراج².

(3) البصمة الرقمية (Hash Value): وهي قيم خوارزمية فريدة تميز ملفاً عن آخر؛ وتستخدم للتأكد من أن بيانات الدفع (كالرصيد أو رقم الحساب) لم يتم تعديلها أو التحريف فيها منذ لحظة ضبطها وحتى عرضها على القضاء، مما يضمن "سلامة الدليل" من الناحية الفنية وتعتبر

(1) ياسر اللمعي، المرجع السابق، ص 197.

(2) المرجع نفسه، ص 199.

هذه البصمة بمثابة "الختم الرقمي" غير القابل للتزوير، حيث تتيح للمحكمة التحقق من مطابقة الدليل الرقمي المعروض لأصله المستخرج من مسرح الجريمة، مما يوصد الباب أمام أي طعون تتعلق بالعبث بمحتوى البيانات المالية أو تغيير معالمها البرمجية أثناء فترة التحقيق¹.

(٤) التوقيع الإلكتروني: ويُعرف بأنه أداة تسمح بتحديد هوية الموقع على المعاملة المالية، وتعتبر عن إرادته بالموافقة على مضمونها؛ ويعد التوقيع دليلاً حاسماً في إثبات أو نفي انتساب عملية التحويل المالي للشخص المقيد بحسابه، كما يضيف صبغة رسمية وقانونية على المحرر الإلكتروني تتساوى مع التوقيع اليدوي².

ثانياً: شروط قبول وحجية الدليل الإلكتروني في الإثبات: لا يكفي القاضي الجنائي بمجرد تقديم مخرجات رقمية للتدليل على وقوع جريمة دفع إلكتروني، بل لا بد من إخضاع هذا الدليل لمعايير صارمة تحدد مدى صلاحيته للاستناد إليه في الحكم القضائي. وتعتبر مسألة "الحجية" هي التحدي الأكبر، نظراً لإمكانية التلاعب بالبيانات وتغييرها دون ترك آثار مرئية، وهو ما فرض وجود شروط تقنية وقانونية تضمن موثوقية هذا الدليل؛ وسنفصل فيها وفق الآتي:

أ /-الشروط الموضوعية والتقنية لقبول الدليل:

لكي يتمتع الدليل الرقمي بالحجية المطلوبة، يجب أولاً إثبات "تكامل البيانات" (Data Integrity)، ويقصد بذلك ضرورة خلو الدليل من أي تبديل أو تحريف منذ لحظة إنشائه أو

(1) داود مسعود، دور التحكيم الإلكتروني في تسوية منازعات التجارة الدولية، مذكرة ماستر في الحقوق، تخصص قانون دولي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2014، ص 197.

(2) المرجع نفسه، ص 82.

تخزينه وحتى لحظة عرضه على جهات القضاء. ويتحقق ذلك تقنياً عبر الاعتماد على أنظمة التشفير المتطورة وشهادات التصديق الإلكتروني التي تمنح المعاملة المالية "صفة الثبات" واليقين كما يشترط في الدليل أن يكون مستخرجاً من نظام معالجة آلية موثوق، يتوفر على سجلات دقيقة ومحمية لا تسمح بالولوج غير المصرح به؛ فالحجية هنا لا تقع على الدليل في حد ذاته فحسب، بل تمتد لتشمل "المنظومة التقنية" التي أنتجته ككل¹.

ب/-الشروط القانونية وحجية الدليل في التشريع الجزائري:

من الناحية القانونية، يجب أن يكون الدليل الرقمي قد ضُبط بطريقة مشروعة لا تصطدم بمبادئ حماية الخصوصية أو تخالف إجراءات التفتيش والضبط المقررة قانوناً، وقد حسم المشرع الجزائري الجدل الفقهي حول حجية هذه الأدلة من خلال المادة 323 مكرر 1 من القانون المدني² التي ساوت صراحة بين الكتابة الإلكترونية والورقية في الإثبات، شريطة إمكانية تحديد هوية الشخص الذي أصدرها وحفظها في ظروف تضمن سلامتها التقنية من أي تدخل خارجي، أما في المسائل الجنائية، وبالرغم من خضوع الدليل لمبدأ «الاقتناع الشخصي للقاضي»، إلا أن القاضي يجد نفسه مقيداً بالتقرير الفني الذي يثبت سلامة الدليل من الناحية التقنية.³ وهذا تصبح، «الموثوقية التقنية» هي المدخل الأساسي المباشر لـ «الحجية القانونية» في جرائم الدفع الإلكتروني، وهو ما يفرض على الجهات القضائية الاستعانة بـ "الخبرة الرقمية" كإجراء جوهري لا يهدف فقط لاستخلاص الدليل، بل لتحسينه من الطعون القانونية التي قد تثار حول التلاعب بمحتواه المعلوماتي.

(1) المرجع نفسه، ص 88.

(2) المادة 323 مكرر 1، الفقرة 02، الأمر رقم 58-75، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005..

(3) المادة 02، القانون رقم 04-15، المؤرخ في 2004/11/10، المعدل والمتمم للأمر رقم 66-156 قانون العقوبات.

ثالثاً: سلامة سلسلة حفظ الدليل الرقمي وعدم التلاعب به: تعتبر سلامة سلسلة الحفظ الضمانة الجوهرية والعمود الفقري لقبول الدليل الرقمي في جرائم الدفع الإلكتروني؛ فبسبب الطبيعة "الهشة" للمعطيات المعلوماتية وسهولة تحريفها أو طمس معالمها بضغط زر واحدة دون ترك آثار مادية مرئية، يتوجب على جهات التحقيق والجهات التقنية إثبات أن الدليل المستخرج من أنظمة المعالجة الآلية هو ذاته الذي عُرض على المحكمة دون أدنى تغيير أو عبث. إن الحفاظ على "عذرية الدليل الرقمي" يتطلب تضافر الجهود التقنية و القانونية ؛ وسنفصل في هذه الآليات وفق الآتي:

أ/- الضوابط التقنية لضمان ثبات ودوام الدليل الرقمي:

لكي يكتسب الدليل الرقمي حجية كاملة، يجب أن يخضع لبروتوكولات فنية تمنع التعديل عليه منذ لحظة رصده وضبطه؛ ومن أهم هذه الوسائل نجد تقنية "البصمة الزمنية" التي تعمل على توثيق لحظة استخراج الدليل بدقة متناهية، مما يمنع التلاعب بالمدى الزمني للجريمة².

ب/- الحماية القانونية للدليل الرقمي من التحريف العمدي :

لم يقف المشرع الجزائري مكتوف الأيدي أمام مخاطر التلاعب بالأدلة الرقمية، بل كرس مبدأ سلامة الدليل كشرط لصحة الإثبات؛ فبموجب المادة 323 مكرر 1 من القانون المدني³، عُلقت حجية الكتابة الإلكترونية على شرط جوهري وهو حفظها في ظروف تضمن سلامتها من أي تدخل خارجي .

(1) داود مسعود، دور التحكيم الإلكتروني في تسوية منازعات التجارة الدولية، مذكرة ماستر في الحقوق، تخصص قانون دولي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2014، ص 82.

(2) المادة 323 مكرر 1، القانون السابق.

(3) ياسر اللامي، المسؤولية الجنائية والمدنية في جرائم الدفع الإلكتروني، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، مصر، العدد 35، ص 83.

رابعاً: دور الخبرة الفنية في كشف الجريمة وضبط الأثر الرقمي: نظراً للطبيعة التقنية المعقدة لجرائم الدفع الإلكتروني، يجد القاضي الجنائي نفسه أمام أدلة رقمية تتجاوز في جوهرها معارفه القانونية التقليدية، مما يجعل الاستعانة بـ "الخبرة الفنية" (Expertise technique) ضرورة حتمية لا ترفاً إجرائياً؛ فالخبير المعلوماتي هو من يمنح الدليل الرقمي "الروح" والوضوح عبر فك التشفير وتحليل البيانات المستخلصة من أنظمة الدفع، وسنفصل في هذا الدور الحيوي وفق الآتي:

أ/- جوهر الخبرة الفنية في التعامل مع الأثر الرقمي:

تتمثل المهمة الأساسية للخبير الفني في "استنطاق" الوسائط الإلكترونية للكشف عن المسار الإجرامي الذي سلكه الجاني؛ ففي حالات اختراق حسابات الدفع أو تزوير البطاقات البنكية، يتولى الخبير تحليل "سجلات الأحداث" وتتبع "العناوين البروتوكولية" (IP Address) لتحديد نقطة الانطلاق الجغرافية للهجوم وتاريخه بدقة. إن دور الخبير هنا لا يقتصر على مجرد تقديم تقرير فني، بل يمتد ليكون صلة الوصل بين التكنولوجيا والقانون، حيث يعمل على تحويل الأكواد البرمجية المعقدة إلى وقائع مادية يستطيع القاضي بناء قناعته الشخصية عليها¹.

ب/- النطاق القانوني للخبرة في التشريع الجزائري والمهام المستحدثة:

منح المشرع الجزائري صلاحيات واسعة لجهات التحقيق للاستعانة بال خبراء أو أي شخص لديه معرفة فنية بأنظمة المعالجة الآلية للمعطيات، وهو ما أكدته القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها². ويشمل نطاق الخبرة الفنية اليوم مهاماً دقيقة

(1) المرجع نفسه، ص 62.

(2) المادة 16، القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47، الصادرة بتاريخ 16 أوت 2009.

مثل "التفتيش الإلكتروني" و"الضبط الرقمي" للبيانات المشفرة التي تخص عمليات الدفع، مع إلزام مقدمي الخدمات والمهنيين - كالبانوك والمؤسسات المالية - بالتعاون الفني لتسهيل مأمورية الخبراء فيتتبع حركة الأموال الرقمية وضمان سلامة المستند من أي تلاعب قد يطاله أثناء مرحلة التحقيق¹، ويعد تقرير الخبرة الفنية في هذا الصدد ركيزةً جوهريةً يستند إليها القاضي في بناء قناعته، خاصة وأن استخلاص الأدلة من بيئة الدفع المعقدة يتطلب "حياداً تقنياً" يضمن عدم المساس بسرية المعطيات البنكية للمستهلك خارج نطاق الجريمة المبحوث عنها².

الفرع الثاني: تحديد مسؤولية الفاعل والمساهمين والشخص المعنوي

تستوجب الطبيعة الخاصة لجرائم الدفع الإلكتروني البحث في كيفية إسناد المسؤولية الجنائية لأطرافها، نظراً لتعدد المتدخلين وصعوبة تحديد الفاعل الحقيقي في الفضاء الافتراضي. ومن هذا المنطلق، m و سنفصل في هذا الفصل على :

*اولاً: تحديد مسؤولية الفاعل والمساهمين في جرائم الدفع الإلكتروني.

*ثانياً: مسؤولية البنك والوسطاء التقنيين في وقوع الضرر الإلكتروني

*ثالثاً: المسؤولية الجنائية للشخص المعنوي في جرائم الدفع الإلكتروني

*رابعاً: إجراءات التحري والتحقيق في جرائم الدفع الإلكتروني

(1) المادة 16، القانون نفسه.

(2) ياسر الدمي، المسؤولية الجنائية والمدنية في جرائم الدفع الإلكتروني، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، مصر، العدد 35، ص 233.

اولاً: تحديد مسؤولية الفاعل والمساهمين في جرائم الدفع الإلكتروني: تطرح جرائم الدفع الإلكتروني إشكالات قانونية بالغة التعقيد عند محاولة إسناد المسؤولية الجنائية لمرتكبيها؛ إذ تفرض الطبيعة "اللامادية" لهذه الجرائم تحديات جسيمة أمام جهات التحقيق، خاصة في ظل إمكانية تنفيذها عبر وسائط تقنية عابرة للحدود وبسرعات فائقة تتيح للجاني التخفي خلف هويات رقمية مستعارة. و هذا ما سنفصله كتالي:

أ/- المسؤولية الجنائية للفاعل الأصلي في ظل السياسات التشريعية المعاصرة:

يُعد الفاعل الأصلي الشخص المضطلع بالتنفيذ المادي للاختراق أو الاستيلاء على بيانات الدفع، وقد واجهه المشرع بنصوص صريحة، حيث نصت المادة 323 مكرر 1 من قانون العقوبات على أنه: « يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج، كل من دخل أو بقي عن طريق الغش، في كل أو جزء من منظومة للمعالجة الآلية للمعطيات »¹. وتنهض مسؤوليته بمجرد الولوج غير المشروع، كما تمتد لتشمل المورد الملزوم بضمان مطابقة المحتوى الرقمي والتبصير ببيانات الخدمة، رهن المسؤولية في حال إحداث الغلط لدى المستهلك².

ب/- المساهمة الجنائية والاشتراك الفني في الجريمة:

تتخذ المساهمة الجنائية طابعاً تقنياً يتمثل في توفير الوسائل كفك الشفريات أو تقديم "التوقيع الإلكتروني" بطرق غير مشروعة لتسهيل مهمة الفاعل الأصلي، وهو ما أخضعه المشرع للقواعد العامة في المادة 44 من قانون العقوبات التي تعامل المساهم كالفاعل الأصلي عقاباً².

(1) المادة 323 مكرر 1، الأمر رقم 66-156، المؤرخ في 08/06/1966، المتضمن قانون العقوبات، المعدل و المتمم

(2) المادة 44، نفس القانون.

ثانياً: مسؤولية البنك والوسطاء التقنيين في وقوع الضرر الإلكتروني: تعد المؤسسات المصرفية والوسطاء التقنيون حجر الزاوية في نظام الدفع الإلكتروني، مما يلقي على عاتقهم مسؤولية مزدوجة ذات أبعاد تقنية وقانونية؛ فالمصرف في البيئة الرقمية ليس مجرد ناقل للأموال بل هو الضامن الأول لسلامة القنوات المشفرة التي تمر عبرها التدفقات المالية. وتثور إشكالية المسؤولية الجنائية والمدنية عندما يقع ضرر للمستهلك نتيجة اختراق أو قصور في أنظمة الحماية وسن فصل فيها وفق الآتي:

أ/- الالتزام بضمان سلامة المحتوى والخدمة الرقمية:

يقع على عاتق المصرف أو المورد التزام مستمر بضمان مطابقة المحتوى الرقمي للخدمة المتعاقد عليها طوال مدة سريان العقد، وهو التزام لا يقبل التجزئة. وبناءً على ذلك، نجد أن التشريعات الحديثة (كالتوجه الأوروبي والفرنسي) أوجبت على المهني إعلام المستهلك بكافة البيانات المتعلقة بوسائل الدفع ومصاريف التشغيل، وهو ما يعرف بـ "الالتزام بالتبصير"¹.

إن أي قصور في تأمين "المحفظة الإلكترونية الافتراضية" — وهي التطبيقات التي تسمح بشحن الرصيد والتحويل اللحظي — يرتب مسؤولية المؤسسة المصدرة لها، خاصة إذا ثبت أن الجاني استغل ثغرة في أنظمة التشفير كان يمكن تلافيها بالحيلة والحذر²، وفي هذا الصدد، يمكننا الاستناد لما ورد في مدونة حماية المستهلك الفرنسية (المادة 3-L217) التي تشدد على أن أي خلل في الأداء الرقمي يعتبر قرينة على تقصير المورد في التزاماته الضمانية³.

(1) المادة 323 مكرر 1، الأمر رقم 58-75، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

(2) شريف محمد غنام، محفظة النقود الإلكترونية: رؤية مستقبلية، جامعة الإمارات العربية المتحدة، 2003، ص 105.

(3) L'article L217-3, Code de la consommation (France), modifié par l'ordonnance n° 2021-1247 du 29 septembre 2021 relative à la garantie légale de conformité pour les biens, les contenus numériques et les services numériques.

ب/-المسؤولية عن مخاطر "التصيد الإلكتروني" وقصور الرقابة:

يعتبر "التصيد الإلكتروني" (Phishing) من أخطر صور الاعتداء المالي، حيث يتم إيهام المستهلك بتحديث بياناته عبر روابط مزيفة. وهنا تبرز مسؤولية البنك في توفير "بيئة آمنة" للتداول؛ فالمستهلك الذي يقع ضحية لهذا الخداع يستند غالباً إلى ضعف أنظمة التأمين ثنائية المرحلة التي يلتزم البنك بتوفيرها. وبالرجوع لأحكام التشريع الجزائري، نجد أن البنك يسأل عن الإهمال في مراقبة العمليات المشبوهة أو الفشل في حماية "التوقيع الإلكتروني الموثق" الذي يعبر عن رضا العميل.

ولقد عرّف الفقه التوقيع الإلكتروني الموثق باقتباس مباشر نصه:

« هو كل علامة تتخذ شكل حروف أو أرقام أو إشارات أو أصوات مدرجة بشكل إلكتروني صادرة من شخص تسمح بتحديد شخص الموقع وتعتبر عن رضاه »¹.

وعليه، فإن أي اختراق لهذا التوقيع نتيجة ضعف شهادات التصديق يضع الوسطاء تحت طائلة المسؤولية. وفي حال نشوب نزاع، تلعب مراكز التحكيم الإلكتروني (مثل منظمة الويبو² OMPI وغرفة التجارة الدولية CCI)³ دوراً حيوياً، حيث تشترط معايير صارمة للخبرة التقنية والحياد في المحكمين الذين يفصلون في هذه المسؤولية، لضمان حماية حقوق المستهلك أمام القوة التقنية والمالية للمؤسسات المصرفية .

(1) داود مسعود، دور التحكيم الإلكتروني في تسوية منازعات التجارة الدولية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون دولي خاص، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح - ورقلة، 2014، ص 82.

(2) المادة 15، قواعد الويبو للتحكيم، مركز الويبو للتحكيم والوساطة، المنظمة العالمية للملكية الفكرية (WIPO)، النافذة اعتباراً من 01/2021.

(3) المادة 10، قواعد التحكيم لغرفة التجارة الدولية (ICC)، باريس، فرنسا، النسخة النافذة اعتباراً من 01 جانفي 2021.

ثالثاً : المسؤولية الجنائية للشخص المعنوي في جرائم الدفع الإلكتروني : لم تعد الجريمة في البيئة الرقمية تقتصر على النشاط الفردي المحدود، بل أضحت تتم غالباً تحت غطاء كيانات مؤسسية تملك الإمكانيات التقنية والمالية والبرمجية لتنفيذ عمليات دفع مشبوهة أو التستر عليها. ونظراً لخطورة هذه الأنشطة على الاستقرار المالي والسيادة الرقمية، أقر المشرع مبدأ المسؤولية الجنائية

أ/- معايير إسناد المسؤولية الجنائية للشخص المعنوي:

لا تقوم مسؤولية المؤسسة (كالبنك أو منصة الدفع الرقمية) بشكل تلقائي، بل استلزم المشرع توافر شروط موضوعية دقيقة؛ حيث نصت المادة 15 مكرر¹ من قانون العقوبات على مبدأ عام مفاده أن الشخص المعنوي يسأل عن الجرائم التي تُرتكب لحسابه من طرف أعضائه .

ب/- النظام العقابي المقرر للشخص المعنوي في التشريع الجزائري:

نظراً لطبيعة الشخص المعنوي الاعتبارية، استحدث المشرع في قانون العقوبات والقانون 04-09² منظومة جزائية خاصة تتناسب مع كيانه الاقتصادي؛ وبموجب المادة 18 مكرر³، فإن العقوبة الأساسية هي الغرامة المالية التي تكون مغلظة جداً، حيث نصت المادة على ما يلي:

« تتراوح الغرامة المطبقة على الشخص المعنوي ما بين خمس (5) إلى عشر (10) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة » .

(1) المادة 15 مكرر، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004.

(2) القانون رقم 04-09، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(3) المادة 18 مكرر، الأمر رقم 66-156، المتضمن قانون العقوبات الجزائري، المعدل والمتمم.

