

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق



الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

الرقم التسلسلي:.....

مذكرة بعنوان:

المصارف الرقمية والتحديات القانونية في مكافحة

غسل الأموال

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

إشراف الأستاذ:

إعداد الطالب (ة):

- أ.د/عبدلي نزار

-صالح آية

-العيادي خلود

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
بوعشة كمال	أستاذ محاضراً	الشاذلي بن جديد - الطارف	رئيساً
عبدلي نزار	أستاذ التعليم العالي	الشاذلي بن جديد - الطارف	مشرفاً ومقرراً
العمري زقار مونية	أستاذ محاضر ب	الشاذلي بن جديد - الطارف	ممتحناً

السنة الجامعية: 2026/2025

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



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

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

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): محمد الحبيب آية

الحامل لبطاقة التعريف الوطنية رقم: 11.000.12.3.000.4.1.9.000.4

الصادرة بتاريخ: 2020 / 03 / 15

عن دائرة: الطارف

المسجل بقسم: الحقوق والمكلف بإنجاز مذكرة تخرج ماستر

عنوانها: المصارف الرقمية والتكنولوجيا القانونية في مكافحة
غسل الأموال

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

التاريخ: 2020/06/09

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق



Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

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

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): العيادي خالد

الحامل لبطاقة التعريف الوطنية رقم: 11 00 30 8 4 100 30 900 06

الصادرة بتاريخ: 13 08 2023

عن دائرة: الشاذلي بن جديد

المسجل بقسم: الحقوق والعلوم السياسية والمكلف بإنجاز مذكرة تخرج ماستر

عنوانها: اعلم اني اوافق على الالتزام بقواعد النزاهة العلمية في

مكافحة غسل الأموال

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

التاريخ: 2026 / 06 / 09

إمضاء المعني

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الشكر

الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام
على أشرف المرسلين نتقدم بجزيل الشكر والعرفان إلى أستاذنا المشرف "عبدلي
نزار"، الذي تفضل بالإشراف على هذا البحث، ولم ييخل علينا بتوجيهاته القيمة
ونصائحه السديدة التي كانت لنا طيلة فترة إعداد
المذكرة كما نتقدم بالشكر إلى أعضاء لجنة المناقشة الموقرين لتفضلهم بقبول تقييم .
هذا العمل
المتواضع وكل من ساهم من قريب أو من بعيد في هذه المذكرة لتكون على ما هو
عليها اليوم.

الاهداء

من قال أنا لها نالها، وأنا لها وان ابت رغما عنها أتيت بها
لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون لم يكن الحلم قريباً ولا الطريق كان مخفوفاً بالتسهيلات
الكنى فعلتها ونلتها

الى الذي زين اسمي بأجمل الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل من علمنى أن الدنيا
كفاح وسلاحه العلم والمعرفة داعمي الاول في مسيرتي وسندي وقوتي وملاذي بعد الله " إلى فخري
واعترازي

أبي محمد.

إلى من جعل الله الجنة تحت أقدامها واحتضني قلبها قبل يدها وسهلت لي الشدائد بدعائها إلى
القلب الحنون والشمعة التي كانت لي في الليالي المظلمات سر قوتي ونجاحي

أمي عبلة

إلى من جعل الله الجنة تحت أقدامها واحتضني قلبها قبل يدها وسهلت لي الشدائد بدعائها إلى
القلب الحنون والشمعة التي كانت لي في الليالي المظلمات سر قوتي ونجاحي
إلى ضلعي الابت وأمان ايامي الى من شددت عضدي بهم فكانوا لي يناييع ارتوي منها إلى خيرة
أيامي وصوفتها إلى قرة عيني. إخوتي ايناس وبحر الزين

إلى زميلتي وشريكتي في هذا العمل

أهديك ثمرة هذا الجهد المتواضع، تقديرًا لكل لحظات التعب والاجتهاد التي تقاسمناها معًا، ولكل دعم

وتشجيع كان دافعًا لنا لإتمام هذه المذكرة

أهديكم هذا الإنجاز وثمره نجاحي الذي لطالما تمثيته ها أنا اليوم أكملت وأتممت أول ثمراته بفضل
سبحانه وتعالى فالحمد لله على ما وهبني.

صالحى اية

الاهداء

ما سلكنا البدايات إلا بتسييره وما بلغنا النهايات إلا بتوفيقه وما حققنا الغايات إلا بفضلله،
فالحمد لله الذي أوفقني لثمين هذه الخطوة في مساري الدراسي.

أهدي ثمرة نجاحي وتخرجي إلى من وهبني الحياة والأمل والنشأة على شغف الإطلاع والمعرفة
ومن علمني أن أرتقي سلم الحياة بحكمة وصبر برا وإحسانا، ووفاءلهما والذي العزيز
"الهادي" ووالدتي العزيزة "جميلة"، حفظهما الله وأطال عمرهما، للتي كان لها ميزة كبيرة في
تشجيعي و تحضيري ملاذي الأول و الأخير أختي العزيزة «شيماء دانيا»

العيادي خلود

قائمة المختصرات

قائمة المختصرات باللغة العربية:

مجلد	م
عدد	ع
صفحة	ص
من صفحة الي صفحة	ص ص
الجريدة الرسمية	ج ر
الجريدة الرسمية للجمهورية الجزائرية	ج ر ر ز
القانون التجاري الجزائري	ق ت ج

قائمة المختصرات باللغة الأجنبية:

Electronica know your Customer	E-kyc
Know your Customer	kyc
One -time password	otp
Cellule de traitement du renseignement financier	CTRF
Application programming intrefac	ApL
Numéro	N°
Page	P

مقدمة

مقدمة:

تعد المصارف أحد أهم الركائز الأساسية التي يقوم عليها الإقتصاد الوطني لأي دولة، فهي تمثل شريان الحياة الإقتصادية لما لها من دور فعال في دفع عجلة التنمية الإقتصادية، حيث يعمل هذا النوع من المؤسسات المالية على توفير خدمات مصرفية متاحة بناء على متطلبات عملائها، إلا أنه وتماشيا مع التطورات المعلوماتية سعت المصارف إلى الإستفادة من هذه التطورات لإنتاج خدمات مصرفية مستحدثة تمتاز بتنوع الخدمات وسهولتها.

نتيجة الثورة الرقمية التي شهدتها العالم في العقود الأخيرة، والتي شملت جميع جوانب الحياة الإقتصادية والإجتماعية من بينها القطاع المصرفي الذي بات يعمل على تحقيق كفاءة إقتصادية والبحث عن فرص لتقديم خدمات مصرفية بأسهل وأفضل الطرق، هذا ما ساهم في ظهور المصارف الرقمية كنموذجا مبتكرا يعتمد على التكنولوجيا ويعمل عبر منصات رقمية.

إلا أنه و بالنظر إلى البيئة الرقمية التي تعمل من خلالها المصارف الرقمية، قد تجعلها تواجه تحديات وتهديدات كبيرة، من خلال إمكانية استغلالها للتطورات التقنية في ارتكاب الجرائم المالية أبرزها جريمة غسل الأموال الإلكتروني، التي اتخذت من الوسائط الإلكترونية كأداة لإضفاء المشروعية على مصادر الأموال غير المشروعة، هذا ما أدى إلى ضرورة فرض الرقابة على المصارف الرقمية لمكافحة جرائم غسل الأموال و التي لا تتحقق إلا بتوحيد الجهود الدولية في تبني الآلية الدولية للحد من انتشار هذه الجرائم في البيئة المصرفية الرقمية.

تكتسي هذه الدراسة أهمية بالغة، فمن الناحية العلمية يتجلى دور هذه الدراسة خاصة في ظل التطور السريع الذي يشهده القطاع المصرفي وظهور المصارف الرقمية التي تعد نموذجا تطبيقيا يعكس التطورات الخدمائية المصرفية الحديثة، مما أدى إلى تنامي جرائم غسل الأموال ، حيث تعالج هذه الدراسة التحديات القانونية والرقابية التي تواجه المصارف الرقمية في مكافحة جرائم غسل الأموال.

أما من الناحية العملية، تمثل هذه الدراسة مساهمة عملية تهدف إلى توعية العملاء المتعاملين مع المصارف الرقمية بمخاطر غسل الأموال التي ترتكب في البيئة الرقمية.

تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف، إذ يمكن تلخيص أبرزها فيما يلي:

- التعرف على المصارف الرقمية و ما يميزها عن المصارف التقليدية .
- التحديد الدقيق لمفهوم غسل الأموال الإلكتروني .
- تسليط الضوء على أن ارتكاب جرائم غسل الأموال يكون عن طريق استغلال الوسائل الحديثة .
- تحديد المسؤولية القانونية للمصارف الرقمية في مكافحة جرائم غسل الأموال مع الإشارة إلى الفجوات التي تعترضها.

من الأسباب التي دفعتنا لاختيار موضوع المصارف الرقمية والتحديات القانونية في مكافحة غسل الأموال، نجد أسباب موضوعية وأخرى ذاتية، أما الأسباب الموضوعية فتتمثل في زيادة الإهتمام والوعي الدولي بمخاطر جرائم غسل الأموال المرتكبة عبر المصارف الرقمية والسعي إلى توحيد الجهود لمكافحةها، ناهيك عن حداثة موضوع المصارف الرقمية وضعف الأنظمة الرقابية، مما جعلها عرضة للتهديدات الإجرامية. أما بالنسبة للأسباب الذاتية فتكمن في الميل لهذه الدراسة والرغبة في فهمها، بالإضافة إلى الإهتمام الشخصي لمعرفة كيفية استغلال الخدمات المصرفية الرقمية في ارتكاب جرائم غسل الأموال، ومعرفة دورها في التصدي لهذه الجرائم.

من خلال ما سبق، فإن إشكالية هذه الدراسة تتمثل في:

كيف ساهمت المصارف الرقمية في مكافحة جرائم غسل الأموال المرتكبة عبر منصاتها الرقمية؟

وحتى يتسنى لنا التحكم في مختلف جوانب الموضوع، إرتأينا تجزئة الإشكالية الرئيسية إلى أسئلة فرعية، على النحو التالي:

- 1- ما المقصود بالمصارف الرقمية؟ وكيف ساهمت في تطوير جرائم غسل الأموال؟
- 2- فيما تكمن الإجراءات التي إتخذتها المصارف الرقمية في مواجهة جرائم غسل الأموال؟ وما هي الثغرات التي واجهتها؟

للإجابة عن هذه الإشكالية إرتأينا إلى إتباع المنهجين الوصفي والتحليلي، حيث تم الاعتماد على المنهج الوصفي نظرا لملائمته لطبيعة الموضوع، إذ تم توظيفه لعرض الإطار المفاهيمي للمصارف الرقمية و وصف مكونات وصور جريمة غسيل الأموال، كما تم الاعتماد على المنهج التحليلي في تحليل النصوص القانونية و التنظيمية ذات الصلة بموضوع الدراسة.

ومن خلال دراستنا لهذا الموضوع واجهتنا صعوبات نذكر منها :

- حداثة الموضوع نسبيا .

- عدم تطرق المشرع الجزائري لتعريف جرائم غسيل الأموال الإلكتروني.

بناء على ما سبق وتماشيا مع إشكالية البحث، قمنا بتقسيم خطة هذا الموضوع إلى فصلين، خصص الفصل الأول لدراسة الإطار المفاهيمي للمصارف الرقمية وتطور غسيل الأموال ويشمل هذا الفصل على مبحثين، تناول المبحث الأول مفهوم المصارف الرقمية، في حين عالج المبحث الثاني تطور جرائم غسيل الأموال في عصر البيئة الرقمية. في المقابل جاء الفصل الثاني تحت عنوان: التزام المصارف الرقمية بمكافحة غسل الأموال بين المسؤولية القانونية و الفجوات العملية، حيث تضمن هذا الفصل مبحثين، تناول المبحث الأول المسؤولية القانونية للمصارف الرقمية في مكافحة غسيل الأموال، بينما تطرق المبحث الثاني للفجوات أو الثغرات التي تهدد مهام المصارف الرقمية في مكافحة غسيل الأموال.

الفصل الأول:

الإطار المفاهيمي للمصارف الرقمية ومخاطر غسل الأموال

تمثل المصارف أحد أهم الركائز الأساسية التي تقوم عليها كافة الإقتصاديات الوطنية ، لما لها من دور بارز في دعم التنمية الإقتصادية للدول، إلا أنه و نظرا لتسارع وتيرة الابتكار التكنولوجي الذي أدى إلى بروز التحول الرقمي و الذي أصبح ضرورة تملّحها متطلبات العصر الحديث والتي أوجدت العديد من التغيرات في كافة القطاعات ومن أبرزها القطاع المصرفي ، حيث أن مفهوم المصارف تطور من المصارف التقليدية التي تعتمد على الكيان المادي و الموقع الجغرافي إلى مصارف رقمية ليس لها كيان مادي ملموس و تقوم بكافة عملياتها المصرفية بسرعة و كفاءة و أقل تكلفة عن طريق إستخدام الوسائل التكنولوجية الحديثة ، مثل شبكة الأنترنت و وسائل الإتصال الحديثة كالحاسوب...إلخ.

ساهم تطور المصارف و بروز المصارف الرقمية بظهور وسائل وأساليب تكنولوجية حديثة، كظهور بطاقات الدفع الإلكتروني من شيكات و بطاقات إئتمانية، العملات المشفرة، والتي ساهمت بدورها في تطوير الخدمات المالية الرقمية، إلا أنه وعبر هذه الوسائل المصرفية المستحدثة وجدت الجرائم الإلكترونية أبرزها جرائم غسيل الأموال الإلكتروني طريقها للإنتشار أكثر، حيث إستفاد منها غاسلو الأموال في تطوير أنشطتهم الإجرامية.

نسعى من خلال هذا الفصل إلى إستعراض: الإطار المفاهيمي للمصارف الرقمية و مخاطر غسل الأموال، والذي تم تقسيمه إلى مبحثين:

- المبحث الأول: ماهية المصارف الرقمية
- المبحث الثاني: تطور جرائم غسل الأموال في عصر البيئة الرقمية

المبحث الأول: ماهية المصارف الرقمية:

أدت التطورات التكنولوجية الهائلة والثورات المعلوماتية التي شهدتها العالم، إلى حدوث تحولات أثرت بشكل ملحوظ على العديد من القطاعات أبرزها القطاع المالي والمصرفي، وتتمثل أبرز مظاهر هذه التغيرات المالية والمصرفية في التحول نحو الحياة الرقمية وظهور ما يسمى بالمصارف الرقمية، التي تعمل على تقديم خدماتها البنكية عبر منصات إلكترونية، تتعامل من خلال وسائل تقنية حديثة دون الحاجة إلى فروع مما يساهم في تحسين جودة هذه الخدمات وتبسيط الإجراءات.

إن ممارسة النشاط المصرفي يقتضي وجود نظام قانوني يحكمه، لذلك عمل المشرع الجزائري - كغيره من التشريعات الأخرى - على وضع قوانين تنظيمية أبرزها القانون النقدي والمصرفي الجديد 09-23 الذي يسمح بإمكانية الترخيص بإنشاء بنوك رقمية¹، تبعه صدور النظام 04-24 المتعلق بالشروط الخاصة بالترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي²، ثم جاءت التعليمات رقم 02-25 التي عاجلت عناصر ملف طلب الترخيص والإعتماد³.

بناءً على ذلك نقسم هذا المبحث إلى مطلبين، نتناول في **المطلب الأول**: مفهوم المصارف الرقمية، في حين يخصص **المطلب الثاني**: للتطرق للمسألة المتعلقة باعتماد المصارف الرقمية.

المطلب الأول: مفهوم المصارف الرقمية:

1- القانون رقم 09-23، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، ج ر ج ج، العدد 43، الصادرة في 27 يونيو 2023.

2- النظام رقم 04-24، المؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص وتأسيس وإعتماد وممارسة نشاط البنك الرقمي، ج ر ج ج، العدد 77، صادرة في 19 نوفمبر 2024.

3- التعليمات رقم 02-25، المؤرخة في 2 مارس 2025، المتعلقة بالشروط الخاصة بالترخيص وتأسيس وإعتماد وممارسة نشاط البنك الرقمي.

تعتبر المصارف الرقمية من أبرز الابتكارات التي شهدتها القطاع المصرفي في الآونة الأخيرة، نتيجة اعتمادها على التكنولوجيا الحديثة في تطوير خدماتها المالية و التجارية و الإدارية، و إتاحة خدمات جديدة تتعلق بفتح الحسابات وإجراء التحويلات المالية ودفع الفواتير والتمويل الشخصي والإستثمار، وجعلت منها تتسم بالسرعة في الأداء و سهولة الوصول و الإستخدام و بتكاليف منخفضة جدا، هذا ما جعل منها نموذجا إقتصاديا جذابا يمتاز عن البنوك التقليدية و التي يعرف بأنها تعتمد على العمليات اليدوية و التفاعل البشري في تقديم خدماتها .

بناءا عليه نقسم هذا المطلب إلى فرعين، نتناول في **الفرع الأول** تعريف المصارف الرقمية وخصائصها، في المقابل نقوم بالتمييز بين المصارف الرقمية والبنوك التقليدية في **الفرع الثاني**.

الفرع الأول: تعريف المصارف الرقمية وخصائصها:

تعرف المصارف الرقمية بأنها نوع من المؤسسات المالية التي إرتبط ظهورها بالتحويلات التكنولوجية، والتي تعمل من خلال منصات رقمية تمتاز بسرعة وكفاءة عالية، تسعى من خلالها إلى تطوير جودة وكفاءة الخدمات المصرفية التقليدية بما يتناسب مع حاجيات الجمهور. ومنه سنتطرق في دراستنا لهذا الفرع لتعريف المصارف الرقمية **أولا**، خصائص المصارف الرقمية **ثانيا**.

أولا: تعريف المصارف الرقمية:

يعتبر مصطلح المصارف الرقمية من المصطلحات الحديثة نسبا في البحوث والدراسات القانونية، مما أدى إلى إختلاف وتباين كل من أراء الفقهاء والتشريعات الوطنية والدولية حول تحديد مفهوم هذا المصطلح، هذا ما سنحاول توضيحه من خلال تطرقنا لتعريفات: (اللغوية والتشريعية والفقهية).

1/التعريف اللغوي للمصارف الرقمية :

ينقسم مصطلح المصارف الرقمية إلى مصطلحين أساسيين ألا وهما "المصارف "و" الرقمية".، ومنه سنتطرق لتعريف كل مصطلح على حدي.

أ- **المصارف:** "جمع مصرف (بكسر الراء) وهو مأخوذ من الصرف بمعنى رد الشيء من حالة إلى حالة أو إبداله بغيره¹."

