

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

المرجع:

قسم: قانون الخاص

مذكرة نهاية الدراسة لنيل شهادة ماستر

الجرائم الإلكترونية الموجهة ضد المؤسسات المالية

التخصص: قانون قضائي

الشعبة: الحقوق

تحت اشراف الأستاذ (ة):

من إعداد الطالب (ة) :

برابح هدى

البريشي نورة

أعضاء لجنة المناقشة

الأستاذ (ة) مهدي نوال رئيسا

الأستاذ (ة) برابح هدى مشرفا مقرر

الأستاذ (ة) مرابط حبيبة مناقشا

السنة الجامعية 2026/2025

نوقشت في: 2026/06 /18

كلية الحقوق والعلوم السياسية

مصلحة الترقيات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية في إنجاز البحث

أنا الممضي أدناه , الطالب (ة) :

اللقب : البريشي

الإسم : بن خورقة

الحامل (ة) لبطاقة التعريف الوطنية رقم : 1.5557.01 ولها والصادرة بتاريخ : 2026/01/27

المسجل (ة) بكلية : الحقوق والعلوم السياسية قسم : القانون الخاص

والمكلف (ة) بإنجاز مذكرة ماستر بعنوان :

الجرائم الإلكترونية كوسيلة من الوسائل المالية

أصرح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية
المطلوبة في إنجاز البحث المذكور أعلاه

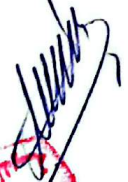
نظرا لشرفية الإعضاء

إمضاء المعني





التاريخ :



* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ وَقُلْ أَعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَى
عِلْمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُمْ بِمَا كُنْتُمْ تَعْمَلُونَ ﴾ ﴿١٠٥﴾

إهداء

إلى من كان لهم الفضل بعد الله في بلوغ هذه اللحظة، وإلى من شكّلوا سنداً لا يميل في دربي،
أهدي هذا العمل المتواضع.

إلى أبي...

ذلك الجبل الذي لا تهزه العواصف، والظل الذي احتमित به في كل تعب، والنور الذي علّمني
أن الكرامة تُبنى بالصبر والعمل. شكراً لأنك كنت دائماً القوة حين أضعف، والحكمة حين
أرتبك، والدعاء الذي لا ينقطع.

إلى أمي...

النبض الذي لا يهدأ، والقلب الذي يسبق قلبي رحمة وحناناً، والعطاء الذي لا ينتظر مقابلاً.
أنتِ الحكاية الأجل في عمري، وأنتِ المعنى الحقيقي للأمان حين تضيق الدنيا.

إلى إخوتي أمينة، وصابرين، وسارة، وملاك، وأخي عبد الرؤوف...

إلى من شاركوني الضحك قبل النجاح، ووقفوا معي في لحظات الضعف قبل الفرح، وساندوني
بصمتهم أحياناً وبكلماتهم أحياناً أخرى. أنتم الروح التي تجعل الطريق أخفّ، والبيت أكثر دفئاً،
والحياة أجمل.

إلى عائلتي الكبيرة...

الامتداد الذي أفخر به، والجذور التي تمنحني الثبات مهما تغيرت الطرق. أنتم الحضور الذي
لا يغيب، والسند الذي لا يُنسى.

إلى أصدقائي...

إلى من جعلوا للحياة طعماً آخر، وشاركوا اللحظات الصغيرة قبل الكبيرة، وكانوا رفقة صادقة لا
تتبدل مع الأيام. بكم تُصبح الأيام أبسط، وبوجودكم تُصبح الذكريات أجمل.

شكر وتقدير

في البداية، أتوجه بخالص الشكر والحمد لله عز وجل الذي وفقني وأعاني على إنجاز هذا العمل، وأمدني بالصبر والإرادة لتجاوز الصعوبات التي واجهتني خلال مسار البحث، فله الحمد والشكر على نعمه التي لا تُعد ولا تُحصى.

كما أتقدم بجزيل الشكر والعرفان إلى أستاذتي المشرفة، التي لم تبخل عليّ بتوجيهاتها العلمية القيمة ونصائحها الدقيقة طيلة فترة إعداد هذا البحث، فكانت نعم الموجهة والمرشدة التي ساعدتني على تصويب الأفكار وتنظيمها، وإثراء هذا العمل بما يلزم من ملاحظات وإضافات علمية ساهمت في تحسينه وإخراجه في صورة أكاديمية لائقة، لقد كانت متابعة أستاذتي المستمرة ودعمها المعنوي والعلمي دافعا كبيرا لي للاستمرار والإصرار على إتمام هذا البحث. فإليها أرفع أسمى عبارات الاحترام والتقدير، سائلة الله أن يجزيها خير الجزاء، وأن يبارك في علمها وعملها، وأن يجعل ما قدمته لي في ميزان حسناتها.

كما أتقدم بالشكر إلى لجنة المناقشة على تخصيصهم من وقتهم لقراءة المذكرة ومناقشتها.

مقدمة

أدى التطور التكنولوجي المتسارع الذي شهده العالم خلال العقود الأخيرة إلى إحداث تحولات عميقة في مختلف المجالات الاقتصادية والمالية، حيث أصبحت المؤسسات المالية تعتمد بشكل متزايد على الأنظمة المعلوماتية والشبكات الإلكترونية في تسيير معاملاتها وتقديم خدماتها، الأمر الذي ساهم في تسهيل العمليات البنكية والمالية وتسريعها وتحقيق قدر كبير من الدقة والفعالية. غير أن هذا التطور، وعلى الرغم من مزاياه العديدة، أفرز في المقابل أنماطا جديدة من الإجرام عرفت بالجرائم الإلكترونية، والتي اتخذت من الفضاء الرقمي وسيلة لارتكاب أفعال غير مشروعة تستهدف البيانات والأنظمة المعلوماتية ذات الطبيعة الحساسة.

المؤسسات المالية من أكثر الهيئات عرضة لهذا النوع من الجرائم، بالنظر إلى ما تتعامل به من أموال ومعطيات مصرفية ومالية ذات قيمة كبيرة، وهو ما جعلها هدفا مباشرا للهجمات الإلكترونية التي تتنوع صورها بين الاختراق غير المشروع للأنظمة، وتعطيل الخدمات المالية، وسرقة البيانات البنكية، والاحتيال الإلكتروني، وتحويل الأموال بطرق غير مشروعة، فضلا عن تزوير المعطيات المالية واستغلال الثغرات التقنية لتحقيق مكاسب غير قانونية¹، وقد ساهم الطابع العابر للحدود الذي تتميز به الجرائم الإلكترونية في زيادة خطورتها وتعقيدها، مما جعل مكافحتها تتطلب آليات قانونية وتقنية متطورة تتلاءم مع طبيعتها المستحدثة.

دفع اتساع نطاق هذه الجرائم بالمشروع الجزائري إلى التدخل من خلال وضع ترسانة قانونية تهدف إلى حماية الأنظمة المعلوماتية والمؤسسات المالية من مختلف الاعتداءات الإلكترونية، وذلك عبر تعديل قانون العقوبات وإدراج نصوص خاصة تجرم الأفعال المرتبطة بالمساس بأنظمة المعالجة الآلية للمعطيات، إضافة إلى استحداث قواعد قانونية تنظم المعاملات الإلكترونية وتعترف بالمحرمات والتوقيعات الإلكترونية كوسائل قانونية معتمدة في

¹ بلحاج محمد، "الجرائم المعلوماتية في التشريع الجزائري وسبل مكافحتها"، مجلة الدراسات القانونية والسياسية، جامعة تلمسان، العدد 8، 2021، ص 45.

المجال المالي،¹ كما عملت الدولة على تعزيز آليات الوقاية والحماية الجزائية لمواجهة التهديدات السيبرانية التي أصبحت تشكل خطرا حقيقيا على استقرار النظام المالي والثقة في المعاملات الإلكترونية.

تكتسي دراسة الجرائم الإلكترونية الموجهة ضد المؤسسات المالية أهمية بالغة، سواء من الناحية النظرية أو العملية، بالنظر إلى ارتباطها الوثيق بحماية الاقتصاد الوطني وضمان أمن المعاملات المالية الإلكترونية. فمن الناحية النظرية، تسهم هذه الدراسة في توضيح المفاهيم القانونية المرتبطة بالجرائم الإلكترونية وإبراز خصائصها وتمييزها عن غيرها من الجرائم المعلوماتية، إضافة إلى تحليل الإطار القانوني المنظم لها في التشريع الجزائري. أما من الناحية العملية، فتبرز أهمية الموضوع في محاولة الوقوف على أهم صور الاعتداءات الإلكترونية التي تستهدف المؤسسات المالية، وبيان مدى فعالية الحماية الجزائية وآليات الوقاية والإثبات في الحد من هذه الجرائم ومكافحتها.

يرجع اختيار موضوع الجرائم الإلكترونية الموجهة ضد المؤسسات المالية إلى جملة من الأسباب العلمية والعملية، لعل أبرزها الانتشار المتزايد لهذا النوع من الجرائم في ظل التطور التكنولوجي والتحول الرقمي الذي مست آثاره مختلف القطاعات، خاصة القطاع المالي الذي أصبح يعتمد بصورة كبيرة على الأنظمة الإلكترونية في تسيير معاملاته وخدماته، ومن بين الدوافع التي شجعت على اختيار هذا الموضوع كذلك، الرغبة في تسليط الضوء على الإطار القانوني الذي اعتمده المشرع الجزائري لمواجهة الجرائم الإلكترونية، ومدى كفايته في حماية المؤسسات المالية من مختلف الاعتداءات الرقمية، خاصة مع التطور المستمر لأساليب الإجرام الإلكتروني وصعوبة اكتشاف مرتكبيه وإثبات أفعالهم.

¹ القانون رقم 24-06 المؤرخ في 19 شوال 1445 هـ الموافق لـ 28 أفريل 2024، الجريدة الرسمية، العدد 40، 2024.

تهدف هذه الدراسة إلى بيان ماهية الجرائم الإلكترونية الموجهة ضد المؤسسات المالية وتحديد أهم صورها وخصائصها، مع إبراز الإطار القانوني المنظم لها في التشريع الجزائري، كما تسعى إلى توضيح مدى فعالية الحماية الجزائية المقررة للمؤسسات المالية في مواجهة هذه الجرائم، وتحليل مختلف آليات الوقاية والإثبات المعتمدة للحد من مخاطرها.

ومن هذا المنطلق نطرح الإشكالية التالية:

كيف عالج المشرع الجزائري الجرائم الإلكترونية الموجهة ضد المؤسسات المالية، وما مدى فعالية الحماية الجزائية وآليات الوقاية والإثبات في مواجهة هذا النوع من الجرائم؟

اعتمدت في هذه الدراسة على المنهج الوصفي التحليلي، باعتباره الأنسب لموضوع الجرائم الإلكترونية الموجهة ضد المؤسسات المالية، وذلك من خلال وصف مختلف المفاهيم المرتبطة بالجرائم الإلكترونية والمؤسسات المالية، وتحليل النصوص القانونية المنظمة لها في التشريع الجزائري.

للإجابة على هذا التساؤل جاءت هذه الدراسة لمعالجة مختلف الجوانب المتعلقة بالجرائم الإلكترونية الموجهة ضد المؤسسات المالية، من خلال التطرق في **الفصل الأول** إلى الإطار المفاهيمي والقانوني للجرائم الإلكترونية والمؤسسات المالية، ثم دراسة التنظيم القانوني لهذه الجرائم والمستند الإلكتروني كوسيلة قانونية في المعاملات المالية. أما **الفصل الثاني** فقد خصص لبيان صور الجرائم الإلكترونية الماسة بالمؤسسات المالية، مع إبراز الحماية الجزائية وآليات الوقاية والإثبات المعتمدة لمواجهة هذا النوع من الجرائم.



الفصل الأول: الإطار المفاهيمي والقانوني

للجرائم الإلكترونية



مع التوسع الكبير في استخدام التقنيات الرقمية في الحياة اليومية والأنشطة الاقتصادية، برزت الحاجة إلى دراسة الجرائم الإلكترونية وتأثيرها على المعاملات المالية والمؤسسات الاقتصادية، فقد أتاح التحول الرقمي فرصًا كبيرة لتطوير النظام المالي، لكنه في المقابل خلق ثغرات قد يستغلها البعض لارتكاب جرائم تستهدف الأفراد أو المؤسسات المالية، مما يستوجب وضع أطر قانونية تحمي المعاملات وتضمن استمراريتها.

لقد تناول هذا الفصل مبحثين، المبحث الأول: الإطار المفاهيمي للجرائم الإلكترونية والمؤسسات المالية ويتضمن المطلب الأول مفهوم الجرائم الإلكترونية وخصائصها وتمييزها عن الجرائم المعلوماتية والمطلب الثاني مفهوم المؤسسات المالية وأنواعها ودورها في النظام المالي، أما المبحث الثاني الإطار القانوني للجرائم الإلكترونية في المجال المالي ويتضمن المطلب الأول التنظيم القانوني للجرائم الإلكترونية في التشريع الجزائري والمطلب الثاني المستند الإلكتروني والتوقيع الإلكتروني كوسائل قانونية في المعاملات المالية.

المبحث الأول: الإطار المفاهيمي للجرائم الإلكترونية والمؤسسات المالية

الجرائم الإلكترونية تمثل أحد الظواهر الحديثة التي ظهرت مع تطور تكنولوجيا المعلومات والاتصالات، وهي تؤثر على جميع القطاعات بما فيها النظام المالي، بينما تلعب المؤسسات المالية دورا مهما في تسيير الموارد الاقتصادية وتسهيل المعاملات.

حيث يتناول هذا المبحث مطلبين: يشمل المطلب الأول مفهوم الجرائم الإلكترونية وخصائصها وتمييزها عن الجرائم المعلوماتية، والمطلب الثاني مفهوم المؤسسات المالية وأنواعها ودورها في النظام المالي.

المطلب الأول: ماهية الجرائم الإلكترونية

أفرز التطور التكنولوجي وانتشار استخدام شبكة الإنترنت نوعاً جديداً من الجرائم يعرف بالجرائم الإلكترونية، والتي أصبحت تشكل خطراً متزايداً على الأفراد والمؤسسات. ولإحاطة بهذا النوع من الجرائم، لا بد من التعرف على مفهومها وخصائصها وأهم صورها.

الفرع الأول: مفهوم الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من الظواهر الحديثة نظرا لارتباطها بتقنية متطورة هي تكنولوجيا المعلومات والاتصالات، مما صعب من وضع تعريف جامع لها، لذا بذل الفقهاء جهودا مضنية في محاولتهم وضع تعريف لها، وأن وضع تعريف قد يضيق من نطاقها وقد يطرح إشكالية التماثل أو الاختلاف بين الجريمة الإلكترونية والجريمة المعلوماتية.¹ حيث برز اتجاهان هما: الاتجاه الأول يعرف بالاتجاه الضيق في تعريفه للجرائم الإلكترونية، ويعرف الثاني بالاتجاه الموسع لها.

¹ د. غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، 2016م، ص 13.

أ-تعريف الفقه للجريمة الإلكترونية:

مما يلاحظ في هذا الشأن هو عدم وجود اتفاق سواء على المستوى التشريعي أو الفقهي على استعمال مصطلح معين للدلالة على هذه الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والإنترنت، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، فهناك من يطلق عليها مصطلح جرائم الغش المعلوماتي، أو الجرائم المعلوماتية، أو الجرائم الإلكترونية، أو جرائم الحاسب الآلي، أو جرائم تقنية المعلومات، أو الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو جرائم التكنولوجيا الحديثة، أو جرائم الكمبيوتر والإنترنت، ويرجع السبب في ذلك إلى عدة عوامل منها التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، مما نتج عنه جرائم مستحدثة اختلفت التشريعات حول وضع مفاهيم موحدة لها.¹ وقد يكون السبب أيضا ترك المجال أمام المشرع لاحتواء التقنيات المتلاحقة في هذا الميدان، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة قد تتبدل في المستقبل. ويثير هذا الإشكال العديد من التحديات أهمها صعوبة مواجهتها وتعذر إيجاد الحلول المناسبة.

ب-الاتجاه الضيق لمفهوم الجرائم الإلكترونية:

قام أنصار هذا الاتجاه بحصر مفهوم الجريمة الإلكترونية باستخدام معايير مختلفة، سواء كانت وفقا لمعيار شخصي يعتمد على المعرفة والخبرة التقنية، أو وفقا لمعيار الموضوع والمعايير المتعلقة بالبيئة التي تم فيها ارتكاب الجريمة.²

توجد العديد من التعريفات للجريمة الإلكترونية وفقا لهذا الاتجاه، فهي تعتبر أنها: "الفعل غير المشروع الذي يستخدم في ارتكابه الحاسب الآلي"³. كما ذهب اتجاه آخر إلى تعريفها

¹ Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader, Beyrouth, Liban, 2004, pp. 18.

² مقالاتي مونة مشري راضية، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، المجلد 6، العدد 01، 2021، ص 493.

بأنها: "فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"¹، في حين عُرفت أيضا بأنها: "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الإنترنت"².

كما اعتبرها بعض الفقه بأنها: "مجموعة المخالفات الجزائية التي تقع ضد شبكات الإعلام الآلي"³. وذهب تعريف آخر إلى اعتبارها: "الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والتي تمس بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كان الهدف من ذلك"⁴.

بينما عرفها الفقيه الألماني تيدمان (Tiedemann) بأنها: "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"⁵.