وبالإضافة للغرامة، أقر المشرع عقوبات "تبعية" تهدف إلى شل النشاط الإجرامي للمؤسسة، كالمصادرة للوسائل والبرمجيات المستخدمة، والمنع من ممارسة النشاط لفترة محددة، وصولاً إلى عقوبة "الحل" النهائي في حال ثبت أن الكيان قد أنشئ أساساً لغرض إجرامي أو غسيل أموال رقمي. كما تبرز عقوبة "نشر الحكم" في الصحف الوطنية كجزاء معنوي قاصد لضرب السمعة التجارية للمؤسسة، مما يشكل رادعاً قوياً يفرض على المؤسسات المالية الالتزام الصارم بمعايير الحوكمة الرقمية¹.

رابعاً: إجراءات التحري والتحقيق في جرائم الدفع الإلكتروني: تتطلب هذه الجرائم منظومة إجرائية خاصة تتجاوز القواعد التقليدية، نظراً للطبيعة الافتراضية للأدلة وسرعة تلاشيها، مما يستلزم مهارات تقنية عالية لضبط المعطيات دون المساس بسلامتها. ويختلف التفتيش هنا بكونه ينصب على "محتوى غير مادي" مخزن داخل وسائط أو سحابات رقمية، حيث يشمل الولوج لأنظمة المعالجة الآلية لضبط السجلات (Logs) وتتبع العمليات المشبوهة. وفي هذا الصدد، أوجب القانون على مقدمي الخدمات والوسطاء التقنيين التعاون مع جهات التحقيق لتحديد هوية المستخدمين وتتبع التدفقات المالية، بما في ذلك "الاعتراض القانوني للمراسلات" وواجب "الحفظ الاستباقي" للبيانات لفترة محددة قانوناً. ومن أجل تفعيل هذه الآلية، أقر المشرع الجزائي تدابير زجرية صارمة ضد كل مقدم خدمة يمتنع عن تنفيذ تسخيرات السلطة القضائية أو يعرقل التحريات، باعتبار هؤلاء الوسطاء هم "الحراس التقنيين" لبوابات الدفع، وبدون تعاونهم تظل جهود التحقيق عاجزة عن اختراق جدار التشفير الرقمي، وهو ما يجسد مفهوماً حديثاً للمسؤولية القانونية التضامنية الهادفة لتحقيق استقرار المنظومة المالية الافتراضية وحماية الحريات الفردية في آن واحد².

(1) ياسر اللامي، المسؤولية الجنائية والمدنية في جرائم الدفع الإلكتروني، مجلة روح القوانين، العدد 103، الجزء 01، 2023، ص 246.

(2) المرجع نفسه، ص 249.

نخلص في ختام هذا الفصل إلى أن نظام الدفع الإلكتروني ليس مجرد آلية تقنية لنقل الأموال، بل هو منظومة قانونية وعقدية متكاملة فرضت واقعاً جديداً يتجاوز مفاهيم الوفاء التقليدي، مما استوجب على المشرع الجزائري التدخل بمرونة لضبط مراكز أطرافها وحماية الطرف الضعيف فيها وهو المستهلك. وقد تبين لنا أن خطورة الجرائم المرتبطة بهذه المنظومة تكمن في طبيعتها الافتراضية العابرة للحدود، والتي أفرزت أنماطاً إجرامية مستحدثة كالتصيد والاختراق والتزوير المعلوماتي، مما خلق تحديات جسيمة في تحديد البنيان القانوني للجريمة الرقمية وقواعد إثباتها. إن الانتقال من مادية الشيء إلى رقمية المعطى أدى بالضرورة إلى تحول في مفاهيم الركن المادي والمعنوي، وصولاً إلى الاعتراف بالحجية القانونية للدليل الإلكتروني كحجر زاوية في الإثبات الجنائي. وعليه، فإن هذا الإطار النظري والمفاهيمي يشكل الأساس المتين الذي سنبنى عليه دراستنا في الفصل الموالي، لتعمق في آليات الحماية الإجرائية وسبل تفعيل المسؤولية الجنائية لمواجهة هذه الاعتداءات وتأمين المعاملات المالية الرقمية.

الفصل الثاني

النظام القانوني لحماية المستهلك في الدفع الإلكتروني

تعد المسألة المتعلقة بتحديد المسؤولية القانونية في بيئة الدفع الإلكتروني من أعقد الإشكالات التي تواجه المشرع والقضاء على حد سواء، نظرًا لخصوصية هذه المعاملات التي تتم في فضاء رقمي عابر للحدود والمكان، وتتداخل فيها أطراف متعددة من مستهلكين، مؤسسات مصرفية، ومقدمي خدمات تقنية، فإذا كانت الحماية الموضوعية تقتضي تجريم الاعتداءات الواقعة على أنظمة الدفع، فإن الفعالية القانونية لا تكتمل إلا بوجود نظام دقيق للمساءلة يضمن جبر الضرر وتعويض الضحايا، موازاةً مع تبني استراتيجيات وقائية استباقية وتفعيل آليات إجرائية مرنة لفض المنازعات. وعليه، سنخصص هذا الفصل لبحث النظام القانوني لمساءلة الأطراف عن أضرار الدفع الإلكتروني، مع تسليط الضوء على القواعد الوقائية والآليات القضائية والبديلة المتاحة لحماية المستهلك، وذلك من خلال تقسيمه إلى مبحثين أساسيين:

المبحث الأول: النظام القانوني لمساءلة الأطراف عن أضرار الدفع الإلكتروني.

المبحث الثاني: القواعد الوقائية والتسوية القضائية لمنازعات الدفع.

المبحث الأول: النظام القانوني لمساءلة الأطراف عن أضرار الدفع الإلكتروني

تقتضي دراسة آليات حماية مستهلك خدمات الدفع الإلكتروني البحث أولاً في النظام القانوني الذي يحكم مسؤولية مختلف الأطراف المتدخلة في هذه العملية، وذلك من خلال تحديد الطبيعة القانونية لهذه المسؤولية والأساس الذي تقوم عليه، سواء من الناحية الجزائية الرادعة أو المدنية التعويضية، وهو ما سنعالجه عبر المطلبين الآتيين:

المطلب الأول: الأساس القانوني للمسؤولية الجزائية في جرائم الدفع الإلكتروني.

المطلب الثاني: ضوابط التعويض وتوزيع الأعباء بين الأطراف.

المطلب الأول: الأساس القانوني للمسؤولية الجزائية في جرائم الدفع الإلكتروني

تعد الحماية الجزائية حجر الزاوية في تأمين معاملات الدفع الإلكتروني، حيث تهدف إلى ردع السلوكيات الإجرامية التي تستهدف الوسائل التقنية أو أموال المستهلكين. ولتحديد معالم هذه الحماية، يقتضي الأمر أولاً ضبط المرتكزات الموضوعية والإجرائية للملاحقة، ثم تحديد نطاق المسؤولية الجنائية للأطراف الفاعلة، وهو ما سنفصله عبر الفرعين الآتيين:

الفرع الأول: المرتكزات الموضوعية والإجرائية للملاحقة الجزائية.

الفرع الثاني: تحديد المسؤولية الجنائية والمدنية.

الفرع الأول: المرتكزات الموضوعية والإجرائية للملاحقة الجزائية

تقتضي الملاحقة الجزائية لجرائم الدفع الإلكتروني الوقوف على طبيعة هذه الأفعال وتكييفها القانوني كخطوة أولى، ثم البحث في الضمانات الإجرائية والدور الذي تلعبه النيابة العامة وصولاً إلى تقييم فاعلية العقوبات، وهو ما سنعالجه في الفقرات الآتية:

أولاً: التكييف القانوني للجرائم المعلوماتية.

ثانياً: دور النيابة العامة في تحريك الدعوى وحماية أموال المستهلك.

ثالثاً: العقوبات الأصلية والتدابير الاحترازية (الردع الخاص).

رابعاً: ملائمة العقوبات لديناميكية الإجرام المعلوماتي.

أولاً: التكييف القانوني للجرائم المعلوماتية: يعد التكييف القانوني للفعل الإجرامي نقطة الارتكاز التي يبنى عليها النظام العقابي برمته؛ وحيث إن جرائم الدفع الإلكتروني تقع في بيئة رقمية افتراضية وغير ملموسة، فقد ثار جدل فقهي وقانوني واسع حول طبيعتها القانونية ومدى انطباق النصوص التقليدية عليها. ويعرف التكييف القانوني بأنه تلك العملية الذهنية التي يقوم بها القاضي أو الباحث للبحث عن النموذج القانوني الذي ينطبق على الفعل المرتكب من أجل إعطائه وصفه الصحيح تمهيداً لتقرير العقوبة المناسبة له.¹ وتكيف هذه الجرائم في المنظومة التشريعية الجزائية على

(1) محمود نجيب حسني، شرح قانون العقوبات - القسم العام، ط06، د.ن.ع، القاهرة، 1989، ص 342.

أنها "جرائم معلوماتية" بالدرجة الأولى، لكونها تمس بسلامة ونزاهة نظم المعالجة الآلية للمعطيات، وهي تتأرجح في وصفها الجنائي بين الجنحة والجنابة بحسب جسامة السلوك الإجرامي والنتيجة المترتبة عليه وتأثيرها على الثقة الائتمانية¹.

وبالرجوع إلى القواعد العامة، نجد أن المشرع الجزائري -ومواكبة منه للتطورات التقنية- قد أفرد فصلاً خاصاً للمساس بأنظمة المعالجة الآلية للمعطيات بموجب التعديلات المتتالية لقانون العقوبات. فعملية الدفع الإلكتروني تعتمد في جوهرها على تدفق بيانات مالية حساسة عبر شبكات المعلومات، وأي اعتداء يقع عليها بغير وجه حق يكيف كجريمة معلوماتية؛ إذ إن المشرع الجزائري لم يضع تعريفاً جامعاً مانعاً لجرائم الدفع الإلكتروني بصفة مستقلة، بل أثر إدراجها ضمن الجرائم المعلوماتية التي تستهدف أنظمة المعالجة الآلية للمعطيات بمختلف صورها وأشكالها التقنية².

وفيما يخص طبيعة هذه الجرائم من حيث الجسامة، فإن الأصل العام فيها أنها جنح بالنظر إلى سقف العقوبات المقرر لها في الحالات العادية؛ حيث نصت المادة 394 مكرر وما يليها من قانون العقوبات على عقوبات الحبس والغرامة لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة معالجة آلية للمعطيات.⁴ ولكن هذا التكييف قد يتغير وصفه ليصبح جنابة في حالات خاصة ومحددة، لاسيما إذا استهدفت هذه الجرائم المعطيات المتعلقة بالدفاع الوطني أو أمن الدولة أو الاقتصاد الوطني في كليته. كما يستوجب التكييف القانوني السليم ضرورة التمييز الدقيق بين "الجرائم المعلوماتية المحضة" التي تستهدف المنظومة التقنية في حد ذاتها ككيان محمي، وبين صور

(1) القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر، العدد 84، الصادرة بتاريخ 24 ديسمبر 2006.

(2) أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، ط. 10، دار هومة، الجزائر، 2010، ص 156.

(3) المادة 394، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم..

النصب والاحتيال التقليدي المرتكب عبر الوسائط الإلكترونية، حيث يظل الوصف الجنائي في الحالة الأخيرة مرتبطاً بجريمة الاحتيال لانتفاء القصد الجنائي الخاص بالاعتداء على البيانات.¹

وعليه، فإن تكيف جرائم الدفع الإلكتروني في الجزائر يتسم بالمرونة التشريعية، فهو يخضع لنوع الاعتداء ومحلّه؛ فإذا انصب الفعل الإجرامي على "البطاقة البنكية" عن طريق التزوير أو التقليد، صرنا أمام تكيف جنائي يتعلق بتزوير المحررات الرسمية أو العمومية نظراً لكون المؤسسات المصرفية المصدرة لها تعمل تحت إشراف الدول.² وهو ما يعكس صرامة المشرع في الإحاطة بكل جوانب الحماية القانونية للمستهلك الإلكتروني وحماية الاقتصاد الوطني من مخاطر السيولة الوهمية والائتمان الزائف.

ثانياً: دور النيابة العامة في تحريك الدعوى وحماية أموال المستهلك: تعتبر النيابة العامة المحرك الأساسي للدعوى العمومية في جرائم الدفع الإلكتروني، حيث تضطلع بدور محوري في حماية المصالح الاقتصادية للمستهلكين وضمان استقرار النظام المالي الرقمي؛ إذ إنها تتولى تمثيل المجتمع والمطالبة بتطبيق القانون، وهي في سبيل ذلك تختص بتحريك الدعوى العمومية ومباشرتها ضد كل من ساهم في ارتكاب جريمة³. ويبدأ هذا الدور بمجرد وصول العلم بالجريمة إليها، سواء عن طريق الشكاوى التي يقدمها المستهلكون المتضررون أو البلاغات الصادرة عن المؤسسات المصرفية والهيئات المتخصصة، وهو ما يفرض على جهاز النيابة ضرورة التعامل بمرونة مع البلاغات الرقمية لمواكبة تطور الإجرام المالي.

(1) أحسن بوسقيعة، المرجع سابق، ص 158.

(2) عبد الله أوهابيه، شرح قانون العقوبات الجزائري (القسم الخاص)، دار هومة، الجزائر، 2012، ص 210.

(3) عبد الله أوهابيه، شرح قانون الإجراءات الجزائية الجزائري (التحري والمتابعة)، دار هومة، الجزائر، 2010، ص 112.

وتتجلى خصوصية دور النيابة العامة في هذا المجال من خلال الصلاحيات الواسعة التي منحها إياها المشرع الجزائري، فبالنظر إلى الطبيعة التقنية لهذه الجرائم وسرعة اختفاء الأدلة الرقمية، خول المشرع لوكيل الجمهورية أو قاضي التحقيق صلاحية الإذن لضباط الشرطة القضائية باستخدام أساليب التحري الخاصة، مثل اعتراض المراسلات الإلكترونية وتفتيش الأنظمة المعلوماتية وحجز البيانات المتعلقة بالعمليات المالية المشبوهة.¹ كما يعد تدخل وكيل الجمهورية في جرائم الدفع الإلكتروني ضماناً أساسية للمستهلك، حيث يسمح باتخاذ إجراءات تحفظية سريعة كحجز المعطيات المعلوماتية لمنع ضياع الحقوق وتكريس الحماية الجنائية الفعالة للذمة المالية.²

وحيث إن الجريمة الإلكترونية تتسم بالسرعة الفائقة في تحويل الأموال، فإن تدخل النيابة العامة يجب أن يتسم بنفس القدر من السرعة لمنع الجناة من تهريب الأموال أو إخفائها، وهو ما يجسد مفهوم "الحماية الإجرائية الاستباقية" التي تهدف إلى شل حركة المجرم المعلوماتي قبل استنزاف رصيد الضحية.³ علاوة على ذلك، تباشر النيابة العامة مهامها وفق ما نصت عليه القواعد العامة للإجراءات الجزائية لضمان المتابعة القانونية السليمة⁴، مما يسهل على المستهلك المتضرر الحصول على التعويض الجابر للضرر أمام القضاء سواء بصفته طرفاً مدنياً أو من خلال دعوى مستقلة، خاصة وأن نجاح النيابة في إثبات الجريمة وإدانة الجاني يعد ركيزة أساسية يستند إليها القاضي المدني عند تقدير حجم الضرر والتعويض المستحق للمستهلك.⁵

(1) المادة 5، القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(2) أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، ط10، دار هومة، الجزائر، 2010، ص 155.

(3) سليمان مرقس، الوافي في شرح القانون المدني (الفعل الضار والمسؤولية المدنية)، المجلد 02، 1988، ص 210.

(4) المادة 36، الأمر رقم 66-155، المؤرخ في 08 جوان 1966، المتضمن ق.إ.ج، المعدل والمتمم.

(5) أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الطبعة السادسة، دار هومة، الجزائر، 2009، ص 180..

ثالثاً: العقوبات الأصلية والتدابير الاحترازية (الردع الخاص): تعتبر المنظومة العقابية الأداة الجوهرية التي يراهن عليها المشرع لتحقيق الردع الخاص، وذلك من خلال إيلاء الجاني بعقوبات تتناسب مع خطورة جرائم الدفع الإلكتروني المرتكبة؛ فالعقوبة هي الجزاء الذي يقرره القانون لمصلحة المجتمع، وتنزل بحكم قضائي على من ثبتت مسؤوليته عن الجريمة، وهي تهدف إلى زجر الجاني ومنعه من العودة لإجرامه مرة أخرى من خلال إضعاف نزعتة الإجرامية وإعادة تأهيله قانونياً.¹ وحيث إن هذه الجرائم تتسم بطابعها التقني العابر للحدود، فقد زواج المشرع الجزائري في قانون العقوبات والقوانين المكملة له بين العقوبات السالبة للحرية وبين العقوبات المالية القاسية، مفرداً لكل اعتداء جزاءً يتناسب مع حجم الضرر اللاحق بالمستهلك الرقمي.

تتمثل العقوبات الأصلية المقررة لهذا النوع من الإجرام في الحبس والغرامة، حيث شدد المشرع الجزائري العقوبة في المادة 394 مكرر من قانون العقوبات، لتصل في بعض حالات المساس بأنظمة المعالجة الآلية للمعطيات إلى عقوبات مشددة إذا استهدفت الأنظمة المالية أو الاستيلاء على أموال المستهلكين عن طريق الغش المعلوماتي.² وقد فرض المشرع عقوبات أصلية ثقيلة تهدف إلى تجريد الجاني من الأرباح غير المشروعة التي حققها عبر القرصنة، كما أقر جملة من التدابير التكميلية والوقائية التي تهدف أساساً إلى شل النشاط الإجرامي للمحترف الرقمي ومنعه من استغلال خبرته التقنية في الاعتداء على أنظمة الدفع المصرفية مجدداً، وهو ما يعزز الثقة في منظومة الاقتصاد الرقمي.³ إذ يهدف هذا التشديد العقابي إلى إحداث توازن بين سرعة وتيرة المعاملات المالية الافتراضية وبين صرامة الردع الجنائي، من خلال إقرار جزاءات لا تكفي بالقصاص من مرتكب الفعل فحسب، بل تمتد لتشمل تخفيف المصادر المالية للإجرام المعلوماتي وحماية الاقتصاد الوطني من تداعيات الثغرات التقنية

(1) محمود نجيب حسني، شرح قانون العقوبات - القسم العام، ط06، د.ن.ع، القاهرة، 1989، ص 815.

(2) المادة 394 مكرر، القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر، العدد 48، الصادرة بتاريخ 10 جوان 1966.

(3) أحسن بوسقيعة، الوجيز في القانون الجنائي العام، ط06، دار هومة، الجزائر، 2009، ص 245.