- "صرف وصارف واصطurf الدينار أي بدلها بدراهم أو دنانير سواها الصراف والصيرف و الصيرفي و جمعها صيارفة هو بيع النقود بنقود غيرها، و الصرافة أو الصيرفة هي حرفة الصراف المصرف (وهي كلمة محدثة) وجمعها مصارف و تعني المؤسسة المالية التي تتعامل بالإقتراض و الإقراض²."

ب- **الرقمنة:** " يطلق لفظة رقمنة على عدة معاني منها التعجيم والتبيان والكتابة والقلم والخط، ويقول ابن منظور: " الرقم والترقيم تعجيم الكتاب، ورقم الكتاب يرقمه رقما أعجمه وبينه، وكتاب مرقوم"، أي قد بينت حروفه بعلاماتها من التنقيط، وقوله عز وجل " كتاب مرقوم" أي كتاب مكتوب والمرقم

القلم: ضرب مخطط من الوشي، ورقم الثوب يرقمه رقما ورقمه خططه³."

2/التعريف التشريعي للمصارف الرقمية:

عملت بعض التشريعات في الدول العربية على وضع تعريف للمصارف الرقمية، وذلك إستجابة لوجودها المتزايد في الواقع العملي، ومسايرةً للتطورات التكنولوجية والتقنية التي عرفها القطاع المصرفي عالميًا.

1- محمد عثمان شبير، "المعاملات المالية المعاصرة في الفقه الإسلامي"، الطبعة السادسة، دار النفائس، الأردن، 1427هـ - 2007م، ص256.

2- عبد الناصر براني، محاضرات في مقياس المصارف الإسلامية، جامعة عبد القادر -قسنطينة، الجزائر، ص11.

3- تقي الدين دغبوج، "النظام القانوني لتأسيس البنوك الرقمية في الجزائر"، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة الشيخ العربي التبسي، تبسة، المجلد 10، العدد 02، ماي 2025، ص607.

- فالمشروع المصري عرف المصارف الرقمية في المادة 01 من قانون البنك المركزي والجهاز المصرفي بأنها "بنوك تقدم، خدمات مصرفية عبر القنوات أو منصات رقمية باستخدام التقنيات التكنولوجية الحديثة"¹.

- أما المشروع السعودي فقد وضع تنظيمًا للمصارف الرقمية، حيث عرفها على أنها: "المصارف التي تزاوّل الأعمال المصرفية بشكل أساسي عن طريق القنوات الرقمية كشبكة الأنترنت وتطبيقات الجوال." (لائحة البنوك الرقمية السعودية).²

- كما عرف المشروع الكويتي المصرف الرقمي من خلال اللائحة الصادرة عن بنك الكويت المركزي بأنها: "البنك (سواء التقليدي أو الإسلامي) الذي يزاول المهنة المصرفية عن طريق القنوات الرقمية."³

- أما بالنسبة للمشروع الجزائري وبالرجوع إلى القانون النقدي والمصرفي 09.23، نجد أنه لم يتطرق لتعريف المصارف الرقمية بل إكتفى بالإشارة إلى الترخيص بإنشائها في المادة 90 منه وأحال تحديد كفاءات وشروط ممارستها لأنشطتها إلى التنظيم⁴، وبالنظر إلى أحكام النظام 04.24 نجد أنه عرف البنك الرقمي في المادة 2 منه: "بأنه كل بنك يقدم خدمات ومنتجات حصرياً عبر قنوات أو منصات أو دعائم رقمية بالاعتماد على التكنولوجيا الحديثة في إطار ممارسة أنشطته." التكنولوجيا الحديثة. المقصودة أعلاه، هي تلك المتعلقة بتكنولوجيات الإعلام والاتصال والتكنولوجيا المالية".⁵

3 : التعريف الفقهي للمصارف الرقمية :

1- أنظر المادة 1 من القانون رقم 194، المؤرخ في 15 سبتمبر 2020، المتضمن قانون البنك المركزي والجهاز المصرفي، الجريدة الرسمية للجمهورية المصرية، العدد 37، ص 5.

2- قرار البنك المركزي السعودي لسنة 2020، بشأن الإرشادات والمعايير الإضافية لطلب منح الترخيص للبنوك الرقمية في المملكة السعودية، ص 3.

3- قرار بنك الكويت المركزي لسنة 2022، بإصداره دليل متطلبات تأسيس البنوك الرقمية في دولة الكويت، ص 3.

4- أنظر المادة 90 من القانون رقم 09-23، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق، ص 16.

5- أنظر المادة 2 من النظام رقم 04.24، المؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاطات البنك الرقمي، المصدر السابق، ص 30.

إهتم فقهاء القانون والإقتصاد بمصطلح المصارف الرقمية، وقدموا تعريفات مختلفة من بينها: "أنه موقع إلكتروني يقدم الخدمات المالية في البيئة الافتراضية"، كما عرف أيضا على أنه: "العمل المصرفي الذي تكون فيه الأنترنت وسيلة الإتصال بين البنك والعميل وبمساعدة أنظمة وبرامج تمكن العميل من الإستفادة من الخدمات والحصول على منتجات مصرفية مختلفة، والتي يقدمها البنك عن بعد".¹

وتم تعريف المصارف الرقمية بأنها: "هي رقمنة كل مستوى من الخدمات المصرفية من الأمام إلى الخلف ما يعني أن البنوك الرقمية تعتمد على الذكاء الاصطناعي لإجراء عمليات الإيداع والحصول قروض والوصول إلى خدمات إدارة الأموال الشخصية".²

كما تم تقديم تعريف للمصرف الرقمي على أنه: "بنك دون فروع يقدم جميع الخدمات المصرفية الفورية عبر قنوات رقمية".³

-من خلال كل من التعريفات اللغوية والقانونية والفقهية، يمكن تقديم تعريف المصارف الرقمية على أنها: المصارف التي تقوم بتقديم كافة خدماتها المصرفية عبر منصات إلكترونية أو قنوات رقمية بإستخدام التقنيات الحديثة، مما يضمن السرعة والأمان في التعاملات البنكية.

ثانيا: خصائص المصارف الرقمية:

تتميز المصارف الرقمية بجملة من الخصائص تميزها عن غيرها من المصارف التقليدية، ويمكن حصر أهم هذه الخصائص في النقاط التالية:

1/سهولة الوصول والإستخدام:

1- حميد سلطاني، "البنوك الرقمية شروط الترخيص بإنشائها واعتمادها في ظل القانون رقم 09./23"، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي بالشلف، الجزائر، المجلد 11، العدد 1، جوان 2025، ص 194 - 195.

2- عاصم محمد طه الفليح، "التنظيم القانوني للبنوك الرقمية في الأردن (دراسة مقارنة)"، رسالة ماجستير، تخصص قانون خاص، جامعة الشرق الاوسط، الأردن، كانون الثاني 2025، ص 17.

3- حنان دريد - طاوس غريب، "الصيرفة الرقمية كتوجه حديث لبنوك الجزائرية (دراسة إحصائية)"، المجلة العلمية المستقبل الاقتصادي، جامعة محمد بوقرة بومرداس، الجزائر، للمجلد 10، العدد 1، جوان 2022، ص 600.

أي أن المصارف الرقمية تمنح للعملاء سهولة الوصول والاستفادة من الخدمات المصرفية والإلكترونية التي تتم عبر الانترنت¹، دون مواجهة أي من الحواجز والصعوبات المتعلقة بالوقت أو المكان، وتتجلى هذه الخاصية في كل من البساطة والوضوح وسهولة الإستعمال.²

2/ توفير الوقت والجهد:

معنى ذلك أن المصارف الرقمية بتقديمها للخدمات المصرفية عبر الانترنت فهي توفر للعملاء عنصر الراحة، مما يلغي الحاجة للتنقل إلى فروع المصارف التقليدية، أي تقوم بالمعاملات البنكية بإستعمال الوسائل التقنية والتي تتمثل في الهاتف والحاسوب.³

3 /الأمان والحماية:

تعمل المصارف الرقمية على حماية البيانات المالية الخاصة بالعملاء باتخاذها لإجراءات وتدابير أمنية عالية⁴، أبرزها: التشفير، المصادقة والتحقق البيومتري، مما يساهم في تعزيز الثقة وزيادة الإقبال على الخدمات المصرفية الإلكترونية.⁵

4/فاعلية التكاليف (خفض التكاليف):

أهم ما يميز المصارف الرقمية عن العادية هو أنها تقدم خدماتها المصرفية بتكاليف منخفضة، مما يساهم في تحديث جودة الخدمة وجلب أكبر عدد من الزبائن مما يجعل تقديم الخدمات البنكية أقل تكلفة

وأكثر كفاءة¹.

1- فلاح حسين ثويني، "المصارف الرقمية والوصول السهل الي التمويل (قراءة في توسيع التمويل وقاعدة الزبائن المصرفيين من خلال المصارف) «، الطبعة الأولى، مركز البيان لدراسة والتخطيط- بغداد، سبتمبر 2024، ص16.

2- سمية زيدان - سفيان عصماني، "دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية (دراسة حالة بنك بنكسي الجزائر)«، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، جامعة محمد بوضياف -المسيلة، المجلد 17، العدد 02، ديسمبر 2024، ص60.

3- سمية زيدان - سفيان عصماني ، المرجع السابق، ص60.

4- فلاح حسين ثويني، المرجع السابق، ص 16.

5- سمية زيدان- سفيان عصماني، المرجع السابق، ص61.

5/ توفير خدمات مصرفية بتكنولوجيا متقدمة:

بالإضافة إلى الخدمات الأساسية التي تقدمها المصارف الرقمية التي هي في الأصل تابعة للبنوك التقليدية، فإنها تعمل على تقديم خدمات مصرفية أكثر تطوراً عبر الإنترنت تتسم بالسرعة في الأداء والكفاءة في الخدمة، ومن بين هذه الخدمات نجد: إمداد العملاء بطريقة لتأكد من أرصدهم لدى البنك، كذلك طرق دفع العملاء للكمبيالات المسحوبة إلكترونياً، إضافة إلى كيفية إدارة المحافظ المالية من أسهم وسندات للعملاء، كما أنها تعمل على تخصيص بطاقات إئتمان وخصم خاص لكبار العملاء من التجار ورجال الأعمال.²

6/ توسيع المجال أمام المؤسسات صغيرة الحجم:

ساهمت المصارف الرقمية من خلال الخدمات المصرفية التي تقدمها في فتح المجال أمام المؤسسات المالية صغيرة الحجم بتطوير استثمارها دون أن يكلفها ذلك دفع أعباء التشييد التي تفرضها عادة البنوك التقليدية، بالنظر لاعتمادها على وسائل التكنولوجيا الحديثة في قيامها بمعاملاتها البنكية.³

الفرع الثاني: التمييز بين المصارف الرقمية والبنوك التقليدية:

تمثل كل من المصارف التقليدية أو الرقمية نموذجين متميزين في القطاع المصرفي، لكن هناك اختلافات جوهرية بينهما، على اعتبار أن الأولى تعتمد على الفروع المادية والتفاعل البشري، بينما تعتمد الثانية في تقديم خدماتها المصرفية على التقنيات الرقمية الحديثة. ومنه تبرز الفروق بين هاذين النموذجين من

1 - صافية كبابي-مريم تيخريباتين، "النظام القانوني المعاملات البنكية الإلكترونية"، مذكرة ماستر في الحقوق، تخصص قانون الأعمال، كلية الحقوق و العلوم السياسية، جامعة أكلي محمد أولحاج -البويرة، 2020-2021، ص18.

2- عاصم محمد طه الفليح، المرجع السابق، ص19.

3- سماح كحل الراس- منية شوايدية، " دور البنوك الالكترونية في تنشيط السوق المالي، الملتقى الوطني عن بعد"الصيرفة الالكترونية والتنمية الاقتصادية"، كلية الحقوق والعلوم السياسية، جامعة 8ماي 1945 قالمة، 3 جوان 2021، ص455.

حيث النشأة أولاً، ومن حيث الهيكل التنظيمي ثانياً، ومن حيث طبيعة المعاملات ثالثاً، ومن حيث التكاليف والتسعير رابعاً، ومن حيث الخدمات المقدمة خامساً.

أولاً: من حيث النشأة:

من المعروف بأن البنوك التقليدية قد نشأت كمحطة لظروف ومتطلبات فرضتها التطورات الاقتصادية والمعاملات التجارية على مدى السنين، بذلك فهي سابقة الظهور عن البنوك الرقمية التي يرجع ظهورها إلى منتصف القرن 12، ويعرف بأن أول بنك تم إنشائه في مدينة البندقية عام 1157 تحت إسم بنك ديريا يتو ويليه بنك أمستردام بهولندا 1609¹، أما المصارف الرقمية لقد جاء ظهورها إنعكاساً للتحويلات التكنولوجية التي حصلت في العالم في العقود الثلاث الأخيرة والتي نقلت العالم بتجاه الإقتصاد الرقمي، وكان أول ظهور لهذا النوع من البنوك في الفترة الممتدة بين 2013 و2015، حيث أنشأ أول بنك رقمي في بريطانيا (Monzo) وبنك (ميم) في السعودية.²

ثانياً: من حيث الهيكل التنظيمي:

تعتمد البنوك التقليدية على بنية تنظيمية قائمة على شبكة من الفروع المادية المنتشرة في المدن الكبرى والمناطق المختلفة، ويعمل فيها عدد كبير من الموظفين لتقديم الخدمات المصرفية بشكل مباشر للعملاء، ويتطلب هذا التنظيم تكاليف تشغيلية مرتفعة تشمل إيجار الفروع، وتجهيزاتها، إضافة إلى أجور الموظفين. ومع ذلك، تتيح هذه الفروع تواصلاً مباشراً مع العملاء، خصوصاً عند تقديم الخدمات المالية المعقدة مثل القروض العقارية أو الإستشارات الإستثمارية.

في المقابل تقوم المصارف الرقمية على نموذج تنظيمي مختلف يعتمد أساساً على المنصات الإلكترونية والتطبيقات الذكية، مما يقلل من الحاجة إلى الفروع المادية، وغالباً ما تستند هذه البنوك إلى بيئة

1- محمد أمين خلاف- إسماعيل أسامة كافي، "البنوك الإلكترونية"، مذكرة ماستر، تخصص قانون شركات، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح -ورقلة، 2017-2018، ص25.

2- عاصم محمد طه، المرجع السابق، ص12.

تكنولوجية حديثة قائمة على الذكاء الاصطناعي، الأمر الذي يساهم في تقليص التكاليف التشغيلية وتحسين كفاءة تقديم الخدمات المصرفية.¹

ثالثاً: من حيث طبيعة المعاملات:

تستوجب البنوك التقليدية للقيام بمعاملاتها المصرفية ضرورة توجه العميل إلى مقر البنك ومقابلة الموظفين المكلفين بتقديم تلك الخدمة مما يزيد من تكلفة وأعباء التنقل، عكس المصارف الرقمية التي تتسم بغياب المعاملات الورقية وإعتمادها على شبكة الأنترنت في تعاملاتها المصرفية على اعتبار أنه ليس لها وجود على أرض الواقع، مما يوفر عنصر الوقت والجهد للعميل.²

رابعاً: من حيث التكاليف والتسعير:

تفترض البنوك التقليدية للقيام بمعاملاتها المالية رسوماً أعلى لتغطية تكاليف كل من الموظفين والفروع، مقارنة بالمصارف الرقمية التي تقدم كافة الخدمات المصرفية التقليدية إلى جانب الخدمات الأكثر تطوراً بتكاليف منخفضة، حيث تبين من خلال دراسات تقديرية أن تكلفة تقديم خدمة عبر فرع البنك تصل إلى 295 وحدة، في حين تقل إلى 4 وحدات إذا قدمت عبر شبكة الأنترنت مما يساهم في جذب العملاء لتعامل مع هذا النوع من البنوك.³

خامساً: من حيث الخدمات المقدمة:

تتميز المصارف الرقمية بأنها تقدم خدماتها المصرفية لعملائها في أي وقت في كافة أيام الأسبوع وعلى مدار الأربعة والعشرون (24) ساعة، أي أنها لا تتقيد بأوقات معينة كالبنوك التقليدية التي تعمل على تقديم خدماتها وفقاً لتوقيت معين مع مراعاة الإجازات والعطل وحالات الغياب

1- حميد سلطاني، المرجع السابق، ص 197.

2- محمد أمين خلاف -أسامة إسماعيل كافي، المرجع السابق، ص 26-27.

3- محمد أمين خلاف -أسامة إسماعيل كافي، المرجع السابق، ص 23.

المتعلقة بالموظفين، مما يشكل عائقاً أمام راحة العميل الذي يسعى للقيام لمعاملاته البنكية عن بعد وفي أي وقت دون أن يكلفه ذلك أعباء أو مصاريف¹.

المطلب الثاني: اعتماد المصارف الرقمية:

تمثل المصارف الرقمية النموذج الأحدث للمصارف إستجابة لمختلف التطورات والاعتماد المتزايد على التكنولوجيا، إلا أنه بالنظر إلى الطبيعة الحساسة التي يمتاز بها هذا النوع من البنوك، فقد أوجب القانون على الراغبين بتأسيس بنوك أو مؤسسات مالية بجملة من الشروط تخص كل من البنك الرقمي والمؤسسين والمساهمين، وأخضع تأسيس البنوك لإجراءات تتمثل في إجراءي الترخيص والاعتماد لضمان الرقبة الفعلية. تم تقسيم هذا المطلب إلى فرعين، نتناول الشروط المطلوبة لإنشاءها في الفرع الأول، في حين نتطرق لإجراءات منح الاعتماد في الفرع الثاني.

الفرع الأول: الشروط المطلوبة لإنشاء المصارف الرقمية

مما لا شك فيه أن المصارف الرقمية كغيرها من الخدمات المالية الإلكترونية تعد بمثابة حافز للتنمية الاقتصادية والنمو في العديد من الدول، إذ يعد إنشاء هذا النوع من المصارف مرحلة هامة وحساسة ولنجاحها اشترط لها المشرع جملة من الشروط، منها ما يتعلق بالشخص المعنوي محل التأسيس (المصرف الرقمي) أولاً، ومنها ما يتعلق بالأشخاص الطبيعيين (المسييرين والمساهمين) ثانياً.

أولاً: شروط التأسيس المتعلقة بالشخص المعنوي (المصرف الرقمي):

اشترطت القوانين والأنظمة ذات العلاقة بالمصارف الرقمية على الأشخاص الراغبين في إنشاء مثل هذه البنوك، بإتخاذ شكل الشخص المعنوي وإنشاء نشاطها في شكل من أشكال الشركات التجارية بما تستوفيه من شروط شكلية وموضوعية، ومنه يمكن حصر أهم هذه الشروط في النقاط التالية:

1- المرجع نفسه، ص 27.