من خلال هذه التعريفات يتضح أن أنصار هذا الاتجاه يربطون الجريمة الإلكترونية بضرورة وجود الحاسوب، سواء باعتباره وسيلة لارتكاب الجريمة أو محلا لها. كما يفترض هذا الاتجاه توفر معرفة مسبقة بتقنيات الحاسوب لدى مرتكب الجريمة، بل وحتى لدى الجهات

³ عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الإلكترونية-دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية، ط1، القاهرة، مصر، 2012م، ص40.

¹ فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والإقتصادية، كلية الحقوق، جامعة عين شمس، مصر، السنة

الرابعة والأربعون، العدد 2، 2002م، ص 485.

² عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجات للطباعة والتجليد، ط1، مصر، 2009، ص 19.

³ Redouane Semlali, art-Cit,p.40, voir aussi, Frédérique Chopin, Les politiques publiques de lutte contre la cybercriminalité, Actualité Juridique Pénal, Editions Dalloz, 2009,p101.

⁴ Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader,Beyrouth,Liban,2004,pp.20.

⁵ عبد العال الديربي ومحمد صادق إسماعيل، المرجع نفسه، ص 41.

المكلفة بملاحقة هذا النوع من الجرائم¹، الأمر الذي يؤدي إلى تضيق نطاق مفهوم الجريمة الإلكترونية رغم اتساعها المستمر نتيجة التطور المتسارع لتكنولوجيا المعلومات.

إضافة إلى ذلك، فإن بعض الجرائم الإلكترونية لا تتطلب مستوى عالياً من المعرفة التقنية، خاصة بعد أن أصبحت وسائل التكنولوجيا في متناول الجميع، مثل إرسال الرسائل النصية عبر الهاتف أو البريد الإلكتروني أو نسخ البيانات من الحاسوب وغيرها من الأفعال المشابهة. كما أن حصر الجرائم الإلكترونية في الأفعال التي تقع فقط على النظام المعلوماتي يعد تضيقاً آخر، إذ يندرج ضمنه نوع محدد من الجرائم يعرف بجرائم المعالجة الآلية للمعطيات، في حين يتم استبعاد العديد من الأفعال غير المشروعة التي يستعمل فيها الحاسوب كوسيلة لارتكاب الجريمة، مثل جرائم الاحتيال المعلوماتي²، ولهذا فإن تعريف هذا الاتجاه للجريمة الإلكترونية يبقى قاصراً، وهو ما أدى إلى ظهور اتجاه فقهي آخر أكثر اتساعاً سنتناوله فيما يأتي.

ج-الاتجاه الموسع لمفهوم الجرائم الإلكترونية:

على خلاف الاتجاه السابق، يرى فريق من الفقهاء ضرورة التوسع في مفهوم الجرائم الإلكترونية أو المعلوماتية وعدم قصرها على الحاسوب فقط أو على موضوع الجريمة أو على شخص مستخدمه، بل ربطها بالتقنية ذاتها المستعملة في مختلف الأجهزة المعلوماتية والإلكترونية. وفي هذا الإطار عُرِفَت الجريمة الإلكترونية بأنها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية يترتب عنه ضرر بالمجني عليه أو منفعة يحققها الفاعل"³. كما عرّفَتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: "كل فعل أو امتناع من شأنه

¹ المرجع نفسه، ص 42.

² نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2005م، ص 30.

³ حنان ربحان مبارك المضحكي، الجرائم المعلوماتية -دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2014، ص 26.

الاعتداء على الأموال المادية أو المعنوية، ويكون ناتجا بصورة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".¹

تتسم هذه التعريفات بالانتساع، إذ تسمح بالإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، كما تعكس الطابع التقني المميز الذي تتطوي عليه أبرز صور هذه الجرائم، فضلا عن أنها تتيح إمكانية استيعاب التطورات التقنية المستقبلية². كما عرفها بعض الفقهاء بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"³، حيث يعتمد هذا التعريف على معيارين أساسيين، يتمثل الأول في وصف السلوك الإجرامي، أما الثاني فيتمثل في ارتباط هذا السلوك بعملية المعالجة الآلية للبيانات أو نقلها.

من ناحية أخرى، يتفق الفقه الفرنسي بصفة عامة على أن فكرة الغش المعلوماتي (Informatique Fraude) التي تقابل جرائم الحاسب الآلي تشمل عددا كبيرا من الأفعال المتنوعة، فقد عرف كل من الفقيه ميشال (Michel) والفقيه ريدو (Redo) الجريمة المعلوماتية بأنها: "سوء استخدام الحاسب، ويشمل ذلك الحالات المتعلقة بالدخول غير المصرح به إلى حاسب المجني عليه أو بياناته، وكذلك الاستعمال غير المشروع لبطاقات الائتمان، واختراق أنظمة الحاسب الآلي بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب، وسرقة الحاسب الآلي نفسه أو أي جزء من أجزائه"⁴.

كما عرفت المادة (01) من القانون العربي النموذجي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2003 الجرائم الإلكترونية بأنها: "كل فعل مؤثم يتم

¹ أحمد خليفة الملط، الجرائم المعلوماتية-دراسة مقارنة، دار الفكر الجامعي، ط2، الإسكندرية، مصر، 2006، ص 37.

² يونس عرب، جرائم الكمبيوتر و الإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، بحث منشور على

الموقع الآتي: <https://www.abhatoo.net.Ma>، اطلع عليه بتاريخ: 2026/02/28 على الساعة 22:24

³ نائلة عادل محمد فريد قورة، المرجع نفسه، ص30

⁴ حنان ربحان مبارك المضحكي، المرجع نفسه، ص 28.

ارتكابه عبر أي وسيط إلكتروني"، وعرفت المادة نفسها الوسيط الإلكتروني بأنه: "شبكة الحاسب الآلي أو الإنترنت أو أي شبكة إلكترونية أخرى"¹.

من خلال هذه التعريفات يتضح أن المفهوم الموسع للجرائم الإلكترونية يشمل كل جريمة تتم بواسطة الحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عبر شبكة الإنترنت أو أي وسيلة إلكترونية أخرى قد تظهر مستقبلا ضمن وسائل الاتصال الحديثة مثل الهاتف النقال أو جهاز الفاكس وغيرها.

لا شك أن هذا الاتجاه يتسم باتساع كبير في تحديد مفهوم الجرائم الإلكترونية، إذ يشمل كل جريمة تتم بمساعدة الحاسوب أو في محيطه أو عبر شبكة الإنترنت أو بواسطة أجهزة الاتصال الحديثة. وبناء على ذلك تتخذ الجريمة الإلكترونية صورا متعددة، فقد يتم استخدام الحاسوب كوسيلة لارتكاب الجريمة، أو قد يكون هو نفسه محلا للاعتداء، كما قد يتم ارتكاب الجريمة باستخدام أي وسيلة إلكترونية أخرى توفرها التقنيات الحديثة²، وبعبارة أخرى فإن الجرائم الإلكترونية تمثل تزاوجا بين تقنيات الحوسبة وتقنيات الاتصال الحديثة.

إذا نظرنا إلى نشأة وتطور تقنية المعلومات نجد أنها تقوم أساسا على فرعين متكاملين هما الحوسبة والاتصال، فالحوسبة تعتمد على استخدام الوسائل التقنية لإدارة البيانات وتنظيمها ومعالجتها في إطار تنفيذ مهام محددة ترتبط بعلمي الحساب والمنطق، أما الاتصال فيعتمد على وسائل تقنية تهدف إلى نقل المعلومات بمختلف أشكالها. وقد حدد الأستاذ زياينغ إكزيوو (Yuexiao Zhange) هذه المعلومات في صور متعددة مثل الرسائل والأخبار والبيانات

¹ د. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر، 2019م، ص 34.

² نائلة عادل محمد فريد قورة، المرجع نفسه، ص 34.

والمعرفة والوثائق والأدب والفكر والرموز والعلامات والإرشادات الخفية والأنباء المفيدة والسرية وغيرها¹.

يتضح أن تعريف منظمة التعاون الاقتصادي والتنمية يعد من أكثر التعريفات وضوحاً وشمولاً للأسباب الآتية:

أنه حدد ماهية السلوك الإجرامي للجريمة، حيث شمل الفعل الإيجابي وكذلك السلوك السلبي المتمثل في الامتناع.

اعتماده مفهوماً واسعاً يسمح بالإحاطة الشاملة بظاهرة الجرائم التقنية، وذلك من خلال ربط الجريمة بأي تدخل للتقنية المعلوماتية سواء كان بشكل مباشر أو غير مباشر، خاصة وأن هذه التقنية تعرف تطوراً مستمراً.

يعبر عن الطابع التقني المميز الذي تتسم به أبرز صور الجرائم الإلكترونية.

يتيح إمكانية مواكبة التطورات المستقبلية في مجال تكنولوجيا المعلومات ونظم الاتصال.

من خلال ما سبق يتبين أن اختلاف الفقه في تعريف الجريمة المعلوماتية أو الإلكترونية يرجع أساساً إلى اختلاف المعايير المعتمدة والزوايا التي ينظر من خلالها كل اتجاه إلى هذه الجريمة المستحدثة، ومع ذلك يمكن صياغة تعريف مختصر يجمع بين هذه الاتجاهات، وهو أن الجريمة الإلكترونية هي: "سلوك غير مشروع يعاقب عليه القانون صادر عن إرادة إجرامية يكون محله معطيات الكمبيوتر"²، فالسلوك هنا يشمل الفعل الإيجابي والامتناع، ويعد غير مشروع لأن المشروعية تنفي عن الفعل صفته الإجرامية، كما أنه معاقب عليه قانوناً لأن الصفة الإجرامية لا تتحقق في القانون الجنائي إلا بنص من المشرع. أما محل جريمة الكمبيوتر فهو معطيات الكمبيوتر بمفهومها الواسع مثل البيانات المدخلة والبيانات المعالجة والمخزنة

¹ يونس عرب، جرائم الكمبيوتر، المرجع نفسه، ص 2.

² د. يزيد بوحليط، المرجع نفسه، ص 41.

والبرامج بمختلف أنواعها والمعلومات المستخرجة أو المتبادلة بين الأنظمة المعلوماتية وغيرها، أما الكمبيوتر فهو النظام التقني الشامل الذي يجمع بين تقنيات الحوسبة والاتصال بما في ذلك شبكات المعلومات¹.

وعلى هذا الأساس فإن محاولة وضع تعريف دقيق لهذا النوع من الجرائم المستحدثة التي ترتكب في بيئة افتراضية يجب أن تراعي عددا من الاعتبارات أهمها:²

1- ضرورة أن يتلاءم التعريف مع الطابع العالمي للمعلومات والاتصالات وأن يكون واضحا على المستوى الدولي.

2- مراعاة التطورات المتلاحقة في مجال الحوسبة والاتصال بما يسمح باستيعاب مختلف الصور المستحدثة للجرائم الإلكترونية.

3- إبراز الخصوصية التي تتميز بها الجرائم الإلكترونية نظرا لتعدد أشكال السلوك الإجرامي فيها ووضوح الدور الذي يلعبه الحاسوب في ارتكابها.

د- التعريف القانوني للجريمة الإلكترونية:

قام المشرع الجزائري بتحديد مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، حيث اعتبر أنها تشمل الأفعال التي تمس بأنظمة المعالجة الآلية للبيانات المنصوص عليها في قانون العقوبات، إضافة إلى أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.³

¹ يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أبريل، 2006م، ص 7.

² نائلة عادل محمد فريد قورة، المرجع نفسه، ص 52.

³ بوضياف اسميان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 3، العدد 11، 2018، ص 351.

يتضح أن المشرع الجزائري جمع بين حالتين أساسيتين، الأولى عندما تكون الأنظمة المعلوماتية وشبكات الاتصال موضوعا للجريمة، والثانية عندما تكون وسيلة أو دعامه لارتكاب جرائم تقليدية.

كما يلاحظ أن هذه الجرائم اكتسبت صفتها المعلوماتية بسبب ارتباطها بالأنظمة المعلوماتية وشبكات الاتصال، إذ لولا وجود هذه الوسائل التكنولوجية لما اكتسبت تلك الأفعال هذا الطابع المعلوماتي، وعلى خلاف ذلك لم يقيم المشرع الفرنسي بتقديم تعريف صريح للجريمة الإلكترونية، بل اكتفى بتجريم الأفعال المرتبطة بالمساح بالأنظمة المعلوماتية دون وضع تعريف شامل لها.

قد أطلق المشرع الجزائري على هذا النوع من الجرائم تسمية "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، حيث عرفها بموجب المادة الثانية من القانون رقم 09-04 على أنها الجرائم المتمثلة في المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات، أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية¹.

الفرع الثاني: خصائص الجرائم الإلكترونية

تتميز الجريمة الإلكترونية بمجموعة من الخصائص التي لا تتوفر في الجرائم التقليدية، كما أن هناك خصائص تميز مرتكبيها عن المجرمين العاديين، وفيما يلي توضيح لهذه السمات:

أولاً: السمات الخاصة بالجريمة الإلكترونية

صعوبة اكتشاف الجريمة: تعتبر الجرائم الإلكترونية غالباً خفية ومستترة، إذ يستخدم الجاني أدوات تقنية متطورة مثل الفيروسات أو سرقة البيانات الخاصة أو إتلافها، مما يجعل من

¹ بوضياف اسميان، المرجع نفسه، ص 352.

الصعب تحديد مرتكبها ومعرفة أثر الجريمة، وهذا الأمر يزيد من تعقيد مهمة المحققين، إذ تتطلب مواجهة هذه الجرائم خبرة فنية عالية ومتخصصة لإثباتها¹.

عبور الحدود الزمنية والجغرافية: تتجاوز الجرائم الإلكترونية الحدود الجغرافية لأي دولة، ومع انتشار شبكة الإنترنت أصبح بإمكان أي شخص ارتكاب جريمة من أي مكان في العالم، حتى وإن كان الضحية في بلد آخر، هذا ما يجعل مسرح الجريمة عالمياً، حيث يمكن تنفيذها دون الحاجة للتواجد المادي للجاني قرب موقع ارتكابها².

جرائم هادئة: الجرائم الإلكترونية لا تحتاج إلى مجهود عضلي كالجرائم التقليدية، بل تعتمد على الدراسة الذهنية والتفكير العملي المدروس القائم على معرفة تقنية الكمبيوتر، وهذا ما يسمح للمجرمين بتنفيذ جرائمهم بشكل متطور ومتسمس، فالجرائم الإلكترونية تعتمد على تعديل والتلاعب بالبيانات المخزنة في ذاكرة الحواسيب، وبالتالي يمكن للمجرمين تغيير أو حذف المعطيات أو البيانات مع التستر على أنشطتهم الإلكترونية³.

جرائم صعبة الإثبات: من الصعب إثبات الجريمة الإلكترونية، حيث يصعب تتبعها أو اكتشافها، إذ لا تترك أثراً مادياً كالتي تستخدم عادة في التحقيقات التقليدية، كما يتطلب تتبع الجرائم الإلكترونية خبرة فنية متخصصة، فالمحقق العادي قد يواجه صعوبة في التعامل مع هذه الجرائم، بالإضافة إلى أن مرتكبي الجرائم الإلكترونية يقومون بتضليل أنشطتهم وإخفاء الأدلة بهدف عدم التعرض، لذا يتطلب التحقيق في الجرائم الإلكترونية فريقاً متخصصاً وتقنيات متقدمة لمواجهة هذه التحديات⁴.

¹ رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، المجلد 16، العدد 41، 2018، ص 441.

² المرجع نفسه، ص 442.

³ المرجع نفسه، ص 442.

⁴ المرجع نفسه، ص 443.

ثانيا: السمات الخاصة بالمجرم الإلكتروني

يتميز مرتكب الجريمة المعلوماتية بصفات خاصة تميزه عن غيره من مرتكبي الجرائم، ومن أهم هذه الصفات:

أنه إنسان اجتماعي: المجرم الإلكتروني لا يظهر عدوانية مفرطة في المجتمع، بل يتكيف ويتعامل بشكل جيد مع البيئة المحيطة به، مما يزيد من خطورته الإجرامية، كما تمكنه هذه القدرة على التكيف الاجتماعي من إخفاء جوانب شخصيته الإجرامية.

أنه إنسان محترف وذكي: يستخدم المجرم المعلوماتي طرقا متنوعة للتلاعب بالبيانات والبرامج الحاسوبية، مثل زرع الفيروسات أو استعمال القنوات المنطقية أو الزمنية لتعطيل حركة النظام المعلوماتي وجعله غير قادر على أداء وظائفه الطبيعية.¹

المجرم المعلوماتي مجرم متخصص: غالبا ما يقتصر نشاطه على الجرائم المعلوماتية فقط، دون الانخراط في الجرائم التقليدية، ما يجعله متخصصا في هذا النوع من الجرائم فقط، ومتمرسا فيه بدقة.

المجرم المعلوماتي غير عنيف: لا يلجأ إلى العنف مطلقا في تنفيذ جريمته، إذ تعتمد الجريمة على الأساليب التقنية والمهارات الفكرية والمعرفة، معتمدة على درجة عالية من الثقافة والخبرة العملية.²

الفرع الثالث: تمييز الجرائم الإلكترونية عن الجرائم المعلوماتية

تعتبر الجرائم الإلكترونية والجرائم المعلوماتية من المصطلحات المتقاربة في ظاهرها، لكن هناك فروق تميز كل منهما عن الآخر من حيث المضمون، الوسائل، والأهداف.

¹ بن مكي نجاه، السياسة الجنائية لمكافحة جرائم المعطيات المعلوماتية، دار الخلدونية، الجزائر، 2017، ص 41.

² شايل نوال، الجريمة الإلكترونية في التشريع الجزائري، مجلة سوسيلوجيا، المجلد 6، العدد 2، ص 69.