وتعد هذه العقوبات والتدابير قائمة أساسية في التصنيف القانوني للجزاءات التي أقرها المشرع في القواعد العامة لقانون العقوبات . حيث يشكل الجمع بين الغرامات المالية الثقيلة والتدابير التقنية (كالمنع من الإقامة أو الحرمان من ممارسة مهنة متصلة بالمعلوماتية) استراتيجية عقابية متكاملة لحماية المستهلك الإلكتروني من المجرمين المتخصصين في السطو الرقمي، بهدف تجريد المجرم من وسائله التقنية وضمان عدم تكرار الاعتداء على الذمة المالية للمتعاملين في الفضاء الافتراضي.¹

رابعاً: ملائمة العقوبات لديناميكية الإجرام المعلوماتي: إن السمة البارزة لإجرام الدفع الإلكتروني هي "الديناميكية" والتطور المستمر، حيث تظهر يومياً أساليب احتيالية وتقنية تتجاوز الأطر التشريعية التقليدية؛ فالسياسة الجنائية المعاصرة لم تعد تهدف فقط إلى العقاب التقليدي للجاني، بل أصبحت تسعى إلى خلق توازن دقيق بين كفالة حقوق الأفراد الرقمية وبين ملاحقة صور الإجرام المستحدثة التي أفرزتها الثورة التكنولوجية². لذا، ثار تساؤل جوهري حول مدى ملائمة العقوبات التي وضعها المشرع الجزائري للسيطرة على هذه الانتهاكات الرقمية، ومدى قدرة السياسة العقابية على توفير حماية حقيقية للمستهلك الإلكتروني في مواجهة مجرمين يتميزون بذكاء تقني فائق، مما يفرض ضرورة مراجعة النصوص الجزائية بصفة دورية لضمان عدم إفلات الجناة من العقاب نتيجة الفراغ التشريعي أو الجمود النصي³.

(1) أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، ط. 10، دار هومة، الجزائر، 2010، ص 215.

(2) ياسر محمد اللامي، انعكاسات السياسة التشريعية المعاصرة على الحماية الجنائية للمستهلك الإلكتروني (دراسة تحليلية مقارنة)، مجلة روح القوانين، كلية الحقوق جامعة طنطا، مصر، العدد 103، الجزء 1، يوليو 2023، ص 17.

(3) ياسر محمد اللامي، المرجع السابق، ص 29.

وتتطلب ملائمة العقوبة في جرائم الدفع الإلكتروني ضرورة وجود نصوص مرنة تستوعب التطورات التقنية المتسارعة، بحيث لا تفقد العقوبة قيمتها الردعية أمام ابتكارات القراصنة والمحتالين الذين يستغلون الثغرات البرمجية العابرة للحدود؛ إذ إن الردع لا يتحقق إلا إذا شعر الجاني بأن الجزاء المقرر يطال المكاسب المالية غير المشروعة التي حققها.¹

ومن مؤشرات الملاءمة في التشريع الجزائري، نجد أن المشرع قد راعى جسامته الضرر الواقع عند تقدير العقوبة وتفريدها،² حيث شدد العقوبات في حالات المساس بأنظمة المعالجة الآلية للمعطيات المالية بالنظر إلى خطورة الأضرار الناتجة عنها وتأثيرها المباشر على الثقة العامة في النظام المصرفي والائتماني للدولة.³

إن الحماية الجنائية للمستهلك لن تصل إلى درجة الكفاية إلا إذا واکبها تطوير جذري في آليات الإثبات الرقمي والتحري الإلكتروني؛ إذ تظل العقوبة معطلة من الناحية العملية ما لم يتم ضبط الدليل التقني وحمايته من التلاشي.⁴ وعليه، فإن المشرع الجزائري يسعى لصياغة منظومة عقابية متطورة تتجاوز الجانب الجزري الصرف لتشمل البعد الوقائي، كدعامة أساسية لضمان استمرارية الثقة في وسائل الدفع الرقمية وحماية المعاملات الإلكترونية من الاعتداءات المتجددة، مما لا بد من المراهنة على تكوين كفاءات قضائية وضبطية متمكنة من لغة البرمجة والأدوات التقنية، مع ضرورة تكثيف آليات التعاون القضائي والأمني الدولي؛ فالجرم المعلوماتي لا يعترف بالحدود الجغرافية، وغالباً ما يحتمي بفضاءات سيبرانية معقدة تتطلب "دبلوماسية جنائية" مرنة تسمح بتبادل البيانات والقبض على الجناة في الوقت المناسب قبل طمس معالم الجريمة.⁵

(1) ياسر محمد الممي، المرجع نفسه، ص 31.

(2) محمود نجيب حسني، شرح قانون العقوبات - القسم العام، ط06، د.ن.ع، القاهرة، 1989، ص 850.

(3) أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، ط10، دار هومة، الجزائر، 2010، ص 240.

(4) المادة 394 مكرر 2، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، ج.ر، العدد 48، الصادرة بتاريخ 10 جوان 1966.

الفرع الثاني: تحديد المسؤولية الجنائية والمدنية

بعد الوقوف على المرتكزات الإجرائية للملاحقة، يستوجب الأمر تحديد نطاق المسؤولية المترتبة على أطراف علاقة الدفع الإلكتروني، سواء كانت مسؤولية جزائية تطل الأشخاص المعنوية أو مسؤولية مدنية بنوعيتها العقدي والتقصيري، وهو ما سنفصله في الفقرات الآتية:

أولاً: المسؤولية الجزائية للشخص المعنوي (المؤسسات المالية).

ثانياً: الإخلال بالتزام الأمان والسرية كمرتکز للمسؤولية العقدية.

ثالثاً: أركان المسؤولية التقصيرية في غياب الرابطة التعاقدية المباشرة.

رابعاً: حالة القوة القاهرة أو الخطأ الأجنبي ودورهما في المسؤولية.

أولاً: المسؤولية الجزائية للشخص المعنوي (المؤسسات المالية): لم يعد نطاق الملاحقة الجزائية في جرائم الدفع الإلكتروني مقتصرًا على الأشخاص الطبيعيين فحسب، بل امتد ليشمل الأشخاص المعنوية، وفي مقدمتها المؤسسات المالية والمصرفية؛ إذ إن المسؤولية الجزائية للشخص المعنوي تعد من أهم المستجدات التي جاء بها التشريع الجنائي المعاصر، حيث أصبحت هذه الكيانات مسؤولة عن الأفعال التي ترتكب لحسابها من طرف ممثليها، وهو ما ينطبق تماماً على البنوك في مجال المعاملات الإلكترونية.¹ ويأتي هذا التوجه التشريعي استجابةً لخطورة الأدوار التي تلعبها هذه الكيانات في إدارة وتأمين العمليات المالية الرقمية.

(1) حليلة بن شعاعة، الحماية الجزائية للمستهلك في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2013، ص 59.

وقد كرس المشرع الجزائري مبدأ المسؤولية الجزائية للشخص المعنوي بصفة عامة في القواعد العامة لقانون العقوبات طبقاً للمادة 15 مكرر¹، ثم فصل شروط قيامها بأن ترتكب الجريمة لحساب الشخص المعنوي ومن طرف أعضائه أو ممثليه الشرعيين كما جاء في المادة 51 مكرر²، وتتجلى خصوصية هذه المسؤولية في أنها لا تقتصر على مجرد الغرامة المالية، بل تمتد لتشمل تدابير أخرى كالمنع من مزاولة النشاط أو مصادرة الوسائل، مما يحقق الردع الكافي لهذه المؤسسات²، وحيث إن جرائم الدفع الرقمي تتسم بالتعقيد، فقد أقر المشرع الجزائري عقوبات نوعية تتلاءم مع طبيعة الشخص المعنوي، تتراوح بين الغرامة المالية التي تصل إلى خمسة أضعاف الغرامة المقررة للشخص الطبيعي³، وبين عقوبات تكميلية تهدف بالدرجة الأولى إلى حماية المستهلك من التعسف أو الإهمال الذي قد يصدر عن هذه المؤسسات في حماية أنظمة الدفع الرقمي⁴.

وعليه، فإن المسؤولية الجزائية للشخص المعنوي في جرائم الدفع الإلكتروني تمثل ضمانة قانونية وقائية؛ فهي لا تهدف فقط للعقاب، بل لتحفيز المؤسسات المالية على تبني معايير أمنية عالمية، حمايةً للمستهلك ومنعاً لتحول هذه المؤسسات إلى قنوات خلفية لتمرير العمليات المالية غير المشروعة أو اختراق الخصوصية المالية للأفراد على الإخلال به قيام مسؤوليته العقدية التي توجب عليه توجب عليه تعويض العميل عن كافة الأضرار المادية والمعنوية التي لحقت به جراء هذا التقصير¹.

(1) المادة 15 مكرر ، الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، ج.ر، العدد 48، الصادرة بتاريخ 10 جوان 1966.

(2) المادة 51 مكرر ، الأمر رقم 66-156،

(3) ياسر محمد اللامي، انعكاسات السياسة التشريعية المعاصرة على الحماية الجنائية للمستهلك الإلكتروني (دراسة تحليلية مقارنة)، مجلة روح القوانين، كلية الحقوق جامعة طنطا، مصر، العدد 103، الجزء الأول، يوليو 2023، ص 25.

(4) المادة 394 مكرر، القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر، العدد 84، الصادرة بتاريخ 24 ديسمبر 2006.

(4) حليلة بن شعاعة، مرجع سابق، ص 61.

ثانياً: الإخلال بالتزام الأمان والسرية كمرتكز للمسؤولية العقدية: ويعد هذان الالتزامان الجوهر الفني والقانوني الذي يمنح المستهلك الثقة الضرورية في استخدام وسائل الدفع الرقمية، وبدونهما تنهار المنظومة الائتمانية برمتها. ويعرف التزام الأمان في عقود الدفع الإلكتروني بأنه التزام ببذل عناية مشددة تتجاوز معيار الشخص المعتاد لتصل إلى معيار "المهني المتخصص"، بل ويذهب الفقه الحديث إلى اعتباره التزاماً بتحقيق نتيجة في جوانبه التقنية، حيث يتعهد البنك بمقتضاه بتوفير تقنيات تشفير ومصادقة متطورة تمنع وصول الأغيار إلى الحسابات أو اختراق البيانات المالية.² أما التزام السرية، فهو يمتد ليشمل صون كافة المعطيات الشخصية والمالية للمستهلك من التداول غير المشروع أو الإفشاء؛ فالسرية المصرفية في البيئة الرقمية تفرض على المصرف حماية بيانات العميل من أي اختراق سيبراني، ويعد تسرب هذه البيانات للغير خطأً عقدياً جسيماً مستوجباً للمسؤولية، حتى لو وقع الفعل من أحد تابعي البنك أو نتيجة ثغرة في النظام المعلوماتي للمؤسسة.³

وتجدر الإشارة إلى أن إثبات الخطأ العقدي في هذا المجال يستند أساساً إلى القواعد العامة التي تقرر أن العقد شريعة المتعاقدين، ومن ثمَّ يجب تنفيذه بحسن نية وطبقاً لما اشتمل عليه من بنود صريحة أو ضمنية تفرضها طبيعة المعاملة الرقمية ومقتضيات الثقة الائتمانية، وذلك عملاً بنص المادة 106 من القانون المدني الجزائري⁴. كما أن المدين (البنك) ملزم بتنفيذ التزامه العقدي بكافة ملحقاته ومستلزماته التقنية، وإلا ترتبت مسؤوليته المباشرة عن الضرر الناتج عن عدم التنفيذ أو التأخير فيه وفقاً لما قرره المادة 178 من القانون ذاته.⁵ وحيث إن البنك يمثل الطرف الأقوى والمهيمن تقنياً واقتصادياً في هذه العلاقة التعاقدية غير المتكافئة، فإنه لا يمكنه بأي حال من الأحوال التحلل من

(1) علي جمال الدين عوض، العمليات المصرفية من الناحية القانونية، د.ن.ع، القاهرة، 1989، ص 140.

(2) المرجع نفسه، ص 142.

(3) عبد الرزاق السنهوري، الوسيط في شرح القانون المدني (نظرية الالتزام بوجه عام)، الجزء الأول، د.إ.ت.ع، بيروت، ص 710.

(4) المادة 106، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

(5) المادة 178، نفس القانون.

مسؤوليته العقدية تجاه المستهلك إلا بإثبات السبب الأجنبي الذي لا يد له فيه، كالقوة المستهلك إلا بإثبات السبب الأجنبي الذي لا يد له فيه، كالقوة القاهرة أو الحادث المفاجئ، أو إثبات وقوع خطأ جسيم وغير مغتفر صادر من المستهلك نفسه أسهم في وقوع الضرر؛ ذلك أن البنك بصفته المحترف الملتزم، يقع على عاتقه التزام بسلامة النظام المعلوماتي وضمان أمن القنوات الرقمية التي وضعها تحت تصرف العملاء¹، مما يجعل مسؤوليته تقترب من المسؤولية عن تحقيق نتيجة وليس مجرد بذل عناية.

ثالثاً: أركان المسؤولية التقصيرية في غياب الرابطة التعاقدية المباشرة: إذا كانت المسؤولية العقدية تحكم العلاقة المباشرة بين البنك وزبونه، فإن "المسؤولية التقصيرية" تبرز كآلية حماية جوهرية للمستهلك في مواجهة أطراف ثالثة قد لا تربطهم به علاقة عقدية مباشرة، مثل "مقدمي خدمات الشبكة" أو "الشركات المصنعة للبرمجيات"، وكذا في الحالات التي يتم فيها اختراق منظومة الدفع من طرف مجهولين. وتقوم هذه المسؤولية على القواعد العامة التي تفرض على الكافة التزاماً قانونياً بعدم الإضرار بالغير، وهي تتجسد في ثلاث أركان كلاسيكية: الخطأ، الضرر، وعلاقة السببية، لكنها تكتسي صبغة "رقمية" خاصة في مجال الدفع الإلكتروني تفرض إعادة النظر في معايير إثباتها التقليدية.²

يعتبر الخطأ في المسؤولية التقصيرية انحرافاً عن السلوك الواجب، ويتمثل في إهمال التدابير الوقائية التي يفرضها العرف التقني والقانون المنظم للاتصالات؛ فالمؤسسة التي تدير منصة دفع وسيطة (بوابة دفع) ترتكب خطأً تقصيرياً إذا لم تقم بتحديث جدران الحماية الخاصة بها، مما سهل عملية القرصنة وأدى لضياع بيانات المستهلكين. وحيث إن إثبات الخطأ في الفضاء الافتراضي يعد تحدياً

(1) علي جمال الدين عوض، العمليات المصرفية من الناحية القانونية، د.ن.ع، القاهرة، 1989، ص 145.

(2) المادة 124، الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، المعدل والمتمم.

تقنياً بالغ التعقيد، فإن القضاء يميل أحياناً إلى الأخذ بمعيار "الخطأ المفترض" أو التوسع في مفهوم "الخطأ المهني" للشركات المزودة للخدمة، خاصة في حالة الإخلال بالتزامات الجوهرية المنصوص عليها في التشريعات التقنية، وذلك لتمكين الطرف الضعيف (المستهلك) من نيل حقه أمام عمالقة التكنولوجيا.¹ أما الركن الثاني وهو الضرر، فيجب أن يكون محققاً ومباشراً وحالاً ليتم جبره؛ وفي جرائم الدفع الإلكتروني، يتخذ الضرر أبعاداً متعددة، فهو لا يقتصر على الجانب المادي الصرف (كالخسارة المالية المباشرة من الرصيد)، بل يمتد ليشمل الضرر المعنوي والنفسي الناتج عن انتهاك الخصوصية المالية للمستهلك وتعرض بياناته الحساسة للتداول². ويقع على عاتق المتضرر إثبات حجم الخسارة اللاحقة به وما فاتته من كسب جراء هذا الفعل غير المشروع، وهو ما يجسد رغبة المشرع في تحقيق التعويض الكامل والشامل للمستهلك طبقاً لأحكام القواعد العامة في القانون المدني الجزائري، التي تلزم المسؤول بجبر كافة الأضرار الناشئة عن فعله الضار³.

وتبقى "علاقة السببية" هي الركن الأكثر إثارة للجدل في البيئة الرقمية؛ إذ يجب إثبات أن الضرر المالي الذي أصاب المستهلك ناتج مباشرة عن خطأ الجهة المدعى عليها وليس نتيجة عامل أجنبي أو خطأ الضحية نفسه. وفي بيئة الدفع الرقمي المعقدة، قد تتعدد الأسباب وتتداخل نتيجة تعدد المتدخلين في السلسلة التقنية، مما يدفع الفقه والقضاء المعاصر لإقرار "المسؤولية التضامنية" بين الأطراف المتسببة في الخرق الأمني، لضمان حصول المستهلك على حقه في التعويض دون الغوص في تعقيدات تقنية تفرق بين مسؤولية مقدم الخدمة ومسؤولية البنك، وهو ما يكرس الحماية الإجرائية والموضوعية للمستهلك من مخاطر تكنولوجيا الدفع⁴.

(1) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، د.ف.ج، الإسكندرية، 2007، ص 215.

(2) عبد الرزاق السنهوري، الوسيط في شرح القانون المدني (مصادر الالتزام)، الجزء الأول، دار إحياء التراث العربي، بيروت، ص 810.

(2) جلال علي العدوة، المسؤولية المدنية عن الأخطاء المهنية في بيئة المعلوماتية، د.ن.ع، القاهرة، 2004، ص 188.

(3) المادة 182 مكرر، الأمر رقم 75-58، المتضمن القانون المدني الجزائري، المعدل والمتمم.

(4) عبد الرزاق السنهوري، المرجع السابق، ص 815.

رابعاً: حالة القوة القاهرة أو الخطأ الأجنبي ودورها في المسؤولية: على الرغم من التشديد في مساءلة المؤسسات المصرفية والتقنية عن أمن المعاملات الرقمية، إلا أن هذه المسؤولية ليست مطلقة؛ إذ إنه إذا أثبت الشخص أن الضرر قد نتج عن سبب أجنبي لا يد له فيه، كقوة القاهرة أو خطأ من الضحية أو فعل من الغير، كان غير ملزم بتعويض هذا الضرر، نظراً لانقطاع رابطة السببية.¹

وتتمثل القوة القاهرة في كل حادث فجائي غير متوقع ومستحيل الدفع، وفي البيئة الرقمية قد تأخذ شكل أعطال تقنية كبرى وشاملة خارجة عن السيطرة البرمجية للمؤسسة، أو كوارث تؤدي لشل الأنظمة المعلوماتية للدولة ككل، حيث يشترط فيها عدم إمكانية التوقع أو المقاومة حتى مع استخدام أكثر أنظمة الأمان تطوراً.² أما الخطأ الأجنبي فيتجسد بوضوح في "خطأ المستهلك" نفسه؛ إذ إن مسؤولية البنك عن سلامة عمليات الدفع الإلكتروني تنتفي إذا ثبت أن الضرر كان نتيجة مباشرة لإهمال العميل أو مخالفته لتعليمات الأمان، كإهماله في الحفاظ على الرقم السري للبطاقة أو تسليمه طواعية للغير، مما يجعل الضرر راجعاً لفعله هو لا لثغرة في نظام البنك.³

ويضاف إلى ما سبق، أن فعل الغير لا يعفي المؤسسة المصرفية من المسؤولية إلا إذا اتصف بخصائص القوة القاهرة، أي أن يكون حادثاً لا يمكن توقعه أو دفعه من طرف البنك، أما إذا كان خرق النظام ناتجاً عن تقادم في برمجيات الحماية أو ثغرات تقنية كان من الممكن تداركها، فإن رابطة السببية تظل قائمة وتحمل المؤسسة تبعات التعويض.

(1) المادة 127، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

(2) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، د.ف.ج، الإسكندرية، 2007، ص 230.

(3) علي جمال الدين عوض، العمليات المصرفية من الناحية القانونية، د.ن.ع، القاهرة، 1989، ص 160.

(4) فرحات رابح، مسؤولية البنك في عمليات الدفع الإلكتروني وتطبيقاتها في التشريع الجزائري، مجلة البحوث والدراسات القانونية والسياسية، جامعة سعد دحلب (البلدية 2)، المجلد 11، العدد 02، ديسمبر 2022، ص 435.

المطلب الثاني: ضوابط التعويض وتوزيع الأعباء بين الأطراف

بعد تحديد الأساس القانوني للمسؤولية، تبرز مسألة جبر الأضرار كأثر مترتب عنها، وهو ما يستوجب ضبط معايير التعويض وكيفية توزيع أعباء الخسارة المالية بين المتدخلين في عملية الدفع، ولإحاطة بهذا الموضوع سنقسم هذا المطلب إلى الفرعين الآتيين:

الفرع الأول: شروط وضوابط المطالبة بالتعويض.