1/- إتخاذ المصرف الرقمي شكل شركة المساهمة :

نص المشرع الجزائري بموجب القانون رقم 09-23 والمتضمن القانون النقدي والمصرفي، وتحديدًا في المادة 91 منه: "يجب أن تأسس البنوك والمؤسسات المالية في شكل شركة ذات أسهم، يقدر المجلس جدوى إتخاذ بنك أو مؤسسة مالية شكل تعاضدية".¹

نلاحظ من خلال استقراء نص هذه المادة، أن المشرع الجزائري أوجب تأسيس المصارف من بينها الرقمية في شكل شركة ذات أسهم باعتبارها النموذج الأمثل لشركات الاموال، واستثناءا يمكن أن تتأسس في شكل تعاضدية، ونلاحظ كذلك بأن المشرع حصر إنشاء المصارف الرقمية في شكل شركات المساهمة واستبعاده لباقي أنواع الشركات الأخرى، عكس بعض التشريعات التي منحت لمؤسسي هذا النوع من البنوك حرية إنشاء إما في شكل شركة تضامن أو توصية بسيطة كالمشرع الفرنسي.²

أ/إعتماد شكل شركة المساهمة في تأسيس المصرف الرقمي:

عرف الفقه شركة المساهمة بأنها: "الشركة التي ينقسم رأسمالها إلى أسهم متساوية القيمة ويكون لكل شريك عدد من الأسهم، ويتفاوت الشركاء تفاوتًا كبيرًا في عدد الأسهم التي يمتلكونها ولا يكون كل شريك مسؤولًا إلا في حدود الأسهم التي يمتلكها".³

1- المادة 91 من القانون رقم 09-23، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق، ص 16.

2- رميساء بولمرقة- رتيبة إيمان شويطر، "الظوابط القانونية لإنشاء البنوك الرقمية في الجزائر"، مجلة البحوث في العقود و قانون الأعمال، جامعة الإخوة منتوري قسنطينة 1، الجزائر، المجلد 10، العدد 01، جوان 2025، ص 127.

3- عبد الصمد حوالف، " شركة المساهمة بين النظامية والتعاقدية"، مجلة القانون والعلوم السياسية، جامعة النعامة، الجزائر، المجلد 09، العدد 01، أفريل 2023، ص 447.

أما بالنسبة للمشرع الجزائري فقد عرفتها من خلال المادة 592 من القانون التجاري بأنها: "الشركة التي يقسم رأسمالها إلى حصص وتتكون من شركاء لا يتحملون الخسائر إلا بقدر حصصهم ولا يمكن أن يقل عدد الشركاء عن سبعة".¹

- تعتبر شركة المساهمة الصورة الأمثل لشركات الأموال التي تتضاءل فيها الإعتبار الشخصي بشكل كبير ويغلب عليها الإعتبار المالي ما يمنحها الإستقلالية بذاتها عن مكوني هذه الشركة، حيث ينصب إهتمامها على حصة الشريك أكثر من الشريك في حد ذاته، كما أنها تمتاز بأنها تلجأ إلى طرح الإكتتاب العام كلما تأسست باللجوء العلني للإدخار وهذا راجع لمشروعاتها الضخمة، أما بالنسبة لعدد الشركاء فقد حدده المشرع الجزائري و الذي لا يجوز أن يقل عن 7 أشخاص (المادة 592/2 من ق ت ج)، وخصص الشريك في شركة المساهمة قابلة للتداول (المادة 715 مكرر 40 من ق ت ج)، وهذه الحصة المقدمة هي التي تحدد مسؤوليته بمعنى أن المسؤولية تحدد بحدود الأسهم التي اكتتب فيها، أما بالنسبة لاسم و عنوان الشركة فإنه يجوز إدراج اسم شريك واحد أو أكثر ويجب أن يتبعه شكل الشركة بمعنى ذكر "شركة مساهمة"، و يتولى إدارتها مجلس للإدارة معين من قبل مجموع المساهمين لأجل محدد.²

- نظرا لضخامة شركات المساهمة فإنها تخضع في تأسيسها لإجراءات طويلة ومعقدة تختلف تبعا لطريقة التأسيس فقد تكون عن طريق اللجوء العلني للإدخار أو دون اللجوء العلني للإدخار أو ما يطلق عليه (التأسيس الفوري)، أما بالنسبة للبنوك فيتم تأسيسها باللجوء العلني للإدخار مع إمكانية اللجوء إلى التأسيس الفوري، وهذا مرتبط بمدى كفاية الذمة المالية لتغطية الحد الأدنى لرأسمال البنك الرقمي.

1- المادة 592 من القانون رقم 05-02، المؤرخ في 6 فيفري 2005، المعدل والمتمم للأمر رقم 75-59 المؤرخ في 25-09-1975، والمتضمن القانون التجاري الجزائري، ج ر ج ج، العدد 11، سنة 2005.

2- نادية فوضيل، "شركات الأموال في القانون الجزائري"، الطبعة الثالثة، ديوان المطبوعات الجامعية، الجزائر، 2008، ص 145-150.

ب- إستبعاد شكل التعاضدية في تأسيس المصرف الرقمي:

لا يمكن أن تتخذ المصارف شكل التعاضدية أو التعاونية المشار إليه في المادة 91 من القانون 09/23 المتضمن القانون النقدي والمصرفي، على اعتبار أن هذا الشكل يخص فئة معينة كالصندوق الوطني للتعاونية الفلاحية، ولا يتناسب مع طبيعة النشاط الربحي للبنك الرقمي.¹

2/ إنشاء المنصة الإلكترونية للمصرف الرقمي :

تمثل البنية التحتية التكنولوجية عنصرا جوهريا لوجود واستمرارية المصرف الرقمي على اعتبار أن نجاح هذا الأخير لا يقتصر على تقديم الخدمات عبر الوسائط الإلكترونية، وإنما يتوقف بشكل أساسي على توفر منظومة تقنية متكاملة وفعالة، تمكنها من أداء خدماتها البنكية بشكل آمن، وبالنظر إلى خصوصية المصارف الرقمية وطبيعتها غير المادية فلقد إشتراط المشرع أن يتم تأسيسها رقميا عبر منصة² تتضمن الشروط المنصوص عليها في التعليمات 02-25³، والتي يستعين بها المهندسون المختصون في تصميم منصة المصرف الرقمي.

أما بالنسبة للمكونات الرئيسية لمنصة المصرف الرقمي فهي تشمل كل من واجهة المستخدم Frontend، الخدمات الخلفية Backend، الأنظمة الأساسية Integrating Layer، طبقة التكامل Core Banking Systems، الأمن السيبراني، البنية التحتية.

تنشئ المنصة الإلكترونية للمصرف الرقمي من خلال إتباع خطوات فنية تفصيلية تكمن في:

- الإعداد والتخطيط: يتم من خلالها تحليل المتطلبات القانونية والتنظيمية وتحديد الخدمات البنكية الأساسية، وتحديد البنية التحتية السحابية ولغات البرمجة وأطر العمل المناسبة.

1- سامي كباهم، "خصوصية شروط ممارسة نشاط البنك الرقمي -دراسة في القانون الجزائري «، مجلة الدراسات القانونية والإقتصادية، المركز الجامعي بربكة، الجزائر، المجلد 08، العدد 02، نوفمبر 2025، ص 229.

2- المرجع نفسه، ص 232.

3- التعليمات 02-25، المؤرخة في 2 مارس 2025، المتعلقة بالشروط الخاصة بالترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي.

- **التصميم والتأسيس:** من خلال تصميم طبقات الخدمات والتخطيط للتوسعة، واعتماد معايير الأمن من تشفير ومصادقة.
- **التطوير:** بناء الخدمات الأساسية وإدارة الحسابات وأنظمة الدفع والاختبار الآلي لوحدة التكامل والأمان.
- **النشر والاطلاق:** بإنشاء بيئة إفتراضية يتم إطلاقها من خلال مرحلتين، الأولى تجريبية مع تحسين الثغرات والثانية الإطلاق الرسمي للجمهور بعد تمام إجراءات الترخيص والإعتماد.
- **التحديث:** يهدف إلى تحسين جودة وأداء البنوك الرقمية.¹

3/ رأس مال المصرف الرقمي :

يمثل رأس المال أحد أهم الركائز الأساسية التي يقوم عليها الكيان المالي والقانوني للمصرف، لما له من دور محوري في ضمان الاستقرار المالي وزيادة ثقة العملاء، ويعرف رأس المال بأنه: "مجموعة من الأموال التي يحتفظ بها البنك كجزء من متطلبات رأس المال الواجب الاحتفاظ به لدى البنك ليضمن الاستقرار المالي والقدرة على تلبية الإلتزامات".²

ولقد تم تحديد الحد الأدنى لرأسمال المصرف الرقمي بمبلغ عشرة (10) ملايين دينار جزائري و10 000 000 000 دج، وهذا ما نصت عليه المادة 2 من النظام رقم 24-02³، ونظرا للطبيعة الخاصة التي يمتاز بها النشاط المصرفي، فقد نص المشرع في المادة 96 من القانون النقدي والمصرفي رقم

1- محمد بولالي- زين الدين عطيط، "النظام القانوني للبنك الرقمي في التشريع الجزائري"، مذكرة ماستر في القانون، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحيى - جيجل، الجزائر، 2024-2025، ص 11-ص13.

2- خالد بلعور- عبد الكريم منصوري، "تأثير المخاطر البنكية على رأس المال في البنوك - دراسة حالة مجموعة من البنوك العربية"، مجلة المنهل الإقتصادي، جامعة الشهيد حمه لخضر الوادي، الجزائر المجلد 07، العدد 01، جوان 2024، ص1024.

3- المادة 2 من النظام رقم 24-02، المؤرخ في 6 فبراير 2024، المتعلق بالحد الأدنى لرأسمال البنوك والمؤسسات المالية العاملة في الجزائر، ج ر ج ج، عدد 18، صادرة في 13 مارس 2024، ص32.

23-09: "يجب أن يتوفر للبنوك والمؤسسات المالية رأسمال محرر كليا ونقدا..."¹، والمقصود بذلك أن يكون مجموع حصص المساهمين عبارة عن حصص من نقود فقط، مع إستبعاد إمكانية تقديم حصص عينية.

ثانيا: شروط التأسيس المتعلقة بالأشخاص الطبيعيين:

على اعتبار أن المصرف الرقمية تأخذ شكل شركة المساهمة، بالتالي فإنها لا تعطي اهتماما للاعتبار الشخصي لأن المسؤولية تحدد بقدر الحصص المقدمة، إلا أنه بالنظر لنص المادة 87 من القانون النقدي والمصرفي نجد أنه أولى اهتمام خاص لفئة من الأشخاص من مسيرين ومساهمين وأقر لهم جملة من الشروط تكمن في:

1/ الشروط المتعلقة بالمسيرين :

يعد المسيريون من الركائز الأساسية لنجاح نشاط المصرف الرقمية، ولقد عرفها المشرع الجزائري من خلال نص المادة 2 من النظام رقم 25-01 الفقرة الأولى على أنهم: "الإطارات المسؤولة التي يتم تعيينهم من أجل التحديد الفعلي لتوجيه ومراقبة نشاط المؤسسة الخاضعة ومسؤولية تسييرها..."²، وأخضعهم لجملة من الشروط منها:

- الحصول على اعتماد: والذي يتم الحصول عليه من محافظ بنك الجزائر، حسب ما نصت عليه المادة 4 من النظام رقم 25-01، وذلك في أجل أقصاه 15 يوم من تاريخ التعيين (المادة 5 من النظام السابق).³

¹ المادة 96 من القانون رقم 23-09، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق، ص 16.
² المادة 2 من النظام 01-25 المؤرخ في 12 مارس 2025، يتضمن تحديد شروط اعتماد مسيري المؤسسات الخاضعة، ج ر ج ج، العدد 23، الصادرة في 22 أبريل 2025، ص 22.
³ المادتان 4 و 5 من النظام رقم 01-25، المؤرخ في 12 مارس 2025، يتضمن تحديد شروط اعتماد مسيري المؤسسات الخاضعة، المصدر نفسه، ص 22، 23.

- عدد المسجلون: اشترط القانون النقدي والمصرفي بأن لا يقل عدد المسجلون عن شخصين إثنين، حسب ما نصت عليه المادة 98 من القانون رقم 23-09.
- الخبرة والكفاءة: والمقصود هنا أنه يشترط في المسجلين توافر الكفاءة المهنية والتي يتم اكتسابها، من خلال الخبرة في الميدان عن طريق القيام بأعمال التسيير للبنوك والمؤسسات المالية الأخرى، حسب ما ورد في نص المادة 99 من القانون 23-09¹. إضافة إلى ضرورة التأكد من أهلية المسجلين، نظرا لاتساع نطاق المسؤوليات التي ترافق عملية تأسيس البنوك، وتجنب وقوع خسائر قد تمس المؤسسة أو الزبائن، وهذا ما نصت عليه المادة 09 من النظام رقم 24-04².

2/ الشروط المتعلقة بالمساهمين :

أولى القانون إهتمام أكبر بالمساهمين في المجال البنكي، فقد أقر لهم بعض الشروط إضافة إلى شرط النزاهة والأمانة، حيث نجد أن نص في المادة 99 من القانون 23-09 على أن المساهمين ملزمين ببيان مصدر الأموال ضمانا للشفافية وتفاديا لعمليات تبييض الأموال³، بالإضافة إلى ما نصت عليه المادة 5 من النظام 24-04 الذي يشترط أن يكون من بين مساهمي البنك الرقمي بنك خاضع لأحكام القانون التجاري، خبير في مجال الخدمات البنكية عبر الانترنت، وامتلاكه ما لا يقل عن نسبة 30% من رأس مال من جهة أخرى، مع ضرورة التأكد من عدم تجاوزها الحصة الفردية لكل من مساهم من المساهمين في رأس المال⁴.

الفرع الثاني: إجراءات منح الإعتماد للمصارف الرقمية:

- 1- المادتان 98 و 99 من القانون 23-09، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق، ص 16.
- 2- المادة 09 من النظام رقم 24-04، المؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، المصدر السابق، ص 3.
- 3- المادة 99 من القانون رقم 23-09، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق، ص 16.
- 4- المادة 5 من النظام رقم 24-04، المؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، المصدر السابق، ص 2.

يخضع تأسيس المصرف الرقمي لأحكام القانون النقدي والمصرفي، وكذا التنظيمات الصادرة عن بنك الجزائر، والتي تحدد الشروط والإجراءات اللازمة لممارسة النشاط البنكي، وتتم عملية التأسيس عبر مرحلتين أساسيتين: تتمثل الأولى في الحصول على الترخيص كإذن مبدئي لإنشاء المصرف، بينما تتمثل الثانية في الحصول على الاعتماد الذي يخول مباشرة النشاط فعليًا بعد استيفاء الشروط القانونية. وعليه، يُعالج هذا الفرع من خلال تقسيمه إلى عنصرين، يُخصص الأول لاستعراض عنصر الترخيص، في حين نتناول في الثاني طلب الاعتماد.

أولا الترخيص:

الترخيص هو أول إجراء يمنحه مجلس النقد والقرض لتأسيس بنك أو مؤسسة مالية، وذلك وفق إجراءات وشروط نص عليها كل من النظام رقم 24-101¹ وأحكام القانون رقم 23/09 فتختلف شروط منحه الترخيص بناء على نوع النشاط لكنها تشترك في مجموعة من المبادئ القانونية العامة وهذا ما سنعالجه في هذا العنصر.

1/تعريف الترخيص:

لم يضع المشرع الجزائري تعريفًا صريحًا لمفهوم الترخيص، سواء ضمن أحكام القانون رقم 23-09 المتعلق بالنقد والصرف أو ضمن الأنظمة الصادرة عن المجلس النقدي والمصرفي، تاركًا بذلك المجال للاجتهاد الفقهي²، حيث اختلفت هذه التعاريف باختلاف الفقهاء وتوجهاتهم واجتهاداتهم، مما انعكس ذلك على عدم وجود تعريف واضح أو موحد بين جميع الفرق الفقهية.

1- النظام رقم 24-01، المؤرخ في 6 فبراير 2024، يتضمن تحديد شروط الترخيص بتأسيس بنك ومؤسسة مالية و إعتمادها، ج ر ج ج، عدد 18، صادرة في 13 مارس 2024.

2- محمد بولالي، زين الدين عطيط، المرجع السابق، ص 28.

فقد عرف الترخيص بأنه، "إذن قانوني مسبق تمنحه جهة مختصة، يخول لصاحبه ممارسة نشاط معين أو التمتع بحق محدد".

يعرفه أيضا محمد الطيب عبد اللطيف: " الترخيص وسيلة من وسائل تدخل الدولة في ممارسة النشاط للوقاية مما قد ينشأ عنه من أضرار، وذلك بتمكين الهيئات الإدارية من فرض ما تراه مناسبا من احتياطات والتي من شأنها منح هذا الضرر أو رفض الإذن بممارسة النشاط إذا كان لا يكفي للوقاية منه واتخاذ الاحتياطات المذكورة أو غير مستوف للشروط¹".

إذن، فالمقصود بالترخيص هو قرار إداري فردي صادر عن سلطة مختصة، يُنشئ مركزًا قانونيًا خاصًا لفائدة طالبه، ينقله من حالة الحظر إلى الإباحة المقيدة، بناءً على طلب مسبق، ويُعدّ عملاً قانونيًا شكليًا يصدر في محرر رسمي، يتمتع بالقوة الإلزامية، ويخضع لمبدأ التوقيت وقابلية السحب أو الإلغاء وفقًا لمقتضيات المصلحة العامة.²

2/ كيفية تقديم ملف إنشاء مصرف رقمي:

إن تأسيس المصارف الرقمية وممارسة النشاطات البنكية والمصرفية الرقمية يتطلب اتباع بعض الاجراءات القانونية، حيث يشترط النظام 04/24 لتأسيس بنك رقمي الحصول على ترخيص، ويتم ذلك من خلال تقديم ملف إلى الجهة المختصة "المجلس النقدي والمصرفي"³، بالإضافة إلى عناصر

1- عبد الرحيم قريول - عبد القادر عزوزي، "النظام القانوني للرخص الإدارية في التشريع الجزائري"، مذكرة ماستر في الحقوق، تخصص الدولة والمؤسسة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، 2020-2021، ص 5.

2- عبد الرحيم قريول - عبد القادر عزوزي، المرجع السابق، ص 5، ص 6.

3- حميد سلطاني، المرجع السابق، ص 201.

الترخيص المنصوص عليه في النظام رقم 24-01¹ يقدم أيضا ملف تكميلي خاص بهذا النوع من البنوك الذي يحدد محتواه بموجب التعليمات 02/25².