أولاً: الجرائم المعلوماتية

الجرائم المعلوماتية هي تلك الأفعال التي تقع مباشرة على نظم المعلومات أو البيانات المخزنة في الحواسيب، بغرض الإضرار بالنظام نفسه أو بالبيانات التي يحتويها، وتشمل التلاعب بالبرامج، الوصول غير المصرح به للأنظمة، سرقة أو تعديل البيانات، واستخدام الحواسيب في الغش أو الاحتيال المالي، وذلك وفقاً للقوانين الوطنية التي نظمت هذا المجال، منها القانون الجزائري رقم 06-06 المعدل، والقوانين الخاصة بحماية المعطيات والمعلوماتية.¹ وتتركز هذه الجرائم على المحتوى الرقمي والنظم المعلوماتية نفسها، باعتبارها الهدف الأساسي للارتكاب.

ثانياً: الجرائم الإلكترونية

إن الجرائم الإلكترونية أوسع نطاقاً من الجرائم المعلوماتية، فهي تشمل كل فعل إجرامي يستخدم الوسائل الإلكترونية أو الحواسيب أو شبكة الإنترنت كأداة أو كبيئة ارتكاب، بغض النظر عن طبيعة الهدف، سواء كان مالياً، شخصياً، أو مؤسسياً². ويمكن أن تندرج تحت هذا المفهوم جرائم الاحتيال عبر الإنترنت، التجسس الإلكتروني، القرصنة على الحسابات البنكية، التجنيد لأغراض إرهابية إلكترونية، وغيرها من الأفعال الإجرامية التي تستغل التقنيات الحديثة كوسيلة وليس كهدف بحد ذاته.

ثالثاً: الفروق الأساسية بين النوعين

يمكن تلخيص هذه الفروق في النقاط التالية:

¹ عائشة بوحبزة، الحماية الجزائرية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013م، ص 35.

² جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة)، دار البلدية، ط1، عمان، الأردن، 2007، ص 222.

الهدف من الجريمة: في الجرائم المعلوماتية، الهدف هو النظام أو البيانات، أما في الجرائم الإلكترونية، فالتقنية وسيلة لتحقيق غاية إجرامية متنوعة.

النطاق التقني: الجرائم المعلوماتية تقتصر غالبا على الأنظمة الحاسوبية والشبكات المحلية، بينما الجرائم الإلكترونية قد تتجاوز الحدود الجغرافية، مستغلة شبكة الإنترنت والوسائل الرقمية الحديثة.

التأثير: الجرائم المعلوماتية تؤثر على النظم المعلوماتية مباشرة، أما الجرائم الإلكترونية فآثارها تمتد لتشمل الأفراد، المؤسسات، وحتى الأمن القومي والاقتصاد.

المعالجة القانونية: بينما نظمت التشريعات الوطنية مثل القانون الجزائري 06-06 وغيره الجرائم المعلوماتية، فإن الجرائم الإلكترونية تخضع لقوانين أوسع تشمل استخدام التقنية والإنترنت في ارتكاب الجريمة، مع مراعاة التحديث المستمر لمواجهة تطور الوسائل الرقمية.¹

يتضح أن الجرائم المعلوماتية جزء من الجرائم الإلكترونية، لكنها لا تشمل جميع أشكالها، وأن التمييز بينهما يساعد الباحثين والمشرعين على صياغة نصوص قانونية أكثر دقة وفعالية لمكافحة هذه الظاهرة الحديثة والمتطورة.

المطلب الثاني: ماهية المؤسسات المالية

تلعب المؤسسات المالية دورا محوريا في دعم النشاط الاقتصادي من خلال تقديم مختلف الخدمات المالية والمصرفية للأفراد والمؤسسات، ولتحديد طبيعة هذه المؤسسات وأهميتها، يتعين التعرف على مفهومها وخصائصها ووظائفها الأساسية.

الفرع الأول: مفهوم المؤسسات المالية

¹ جعفر حسن جاسم الطائي، المرجع نفسه، ص 224.

"المؤسسات المالية هي شركات أعمال تعتمد في أساس أصولها على الموارد المالية، مثل الأسهم والسندات والقروض، بدلاً من الأصول المادية كالمباني والمعدات والمواد الأولية، وتقوم هذه المؤسسات بمنح القروض للعملاء أو شراء واستثمار الأوراق المالية المتداولة في الأسواق المالية"¹.

تعرف المؤسسات المالية بأنها: "جهات وسيطة تعمل على تسهيل العلاقة بين من يرغبون في زيادة دخلهم وبين من يرغبون في استثمار أموالهم، بحيث توفر آليات لتحويل الأموال واستخدامها بشكل يحقق الفائدة لكلا الطرفين"².

كما تعرف كذلك بأنها: "وسيط مالي يتولى مهمة توجيه الأموال من المقرضين إلى المقترضين وتعبئة الموارد المالية من الأفراد والمؤسسات في الاقتصاد بهدف تقديم القروض والاستثمارات"³.

يتضح أن جميع التعريفات السابقة تتفق على أن المؤسسات المالية هي وسائط تهدف إلى تجميع الموارد المالية وإعادة توجيهها واستثمارها لخدمة مختلف الوحدات الاقتصادية، سواء عن طريق الأموال النقدية أو أدوات مالية أخرى.

الفرع الثاني: أنواع المؤسسات المالية

كانت التصنيفات القديمة للمؤسسات المالية تركز على تقسيمها إلى مجموعتين رئيسيتين: الوسطاء النقديون والوسطاء غير النقديين، إلا أنه مع التطور الحاصل في أواخر القرن

¹ عبد الغفار حنفي، رسمية زكي قرياصة، البورصات والمؤسسات المالية، الدار الجامعية، الإسكندرية، 2002، ص 12.

² أ.د. بشير علوان حمد، "دور المؤسسات المالية في تحفيز النشاط الاقتصادي في ظل الاقتصاد المعولم"، مجلة دراسات محاسبية ومالية، المجلد الرابع، العدد 19، الفصل الثاني، جامعة بغداد، المعهد العالي لدراسات المحاسبية والمالية، 2012، ص 188.

³ سلسبيل بن سماعيل، المسؤولية الجزائية للمؤسسات المالية، أطروحة دكتوراه في القانون العام، تخصص قانون عام اقتصادي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2020-2021، ص 13.

العشرين، وبحسب اختصاصات هذه المؤسسات، أصبح تصنيفها اليوم إلى نوعين رئيسيين: مؤسسات ودائعية ومؤسسات غير ودائعية.

أولاً: المؤسسات المالية الدائعية (مؤسسات الإيداع)

تعرف المؤسسات الدائعية على أنها مؤسسات مالية تقبل الودائع من الأفراد والمؤسسات، وتلعب دوراً أساسياً في عرض النقد بقدرتها على تغطية الودائع المسحوبة¹، كما تركز استثماراتها في سوق النقود نظراً لحاجة هذه السوق المستمرة للسيولة اللازمة لتعويض الودائع المسحوبة، إضافة إلى قدرتها على الاستثمار في الأوراق المالية.

وتشمل المؤسسات الدائعية عدة أنواع، أهمها: البنوك التجارية، مؤسسات الادخار والإقراض، بنوك الادخار، واتحادات الائتمان (بنوك اتحادات الجمهور).

وفيما يلي شرح لهذه الأنواع:

أ- البنوك التجارية:

تعد البنوك التجارية مؤسسات وساطة بين المودعين والمقترضين، حيث تقدم مجموعة من الخدمات المصرفية مثل قبول الودائع وتقديم القروض المباشرة، كما تشارك البنوك التجارية في البورصة لشراء وبيع الأوراق المالية. وسيكون لنا عودة لاحقة لتفصيل دور البنوك التجارية في المحاضرات المقبلة.

ب- مؤسسات الادخار والإقراض:

¹ توماس ماير، جيمس إسدوستيري، ترجمة أحمد عبد الخالق، النقود والبنوك والاقتصاد، دار المريخ للنشر، 2002، ص 61.

تختص هذه المؤسسات بما يعرف بالادخار الشخصي، حيث تحصل على مواردها من الودائع الادخارية مقابل شيكات ادخار تقدمية للمودعين لديها، كما تستثمر هذه الموارد في أدوات مالية طويلة الأجل، مع تركيز قروضها في مجال السكن.¹

ج-بنوك الادخار:

تعتبر بنوك الادخار مؤسسات مالية مشابهة إلى حد كبير لمؤسسات الادخار والإقراض، حيث تحصل على مواردها من الودائع الادخارية مقابل شيكات الإيداع، وتستخدم هذه الودائع عادة في منح القروض العقارية. وتمثل هذه البنوك في البداية المصدر الوحيد للفئات ذات الدخل المنخفض والمدخرات الصغيرة، إلا أنها تطورت لاحقاً لتصبح قادرة على منح قروض استهلاكية خارج نطاق السكن.²

د-اتحادات الائتمان:

تعتبر اتحادات الائتمان مؤسسات مالية صغيرة، يتركز نشاطها عادة في قطاع محدد، حيث تحصل على مواردها من ودائع الأعضاء الذين غالباً ما ينتمون إلى فئة اجتماعية معينة، مثل اتحاد ائتمان العمال، أو اتحاد ائتمان العاملين في المناجم، وغيرها. ومع مرور الوقت، أصبح بإمكان هذه الاتحادات تقديم قروض استهلاكية للفئات المنتمية لها، إضافة إلى قروض عقارية أو تمويلات متعلقة بالسكن.

¹ بن قبيلة زين الدين، أثر التطور المالي على النمو الاقتصادي في الجزائر، رسالة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة تمساف، 2015-2016، ص 39.

² بن عزوز عبد الرحمن، دور الوساطة المالية في تنشيط سوق الأوراق المالية مع الإشارة لحالة بورصة تونس، مذكرة ماجستير، تخصص إدارة عامة، كلية العلوم الاقتصادية والإدارية، جامعة قسنطينة، 2011-2012م، ص 85.

تعد اتحادات الائتمان أصغر أنواع المؤسسات الوداعية، لكنها الأكثر نموًا، ففي عام 1994 تضاعفت أصولها أربع مرات مقارنة بما كانت عليه في عام 1980 في الولايات المتحدة الأمريكية.¹

ثانياً: المؤسسات المالية غير الوداعية (مؤسسات الادخار التعاقدية)

هي مؤسسات مالية تحصل مواردها على فترات محددة وبأسس تعاقدية، بحيث تقدّم أنواعاً من الخدمات المالية، لكنها لا تتلقى ودائع كما هو الحال في المؤسسات الوداعية، وهذا هو الفارق الأساسي بينها وبين المؤسسات المالية الوداعية، وأهم أمثلتها: شركات التأمين، صناديق الاستثمار، وصناديق معاشات التقاعد.

أ- شركات التأمين:

هي مؤسسات مالية تجمع الأموال من الأفراد على شكل أقساط، لإعادة استثمارها نيابة عنهم مقابل عائد معين، وتتمثل وظيفتها الرئيسية في حماية الأفراد من أخطار محددة، لكنها تمارس أيضاً وظيفة الوساطة المالية كجزء من نشاطها المالي.²

ب- صناديق الاستثمار:

تُعرف صناديق الاستثمار بأنها مؤسسات مالية تحتوي على مجموعة متنوعة من الأسهم والسندات تُشترى من قبل مجموعة من المستثمرين، وتُدار بواسطة متخصصين في مجال الإدارة أو تنظيم الاستثمارات، كما يمكن أن تُنشأ شركات متخصصة أو بنوك تجارية لتتولى إدارتها.³

وبشكل عام يمكن تعريف صناديق الاستثمار على أنها:

¹ المرجع نفسه، ص 87.

² جمال جويديان الجمل، دراسات في الأسواق المالية والنقدية، دار الصفاء للنشر والتوزيع، ط1، عمان، 2002، ص 40.

³ بن عزوز عبد الرحمن، المرجع نفسه، ص 88.

"إحدى مؤسسات الاستثمار الجماعي التي قد تتخذ شكل شركة مساهمة أو وحدة تنظيمية مستقلة داخل الجهة المنشئة لها (شركة/بنك مثلاً)، وتعمل كوعاء مالي لجمع الأموال من الأشخاص الطبيعيين أو الاعتباريين مقابل وثائق استثمار يحصّون عليها، ويتم استثمار هذه الأموال في محافظ الأوراق المالية التي يديرها مديرون محترفون بهدف زيادة العائد وتقليل المخاطر، وتوفير السيولة وتحقيق باقي أهداف الصندوق."¹

ج-صناديق معاشات التقاعد:

هي مؤسسات مالية غير ودائعية تجمع مواردها من أقساط معاشات التقاعد التي يدفعها الموظفون مقابل توفير قيمة مالية ثابتة عند التقاعد، لتعويض المعاش عن الأجر الذي كان يتقاضاه الموظف أثناء عمله.²

إن المؤسسات المالية سواء كانت ودائعية أو غير ودائعية، تؤدي دوراً فعالاً في تجميع الموارد المالية وإعادة توجيهها للاستثمار، حيث توازن بين تأمين المدخرات وتحقيق العوائد، مع اختلاف آليات عملها بحسب نوعها وطبيعة خدماتها المالية.

الفرع الثالث: دور المؤسسات المالية في النظام المالي

تلعب المؤسسات المالية دوراً أساسياً في دعم الاقتصاد وضمان استقرار النظام المالي، فهي تعمل كحلقة وصل بين الأطراف الاقتصادية المختلفة، حيث تجمع المدخرات من الأفراد والشركات وتحولها إلى استثمارات منتجة، من خلال هذه الوساطة، تساهم المؤسسات المالية في تعزيز السيولة، وتحفيز النمو الاقتصادي، وتوفير التمويل اللازم للمشاريع المختلفة، مع إدارة المخاطر المالية بطرق منظمة.³

¹ محمد عنتر أحمد، الإدارة المالية والاستثمار، الأكاديمية العربية للمعارف المالية والمصرفية، ط1، عمان، 2009، ص 24.

² محمد عنتر أحمد، المرجع نفسه، ص 24.

³ المرجع نفسه، ص 63.

وتشمل هذه المؤسسات البنوك التجارية، مؤسسات الادخار والقروض، شركات التأمين، وصناديق الاستثمار، وكل منها يؤدي وظائف محددة تكمل بعضها البعض، البنوك التجارية على سبيل المثال، تتولى جمع الودائع وتقديم التمويل للأفراد والشركات، بينما تشجع مؤسسات الادخار على تراكم المدخرات وتحويلها إلى استثمارات طويلة الأمد، أما شركات التأمين، فهي توفر حماية مالية للأفراد والشركات من المخاطر المحتملة، بينما تدير صناديق الاستثمار الموارد المجمعة وتوظفها في الأسواق المالية لتحقيق عائد مناسب مع التحكم في المخاطر.¹

وهذه الطريقة توفر المؤسسات المالية بنية تحتية متكاملة للنشاط الاقتصادي، تمكن السوق المالي من العمل بكفاءة، وتتيح للأفراد والشركات الوصول إلى الأدوات التمويلية التي تساعدهم على تطوير أعمالهم ومشاريعهم، كما تساهم في ضبط حركة النقد، وتنظيم الأسواق، وتعزيز ثقة المتعاملين في النظام المالي، مما ينعكس إيجاباً على التنمية الاقتصادية المستدامة.

المبحث الثاني: الإطار القانوني للجرائم الإلكترونية في المجال المالي

يحدد الإطار القانوني للجرائم الإلكترونية في المجال المالي القواعد والضوابط التي تحكم المعاملات الرقمية ويضمن حماية المعاملات المالية الإلكترونية، حيث يشمل هذا المبحث مطلبين: المطلب الأول التنظيم القانوني للجرائم الإلكترونية في التشريع الجزائري، والمطلب الثاني المستند الإلكتروني والتوقيع الإلكتروني كوسائل قانونية في المعاملات المالية.

المطلب الأول: التنظيم القانوني للجرائم الإلكترونية في التشريع الجزائري

أولى المشرع الجزائري أهمية كبيرة لتنظيم الجرائم الإلكترونية، وذلك من خلال سن مجموعة من القوانين العامة وأخرى خاصة، وهو ما سيتم التطرق إليه فيما يأتي.

¹ جمال جويدان الجمل، المرجع نفسه، ص 34.

الفرع الأول: قانون العقوبات

تعرض المشرع الجزائري لتجريم الأفعال الماسة بأنظمة الحاسب الآلي في قانون العقوبات بموجب القانون 04-15، وذلك تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"¹، ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 8.

وفي عام 2006 أدخل المشرع تعديلا آخر على قانون العقوبات بموجب القانون 06-23²، حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبات المقررة لهذه الأفعال. ويرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام، باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى.³

أما بالنسبة لأنواع الجرائم الإلكترونية المنصوص عليها في قانون العقوبات، والتي يمكن تصنيفها فيما يلي:

- الغش أو الشروع فيه في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.
- حذف أو تغيير المعطيات المنظمة.
- إدخال أو تعديل في نظام المعطيات.
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار بوسائل موجهة لارتكاب هذه الجرائم.
- حيازة أو إفشاء أو نشر أو استعمال المعطيات.

¹ المادة 394 مكرر إلى المادة 394 مكرر 8 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

² القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات، ج ر، العدد 84، 2006.

³ د. يزيد بوحليط، المرجع نفسه، ص 134

-تكوين جمعية الأشرار.

يمكن تكييف هذه الأفعال الإجرامية على أنها جرائم ضد أموال الغير والمضرة بالمجتمع.