الفرع الثاني: توزيع الأعباء والمسؤولية عن فعل الغير.

الفرع الأول: شروط وضوابط المطالبة بالتعويض

يتوقف حصول المستهلك على جبر للأضرار الناتجة عن حوادث الدفع الإلكتروني على مدى استيفاء دعوى التعويض لشروطها القانونية والموضوعية¹، وهو ما يتطلب بحث أركان الضرر الرقمي وكيفية تقديره في ضوء التشريع الوطني، وذلك وفقاً للأجزاء الآتية:

أولاً: إثبات الضرر المباشر المتولد عن الجريمة.

ثانياً: تقدير التعويض المالي المناسب (الخسارة الفعلية والكسب الفائت).

ثالثاً: التعويض عن الأضرار المعنوية الناتجة عن اختراق البيانات.

رابعاً: شروط التعويض في ضوء التشريع الوطني.

(1) المادة 178 ، الأمر رقم 58-75، المؤرخ في 26 سبتمبر، المتضمن القانون المدني الجزائري، المعدل والمتمم.

أولاً: إثبات الضرر المباشر المتولد عن الجريمة: يُعد الضرر الركن الجوهري في دعوى التعويض، إذ لا تنهض مسؤولية المؤسسة المالية أو أي طرف متدخل في عملية الدفع الإلكتروني إلا إذا ترتب عن الخطأ المرتكب ضرر فعلي أصاب المستهلك. فالضرر هو الركن الأساسي في المسؤولية، فإذا انعدم الضرر فلا محل للتعويض، ويشترط في الضرر الذي يوجب التعويض أن يكون محققاً ومباشراً وحالاً.¹ وفي سياق المعاملات الرقمية، يكتسي الضرر طابعاً خاصاً يتجاوز الصور التقليدية، مما يفرض تحديات قانونية في كيفية إثباته وتكييفه كضرر مباشر ومحقق يوجب الجبر القانوني وفق ما تقضي به القواعد العامة للمسؤولية.²

ويقصد بالضرر المباشر في هذا المجال تلك الخسارة المالية التي تلحق بذمة المستهلك وتكون نتيجة طبيعية ومباشرة للفعل الإجرامي أو الخلل التقني؛ حيث يعد الضرر نتيجة طبيعية إذا لم يكن في استطاعة الدائن تفاديه ببذل جهد معقول.³ وحسب القواعد العامة، فإن التعويض يشمل ما لحق الدائن من خسارة وما فاتته من كسب، بشرط أن يكون ذلك نتيجة طبيعية لعدم الوفاء بالالتزام أو للتأخر فيه.⁴ كما أن إثبات الضرر في بيئة الدفع الإلكتروني يقع في الأصل على عاتق المستهلك المدعي، غير أن خصوصية الإثبات الرقمي تجعل من هذا العبء ثقيلاً، خاصة عند التمييز بين الضرر المادي والضرر المعنوي الناتج عن انتهاك الخصوصية المالية للمستهلك.⁵

(1) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة 01، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 162.

(2) المادة 124، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، ح.ر رقم 78، الصادرة بتاريخ 30 سبتمبر 1975.

(3) محمد بودالي، المرجع السابق، ص 164.

(4) المادة 182، الأمر رقم 75-58، المعدل و المتمم.

(5) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، ط 01، د.ف.ج، الإسكندرية، 2007، ص 245.

لذا، فإن إثبات الضرر في منازعات الدفع الإلكتروني يتطلب تقارير فنية تثبت وجه الربط بين الخلل التقني ونقص القيمة المالية للحساب المصرفية،¹ لضمان عدم ضياع حقوق الضحايا أمام تعنت المؤسسات المصرفية في الاعتراف بالقصور الأمني لأنظمتها، الأمر الذي يجعلنا نؤكد على ضرورة تفعيل دور الخبرة التقنية كآلية مساعدة للقضاء في تقدير الضرر، وعدم الاكتفاء بالظاهر القانوني فقط، خاصة وأن المستهلك يواجه "قوة برمجية" لا يملك أدوات كشفها أو التصدي لها بمفرده.²

ثانياً: تقدير التعويض المالي المناسب (الخسارة الفعلية والكسب الفائت): بمجرد إثبات ركن الضرر، تبرز مسألة التقدير القضائي كخطوة حاسمة وجوهرية في مسار جبر الضرر الذي لحق بالمستهلك، حيث يهدف التعويض في منازعات الدفع الإلكتروني بصفة أساسية إلى إعادة ذمة الضحية المالية إلى ما كانت عليه قبل وقوع الاعتداء؛ إذ يتحدد مقدار التعويض بمقدار الضرر الذي لحق بالدائن فعلياً، ويشمل التعويض قانوناً ما لحق الدائن من خسارة وما فاتته من كسب محقق، بشرط أن يكون ذلك نتيجة طبيعية ومباشرة لعدم الوفاء بالالتزام أو التقصير فيه.³ ويستند القضاء في تقديره هذا على السلطة التقديرية الواسعة لقاضي الموضوع في تحديد قيمة التعويض الجابر للضرر المادي والمعنوي، بناءً على ما توفر لديه من قرائن وأدلة تقنية تثبت حجم التآكل الذي أصاب الذمة المالية للمستهلك.⁴

(1) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط01، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 167.

(2) المرجع نفسه.

(3) المادة 182، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

(4) محمد بودالي، المرجع السابق، ص 168.

تتمثل الخسارة الفعلية في المبالغ المالية التي سُحبت فعلاً من حساب المستهلك أو القيمة المالية التي فقدتها جراء العملية الاحتيالية؛ حيث يجب أن يشمل التعويض هنا مبدأ "الجبر الكامل للضرر"، بحيث لا يقل التعويض عما أصاب الدائن من خسارة مالية واضحة، مع ضرورة مراعاة الظروف والملابسات المحيطة بالخطأ، لا سيما في ظل تزايد مخاطر القرصنة التقنية.³ وفي نطاق المسؤولية العقدية للمصارف، يقتصر التعويض عادةً على الضرر الذي كان يمكن توقعه وقت التعاقد، أن عدم تنفيذ الالتزام من طرف البنك كان ناشئاً عن غشه أو خطئه الجسيم في تأمين المعطيات، وهو ما يعد ضماناً قوية للمستهلك في مواجهة القصور التقني للمؤسسات المالية.¹

أما الكسب الفائت، فهو يمثل تلك الفوائد والمزايا المالية التي كان المستهلك سيحصل عليها يقيناً لولا وقوع الفعل الإجرامي؛ وفي المعاملات المالية الإلكترونية لا يُقدر الكسب الفائت على أساس الاحتمال أو التخمين، بل يجب أن يثبت الدائن ضياع فرصة حقيقية وجدية كانت ستدر عليه نفعاً مادياً مؤكداً لو لم يتم تجميد رصيده أو السطو عليه.² ومن أجل الوصول إلى تقدير عادل ومنصف، يلجأ القضاء غالباً إلى ندب أهل الخبرة من الخبراء المصرفيين والمهندسين التقنيين، لمساعدة القاضي على فهم وفك رموز الخسائر المالية المعقدة الناتجة عن عمليات التلاعب بالبيانات الرقمية،³ وذلك لضمان حماية فاعلة للمستهلك تضمن له استرداد أصل ماله المنهوب، وجبر كافة الآثار التبعية التي ترتبت على خرق أمنه المالي وصدقية تعاملاته الرقمية.⁴

(1) المادة 182، الفقرة 2، الأمر رقم 75-58، المعدل و المتمم.

(2) عبد الرزاق السنهوري، الوسيط في شرح القانون المدني (نظرية الالتزام)، الجزء الأول، د.إ.ت.ع، بيروت، ص 715.

(3) جلال علي العدوة، المسؤولية المدنية عن الأخطاء المهنية في بيئة المعلوماتية، د.ن.ع، القاهرة، 2004، ص 205.

(4) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط01، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 171.

ثالثاً: التعويض عن الأضرار المعنوية الناتجة عن اختراق البيانات: لا تتوقف آثار جرائم الدفع الإلكتروني عند الحدود المادية المحسوسة، بل تمتد لتصيب الجانب المعنوي والنفسي للمستهلك؛ إذ يشمل التعويض الضرر المعنوي أيضاً، وهو كل ما يصيب الشخص في كرامته أو شعوره أو شرفه، ويقدره القاضي تبعاً لظروف كل حالة وبما يحقق الترضية العادلة للمتضرر.¹ ويعد التعويض عن الضرر المعنوي في البيئة الرقمية من أدق المسائل القانونية نظراً لطبيعته غير الملموسة، غير أن المشرع الجزائري أقر صراحة مبدأ التعويض عنه بصفة مستقلة في المادة 182 مكرر من قانون المدني.²

يتجسد الضرر المعنوي في هذا السياق في الآلام النفسية والقلق والاضطراب الذي يصيب المستهلك بمجرد علمه بوقوع اختراق لبياناته السرية؛ فإن المساس بالخصوصية المعلوماتية للمستهلك يعد ضرراً معنوياً موجباً للتعويض، لما يسببه من قلق نفسي واضطراب في السكينة الخاص للضحية.³ كما يمتد هذا الأثر ليشمل السمعة المالية والائتمانية للمستهلك في الفضاء الرقمي، وهو ما يستوجب تدخلاً قضائياً لتقدير تعويض مادي يكون بمثابة ترزية للمتضرر تماشياً مع معايير حماية المستهلك الإلكتروني.⁴

وتجدر الإشارة إلى أن حق المطالبة بالتعويض يجد أساسه أيضاً في القواعد التي تمنع التعسف في استعمال الحق والمساس بحقوق الغير الشخصية.³ حيث يهدف القضاء من خلال سلطته التقديرية إلى جبر الأضرار المعنوية الناتجة عن تسريب البيانات. ولا يهدف التعويض عن الضرر المعنوي إلى إثراء الضحية، بل إلى جبر الانكسار النفسي الذي خلفه الفعل الضار.

(1) المادة 182 مكرر، الأمر رقم 75-58، المعدل و المتمم

محمد بودالي، المرجع السابق، ص 172.

(2) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، الطبعة 01، د.ف.ج، الإسكندرية، 2007، ص 250.

(3) المادة 124 مكرر، الأمر رقم 75-58، المعدل و المتمم.

(4) محمد بودالي، مرجع سابق، ص 173.

رابعاً: مشروط التعويض في ضوء التشريع الوطني: لا يكفي وقوع الضرر المباشر أو المعنوي للمستهلك حتى يستحق التعويض، بل استلزم المشرع الجزائري توفر شروط إجرائية وموضوعية محددة لضمان استحقاق هذا الجبر المالي؛ إذ لا يستحق التعويض إلا بعد إعدار المدين، ما لم ينص القانون على غير ذلك، ويكون الإعدار بإنذار الدائن للمدين بوفاء الالتزام.¹ وفي بيئة الدفع الإلكتروني، يتخذ الإعدار طابعاً زمنياً حرجاً، حيث يلعب الإخطار الفوري دوراً جوهرياً في حماية حق المستهلك وتحديد مسؤولية المؤسسة عن العمليات غير المصرح بها.² ويتعلق الشرط الثاني بإثبات الخطأ والضرر، حيث إن إثبات الضرر في منازعات الاستهلاك الرقمي يتطلب تضافر القرائن القانونية والوسائل التقنية، ويقع على البنك عبء إثبات أن النظم الأمنية كانت تعمل بكفاءة لحظة وقوع الاختراق.³ وتماشياً مع هذا التوجه، يبرز الشرط الثالث المرتبط بعدم وجود اتفاق مسبق على الإعفاء من المسؤولية، حيث يعتبر المشرع الجزائري بنود الإعفاء من المسؤولية في عقود الاستهلاك الإلكتروني باطلة بطلاناً مطلقاً لتعارضها مع النظام العام.⁴

وتجدر الإشارة إلى أنه في حالة عدم النص على مقدار التعويض في العقد أو في القانون، فإن القاضي هو من يتولى تقديره بما يجبر الضرر الواقع فعلاً؛⁵ وتعتبر حماية المستهلك من البنود التعسفية التي تدرجها المؤسسات المالية لإعفاء نفسها من مسؤولية تأمين وسائل الدفع حجر الزاوية في التشريع الوطني الحديث.⁶ وعليه، فإن شروط التعويض تعكس رغبة المشرع في إيجاد حماية فعلية تضمن جبر الضرر كاملاً للمستهلك كطرف ضعيف في العلاقة التعاقدية الرقمية.

(1) المرجع السابق، ص 175.

(2) المادة 15، القانون رقم 09-03، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، ج.ر، رقم 15، الصادرة بتاريخ 08 مارس 2009.

(3) المادة 182، الأمر رقم 75-58، المعدل و المتمم.

(4) محمد بودالي، مرجع سابق، ص 176.

الفرع الثاني: توزيع الأعباء والمسؤولية عن فعل الغير

لا تقتصر المساءلة القانونية في منظومة الدفع الإلكتروني على مرتكب الفعل الضار فحسب، بل تمتد لتشمل أطرافاً أخرى قد تتحمل عبء التعويض بناءً على علاقات التبعية أو التقصير في الرقابة، كما قد يساهم سلوك المستهلك نفسه في تحديد نطاق هذا التعويض، و سنفصل فيه كتالي:

أولاً: مسألة تحمل المستهلك لجزء من الخسارة (الخطأ المشترك).

ثانياً: مسؤولية البنك عن خطأ موظفيه أو وكلائه.

ثالثاً: مسؤولية التاجر عن أمن منصته الرقمية.

رابعاً: تحديد المسؤولية عن فعل الغير (التابعين والمقاولين الفرعيين).

أولاً: مسألة تحمل المستهلك لجزء من الخسارة (الخطأ المشترك): تعد الحماية القانونية للمستهلك في مجال الدفع الإلكتروني حماية نسبية وليست مطلقة، إذ تنقيد بسلوك المستهلك ومدى التزامه بواجبات الحيطة والحذر؛ حيث يجوز للقاضي أن ينقص مقدار التعويض أو لا يحكم بشيء إذا كان المتضرر قد اشترك بخطئه في إحداث الضرر أو زاد فيه.¹ وتبرز أهمية هذه المسألة في الفضاء الرقمي حيث يشترك المستهلك تقنياً مع المصرف في إدارة وسيلة الدفع، مما يفرض فكرة توزيع المسؤولية بين البنك والعميل في حالة الخطأ المشترك وتأثير ذلك على قيمة جبر الضرر المالي.²

(1) المادة 177، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، ج.ر، رقم 78، الصادرة بتاريخ 30 سبتمبر 1975.

(2) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة 01، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 177.

ويتحقق الخطأ المشترك عندما يجتمع خطأ المؤسسة المالية مع إهمال المستهلك؛ إذ إن المستهلك يلتزم ببذل عناية الرجل المعتاد في الحفاظ على رموز الولوج إلى حساباته الإلكترونية، وأي إخلال بهذا الالتزام يعتبر خطأً يساهم في وقوع الضرر ويؤدي حتماً إلى إنقاص التعويض.¹ وفي هذا السياق، نجد أنه في العقود الدولية للدفع الإلكتروني، يُحمل المستهلك مسؤولية العمليات التي تتم قبل التبليغ عن ضياع البطاقة في حدود سقف مالي معين.²

ويلعب معيار الخطأ الجسيم للمستهلك دوراً حاسماً في إعفاء المؤسسة المصرفية من مسؤوليتها العقدية إذا ثبت أن الانحراف عن السلوك الواجب كان فادحاً.³ ومع ذلك، تظل الحماية قائمة في الحالات التقنية المعقدة؛ إذ لا يعتبر المستهلك مخطئاً إذا كان الاختراق ناتجاً عن ثغرات برمجية معقدة لا يدركها الشخص العادي، ولو ساهم بطريقة غير مباشرة في تسهيل الدخول للمنظومة.⁴

ثانياً: مسؤولية البنك عن خطأ موظفيه أو وكلائه: تعتبر مسؤولية البنك عن أخطاء موظفيه تطبيقاً جوهرياً لقاعدة مسؤولية المتبوع عن أعمال تابعه؛ إذ يكون المتبوع مسؤولاً عن الضرر الذي يحدثه تابعه بفعله الضار، متى كان واقعاً منه في حال تأدية وظيفته أو بسببها.⁵ وهي مسؤولية تشدد أهميتها في مجال الدفع الإلكتروني نظراً لخطورة الصلاحيات التقنية الممنوحة للموظفين، حيث تتحدد علاقة التبعية بين البنك وموظفيه من خلال سلطة الرقابة والإشراف التي تمارس على إدارة الأنظمة المعلوماتية للدفع.⁶

(1) المرجع السابق، ص 178.

(2) نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، الطبعة 01، منشورات الحلبي الحقوقية، بيروت، لبنان، 2004، ص 312.

(3) المرجع السابق، ص 314.

(4) محمد بودالي، مرجع سابق، ص 180.

(5) المادة 129، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، ج.ر، رقم 78، الصادرة بتاريخ 30 سبتمبر 1975.

(6) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة 01، د ف ن.ت، القاهرة، 2006، ص 182.

وتنهض هذه المسؤولية كلما ارتكب الموظف خطأً أثناء تأدية وظيفة الدفع الإلكتروني، حيث إن مسؤولية المؤسسات المصرفية عن فعل موظفيها هي مسؤولية موضوعية، تهدف إلى توفير حماية فعالة للعميل ضد الأخطاء الداخلية التي قد تؤدي إلى اختراق سرية حساباته.¹ ويجد هذا المبدأ سنده القانوني في القواعد المتعلقة بمسؤولية الشخص المعنوي عن الأفعال الضارة الصادرة عن ممثليه،² مما يفرض على البنك التزاماً مشدداً بالرقابة والإشراف على التقنيين والمبرمجين الذين يديرون منصات الدفع.³

ولا يشترط لقيام مسؤولية البنك أن يصدر أمر مباشر من المدير للموظف بالقيام بالفعل الضار، بل يكفي أن يكون العمل قد تم تحت غطاء الوظيفة المصرفية؛⁴ مما يوفر للمستهلك حماية موضوعية تجنبه عناء ملاحقة الموظفين بصفته الشخصية، ويجعل من البنك الضامن الفعلي لسلامة تصرفات أطقمه البشرية والتقنية في مواجهة المستهلك.

ثالثاً: مسؤولية التاجر عن أمن منصته الرقمية: في منظومة التجارة الإلكترونية، لا يقتصر أطراف عملية الدفع على البنك والمستهلك فحسب، بل يبرز التاجر كحلقة وصل أساسية ومصدر محتمل للمخاطر؛ إذ يلتزم المورد الإلكتروني بضمان أمن المعاملات التي تتم عبر منصته الإلكترونية، ويتحمل المسؤولية عن كل ضرر يلحق بالمستهلك ناتج عن نقص في تدابير الحماية التقنية للموقع.⁵

(1) نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، ط01، منشورات الحلبي الحقوقية، بيروت، لبنان، 2004، ص 316.

(2) المادة 124 مكرر 1، الأمر رقم 75-58، المعدل و المتمم.

(3) نزيه نعيم شلالا، مرجع سابق، ص 318.

(4) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط01، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 185.

(5) المادة 18، القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، رقم 28، الصادرة بتاريخ 16 ماي 2018.