كما نصت المادتان 8 و 9 من النظام 04/24 المتعلق بالشروط الخاصة للترخيص بتأسيس واعتماد وممارسة نشاط البنك الرقمي، حيث أخضعت هذه البنوك لنفس الإطار القانوني والتنظيمي المطبق على البنوك التقليدية، مع مراعاة خصوصيات نشاطها الرقمي. كما حدّد هذا النظام الشروط الواجب توفرها للحصول على الاعتماد، إضافة إلى كيفية الالتحاق بالهيئة المصرفية، وقد أنيطت بالسلطة المختصة مهمة إصدار الأنظمة التي تضبط إنشاء البنوك والمؤسسات المالية، مع بيان المتطلبات التي يجب أن تستوفيها هذه المؤسسات، سواء من حيث الحد الأدنى لرأس المال أو إجراءات التأسيس والتنظيم، وصولاً إلى المعايير الموحدة التي تحكم نشاطها.³

3/ عناصر ملف إنشاء بنك رقمي:

إن تقديم طلب الترخيص يكون مرفق بملف، وهذا ما أشارت إليه المادة 3 من التعليمات رقم 02-25 " يجب أن يتضمن الملف من نسختين إحداها رقمية لتأسيس مصرف رقمي"، كما تضمنت المادة 4 من نفس التعليمات الإشارة إلى أهم العناصر والمعلومات والوثائق التي يحتويها هذا الملف والمشار إليه في المادة 3 أعلاه، من أهم هذه العناصر نجد:

أ. عرض موجز للمشروع.

ب. مشروع القانون الأساسي.

ج. صفة المؤسسين مقدمي الأموال والمستفيدين الحقيقيين.

1- النظام رقم 24 / 01، المؤرخ في 6 فبراير 2024، يتضمن تحديد شروط الترخيص بتأسيس بنك ومؤسسة مالية وإعتمادها، ج رج ج، عدد 18، صادر في 13 مارس 2024

2- التعليمات 02/ 25، المؤرخ في 02 مارس 2025، المتعلق بالشروط الخاصة للترخيص بتأسيس وإعتماد وممارسة نشاط البنك.

3- تقي الدين دغبوج، المرجع السابق، ص 266.

د. دراسة تقنية اقتصادية متعلقة بالمشروع المزعم انجازه.

هـ. وصف موجز للأنظمة الخاصة حسب الأطر التنظيمية سارية المفعول.¹

كما ألزمت المادة 5 من نفس التعليمات مقدمي الطلبات للحصول على الترخيص بتأسيس بنك ومؤسسة مالية واعتمادها على تقديم ملف تكميلي، وعملا بأحكام المادة 8 من النظام 04/24، يحتوي هذا الملف على الخصوص العناصر التالية:

أ. وصف متعلق بنية نظام المعلومات.

ب. المراجع السياسات الأجهزة والتدابير المزعم تكريسها في مجال أمن نظام المعلومات، المراجع المعيارية التشريعية التنظيمية المتعلقة بأمن نظام المعلومات.

ج. الأجهزة والتدابير المتعلقة بإدارة الحوادث واستمرارية الأنشطة، الإجابة على جميع الاسئلة التي تضمنتها الملاحق المنصوص عليها في التعليمات 02/25 وعلى جميع البنود بدقة.²

4/البث في طلب الترخيص :

بعد القيام بالإجراءات التي تطرقنا إليها سابقا من خلال نصوص المواد 4 و 5 من التعليمات 02/25 إلى رئيس المجلس النقدي والمصرفي يتم عرض الطلب على المجلس من أجل دراسته والتأكد من أن الملف يحتوي على جميع الشروط المطلوبة، ويكون الرد إما بمنح الترخيص أو رفضه.¹

1- المادتان 3 و 4 من التعليمات رقم 02-25، المؤرخ في 2 مارس 2025، المتعلقة بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، المصدر السابق.

2- المادة 5 من التعليمات رقم 02-25، المؤرخ في 2 مارس 2025، المتعلقة بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، المصدر نفسه.

أ. منح الترخيص:

بعد توفر جميع الشروط والاجراءات الواجب توفرها في طلب الترخيص المنصوص عليها في القانون رقم 09-23، والأنظمة الصادرة عن بنك الجزائر والتعليمة رقم 02-25، يتم منح ترخيص تأسيس واستغلال بنك رقمي من قبل المجلس النقدي والمصرفي، ويتولى الأمين العام تبليغ مقرر منح الترخيص إلى المعنيين.

كما يمكن أن يكون الترخيص مقترناً بشروط خاصة أو التزامات أو توصيات، وفقاً لما تتطلبه المادة 05 من النظام رقم 01-24²، ويترتب على قرار منح الترخيص تأسيس شركة خاضعة للقانون الجزائري وقيدتها في السجل التجاري، حيث يكتسب مشروع البنك الرقمي الشخصية المعنوية وذلك من خلال إيداع العقود التأسيسية وشهرها لدى المركز الوطني وإلا كانت باطلة وهذا طبقاً لأحكام المادة 548 من القانون التجاري، والمادة 04 من القانون رقم 04-08 المتعلقة بشروط ممارسة الأنشطة التجارية. ويرتب عن هذا الترخيص آثار، كما يتعين تقديم طلب للحصول على اعتماد بنك رقمي متى استوفت الشروط المنصوص عليها في القانون رقم 09-23، وكذا الشروط الخاصة المرفقة بالترخيص، وفقاً لأحكام المادة 100 فقرة 02 من نفس القانون.³

ب. رفض منح الترخيص:

1- محمد الطاهر سعيود، "إجراءات تأسيس البنك الرقمي في التشريع الجزائري"، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد 18، العدد 1، مارس 2026، ص 199.

2- محمد الطاهر سعيود، المرجع السابق، ص 199.

3- المرجع نفسه، ص 200.

في حالة عدم توفر الشروط المنصوص عليها في القانون 09/23 والأنظمة الصادرة عن بنك الجزائر يجوز للمجلس النقدي والمصرفي رفض طلب الترخيص، ويتمتع المجلس في هذا الإطار بسلطة تقديرية واسعة في دراسة الطلبات، دون الالتزام بتسبب قرار الرفض.¹

ويتم التبليغ مقرر الرفض من طرف الأمين العام للمجلس إلى صاحب الطلب، وله حق الطعن في القرار في 02 أجل 60 يوم أمام المحكمة الإدارية الاستئنافية لمدينة الجزائر، وهذا طبقاً لأحكام المادتين 67 و95 من القانون 23-09²، في السابق كان يشترط تقديم الطعن الثاني بعد 10 أشهر من أجل تبليغ القرار الأول، وهذا ما نص عليه الأمر 11-03 المتضمن قانون النقد والقرض (الملغى)، لكن التعليم 02/25 والقانون 23-09 وأنظمتها المعمول بها حالياً لا تشترط الطعن الثاني بل التوجه بالطعن مباشرة إلى القضاء الإداري.³

ج. أجل دراسة الملف:

لم يحدد المشرع الجزائري أجلاً معيناً للفصل في طلبات الترخيص بتأسيس مصرف رقمي، لكن في ظل القانون رقم 2000-03 المعدل والمتمم للنظام رقم 93-01 كانت الآجال مقيدة بشهرين، من ناحية أخرى نجد أن النظام رقم 08-03 الذي حدد شروط إنشاء بنوك ومؤسسات مالية، قد أخضع دراسة طلبات الاعتماد لآجال محددة، حيث يتعين على بنك الجزائر الفصل في الطلب خلال أجل أقصاه خمسة (05) أشهر ابتداءً من تاريخ استلام الملف القانوني.⁴

ثانياً: طلب الاعتماد:

1- محمد بولالي، زين الدين عطيط، المرجع السابق، ص 33.

2- المادتان 67 و95 من القانون 23-09، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق.

3- محمد الطاهر سعيود، المرجع السابق، ص 200.

4- النظام رقم 08-03، المؤرخ في 21 يوليو 2008، المتضمن تحديد شروط الترخيص بإقامة تعاونيات الإدخار والفرص وإعتمادها، ج ر ج ج، عدد 15، صادرة في 8 مارس 2009.

بعد إستيفاء الترخيص للشروط والإجراءات المنصوص عليها في النظام 01/24 والقانون 09/23 لا يعني انه قادر على القيام بالاجراءات والعمليات المصرفيه لابد من الحصول على الإعتماد حيث أنه الزمة القانون النقدي والمصرفي في 09/23 على أنه يجب المرور بمجموعة من الشروط والإجراءات لطلب الإعتماد.

1/ مفهوم الاعتماد :

بعد الحصول على الترخيص واستيفائه على جميع الشروط المنصوص عليها في القانون رقم 09-23 والنظام رقم 04-24، لا يخول للبنك الرقمي مباشرة نشاطه المصرفي إلا بعد نيل الاعتماد، حيث ألزم القانون النقدي والمصرفي في مادته 100 فقرة 4 الحصول على الاعتماد قبل ممارسة النشاط البنكي، ويتم منحه من قبل محافظ بنك الجزائر، وينشر في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية¹.

وعليه فإن طلب الاعتماد هو ذلك المقرر الذي يصدر عن محافظ بنك الجزائر والموجه لطالبيه بعد الحصول على ترخيص مسبق من مجلس النقد والقرض، والذي بموجبه يكتسب الشخص المعنوي صفة بنك أو مؤسسة مالية، ويخوله الحق في مباشرة الأعمال المصرفية المنصوص عليها في قانون النقد والقرض والأنظمة البنكية الصادرة عن بنك الجزائر².

2/ شروط طلب الاعتماد :

بعد تحصل المصرف على الترخيص واستيفائه لجميع الشروط المنصوص عليها في المواد سالفه الذكر من الهيئة المختصة، لابد أن يطلب الاعتماد في أجل أقصاه 12 شهرا لدى محافظ البنك مع

1- المادة 100 من القانون 09-23، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي..، المصدر السابق.

2- محمد بولالي، زين الدين عطيط، المرجع السابق، ص 35، ص 36.

إلزامية أن يكون الملف من نسختين الأولى رقمية والثانية ورقية، ومن بين أهم هذه الشروط والجراءات الذي يتضمنها ملف طلب الاعتماد:

- السجل التجاري

- نسخة أصلية من تقرير مندوبي الحصص.

- نسخة تثبت الاستقلالية في رأس المال محررة من طرف الموثق ومرفقة بإثبات بنك.¹

يجب أن تكون المؤسسة قد استوفت جميع الشروط المنصوص عليها والتي حددها القانون والأنظمة الخاصة بتأسيس المصرف ومسيريه، مع إلزامية قيام الجمعية العامة الخاصة بتأسيس البنوك والمؤسسات المالية إرسال قائمه المسيرين مرفقة ببيان مساهم المهني من أجل المصادقة عليها من قبل محافظ البنك.²

3/ البث في طلب الاعتماد :

أ. منح الاعتماد:

يمنح الاعتماد من طرف محافظ بنك الجزائر وذلك في حاله استيفاء الطلب لجميع الشروط والالتزامات الذي حددها المشرع، وذلك حسب ما نصت عليه المادة 100 من القانون رقم 09/23، ويصدر الاعتماد في شكل مقرر حيث يحدد مقرر الاعتماد صنف المؤسسة المصرفية كأن تكون بنك أو مؤسسة مالية أوفرع بنك أو مؤسسة مالية أجنبية كذلك مقر الشركة وأسماء أهم المسيرين ورأس مالها ... الخ.³

1- محمد الطاهر سعيود، المرجع السابق، ص 201، ص 202.

2- تقي الدين دغبوج، المرجع السابق، ص 618.

3- تقي الدين دغبوج، المرجع السابق، ص 618.

يقوم الأمين العام للمجلس بتبليغ مقرر الاعتماد، ويدخل حيز النفاذ ابتداء من تاريخ تبليغه، حيث تكون مرخصة من طرف البنك الرقمي وممارسة أنشطتها المصرفية طبقاً لأحكام المادة 11 من النظام رقم 04-24 إمكانية ممارسة البنوك الرقمية كل العمليات¹ المنصوص عليها في المواد من 68 إلى 75 من القانون 09-23، كما يمكن الاعتماد في الحالات المنصوص عليها في المادة 140 من القانون 09-23.

- إذا أصبحت الشروط التي يخضع لها الاعتماد غير متوفرة.
 - عدم الإستغلال الاعتماد لمدة 12 شهراً.
 - إذا توقف النشاط موضوع الاعتماد لمدة 06 أشهر.²
- كذلك، يمكن سحب الاعتماد في حالة إخلال أحد الخاضعين للأحكام التشريعية أو التنظيمية المتعلقة بنشاطها، وهذا طبقاً لأحكام المادة 126 من القانون 09-23³. وعليه، فإن سحب الاعتماد تختص به كل من اللجنة المصرفية والمجلس النقدي والمصرفي بالرغم أن صلاحيات منحه تكون من طرف محافظ بنك الجزائر.

ب. رفض طلب الإعتماد:

لم يتناول المشرع الجزائري حالة رفض طلب الإعتماد في أحكام القانون 09-23 للأنظمة الصادرة عن بنك الجزائر أو كيفية الطعن فيه، ولكن بالرجوع إلى الأحكام العامة المنصوص عليها في قانون الإجراءات المدنية والإدارية على إمكانية الطعن.

1- المادة 11 من النظام رقم 04-24، مؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة للترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، المصدر السابق.

2- المواد من 68 إلى 75 من القانون 09-23، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق

3- المادة 126 من القانون 09-23، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، المصدر السابق.

وعليه وبعد الرجوع الى المادة 900 مكرر من القانون 09/08 المعدل والمتمم بالقانون 13/22 التي تنص "تختص المحاكم الإدارية الاستئنافية للجزائر بالفصل كدرجة أولى في دعاوى إلغاء وتفسير وتقدير مشروعيه القرارات الإدارية الصادره عن السلطات الإدارية المركزية والهيئات العمومية الوطنية والمنظمات المهنية الوطنية"¹. وعليه أنه يمكن الطعن في القرار المتضمن رفض الاعتماد أمام المحكمة الادارية الاستئنافية للجزائر.

المبحث الثاني: تطور جرائم غسل الأموال في عصر البيئة الرقمية:

تعد جريمة غسل الأموال من الجرائم الإقتصادية العابرة للحدود التي تهدد أمن وإستقرار الدول نظرا لتأثيرها المباشر على الإقتصاد الوطني، حيث يسعى مرتكبي هذا النوع من الجرائم إلى إضفاء الصفة الشرعية على أموال متأتية من فعل غير مشروع يجرمه القانون، كتجارة المخدرات أو السلاح وغيرها من جرائم الفساد ودمجها في الدورة المالية عبر القنوات المصرفية وإعادة إستغلالها بشكل قانوني.

وقد ساهم التطور الهائل للأنظمة التكنولوجية إلى ظهور جرائم غسل الأموال أكثر حداثة ومواكبة للتطورات، ترتكب بطرق حديثة أكثر تعقيدا وخفاء مستغلة في ذلك الوسائل الحديثة التي تعتمد عليها المصارف الرقمية في تسهيل خدماتها المالية، كإستغلال وسائل الدفع الإلكتروني، والعملات المشفرة في تنفيذ مخططاتهم الإجرامية.

وبناء عليه نقسم هذا المبحث إلى مطلبين: نتناول في **المطلب الأول**: مفهوم غسل الأموال الإلكتروني، وفي **المطلب الثاني**: الأدوات الحديثة المستخدمة في إرتكاب جريمة غسل الأموال.

1- المادة 900 من القانون 09-08، المؤرخ في 25 فبراير 2008، يتضمن قانون الإجراءات المدنية و الإدارية، ج ر ج ج ، العدد 21، الصادرة في 23 ابريل 2008، المعدل و المتمم بالقانون رقم 22-13 المؤرخ في 12 يوليو 2022، ج ر ج ج ، العدد 48، الصادرة في 19 يوليو 2022.

المطلب الأول: مفهوم غسل الأموال الإلكتروني:

إن التسهيلات الخدماتية المصرفية التي تقدم من طرف المصارف الرقمية، والتي تمتاز بأنها مواكبة لتكنولوجيا المعلومات والابتكارات المستمرة في التقنيات المصرفية، أضحت تشكل عاملا جذابا للأشخاص المتورطين في الجرائم المنظمة أبرزها "جريمة غسل الأموال"، من منطلق أنها ساهمت في تبسيط الإجراءات المتعلقة بتحويل الأموال عبر الحسابات سواء كانت على مستوى محلي أو دولي، إضافة إلى أنها وفرت لمرتكبي هذه الجريمة الوقت والسرعة، حيث كان تنفيذ هذه العمليات يستغرق وقتا طويلا في حين أصبح القيام بها حاليا لا يتطلب إلا ثواني معدودة، أي بمجرد إدخال رموز رقمية سرية عبر أيقونات جهاز الكمبيوتر، هذا كله ساهم في جعل الفضاء الإلكتروني -رغم إيجابياته- يشكل خطرا بالنظر لإمكانية استغلاله من طرف المنظمات الإجرامية.

ومنه سنتطرق في تقسيم هذا المطلب إلى تعريف غسيل الأموال الإلكتروني (الفرع الأول)، نشأة وتطور غسيل الأموال الإلكتروني (الفرع الثاني).

الفرع الأول: تعريف غسل الأموال الإلكتروني:

تعد جريمة غسل الأموال الإلكتروني من الجرائم الاقتصادية الأكثر خطورة لارتباطها بالجرائم المنظمة والجرائم الإرهابية وجرائم الفساد، وقد حظي هذا النوع من الجرائم بإهتمام من قبل الدول من منطلق أن تأثيرها يتعدى حدود الدولة على اختلاف وضعها السياسي والاقتصادي والاجتماعي، ولقد تعددت الوسائل المعتمدة من قبل مرتكبي جريمة غسيل الأموال من وسائل تقليدية معروفة كالشركات الوهمية، القمار، شراء العقارات... إلخ وصولا إلى الوسائل التي تعتمد على التكنولوجيا الحديثة أبرزها اللجوء إلى التعامل بالنقود الإلكترونية، بطاقات الدفع الإلكتروني، البنوك الإلكترونية... إلخ، مما ساهم في ظهور مصطلح مغاير المفهوم التقليدي شكلا و مضمونا يطلق عليه "غسيل الأموال الإلكتروني".

وهذا ما سنتطرق إليه في دراستنا لهذا الفرع بتقسيمه إلى: تعريفات تشريعية أولاً، وتعريفات فقهية ثانياً.