تجدر الإشارة إلى أن المشرع الجزائري قام بتعديل قانون العقوبات سنة 2016، مستحدثا بذلك نصا جديدا وهو المادة 87 مكرر 12، والتي أوجدت جريمة جديدة تتمثل في جناية تجنيد الأشخاص لصالح إرهابي أو منظمة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال.¹

الفرع الثاني: قانون الإجراءات الجزائية

فيما يتعلق بمتابعة الجريمة الإلكترونية، فإنها تتم في الغالب بنفس الإجراءات التي تتبع في الجرائم التقليدية، مثل التفتيش والمعاينة، واستجواب المتهم، والضبط، والتسرب، والشهادة، والخبرة. غير أن المشرع الجزائري نص على بعض الأحكام الخاصة، من بينها تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية.²

كما نص في المادة 45 الفقرة 7 من نفس القانون المعدلة على أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد العامة، سواء من حيث الشروط الشكلية أو الموضوعية.³

كما نص المشرع كذلك على التوقيف للنظر في جريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 51 الفقرة 6⁴، إضافة إلى إمكانية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، أما باقي إجراءات التحقيق والمحاكمة فتطبق بشأنها نفس الإجراءات الخاصة بالجرائم التقليدية.

¹ القانون رقم 16-02 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات، ج ر، العدد 39، 2016.

² المادة 37 من القانون رقم 17-07 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية، ج ر، العدد 20، 2017.

³ المادة 45 الفقرة 7 من نفس القانون.

⁴ المادة 51 الفقرة 6 من نفس القانون.

قد تبنى هذا القانون تعريفا للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كما حدد مختلف المفاهيم المرتبطة بها، لاسيما ما يتعلق بالمنظومة المعلوماتية ومعطيات المعلومات ومقدمي الخدمات¹، وذلك بهدف ضبط الإطار القانوني لهذه الجرائم المستحدثة وتوضيح مختلف الأطراف المتدخلة في البيئة الرقمية.

كما سعى المشرع من خلال هذا التنظيم إلى مواكبة التطورات المتسارعة في مجال تكنولوجيا المعلومات والاتصال، وتوفير آليات قانونية فعالة لمكافحة الأفعال الإجرامية التي قد تمس بالأنظمة المعلوماتية أو تستغلها كوسيلة لارتكاب الجرائم.

قد خول هذا القانون جملة من الإجراءات الخاصة التي تطبق في مجال مكافحة الجرائم الإلكترونية، نظرا لخصوصية هذا النوع من الجرائم التي ترتكب في بيئة رقمية وتستلزم وسائل تحقيق تتلاءم مع طبيعتها التقنية، ومن بين هذه الإجراءات:

-تفتيش المنظومة المعلوماتية.

-مراقبة الاتصالات الإلكترونية.

-حجز المعطيات المعلوماتية.²

تعد هذه الإجراءات من الوسائل القانونية المهمة التي تمكن الجهات القضائية والأمنية من تتبع الأنشطة الإجرامية المرتبطة بتكنولوجيا الإعلام والاتصال، والكشف عن مرتكبيها، وجمع الأدلة الرقمية التي يمكن الاعتماد عليها في مراحل التحقيق والمحاكمة.

¹ المادة 2 من القانون 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ، العدد 47، 2009.

² المادة 6 من نفس القانون.

كما أنشأ المشرع بموجب هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، تتولى القيام بعدة مهام من أجل تعزيز الحماية القانونية للأنظمة المعلوماتية، ومن أهم مهامها:

- تفعيل التعاون القضائي والأمني، وإدارة وتنسيق العمليات الوقائية المرتبطة بمكافحة الجرائم الإلكترونية.

- تبادل المعلومات مع الجهات الأجنبية بهدف تعزيز حماية المنظومة المعلوماتية من مختلف الأخطار التي قد تهدد مؤسسات الدولة أو تمس بالدفاع الوطني أو بالمصالح الاستراتيجية للاقتصاد الوطني.¹

من خلال هذه الآليات يسعى المشرع الجزائري إلى تدعيم منظومة الحماية القانونية للفضاء المعلوماتي، والحد من المخاطر الناجمة عن الاستعمال غير المشروع لتكنولوجيا الإعلام والاتصال.

الفرع الثالث: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد تبنى هذا القانون تعريفا للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكل ما يتعلق بالمنظومة المعلوماتية ومعطيات المعلومات ومقدمي الخدمات.

كما خول هذا القانون اتخاذ بعض الإجراءات الخاصة التي تطبق على الجرائم الإلكترونية، من بينها:

- مراقبة الاتصالات الإلكترونية.

- تفتيش المنظومة المعلوماتية.

¹ سعيد عبد الفتاح، إدارة المؤسسات المالية والمصرفية، دار الجامعة الجديدة، الإسكندرية، مصر، 2017، ص 35.

-حجز المعطيات المعلوماتية.¹

قد أنشأ بموجب هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي من مهامها:

-تفعيل التعاون القضائي والأمني، وإدارة وتنسيق العمليات الوقائية.

-تبادل المعلومات مع الجهات الأجنبية من أجل تعزيز حماية المنظومة المعلوماتية من كل خطر يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.²

المطلب الثاني: المستند الإلكتروني والتوقيع الإلكتروني كوسائل في المعاملات المالية

مع تطور التجارة الإلكترونية والخدمات المالية الرقمية، أصبح المستند الإلكتروني والتوقيع الإلكتروني من أهم الوسائل المعتمدة لإبرام المعاملات المالية وإثباتها. لذلك يقتضي الأمر التعرف على مفهوم كل منهما وبيان أهميتهما في تعزيز الثقة والأمان في البيئة الرقمية.

الفرع الأول: المستند الإلكتروني كوسيلة في المعاملات المالية

المستند الإلكتروني هو كل وثيقة رقمية تحتوي على معلومات قابلة للقراءة، تم إنشاؤها أو تبادلها أو تخزينها باستخدام الوسائل الإلكترونية أو الحاسوبية، ويمكن استخدامها كدليل أو مرجع قانوني في المعاملات المالية والمعاملات القانونية الأخرى.³

كما يعرف أيضا بأنه: "كل ملف أو وثيقة رقمية تحمل بيانات تثبت حقا أو التزاما أو إجراء مالي، ويكون قابلاً للتحقق والتوقيع إلكترونياً لضمان صدقه وسريانه بين الأطراف المختلفة".⁴

¹ محمد عنتر أحمد، المرجع نفسه، ص 35.

² المادة 14 من القانون 09-04 السابق ذكره.

³ محمد فواز محمد المطالفة، الوجيز في عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2015، ص 134.

يتيح استخدام المستندات الإلكترونية تسهيل المعاملات المالية، وتقليل الوقت والتكاليف المرتبطة بالإجراءات الورقية، مثل إصدار الفواتير، العقود، تحويل الأموال، وإتمام الصفقات المالية، كما يمكن توقيع هذه المستندات إلكترونياً مما يمنحها القوة القانونية نفسها للمستند الورقي، مع ضمان الأمان والدقة، وحماية المعاملات من التزوير أو التلاعب من خلال تقنيات التحقق والتشفير الرقمية، بما فيها التوقيع الرقمي وتقنيات البلوك تشين في بعض المؤسسات المالية.¹

كما يسهل المستند الإلكتروني عمليات الرقابة والمراجعة، لأنه يمكن تتبعه بسهولة من خلال نظم التوثيق الرقمي، ويتيح الوصول السريع إليه عند الحاجة، مما يجعله أداة فعالة وضرورية في التحول الرقمي للمعاملات الاقتصادية.

الفرع الثاني: التوقيع الإلكتروني كوسيلة في المعاملات المالية

أ- تعريف التوقيع الإلكتروني:

اهتمت العديد من التشريعات والهيئات القانونية بتحديد مفهوم التوقيع الإلكتروني، نظراً لأهميته في توثيق المعاملات الإلكترونية وضمان مصداقيتها، فقد عرّفه القانون العربي النموذجي الموحد بأنه: "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو متصلة بها منطقياً، يمكن استعمالها لتحديد هوية الموقع بالنسبة إلى رسالة البيانات، وكذلك للدلالة على موافقته على المعلومات الواردة فيها"².

⁴ شايل نوال، المرجع نفسه، ص 73.

¹ عبد الحميد بلعباس، "أساليب حماية الوثائق الإلكترونية في ضوء التوقيع الإلكتروني الجزائري رقم 06 الصادر بتاريخ 10 فبراير 2015: دراسة مقارنة"، جامعة محمد بوضياف، المسيلة، ص 168، مقال منشور على الموقع الإلكتروني <https://www.asjp.cerist.dz>، تم الاطلاع عليه بتاريخ : 2026/03/07، الساعة 15:54.

² أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، ط2، الجزائر، 2007م، ص 37.

كما عرفه قانون الاتحاد الأمريكي بأنه: "صوت أو رمز أو معالجة إلكترونية تكون مرفقة أو مرتبطة بعقد أو سجل آخر، ويتم تنفيذها أو اعتمادها من طرف شخص لديه نية التوقيع على ذلك السجل"¹.

في الإطار ذاته، عرفه المشرع المصري في المادة (01) من مشروع قانون التجارة الإلكترونية لسنة 2001 بأنه: "حروف أو أرقام أو رموز أو إشارات ذات طابع مميز تسمح بتحديد هوية صاحب التوقيع وتمييزه عن غيره"².

أما المشرع الجزائري فلم يبتعد عن هذه التعريفات، حيث عرّف التوقيع الإلكتروني في المادة (02/1) من القانون 04-15 بأنه: "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقياً ببيانات إلكترونية أخرى، وتستعمل كوسيلة للتوثيق"، ويقارب هذا التعريف ما جاء في المادة (02/1) من التوجيه الأوروبي رقم 99/93 المؤرخ في 13 ديسمبر 1999، التي عرّفت التوقيع الإلكتروني بأنه: "معطيات في شكل إلكتروني ترتبط بمعطيات إلكترونية أخرى وتستخدم كوسيلة لإثبات صحتها"³.

كما أقرّ المشرع الجزائري مبدأ المساواة بين التوقيع الإلكتروني والتوقيع المكتوب، وذلك بموجب نص المادة (08) من القانون 04-15 التي تنص على أنه: "يعتبر التوقيع الإلكتروني الموصوف وحده مماثلاً للتوقيع المكتوب سواء تعلق الأمر بشخص طبيعي أو معنوي"، على أن يستوفي هذا التوقيع مجموعة من الشروط القانونية التي حددها المشرع، والتي سيتم التطرق إليها لاحقاً.

¹ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني - دراسة مقارنة، دار النهضة العربية، ط1، القاهرة، مصر، 2006، ص 46.

² عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015م، ص 196.

³ التوجيه الأوروبي رقم 99/93 بشأن الإطار المشترك للتوقيعات الإلكترونية الصادر بتاريخ 1999/12/13.

ينظر المشرع الجزائري إلى التوقيع الإلكتروني باعتباره مجموعة من المعطيات التي تأخذ شكلا إلكترونيا، مثل الحروف أو الأرقام أو الرموز أو الإشارات، سواء كانت مرفقة بالسند الإلكتروني أو مرتبطة به ارتباطا منطقيا بمعطيات إلكترونية أخرى، ويكون الهدف من استعمالها توثيق مختلف المعاملات الإلكترونية، ومن هذا المنطلق يعكس التوقيع الإلكتروني بعدا تقنيا وقانونيا في الوقت نفسه، إذ يمثل وسيلة تكنولوجية تساعد على تحقيق الأمان والسرية في التعاملات الإلكترونية¹، كما يساهم في الحد بدرجة كبيرة من احتمالات التزوير بفضل التطور المستمر في تقنيات حفظ ومعالجة البيانات.

ب- دور التوقيع الإلكتروني في تعزيز أمان المعاملات المالية:

يعتبر التوقيع الإلكتروني أحد الأدوات الأساسية التي تعزز الأمان والمصادقية في المعاملات المالية الرقمية، حيث يُتيح التأكد من هوية الأطراف المتعاقدة وضمان سلامة البيانات المتبادلة، ويمنع أي تلاعب أو تزوير قد يحدث أثناء تنفيذ العمليات المصرفية أو الاستثمارية عبر الشبكات الإلكترونية.

كما يعتمد التوقيع الإلكتروني على تقنيات التشفير الرقمي التي تربط بين هوية صاحب التوقيع والمستند الموقع، مما يجعل أي تعديل لاحق على الوثيقة قابلا للاكتشاف بسهولة، ولهذا فهو يلعب دور الوسيط الأمني بين المؤسسات المالية والمودعين أو المستثمرين، خصوصا في العمليات التي تتم عن بُعد مثل التحويلات البنكية، فتح الحسابات، شراء الأوراق المالية، أو إتمام العقود الاستثمارية².

¹ سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته -صوره- حجيته في الإثبات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ط2، 2006، ص 60.

² المرجع نفسه، ص 67.

يساهم التوقيع الإلكتروني في تسريع وتسهيل العمليات المالية، إذ يقلل من الحاجة إلى الوثائق الورقية والانتقالات الميدانية، ويضمن تسجيلًا دقيقًا للمعاملات، مما يعزز الشفافية والثقة في النظام المالي الإلكتروني.

خلاصة الفصل:

في ختام هذا الفصل، يتبين أن الجرائم الإلكترونية الموجهة ضد المؤسسات المالية تعد من أخطر صور الجرائم الحديثة المرتبطة بتطور التكنولوجيا والتحول الرقمي، حيث ترتبط باستخدام الوسائل المعلوماتية في الاعتداء على الأنظمة المالية أو المساس بأمنها، كما أن فهم هذا النوع من الجرائم يقتضي الإحاطة بمفهوم الجرائم الإلكترونية وخصائصها وتمييزها عن الجرائم المعلوماتية من جهة، ومعرفة طبيعة المؤسسات المالية ودورها الحيوي في النظام المالي من جهة أخرى، وقد أظهر الإطار القانوني أن المشرع الجزائري أولى اهتماما متزايدا بهذه الجرائم من خلال نصوص قانونية خاصة تهدف إلى مكافحتها وتنظيمها، كما برز دور المستند الإلكتروني والتوقيع الإلكتروني كوسائل قانونية حديثة في المعاملات المالية، بما يعزز موثوقية التعاملات الرقمية، وبذلك يتضح أن الإطار المفاهيمي والقانوني يشكل الأساس لفهم هذه الجرائم والتصدي لها بفعالية داخل البيئة الرقمية.



الفصل الثاني: صور الجرائم الإلكترونية الموجهة



ضد المؤسسات المالية وآليات مكافحتها

يشهد القطاع المالي في العصر الرقمي تحولات متسارعة بفعل الاعتماد المتزايد على نظم المعلومات والتقنيات الحديثة في تسيير المعاملات والخدمات، وهو ما جعله في الوقت ذاته عرضة لمخاطر إلكترونية متنامية تستهدف بنيته التحتية وموارده وبياناته الحساسة، حيث لم تعد الجرائم التقليدية قادرة على مواكبة التطور الذي عرفته الأساليب الإجرامية، بل ظهرت أنماط جديدة تعتمد على الاختراق والاستغلال غير المشروع للأنظمة المعلوماتية بغرض تحقيق مكاسب مالية أو إلحاق أضرار بالمؤسسات، الأمر الذي فرض ضرورة البحث في طبيعة هذه الجرائم وصورها المختلفة، وكذا الوقوف على الإطار القانوني والآليات الكفيلة بمواجهتها والحد من آثارها، وعليه سنتطرق في هذا الفصل إلى مبحثين رئيسيين:

المبحث الأول: صور الجرائم الإلكترونية الماسة بالمؤسسات المالية.

المبحث الثاني: الحماية الجزائية وآليات الوقاية.

المبحث الأول: صور الجرائم الإلكترونية الماسة بالمؤسسات المالية

تتعدد أشكال الجرائم الإلكترونية التي تمس المؤسسات المالية تبعا لتنوع الأهداف والأساليب التي يعتمدها الجناة، حيث تتراوح بين الاعتداء المباشر على الأنظمة المعلوماتية ومحاولة اختراقها أو تعطيلها، وبين الجرائم ذات الطابع المالي التي تستهدف المعاملات والبيانات لتحقيق منافع غير مشروعة، وهو ما يستدعي تصنيف هذه الصور وتحديد خصائص كل منها من أجل فهم أبعادها وخطورتها،¹ وعليه سيتم التطرق في هذا المبحث إلى جرائم الاعتداء على أنظمة المعلومات المالية، ثم الجرائم الإلكترونية ذات الطابع المالي.

المطلب الأول: جرائم الاعتداء على أنظمة المعلومات المالية

تتخذ هذه الاعتداءات صورا متعددة تختلف من حيث الأسلوب والنتائج لكنها تشترك في كونها تستهدف البنية التقنية للمؤسسة، وعليه سيتم التطرق إلى جريمة الاختراق باعتبارها مدخلا غير مشروع للأنظمة، ثم تعطيل الأنظمة لما له من تأثير مباشر على استمرارية الخدمات، وأخيرا سرقة البيانات المصرفية لما تمثله من قيمة مالية ومعلوماتية حساسة.

الفرع الأول: الاختراق

يعد الاختراق من أخطر صور الجرائم الإلكترونية التي تستهدف أنظمة المعلومات المالية، حيث يقوم على الدخول غير المشروع إلى الأنظمة أو الشبكات أو قواعد البيانات بهدف الاطلاع أو التعديل أو الإتلاف أو الاستغلال غير القانوني للمعطيات²، وقد ازدادت خطورته مع تطور التقنيات الرقمية واعتماد المؤسسات المالية على البنى التحتية المعلوماتية في إدارة عملياتها.

¹ أحمد عبد الكريم سلامة، الجرائم الإلكترونية وأمن المعلومات، دار النهضة العربية، القاهرة، 2012، ص 145.