وتنهض هذه المسؤولية كلما ثبت وجود تقصير في معايير الأمان، خاصة فيما يتعلق بالالتزام بحماية البيانات ذات الطابع الشخصي للمستهلكين ومنع وصول الغير إليها.¹ وتتجسد مسؤولية التاجر في كونها مسؤولية مهنية؛ إذ إن مسؤولية المورد الإلكتروني في تأمين الدفع لا تتوقف عند حدود إتمام البيع، بل تمتد لتشمل حماية مسار البيانات المالية للعميل، ويعد تسرب هذه البيانات خطأً مهنيًا ثابتاً في حقه،² وفي هذا الإطار، يميل الفقه والقضاء نحو تكييف مسؤولية التاجر كمسؤولية موضوعية في مواجهة المستهلك الإلكتروني لضمان جبر الأضرار بفعالية،³ وهو ما يتماشى مع الالتزام العام بضمان أمن المنتجات الذي يفرضه قانون حماية المستهلك وقمع الغش.⁴

ولا يعفى التاجر من المسؤولية بالادعاء بأن الاختراق وقع من طرف قرصان ما دام أن النظام الأمني للموقع كان هشاً ولا يرقى للمعايير التقنية المعمول بها؛⁵ إذ يقع على عاتقه إثبات أن الخرق ناتج عن سبب أجنبي خارج عن سيطرته التقنية تماماً ولا يد له في حدوثه. وعليه، فإن مساءلة التاجر عن أمن منصته الرقمية تمثل حماية مزدوجة؛ فهي تحمي المستهلك من استهداف المواقع غير المؤمنة، وتدفع التجار نحو الاستثمار في تقنيات التشفير والمصادقة القوية، مما يحول دون تحول المنصات الرقمية إلى ثغرات قانونية وتقنية يُهدر فيها أمان البيانات المالية للمواطنين، الأمر الذي يعزز في النهاية الثقة في سوق التجارة الإلكترونية الوطنية.

(1) القانون رقم 07-18، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر، رقم 34، الصادرة بتاريخ 10 جوان 2018.

(2) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط 01، د.ف.ن.ت، القاهرة، 2006، ص 188.

(3) نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، ط 01، منشورات الحلبي الحقوقية، لبنان، 2004، ص 320.

(4) المادة 15، القانون رقم 09-03، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، ج.ر، رقم 15، الصادرة بتاريخ 08 مارس 2009.

(5) محمد بودالي، مرجع سابق، ص 190.

رابعاً: تحديد المسؤولية عن فعل الغير (التابعين والمقاولين الفرعيين): تتعدّد مسألة المسؤولية في أنظمة الدفع الإلكتروني نظراً لتعدد المتدخلين التقنيين؛ إذ غالباً ما يتم الاستعانة بجهات خارجية لإدارة الخوادم أو صيانة البرمجيات. وتستند مسؤولية المؤسسة المصرفية عن أفعال هؤلاء الأغيار إلى فكرة التبعية؛ إذ يكون المتبوع مسؤولاً عن الضرر الذي يحدثه تابعه بفعله الضار، متى كان واقعاً منه في حال تأدية وظيفته أو بسببها، وتقوم علاقة التبعية ولو لم يكن المتبوع حراً في اختيار تابعه متى كانت له عليه سلطة فعلية في الرقابة والتوجيه.¹ ويمتد هذا المفهوم ليشمل شركات الصيانة البرمجية والمقاولين الفرعيين الذين يعملون تحت إشراف البنك لإدارة خدمات الدفع.²

وفي حالة وقوع اختراق ناتج عن ثغرة صممها مقاول فرعي، فإن تعاقد البنك مع طرف ثالث لإدارة العمليات التقنية لا يعفيه من المسؤولية تجاه العميل، إذ يظل البنك ضامناً لكل خلل يصيب نظام الدفع ولو كان مصدره المقاول الفرعي.³ ويجد هذا التوجه سنده في الالتزامات المفروضة على المسؤول عن معالجة البيانات تجاه المناول (المقاول من الباطن) لضمان حماية المعطيات ذات الطابع الشخصي للمستهلكين،⁴ وهو ما يتماشى مع المبدأ العام لمسؤولية الشخص المعنوي عن أفعال تابعيه الضارة. فالمستهلك يرتبط عقدياً بالبنك ولا تجمععه أي علاقة قانونية مباشرة بالمقاول الفرعي، مما يجعل البنك في مواجهة العميل هو المسؤول الأول والأخير عن "سلامة النتيجة التقنية".⁵

(1) المادة 129، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، ج.ر، رقم 78، الصادرة بتاريخ 30 سبتمبر 1975.

(2) نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، ط 01، منشورات الحلبي الحقوقية، لبنان، 2004، ص 322.

(3) المرجع السابق، ص 324.

(4) المادة 34، القانون رقم 18-07، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر، رقم 34، الصادرة بتاريخ 10 جوان 2018.

(5) المادة 124 مكرر 1، الأمر رقم 75-58، المتضمن القانون المدني .

ويجب على المؤسسة المصرفية أن تضمن سلامة الوسائل التي تضعها تحت تصرف الجمهور، وهي مسؤولة عن كل تقصير يصدر عن تجهيز هذه الوسائل من الأغيار؛¹ إذ يهدف هذا النظام إلى تركيز الحماية حول المستهلك بمنحه حق مواجهة الواجهة التعاقدية التي يثق بها، مما يجعل البنوك والتجار حراساً حقيقيين ليس فقط على أنظمتهم، بل على تصرفات كل من يستعينون بهم في إدارة هذه التكنولوجيا المعقدة.

المبحث الثاني: القواعد الوقائية والتسوية القضائية لمنازعات الدفع

بعد الإحاطة بنظام المسؤولية القانونية وضوابط التعويض عن أضرار الدفع الإلكتروني، يستوجب البحث الانتقال إلى الجانب العملي المتمثل في سبل الوقاية من هذه المخاطر وآليات فض النزاعات الناشئة عنها؛ إذ لا تكتمل الحماية القانونية للمستهلك إلا بوجود نصوص وقائية استباقية، وإجراءات قضائية وودية فعالة تضمن سرعة استرجاع الحقوق، ولتسليط الضوء على هذه الجوانب سنقسم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: الدور الوقائي للتشريعات والرقابة في مكافحة الجرائم.

المطلب الثاني: آليات التسوية القضائية والبديلة للمنازعات.

(1) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 192.

المطلب الأول: الدور الوقائي للتشريعات والرقابة في مكافحة الجرائم

إن مواجهة مخاطر الدفع الإلكتروني لا تتوقف عند حدود توقيع العقاب أو جبر الأضرار بعد وقوعها، بل تقتضي وجود ترسانة قانونية ورقابية تعمل على تحصين المعاملات الرقمية استباقياً. ويتجلى هذا الدور في تضافر القواعد القانونية المنظمة للسلامة المعلوماتية مع الآليات الفنية والرقابية التي تفرضها الهيئات المصرفية لضمان بيئة دفع آمنة، ولتسليط الضوء على هذه الآليات الوقائية سنعتمد التقسيم الآتي:

الفرع الأول: القواعد القانونية المنظمة لضمان سلامة المعاملات.

الفرع الثاني: دور المصارف ومقدمي الخدمات في تحقيق الحماية.

الفرع الأول: القواعد القانونية المنظمة لضمان سلامة المعاملات

تتعدد النصوص التشريعية التي تشكل السياق الواقعي للمستهلك الإلكتروني، حيث تتداخل القواعد الجزرية لقانون مكافحة الجرائم المعلوماتية مع المبادئ الحمائية لقانون حماية المستهلك، وصولاً إلى التنظيمات التقنية الدقيقة التي تفرضها السلطات النقدية والرقابية، ولإحاطة بهذه القواعد سنقسم هذا الفرع إلى الأجزاء الآتية:

أولاً: دور قانون مكافحة الجريمة الإلكترونية (الردع العام).

ثانياً: دور قانون حماية المستهلك في البيئة الرقمية.

ثالثاً: دور التشريع المصرفي والتعليمات الرقابية.

رابعاً: دور المعايير الدولية والجهود المقارنة (GDPR, PCI DSS).

أولاً: دور قانون مكافحة الجريمة الإلكترونية (الردع العام): يُعد قانون مكافحة الجريمة الإلكترونية الركيزة الأساسية في الاستراتيجية الوطنية للوقاية من مخاطر الدفع الرقمي؛ إذ تهدف الفلسفة التشريعية للجزائر إلى خلق بيئة رقمية آمنة تعزز ثقة المستهلك عبر فرض رقابة تقنية صارمة¹. وفي هذا الإطار، تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تكلف أساساً بوضع آليات تقنية للوقاية من الجرائم الإلكترونية وتنسيق الجهود بين مختلف الفاعلين لضمان أمن الشبكات².

وتتحقق الوظيفة الوقائية لهذا القانون من خلال فرض التزامات تقنية على مقدمي الخدمات، لضمان السرية التامة للمعطيات المخزنة والتبليغ الفوري عن أي محاولة اختراق تستهدف المستهلكين³. ويتم تفعيل هذه الرقابة الإلكترونية الاستباقية تحت إشراف النيابة العامة لضمان مشروعية الإجراءات واحترام الحريات الفردية⁴ وهو ما يمنع استغلال الثغرات البرمجية في تنفيذ عمليات قرصنة واسعة النطاق حيث تهدف هذه المقاربة التشريعية إلى خلق "بيئة رقمية آمنة" تُعزز من ثقة المستهلك في أنظمة الدفع الإلكتروني.

كما يتجسد الردع العام من خلال المنظومة العقابية المشددة التي أقرها المشرع الجزائري لمواجهة المساس بأنظمة المعالجة الآلية للمعطيات⁵ حيث يهدف الردع العام في القوانين السيبرانية إلى إعلام الجمهور بجسامة العقوبات المترتبة على جرائم الدفع الإلكتروني، مما يقلص من معدلات

(1) المادة 12، القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، رقم 47، الصادرة بتاريخ 16 أوت 2009.

(2) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، الطبعة 02، د.م.ج، الإسكندرية، 2010، ص 85.

(4) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، الطبعة 01، د.م.ج، الإسكندرية، 2003، ص 87.

(5) المادة 394 مكرر، الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، المعدل والمتمم.

الإجرام الرقمي الناجم عن استغلال الثغرات البسيطة.¹ وبذلك، يمثل قانون مكافحة الجريمة الإلكترونية صمام الأمان الذي يعمل على تخفيف منابع الخطر السيبراني قبل وقوع الضرر الفعلي بالمستهلك.

ثانياً: دور قانون حماية المستهلك في البيئة الرقمية: يمثل قانون حماية المستهلك وقمع الغش حجر الزاوية في المنظومة الوقائية ضد مخاطر الدفع الإلكتروني؛ إذ لم تعد الحماية تقتصر على السلع المادية، بل امتدت لتشمل الخدمات الرقمية وما يرافقها من عمليات دفع.² وتتجلى هذه الحماية في وجوب أن يزود كل متدخل المستهلك بكل المعلومات المتعلقة بالمنتج أو الخدمة التي وضعها للاستهلاك، لاسيما الشروط المتعلقة بأمن المعاملة المالية وضمانات حمايتها.³

كما يمتد الدور الوقائي للقانون إلى مكافحة البنود التعسفية التي تدرجها المؤسسات المالية لإعفاء نفسها من المسؤولية؛ إذ يعتبر تعسفاً كل بند يهدف إلى إعفاء المورد من التزاماته الأساسية في توفير الأمن للمستهلك أثناء تنفيذ عقد الاستهلاك الإلكتروني، ويعد هذا البند لاغياً ولا أثر له.⁴ ويؤكد الفقه في هذا الإطار أن بطلان هذه البنود يمثل ضماناً أساسية لاستقرار المركز القانوني للمستهلك في مواجهة الموردين المحترفين.⁵

(1) ممدوح إبراهيم، المرجع السابق، ص 89.

(2) المادة 17 ، القانون رقم 09-03، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، ج.ر، رقم 15، الصادرة بتاريخ 08 مارس 2009.

(3) المادة 15 ، القانون نفسه.

(5) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة 01، دار الفجر للنشر والتوزيع، القاهرة، 2006، ص 210.

علاوة على ذلك، يفرض التشريع الوطني على المورد الإلكتروني التزاماً بضمان سلامة المستهلك من الأضرار التي قد تلحق بذمته المالية جراء عيوب أنظمة الدفع المعتمدة،¹ وهو ما يخلق توازناً ضرورياً في العلاقة التعاقدية؛ ذلك أن الحماية الوقائية للمستهلك الرقمي تقتضي وجود توازن بين حرية التعاقد والالتزام بضمان الأمن المعلوماتي، وهو ما كرسه المشرع الجزائري من خلال قواعد النظام العام الاستهلاكي.² وبذلك، يكتمل الدور الوقائي بتأطير المورد وحماية الضحية من التغول التقني.

ثالثاً: دور التشريع المصرفي والتعليمات الرقابية: يعتبر التشريع المصرفي الأداة التنفيذية الأكثر دقة في مجال الوقاية من مخاطر الدفع الإلكتروني؛ إذ يتولى بنك الجزائر، عبر مجلس النقد والمصرفية، وضع القواعد التقنية والإدارية لضمان سلامة العمليات المصرفية الرقمية،³ حيث يمتلك مجلس النقد والمصرفية صلاحيات واسعة في تحديد المعايير التقنية والأمنية لوسائل الدفع الإلكتروني لضمان سلامة المستهلكين.⁴ وتعمل هذه الرقابة القبليّة كفلتّر أمني يمنع دخول أدوات دفع هشة إلى السوق المالية، مما يقلص من فرص وقوع المستهلك ضحية لثغرات تقنية. بالإضافة إلى ذلك، يضطلع بنك الجزائر بدور محوري في مراقبة الأنظمة المعلوماتية للبنوك، حيث يفرض عليها الالتزام بالمعايير

(1) المادة 18، القانون رقم 05-18، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 ماي 2018.

(2) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، ط 01، د.ف.ج، الإسكندرية، 2007، ص 315.

(3) المادة 92، القانون رقم 09-23، المؤرخ في 21 جوان 2023، المتعلق بالنقد والمصرفية، ج.ر، العدد 43، الصادرة بتاريخ 09 جويلية 2023.

(4) المادة 95، القانون رقم 09-23.

الدولية للأمن المعلوماتي لضمان سرية وسلامة التحويلات المالية الإلكترونية، وفي حالة اكتشاف أي تقصير، يمتلك بنك الجزائر سلطة توقيع جزاءات إدارية ومالية صارمة على المؤسسات المخالفة لضمان التحديث المستمر لبرمجيات الحماية، كما يفرض النظام المصرفي على البنوك التزاماً بتبليغ سلطة النقد عن أي خروقات أمنية تمس حسابات الزبائن والتدابير المتخذة لمعالجتها¹.

رابعاً: دور المعايير الدولية والجهود المقارنة (GDPR, PCI DSS): نظراً للطبيعة العابرة

للحدود التي تنسم بها عمليات الدفع الإلكتروني، استوجب الأمر الاستناد إلى معايير دولية تضمن حداً أدنى من الأمان الرقمي؛ إذ تعتبر اتفاقية بودابست المبرمة في 23 نوفمبر 2001 أول صك دولي يسعى لمواجهة الجرائم المرتكبة عبر شبكات المعلوماتية، من خلال وضع آليات دولية لتبادل المعلومات الرقمية والتعاون القضائي السريع².

ساهمت القواعد الأوروبية (GDPR) في تعزيز الحق في الخصوصية المالية، وهو ما استلهمه التشريع الوطني لضمان أمن المعطيات وحمايتها من الوصول غير المصرح به، لاسيما في ظل مخاطر معالجة البيانات الضخمة (Big Data). ومن الناحية التقنية، تبرز معايير أمن بيانات صناعة بطاقات الدفع (PCI DSS) كأهم آلية وقائية تلتزم بها البنوك لتقليل احتمالية تسريب البيانات المالية عبر بروتوكولات أمان عالمية. وبموجب هذه المعايير، يُمنع التاجر الإلكتروني من الاحتفاظ بالبيانات الحساسة للمستهلك³.

(1) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط. 01، د.ف.ج، الإسكندرية، 2006، ص 93.

(2) المادة 13، نظام بنك الجزائر رقم 02-20، المؤرخ في 15 مارس 2020، المتعلق بالعمليات المصرفية وتدقيق البيانات المالية، ج.ر، العدد 21، السنة 2020.

(3) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، ط 01، د.ف.ج، الإسكندرية، 2007، ص 318.

الفرع الثاني: دور المصارف ومقدمي الخدمات في تحقيق الحماية

إذا كانت القواعد القانونية تضع الإطار العام للأمان الرقمي، فإن العبء العملي يقع بصفة مباشرة على المصارف ومقدمي خدمات الدفع؛ باعتبارهم الطرف الأكثر تمكناً من الأدوات التقنية. وتتجسد هذه الحماية في مجموعة من الالتزامات المهنية الفنية التي تهدف إلى تحصين المعاملات المالية من الاختراقات، وللوقوف على ملامح هذا الدور الوقائي التقني و سنقسم هذا الفرع كالتالي:

أولاً: الالتزامات القانونية لمقدمي الخدمة تجاه المستهلك.

ثانياً: الالتزام ببذل عناية خاصة في حماية الأموال والبيانات.

ثالثاً: الآليات الفنية لتعزيز أمن المعاملات (التشفير والمصادقة MFA).

رابعاً: أنظمة كشف ومنع الاحتيال (Fraud Detection Systems).

أولاً: الالتزامات القانونية لمقدمي الخدمة تجاه المستهلك: تُشكل الالتزامات القانونية الملزمة على عاتق مقدمي خدمات الدفع الإلكتروني حجر الزاوية في بناء الثقة الرقمية؛ إذ يلتزم المورد الإلكتروني بضمان أمن المعاملات التي تتم عبر منصته، ويتحمل المسؤولية عن كل خلل يؤدي إلى تسريب البيانات المالية للمستهلك، ما لم يثبت وجود سبب أجنبي.¹ ولا يقف هذا الواجب عند حدود الوسائل التقنية، بل يمتد ليشمل التزام مقدم الخدمة بتزويد المستهلك بالمعلومات المتعلقة بشروط استخدام وسيلة الدفع والمخاطر المرتبطة بها قبل التعاقد.²

(1) المادة 18، القانون رقم 05-18، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ررقم 28، الصادرة بتاريخ 16 ماي 2018.

(2) المادة 12، القانون رقم 05-18.

كما يبرز الالتزام بالحفاظ على السر المهني والمصرفي كالتزام جوهري؛ حيث إن الالتزام بالسرية المصرفية في مجال الدفع الإلكتروني يعد التزاماً بتحقيق نتيجة، تقع بموجبه على البنك مسؤولية ضمان عدم وصول الأغيار إلى الأرقام السرية أو المعطيات الشخصية للعملاء.¹ وفي هذا السياق، يبرز دور البنوك في تحديث بروتوكولات الأمان بصفة دورية لضمان استمرارية الحماية ضد الأساليب الإجرامية المتطورة،² وهو ما يجد سنده القانوني في النصوص التي تلزم مستخدمي البنوك والمؤسسات المالية بوجوب الحفاظ على السر المهني تحت طائلة العقوبات.³

علاوة على ذلك، يعد الإخلال بالالتزام بالإعلام والتبصير من طرف مقدم الخدمة خطأً مهنيًا يستوجب المسؤولية، خاصة إذا أدى نقص المعلومات إلى وقوع المستهلك في فخ الاحتيال الإلكتروني.⁴ وبذلك، تتحول هذه الالتزامات من مجرد واجبات تعاقدية إلى ضمانات قانونية تهدف إلى حماية الطرف الضعيف في العلاقة الرقمية، موازنةً بين الامتيازات التي يحققها مقدمو الخدمة والمسؤوليات الجسيمة التي يتحملونها لضمان بيئة دفع آمنة.