أولاً: التعريف التشريعي لغسل الأموال الإلكتروني:

لقد تباينت مواقف التشريعات الوطنية والدولية بشأن تعريف غسل الأموال الإلكتروني، حيث عرف المشرع الإماراتي جريمة غسل الأموال الإلكتروني في المادة 30 من مرسوم بقانون إتحادي رقم 34 لسنة 2021 بشأن مكافحة الجرائم الإلكترونية بأنها: "هي كل من أتى عمداً باستخدام شبكة معلوماتية أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات أياً من الأفعال الآتية: -تحويل الأموال غير المشروعة، أو نقلها، أو إيداعها بقصد إخفاء أو تمويه المصدر غير المشروع لها -إخفاء أو تمويه حقيقة الأموال غير المشروعة، أو مصدرها، أو حركتها، أو الحقوق المتعلقة بها أو ملكيتها

- إكتساب، أو حيازة أو استخدام الأموال غير المشروعة مع العلم بعدم مشروعيتها مصدرها."¹ أما بالنسبة للمشرع المصري فلم يتطرق إلى تعريف غسل الأموال الإلكتروني في القانون رقم 175 لسنة 2018، بشأن جرائم تقنية المعلومات²، كما فعل المشرع الإماراتي واكتفى بتعريف غسيل الأموال التقليدي.

وفي هذا السياق نجد أن المشرع الجزائري تبنى نفس النهج الذي إعتمده المشرع المصري، ولم يتطرق لتعريف غسيل الأموال الإلكتروني واكتفى بذكر الحالات التي تشكل جريمة تبييض الأموال في نص

1- المادة 30 من مرسوم بقانون إتحادي رقم 34، المؤرخ في 20 سبتمبر 2021، المتضمن مكافحة الشائعات و الجرائم الإلكترونية، ج ر ، عدد 712، صادرة في 26 سبتمبر 2021، ص 17.(المعدل و المتمم)

2- القانون رقم 175 لسنة 2018، بشأن مكافحة جرائم تقنية المعلومات، ج ر، العدد 32، صادرة في 14 أغسطس 2018.

المادة 2 من القانون رقم 01-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم بموجب القانون رقم 10-25.¹

ثانيا: التعريف الفقهي لغسل الأموال الإلكتروني:

نظرا للانتشار المتزايد لجرائم غسل الأموال الإلكتروني، جعل منه محل إختلاف من قبل الفقهاء حول تحديد، ومن بين التعريفات الفقهية نجد ما يلي:

يعرف غسل الأموال الإلكتروني على أنه: "غسل الأموال الذي ينفذ عبر الشبكة العنكبوتية"، ويعرف بأنه: «إظهار الأموال الناتجة عن جرائم متعلقة بالتجارة غير المشروعة كالمخدرات والإرهاب وغيرها، وذلك من خلال نوع الصفة القدرة لها واستخدامها عبر الانترنت كوسيلة لإخفاء مصدرها غير الشرعي».²

وعرف كذلك على أنه: "هو ظهور الأموال المتحصلة من جرائم الاتجار بالتجارة غير المشروعة مثل المخدرات والإرهاب والقمار وغيرها بصورة أموال تتمتع بقانونية المصادر وشرعيتها، عبر استخدامها لشبكة الأنترنت كأداة لإخفاء هذا المصدر غير المشروع الذي تحصلت منه هذه الأموال".³

وتم تعريفه كذلك بأنه: "عملية تهدف إلى إضفاء صفة المشروعية على أموال ناتجة عن أنشطة غير قانونية مثل تجارة المخدرات أو الإرهاب أو القمار، وذلك من خلال استغلال شبكة الانترنت

1- المادة 2 من القانون رقم 01-05، المؤرخ في 6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم بموجب القانون رقم 10-25، ج ر، العدد 11، الصادرة في 9 فبراير 2005، ص 4.

2- سفيان بن تقي، " جريمة غسيل الأموال بين الوسائط الإلكترونية والمنصوص التجريمية "، مجلة الأبحاث القانونية والسياسية، جامعة سطيف 2، الجزائر، المجلد 03، العدد 02، أبريل 2021، ص 157.

3- بختة كرفاح، "غسيل الأموال عبر الوسائط الإلكترونية"، مذكرة ماستر في الحقوق، تخصص القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس -مستغانم، الجزائر، جوان 2022، ص 44.

كوسيلة لإخفاء الأصل غير القانوني لهذه الأموال بحيث تبدو وكأنها أموال ناتجة عن مصادر قانونية ومشروعة.¹

كما تم تعريف هذا المصطلح بأنه: "إظهار الأموال الناتجة عن جرائم متعلقة بالتجارة غير المشروعة كالمخدرات والإرهاب وغيرها، وذلك من خلال نزع الصفة الغير مشروعة لها، واستخدامها عبر الانترنت كوسيلة لإخفاء مصدرها غير الشرعي".²

ما يلاحظ من خلال التعريفات الفقهية السابقة أن جريمة غسل الأموال الإلكتروني هي عبارة عن تحويل الأموال المتأتية من مصادر غير مشروعة إلى أموال مشروعة باستخدام الوسائل التكنولوجية الحديثة، لإخفاء مصدرها الأصلي.

الفرع الثاني: نشأة وتطور غسل الأموال الإلكتروني:

ظهر مصطلح غسل الأموال الإلكتروني في العصور الوسطى إبان الكنيسة وتجرّمها الربا بوصفه جرماً يعاقب عليه، مما أدى بالتجار الراغبين في تخزين وإخفاء الفوائد التي يتحصلون عليها باللجوء إلى إنشاء الشركات الوهمية أو تزوير الفواتير.

وكان ظهور مصطلح غسل الأموال بمفهومه الحديث في الولايات المتحدة الأمريكية ما بين (1920-1930)، من خلال إستغلال رجال المافيا الأموال الغير مشروعة والمتحصل عليها من عمليات القمار والإبزاز وجعلها مشروعة وإستثمارها في إنشاء محلات تجارية.³

1- عبد العزيز منصور المليل، "جريمة غسيل الأموال عبر الفضاء الإلكتروني (دراسة تشريعية مقارنة)"، مجلة البحوث القانونية والاقتصادية، العدد 93، سبتمبر 2020، ص 795-796.

2- محمد طابع الهاني، "جريمة غسل الأموال عبر الأنترنت في التشريعين المصري والإماراتي"، مجلة الدراسات القانونية، جامعة أسيوط، مصر، العدد 66، الجزء 02، ديسمبر 2024، ص 721.

3- عبد الرحيم نادية -أمين بن سعيد، جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية، مجلة الدراسات الاقتصادية والمالية، جامعة الشهيد حمه لخضر -الوادي، الجزائر، العدد 10، الجزء 2، 2017، ص 28.

ومن أشهر قضايا غسل الأموال، قضية "Meyer Lansky" التي قام من خلالها بتحويل النقود من الولايات المتحدة الأمريكية وإيداعها لدى بنوك سويسرية بالإعتماد على قروض وهمية، وتليها قضية "ووترغيت" التي تم فيها إستغلال أموال غير مشروعة في تمويل حملة إعادة انتخاب الرئيس الأمريكي نيكسون.¹

إلا أن التطور الملحوظ الذي يشهده القطاع المصرفي في الآونة الأخيرة والتزايد المستمر لإستخدامات الأنترنت، أدى إلى ظهور المصارف الرقمية التي تعمل من خلال تقنيات تكنولوجيا حديثة إلا أنه وعلى الرغم من إيجابياتها إلا أنها فتحت أبوابا لظهور و إنتشار الجرائم الإلكترونية من بينها جريمة غسل الأموال الإلكترونية التي عملت على إستغلال الوسائل الحديثة وجعلها سلاحا إجراميا لتحقيق أهداف غير مشروعة طبقا لما يخدم المصالح، مما جعل هذا النوع من الجرائم سريع الإنتشار و يصعب القضاء عليه.

أضحت جريمة غسل الأموال الإلكترونية ترتكب من قبل المنظمات الإجرامية، مروراً بثلاثة مراحل أساسية تتمثل في، التبديل والإحلال التي يتم فيها تحويل كميات ضخمة من العائدات الغير مشروعة وتحويلها من سيولة إلى أرصدة عبر صفقات إلكترونية، بعدها يتم التعتيم والتغطية المالية بإضفاء صفة المشروعة على الأموال الغير مشروعة بإستخدام التقنيات الحديثة²، وأخيرا يتم دمج المصادر الغير مشروعة مع الأموال المشروعة ليصعب الكشف عنها وإستغلالها في عمليات بيع وشراء إلكترونية³.

1- عبد العزيز منصور الميل، المرجع السابق، ص 799.

2- المرجع نفسه، ص 799.

3- حشيفة مجدوب، "تبييض الأموال عبر أساليب الوفاء الإلكترونية"، مجلة القانون و العلوم السياسية، جامعة النعمانية، المجلد 8، العدد 2، ماي 2022، ص 661.

ومن أجل تطوير جرائم غسل الأموال الإلكتروني عمل مرتكبوها على الإستعانة بوسائط إلكترونية لجعلها من الجرائم المنظمة الأكثر تطورا ، نجد من بينها الإعتماد على البطاقات الإلكترونية التي تتيح لهم دفع المال دون الحاجة إلى حيازته نقدا، مما يتيح لهم إمكانية إستغلال بطاقات مسروقة أو مفقودة أو مزورة عبر شبكة الأنترنت¹، بالإضافة إلى اللجوء للبنوك الإلكترونية و التي تعد من أخطر الوسائل الحديثة المتبعة في تبييض الأموال ، لأنها تعتبر وسيلة مساعدة لمرتكبي هذا النوع من الجرائم حيث تمكنهم من تحويل كميات ضخمة من الأموال بسهولة و سرية بمجرد إدخال شفرة سرية في الكمبيوتر ، فهي تعمل في محيط من السرية التامة على إعتبار أن المتعاملون فيها غير معروفين الهوية.²

و يضاف إليها اللجوء إلى التحويل الإلكتروني للأموال الغير مشروعة الذي يتم من خلال الإستعانة بأحد الأنظمة التالية :نظام شيبس Chips ، نظام سويفت Swift، نظام الفيدواير Fed wire،³ كما يتم الإستعانة بالنقود الإلكترونية التي تشكل قيمة نقدية إلكترونية لعملة تصدر بشكل إلكتروني من قبل القطاع العام أو الخاص و يتم تخزينها في جهاز إلكتروني⁴، و هي تعد بمثابة وسيلة أستغلت من قبل غاسلي الأموال من ناحية أنها تسهل عملية غسيل الأموال ذلك أن التعامل بها لا يحتاج للإفصاح عن الهوية الحقيقية ، كما أنها توسع محل الجريمة فإستخدامها ينتج عنه زيادة حالات التهرب الضريبي ومنه صعوبة مراقبة الصفقات و فرض الضرائب.⁵

1- ذهبية لعجال -سي يوسف قاسي، " الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي "، مجلة الإجتهد القضائي، جامعة محمد خيضر -بسكرة، المجلد 13، العدد 25، جانفي 2021، ص 909.

2- بن تقي سفيان، المرجع السابق، ص 160.

3- ذهبية لعجال، المرجع السابق، ص 907.

4- باسم أحمد الزلي -عبود السراج، "دور النقود الإلكترونية في عمليات غسل الأموال"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، جامعة دمشق، المجلد 26، العدد الأول، 2010، ص 547.

5- العربي مولاي على -هاجر عاشي، "أثر النقود الإلكترونية على غسيل الأموال"، مذكرة مقدمة لنيل شهادة الماستر، تخصص إدارة مالية، جامعة ابن خلدون - تيارت، الجزائر، 2018-2019، ص 141، 142.

وبناء على ذلك يمكن القول بأن مصطلح غسل الأموال شهد إنتقلا ملحوظا من العالم الحقيقي إلى العالم الافتراضي معتمدا في ذلك على أساليب تقنية حديثة، وهو ما يشكل خطرا بالغاً لصعوبة تتبع آثار هذا النوع من الجرائم ومنه صعوبة القضاء عليه.

المطلب الثاني: الأدوات الحديثة المستخدمة في ارتكاب جريمة غسل الأموال:

سعت المصارف الرقمية لتسهيل عملياتها المصرفية و التقليل من الأعباء و التكاليف ، بتحديث وسائل تكنولوجيا حديثة تتيح إمكانية القيام بالمعاملات المالية في فترات وجيزة كالبطاقة الائتمانية الإلكترونية و الشيكات الإلكترونية و العملات المشفرة ، إلا أنه و بالرغم من التسهيلات التي حققتها إلا أنها أنشأت وبشكل غير مباشر وسائل خطيرة تم إستغلالها من قبل مرتكبي جريمة غسل الأموال ، كأحد أسرع و أضمن الطرق للقيام بهذه الجريمة ، على إعتبار أن وسائل الوفاء الحديثة تتسم بإنعدام و ضعف الرقابة على مصدر تلك الأموال ، من منطلق أن الوفاء يتم في بيئة رقمية.

ومنه نقسم هذا المطلب إلى فرعين نخصص: الفرع الأول: العملات المشفرة، الفرع الثاني: أدوات الدفع الإلكتروني.

الفرع الأول: العملات المشفرة:

العملات المشفرة هي عملات تتم عبر وسائط الإلكترونية، فهي من أبرز التطورات المالية الحديثة وهي ليست جريمة في حد ذاتها، فقد يكون استخدامها بشكل مشروع وقانوني، كما يمكن أن يكون استخدامها بطريقه غير شرعية، كإستخدامها في جريمة تبييض الأموال الإلكترونية، فهي تساعد على تسهيل إرتكاب هذه الجريمة، من خلال الخصائص والمزايا التي تتميز بها من بينها، أنها تخفي الهوية في نقطة إنشائها بمعنى أنها لا إسمية ولا تخضع إلى أي سلطة مركزية.

ومنه يمكننا تقسيم هذا الفرع إلى: تعريف العملات المشفرة أولاً، خصائصها ثانياً، أنواعها ثالثاً، العملة المشفرة كأداة لإرتكاب الجرائم رابعاً.

أولاً: تعريف العملات المشفرة:

العملات المشفرة هي "عملات رقمية، وليس لها وجود مادي مثل: "الدينار أو الدولار" وهي تعتمد على نظام لا مركزي، بحيث لا تخضع لحكم البنك المركزي أو غيره، بل تعتمد على نظام سلسلة الكتل "Blockchain" وهو نظام رقمي يعمل بطريقة آمنة وشفافة، "لأنه يمثل قاعدة بيانات قائمة على تخزين المعلومات في شكل قوالب تسمى الكتل، وتعمل على شكل تقسيم البيانات في شكل الكتل "blocks" وكل كتله تحتوي على بيانات، مثل: معاملات مالية توقيت العملية والرابطة بالكتلة السابقة، وهذا ما يشكل سلسلة، وتستخدم كدفتر حسابات موزع يتم فرضه من خلال أجهزة الكمبيوتر التي تحمل نسخة من هذا الدفتر.

"فالعملات الرقمية المشفرة هي عملات رقمية افتراضية، يتم تأمينها بالتشفير".¹

كما تعرف العملات المشفرة بأنها لا إسمية بمعنى أن مستخدميها مجهولي الهوية، وهذا راجع إلى عدم خضوعها إلى أي سلطة مركزية، وبالتالي فالهدف من هذا هو ضمان الثقة بين المستخدمين، وعدم الكشف عن هويتهم مع إمكانية فتح العديد من الحسابات بأسماء مستعارة.²

ثانياً: خصائص العملات المشفرة:

1- لامركزية: أي أنها عملة غير نظامية، وليست مدعومة من أي جهة رسمية أو منظمة دولية.

1- عبد الله لعور، عبد الرزاق كبوط، "العلاقة بين النقود الإلكترونية، العملات الرقمية، العملات الافتراضية، والعملات المشفرة: البحث في المفهوم"، مجلة الاقتصاد الصناعي (خوارتاك)، جامعة الحاج لخضر 1-باتنة، الجزائر، المجلد 11، العدد 02، 2021، ص 13.

2- عبد القادر مهاوات، محمد طه حميدي، "النقود المشفرة في الفقه الإسلامي"، مجلة المدونة، مجمع الفقه الإسلامي-بالهند، المجلد 7، العدد 26-27، أكتوبر 2010، ص 21.

2-محدودية العرض والندرة: ليست مثل البنوك المركزية للدول يمكنها طباعة النقود دون حدود لأن العملة المشفرة لها حدود للمعروض النقدي، ويتم تحديده عند برمجة الخوارزميات الأساسية لإنشائها.¹

3-الدقة والسرعة: أي أنه يمكن القيام بخدمات "البيع، الشراء" بطريقة سهلة وسريعة، وذلك لطبيعتها اللامركزية.²

4-مؤمنة: من خلال تأمين المعاملات وتشفيرها والتحكم فيها، كذلك إنشاء وحدات جديدة.³

ثالثا: أنواع العملات المشفرة:

من أهم العملات المشفرة هي:

"-البيتكوين كاش (Bitcoin cash) ويرمز لها Bch.

-الايثيريوم (Ethereum) ويرمز لها بالرمز ETH

- الريببل (Ripple) ويرمز لها XRP.

-الليتكوين (Litecoin) ويرمز لها LTC.

-المونيرو (monero) ويرمز لها XMR. "⁴.

رابعا: العملة المشفرة كأداة لإرتكاب الجرائم:

من المعروف أن العملات المشفرة هي عملة نقدية لامركزية أي أنها غير خاضعة إلى أي سلطة مركزية أو مؤسسة مثل "البنك المركزي"، وأنها لا إسمية بمعنى أن متعمليها مجهولي الهوية... إلخ، هذا

1- عبد الله لعور، عبد الرزاق كبوط، المرجع السابق، ص 16.

2- عبد القادر مهاوات، محمد طه حميدي، المرجع السابق، ص 21.

3- مزاجة تواتية، " العملات الرقمية في الجزائر: بين الموقف الاحترازي والتحول الرقمي"، مجلة المنتدى الدراسات والأبحاث الإقتصادية،

جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد 09، العدد 02، أكتوبر 2025، ص 102.

4- عبد القادر مهاوات، محمد طه حميدي، المرجع السابق، ص 20.