² أحمد بن عيسى، جرائم الاختراق الإلكتروني في التشريع الجزائري، رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2019، ص 43.

يعرف الاختراق بأنه: "الولوج غير المشروع إلى نظام معلوماتي أو جزء منه دون إذن مسبق من صاحبه أو المسؤول عنه، بقصد الاطلاع على البيانات أو استغلالها أو التلاعب بها".¹

كما يعرف بأنه: "كل فعل يهدف إلى تجاوز أنظمة الحماية والدخول إلى الشبكات أو الأجهزة المعلوماتية بطرق غير مشروعة بغرض الحصول على معلومات أو إحداث ضرر بالنظام".²

يعرف أيضا بأنه: "استخدام وسائل تقنية أو برامج خاصة لاختراق نظم المعالجة الآلية للبيانات دون ترخيص، بما يؤدي إلى المساس بسرية المعلومات أو سلامة النظام أو استمرارية عمله".³

لا يقتصر الاختراق على مجرد الولوج غير المشروع، بل يتخذ أشكالا متعددة تختلف باختلاف أهداف الجاني والوسائل المستخدمة، فقد يكون بغرض التجسس وسرقة المعلومات المالية كبيانات الحسابات والتحويلات، وقد يكون بهدف تعطيل الأنظمة أو إتلافها مما يؤثر على استمرارية الخدمات المالية، كما يمكن أن يستعمل كوسيلة تمهيدية لارتكاب جرائم أخرى كتحويل الأموال بطرق غير مشروعة أو التلاعب بالمعطيات المحاسبية.⁴

¹ محمد حجازي، جرائم الحاسب الآلي والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 45.

² عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص 112.

³ أحمد عبد الله عبد الكريم، جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، مصر، 2015، ص 67.

⁴ محمد عنتر أحمد، المرجع نفسه، ص 134.

تعتمد عمليات الاختراق غالباً على استغلال الثغرات التقنية في البرمجيات أو ضعف أنظمة الحماية أو حتى الأخطاء البشرية داخل المؤسسة، حيث يلجأ القراصنة إلى تقنيات متعددة مثل الهندسة الاجتماعية أو البرمجيات الخبيثة أو هجمات القوة الغاشمة للوصول إلى الأنظمة.¹

كما أن خطورة الاختراق تكمن في آثاره الممتدة التي لا تقتصر على الخسائر المالية المباشرة، بل تمتد إلى المساس بسمعة المؤسسة وثقة العملاء فيها، وهو ما قد يؤدي إلى تداعيات اقتصادية وقانونية جسيمة،² الأمر الذي يفرض التعامل معه بصرامة سواء من خلال التشريعات الجزائية أو عبر تبني استراتيجيات أمنية متطورة قادرة على التصدي لهذه التهديدات المتجددة.

الفرع الثاني: تعطيل الأنظمة

يعرف تعطيل الأنظمة بأنه: "كل فعل يؤدي إلى إعاقة أو إيقاف التشغيل العادي لنظام معلوماتي أو شبكة معلوماتية، سواء بصفة كلية أو جزئية، نتيجة تدخل غير مشروع".³

كما يعرف بأنه: "كل سلوك تقني أو مادي من شأنه التأثير على كفاءة النظام المعلوماتي من خلال تعطيله أو إبطائه أو منع الوصول إلى خدماته، بما يخل بوظائفه الأساسية".⁴

تتخذ هذه الجريمة عدة أساليب، من أبرزها هجمات حجب الخدمة التي تعتمد على إرسال عدد هائل من الطلبات لإرباك الخوادم وإخراجها عن الخدمة، إلى جانب إدخال برمجيات خبيثة

¹ د. يزيد بوحليط، المرجع نفسه، ص 434.

² المرجع نفسه، ص 435.

³ عبد الفتاح بيومي حجازي، المرجع نفسه، ص 178.

⁴ محمود أحمد طه، الحماية الجنائية لنظم المعلومات، دار النهضة العربية، القاهرة، مصر، 2012، ص 96.

تعمل على تعطيل البرامج أو إتلاف الملفات أو إبطاء النظام بشكل متعمد، كما قد يتم استهداف البنية التحتية التقنية بإتلاف بعض مكوناتها أو تعطيل قنوات الاتصال بين الأنظمة.¹

تتعرض آثار هذا النوع من الاعتداء بشكل مباشر على المؤسسات المالية، حيث يؤدي إلى توقف العمليات البنكية وتعذر تنفيذ التحويلات وخدمات الدفع، إضافة إلى إرباك مصالح العملاء وإضعاف الثقة في كفاءة المؤسسة²، وهو ما قد يترتب عنه خسائر مادية ومعنوية معتبرة

كما أن صعوبة التنبؤ بهذه الهجمات وسرعة انتشارها في البيئة الرقمية تجعل من الضروري اعتماد وسائل وقائية متقدمة، من بينها أنظمة المراقبة المستمرة وتحديث البرمجيات وتعزيز قدرات الاستجابة السريعة، فضلا عن وضع خطط بديلة لضمان استمرارية الخدمة في حال وقوع مثل هذه الاعتداءات.³

الفرع الثالث: سرقة البيانات المصرفية

تشكل سرقة البيانات المصرفية أحد أخطر التهديدات التي تواجه المؤسسات المالية في البيئة الرقمية، بالنظر إلى القيمة العالية للمعلومات التي يتم استهدافها.

تعرف سرقة البيانات المصرفية بأنها: "الاستحواذ غير المشروع على المعلومات المالية الحساسة المخزنة أو المتداولة عبر الأنظمة المعلوماتية، بقصد استخدامها أو استغلالها دون إذن من صاحبها".⁴

¹ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2010، ص 56.

² رامي متولي القاضي، مكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2011، ص 234.

³ المرجع نفسه، ص 235.

⁴ محمد حجازي، المرجع نفسه، ص 121.

كما تعرف بأنها: "كل فعل يهدف إلى الحصول على بيانات مصرفية ذات طابع سري، سواء عن طريق اعتراضها أثناء انتقالها أو استخراجها من قواعد البيانات، بما يؤدي إلى المساس بسرية المعطيات المالية".¹

يعرفها كذلك بعض الفقه بأنها: "استخدام وسائل تقنية أو احتيالية للوصول إلى معلومات مالية شخصية أو مؤسسية، واستغلالها في تحقيق منافع غير مشروعة أو الإضرار بأصحابها".²

تعتمد سرقة البيانات المصرفية على مجموعة من الأساليب المتطورة التي تتغير بتغير مستوى الحماية داخل المؤسسات المالية، حيث يلجأ الفاعلون إلى استغلال نقاط الضعف الموجودة في البنية التقنية أو في سلوك المستخدمين أنفسهم، فمن الناحية التقنية يتم التسلل إلى قواعد البيانات أو الخوادم التي تحتوي على المعلومات الحساسة بهدف استخراجها بشكل مباشر، كما يتم في حالات أخرى اعتراض تدفق البيانات أثناء انتقالها عبر الشبكات، خاصة إذا كانت غير مؤمنة بشكل كاف.³

كما تستعمل برامج خفية يتم إدخالها إلى الأنظمة أو أجهزة المستخدمين، تقوم بتسجيل كل المعطيات المدخلة مثل كلمات المرور وأرقام البطاقات، دون أن يشعر الضحية بذلك، وفي مقابل ذلك تظهر أساليب تعتمد على الخداع، من خلال إنشاء واجهات رقمية شبيهة بالمواقع الرسمية للمؤسسات المالية، يتم من خلالها استدراج المستخدم للكشف عن معلوماته بنفسه⁴، حيث يعكس انتقال هذا النوع من الجرائم من الطابع التقني البحت إلى توظيف الجانب النفسي والسلوكي.

¹ عبد الفتاح بيومي حجازي، المرجع نفسه، ص 88.

² أحمد عبد الله عبد الكريم، المرجع نفسه، ص 143.

³ عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، دار الوراق، ط1، بيروت، لبنان، 2004، ص 92.

⁴ المرجع نفسه، ص 93.

تتجاوز آثار هذه الممارسات مجرد الحصول على البيانات، إذ يتم استغلالها لاحقا في تنفيذ عمليات مالية بطرق غير مشروعة، مثل إجراء تحويلات أو سحب أموال أو الدخول إلى الحسابات وتغيير معطياتها، وقد يتم كذلك إعادة بيع هذه المعلومات ضمن شبكات غير قانونية،¹ مما يؤدي إلى اتساع دائرة الاستغلال وتعدد الضحايا.

تظهر خطورة هذا النوع من الجرائم في صعوبة اكتشافه في الوقت المناسب، خاصة إذا تم بشكل تدريجي أو باستعمال تقنيات متقدمة تخفي آثارها، كما أن استرجاع البيانات أو الحد من آثار تسريبها يصبح أكثر تعقيدا بعد انتشارها²، الأمر الذي يفرض على المؤسسات المالية اعتماد مقاربة شاملة تقوم على تأمين الأنظمة من الداخل ومراقبة تدفق المعلومات بشكل مستمر، إلى جانب رفع مستوى الوعي لدى المستخدمين باعتبارهم عنصرا أساسيا في منظومة الحماية الرقمية.

المطلب الثاني: الجرائم الإلكترونية المالية

تتمثل الجرائم الإلكترونية المالية في الأفعال التي تستهدف الأموال والمعاملات عبر الوسائط الرقمية باستخدام أساليب احتيالية أو غير مشروعة، حيث يسعى الفاعلون إلى تحقيق مكاسب مالية بطرق يصعب تتبعها في البيئة الرقمية، وعليه سيتم التطرق إلى الاحتيال الإلكتروني، ثم تحويل الأموال غير المشروع، وأخيرا تزوير المعطيات المالية.

الفرع الأول: الاحتيال الإلكتروني

اختلف الفقهاء في الوصول إلى تعريف دقيق لجريمة الاحتيال، ويرجع ذلك إلى اختلاف الزاوية التي ينظر منها كل فقيه إلى هذه الجريمة، ومن بين التعريفات الاصطلاحية التي قدمت في هذا المجال نذكر على سبيل المثال أن جريمة الاحتيال " تتمثل في الاستيلاء على الحياة

¹ عبد الرحمن بن عبد الله السند، المرجع نفسه، ص 93.

² رامي متولي القاضي، المرجع نفسه، ص 79.

الكاملة لمال الغير باستعمال وسيلة يشوبها الخداع، تؤدي في النهاية إلى تسليم ذلك المال"¹، كما عرفت أيضا بأنها: "استعمال إحدى وسائل التدليس التي حددها القانون على سبيل الحصر، بقصد حمل المجني عليه على تسليم الجاني مالا مملوكا له نتيجة وقوعه في الغلط"².
قد اختلفت التشريعات في تسمية هذه الجريمة وتنظيمها، كما هو الشأن في القانون الفرنسي الذي تناول لأول مرة مفهوم الطرق الاحتيالية، واعتبر الاحتيال جريمة قائمة بذاتها، حيث نصت المادة 405 على أنه كل من يتوصل إلى سلب مال الغير أو يحاول ذلك يعد مرتكبا لجريمة الاحتيال،³ كما أقر المشرع ظرفا مشددا في حالة ارتكاب هذه الجريمة بانتحال صفة ضابط في الشرطة القضائية أو أحد أعوان السلطة العمومية أو الانتماء إلى جهات رسمية كالعسكرية.⁴

أما المشرع الجزائري فقد تناول جريمة الاحتيال ضمن قانون العقوبات، حيث نصت المادة 372⁵ على أنه كل من توصل إلى استلام أو تلقى أموالا أو منقولات أو سندات أو تصرفات أو أوراقا مالية أو وعودا أو مخالصات أو إبراء من التزامات، أو سعى إلى الحصول على أي منها، وكان ذلك عن طريق الاحتيال بقصد الاستيلاء على كل ثروة الغير أو جزء منها، سواء باستعمال أسماء أو صفات كاذبة أو ادعاء سلطة أو اعتماد مالي وهمي، أو بإيهام الضحية

¹ هيثم حمود الشلبي، إدارة مخاطر الاحتيال في قطاع الاتصالات، دار صفاء للنشر والتوزيع، ط 1، عمان، الأردن، 2009، ص 22.

² عبيد علي، ناصر موفق وآخرون، ماهية جريمة الاحتيال الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، كلية الحقوق، جامعة بغداد، تكريت، ص 336.

³ المرجع نفسه، ص 337.

⁴ طاهر جليل الحبوش، جرائم الاحتيال: الأساليب والوقاية والمكافحة، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، 2006، ص 08.

⁵ المادة 372 من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 71، سنة 2004

بالفوز بشيء أو بوقوع حادث أو واقعة غير حقيقية أو التخويف من حدوثها، يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة مالية تتراوح بين 500 و 20.000 دينار جزائري.

تقوم جريمة الاحتيال على فكرة أساسية تتمثل في استعمال وسائل خادعة تؤدي إلى تضليل الضحية ودفعه إلى تسليم مال أو قيمة مالية برضاه الظاهر، بينما يكون هذا الرضا قائما على وهم أو خطأ ناتج عن تلك الوسائل،¹ وهو ما يميزها عن باقي الجرائم المالية التي تعتمد على الاستيلاء المباشر أو الإكراه، إذ يظهر فيها عنصر الرضا المشوب بالغلط كعنصر أساسي في تحقق الجريمة.

تتجسد هذه الوسائل في صور متعددة، من بينها انتحال صفة غير صحيحة لإضفاء المصداقية على الجاني، أو تقديم وعود كاذبة بإمكانية تحقيق أرباح أو خدمات مالية، أو استعمال مستندات ومعلومات مضللة توهي بوجود معاملات حقيقية، حيث يتم توظيف هذه الأساليب بشكل مدروس يستهدف ثقة الضحية ويستغل ضعف خبرته أو حاجته المالية.²

في السياق الرقمي، تطورت أساليب الاحتيال بشكل ملحوظ مع انتشار الخدمات الإلكترونية، فأصبحت تنفذ عبر منصات رقمية ومواقع مزيفة ورسائل إلكترونية تحمل طابعا رسميا، ما يسمح للجاني بالوصول إلى عدد كبير من الضحايا في وقت قصير دون الحاجة إلى احتكاك مباشر،³ وهو ما زاد من خطورة هذا النوع من الجرائم وصعوبة كشفه.

¹ محمد عبد الرزاق محمد عباس، النظام القانوني لعقد الاشتراك في خدمة الانترنت، دار الفكر والقانون للنشر والتوزيع، مصر، 2016، ص 74.

² خالد زريقات، عقد التجارة الإلكترونية (عقد البيع عبر الانترنت)، دار الحامد للنشر والتوزيع، ط1، الأردن، 2007، ص 72.

³ المرجع نفسه، ص 75.

تتعرض آثار الاحتيال على المؤسسات المالية والأفراد في آن واحد، حيث تؤدي إلى خسائر مالية مباشرة، كما تساهم في زعزعة الثقة في المعاملات الإلكترونية وتضعف الإقبال على الخدمات الرقمية.

الفرع الثاني: تحويل الأموال غير المشروع

يعد هذا السلوك من أخطر صور الاعتداء المالي في البيئة الرقمية، لأنه لا يقتصر على الاستيلاء على الأموال، بل يتجاوز ذلك إلى إعادة توجيهها عبر مسارات مصرفية متعددة بهدف إخفاء مصدرها الحقيقي وإضفاء طابع قانوني ظاهري عليها،¹ وهو ما يجعل تتبعها أكثر تعقيدا مقارنة بباقي الجرائم المالية الأخرى، خاصة مع اعتماد المؤسسات على أنظمة تحويل إلكترونية سريعة وعابرة للحدود.

يقوم هذا الفعل على نقل مبالغ مالية من حساب إلى آخر دون وجه حق، سواء تم ذلك عبر اختراق الأنظمة المصرفية أو باستعمال بيانات مالية تم الحصول عليها بطرق غير مشروعة، أو من خلال استغلال ثغرات في آليات الدفع الإلكتروني، حيث يتم تنفيذ العمليات بشكل يبدو عاديا في الظاهر رغم أنه مبني على أساس غير قانوني.²

تتطور هذه الممارسات عادة عبر عدة مراحل، تبدأ بالحصول على الأموال بطرق غير مشروعة، ثم تمر بمرحلة الإخفاء عبر تمريرها في حسابات وسيطة متعددة، وصولا إلى مرحلة الإدماج داخل الدورة المالية بشكل يجعل تمييزها عن الأموال المشروعة أمرا صعبا،³ وهذا يعكس طابعا تنظيميا يعتمد على التخطيط والتدرج.

¹ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار الكتب القانونية، مصر، 2008، ص 32.

² المرجع نفسه، ص 34.

³ المرجع نفسه، ص 34.

تستعمل في هذا السياق تقنيات رقمية متقدمة مثل الحسابات الوهمية، وخدمات الدفع الإلكتروني غير المباشرة، وأحياناً العملات المشفرة كوسيلة لزيادة صعوبة التتبع، إضافة إلى الاستفادة من السرعة الكبيرة التي تميز التحويلات البنكية الحديثة.

تترتب عن هذه الأفعال آثار مالية وتنظيمية عميقة، إذ تؤدي إلى اختلال في حركة الأموال داخل المؤسسات المالية، كما تضعف القدرة على الرقابة والمطابقة المحاسبية، فضلاً عن الإضرار بسمعة النظام المصرفي ككل،¹ خاصة عندما ترتبط هذه العمليات بشبكات منظمة عابرة للحدود.

تفرض خطورة هذا النوع من السلوك اعتماد آليات رقابية أكثر صرامة، تقوم على تتبع مسار المعاملات بشكل دقيق، وتفعيل أنظمة الإنذار المبكر، إلى جانب تعزيز التعاون بين المؤسسات المالية والهيئات الرقابية، ما يسمح بالحد من فرص استغلال القنوات الرقمية في تنفيذ عمليات غير قانونية وإعادة توجيه الأموال خارج الإطار المشروع.