ثانياً: الالتزام ببذل عناية خاصة في حماية الأموال والبيانات: يُعد الالتزام ببذل العناية في حماية الودائع والبيانات أحد أقدم الالتزامات المصرفية، إلا أنه اكتسب في ظل الدفع الإلكتروني أبعاداً تقنية معقدة تفرض على البنك عناية خاصة تتجاوز عناية الشخص العادي إلى عناية المهني المحترف؛ حيث يلتزم البنك ببذل العناية اللازمة لحماية أموال زبائنه، وتعتبر هذه العناية من طبيعة

(1) نبيل إبراهيم سعد، الالتزام بالإعلام في عقود استهلاك الخدمات المصرفية، د.ج.ج، الإسكندرية، 2004، ص 115.

(2) نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، الطبعة 01، منشورات الحلبي الحقوقية، لبنان، 2004، ص 342.

(3) المادة 117، القانون رقم 23-09، المؤرخ في 21 جوان 2023، المتعلق بالنقد والمصرفية، ج.ر، رقم 43، الصادرة بتاريخ 09/07/2023.

(4) نزيه نعيم شلالا، المرجع السابق، ص 350.

خاصة بالنظر إلى الصفة المهنية للمصرفي، الذي يضمن سلامة المنظومة التقنية التي يضعها تحت تصرف الجمهور.¹ ويميل التوجه التشريعي والقضائي الحديث إلى تكييف التزام البنك بضمان أمن وسائل الدفع كالتزام بتحقيق نتيجة لا يرى المصرف منه إلا إثبات القوة القاهرة أو خطأ الزبون.²

ويتسع نطاق هذا الالتزام ليشمل حماية البيانات ذات الطابع الشخصي المرتبطة بعمليات الدفع؛ إذ إن مسؤولية البنك في الحفاظ على سرية البيانات وسلامة الأموال تتعدى القواعد العامة في الوديعة، لتصل إلى مستوى الالتزام بضمان الحصانة الرقمية للحسابات ضد كافة أنواع التطفل المعلوماتي.³ ويفرض القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وجوب اتخاذ التدابير التقنية والتنظيمية اللازمة لحماية هذه المعطيات من الإتلاف أو الضياع أو الولوج غير المصرح به،⁴ مما يجعل البنك مسؤولاً عن توفير بيئة دفع محصنة تقنياً بصفة مستمرة.

علاوة على ذلك، يمتد مفهوم العناية الخاصة ليشمل الالتزام بالمتابعة المستمرة لنشاط الحسابات ورصد العمليات المشبوهة لتفادي وقوع الضرر أو تفاقمه.⁵ ويعد البنك مسؤولاً عن كل إهمال في تحديث برمجيات الحماية، حيث أن التزامه ببذل العناية يقتضي متابعة التطورات المتلاحقة

(1) المادة 112، القانون رقم 09-23، المؤرخ في 21 جوان 2023، المتعلق بالنقد والمصرفية، ج.ر، العدد 43، الصادرة بتاريخ 2023/07/09.

(2) المادة 19، القانون رقم 05-18، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 ماي 2018.

(3) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط 01، د.ف.ج، الإسكندرية، 2006، ص 155.

(4) المادة 34، القانون رقم 07-18، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر، العدد 34، الصادرة بتاريخ 10 جوان 2018.

(5) نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، ط 01، منشورات الحلبي الحقوقية، لبنان، 2004، ص 362.

في أساليب القرصنة المالية وتوفير الحلول التقنية المضادة لها.¹ وعليه، فإن تكريس هذا الالتزام يهدف إلى نقل عبء المخاطر التقنية من كاهل المستهلك إلى كاهل المؤسسة المالية المتمكنة، لضمان سلامة الذمة المالية وسرية البيانات ككل لا يتجزأ.

ثالثاً: الآليات الفنية لتعزيز أمن المعاملات (التشفير والمصادقة MFA): تُمثل الآليات الفنية خط الدفاع المادي والأكثر فاعلية في حماية المستهلك من جرائم الدفع الإلكتروني؛ إذ لا تكفي النصوص القانونية وحدها لصد الهجمات السيبرانية ما لم تكن مدعومة بروتوكولات تقنية متطورة. ويعد التشفير من أهم الوسائل التقنية المعتمدة لتأمين وسائل الدفع الإلكتروني، حيث يعمل على إخفاء حقيقة البيانات المتبادلة بين أطراف المعاملة المالية ويمنع الأغيار من الاطلاع عليها أو تعديلها.² وتلتزم المؤسسات المالية بتبني بروتوكولات تشفير متطورة لضمان أمن الشبكات وحماية المعطيات المصرفية من مخاطر القرصنة التقنية،³ وهو ما يتعزز باستخدام التوقيع الإلكتروني الذي يضمن تحديد هوية الموقع وصحة صدور المعاملة منه.⁴ حيث تفرض هذه المنظومة التقنية ما يعرف بـ "المصادقة المتعددة العوامل" (Multi-Factor Authentication)، التي تشكل طبقة حماية إضافية تتجاوز كلمة السر التقليدية لتشمل رموزاً مؤقتة أو بصمات حيوية، مما يقلص من فرص نجاح عمليات انتحال الشخصية الرقمية حتى في حالة تسريب بيانات الدخول الأساسية.

(1) نزيه نعيم شلالا، المرجع السابق، ص 365.

(2) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، ط 02، د.م.ج، الإسكندرية، 2010، ص 112.

(3) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، الطبعة 01، د.م.ج، الإسكندرية، 2003، ص 140.

(4) المادة 02، القانون رقم 15-04، المؤرخ في 2015/02/1، المتعلق بالتوقيع والتصديق الإلكترونيين، ج.ر، العدد 06، الصادرة بتاريخ 2015/02/10.

علاوة على ذلك، تلعب جدران الحماية وأنظمة التشفير دوراً جوهرياً في تحقيق الرقابة الاستباقية على تدفق البيانات المالية ومنع محاولات الدخول غير المصرح به لقواعد البيانات.¹ وبدمج هذه الوسائل التقنية مع التدابير القانونية، نكون أمام منظومة حماية متعددة الطبقات تضمن للمستهلك بيئة دفع رقمية تتسم بالموثوقية العالية.

رابعاً: أنظمة كشف ومنع الاحتيال (Fraud Detection Systems): تمثل أنظمة

كشف ومنع الاحتيال الذروة التقنية في منظومة الحماية الوقائية للمستهلك؛ إذ تعتمد الرقابة الإلكترونية الاستباقية على أنظمة برمجية ذكية تقوم بتحليل حركات الدفع لحظة وقوعها، وربطها بسلوك المستخدم المعتاد لكشف أي محاولة تلاعب بالبيانات أو انتحال للشخصية الرقمية. وتلتزم البنوك بتطبيق معايير اليقظة المعلوماتية واستخدام أنظمة الإنذار المبكر للحد من مخاطر الهجمات السيبرانية على حسابات الزبائن.²

فضلاً على ذلك، ترتبط هذه الأنظمة بقواعد بيانات دولية محدثة تحتوي على القوائم السوداء للمواقع والمنصات المشبوهة، مما يوفر حماية ديناميكية تتغير بتغير التهديدات المحيطة بالبيئة الرقمية.³ إن أنظمة منع الاحتيال تمثل الوسيلة الأكثر نجاعة في مواجهة الإجرام المعلوماتي العابر للحدود، كونها توفر حماية تقنية فورية لا تتأثر بالحدود الجغرافية وتعمل على إحباط العمليات المشبوهة قبل اكتمال مسارها المالي.⁴

(1) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، ط 02، د.م.ج، الإسكندرية، 2010، ص 118

(2) المرجع نفسه، ص 220.

(3) خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، ط 01، د.ف.ج، الإسكندرية، 2007، ص 360.

(4) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، ط 01، د.م.ج، الإسكندرية، 2003، ص 215.

ويجد هذا الالتزام التقني سنده في التشريع المصرفي الجديد الذي يلزم البنوك والمؤسسات المالية بضمان أمن وسلامة نظمها المعلوماتية واعتماد آليات رقابية فعالة لحماية ودائع الزبائن،¹ حيث يلعب الذكاء الاصطناعي دوراً محورياً في تعزيز هذه الآليات وتوفير حلول تقنية مضادة لأساليب القرصنة المالية الحديثة.² وبذلك، تكتمل حلقة الأمان الوقائي التي تضمن استقرار النظام المالي وتعزز من إقبال المواطنين على استخدام وسائل الدفع الإلكتروني بكل أمان.

المطلب الثاني: آليات التسوية القضائية والبديلة للمنازعات

إنَّ فعالية الحماية القانونية للمستهلك في مجال الدفع الإلكتروني لا تكتمل إلا بوجود منظومة إجرائية تسمح له بالوصول إلى حقه ومواجهة الأضرار الناتجة عن المعاملات الرقمية. ونظراً لخصوصية هذه النزاعات وما تتطلبه من سرعة وخبرة تقنية، فإنَّ المشرع لم يكتفِ بالمسار القضائي التقليدي، بل فتح المجال أمام الوسائل البديلة والودية التي تتناسب مع طبيعة التجارة الإلكترونية. وبناءً على ذلك، سنقوم بدراسة آليات فض النزاعات من خلال تقسيم هذا المطلب إلى الفرعين التاليين:

الفرع الأول: الحماية القضائية عبر رفع الدعاوى والطعون.

الفرع الثاني: التسوية الودية للمنازعات والتوصيات المستقبلية

(1) المادة 94، القانون رقم 23-09، المؤرخ في 21 جوان 2023، المتعلق بالنقد المصرفية، ج.ر، العدد 43، الصادرة بتاريخ 09 جويلية 2023.

(2) محمد أمين الرومي، المرجع السابق، ص 228.

الفرع الأول: الحماية القضائية عبر رفع الدعاوى والطعون

بمجرد وقوع التعدي على الحقوق المالية للمستهلك في بيئة الدفع الرقمي، تبرز الحماية القضائية كضمانة دستورية وقانونية أساسية لاستعادة التوازن العقدي وجبر الضرر. وتقتضي هذه الحماية تفعيل القواعد الإجرائية والموضوعية التي تمكن المتضرر من ملاحقة الجناة أو أمام الجهات القضائية المختصة. ولتسليط الضوء على آليات هذه الحماية، سنقوم بتقسيم كالاتية:

أولاً: إجراءات رفع الدعوى المدنية للمطالبة بالتعويض.

ثانياً: استخدام الدعوى الجنائية كأداة ضغط للحصول على الحقوق.

ثالثاً: دور الدعوى الجزائية في خدمة الحق المدني للمستهلك.

رابعاً: الإشكالات الإجرائية في تنفيذ الأحكام القضائية ضد الجناة.

أولاً: إجراءات رفع الدعوى المدنية للمطالبة بالتعويض: تعد الدعوى المدنية الوسيلة القانونية الجوهرية التي يلوذ بها المستهلك لجبر الأضرار المادية والمعنوية الناتجة عن تعثر أو قرصنة عمليات الدفع الرقمي؛ حيث تنعقد الخصومة القضائية كأصل عام أمام الجهة القضائية التي يقع في دائرة اختصاصها موطن المدعى عليه، مع مراعاة القواعد الخاصة بحماية المستهلك المكرسة قانوناً.¹ وتخضع هذه المنازعات للقواعد العامة في الاختصاص القضائي، مع ضرورة تكييف القواعد الإجرائية بما يضمن حماية الطرف الضعيف تقنياً في مواجهة المؤسسات المصرفية.²

(1) المادة 37، القانون رقم 08-09، المؤرخ في 25 فيفري 2008، المتضمن قانون إ.م.إ.، ج.ر، العدد 21، الصادرة بتاريخ 23 أبريل 2008.

(2) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط 01، د.ف.ج، الإسكندرية، 2006، ص 120.

وتقتضي مباشرة هذه الدعوى دوراً حيوياً للقاضي في تكييف المسؤولية المدنية للمصرف بناءً على طبيعة الالتزام بضمان أمن وسائل الدفع الإلكترونية،¹ ومحاولة ردم الفجوة التقنية بين طرفي النزاع. وحيث إن إثبات الخطأ في جانب البنك يُعدّ أمراً عسيراً على المستهلك، فإن ذلك يتطلب في الغالب الاستعانة بخبير قضائي في المعلوماتية لتحديد مسؤولية كل طرف عن الخلل الذي أصاب النظام المصرفي؛² إذ يهدف هذا المسار إلى تقدير التعويض الذي يشمل ما لحق الدائن من خسارة وما فاتته من كسب، بشرط أن يكون هذا نتيجة طبيعية لعدم الوفاء بالالتزام.³

علاوة على ذلك، ترتبط جدية المطالبة بالحقوق بمدى التزام المستهلك بالضوابط الإجرائية المتعلقة بالإثبات الرقمي والإخطار، لضمان قيام مسؤولية المصرف عن مخاطر التقدم التقني وعيوب الأنظمة المعلوماتية؛⁴ فالدعوى المدنية تظل الحصن الذي يعيد الأمور إلى نصابها ويجبر مقدمي الخدمة على تحمل تبعات المخاطر الرقمية، مما يكرس سيادة القانون في الفضاء المالي الافتراضي.

ثانياً: استخدام الدعوى الجنائية كأداة ضغط للحصول على الحقوق: لا يقتصر دور القضاء الجزائي في منازعات الدفع الإلكتروني على إنزال العقوبة بالفاعل فحسب، بل يمتد ليكون أداة ضغط قانونية فعالة بيد المستهلك لاسترداد حقوقه المالية المسلوقة؛ إذ تساهم الدعوى العمومية بشكل أساسي في كشف الحقيقة التقنية التي يعجز المستهلك عن إثباتها بمفرده، مما يسهل عليه

(1) نبيل إبراهيم سعد، الالتزام بالإعلام في عقود استهلاك الخدمات المصرفية، د.ج.ج، الإسكندرية، 2004، ص 175.

(2) نبيل إبراهيم سعد، المرجع السابق، ص 180.

(3) المادة 182، الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، ج.ر، العدد 78، الصادرة بتاريخ 30 سبتمبر 1975.

(4) محمد بودالي، المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة 01، د.ف.ج، الإسكندرية، 2006، ص 142.

الحصول على التعويض لاحقاً من خلال الاستناد إلى قوة الأدلة الجنائية المستخلصة.¹ ويتجلى ذلك من خلال الدور الرقابي والقانوني الذي تمارسه النيابة العامة في تحريك الدعوى العمومية ومباشرتها لضمان سير العدالة.²

كما تبرز فاعلية هذا المسار في دور الضبطية القضائية المتخصصة في تتبع الجرائم المعلوماتية، وتوفير الأدلة الرقمية التي تخدم مصلحة الضحية في استرداد أمواله من خلال محاضر رسمية تضع الجهة المتسببة في الخلل أمام مسؤوليتها.³ ويستند ذلك إلى الصلاحيات الواسعة التي منحها المشرع لسلطات التحقيق في مراقبة الاتصالات وتفتيش المنظومات المعلوماتية في إطار الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.⁴

علاوة على ذلك، فإنّ الضغط الذي تمارسه الدعوى الجزائية يدفع المؤسسات المالية أحياناً للتعويض الطوعي لتفادي الإحراج القانوني الناتج عن ثبوت وجود ثغرات أمنية قد تكسر مسؤوليتها التقصيرية بموجب أحكام قضائية نهائية؛⁵ إذ إنّ إجراءات تجميد الحسابات والمعطيات المعلوماتية تساهم بشكل مباشر في تأمين الحقوق المالية ومنع تهريبها.⁶

(1) خالد ممدوح إبراهيم، التحقيق الجنائي في الجرائم المستحدثة (جرائم الكمبيوتر والإنترنت)، ط 01، د.ف.ج، الإسكندرية، 2008، ص 45.

(2) المادة 35، الأمر رقم 66-155، المؤرخ في 08 جوان 1966، المتضمن ق.إ.ج، المعدل والمتمم، ج.ر، العدد 48، الصادرة بتاريخ 10 جوان 1966.

(3) خالد ممدوح إبراهيم، المرجع السابق، ص 112.

(4) المادة 04، القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47، الصادرة بتاريخ 16 أوت 2009.

(5) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، الطبعة الأولى، د.م.ج، الإسكندرية، 2003، ص 190.

(6) المادة 12، القانون رقم 09-04.

ثالثاً: دور الدعوى الجزائية في خدمة الحق المدني للمستهلك: تعتبر الدعوى الجزائية في منازعات الدفع الإلكتروني قاطرة حقيقية للحق المدني؛ إذ تسمح الدعوى المدنية التبعية للمستهلك المتضرر من الجرائم المصرفية الإلكترونية بالمطالبة بالتعويض أمام القاضي الجزائي، مما يجنبه تعقيدات الإثبات في الدعوى المدنية المستقلة، ويضمن له سرعة الحصول على حقوقه.¹ وينشأ هذا الحق للمستهلك عن كل جريمة تسببت له في ضرر جسماني أو مادي أو أدبي، حيث يمكنه ملاحقة هذا الحق تبعاً للدعوى العمومية في آن واحد أمام القاضي الجزائي.²

وتتجلى خدمة الدعوى الجزائية للحق المدني في مبدأ حجية الحكم الجزائي أمام القضاء المدني؛ فإدانة الجاني معلوماتياً تؤدي بالضرورة إلى تثبيت حق المستهلك في التعويض المالي الكامل، مما يختصر شوطاً طويلاً في إثبات أركان المسؤولية التقصيرية.³ ويجد هذا المسار سنداً في القواعد الخاصة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي تمنح القضاء صلاحيات واسعة في جمع الأدلة الرقمية التي تخدم الحقوق المالية للضحايا.⁴

كما أنّ ارتباط الحق المدني بالمسار الجزائي في منازعات الدفع الإلكتروني يمنح المستهلك ميزة الاستفادة من الخبرات التقنية التي تجربها الضبطية القضائية لإثبات وقوع الضرر ومقداره،⁵ وهو

(1) آية صويلح وسناء حمود، تسوية منازعات العمليات المصرفية الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالة، 2024، ص 80.

(2) المادة 02، الأمر رقم 66-155، المؤرخ في 08 جوان 1966، المتضمن ق.إ.ج، المعدل والمتمم، ج.ر، العدد 48، الصادرة بتاريخ 10 جوان 1966.

(3) إسحق إبراهيم منصور، دراسات في المسؤولية الطبية والقضائية، ط 01، د.م.ج، الإسكندرية، 2002، ص 145.

(4) المادة 15، القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47، الصادرة بتاريخ 16 أوت 2009.

(5) آية صويلح وسناء حمود، المرجع السابق، ص 81.

ما يعد امتيازاً إجرائياً هاماً في مواجهة المؤسسات المصرفية. وتخضع هذه الدوى التبعية لشروط قبول محددة تضمن اتصال القاضي الجزائي بالشق المدني للنزاع بشكل قانوني سليم¹.

رابعاً: الإشكالات الإجرائية في تنفيذ الأحكام القضائية ضد الجناة: تعتبر مرحلة تنفيذ الأحكام القضائية هي الثمرة النهائية التي يريجوها المستهلك من وراء لجوئه للقضاء، إلا أن هذه المرحلة في منازعات الدفع الإلكتروني تصطدم بجملة من الإشكالات؛ إذ إن إشكالية تنفيذ الأحكام القضائية في المادة المصرفية الإلكترونية تعد من أعقد المسائل القانونية، نظراً لارتباطها بجناة غالباً ما يكونون مجهولين أو يمارسون نشاطهم من خارج الحدود الوطنية، مما يعطل تفعيل القوة التنفيذية للسند القضائي². وتخضع هذه المرحلة في أصلها للقواعد العامة للتنفيذ الجبري التي تستلزم وجود سند تنفيذي مستوفٍ للشروط القانونية لضمان استرداد الحقوق³.