يجعلها أكثر وسيلة لارتكاب الجرائم من بينها جريمة غسل الأموال، التمويل والإرهاب، والبيع غير المشروع للأسلحة النارية وغيرها من الجرائم الأخرى، إذن سنوضح أهم هذه الجرائم فيما يلي:

1- العملات المشفرة وسيلة لإرتكاب جريمة غسل الأموال الإلكتروني:

من المعروف أن جرمه تبييض الأموال جريمة يعاقب عليها القانون، وأنها عبارة عن تحويل لعائدات مالية إجرامية إلى أموال مشروعة قابلة للتداول، بكل حرية وذلك من خلال المرور بمجموعة من المراحل، التي تم التطرق اليها سابقا وباستخدام مجموعة من التقنيات والأساليب الحديثة، في ارتكاب هذه الجريمة من بينها العملات المشفرة، ومن أهم الخصائص التي تتمتع بها العملات المشفرة هي أنها لا مركزية ولا إسمية، هذه الميزة تجعلها وسيلة أو أداة سهلة في ارتكاب جريمة غسل الأموال الإلكترونية، لأنها لا تحتاج إلى بروتوكولات خاصة، مثل الحصول على بيانات الشخصية للمستخدمين، أو الكشف عن هوياتهم وبالتالي فإن العملات المشفرة مثل ما لديها من مميزات، لديها مخاطر و التي يتم إستعمالها في عمليات غير مشروعة، وذلك لسريتها وغيرها من الخصائص التي تساعد في عملياتهم.¹

كما أن العملات المشفرة تصدر على عكس النقود الورقية الصادرة من جهة رسمية وهذا الأمر مغري بالنسبة للمجرمين وذلك ما يجعلها سهلة النقل والتخزين وتجنب من الوقوع في التحقيق والتفتيش، فالعملات المشفرة لا تكشف عن هوية الأشخاص، إذ أصبح الجناة يقومون بالعثور على طريقة لتحويل الأموال من د خل غير مشروع، الى ظاهر مشروع وإستخدامها في مشاريع إقتصادية، وغيرها من هذه النوع من المشاريع.²

1- جيلالي مانيو، "الاستخدام الإجرامي للعملات المشفرة"، مجلة القانون والعلوم السياسية، جامعة النعامة، الجزائر، المجلد 06، العدد 10، أوت 2020، ص 141.

2- أمل مرزوق، "البتكوين نقود جديدة أم فعالية مالية؟"، مجلة شعاع للدراسات الاقتصادية، جامعة تلمسان، الجزائر، المجلد 03، العدد 2، سبتمبر 2019، ص 78.

2- العملات المشفرة وسيلة لشراء وبيع الاحجار الكريمة والعقارات بطرق غير مشروعة:

تساعد العملات المشفرة المجرمين في القيام بعمليات غسل الأموال الإلكترونية، عبر شراء المجوهرات والعقارات، باستخدام بطاقات او أجهزة الصرف الالي أو عن طريق المقايضة، بهدف دخول الأموال من بلد الى بلد اخر كأنها أموال مشروعة.¹

3- العملات المشفرة وتمويل الإرهاب:

العملات المشفرة هي عملة تساعد على تسهيل الخدمات المصرفية لمستخدميها لكن هناك من يستعملها بطريقة غير قانونية من خلال جمع التبرعات والإسهامات المالية بغض النظر عن مصدرها داخلي أو خارجي، من أجل تمويل الجماعات الإرهابية، وقد تكون هذه الأموال من مصادر مشروعة أو غير مشروعة، وعلى الرغم من أن تمويل الإرهاب قد يكون مشروع لكن يبقى تمويل الإرهاب جريمة يعاقب عليها القانون.²

الفرع الثاني: الشيكات الإلكترونية وبطاقات الائتمان:

تعد الشيكات الإلكترونية وبطاقات الائتمان من أهم وسائل الدفع الحديثة التي انتشرت مع التطور التكنولوجي وازدهار التجارة الإلكترونية، حيث ساهمت في تسهيل المعاملات المالية وجعلها

1- هواري قعموسي، "تجريم العملات الافتراضية الرقمية بقانون تبيض الأموال 10/25 بالجزائر"، المجلة الجزائرية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، المجلد 10 العدد 02، ديسمبر 2025، ص 6.

2- هنية شريف، الأساليب الحديثة للإجرام المنظم - تبيض الأموال نموذجاً -، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجزائر، المجلد 12، العدد 2. سبتمبر 2019، ص 14-ص 15.

أكثر سرعة ومرونة مقارنة بالوسائل التقليدية. فالشيكات الإلكترونية تُمكن من تحويل الأموال رقمياً بين الحسابات البنكية، بينما تسمح بطاقات الائتمان بشراء السلع والخدمات والدفع لاحقاً ضمن حد ائتماني يحدده البنك، كما تتميز هذه الوسائل بسهولة الاستخدام وإمكانية إتمام العمليات المالية عبر الإنترنت في أي وقت ومن أي مكان، إلا أنها تتطلب أنظمة أمان وحماية قوية لتجنب مخاطر الاحتيال والاختراق الإلكتروني. وهذا ما سنعالجه في هذا الفرع، من خلال التطرق للشيكات الإلكترونية أولاً، وبطاقات الائتمان ثانياً.

أولاً: الشيك الإلكتروني:

الشيك الإلكتروني هو مستند رقمي يُستخدم لإتمام عمليات الدفع والتحويل المالي عبر الإنترنت، ويحتوي على نفس البيانات الموجودة في الشيك الورقي التقليدي مثل: اسم الساحب، اسم المستفيد، قيمة المبلغ، تاريخ الإصدار والتوقيع الإلكتروني. ويتم إرسال الشيك ومعالجته إلكترونياً عبر أنظمة مصرفية آمنة دون الحاجة إلى استعمال الورق.¹

1/تعريف الشيك الإلكتروني :

1- محمد الامين بن قايد علي، "الشيك الإلكتروني امتداد وتطور الشيك التقليدي"، مجلة بحوث في القانون والتنمية، جامعة أحمد بوقرة، بومرداس، الجزائر، المجلد 2، العدد 2، 2022/12، ص 85، ص 86.

لم يضع المشرع الجزائري تعريفاً صريحاً للشيك الإلكتروني، لكنه أشار إلى وسائل الدفع الإلكترونية في بعض النصوص القانونية، ومن أهمها:¹

القانون رقم 03-11 المتعلق بالنقد والقرض، وخاصة المادة 69 التي تنص على أن وسائل الدفع تشمل كل الأدوات التي تمكن من تحويل الأموال مهما يكن السند أو الأسلوب التقني المستعمل.²

الأمر رقم 05-06 المؤرخ في 23 أوت 2005 المتعلق بمكافحة التهريب، والذي استعمل صراحة مصطلح "وسائل الدفع الإلكتروني".³

وبسبب غياب تعريف قانوني دقيق، اجتهد الفقه في تعريف الشيك الإلكتروني باعتباره: " محرراً رقمياً يُعالج إلكترونياً كلياً أو جزئياً، يتضمن أمراً من الساحب إلى البنك بدفع مبلغ مالي لفائدة المستفيد أو الحامل". ويعتمد الشيك الإلكتروني على التوقيع الإلكتروني والمعالجة الرقمية للبيانات بين الأطراف والبنوك.⁴

يحتوي الشيك الإلكتروني على البيانات التالية: رقم الصك واسم الدافع ورقم حساب الدفع واسم المصرف واسم المستفيد والقيمة التي ستدفع ووحدة العملة المستعملة وتاريخ الصلاحية والتوقيع الإلكتروني ولا يشترط أن يكون مكتوب بخط اليد وموقعا بواسطة الشخص الذي يصدره.⁵

1- نبيلة كردي، " الشيك الإلكتروني"، مجلة العلوم الاجتماعية والسياسية، جامعة العربي التبسي، الجزائر، المجلد 10، العدد 2، جوان 2017 ص 249.

2- المادة 69 من الأمر رقم 03-11، المؤرخ في 26 غشت 2003، يتعلق بالنقد والقرض، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 52، الصادرة 27 أوت 2003.

3- الأمر رقم 05-06، المؤرخ في 23 غشت 2005، يتعلق بمكافحة التهريب، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 59، الصادرة في 28 غشت 2005.

4- كردي نبيلة، المرجع السابق، ص 250، ص 251.

5- ذهبية لعجال - قاسي سي يوسف " الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي"، مجلة الإجتهد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد 13، العدد 1، جانفي 2021، ص 215.

يتم تداول الشيك الإلكتروني عبر منظومة بنكية رقمية تتيح إنشاء الشيك وإرساله واستقباله بشكل إلكتروني دون استعمال الورق، حيث يقوم الساحب بإصدار الشيك من خلال تطبيق البنك أو منصته الرقمية، مع تحديد بيانات المستفيد والمبلغ والتاريخ، ثم يُوقَّع الشيك بتوقيع رقمي مشفّر يضمن صحته وأمانه. بعد ذلك يُرسل الشيك إلى المستفيد الذي يتلقاه إلكترونياً، ويمكنه تقديمه للبنك للحصول أو إيداعه في حسابه.

يقوم النظام البنكي بالتحقق آلياً من صحة الشيك وتوفر الرصيد ومنع التكرار أو التزوير، ثم تتم عملية تحويل الأموال عبر أنظمة المقاصة الإلكترونية بين البنوك إذا لزم الأمر، ليتم في النهاية إيداع المبلغ في حساب المستفيد بشكل سريع وآمن¹.

2/ مميزات الشيك الإلكتروني :

* يتميز الشيك الإلكتروني بمجموعة من المميزات نجملها فيما يلي:

- التخلص من مشكلة الشيكات المرتدة والمؤجلة، وذلك من خلال وجود الشكل المغنط والذي يتطلب توفر رصيد بنك المسحوب عليه في رصيد الساحب.

- التقليل من عمليات غسيل الأموال من خلال تحويل الأموال المتحصل عليها من الأنشطة الإجرامية إلى أموال تتمتع بمصدر قانوني سليم².

- يوفر التعامل به حوالي 50% من الرسوم التشغيل بالمقارنة ببطاقات الائتمان.

- التحقق من المدفوعات خلال 48 ساعة فقط من بالمقارنة بالشيكات العادية التي تأخذ وقت طويل من خلال غرفه المقاصة¹.

1- جميلة خرباش، "الشيك الإلكتروني أداة وفاء عن بعد في التجارة الإلكترونية"، مجلة البيان للدراسات القانونية والسياسية، جامعة برج بوعريش، الجزائر، المجلد 3 العدد 1، جوان 2018، ص ص 188، 190.

2- نبيلة كردي، المرجع السابق، ص 255

- بعث الثقة في المتعاملين بالشركات يعزز الشيك الإلكتروني الثقة بين الأطراف بفضل دقه التحقق من البيانات والتأكد من وجود الرصيد الكافي قبل تنفيذ العملية².

3/ استخدام الشيك الإلكتروني في عمليات غسل الأموال :

أدت التطورات التكنولوجية الحديثة إلى استغلال الوسائل الإلكترونية في عمليات تبييض الأموال، من خلال استخدام الحسابات البنكية الرقمية ووسائل الدفع الإلكتروني لتحويل الأموال وإخفاء مصدرها غير المشروع.

وتتم هذه العمليات عبر تحويل الأموال بين عدة حسابات أو جهات داخلية وخارجية بسرعة كبيرة، مما يصعب على الجهات المختصة تتبعها وكشف حقيقتها، كما ساهمت شبكة الإنترنت والتقنيات الحديثة في تسهيل هذه الجرائم ومنحها طابعاً عابراً للحدود.

لذلك، أصبحت مكافحة تبييض الأموال الإلكترونية تتطلب تعزيز الرقابة القانونية وتطوير وسائل التتبع والتحري الرقمي للحد من هذه الجرائم³.

ثانياً: بطاقة الائتمان الإلكترونية:

تعد بطاقات الائتمان من وسائل الدفع الحديثة، والتي كان ظهورها نتاجاً للاستخدامات الواسعة للحسابات الآلية وانتشارها في جل القطاعات، ومن أبرزها القطاع المصرفي، حيث تعمل هذه الوسيلة على تسوية المعاملات البنكية بين البنوك والأفراد، معتمدة في ذلك على نظام التحويل الآلي للنقود، هذا ما ساهم في زيادة التعامل بها من قبل العملاء.

1- ذهبية لعجال، قاسي سي يوسف المرجع السابق، ص 915، ص 916.

2- جميلة خرباش، المرجع السابق، ص 186.

3- ذهبية لعجال - قاسي سي يوسف، المرجع السابق، ص 916.

1-تعريف بطاقة الائتمان الإلكترونية :

تعددت وتنوعت التعريفات الخاصة بهذا المصطلح، مما أدى إلى تباين المصطلحات التي تطلق على هذا النوع من البطاقات مثل: بطاقة الدفع الإلكتروني، بطاقات الاعتماد، بطاقات الوفاء الحديثة، إلا أن الأكثر شيوعاً وتعبيراً على حقيقتها من الناحية اللغوية والعملية هو بطاقة الائتمان.

تعرف بطاقات الائتمان على أنها: " البطاقات التي تصدرها المصارف في حدود مبالغ معينة ويتم استخدامها كأداة ضمان، و تتميز هذه البطاقات بأنها توفر كلا من الوقت و الجهد لحاملها، وكذلك تزيد من إجراءات البنك المصدر لها لما يحصل عليه من رسوم مقابل الخدمات أو من فوائد مقابل التأخر في السداد، ولا يتم إصدار هذه البطاقات إلا بعد دراسة جيدة لموقف العميل حتى لا يواجه البنك المصدر مخاطر عالية في حالة عدم السداد."¹

كما تعرف بأنها: " أداة مصرفية للوفاء بالتزامات مقبولة على نطاق واسع محليا ودوليا، كبديل للنقود لدفع قيمة السلع والخدمات المقدمة لحامل البطاقة، مقابل توقيعه على إيصال بقيمة التزامه الناشئ عن شرائه للسلعة أو حصوله على الخدمة."²

2-أنواع البطاقات الائتمانية :

هناك نوعان من البطاقات الائتمانية تتجلى في:

1- إبتسام السائيس - صفاء نيلي، "وسائل الدفع في التجارة الإلكترونية"، مذكرة ماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح -ورقلة، 2019-2020، ص38.

2- نوال بلعباس، "بطاقة الائتمان كوسيلة من وسائل الدفع الحديثة"، أطروحة دكتوراه علوم في القانون، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر 1، 2016-2017، ص 30.

أ- البطاقات الائتمانية المتجددة: هذا النوع هو الأكثر انتشارا يصدر عن بنك تجاري يحتوي على حساب نقدي لصاحب البطاقة، بحيث يتولى البنك المصدر تسديد فواتير الشراء وإرسالها شاملة للعميل حسب المشتريات، وهنا حامل البطاقة مخير إما سداد كل قيمة الفاتورة خلال فترة الاستفادة أو تسديد جزء منها فقط مع استكمال الباقي خلال فترة لاحقة، ويتم في كلتا الحالتين تجديد القرض لذلك سميت بالبطاقة المتجددة، ومن أمثلة هذه البطاقة نجد: فيزا visa، ماستركارد Master card¹.

ب- البطاقات الائتمانية غير المتجددة: تختلف عن النوع الأول، ذلك أنها تشترط على حامل البطاقة أن يكون السداد كاملا للمبلغ في المدة المحددة والتي تقدر بـ 40 يوما، وفي حالة عدم التسديد لا يمنح حاملها قرضا جديدا وإنما تسحب منه البطاقة، ومن أهم المؤسسات المصدرة لهذا النوع من البطاقات نجد داينيرز كلوب وأمريكان اكسبريس.²

3- الجهات المصدرة لبطاقة الائتمان: نجد أبرزها:

- أ- المنظمات العالمية: والتي تعمل على منح تراخيص إصدار البطاقات الائتمانية وإدارة خدماتها.
- ب- المؤسسات المالية الكبيرة: تعمل على إصدار البطاقات الائتمانية مباشرة دون أن تخول أي مصرف أو مؤسسة مالية، أبرزها الدينيرز كلوب والتي تبلغ عدد بطاقتها 6.9 مليون بطاقة.
- ج- المؤسسات التجارية الكبرى: أصدرت المؤسسات والمحلات التجارية بطاقات تخص العملاء المتميزين والتي تتيح لهم إقتناء السلع والخدمات في حدود قيمة إئتمان محدد.

1- هشام لبزة- محمد الهادي ضيف الله، " واقع وتحديات وسائل الدفع الإلكترونية في الجزائر"، مجلة الدراسات والبحوث الاجتماعية، جامعة الشهيد حمه لخضر -الوادي، الجزائر، العدد 24، ديسمبر 2017، ص 282.

2- عبد القادر مطاي- كريمة بن شنيعة- محمد صلاح، " وسائل الدفع الإلكترونية ودورها في عصنة المنظومة المصرفية الجزائرية، مجلة الإقتصاد الحديث والتنمية المستدامة، جامعة تيسمسيلت، المجلد 2، العدد 2، جوان 2020، ص 33.

4- أطراف البطاقة الائتمانية :

بما أن بطاقة الائتمان تمنح لحاملها حق الحصول على السلع والخدمات دون الوفاء بثمنها حالا، مما يدل على أن تفعيلها يحتاج إلى تعدد الأطراف فيها، والتي تتمثل في:

أ- **مصدر البطاقة L'émetteur**: وتتمثل في كل من البنك والمؤسسات المالية التي يخول لها قانونا إصدار البطاقة لحاملها، والتعاقد مع مقدمي الخدمات لقبول التعامل بهذه البطاقة من قبل عملائه للحصول على السلع أو الخدمات.

ب- **مقدم الخدمة Fournisseur**: وهو الجهة التي توافق على التعامل ببطاقة الائتمان من قبل حاملها واستعمالها كوسيلة دفع مقابل ما تم إقتناؤه من سلع أو ما تم الحصول عليه من خدمات، ولا يتم قبول التعامل بها إلا في حالة وجود تعاقد سابق مع مصدر البطاقة لضمان الوفاء بها.

ج- **حامل البطاقة أو العميل le titulaire**: وهو الشخص الذي أصدر البطاقة لصالحه، بغرض استخدامها كوسيلة دفع للحصول على خدماته ويتم الحصول عليها عن طريق التعاقد مع الجهة المصدرة بعد التوقيع على شروط حسن إستعمالها، ويتم دراسة الطلب بعد التأكد من توفر الضمانات الكافية.¹

5- إستخدام بطاقة الائتمان في عمليات غسل الأموال:

تعد بطاقة الائتمان من وسائل الدفع الإلكترونية التي تسهل جريمة غسيل الأموال، على اعتبار أنها أصبحت تستعمل من قبل مرتكبي الجريمة كأسلوب حديث في ارتكاب هذا النوع من الجرائم. ومن أبرز استعمالاتها نجد:

- استغلال بطاقة مسروقة أو مفقودة أو مزورة بالحصول على أرقامها عبر شبكة الأنترنت.

¹ - عبد القادر مطاي - كريمة بن شنيعة، المرجع السابق، ص 34.

- استغلالها لإدخال الأموال الغير مشروعة في الحركة المالية.
- تزوير بطاقات الائتمان والتحايل لمعرفة المعلومات المتعلقة بالرقم السري لصاحب الحساب بهدف سحب الأموال.
- تدوير الأموال الغير مشروعة وذلك بإصدار العميل بقيمة تتجاوز قيمة البطاقة ومنه يقوم بتسديد مستحقات البنك مصدر البطاقة أو المستفيد من البنك إذا قام بالرجوع عليه من الأموال التي تحصل عليها من مصدر غير مشروع.¹

¹ - ذهبية لعجال - سي يوسف قاسي، المرجع السابق، ص 909-ص919.