الفرع الثالث: تزوير المعطيات المالية

يعد تزوير المعطيات المالية من أخطر صور الاعتداء على النظم المعلوماتية داخل المؤسسات المالية، لأنه لا يستهدف مجرد وثائق عادية، بل يمس جوهر البيانات الرقمية التي تُبنى عليها القرارات المحاسبية والمالية، ويندرج هذا السلوك ضمن صور التلاعب غير المشروع بالمعلومات الإلكترونية، حيث يتم تغييرها أو إعادة تشكيلها بما يخالف الحقيقة الاقتصادية للمعاملات،² ولإحاطة هذا الموضوع بشكل منهجي، سيتم التطرق إلى الإطار المفاهيمي للتزوير الرقمي للمعطيات المالية، ثم دراسة أنماط التلاعب داخل السجلات المالية الإلكترونية،

¹ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الرابعة، دار النهضة العربية، مصر، 2006، ص 256.

² المرجع نفسه، ص 257.

وبعدها تحليل آليات التنفيذ داخل البيئة الرقمية، وأخيرا بيان أهم الانعكاسات التنظيمية والمالية الناتجة عنه.

أ- الإطار المفاهيمي للتزوير الرقمي للمعطيات المالية:

يقصد بهذا السلوك كل تدخل غير مشروع يمس المحتوى الرقمي ذو الطابع المحاسبي أو البنكي، من خلال إعادة تشكيله أو تحريفه بما لا يعكس الحقيقة الاقتصادية للمعاملات، حيث يتم إنتاج بيانات مغايرة للواقع يتم اعتمادها داخل الأنظمة المعلوماتية وكأنها صحيحة¹، وهو ما يؤدي إلى خلل في تمثيل الوضع المالي الحقيقي للمؤسسة ويؤثر على دقة التقارير المعتمدة في التسيير واتخاذ القرار، ويتميز هذا النوع من السلوك بكونه يعتمد على بيئة إلكترونية بالكامل دون الحاجة إلى وثائق مادية تقليدية.

ويكتسب هذا المفهوم أهمية خاصة في ظل التحول الرقمي للمؤسسات المالية، حيث أصبحت البيانات هي الأساس في اتخاذ القرار، مما يجعل أي تعديل غير مشروع لها يمس مباشرة بمصداقية النظام المالي ككل ويؤثر على الثقة في المعاملات الإلكترونية.

ب- أنماط التلاعب داخل السجلات المالية الإلكترونية:

يتخذ هذا الفعل عدة مظاهر داخل النظام المعلوماتي للمؤسسة، فقد يظهر في شكل إعادة ضبط الأرقام المحاسبية بما يخدم صورة مالية غير دقيقة، أو إدراج عمليات وهمية ضمن دفاتر الحسابات لإظهار نشاط غير حقيقي، كما يمكن أن يتمثل في حذف أو إخفاء معاملات فعلية بهدف التأثير على التوازن العام للحسابات، إضافة إلى إدخال تعديلات على البيانات التاريخية

¹ عبد الله حسين علي محمود، المرجع نفسه، ص 257.

للمعاملات المالية بما يغير من دلالتها الأصلية ويؤثر على مسارها التحليلي داخل النظام المحاسبي.¹

كما أن خطورة هذه الأنماط تكمن في صعوبة اكتشافها في الوقت الفعلي، خاصة عندما تتم بشكل تدريجي أو عبر صلاحيات داخلية، مما يجعلها أكثر تأثيراً على المدى المتوسط والبعيد، حيث لا تظهر آثارها إلا عند عمليات التدقيق أو المراجعة الشاملة للحسابات.

ج- آليات التنفيذ داخل البيئة الرقمية:

يعتمد هذا السلوك على تقنيات متقدمة تسمح بالتعامل المباشر مع قواعد البيانات الخاصة بالمؤسسة، حيث يتم الولوج إلى النظام عبر حسابات داخلية أو باستغلال ثغرات في منظومة الحماية، كما يمكن استعمال برمجيات مخصصة لإعادة كتابة البيانات أو تعديلها بشكل غير مرئي للمستخدمين العاديين، وفي بعض الحالات يتم توظيف امتيازات وظيفية داخل المؤسسة للوصول إلى المستويات الحساسة من المعلومات²، ما يجعل العملية أكثر تعقيداً وصعوبة في الاكتشاف الفوري.

وتبرز خطورة هذه الآليات في كونها تعتمد على الدمج بين المعرفة التقنية والصلاحيات الإدارية داخل المؤسسة، مما يصعب معه الفصل بين الاستخدام المشروع للنظام والاستغلال غير المشروع له، خاصة في غياب أنظمة رقابة داخلية فعالة أو تحديث مستمر لوسائل الحماية الإلكترونية.

¹ مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية للنشر والتوزيع، مصر، 2011، ص 94.

² المرجع نفسه، ص 94.

د- الانعكاسات التنظيمية والمالية:

-ينتج عن هذا النوع من الممارسات اضطراب في دقة المعلومة المحاسبية، الأمر الذي ينعكس مباشرة على جودة التقارير المالية المعتمدة في التقييم والمراقبة.

وهو ما يؤدي إلى تشويه الصورة الحقيقية للوضع المالي للمؤسسة ويجعل قرارات الإدارة مبنية على معطيات غير دقيقة.

-اتخاذ قرارات غير مبنية على معطيات صحيحة سواء على مستوى الاستثمار أو التسيير الداخلي.

مما قد يترتب عنه خسائر مالية أو سوء توجيه للموارد داخل المؤسسة نتيجة الاعتماد على بيانات مضللة.

-فقدان الثقة في مصداقية المؤسسة لدى الشركاء والمتعاملين.

وهو أثر مباشر وخطير، لأن السمعة المالية للمؤسسة تعتبر من أهم عناصر استمراريته في السوق، وأي خلل فيها ينعكس على علاقاتها التعاقدية والاقتصادية.

-إضعاف فعالية الرقابة الداخلية وزيادة هامش المخاطر المرتبطة بالبيئة الرقمية.¹

إذ أن نجاح عمليات التزوير الرقمي يكشف وجود ثغرات في أنظمة الحماية والرقابة، مما يستدعي إعادة تقييم شامل لآليات الأمن المعلوماتي داخل المؤسسة.

يتضح أن تزوير المعطيات المالية يمثل تهديدا مباشرا لسلامة النظم المعلوماتية داخل المؤسسات المالية، لكونه يضرب دقة البيانات ويؤثر على مصداقية التقارير المعتمدة.

¹ مصطفى محمد موسى، المرجع نفسه، ص 95.

المبحث الثاني: الحماية الجزائية وآليات الوقاية

أمام تصاعد التهديدات الإلكترونية التي تواجه المؤسسات المالية، برزت الحاجة إلى وضع إطار قانوني فعال يضمن تجريم هذه الأفعال ومعاقبة مرتكبيها، إلى جانب اعتماد تدابير وقائية وتقنية تحد من وقوعها وتساعد على كشفها وإثباتها، حيث يشكل التكامل بين الحماية الجزائية والآليات الوقائية أساسا لمواجهة هذا النوع من الجرائم، ومن ثم سيتم في هذا المبحث تناول الحماية الجزائية المقررة للمؤسسات المالية، ثم استعراض آليات الوقاية والإثبات في الجرائم الإلكترونية.

المطلب الأول: الحماية الجزائية للمؤسسات المالية من الجرائم الإلكترونية

في إطار التطور المتسارع الذي عرفته الوسائط الرقمية وتزايد الاعتماد على الأنظمة المعلوماتية في تسير المعاملات المالية، برزت الحاجة إلى تدعيم الإطار القانوني الخاص بحماية هذا القطاع، من خلال إقرار قواعد جزائية واضحة تجرم مختلف الأفعال التي تمس أمن وسلامة المعطيات المالية، وتحدد المسؤوليات المترتبة عنها.

الفرع الأول: التجريم القانوني للجرائم الإلكترونية المالية

يستند التجريم القانوني للجرائم الإلكترونية المالية إلى تحديد دقيق للأفعال التي تمس سلامة الأنظمة المالية الرقمية، حيث انتقل الاهتمام التشريعي من حماية الأموال في صورتها التقليدية إلى حماية المعطيات والأنظمة التي تُدار عبرها المعاملات البنكية الإلكترونية،¹ ويرجع هذا التحول إلى الطبيعة الخاصة للجريمة الإلكترونية التي تعتمد على بيئة غير مادية، تتسم بالسرعة والتطور المستمر، وتسمح بالوصول غير المشروع إلى البيانات المالية أو تعديلها أو تعطيلها دون وجود احتكاك مادي مباشر.

¹ إبراهيم بن داود، أشرف شعت، الاطلاع على البريد الإلكتروني، مجلة دفاتر السياسة والقانون، جامعة ورقلة، الجزائر، المجلد 9، العدد 16، جانفي 2017، ص 456.

يشمل نطاق هذا التجريم مختلف صور السلوك غير المشروع، مثل اختراق الأنظمة المعلوماتية للمؤسسات المالية، أو الاستيلاء على الحسابات البنكية، أو انتحال الهوية الرقمية بغرض تنفيذ عمليات مالية احتيالية، إضافة إلى التلاعب بالمعطيات أو اعتراض التحويلات الإلكترونية أثناء تنفيذها،¹ ويمتد التجريم كذلك إلى الوسائل المستعملة في ارتكاب هذه الأفعال، خاصة البرمجيات الخبيثة وأدوات القرصنة، وهو ما يعكس توجهها قانونيا يربط بين الفعل الإجرامي وأدواته التقنية في إطار واحد متكامل.

تتميز السياسة التشريعية في هذا المجال بطابعها المرن، حيث صيغت النصوص بطريقة عامة تسمح باستيعاب صور جديدة من الاعتداءات الرقمية دون الحاجة إلى تعديل مستمر، وذلك بالنظر إلى التطور السريع لأساليب الجريمة الإلكترونية²، هذا الطابع المرن يقوم على صياغات قانونية واسعة النطاق تضمن قابلية التطبيق على مختلف الأفعال المستجدة في البيئة الرقمية المالية.

يرتبط هذا التجريم ارتباطا مباشرا بحماية استقرار النظام المالي، لأن المساس بالمعطيات أو الأنظمة الإلكترونية يمتد إلى الإضرار بالثقة العامة في المعاملات الرقمية، وهو عنصر أساسي في عمل المؤسسات المالية الحديثة، لذلك فإن التجريم لا يهدف فقط إلى العقاب، بل يسعى إلى تأمين البيئة الرقمية وتقوية موثوقيتها باعتبارها أساس النشاط الاقتصادي المعاصر.

يتضح أن التجريم القانوني للجرائم الإلكترونية المالية يشكل إطارا تنظيميا متقدما يعيد تعريف الجريمة المالية في سياقها الرقمي، من خلال الجمع بين الحماية القانونية للبيانات والأنظمة وبين ضمان استمرارية الثقة في المعاملات الإلكترونية.

¹ أنسام سمير طاهر، جريمة السرقة الإلكترونية، مجلة بابل للعلوم الإنسانية، الجامعة الإسلامية، بابل، العراق، المجلد 27، العدد 5، ديسمبر 2019، ص 523.

² المرجع نفسه، ص 526.

الفرع الثاني: العقوبات المقررة على مرتكبي الجرائم الإلكترونية

تقوم العقوبات المقررة على مرتكبي الجرائم الإلكترونية المالية على مبدأ التناسب بين جسامة الفعل الإجرامي وحجم الضرر الناتج عنه، مع مراعاة خصوصية هذا النوع من الجرائم التي تقع في بيئة رقمية سريعة التطور وتستهدف في الغالب أنظمة مالية حساسة. ويظهر من خلال السياسة التشريعية أن المشرع يعتمد منظومة عقابية مركبة تجمع بين العقوبات الأصلية والتكميلية لضمان فعالية الردع.

تتمثل العقوبات الأصلية أساسا في العقوبات السالبة للحرية، حيث تطبق عقوبة الحبس أو السجن بحسب خطورة الفعل، خاصة في الحالات التي يتضمن فيها الاعتداء اختراقا لأنظمة بنكية أو استيلاء غير مشروع على أموال أو معطيات مالية،¹ ويزداد التشديد كلما ترتب عن الفعل ضرر مالي جسيم أو مساس واسع النطاق بالمؤسسات المالية أو الزبائن.

إلى جانب ذلك تفرض الغرامات المالية باعتبارها وسيلة لتعويض الطابع المالي للجريمة²، حيث تهدف إلى إلحاق ضرر اقتصادي مباشر بالجاني يتناسب مع المكاسب غير المشروعة التي قد يكون حققها من الجريمة، وغالبا ما تحدد هذه الغرامات بشكل مرتفع لضمان عدم تحول الجريمة الإلكترونية إلى نشاط مربح.

أما العقوبات التكميلية فتأخذ أهمية خاصة في هذا المجال، إذ تشمل مصادرة الأدوات والوسائل المستعملة في ارتكاب الجريمة مثل الأجهزة الحاسوبية أو البرمجيات أو الوسائط الرقمية التي استعملت في الاختراق أو التلاعب بالمعطيات،³ كما يمكن أن تتضمن منع الجاني

¹ مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة القانون، جامعة غليزان، الجزائر، المجلد 9، العدد 1، جوان 2020، ص 234.

² المرجع نفسه، ص 235.

³ المرجع نفسه، ص 235.

من ممارسة بعض الأنشطة المهنية المرتبطة بتكنولوجيا الإعلام والاتصال، خصوصا إذا كان الفعل قد ارتكب باستغلال خبرة تقنية أو صفة مهنية.

إن المشرع قد يقر عقوبات إضافية ذات طابع وقائي مثل تقييد الولوج إلى بعض الأنظمة أو فرض رقابة قضائية في حالات معينة، وذلك بهدف الحد من إمكانية العودة إلى ارتكاب نفس الأفعال مستقبلا.

يتضح أن العقوبات المقررة في مجال الجرائم الإلكترونية المالية لا تقتصر على الردع التقليدي، بل تمتد إلى معالجة البعد التقني والاقتصادي للجريمة.

الفرع الثالث: المسؤولية الجزائية للأشخاص الطبيعية والمعنوية

تطرح الجرائم الإلكترونية المالية إشكالية خاصة على مستوى تحديد المسؤولية الجزائية، بالنظر إلى طبيعتها التقنية وتعدد الفاعلين فيها وتداخل الأدوار بين المستخدمين والوسطاء التقنيين والمؤسسات، لذلك اتجهت التشريعات الحديثة إلى توسيع نطاق المسؤولية لتشمل الأشخاص الطبيعية والأشخاص المعنوية على حد سواء.

بالنسبة للأشخاص الطبيعية، تقوم المسؤولية الجزائية متى ثبت أن الفاعل ارتكب فعلا ماديا أو شارك أو ساهم في جريمة تمس الأنظمة المالية الإلكترونية، سواء تم ذلك عن طريق الدخول غير المشروع إلى الأنظمة المعلوماتية، أو التلاعب بالمعطيات البنكية، أو استعمال وسائل تقنية للاحتيال المالي¹، ولا يشترط في هذه المسؤولية أن يكون الفعل مباشرا دائما، بل يمكن أن تتحقق حتى في حالة التحريض أو المساعدة أو تقديم الأدوات التقنية اللازمة لارتكاب الجريمة، ما دام هناك ارتباط سببي بين السلوك والنتيجة الإجرامية.

¹ مصطفى محمد موسى، التحري في جرائم تقنية المعلومات، دار الكتب القانونية، القاهرة، مصر، 2015، ص 88.

أما الأشخاص المعنوية، فقد أصبحت محل مساءلة جزائية في الجرائم الإلكترونية المالية عندما ترتكب الأفعال لحسابها أو باسمها من قبل مسيرها أو موظفيها، أو عندما تسهم بصفة مباشرة أو غير مباشرة في تسهيل ارتكاب الجريمة،¹ ويقوم هذا النوع من المسؤولية على فكرة أن المؤسسة قد تتحول إلى وسيلة لارتكاب الاعتداءات المالية إذا غابت الرقابة الداخلية أو تم استغلال بنيتها الرقمية بشكل غير مشروع.

تترتب عن المسؤولية الجزائية للأشخاص المعنوية مجموعة من الجزاءات التي تتلاءم مع طبيعتها، مثل الغرامات المالية ذات الطابع الردعي، أو الحل في الحالات الخطيرة، أو الغلق المؤقت أو النهائي، أو المنع من ممارسة نشاط معين، أو إخضاعها لرقابة قضائية،² وتهدف هذه التدابير إلى ضمان عدم تحول المؤسسة إلى فضاء خصب لارتكاب الجرائم الإلكترونية أو التستر عليها.

كما تعكس هذه المسؤولية توجهها حديثاً في السياسة الجنائية يقوم على تجاوز المفهوم التقليدي للجريمة المرتبطة بالفرد فقط، نحو نموذج أكثر شمولية يراعي تعقيد البيئة الرقمية وتعدد الفاعلين فيها، مع تعزيز مبدأ عدم الإفلات من العقاب سواء كان الفاعل شخصاً طبيعياً أو معنوياً.

المطلب الثاني: آليات الوقاية والإثبات في الجرائم الإلكترونية

في ظل تعدد صور الاعتداءات الإلكترونية وتطور أساليبها، لم يعد الاكتفاء بالجانب الجزائي كافياً لمواجهة هذه الظاهرة، بل أصبح من الضروري الاعتماد على مجموعة من الآليات الوقائية والتنظيمية والتقنية التي تهدف إلى الحد من وقوع هذه الجرائم قبل حدوثها، إلى جانب تطوير وسائل الإثبات الرقمية التي تسمح بكشفها وتحديد مرتكبيها بدقة.