وتتمثل أبرز هذه العقبات في التحديات التقنية والقانونية التي تواجه المحضر القضائي عند محاولة تنفيذ أحكام تتعلق برد مبالغ مالية مختلصة عبر وسائط إلكترونية عابرة للحدود، خاصة عند محاولة تتبع الأموال في بيئات رقمية معقدة، ويفرض هذا الوضع ضرورة تفعيل آليات التعاون القضائي الدولي التي أقرها المشرع في مجال جمع الأدلة الرقمية وتنفيذ الإنابات القضائية، لملاحقة الجناة والمنصات التي تقع خارج الإقليم الوطني⁴.

(1) المادة 03، الأمر رقم 66-155.

(2) آية صويلح وسناء حمود، تسوية منازعات العمليات المصرفية الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قلعة، 2024، ص 75.

(3) المادة 600، القانون رقم 08-09، المؤرخ في 25 فيفري 2008، المتضمن ق.إ.م.إ، ج.ر، العدد 21، الصادرة بتاريخ 23 أفريل 2008.

(4) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، ط 01، د.م.ج، الإسكندرية، 2003، ص 210.

الفرع الثاني: التسوية الودية للمنازعات والتوصيات المستقبلية

نظراً لما تتسم به منازعات الدفع الإلكتروني من تعقيد تقني وحاجة ملحة للسرعة في الحسم، فإنَّ المسار القضائي التقليدي قد لا يكون دائماً الخيار الأمثل للمستهلك أو للمؤسسات المصرفية على حد سواء. ومن هذا المنطلق، برزت الوسائل البديلة والودية كخيار استراتيجي يهدف إلى تفعيل العدالة الرضائية وتخفيف العبء عن المحاكم، مع استشراف آفاق قانونية لتعزيز أمان هذه المعاملات مستقبلاً. ولإحاطة بجوانب هذا الفرع، سنقوم بتناول الأجزاء الآتية:

أولاً: دور لجان التحكيم والوساطة المتخصصة.

ثانياً: دور هيئات حماية المستهلك ومكاتب الشكاوى المصرفية.

ثالثاً: التوصيات لتعزيز الحماية القانونية للمستهلك مستقبلاً.

رابعاً: الدعوة لإنشاء هيئة متخصصة لفض منازعات الدفع الإلكتروني.

أولاً: دور لجان التحكيم والوساطة المتخصصة: أمام تزايد حجم وتعقيد منازعات الدفع الإلكتروني، أثبتت الوسائل البديلة لتسوية المنازعات نجاعة كبيرة في الحفاظ على الروابط التعاقدية؛ إذ تعد الوساطة والتحكيم من أهم الوسائل البديلة التي تضمن للمستهلك والمصرف تسوية عادلة وسريعة للمنازعات الناتجة عن العمليات المصرفية الإلكترونية¹. وتعتبر الوساطة آلية رضائية يسعى من خلالها الأطراف بمساعدة وسيط محايد إلى إيجاد حل ودي للنزاع، وهي إجراء نظمه المشرع ضمن أحكام قانون الإجراءات المدنية والإدارية كخيار لفض الخصومات.²

(1) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، ط. 02، د.م.ج، الإسكندرية، 2010، ص 210.

(2) المادة 990، القانون رقم 08-09، المؤرخ في 25 فيفري 2008، المتضمن ق.إ.م.إ، ج، العدد 21، الصادرة بتاريخ 23 أفريل 2008.

وتبرز أهمية الوسيط المصرفي في تفعيل العدالة الرضائية وتسهيل حصول المستهلك على تعويضات سريعة بعيداً عن تعقيدات القضاء العام،¹ خاصة وأن مرونة هذا الإجراء تسمح بإجرائه عن بُعد بما يتماشى مع طبيعة المعاملات الرقمية. أما التحكيم، فيعتبر وسيلة قضائية خاصة تتطلب كفاءة تقنية عالية لمواكبة التطورات السريعة في أنظمة الدفع الرقمي، وهو ما توفره مراكز التحكيم المتخصصة؛² حيث منح القانون للأطراف حق اللجوء إلى التحكيم في المسائل التي يجوز فيها الصلح وفق إجراءات محددة.³

بالرغم من القيمة الإجرائية للتحكيم، إلا أن إدراج شرط التحكيم في العقود الإلكترونية يثير إشكالات قانونية حول مدى توافقها مع القواعد الآمرة لحماية المستهلك في التشريع الجزائري، لا سيما في عقود الإذعان.⁴ ومع ذلك، تظل هذه الوسائل البديلة رافداً أساسياً يدعم الثقة في القنوات الرقمية للدفع، من خلال توفير ضمانات المحاكمة العادلة وشفافية الإجراءات، مما يجعلها ضرورة حتمية لمواجهة تحديات الفضاء الافتراضي.

ثانياً: دور هيئات حماية المستهلك ومكاتب الشكاوى المصرفية: إلى جانب الوسائل القضائية والبديلة، تلعب الهيئات الإدارية والرقابية دوراً جوهرياً في إرساء دعائم الحماية الاستباقية للمستهلك في بيئة الدفع الرقمي؛ إذ تعتبر مكاتب الشكاوى داخل المؤسسات المصرفية الآلية الأولى التي يلجأ إليها المستهلك لاسترجاع حقوقه، وهي تعكس مدى التزام البنك بتقديم خدمة آمنة

(1) فريدة بن يونس، الوساطة كآلية بديلة لتسوية المنازعات في القانون الجزائري، دار هومة للنشر والتوزيع، الجزائر، 2011، ص 45.

(2) عبد الفتاح بيومي حجازي، نحو قانون عالمي للتجارة الإلكترونية، ط01، د.ف.ج، الإسكندرية، 2002، ص 87.

(3) المادة 1006، القانون رقم 08-09.

(4) عمر سعد الله، قانون التحكيم التجاري الدولي (دراسة مقارنة)، ط02، د.م.ج، الإسكندرية، 2005، ص 112.

وشفافة لزيائته في ظل تنامي مخاطر الدفع الإلكتروني.¹ ويفرض القانون على مقدمي الخدمات ضرورة توفير ضمانات الأمان والتحقق من جودة الخدمات الرقمية المقدمة للجمهور.²

من جهة أخرى، تؤدي جمعيات حماية المستهلك دوراً رقائياً وتوعوياً لا يستهان به، من خلال تمثيل المشتركين أمام الهيئات المصرفية وتوجيههم إجرائياً لاسترداد الأموال المختلسة رقمياً،³ بالإضافة إلى حقها في ممارسة التقاضي الجماعي للدفاع عن المصالح المشتركة للمستهلكين. ويسمح القانون للمستهلك المتضرر بتقديم تظلم إداري ضد كل معاملة تجارية إلكترونية غير قانونية أو عند الإخلال بالتزامات الأمان،⁴ مما يعزز من فاعلية الرقابة الاستباقية، وهو ما يفرض على البنوك ضرورة الاستجابة الفورية لهذه الإخطارات تحت طائلة المساءلة أمام سلطات الضبط المالي، لضمان استمرارية الثقة الرقمية بين المؤسسة وعملائها.

إنَّ الصلح الإداري الذي تشرف عليه مكاتب الشكاوى المصرفية يهدف أساساً إلى الحفاظ على سمعة البنك وتجنب العقوبات التي قد تفرضها السلطات الرقابية في حال ثبوت تقصيرها؛⁵ إذ منح المشرع لجمعيات حماية المستهلك صلاحية التدخل في الدعاوي القائمة والمطالبة بالتعويضات المناسبة عن الأضرار اللاحقة بالمستهلكين.

(1) محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، ط01، د.ف.ج، الإسكندرية، 2006، ص 42.

(2) المادة 20، القانون رقم 03-09، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، المعدل والمتمم، ج.ر، العدد 15، الصادرة بتاريخ 08 مارس 2009.

(3) محمد بودالي، المرجع السابق، ص 88.

(4) المادة 30، القانون رقم 05-18، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 ماي 2018.

(5) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، ط02، د.م.ج، الإسكندرية، 2010، ص 150.

ثالثاً: التوصيات لتعزيز الحماية القانونية للمستهلك مستقبلاً: إنّ المتتبع لمسار الحماية القانونية للمستهلك في مجال الدفع الرقمي يدرك أنّ النصوص التشريعية الحالية تظل في سباق مستمر مع التطورات التقنية؛ إذ تعد عملية تحديث المنظومة القانونية لمواكبة تقنيات الدفع الإلكتروني ضرورة حتمية، لا تقتصر فقط على الجانب الردعي، بل يجب أن تشمل آليات وقائية تضمن حماية استباقية لبيانات وأموال المستهلكين.¹ ويفرض القانون على المورد الإلكتروني الالتزام بضمان سرية البيانات وأمن المعاملات وفق المعايير التقنية المعتمدة، وهو ما يستوجب تحييناً مستمراً للضوابط الإجرائية.

وتأسيساً على ذلك، تبرز أهمية إنشاء صناديق ضمان خاصة لتعويض ضحايا الاحتيال الإلكتروني في غياب المسؤولية المباشرة للمصرف، كآلية اجتماعية وقانونية لحماية الطرف الضعيف في هذه العلاقة الرقمية، مما يرفع عن كاهل المستهلك عبء إثبات الأخطاء التقنية المعقدة. إنّ بناء الثقة في المعاملات الرقمية يتطلب من المشرع تبني سياسة جنائية مرنة وقادرة على التعامل مع الطبيعة الافتراضية للجريمة المعلوماتية وحماية المستهلك من الشروط التعسفية في العقود المصرفية.²

كما يجب تفعيل حق المستهلك في الأمان والتعويض عن الأضرار اللاحقة به جراء استخدام الخدمات الرقمية، وهو ما يستدعي بالضرورة تفعيل آليات الرقابة التقنية المستمرة من طرف الهيئات المصرفية المركزية لضمان سلامة قنوات الدفع وحمايتها من الاختراقات.³ إنّ تبني هذه التوصيات سيساهم في نقل الحماية من حيز النصوص الجامدة إلى واقع ملموس، مما يساهم في بناء جسور الثقة بين المواطن ومنظومة الدفع الإلكتروني، ويحفز على الانخراط الفعال في التحول الرقمي الشامل.

(1) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، ط02، د.م.ج، الإسكندرية، 2010، ص 45.

(2) المادة 27، القانون رقم 05-18، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 ماي 2018.

(3) عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، ط01، د.ف.ج، الإسكندرية، 2002، ص 315.

رابعاً: الدعوة لإنشاء هيئة متخصصة لفض منازعات الدفع الإلكتروني: إنَّ القصور الذي تعاني منه الآليات التقليدية في استيعاب الخصوصية الفنية لمنازعات الدفع الإلكتروني، يفرض لزماً التفكير في ابتكار مؤسساتي يتجاوز الحلول الترقيعية؛ إذ يقتضي نظام التقاضي الإلكتروني وجود بيئة تقنية وقانونية تسمح بمواكبة الطبيعة الافتراضية للمنازعات، بما يضمن سرعة الفصل فيها من خلال هيئات تمتلك الكفاءة المعلوماتية اللازمة.¹ ويمنح القانون للجهات الإدارية صلاحية اتخاذ تدابير وقائية وعقوبات إدارية لضمان سلامة التعاملات الإلكترونية وحماية المستهلك.²

وتكمن أهمية التحكيم المؤسسي والهيئات المتخصصة في تعزيز الثقة بالمعاملات المصرفية عبر الإنترنت، كونها توفر حماية تقنية فورية لا تتأثر بالحدود الجغرافية وتعمل على إحباط العمليات المشبوهة قبل اكتمال مسارها المالي.³ ويجب أن تتمتع هذه الهيئات بالاستقلالية والحياد، مع منح قراراتها الصبغة التنفيذية لضمان استقرار المراكز القانونية، لا سيما وأنَّ القانون يحدد بدقة السندات التي تكتسي القوة التنفيذية الجبرية، وهذا ما يجعل من أحكام التحكيم وسيلة فعالة لتجاوز بطء الإجراءات القضائية التقليدية، من خلال إصدار قرارات ملزمة تتمتع بـ "حجية الشيء المقضي به" وتكون قابلة للتنفيذ الجبري بمجرد تذييلها بأمر التنفيذ من الجهة القضائية المختصة، مما يضمن للمستهلك والمؤسسة على حد سواء سرعة استعادة الحقوق المالية في بيئة رقمية لا تحتمل التأخير.⁴

(1) المادة 15، القانون رقم 09-03، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، المعدل والمتمم، ج.ر، العدد 15، الصادرة بتاريخ 08 مارس 2009.

(2) خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، مرجع سابق، ص 188.

(3) خالد ممدوح إبراهيم، التقاضي الإلكتروني (الدعوى الإلكترونية وإجراءات المحاكمة أمام القضاء الإلكتروني)، ط 01، د.ف.ج، الإسكندرية، 2008، ص 52.

(4) المادة 40، القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج.ر، العدد 28، الصادرة بتاريخ 16 ماي 2018.

نخلص في ختام هذا الفصل إلى أنَّ النظام القانوني لمساءلة الأطراف عن أضرار الدفع الإلكتروني قد شهد تحولاً نوعياً يهدف إلى استيعاب الطبيعة الرقمية للمخاطر، حيث اتضح لنا أنَّ تحديد المسؤولية وتوزيع أعباء التعويض يركز على الموازنة بين مصلحة المؤسسات المالية وحق المستهلك في الأمان المالي. كما تبين أنَّ تفعيل القواعد الوقائية، إلى جانب آليات التسوية القضائية والبديلة، يُمثل حجر الزاوية في بناء منظومة دفع رقمي آمنة تعزز الثقة والشفافية في المعاملات. وبناءً على ما تقدّم من تحليل للمسؤولية والآليات الحمائية، نكون قد استكملنا دراسة الجوانب الإجرائية والموضوعية لهذا البحث. ولربط هذه النتائج الجزئية بالنتائج الكلية للمذكرة، سنتقل في المحطة التالية إلى صياغة الخاتمة العامة التي ستجيب بشكل نهائي على الإشكالية المطروحة وتستعرض أهم التوصيات المقترحة لتعزيز حماية المستهلك مستقبلاً.

خاتمة

تعد هذه الدراسة محاولة قانونية جادة ومتواضعة لتسليط الضوء على واحد من أعقد وأبرز المواضيع المعاصرة التي فرضتها الثورة الرقمية المتسارعة على المنظومة المصرفية والمالية العالمية والوطنية على حد سواء، وهو موضوع "حماية المستهلك من مخاطر الدفع الإلكتروني". ومن خلال الرحلة البحثية العميقة والمركزة التي خضناها عبر فصول هذه المذكرة، وما رافقها من تحليل دقيق ومقارن للنصوص التشريعية الوطنية، تبين لنا بوضوح أن المشرع الجزائري، وبالرغم من امتلاكه لترسانة قانونية كلاسيكية متينة وفرت حماية تقليدية لسنوات طويلة، وجد نفسه فجأة أمام نمط جديد كلياً من المعاملات يتسم بالافتراضية الكاملة، والسرعة الفائقة، والتحلل من القيود المكانية والزمانية، مما خلق فجوة واضحة تتطلب مرونة تشريعية وتقنية عالية تتجاوز القواعد التقليدية التي صُممت لبيئة مادية ملموسة، وصولاً إلى ضرورة ابتكار آليات قانونية تكيف مع طبيعة النبضات الإلكترونية والتدفقات المالية الافتراضية التي لا تعترف بالحدود الجغرافية.

ولقد استخلصنا من خلال البحث الدقيق في التكييف الجنائي لجرائم الدفع الإلكتروني ودراسة النظام القانوني لحماية المستهلك جملة من النتائج الجوهرية نلخصها فيما يلي:

- تحول الأفعال الإجرامية من الصور المادية البسيطة إلى جرائم ذكية وعابرة للحدود تستخدم تقنيات برمجية خبيثة وأساليب هندسة اجتماعية متطورة تستهدف الأرصدة والبيانات الشخصية الحساسة في آن واحد.

- تكريس وضعية المستهلك الإلكتروني كطرف الأضعف في العلاقة التعاقدية نتيجة انعدام تكافؤ المعرفة الرقمية بينه وبين المؤسسات المالية الكبرى التي تملك ناصية التكنولوجيا وتدير أنظمة الدفع المعقدة.

- عجز القواعد الإجرائية التقليدية عن مواكبة طبيعة الدليل الرقمي غير المادية وسريعة التلاشي، مما يضع جهات التحقيق والقضاء أمام تحديات كبرى في ضبط وإثبات الاعتداءات السيبرانية.

- تحول فلسفة المسؤولية المصرفية في البيئة الرقمية نحو المسؤولية الموضوعية القائمة على فكرة تحمل المخاطر، حيث أصبح الالتزام بالأمان التزاماً بتحقيق نتيجة يوجب التعويض الفوري للمتضرر. وبناءً على هذه المعطيات المتشابكة، وتجسيدا للمقترحات والتوصيات التي نراها كفيلة بتعزيز الحماية القانونية للمستهلك، فإننا نوصي بما يلي:
- ضرورة صياغة إطار قانوني موحد ومستقل يعنى حصراً بحماية المستهلك في الفضاء الرقمي لإنهاء حالة تشتت النصوص بين قانون العقوبات وقانون التجارة الإلكترونية.
- تفعيل آليات رقابية استباقية بإنشاء هيئات وطنية تقنية متخصصة تتولى مراقبة جودة الأنظمة البنكية وتطوير معايير التشفير وضمان أمن المعاملات المالية اللحظية.
- تكثيف الحملات التحسيسية لنشر الوعي القانوني والتقني لدى المواطنين بأساليب بسيطة للوقاية من مخاطر الاحتيال الإلكتروني والهندسة الاجتماعية المستجدة.
- الاعتماد على الوسائل البديلة لفض المنازعات كالوساطة والصلح لتجاوز ببطء الإجراءات القضائية الكلاسيكية التي لا تتناسب مع سرعة التدفقات المالية الرقمية.
- إلزام المؤسسات المصرفية بفرض نظام تأمين إجباري على كافة العمليات المالية الإلكترونية ضد مخاطر القرصنة لضمان جبر الضرر واستعادة الثقة في النظام المالي الوطني.
- وفي الأخير، نخلص إلى أن الحماية القانونية للمستهلك في الفضاء الرقمي ليست مجرد نصوص جامدة تُسطر في الجرائد الرسمية، بل هي ثقافة مجتمعية متكاملة تتطلب تكاتفاً وثيقاً وجهوداً منسقة بين المشرع، والمؤسسات المصرفية، وجمعيات حماية المستهلك، وصولاً إلى بناء وعي تقني وقانوني صلب لدى المواطن يمثل خط الدفاع الأول الذي يحميه من الوقوع ضحية للاعتداءات الرقمية المتطورة. إن هذا التحول الرقمي الذي نعيشه يفرض علينا إعادة النظر في المفاهيم القانونية التقليدية والعمل على تطويرها لتواكب مقتضيات العصر، آمليين بصدق أن تكون هذه الدراسة المتواضعة لبنة أكاديمية بسيطة تساهم في إثراء النقاش القانوني حول هذا الموضوع الحيوي والحساس،

وتفتح آفاقاً واسعة وبحثة جديدة أمام الباحثين والدارسين لمواكبة ما سيفرزّه الذكاء الاصطناعي والثورات التكنولوجية القادمة من تحديات قانونية وأخلاقية وقضائية جديدة في عالم المال والأعمال، بما يضمن تحقيق الأمان الرقمي الشامل وتكريس دولة الحق والقانون في الفضاء الافتراضي..

قائمة المصادر و المراجع

قائمة المصادر والمراجع

أولاً: قائمة المصادر

1. الاتفاقيات:

* قانون اليونيسترال النموذجي بشأن التحويلات الدولية، 1992.

2. القوانين الوطنية:

* الأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

* الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

* القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

* القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 84، الصادرة بتاريخ 24 ديسمبر 2006.