خلاصة الفصل:

نتيجة للتطورات السريعة والتغيرات التي يشهدها القطاع المصرفي وتلبية للإحتياجات المتنامية الزبائن، سعت العديد من المصارف إلى الاندماج في التحول الرقمي بغاية تحسين جودة الخدمات وكفاءتها وسهولة تقديمها، هذا ما ساهم في ظهور مصطلح المصارف الرقمية كنموذج متقدما للمصارف يعمل على تقديم خدمات مصرفية تتماشى مع التطور التكنولوجي الحديث، مستعينة في ذلك بوسائل مصرفية أكثر حداثة كبطاقات الدفع الإلكتروني والتحويلات الإلكترونية. إلا أن التسهيلات التي تقدمها المصارف الرقمية لم يتم إستغلالها من الجانب الإيجابي، وإنما تم إستغلالها في الجانب السلبي و إتخذوا منها أداة للقيام بعملياتهم الإجرامية، و أبرزها جريمة غسل الأموال التي سعى من خلالها غاسيلي الأموال إلى إضفاء الصفة القانونية على أموالهم غير المشروعة بإستعمال الوسائل المصرفية المستحدثة.

الفصل الثاني

إلتزام المصارف الرقمية بمكافحة غسل الأموال بين
المسؤولية القانونية والفجوات العملية

تعتبر جريمة غسل الأموال أحد أخطر جرائم عصر الاقتصاد الرقمي ، عل اعتبار أنها أصبحت تشكل التحدي الحقيقي أمام المؤسسات المالية بالنظر إلى ارتباطها بالاقتصاد الوطني، وقد تطورت هذه الجرائم مع مرور الزمن تماشياً مع التطور التكنولوجي ، إلا أنه ومن المعروف أن المصارف الرقمية أضحت تلعب دوراً هاماً في تسيير عمليات غسيل الأموال من منطلق إمكانية إستغلالها من قبل مرتكبي جريمة غسل الأموال ، و قد أدى تنامي مخاطر غسل الأموال في البيئة الرقمية إلى ضرورة تحميل المصارف الرقمية مسؤولية قانونية متزايدة مجال مكافحة هذا النوع من الجرائم ، وذلك من خلال إخضاعها لمنظومة من القواعد و الأنظمة الرقابية و الحاكمة التي تهدف إلى ضمان سلامة العمليات المصرفية الرقمية و مشروعيتها ، ويتجسد ذلك في إلزامها بالتحقق من هوية العملاء بإستخدام تقنيات متطورة و مراقبة المعاملات المالية بصورة مستمرة و رصد العمليات المشبوهة و الإبلاغ عنها للجهات المختصة بما يكفل حماية البيانات الشخصية للعملاء و الحد من مخاطر الإعتداء عليها وإساءة إستخدامها .

غير أن فعالية المصارف الرقمية في مكافحة جرائم غسل الأموال قد تواجهه العديد من الفجوات والثغرات التي تشكل نقاط ضعف يمكن إستغلالها من قبل المجرمين لتنفيذ أنشطتهم الغير مشروعة، والتي تتمثل أساساً في الهجمات السيبرانية التي تستهدف الأنظمة المعلوماتية، إضافة إلى الفجوات الرقابية الناجمة عن التباين العالمي في الأنظمة الرقابية وزيادة الاعتماد على مزودي الخدمات دون تراخيص وعدم توافر آليات رقابية لحماية تبادل البيانات الشخصية.

سوف نسعى من خلال هذا الفصل إلى إستعراض: إلزام المصارف الرقمية بمكافحة غسل الأموال بين المسؤولية القانونية والفجوات العملية، والذي تم تقسيمه إلى مبحثين:

- المبحث الأول: المسؤولية القانونية للمصارف الرقمية في مكافحة غسل الأموال.
- المبحث الثاني: الفجوات والثغرات التي تهدد مهام المصارف الرقمية في مكافحة غسل الأموال.



المبحث الأول: المسؤولية القانونية للمصارف الرقمية في مكافحة غسل الأموال.

تعد المصارف الرقمية أحد أهم المقاصد التي يلجأ إليها غاسيلي الأموال غير المشروعة لإضفاء الصفة القانونية عليها، نظراً لما يتمتع به هذا النوع من المؤسسات المالية من سرعة وكفاءة في عملياتها المصرفية، الأمر الذي جعل منها أكثر فضاء ملائم لإرتكاب جرائم غسيل الأموال، وهذا الدور في تزايد نتيجة لتقدم العمليات المصرفية واستخدام الوسائل والأساليب التقنية الحديثة. الأمر الذي يضع المصارف الرقمية أمام مسؤولية تتمثل في مكافحة جرائم غسيل الأموال، بإتاحة جملة من الإلتزامات كضرورة التحري عن هوية العملاء ومراقبة عملياته والإبلاغ في حالة الإشتباه بإرتباطها بغسيل الأموال للهيئات المعنية الموكلة لها هذه المهمة، مع الأخذ بضرورة تطوير وحسن إستغلال التقنيات الرقمية.

بناءً عليه نقسم هذا المبحث إلى مطلبين: **المطلب الأول: المسؤولية عن تطبيق الأنظمة الحاكمة والرقابية. المطلب الثاني: المسؤولية عن حسن إستعمال التقنيات الرقمية الحديثة**

المطلب الأول: المسؤولية عن تطبيق الأنظمة الحاكمة والرقابة

تشكل الحوكمة والرقابة في المصارف الرقمية إطاراً أساسياً لضمان سلامة العمليات المصرفية وحماية العملاء وتعزيز الثقة في الخدمات الرقمية، وتقع مسؤولية تطبيقها على الإدارة والجهات الرقابية داخل المصرف من خلال الإلتزام بالمتطلبات القانونية والتنظيمية، وتطبيق مبدأ إعراف عميلك الإلكتروني (e-KYC) للتحقق من هوية العملاء، ومراقبة المعاملات للكشف عن الأنشطة المشبوهة ومكافحة غسل الأموال، إضافة إلى إدارة المخاطر وضمان الشفافية والامتثال وتحقيق الإستقرار والكفاءة والاستدامة في العمل المصرفي الرقمي.

وهذا ما سنعالجه في هذا المطلب من خلال تقسيمه إلى فرعين: التحقق من هوية العملاء ومن مصادر الأموال **الفرع الأول**، الإبلاغ عن الأنشطة المشبوهة **الفرع الثاني**.

الفرع الأول: التحقق من هوية العملاء ومن مصادر الأموال:

مع التطور السريع للخدمات المالية الرقمية، أصبحت المصارف الرقمية تعتمد على وسائل حديثة للتحقق من هوية العملاء وضمان مصداقية المعلومات المقدمة، بهدف تعزيز الأمان والحد من الجرائم المالية، وتشمل هذه الوسائل تقنيات رقمية متطورة تتيح التعرف على العملاء عن بُعد مثل التحقق الإلكتروني من الهوية واستخدام البيانات البيومترية، إضافة إلى تحليل البيانات ومراقبة مصادر الأموال في إطار الامتثال للأنظمة الرقابية. وفي هذا السياق، يبرز في النهاية مبدأ اعرف عميلك (KYC) واعرف عميلك إلكترونياً (e KYC) كأساسين مهمين لضمان الشفافية وبناء الثقة في القطاع المصرفي الرقمي،

وهذا ما سنعالجه في هذا الفرع: أولاً: مفهوم الهوية الرقمية المصرفية، ثانياً: آليات الكشف عن هوية العملاء.

أولاً: مفهوم الهوية الرقمية المصرفية:

تُعد الهوية الرقمية المصرفية أداة أساسية ضمن الإطار الحديث لتعزيز الشمول المالي، حيث تُمكن المؤسسات المالية من التحقق من هوية العملاء عن بُعد بطريقة آمنة وموثوقة، بما يتوافق مع المعايير الدولية، لاسيما توصيات مجموعة العمل المالي المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب.

1/تعريف الهوية الرقمية:

يمكن تعريف الهوية الرقمية على أنها "مجموعة السمات ووثائق الاعتماد التي يتم تسجيلها وتخزينها إلكترونياً، والتي يمكن أن تحدد هوية الشخص بصورة مميزة «، حيث يمكن استخدام الهوية

الرقمية مثلاً: كالهوية التأسيسية أو وظيفية أو وثيقة هوية، التي تثبت هوية الشخص، حيث قد إلى الهوية مادية لكونها مرتبطة بالبيانات المركزية وليس وقتياً.¹

عرفها معهد ما كيزي العالمي (MCK) على "أنها عملية تحديد الهوية ويجب أن يتم التحقق من صحتها ومصداقيتها درجة عالية من التأكيد بالاعتماد على تقنيات رقمية عالية الكفاءة والتي تقلدها وتزويرها، الأمر الذي يعمل على ضمان كل من خصوصية وأمن المعلومات والبيانات المتعلقة".²

2/تعريف الهوية الرقمية المصرفية :

"هي عبارة عن وسيلة تدعم المؤسسات المصرفية، عن طريق (الفحص والتحري)، حول هوية العملاء من خلال مرحلتين: الانضمام، التحديث، وهذا ما يجعلها طريقة آمنة تساعد المؤسسات المالية التحقق من بيانات ومعلومات العملاء، بالاعتماد على التقنية الرقمية".³، "بما يتوافق مع المعايير الدولية، لاسيما توصيات مجموعة العمل المالي المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب".⁴

"كما تُعرّف بأنها منظومة بيانات رقمية مميّزة تُستخدم للتحقق من شخصية العميل عبر قنوات إلكترونية، وتعتمد على تقنيات حديثة مثل التشفير والقياسات الحيوية (البصمة، التعرف على الوجه بما يضمن عدم إمكانية تزويرها أو تقليدها، مع الحفاظ على سرية البيانات الشخصية".⁵ "بساطة هي "بطاقة تعريف رقمية" تحتوي على معلوماتك الشخصية (مثل الاسم، رقم الهوية، رقم الحساب...) وتُستخدم للدخول إلى الخدمات البنكية عبر الإنترنت أو الهاتف".

¹ - هند زيتوني - ذهبية ريمة بوبعاية، "حلول الهوية الرقمية في معرفة العميل ودورها في تعزيز الشمول المالي"، مجلة التمويل والاستثمار والتنمية المستدامة، جامعة فرحات عباس بسطيف 1، الجزائر المجلد 08، العدد 01، جوان 2023، ص 523.

² - رمزي طبائية: "الهوية الرقمية المصرفية كتوجه حديثي تحسين الخدمات المصرفية الإلكترونية نظام Aadhaar الهندي نموذجاً"، المجلة الجزائرية للعلوم الاجتماعية الإنسانية، جامعة الجزائر 3، الجزائر، المجلد 11، العدد 02، نوفمبر 2023، ص 141.

³ - المرجع نفسه، ص 141، 142.

⁴ - هند زيتوني، ذهبية ريمة بوبعاية، المرجع السابق، ص 533.

⁵ - حدة مشراوي - عائدة عبير بالعبدي، "دور الهوية الرقمية المصرفية في رفع مستويات الشمول دراسة حالة بعض الدول العربية"، مجلة الاقتصادية المالية البنكية إدارة الأعمال، جامعة محمد خيضر بسكرة، الجزائر، المجلد 12، العدد 01، أبريل 2023، ص 221.

ثانياً: آليات الكشف عن هوية العملاء ومصادر الأموال:

يُعد مبدأ "اعرف عميلك" (KYC) من الآليات الأساسية في القطاع المالي، حيث يهدف إلى التحقق من هوية العميل والتأكد من صحة بياناته، إضافة إلى فحص مصادر أمواله للتثبت من مشروعيتها. ويساهم هذا الإجراء في الحد من الجرائم المالية وتعزيز الشفافية، خاصة في ظل تزايد الاعتماد على المعاملات الرقمية.

1/ مبدأ إعرف عميلك (kyc):

هو وسيلة يتم من خلالها التعرف على هوية العميل والأوضاع القانونية، كما يستخدم هذا المصطلح في تحديد نوع المستفيدين الحقيقيين، أشخاص طبيعيين أو اعتباريين، من خلال وسائل إثبات القانونية، حيث يتوجب على البنوك القيام بطلب جميع البيانات والمعلومات الخاصة بعملائهم، وطبيعة الأنشطة التي لا يقومون بها ومصادر أموالهم وغيرها ذلك من خلال: جمع وتحليل البيانات الأساسية للعميل من مصادر موثوقة، وتقييم مستوى المخاطر المرتبطة به، خاصة فيما يتعلق باحتمال تورطه في جرائم غسل الأموال أو تمويل الإرهاب. كما تتضمن إنشاء ملف تعريف شامل للعميل يحدد طبيعة أنشطته المتوقعة، مع إخضاع معاملاته لرقابة مستمرة لمقارنتها بالسلوك المتوقع والكشف عن أي انحرافات¹.

كما أكدت مجموعة العمل المالي (FATF) في توصياتها² 40، أنه لا يمكن فتح أي حساب من الحسابات المصرفية، أو قبول أموال أو ودائع مجهولة المصدر قبل التأكد من هوية العميل، وهذا بهدف

¹ - هند زيتوني - بوعاية ذهبية ربة، المرجع السابق، ص 525-526.

² - مجموعة العمل المالي، المعايير الدولية لمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسليح، مجموعة العمل المالي، باريس، فرنسا، 2003.2.12، www.fatf-gafi.org/recommendations.html، تاريخ الاطلاع 21/05/2026، 10:56.

عدم وجود أي شبهات في العمليات التي يجريها العميل، وعملية هي لا تقتصر فقط على معرفة هوية العميل، بل تراقب حركة ونشاط حساب العميل، والتعرف على أي نشاطات مشبوهة¹.

بالرغم من ارتباط مبدأ اعرف عميلك بجريمة غسل الأموال ارتباط وثيقاً، وذلك من خلال أنها أظهرت أنها تستهدف القطاع المصرفي في المقام الاول، ولكي تضمن المؤسسات المالية أنها تعرف عملائها جيداً تحتاج إلى بدل العناية الواجبة تجاه العملاء أثناء الإعداد، وذلك من خلال الإلتزام المؤسسات المالية بتطبيق سياسات داخلية تشمل:

- التحقق الدقيق من هوية العملاء.
- التحديث المستمر لبياناتهم.
- المراقبة الدورية للعمليات المالية.
- اعتماد نظام فعال لإدارة المخاطر.
- تطبيق إجراءات العناية الواجبة، خاصة تجاه الفئات أو العمليات عالية المخاطر².

2/مبدأ اعرف عميلك الالكتروني: e-kyc

مبدأ اعرف عميلك الالكتروني e kyc، ويستخدم خاصة في البنوك، وهذا راجع إلى التطور في مجال التقنيات المالية، في جلب حلول مبتكرة التي تواجه التحول الرقمي، وذلك من أجل تسهيل عملية التعرف ورقمنة الإجراءات، وذلك من خلال تقليل الوقت في فحص الهوية والتحقق من معلومات العميل، بالإضافة إلى تحسين الجودة وموثوقية بيانات العملاء، والمقصود بهذا المصطلح هو أنه يشير إلى إتباع الإجراءات عبر التقاط البيانات البيومترية من وثائق التعريف المعتمدة، أو الهوية الذكية الصادرة عن الحكومات، ويترتب على ذلك تحسين جودة البيانات وتعزيز موثوقيتها، إلى جانب خفض تكاليف الامتثال لإجراءات العناية الواجبة.

¹ - محمد رضا تهامي - يحي سعيدي، "دور البنوك في عملية غسيل الأموال بين مبدأ السرية المصرفية ومبدأ اعرف عميلك"، مجلة الباحث الاقتصادي، جامعة برج بوعريش، الجزائر المجلد 5، العدد 1، سبتمبر 2018، ص 309.

² - هند زيتوني - ذهبية ريمة بوعباية، المرجع السابق، ص 527.

كما تتيح هذه التقنيات توسيع نطاق الخدمات المصرفية الإلكترونية وفتح آفاق جديدة أمام المؤسسات المالية، حيث يمكن للعملاء إتمام إجراءات التسجيل والتحقق عن بُعد عبر تطبيقات الهاتف أو الإنترنت، مثل التقاط صورة لبطاقة الهوية أو تسجيل فيديو للتحقق من الهوية.

وقد اعتمدت بعض الدول نماذج متقدمة في هذا المجال، حيث سمحت باستخدام تقنيات التعرف على الوجه والفيديو لفتح الحسابات المصرفية عن بُعد، وفق ضوابط تنظيمية محددة. كما أصدرت الجهات التنظيمية تعليمات واضحة تفرض على المؤسسات المالية الالتزام بمعايير التحقق الرقمي، مع ضرورة مراجعة هذه العمليات واعتمادها من قبل السلطات المختصة.

وفي هذا السياق، وضعت بعض الدول مثل ماليزيا، إطارًا تنظيميًا متكاملًا لخدمات (KYC-e)، يسمح لمزودي الخدمات المالية باستخدام تقنيات التحقق عن بُعد، بما في ذلك مكالمات الفيديو والتعرف البيومتري، لضمان دقة تحديد هوية العملاء.¹

وعليه يمكن القول، أن مبدأ اعرف عميلك الإلكتروني (eKYC) هو عملية رقمية تُستخدم للتحقق من هوية العملاء عن بُعد دون الحاجة إلى حضورهم شخصيًا، حيث تعتمد المؤسسات المالية والتطبيقات الإلكترونية على تقنيات حديثة مثل التعرف على الوجه، تصوير وثائق الهوية، والتحقق عبر الفيديو، إضافةً إلى استخدام رمز التحقق لمرة واحدة (OTP) لتعزيز الأمان والتأكد من أن المستخدم هو صاحب الحساب. يهدف هذا النظام إلى تسهيل الإجراءات وتسريعها مع ضمان الحماية من الاحتيال وغسل الأموال، وذلك من خلال:

التحقق من هوية العميل يتم بشكل إلكتروني بالكامل

يعتمد على تقنيات مثل التعرف على الوجه والذكاء الاصطناعي

استخدام OTP (رمز لمرة واحدة) لتأكيد هوية المستخدم

يساعد في منع الاحتيال وغسل الأموال

¹ - هند زيتوني، ذهبية رمة بوبعاية، المرجع السابق، ص 527، ص 528.

يُستخدم في البنوك الرقمية والتطبيقات المالية

يختصر الوقت مقارنة بـ KYC التقليدي

لا يتطلب الحضور الشخصي أو الوثائق الورقية¹.