¹ مصطفى محمد موسى، المرجع نفسه، ص 92.

² يونس عرب، المرجع نفسه، ص 175.

الفرع الأول: التدابير التقنية للوقاية من الجرائم الإلكترونية

تتجلى التدابير التقنية للوقاية من الجرائم الإلكترونية في المؤسسات المالية في جملة من الآليات والإجراءات التي تهدف إلى تعزيز الحماية الرقمية وتقليل مخاطر الاختراق والتلاعب بالمعطيات المالية، ويمكن إبراز أهم هذه التدابير فيما يلي:¹

-أنظمة الحماية الشبكية ومراقبة حركة الشبكات.

-برمجيات مكافحة الفيروسات والبرامج الخبيثة.

-أنظمة كشف ومنع التسلل داخل الشبكات المعلوماتية.

-تقنيات التشفير لحماية البيانات والمعطيات المالية.

-بروتوكولات الاتصال الآمن أثناء تبادل المعلومات.

-أنظمة التحقق متعدد العوامل عند الولوج إلى الحسابات.

-التحديث المستمر للأنظمة والبرمجيات لسد الثغرات الأمنية.

-اختبارات الاختراق الدورية لتقييم مستوى الحماية وكشف نقاط الضعف.

وتجدر الإشارة إلى أن فعالية التدابير التقنية لا تتحقق بمجرد توفرها بشكل منفصل، بل ترتبط بمدى تكاملها داخل منظومة أمنية موحدة تعتمد على التنسيق بين مختلف أدوات الحماية والمراقبة، حيث إن كل تدبير يكمل الآخر في سد الثغرات المحتملة وتقليل فرص الاختراق، مما يجعل الحماية الرقمية عملية مستمرة وليست إجراءات معزولة أو ظرفية.

¹ نائلة عادل محمد فريد قورة، المرجع نفسه، ص 93.

أ- أنظمة إدارة الجدران النارية المتقدمة (Firewall Management):

تعد الجدران النارية من أهم أدوات الحماية، لكنها في صورتها المتقدمة لا تقتصر على المنع فقط، بل تقوم بتحليل حركة البيانات وتصنيفها وفق درجة الخطورة، مما يسمح بفترة دقيقة للاتصالات المشبوهة، وتساعد هذه الأنظمة على مراقبة التدفق الشبكي بشكل لحظي، وبالتالي منع أي محاولة دخول غير مصرح بها قبل وصولها إلى النظام الداخلي.¹

ب- أنظمة المراقبة اللحظية وتحليل السلوك الرقمي (Real-Time Monitoring):

تعتمد هذه الأنظمة على متابعة نشاط المستخدمين داخل النظام المعلوماتي بشكل مستمر، ورصد أي سلوك غير معتاد مثل الدخول في أوقات غير طبيعية أو محاولة الوصول إلى ملفات حساسة، وتكمن أهميتها في أنها تحول دون وقوع الهجوم من خلال اكتشافه أثناء بدايته وليس بعد حدوث الضرر²، مما يعزز القدرة الاستباقية للمؤسسة.

ج- إدارة صلاحيات المستخدمين وتحديد مستويات الوصول:

تقوم المؤسسات المالية بتحديد دقيق لصلاحيات كل مستخدم داخل النظام، بحيث لا يتمكن أي موظف من الوصول إلا إلى البيانات المرتبطة بمهامه فقط، ويؤدي هذا التقييد إلى تقليل المخاطر الداخلية، خاصة تلك الناتجة عن الاستعمال غير المشروع للصلاحيات أو إساءة استخدامها داخل المؤسسة.³

¹ أحمد بن عيسى، الجرائم الإلكترونية وآليات مكافحتها في ظل التطور التكنولوجي، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة قسنطينة 1، الجزائر، 2019، ص 157.

² أحمد بن عيسى، المرجع نفسه، ص 157.

³ المرجع نفسه، ص 157.

د- أنظمة النسخ الاحتياطي واسترجاع البيانات (Backup Systems):

تعتبر هذه الأنظمة من التدابير الحيوية، حيث تسمح بحفظ نسخ دورية من البيانات المالية واسترجاعها عند حدوث أي اختراق أو تلف، وتكمن أهميتها في ضمان استمرارية العمل وعدم فقدان المعلومات الحساسة حتى في حالة التعرض لهجوم سيبراني ناجح.¹

هـ- تقنيات الذكاء الاصطناعي في كشف التهديدات:

أصبحت بعض المؤسسات تعتمد على أنظمة ذكية قادرة على تحليل كميات ضخمة من البيانات لاكتشاف الأنماط المشبوهة تلقائياً، وهذا يسمح بالتنبؤ بالهجمات المحتملة بناء على سلوكيات رقمية سابقة، مما يرفع من مستوى الحماية ويقلل من التدخل البشري المباشر في عمليات المراقبة.²

يتضح أن التدابير التقنية تمثل منظومة متكاملة ومتراصة تهدف إلى تحصين البيئة الرقمية للمؤسسات المالية، من خلال رفع مستوى الأمان السيبراني وتقليل فرص وقوع الجرائم الإلكترونية عبر معالجة المخاطر قبل تحولها إلى اعتداءات فعلية.

الفرع الثاني: الوقاية التنظيمية والإدارية داخل المؤسسات المالية

تعد الوقاية التنظيمية والإدارية داخل المؤسسات المالية مكملًا أساسيًا للتدابير التقنية، إذ لا يتحقق الأمن المعلوماتي بالوسائل التقنية وحدها، بل يستلزم إطاراً تنظيمياً دقيقاً يضبط طريقة العمل داخل المؤسسة ويحدد بدقة صلاحيات الأفراد ومسؤولياتهم، ويهدف هذا الإطار إلى تقليل المخاطر المرتبطة بالعامل البشري، باعتباره أحد أبرز نقاط الضعف التي قد تستغل في ارتكاب الجرائم الإلكترونية المالية.

¹نادية بن يوسف: الأمن المعلوماتي في المؤسسات المالية ودوره في الوقاية من الجرائم الإلكترونية، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة سطيف 1، الجزائر، 2021، ص 231.

² المرجع نفسه، ص 232.

تتمثل أهمية هذا الجانب في كونه يخلق نوعاً من الانضباط المؤسسي داخل البيئة المالية، حيث تتحول الحماية من مجرد أدوات تقنية إلى ثقافة عمل قائمة على الالتزام الداخلي بالقواعد والإجراءات، مما يجعل كل موظف جزءاً من منظومة الحماية وليس مجرد مستخدم للنظام.

تتجلى هذه الوقاية في وضع سياسات داخلية صارمة لأمن المعلومات، تحدد قواعد استعمال الأنظمة الرقمية، وشروط الولوج إلى البيانات المالية، وفق مبدأ تقييد الصلاحيات حسب طبيعة المهام، كما يتم اعتماد آليات دقيقة لتوزيع الاختصاصات بما يمنع تركيز المهام الحساسة في يد واحدة¹، تقادياً لأي استغلال غير مشروع للمعطيات أو التلاعب بالعمليات المالية.

كما أن هذا التوزيع الوظيفي يهدف إلى خلق مبدأ الرقابة المتبادلة داخل المؤسسة، بحيث لا تكون أي عملية مالية خاضعة لشخص واحد فقط، بل تمر عبر مراحل متعددة من التحقق، مما يقلل من احتمالية وقوع التلاعب أو الاختراق الداخلي.

تساهم الرقابة الداخلية في تدعيم هذا الجانب من خلال أجهزة مختصة تتولى متابعة العمليات بشكل مستمر، والكشف عن أي سلوك غير عادي أو نشاط مشبوه قد يشير إلى محاولة اختراق أو احتيال إلكتروني². وتقوم هذه الرقابة على مبدأ التدقيق الدوري للمعاملات، بما يسمح برصد الانحرافات في وقت مبكر ومعالجتها قبل تطورها إلى اعتداء فعلي.

تتميز هذه الرقابة بكونها آلية استباقية وليست مجرد وسيلة كشف بعدية، إذ تعتمد على تحليل سلوك العمليات المالية بشكل مستمر، حيث يساعد على بناء قاعدة بيانات داخلية عن الأنماط الطبيعية للنشاط المالي، وبالتالي سهولة اكتشاف أي انحراف عنها.

¹ حنان ربحان مبارك المضحكي، المرجع نفسه، ص 43.

² المرجع نفسه، ص 45.

كما تحظى مسألة التأهيل والتكوين باهتمام بالغ داخل المؤسسات المالية، حيث يتم تنظيم دورات تدريبية منتظمة لفائدة الموظفين، بهدف رفع مستوى الوعي بالمخاطر السيبرانية، وتطوير قدرتهم على التعرف على أساليب الاحتيال الإلكتروني مثل التصيد أو استغلال الثغرات البشرية، مع ترسيخ ثقافة الأمن الرقمي في بيئة العمل.¹

ويعد العنصر البشري في هذا السياق محور الحماية وليس نقطة الضعف فقط، لأن رفع كفاءته في التعامل مع التهديدات الرقمية يساهم في تقليل نسبة الأخطاء الناتجة عن الجهل أو سوء الاستخدام، مما يعزز فعالية النظام الأمني ككل.

تشمل هذه الوقاية أيضا اعتماد إجراءات تنظيمية تتعلق بحفظ وتوثيق العمليات المالية بشكل دقيق، بما يضمن إمكانية تتبعها عند الحاجة، وينمي مبدأ الشفافية والمساءلة داخل المؤسسة، إضافة إلى ذلك يتم إعداد خطط داخلية للتعامل مع الحوادث السيبرانية، تسمح بالتدخل السريع عند وقوع أي اختراق، والحد من آثاره على النظام المالي.²

يتضح أن الوقاية التنظيمية والإدارية تمثل دعامة أساسية لحماية المؤسسات المالية، من خلال بناء منظومة داخلية منضبطة تقلل من الأخطار البشرية والتنظيمية، وتدعم فعالية الأمن السيبراني في مواجهة التهديدات الإلكترونية المتزايدة.

الفرع الثالث: وسائل الإثبات في الجرائم الإلكترونية المالية

تتميز وسائل الإثبات في الجرائم الإلكترونية المالية بخصوصية ناتجة عن الطبيعة غير المادية للدليل الرقمي، مما يفرض على المنظومة القانونية اعتماد آليات إثبات مرنة تجمع بين القواعد الإجرائية التقليدية والتقنيات الحديثة، بما يسمح بكشف الحقيقة دون الإخلال بضمانات

¹ عبد الفتاح بيومي حجازي، مكافحة جرائم الإنترنت في التشريع العربي والمقارن، دار الكتب القانونية، مصر، 2014، ص 210، ص 73.

² المرجع نفسه، ص 75.

المحاكمة العادلة، وقد أولى المشرع الجزائري هذا الجانب أهمية من خلال نصوص قانونية خاصة تتعلق بالجرائم المرتكبة عبر تكنولوجيات الإعلام والاتصال، وعلى رأسها القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.¹

تعكس هذه الخصوصية تطورا في طبيعة الإثبات الجنائي، حيث أصبح التعامل مع الجريمة المالية الرقمية يتطلب أدوات تحليل متقدمة قادرة على تتبع الأثر الإلكتروني بدل الاعتماد فقط على الوسائل التقليدية.

يمكن إبراز أهم وسائل الإثبات في هذا المجال فيما يلي:

أولا: الدليل الإلكتروني (Electronic Evidence)

يعد الدليل الإلكتروني من أهم وسائل الإثبات في الجرائم المالية الرقمية، ويشمل المعطيات المخزنة أو المتبادلة عبر الأنظمة المعلوماتية، مثل سجلات الدخول، العمليات البنكية الإلكترونية، الرسائل الرقمية، وسجلات الشبكات، وقد اعترف التشريع الجزائري بحجية الدليل الإلكتروني ضمنا من خلال إقراره بمشروعية وسائل الإثبات الحديثة، خاصة في إطار قانون 04²-09 الذي أجاز اعتماد المعطيات المعلوماتية كوسيلة للكشف والإثبات، شريطة ضمان سلامتها وعدم التلاعب بها، كما يدعم هذا التوجه قانون الإجراءات المدنية والإدارية الذي يكرس مبدأ حرية الإثبات في المواد ذات الطابع غير المدني الصرف عند توفر وسائل تقنية موثوقة.

تكمّن قوة هذا الدليل في قابليته للتتبع وإعادة بناء الوقائع الرقمية بشكل دقيق، مما يسمح بتحديد التسلسل الزمني للأحداث وربطها بمصادرها الأصلية داخل النظام المعلوماتي.

¹ نائلة عادل محمد فريد قورة، المرجع نفسه، ص 109.

² المادة 03 من القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، 2009.

كما أن دور الخبير لا يقتصر على التحليل فقط، بل يمتد إلى إعادة تفسير المعطيات الرقمية بلغة قانونية مفهومة للقاضي، مما يربط بين الجانب التقني والبعد القضائي في عملية الإثبات.

ثانيا: الخبرة التقنية القضائية

تلعب الخبرة التقنية دورا مهما في تحليل الأدلة الرقمية، نظرا للطابع المعقد للجرائم الإلكترونية، حيث يتم اللجوء إلى خبراء مختصين في الأمن المعلوماتي لفك الشيفرات، واسترجاع البيانات المحذوفة، وتتبع مصادر الهجمات الإلكترونية، وتحديد هوية الفاعلين عبر الآثار الرقمية،¹ وتكتسي هذه الخبرة طابعا حاسما في تكوين اقتناع القاضي، خاصة عندما تكون الأدلة غير مباشرة أو تحتاج إلى تفسير تقني دقيق.

تبرز أهمية هذه الإجراءات في كونها تمثل مرحلة حاسمة في مسار الإثبات، لأن سلامة جمع الدليل الرقمي تؤثر مباشرة على قيمته القانونية أمام القضاء، وقد تؤدي أي مخالفة فيها إلى استبعاده من ملف الدعوى.

ثالثا: إجراءات التفتيش والحجز الرقمي

تخضع عمليات جمع الأدلة الرقمية إلى إجراءات قانونية دقيقة تتمثل في التفتيش الإلكتروني وحجز الأجهزة والوسائط المعلوماتية، مع ضرورة احترام الضوابط القانونية لضمان مشروعية الدليل، وقد نظم المشرع هذه الإجراءات في إطار قانون 04-09، الذي أجاز للسلطات القضائية والأمنية اتخاذ تدابير تقنية لجمع الأدلة، بشرط احترام حقوق الأفراد وعدم

¹ المادة 05 من القانون رقم 04-09 السابق ذكره.

المساس غير المشروع بخصوصيتهم، بما ينسجم أيضا مع المبادئ الدستورية المتعلقة بحماية الحياة الخاصة وسرية المراسلات، كما ورد في الدستور الجزائري المعدل.¹

يؤكد هذا التكامل أن نجاح الإثبات في هذا النوع من الجرائم لا يعتمد على وسيلة واحدة، بل على انسجام منظومة كاملة تجمع بين التقنية والخبرة والإطار القانوني لضمان الوصول إلى الحقيقة القضائية.

رابعاً: سجلات التتبع الرقمي (Logs) داخل الأنظمة المالية

تعد سجلات التتبع من الوسائل المهمة في كشف الجرائم الإلكترونية المالية، إذ تسجل بشكل تلقائي كل العمليات التي تتم داخل النظام المعلوماتي، مثل تسجيل الدخول، تعديل البيانات، أو تنفيذ التحويلات المالية،² وتسمح هذه السجلات بإعادة تتبع النشاط الرقمي للمستخدمين بدقة، مما يساعد على تحديد اللحظة التي وقع فيها التلاعب والمسار الذي سلكه داخل النظام.

خامساً: الرسائل الإلكترونية والتواصل الرقمي كوسيلة إثبات

يمكن أن تشكل المراسلات الإلكترونية بين الأطراف، سواء عبر البريد الإلكتروني أو تطبيقات الاتصال، دليلاً مهماً في إثبات نية الجريمة أو طريقة تنفيذها، وتكمن أهميتها في أنها تعكس الجانب السلوكي والتواصلي للفاعل³، مما يساعد على ربط الأفعال التقنية بالسياق الإجرامي العام.

¹ المادة 47 من الدستور الجزائري المعدل لسنة 2020، الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 82، الصادرة بتاريخ 30 ديسمبر 2020.

² بخوش فاطمة الزهراء، الجرائم المعلوماتية ووسائل إثباتها في التشريع الجزائري، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، الجزائر، 2019، ص 87.

³ حنان ريجان مبارك المضحكي، المرجع نفسه، ص 53.

تكتسي المراسلات الإلكترونية أهمية خاصة في المجال الجنائي المالي، باعتبارها وسيلة تعكس التفاعل المباشر بين الأطراف داخل الفضاء الرقمي، حيث يمكن أن تتضمن تعليمات تنفيذ عمليات مالية، أو اعترافات ضمنية، أو اتفاقات غير مشروعة يصعب إثباتها بالوسائل التقليدية، كما أن تحليل محتوى هذه الرسائل يساعد على فهم النية الإجرامية وربطها بالفعل المادي، إضافة إلى إمكانية تحديد تسلسل التواصل بين الأطراف المعنية.

سادسا: الأدلة المستخرجة من أجهزة التخزين المحمولة

تشمل هذه الوسيلة البيانات الموجودة على الحواسيب والأقراص الصلبة والهواتف الذكية، حيث يمكن استخراج ملفات أو آثار رقمية تدل على عمليات التلاعب المالي، وتتميز هذه الأدلة بقدرتها على كشف الأنشطة المخفية حتى بعد حذفها ظاهريا، من خلال تقنيات الاسترجاع والتحليل الجنائي الرقمي.