* القانون رقم 09-03، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية، رقم 15، الصادرة بتاريخ 08 مارس 2009.

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

* القانون رقم 08-09، المتضمن قانون إجراءات مدنية وإدارية.

* القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28، الصادرة بتاريخ 16 ماي 2018.

* القانون رقم 18-07، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادرة بتاريخ 10 جوان 2018.

* القانون رقم 23-09، المؤرخ في 21 جوان 2023، المتعلق بالنقد والمصرفية، الجريدة الرسمية، العدد 43، الصادرة بتاريخ 09 جويلية 2023.

* الأمر رقم 66-155، المؤرخ في 08 جوان 1966، المتضمن قانون إجراءات جزائية، المعدل والمتمم، الجريدة الرسمية، العدد 48، الصادرة بتاريخ 10 جوان 1966.

3. القوانين الأجنبية:

* النقدي والمالي الفرنسي.

ثانياً: قائمة المراجع

1. الكتب:

أ. الكتب العامة:

* سليمان مرقس، الوافي في شرح القانون المدني (الفعل الضار والمسؤولية المدنية)، المجلد 02، 1988.

* عبد الرزاق السنهوري، الوسيط في شرح القانون المدني (نظرية الالتزام بوجه عام - مصادر الالتزام)، الجزء الأول، دار إحياء التراث العربي، بيروت.

* محمود نجيب حسني، شرح قانون العقوبات - القسم العام، الطبعة 06، دار النهضة العربية، القاهرة، 1989.

* فتوح عبد الله الشاذلي، قانون العقوبات - القسم العام (الجريمة والمسؤولية الجنائية)، دار المطبوعات الجامعية، الإسكندرية، 2001.

ب. الكتب المتخصصة:

* أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، دار هومة، الجزائر، الطبعة 15، 2018.

* أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الطبعة السادسة، دار هومة، الجزائر، 2009.

* أحسن بوسقيعة، قانون العقوبات الخاص (الجرائم الرقمية)، الطبعة 08، دار هومة، الجزائر، 2022.

* عبد الصمد حوالف، النظام القانوني لوسائل الدفع في الجزائر: دراسة مقارنة، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2017.

* طارق محمد حمزة، النقود الإلكترونية كإحدى وسائل الدفع (تنظيمها القانوني والمسائل الناشئة عن استعمالها)، الطبعة 1، منشورات زين الحقوقية، بيروت، 2011.

* عطية سالم، بطاقات الدفع الإلكترونية وأهميتها في عصرنا الحديث، منشورات معهد الدراسات المصرفية، القاهرة، 1998.

* ذكري عبد الرزاق محمد، النظام القانوني للبنوك الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2010.

* كوثر سعيد عدنان خالد، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2012.

* جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992.

* خالد ممدوح إبراهيم، جرائم نظام الدفع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

* طارق إبراهيم الدسوقي، ثورة المعلومات والجريمة المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011.

* مدحت رمضان، جرائم الاعتداء على الأشخاص والأموال في تكنولوجيا المعلومات، دار النهضة العربية، القاهرة، 2000.

* محمد الأمين بن خدة، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2012.

* نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، دار النهضة العربية، دون طبعة، القاهرة، 1994.

* هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، القاهرة، 1992.

* هلالى عبد الله أحمد، جرائم الكمبيوتر والإنترنت، دار النهضة العربية، القاهرة، 2011.

* ممدوح عبد الحميد عبد المطلب، الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2001.

* محمد محمود محمد جبران، النظام القانوني للتوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2004.

* عبد الله أوهائية، شرح قانون العقوبات الجزائري (القسم الخاص)، دار هومة، الجزائر، 2012.

* عبد الله أوهائية، شرح قانون الإجراءات الجزائية الجزائري (التحري والمتابعة)، دار هومة، الجزائر، 2010.

* علي جمال الدين عوض، العمليات المصرفية من الناحية القانونية، دار النهضة العربية، القاهرة، 1989.

* خالد ممدوح إبراهيم، حماية المستهلك في التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2007.

* جلال علي العدو، المسؤولية المدنية عن الأخطاء المهنية في بيئة المعلوماتية، دار النهضة العربية، القاهرة، 2004.

* محمد بودالي، حماية المستهلك في القانون المقارن (دراسة مقارنة مع القانون الفرنسي)، الطبعة 01، دار الفجر للنشر والتوزيع، القاهرة، 2006.

* نزيه نعيم شلالا، التكنولوجيا القانونية (القانون والقضاء في عالم المعلوماتية)، الطبعة 01، منشورات الحلبي الحقوقية، بيروت، لبنان، 2004.

* نبيل إبراهيم سعد، الالتزام بالإعلام في عقود استهلاك الخدمات المصرفية، دار الجامعة الجديدة، الإسكندرية، 2004.

* إسحق إبراهيم منصور، دراسات في المسؤولية الطبية والقضائية، الطبعة 01، دار المطبوعات الجامعية، الإسكندرية، 2002.

* فريدة بن يونس، الوساطة كآلية بديلة لتسوية المنازعات في القانون الجزائري، دار هومة للنشر والتوزيع، الجزائر، 2011.

* عبد الفتاح بيومي حجازي، نحو قانون عالمي للتجارة الإلكترونية، الطبعة 01، دار الفكر الجامعي، الإسكندرية، 2002.

* عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الطبعة 01، دار الفكر الجامعي، الإسكندرية، 2002.

* عمر سعد الله، قانون التحكيم التجاري الدولي (دراسة مقارنة)، الطبعة 02، دار المطبوعات الجامعية، الإسكندرية، 2005.

* بن الشيخ أمال، الجوانب الموضوعية والإجرائية للجريمة المعلوماتية في التشريع الجزائري، دار الجامعة الجديدة، الجزائر، 2021.

* خالد ممدوح إبراهيم، أمن وحماية المعاملات الإلكترونية، الطبعة 02، دار المطبوعات الجامعية، الإسكندرية، 2010.

* محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، الطبعة 01، دار المطبوعات الجامعية، الإسكندرية، 2003.

2. الأطروحات والمذكرات:

أ. رسائل الماجستير:

* شمة جاسم سيف الدين السليطي، الجوانب القانونية لوسائل الدفع الإلكترونية، مذكرة ماجستير، كلية القانون، جامعة قطر، 2021.

ب. مذكرات الماستر:

* غلام بونفلة، عيدة موالكية، واقع وسائل الدفع الإلكتروني في الجزائر، مذكرة ماستر، جامعة قلمة، 2021.

* محمد عبد الله بوكار، محمد سلامة، حماية المستهلك الإلكتروني، مذكرة لنيل شهادة الماستر، تخصص قانون أعمال، جامعة أدرار، 2017/2018.

* زكرياء دقيوق ومحمد ليامين، الآليات القانونية للدفع الإلكتروني في القانون الجزائري، مذكرة لنيل شهادة ماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد ابن باديس، مستغانم، 2023/2022.

* جمال أوجاني، النظام القانوني لبطاقة الإئتمان، مذكرة لنيل شهادة الماستر، تخصص قانون أعمال، جامعة قالمة، 2015/2016.

* بوزيدي مريم، الآليات القانونية لحماية المستهلك عبر الإنترنت، مذكرة لنيل شهادة الماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة سعيدة، 2024.

* حليلة بن شعاعة، الحماية الجزائية للمستهلك في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2013.

* داود مسعود، دور التحكيم الإلكتروني في تسوية منازعات التجارة الدولية، مذكرة ماستر، جامعة ورقلة، 2014.

* آية صويلح و سناء حمود، تسوية منازعات العمليات المصرفية الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، 2024.

3. المجالات والدوريات:

* سيف الدين رخالي، "مخاطر الدفع الإلكتروني على المستهلك الإلكتروني"، مجلة البحوث والدراسات القانونية والسياسية، جامعة بومرداس، المجلد 02، العدد 11، 2021.

* سعاد يحياوي، ربيعة خلافي، "التجربة الجزائرية لحماية المستهلك في مواجهة المخاطر المتعلقة بوسائل الدفع الإلكتروني"، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، جامعة معسكر، المجلد 06، العدد 02، 2022.

* آمنة نويوي، "الحماية الجنائية للمستهلك من جريمة سرقة الهوية الرقمية"، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد 26، العدد 04، 2022.

* طاهري حسين، "الحماية الجنائية للتجارة الإلكترونية في القانون الجزائري"، مجلة المفكر، جامعة بسكرة، العدد 04، 2009.

* ياسر محمد اللمعي، "المسؤولية الجنائية والمدنية في جرائم الدفع الإلكتروني" / "انعكاسات السياسة التشريعية المعاصرة على الحماية الجنائية للمستهلك الإلكتروني (دراسة تحليلية مقارنة)"، مجلة روح القوانين، كلية الحقوق جامعة طنطا، مصر، العدد 103، الجزء الأول، يوليو 2023.

فهرس المحتويات

العناوين	الصفحات
شكر و تقدير	
اهداء	
قائمة المختصرات	
مقدمة	02
الفصل الاول: التكيف الجنائي لجرائم الدفع الالكتروني	06
المبحث الاول: ماهية نظام الدفع الإلكتروني وتصنيف الجرائم المرتبطة به.....	07
المطلب الاول: المفهوم القانوني للدفع الإلكتروني وأطراف العلاقة.....	07
الفرع الاول :تحديد مفهوم الدفع الإلكتروني وخصائصه.....	08
أولاً: التعريف الفقهي والتشريعي للدفع الإلكتروني.....	08
ثانياً: العناصر الأساسية لعملية الدفع الرقمي.....	10
ثالثاً: أنواع أدوات الدفع الإلكتروني (البطاقات، المحافظ، التحويلات).....	11
رابعاً: الخصائص القانونية المميزة لعملية الدفع الإلكتروني.....	13
الفرع الثاني: تحليل أطراف العلاقة القانوني.....	14
أولاً: المركز القانوني للمستهلك (الطرف الضعيف).....	15

17	ثانياً: التزامات البنوك ومقدمي خدمات الدفع.....
17	ثالثاً: دور التاجر الإلكتروني في عملية الدفع.....
19	رابعاً: التمييز بين الجريمة الإلكترونية والجرائم التقليدية المشابهة.....
21	المطلب الثاني: التصنيف القانوني لأبرز جرائم الدفع الإلكتروني.....
21	الفرع الاول: الجرائم الواقعة على البيانات والأنظمة المعلوماتية للدفع.....
22	أولاً: جريمة التصيد الإلكتروني وسرقة الهوية المالية.....
24	ثانياً: جريمة اعتراض البيانات والتنصت الإلكتروني.....
26	ثالثاً: جريمة تزوير وتزييف وسائل الدفع الإلكتروني.....
28	رابعاً: جرائم اختراق وتعطيل قواعد بيانات الأنظمة البنكية.....
29	الفرع الثاني: الجرائم الماسة بالمعاملات المالية الإلكترونية.....
30	أولاً: جريمة الاحتيال في المعاملات المالية وعدم تسليم السلع.....
32	ثانياً: جرائم الحرمان من الخدمة (DDoS) وأثرها على عمليات الدفع.....
33	رابعاً: جريمة الإكراه والتهديد الإلكتروني للحصول على بيانات الدفع.....
36	المبحث الثاني: البنيان القانوني للجريمة الرقمية وقواعد الإثبات الجنائي
37	المطلب الاول: الأركان العامة والخاصة للجرائم الماسة بالدفع الإلكتروني.....
37	الفرع الاول: الركن المادي للجريمة الرقمية وعلاقة السببية.....

38	أولاً: الأفعال المكونة للاعتداء على نظام الدفع أو بياناته.....
38	ثانياً: النتيجة الإجرامية في جرائم الدفع الإلكتروني.....
40	ثالثاً: علاقة السببية وإشكالية الإثبات التقني.....
41	رابعاً: صور الشروع في اعتداءات الدفع الرقمي.....
42	الفرع الثاني: الركن المعنوي والاختصاص القضائي.....
44	أولاً: القصد الجنائي العام في الجرائم الإلكترونية.....
44	ثانياً: القصد الجنائي الخاص ونية الاستيلاء.....
45	ثالثاً: مكان وقوع الجريمة في الفضاء السيبراني.....
46	رابعاً: تحديد القانون الواجب التطبيق.....
47	المطلب الثاني: آليات إثبات الجريمة الإلكترونية وتحديد المسؤولية الجنائية.....
49	الفرع الأول: الطبيعة الخاصة للدليل الإلكتروني وحجيته في الإثبات.....
50	أولاً: مفهوم الدليل الرقمي وأنواعه (السجلات، البصمات).....
52	ثانياً: شروط قبول وحجية الدليل الإلكتروني في الإثبات.....
54	ثالثاً: سلامة سلسلة حفظ الدليل الرقمي وعدم التلاعب به.....
55	رابعاً: دور الخبرة الفنية في كشف الجريمة وضبط الأثر الرقمي.....
56	الفرع الثاني: تحديد مسؤولية الفاعل والمساهمين والشخص المعنوي.....

57	أولاً: تحديد مسؤولية الفاعل والمساهمين في جرائم الدفع الإلكتروني.....
58	ثانياً: مسؤولية البنك والوسطاء التقنيين في وقوع الضرر الإلكتروني.....
60	ثالثاً: المسؤولية الجنائية للشخص المعنوي في جرائم الدفع الإلكتروني.....
61	رابعاً: إجراءات التحري والتحقيق في جرائم الدفع الإلكتروني.....
62	خلاصة الفصل
63	الفصل الثاني: المسؤولية القانونية وآليات حماية المستهلك في الدفع الرقمي ...
65	المبحث الأول: النظام القانوني لمساءلة الأطراف عن أضرار الدفع الإلكتروني.....
65	المطلب الاول :الأساس القانوني للمسؤولية الجزائية في جرائم الدفع الإلكتروني.....
66	الفرع الاول : المرتكزات الموضوعية والإجرائية للملاحقة الجزائية.....
66	أولاً: التكييف القانوني للجرائم المعلوماتية.....
68	ثانياً: دور النيابة العامة في تحريك الدعوى وحماية أموال المستهلك.....
70	ثالثاً: العقوبات الأصلية والتدابير الاحترازية (الردع الخاص).....
71	رابعاً: ملائمة العقوبات لديناميكية الإجرام المعلوماتي.....
73	الفرع الثاني : تحديد المسؤولية الجنائية والمدنية.....
73	أولاً: المسؤولية الجزائية للشخص المعنوي (المؤسسات المالية).....
79	ثانياً: الإخلال بالتزام الأمان والسرية كمرتكز للمسؤولية العقدية.....

79	ثالثاً: أركان المسؤولية التقصيرية في غياب الرابطة التعاقدية المباشرة.....
80	رابعاً: حالة القوة القاهرة أو الخطأ الأجنبي ودورها في المسؤولية.....
81	المطلب الثاني: ضوابط التعويض وتوزيع الأعباء بين الأطراف.....
83	الفرع الأول: شروط وضوابط المطالبة بالتعويض.....
84	أولاً: إثبات الضرر المباشر المتولد عن الجريمة.....
85	ثانياً: تقدير التعويض المالي المناسب (الخسارة الفعلية والكسب الفائت).....
86	ثالثاً: التعويض عن الأضرار المعنوية الناتجة عن اختراق البيانات.....
87	رابعاً: شروط التعويض في ضوء التشريع الوطني.....
89	الفرع الثاني: توزيع الأعباء والمسؤولية عن فعل الغير.....
90	أولاً: مسألة تحمل المستهلك لجزء من الخسارة (الخطأ المشترك).....
91	ثانياً: مسؤولية البنك عن خطأ موظفيه أو وكلائه.....
91	ثالثاً: مسؤولية التاجر عن أمن منصته الرقمية.....
92	رابعاً: تحديد المسؤولية عن فعل الغير (التابعين والمقاولين الفرعيين).....
93	المبحث الثاني: لقواعد الوقائية والتسوية القضائية لمنازعات الدفع.....
94	المطلب الأول: الدور الوقائي للتشريعات والرقابة في مكافحة الجرائم.....
95	الفرع الأول: القواعد القانونية المنظمة لضمان سلامة المعاملات.....

96	أولاً: دور قانون مكافحة الجريمة الإلكترونية (الردع العام).....
96	ثانياً: دور قانون حماية المستهلك في البيئة الرقمية.....
97	ثالثاً: دور التشريع المصرفي والتعليمات الرقابية.....
99	رابعاً: دور المعايير الدولية والجهود المقارنة (GDPR, PCI DSS).....
100	الفرع الثاني: دور المصارف ومقدمي الخدمات في تحقيق الحماية.....
101	أولاً: الالتزامات القانونية لمقدمي الخدمة تجاه المستهلك.....
102	ثانياً: الالتزام ببذل عناية خاصة في حماية الأموال والبيانات.....
102	ثالثاً: الآليات الفنية لتعزيز أمن المعاملات (التشفير والمصادقة MFA).....
103	المطلب الثاني: آليات التسوية القضائية والبديلة.....
105	الفرع الأول: الحماية القضائية عبر رفع الدعاوى.....
106	أولاً: إجراءات رفع الدعوى المدنية للمطالبة بالتعويض.....
107	ثانياً: استخدام الدعوى الجنائية كأداة ضغط للحصول على الحقوق.....
107	ثالثاً: دور الدعوى الجزائية في خدمة الحق المدني للمستهلك.....
106	رابعاً: الإشكالات الإجرائية في تنفيذ الأحكام القضائية ضد الجناة.....
107	الفرع الثاني: التسوية الودية للمنازعات والتوصيات المستقبلية.....
107	أولاً: دور لجان التحكيم والوساطة المتخصصة.....

108	ثانياً دور هيئات حماية المستهلك ومكاتب الشكاوى المصرفية.....
110	ثالثاً: التوصيات لتعزيز الحماية القانونية للمستهلك مستقبلاً.....
111	رابعاً: الدعوة لإنشاء هيئة متخصصة لفض منازعات الدفع الإلكتروني.....
112	خلاصة الفصل.....
114	خاتمة.....
118	قائمة المصادر و المراجع.....

ملخص الدراسة

تناولت هذه الدراسة موضوع الحماية القانونية للمستهلك في ظل نظام الدفع الإلكتروني، وذلك بهدف تسليط الضوء على الآليات التشريعية التي أقرها المشرع الجزائري لمواجهة المخاطر الجنائية والمدنية المرتبطة بالرقمنة المالية. وقد تم التركيز في القسم الأول على التكييف الجنائي للجرائم المعلوماتية المستحدثة وخصوصية الدليل الرقمي في إثباتها، بينما عالج القسم الثاني قواعد المسؤولية المدنية والآليات الوقائية الكفيلة بحماية المستهلك وجبر أضراره. وقد خلصت الدراسة إلى ضرورة تحديث المنظومة القانونية بما يتماشى مع تسارع التقنيات الرقمية، وتعزيز نظام المسؤولية الموضوعية للمؤسسات المصرفية لضمان أمن وحقوق المستهلك الإلكتروني.

الكلمات المفتاحية: حماية المستهلك، الدفع الإلكتروني، الجريمة المعلوماتية، المسؤولية الموضوعية، الدليل الرقمي.

Abstract

This study examines the legal protection of consumers within the electronic payment system, aiming to highlight the legislative mechanisms established by Algerian law to address the criminal and civil risks associated with financial digitalization. The first part focuses on the legal characterization of emerging cybercrimes and the specificity of digital evidence in criminal proceedings. The second part explores the rules of civil liability and the preventive mechanisms designed to protect consumers and ensure compensation for damages. The study concludes that it is essential to modernize the legal framework to keep pace with rapid digital advancements and to strengthen the objective liability of banking institutions to ensure the security and rights of electronic consumers.

Keywords: Consumer Protection, Electronic Payment, Cybercrime, Objective Liability, Digital Evidence