تعد الأجهزة الرقمية مثل الحواسيب والهواتف والأقراص الصلبة خزانا مهما للمعلومات التي قد تحمل آثارا مباشرة أو غير مباشرة للجريمة، إذ يمكن أن تحتوي على ملفات محذوفة، أو برامج مستخدمة في التلاعب، أو نسخ احتياطية لعمليات مالية غير مشروعة،¹ وتبرز أهمية هذه الأدلة في كونها قابلة للاسترجاع عبر تقنيات متخصصة، حتى بعد محاولة إخفائها أو إتلافها.

¹ بخوش فاطمة الزهراء، المرجع نفسه، ص 87.

سابعاً: البصمة الرقمية للمستخدم (Digital Footprint)

تتمثل في الأثر الذي يتركه المستخدم أثناء تفاعله مع الأنظمة المعلوماتية، مثل عناوين IP وسجل التصفح ونمط الاستخدام،¹ وتساعد هذه البصمة في تحديد هوية الفاعل وربط نشاطه الرقمي بسلوك معين داخل النظام، مما يجعلها عنصراً مساعداً في بناء القناعة القضائية.

يتضح أن وسائل الإثبات في الجرائم الإلكترونية المالية تقوم على مزيج دقيق بين الدليل الرقمي والخبرة التقنية والإجراءات القانونية المنظمة لجمعه.

¹بخوش فاطمة الزهراء، المرجع نفسه، ص 87.

خلاصة الفصل:

تناول هذا الفصل صور الجرائم الإلكترونية الموجهة ضد المؤسسات المالية من خلال إبراز مختلف الأفعال غير المشروعة التي تمس أمنها المعلوماتي واستقرارها المالي، حيث تطرق إلى جرائم الاعتداء على أنظمة المعلومات المالية مثل الاختراق، وتعطيل الأنظمة، وسرقة البيانات المصرفية، إضافة إلى الجرائم الإلكترونية المالية كعمليات الاحتيال الإلكتروني، وتحويل الأموال بطرق غير مشروعة، وتزوير المعطيات المالية، كما تم التطرق إلى الآليات القانونية والجزائية المقررة لحماية هذه المؤسسات، إلى جانب الوسائل الوقائية والإثباتية التي تهدف إلى الحد من هذه الجرائم وكشف مرتكبيها، ويُستنتج من ذلك أن مواجهة الجرائم الإلكترونية المالية تتطلب تكاملاً بين الحماية الجزائية والإجراءات التقنية والتنظيمية لضمان أمن النظام المالي واستقراره.

خاتمة

يتضح من خلال هذه الدراسة أن الجرائم الإلكترونية الموجهة ضد المؤسسات المالية أصبحت تشكل أحد أخطر التحديات التي تواجه الأنظمة القانونية والاقتصادية في العصر الرقمي، وذلك بالنظر إلى تطور أساليب ارتكابها واعتمادها على تقنيات متقدمة تسمح بالاختراق والتلاعب بالأنظمة المعلوماتية والبيانات المالية، وقد أبرزت الدراسة أن هذا النوع من الجرائم يتميز بطابع خاص يجمع بين التعقيد التقني والامتداد العابر للحدود، مما يجعل مكافحته تتطلب مقاربة قانونية وقضائية وتقنية متكاملة، كما تبين أن المشرع الجزائري قد سعى إلى مواكبة هذه التحولات من خلال إرساء منظومة قانونية تهدف إلى حماية الأنظمة المعلوماتية وتعزيز الأمن المالي، غير أن فعالية هذه المنظومة تبقى مرتبطة بمدى تطبيقها العملي وقدرتها على مجاراة التطور المستمر لوسائل الإجرام الإلكتروني.

وتجدر الإشارة كذلك إلى أن هذه الظاهرة لا تقتصر آثارها على الجانب المالي فقط، بل تمتد لتشمل فقدان الثقة في الأنظمة المصرفية الرقمية وإضعاف مصداقية المؤسسات المالية، مما ينعكس سلبا على الاستقرار الاقتصادي العام، كما أن تعقيد هذا النوع من الجرائم وتطور أدواته يفرض على مختلف الفاعلين في المجال المالي والقانوني ضرورة تبني مقاربة وقائية تعتمد على اليقظة المستمرة وتحديث آليات الحماية بشكل دوري، إضافة إلى تعزيز الوعي الرقمي لدى المستخدمين باعتبارهم الحلقة الأساسية في منظومة الأمن المعلوماتي.

وتوصلت هذه الدراسة إلى عدة نتائج نبرزها فيما يلي:

-تبين أن الجرائم الإلكترونية الموجهة ضد المؤسسات المالية تتسم بالتطور المستمر وتعدد أساليب ارتكابها، مما يزيد من صعوبة ضبطها قانونيا.

-أظهر المشرع الجزائري اهتماما متزايدا بحماية الأنظمة المعلوماتية من خلال إدراج نصوص عقابية وتنظيمية خاصة.

-رغم وجود إطار قانوني، إلا أن التطبيق العملي يواجه صعوبات تقنية مرتبطة بإثبات الجريمة وتحديد هوية الجاني.

-تعتمد المؤسسات المالية بشكل كبير على الأنظمة الرقمية، مما يجعلها أكثر عرضة للاختراق والاحتيال الإلكتروني.

-يلعب القضاء دورا مهما في تكييف النصوص القانونية مع الوقائع المستجدة في المجال الرقمي.

-تظل فعالية الحماية الجزائية رهينة بتطور وسائل التحقيق الرقمي وتعزيز الكفاءات المتخصصة.

ومن بين الاقتراحات والتوصيات نذكر:

-ضرورة تحديث التشريعات الوطنية بشكل مستمر لمواكبة التطور السريع للجرائم الإلكترونية.

-تعزيز التعاون بين المؤسسات المالية والهيئات الأمنية لتبادل المعلومات حول التهديدات السيبرانية.

-دعم التكوين المتخصص للقضاة وأعوان الضبطية القضائية في مجال الجرائم المعلوماتية.

-تطوير البنية التحتية التقنية للمؤسسات المالية لتعزيز أنظمة الحماية والوقاية.

-تشجيع البحث العلمي في مجال الأمن السيبراني والقانون الرقمي.

-تفعيل آليات الرقابة الداخلية داخل المؤسسات المالية للحد من مخاطر الاختراق والاحتيال.

-تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ذات الطابع العابر للحدود.



قائمة المصادر والمراجع



أولاً: قائمة المصادر والمراجع

1-النصوص القانونية:

أ-الدستور:

-الدستور الجزائري المعدل لسنة 2020، الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 82، الصادرة بتاريخ 30 ديسمبر 2020.

ب-القوانين:

-الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

-القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 71، سنة 2004.

-القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات، ج ر، العدد 84، 2006.

-القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، العدد 47، 2009.

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

-القانون رقم 16-02 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات، ج ر، العدد 39، 2016.

-القانون رقم 17-07 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية، ج ر، العدد 20، 2017.

2-الكتب:

أ-الكتب العامة:

-أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة، دار النهضة العربية، ط1، القاهرة، مصر، 2006.

-بن مكي نجا، السياسة الجنائية لمكافحة جرائم المعطيات المعلوماتية، دار الخلدونية، الجزائر، 2017.

-جمال جويدان الجمل، دراسات في الأسواق المالية والنقدية، دار الصفاء للنشر والتوزيع، ط1، عمان، 2002.

-هيثم حمود الشلبي، إدارة مخاطر الاحتيال في قطاع الاتصالات، دار صفاء للنشر والتوزيع، ط1، عمان، الأردن، 2009.

-محمد عنتر أحمد، الإدارة المالية والاستثمار، الأكاديمية العربية للمعارف المالية والمصرفية، ط1، عمان، 2009.

-محمد فواز محمد المطالقة، الوجيز في عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2015.

- محمد عبد الرزاق محمد عباس، النظام القانوني لعقد الاشتراك في خدمة الانترنت، دار الفكر والقانون للنشر والتوزيع، مصر، 2016.
- محمد حجازي، جرائم الحاسب الآلي والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2008.
- خالد زريقات، عقد التجارة الإلكترونية (عقد البيع عبر الانترنت)، دار الحامد للنشر والتوزيع، ط1، الأردن، 2007.
- توماس ماير، جيمس إسدوستيري، ترجمة أحمد عبد الخالق، النقود والبنوك والاقتصاد، دار المريخ للنشر، 2002.
- طاهر جليل الحبوش، جرائم الاحتيال: الأساليب والوقاية والمكافحة، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، 2006.
- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجات للطباعة والتجليد، ط1، مصر، 2009.
- عبد الغفار حنفي، رسمية زكي قرياصة، البورصات والمؤسسات المالية، الدار الجامعية، الإسكندرية، 2002.
- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، دار الوراق، ط1، بيروت، لبنان، 2004.
- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002.

-عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

-عبد الفتاح بيومي حجازي، مكافحة جرائم الإنترنت في التشريع العربي والمقارن، دار الكتب القانونية، مصر، 2014.

-سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته -صوره- حجته في الإثبات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ط2، 2006.

-نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2005.

-حنان ربحان مبارك المضحكي، الجرائم المعلوماتية -دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2014.

ب-الكتب المتخصصة:

-أحمد خليفة الملط، الجرائم المعلوماتية-دراسة مقارنة، دار الفكر الجامعي، ط2، الإسكندرية، مصر، 2006.

-أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، ط2، الجزائر، 2007.

-أحمد عبد الكريم سلامة، الجرائم الإلكترونية وأمن المعلومات، دار النهضة العربية، القاهرة، 2012.

-أحمد عبد الله عبد الكريم، جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، مصر، 2015.

- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة)، دار البلدية، ط1، عمان، الأردن، 2007.
- د. غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، 2016.
- د. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر، 2019.
- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار الكتب القانونية، مصر، 2008.
- مصطفى محمد موسى، التحري في جرائم تقنية المعلومات، دار الكتب القانونية، القاهرة، مصر، 2015.
- محمود أحمد طه، الحماية الجنائية لنظم المعلومات، دار النهضة العربية، القاهرة، مصر، 2012.
- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الرابعة، دار النهضة العربية، مصر، 2006.
- عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الإلكترونية-دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية، ط1، القاهرة، مصر، 2012.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2010.
- رامي متولي القاضي، مكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2011.

3- الأطروحات والرسائل الجامعية:

أ- أطروحات الدكتوراه:

- أحمد بن عيسى، الجرائم الإلكترونية وآليات مكافحتها في ظل التطور التكنولوجي، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة قسنطينة 1، الجزائر، 2019.

- بخوش فاطمة الزهراء، الجرائم المعلوماتية ووسائل إثباتها في التشريع الجزائري، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، الجزائر، 2019.

- بن قبيلة زين الدين، أثر التطور المالي على النمو الاقتصادي في الجزائر، رسالة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة تمساف، 2015-2016.

- نادية بن يوسف: الأمن المعلوماتي في المؤسسات المالية ودوره في الوقاية من الجرائم الإلكترونية، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة سطيف 1، الجزائر، 2021.

- سلسبيل بن سماعيل، المسؤولية الجزائية للمؤسسات المالية، أطروحة دكتوراه في القانون العام، تخصص قانون عام اقتصادي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2020-2021.

ب- رسائل ماجستير:

- أحمد بن عيسى، جرائم الاختراق الإلكتروني في التشريع الجزائري، رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2019-2020.

-بن عزوز عبد الرحمن، دور الوساطة المالية في تنشيط سوق الأوراق المالية مع الإشارة لحالة بورصة تونس، مذكرة ماجستير، تخصص إدارة عامة، كلية العلوم الاقتصادية والإدارية، جامعة قسنطينة، 2011-2012.

-عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013.

4-المقالات العلمية

-أنسام سمير طاهر، جريمة السرقة الإلكترونية، مجلة بابل للعلوم الإنسانية، الجامعة الإسلامية، بابل، العراق، المجلد 27، العدد 5، ديسمبر 2019.

-أ.د. بشير علوان حمد، "دور المؤسسات المالية في تحفيز النشاط الاقتصادي في ظل الاقتصاد المعولم"، مجلة دراسات محاسبية ومالية، المجلد الرابع، العدد 19، الفصل الثاني، جامعة بغداد، المعهد العالي لدراسات المحاسبية والمالية، 2012.

-إبراهيم بن داود، أشرف شعت، الاطلاع على البريد الإلكتروني، مجلة دفاتر السياسة والقانون، جامعة ورقلة، الجزائر، المجلد 9، العدد 16، جانفي 2017.

-رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، المجلد 16، العدد 41، 2018.

-مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة القانون، جامعة غليزان، الجزائر، المجلد 9، العدد 1، جوان 2020.

-مقلاتي مونة مشري راضية، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، المجلد 6، العدد 01، 2021.

-فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والإقتصادية، كلية الحقوق، جامعة عين شمس، مصر، السنة الرابعة والأربعون، العدد 2، 2002.

شایل نوال، الجريمة الإلكترونية في التشريع الجزائري، مجلة سوسيوولوجيا، المجلد 6، العدد 2، 2017.

-عبيد علي، ناصر موفق وآخرون، ماهية جريمة الاحتيال الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، كلية الحقوق، جامعة بغداد، تكريت.

5-المواقع الإلكترونية:

-عبد الحميد بلعباس، "أساليب حماية الوثائق الإلكترونية في ضوء التوقيع الإلكتروني الجزائري رقم 06 الصادر بتاريخ 10 فبراير 2015: دراسة مقارنة"، جامعة محمد بوضياف، المسيلة، ص 168، مقال منشور على الموقع الإلكتروني <https://www.asjp.cerist.dz>

-يونس عرب، جرائم الكمبيوتر و الإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، بحث منشور على الموقع الآتي: <https://www.abhatoo.net.Ma>

ثانيا: قائمة المراجع باللغة الفرنسية

Ouvrages :

-Frédérique chopin, Les politiques publiques de lutte contre la cybercriminalité, Actualité Juridique Pénal, Editions Dalloz, 2009.

-Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader,Beyrouth,Liban,2004.

فهرس المحتويات:

شكر وتقدير

إهداء

مقدمة 1-2-3

الفصل الأول: الإطار المفاهيمي والقانوني للجرائم الإلكترونية 04

المبحث الأول: الإطار المفاهيمي للجرائم الإلكترونية والمؤسسات المالية 05

المطلب الأول: مفهوم الجرائم الإلكترونية وخصائصها وتمييزها عن الجرائم
المعلوماتية..... 05-13

المطلب الثاني: مفهوم المؤسسات المالية وأنواعها ودورها في النظام المالي 13-19

المبحث الثاني: الإطار القانوني للجرائم الإلكترونية في المجال المالي..... 19

المطلب الأول: التنظيم القانوني للجرائم الإلكترونية في التشريع الجزائري 19-24

المطلب الثاني: المستند الإلكتروني والتوقيع الإلكتروني كوسائل في المعاملات المالية ()
المستند الإلكتروني كأداة قانونية فقط)..... 24-28

خلاصة الفصل 29

الفصل الثاني: صور الجرائم الإلكترونية الموجهة ضد المؤسسات المالية وآليات
مكافحتها..... 30

المبحث الأول: صور الجرائم الإلكترونية الماسة بالمؤسسات المالية..... 32

المطلب الأول: جرائم الاعتداء على أنظمة المعلومات المالية الاختراق..... 32-34

35-34.....	تعطيل الأنظمة
37-35.....	سرقة البيانات المصرفية
37.....	المطلب الثاني: الجرائم الإلكترونية المالية
40-37.....	الاختيال الإلكتروني
41-40.....	تحويل الأموال غير المشروع
44-41.....	تزوير المعطيات المالية
45.....	المبحث الثاني: الحماية الجزائية وآليات الوقاية
49-45.....	المطلب الأول: الحماية الجزائية للمؤسسات المالية من الجرائم الإلكترونية
63-49.....	المطلب الثاني: آليات الوقاية والإثبات في الجرائم الإلكترونية
65.....	خلاصة الفصل
68-67.....	خاتمة
77-70.....	قائمة المصادر والمراجع

ملخص الدراسة:

تتناول هذه الدراسة موضوع الجرائم الإلكترونية الموجهة ضد المؤسسات المالية من خلال تحليل الإطار المفاهيمي والقانوني لهذه الجرائم، وبيان مختلف صورها وخصائصها، إضافة إلى دراسة الآليات القانونية المعتمدة في التشريع الجزائري لحماية المؤسسات المالية من الاعتداءات الإلكترونية، كما تسلط الضوء على أهم الوسائل التقنية والقانونية المستعملة في الوقاية من هذه الجرائم وإثباتها، مع إبراز التحديات التي تعيق فعاليتها في الواقع العملي، في ظل التطور السريع للتقنيات الرقمية وتزايد الاعتماد على الأنظمة المعلوماتية في القطاع المالي.

الكلمات المفتاحية:

الجرائم الإلكترونية، المؤسسات المالية، الحماية القانونية، الأنظمة المعلوماتية، الأمن السيبراني.

Summary:

This study addresses cybercrimes targeting financial institutions by analyzing their conceptual and legal framework, identifying their various forms and characteristics, and examining the legal mechanisms adopted in Algerian legislation to protect financial institutions from cyberattacks. It also highlights the main technical and legal tools used for preventing and proving such crimes, while shedding light on the practical challenges that limit their effectiveness in light of the rapid development of digital technologies and the increasing reliance on information systems in the financial sector.

Keywords:

Cybercrimes, financial institutions, legal protection, information systems, cybersecurity.