الفرع الثاني: الإبلاغ عن الأنشطة المشبوهة:

نظرا لمدى خطورة جرائم غسل الأموال وانعكاساتها السلبية التي تمس جل القطاعات، مما جعل من تجريم هذا النشاط ضرورة لا مفر منها، وعليه سعت التشريعات الدولية والوطنية إلى فرض التزامات وقيود على المعاملات المالية التي تتم عبر البنوك والمؤسسات المالية، حتى تتمكن من تحديد المعاملات المتصلة بالأنشطة الإجرامية والإبلاغ عنها، وقد خول المشرع الجزائري مهمة تلقي الإبلاغات وتحليلها هيئة يطلق عليها خلية معالجة الإستعلام المالي (CTRF).

ومنه سنتناول في هذا الفرع تعريف الإبلاغ عن الأنشطة المشبوهة (أولا)، مؤشرات الإشتباه (ثانيا)، الجهة المكلفة بتلقي الإبلاغ عن الأنشطة المشبوهة (ثالثا).

أولا: تعريف الإبلاغ عن الأنشطة المشبوهة:

سعى المشرع الجزائري - كغيره من التشريعات الوطنية الأخرى - إلى تفعيل دور البنوك والمؤسسات المالية في مجال مكافحة الجرائم التي تتم على مستواها، وذلك بإلزامها على الإفصاح عن المعلومات التي تتعلق بمعاملة مالية يشتبه فيها أنها تتعلق بجريمة غسل الأموال، والإبلاغ عنها للسلطات المعنية. ومنه سنتطرق لتعريف هذا المصطلح من الناحية القانونية والفقهية:

¹ - رمزي طبائية، المرجع السابق، ص 150.

1-التعريف التشريعي :

تباينت موقف التشريعات الوطنية والدولية، حيث أنها لم تعطي تعريفا دقيقا للإبلاغ عن الأنشطة المشبوهة وإنما اكتفت بالنص على إلزاميته بالنسبة للجهات المخول لها. فالمشرع الكويتي لم يقدم تعريفا صريحا لمصطلح الإبلاغ عن الأنشطة المشبوهة واكتفى من خلال نص المادة 12 من القانون 106 لسنة 2013 والمتعلق بمكافحة غسل الأموال وتمويل الإرهاب بالتأكيد على إلزامية الإخطار بالشبهة، حيث جاء فيها: " تلتزم المؤسسات المالية والأعمال والمهن غير المالية بصرف النظر عن قيمتها، إذا إشتبهت أو توافرت دلائل كافية للإشتباه في أن تلك المعاملات تجري بأموال متحصلة من جريمة أو أموال مرتبطة أو لها علاقة بها أو يمكن إستعمالها للقيام بعمليات غسل الأموال أو تمويل الإرهاب."¹

أما موقف المشرع المصري فقد تجلّى في نص المادة الثامنة من القانون 80 لسنة 2002 المتعلق بمكافحة غسل الأموال والتي جاء فيها: " تلتزم المؤسسات المالية بإخطار الوحدة عن العمليات المالية التي يشتبه في أنها تتضمن غسل أموال المشار إليها في المادة 4 من هذا القانون وعليها وضع النظم الكفيلة بالحصول على بيانات التعرف عن الهوية والأوضاع القانونية للعملاء والمستفيدين الحقيقيين من الأشخاص الطبيعيين، أو الأشخاص الاعتبارية."²

أما بالنسبة للمشرع الجزائري فإنه لم يتولى إعطاء تعريف للإبلاغ عن الأنشطة المشبوهة واكتفى من خلال نص المادة 20 من القانون 05-01 المعدل والمتمم³، بالتأكيد على إلزامية الإخطار

¹ - القانون رقم 106 لسنة 2013، المؤرخ في 8 مايو 2013، المتعلق بمكافحة غسل الأموال وتمويل الإرهاب، ج ر، العدد 1137، الصادرة في 23 يونيو 2013، ص 10. (المعدل والمتمم).

² - القانون رقم 80 لسنة 2002، المؤرخ في 22 مايو سنة 2002، يتضمن قانون مكافحة غسل الأموال، ج ر، العدد 20، الصادرة في 22 مايو 2002، ص 5. (المعدل والمتمم).

³ - المادة 20 من القانون رقم 05-01، المؤرخ في 6 فبراير 2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب و مكافحتهم، ج ر ج، العدد 11، الصادرة في 9 فبراير 2005، ص 6.

بالشبهة، وكذلك هو الحال بالنسبة للمرسوم التنفيذي 05-06 الذي لم يعرف من جانبه الإخطار بالشبهة واكتفى بتحديد شكله ونموذجه ومحتواه ووصل إستلامه.¹

إلا أنه وباستقراء نص المادة 20 من القانون 05-01 المعدل والمتمم، يمكن تعريف الإخطار عن الأنشطة المشبوهة على أنه: إبلاغ الخاضعين للهيئة المتخصصة بكل عملية تتعلق بأموال يشتبه فيها أنها متحصلة من جريمة منظمة أو أنها موجهة لتمويل الإرهاب.²

2-التعريف الفقهي:

تتعدد التعريفات الفقهية بشأن هذا المصطلح نذكر منها ما يلي:

يعرف الإبلاغ على أنه: "إفصاح البنوك وغيرها من المؤسسات المالية التي حددها القانون عما يكون لديها من معلومات متعلقة بعملية مالية، يبدو من قيمتها أو الظروف التي تتم فيها، بأنها متعلقة بغسل الأموال غير المشروعة".

كما يعرف على أنه: "إلتزام يقع على عاتق الخاضعين له بإبلاغ الهيئة المتخصصة عن العمليات المشتبه فيها بجريمة تبييض الأموال، قصد التحري والكشف المبكر عن الجريمة تحت طائلة العقوبات المقررة قانونا".

ثانيا: مؤشرات الإشتباه:

أصدرت العديد من الهيئات الدولية مؤشرات بإمكانها الكشف عن وجود شبهات تتعلق بعمليات غسل الأموال من عدمها، وتم حصرها في معيارين يتمثل الأول في المعيار الموضوعي أما الثاني فيتجسد في المعيار الشخصي.

¹ - المرسوم 05-06، المؤرخ في 9 يناير 2006، يتضمن شكل الإخطار بالشبهة و نموذجه و محتواه ووصل إستلامه، ج ر ج ج ، العدد 2، الصادرة في 15 يناير 2006.

² - المادة 20 من القانون رقم 05-01، المؤرخ في 6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم، المصدر السابق، ص 6.

1- المعيار الموضوعي:

يطلق عليه أيضا بالمعيار التلقائي، ويتضمن المؤشرات التي تساعد المكلفين بترقب العمليات المشبوهة والإبلاغ عنها وتشمل:

أ- الإشتباه في مقدار المال:

معنى ذلك أن يكون الإخطار عن العمليات المشبوهة مرتبطا بمقدار مالي محدد قانونا، فبمجرد تجاوز العملية المقدار المالي المحدد يتم التبليغ عنها، ونجد أن الولايات المتحدة الأمريكية من بين التشريعات التي عملت بهذا المبدأ، واعتبرت أن كل عملية تتجاوز قيمتها مبلغ عشرة آلاف دولار أمريكي يتم التبليغ عنها.

إلا أنه وبالنظر إلى ما قد ينجم عنه من انعكاسات سلبية مست بحقوق الأفراد وحياتهم الخاصة، ساهم في تراجع تبني الدول لهذا المؤشر، من منطلق أنه ليس كل عملية تتجاوز تلك القيمة تكيف على أنها غسيل للأموال.¹

ب- الإشتباه في مصدر الأموال:

حيث أنه يقع على عاتق البنوك و المؤسسات المالية عملية البحث و التحري عن مصدر هذه الأموال، هذا ما جاءت به نص المادة 05 (الفقرات 3، 5 و 6) من المرسوم التنفيذي رقم 06-05 المتضمن شكل الإخطار بالشبهة و نموذج و محتواه ووصل استلامه جاء فيها: " الجهات الأخرى الخاضعة للإخطار، يجب إعطاء كل المعلومات المتعلقة بطبيعة العملية (إيداع- مبادلات- توظيفات- تحويلات - أو أية حركة لرؤوس الأموال) المتعلقة بعلاقة الأعمال (مكان علاقة الأعمال

¹ - أحمد بدراني - سعيد فروحات، "أحكام الإخطار بالشبهة المالية لمكافحة جريمة تبييض الأموال في التشريع الجزائري"، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 14، العدد 1، نوفمبر 2020، ص 890.

و مكان مسك المحاسبة و مكان البيع ومكان التصريح بالأعمال، طريقة الدفع نقدا أو غيرها...) ومعلومات حول غرض وطبيعة العملية و إبراز دواعي إثارة الشبهة بدقة".¹

ج-الإشتباه في المعاملات المالية:

تشكل بعض المعاملات التجارية التي تتم عبر المصارف حالات اشتباه بقيام جريمة غسل الأموال وهي كالتالي:

- تحويل مبالغ كبيرة لمصلحة زبائن غير مقيمين بالدولة.
- استقبال تحويلات كبيرة من بنوك أجنبية لصالح زبون ، لا تتناسب مع نشاطه في العالم الخارجي.
- الإشتباه في وجود تحويلات قادمة من أو متجهة نحو دول لا تتوفر على أنظمة تشريعية كافية لمكافحة غسل الأموال.²

2-المعيار الشخصي :

مفاده أن الإبلاغ عن الأنشطة المشبوهة يكون استنادا لوجود أحد المؤشرين:

أ-الإشتباه في الزبون أو مثله:

- بعد إتمام الإجراءات الخاصة بمعرفة هوية الزبون أو مثله "قاعدة إعرف عميلك"، يتم إما قبول طلب فتح حساب من خلال التأكد من أن الزبون لا يشكل خطرا أو رفض ذلك الطلب في حالة الشك، مما يستوجب إخطار الجهات المختصة بذلك³. ومن أبرز حالات الإشتباه في الزبون نجد:
- الإشتباه في تردد الزبائن على بنوك دول تتسم بضعف الأنظمة التشريعية والرقابية.

¹ - المادة 5 من المرسوم 06-05، المؤرخ في 9 يناير 2006، يتضمن شكل الإخطار بالشبهة ونموذجه ومحتواه ووصل إستلامه، ج ر ج

ج، العدد 2، الصادرة في 15 يناير 2006، ص 7.

² - رقية أحمد داود، المرجع السابق، ص ص 152-153.

³ - أحمد بدراني - سعيد فروحات، المرجع السابق، ص 891.

– الإشتباه في الزبائن الذين يمارسون الأنشطة التجارية المشبوهة كالتى تتعلق: بسلع ثمينة كالمجوهرات والأنشطة العقارية وأندية القمار.¹

ب- الإشتباه في هوية المستفيد:

من المعروف أن المستفيد لا يسأل عن الأموال التي تحول إليه، مما يسهل عمليات غسل الأموال، لذلك تلتزم كل من البنوك والمؤسسات المالية بالتحقق من هوية المستفيد، وفي حالة وجود أي شبهة يتم إخطار الهيئة المختصة.²

ثالثا: الجهة المكلفة بتلقي الإبلاغ عن الأنشطة المشبوهة:

على إعتبار أن معظم أنشطة غسل الأموال تتم عبر القنوات البنكية، لذا وجب تفعيل دور البنوك والمؤسسات المالية لمكافحة هذه الظاهرة، لذلك سعت كل من التشريعات الدولية والوطنية إلى إلزام البنوك بالإخطار عن العمليات المشبوهة، وأسندت هذه المهمة إلى هيئات متخصصة تعمل على تلقي الإبلاغ عن الشبهات وتحليلها ومعالجتها.

لا بد من الإشارة إلا أن المشرع الجزائري لم يخصص هيئة مستقلة تعمل على تلقي الإبلاغ عن الأنشطة المشبوهة التي تصدر عن المصارف الرقمية، وجعل من خلية الإستعلام المالي هي الجهة المكلفة بتلقي الإبلاغ الصادر من المصارف التقليدية أو الرقمية.

¹ - رقية أحمد داود، المرجع السابق، ص 152.

² - أحمد بدراني - سعيد فروحات، المرجع السابق، ص 892.

1-تعريف خلية معالجة الإستعلام المالي:

بعد مصادقة الجزائر على الاتفاقيات الدولية لمكافحة الجرائم المنظمة عبرالحدود الوطنية، استحدثت خلية معالجة الإستعلام المالي وذلك بموجب المرسوم التنفيذي رقم 02-127 المعدل والمتمم.¹

تعرف هذه الخلية على أنها: " عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى الوزير المكلف بالمالية، تتلقى الإخطارات والمعلومات عن أي من العمليات التي يشتهب في أنها تشكل أو تتضمن تبييضا للأموال وتمويلا للإرهاب أو مجرد محاولات للقيام بهذه الأفعال عن طريق القطاع المصرفي."²

2-تشكيلة خلية معالجة الإستعلام المالي:

نظرا لأهمية نشاط خلية معالجة الإستعلام المالي في مكافحة غسيل الأموال، عمل المشرع الجزائري على وضع إطار تنظيمي تفاديا للعراقيل وحفاظا على سرية أعمالها، وتتكون الخلية من 3 هياكل أساسية وهي:

أ- المجلس: الذي يعتبر أهم هيكل إداري على مستوى الخلية، ويتكون من 7 أعضاء من بينهم الرئيس و4 أعضاء يمتازون بالكفاءة في المجال البنكي والمالي إضافة إلى قاضيان يعينان من قبل وزير العدل.

ب- الأمانة العامة: تمثل الهيكل الإداري الثاني للخلية، يرأسها أمين عام يعمل على إدارة الشؤون الإدارية والوسائل المادية والبشرية للخلية، ويسعى إلى توفير الخدمات اللازمة لضمان حسن سير أدائها.

¹ - المرسوم التنفيذي رقم 02-127، المؤرخ في 7 أبريل 2002، يتضمن إنشاء خلية معالجة الإستعلام المالي وتنظيمها وعملها، (المعدل والمتمم)، ج ر ج ج، عدد 23، الصادرة في 7 أبريل 2002.

² - عبد الحق حميل - سيد أحمد مسيردي، " مظاهر إستقلال خلية معالجة الإستعلام المالي -قراءة في المرسوم التنفيذي رقم 22-36"، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي - الأغواط، الجزائر، المجلد 7، العدد 01، ماي 2023، ص 326.

ج- المصالح التقنية والإدارية للخلية: وتشمل كل من مصلحة التحقيقات والتحريرات والتي تتلقى الإبلاغات بالشبهة التي ترد إلى الخلية وفحصها، المصالح القانونية والتي تعمل على تحليل الوقائع، مصلحة الوثائق وقاعدة البيانات تتولى جمع المعلومات وتشكيل بنك المعلومات لحسن سير الخلية، مصلحة التعاون تدير العلاقات مع المؤسسات الأجنبية التي تعمل في نفس الميدان.¹

3- مهام خلية معالجة الإستعلام المالي:

لتمكين الخلية من القيام بمهامها المتعلقة بتلقي الإخطارات بالشبهة، خول لها المشرع جملة من الامتيازات تكمن في:

أ- تلقي الإخطارات بالشبهة: تعمل الخلية على إستلام التصريحات بالشبهة لكل العمليات التي يشتهب فيها غسلا للأموال، من قبل الخاضعين الواجب الإخطار وتشمل البنوك والمؤسسات المالية والمصالح المالية لبريد الجزائر والمؤسسات المالية المشاركة ومكاتب الصرف، واشترطت الخلية أن يكون الإبلاغ عن الأنشطة المشبوهة باستخدام الوسائل الإلكترونية، متضمنة معلومات حول الشبهة مع توقيع الجهة التي قامت بالإخطار.

ب- تحليل ومعالجة المعلومات: حيث تقوم الخلية بمجرد تلقيها المعلومات الخاصة بالإخطار بتحليلها وفحصها وتحديد مصدر الأموال ورصد حركتها، ويتم ذلك من قبل أشخاص ذو خبرة فنية وتقنية.

ج- إتخاذ تدابير تحفظية: يمكن للخلية بصفة تحفظية منع أو توقيف المعاملات البنكية لأي شخص طبيعي أو معنوي مشتبه به في عملية غسيل الأموال، لمدة أقصاها 72 ساعة مع إمكانية تمديد المدة بعد موافقة رئيس محكمة الجزائر.

¹ - جمال حباش، " صلاحيات خلية معالجة الإستعلام المالي في مواجهة تبيض الأموال "، مجلة الإدارة والتنمية للبحوث والدراسات، جامعة البليدة 2، المجلد 10، العدد 2، ديسمبر 2021، ص ص 62-65.

د- اتخاذ قرار بشأن العملية المشبوهة: بعد تلقي المعلومات المتعلقة بالإبلاغ عن الأنشطة المشبوهة وتحليلها، تصدر الخلية قرر إما بحفظ المعلومات التي تلقتها في حالة التأكد من عدم وجود شبهة، أو إرسالها إلى وكيل الجمهورية إذا تبين ارتباط العمليات المشتبه بها بعمليات غسيل الأموال.¹

المطلب الثاني: المسؤولية عن حسن إستعمال التقنيات الرقمية الحديثة:

تعتبر التقنيات الحديثة في المصارف الرقمية وسيلة أساسية لتطوير الخدمات وتسريع المعاملات، لكنها تفرض مسؤولية كبيرة لضمان استخدامها بشكل آمن، لذلك تعتمد المصارف على وسائل للكشف عن الاحتيال مثل الذكاء الاصطناعي ومراقبة العمليات المشبوهة، إضافة إلى تقنيات التحقق لحماية الحسابات، كما تعمل على تطوير منصات باستمرار لتحقيق الامتثال للقوانين المصرفية وحماية البيانات، مما يعزز الأمان والثقة ويجعل مسؤولية الاستخدام مشتركة بين المؤسسة والمستخدم. ومنه نقسم هذا المطلب إلى فرعين: تطوير الوسائل والأدوات التقنية لكشف محاولات الإحتيال **الفرع الأول**، تطوير المنصات الرقمية لتحقيق الدقة والفعالية في التحقق والامتثال **الفرع الثاني**.

الفرع الأول: تطوير الوسائل والأدوات التقنية لكشف محاولات الإحتيال:

تلعب تقنيات تحليل البيانات الضخمة دوراً مهماً في اكتشاف الشبكات الاحتيالية، حيث يتم جمع وتحليل كميات هائلة من البيانات المالية للكشف عن العلاقات والأنماط غير الطبيعية بين الحسابات والمعاملات. كما تستفيد بعض المصارف من تقنية البلوك تشين لما توفره من شفافية وصعوبة في التلاعب بالسجلات المالية.²

ومنه يمكننا تقسيم هذا الفرع إلى: تعريف الإحتيال في المصارف الرقمية أولاً، مسؤولية المصارف الرقمية في تحديث أساليب الكشف عن الإحتيال ثانياً.

¹ - جمال حباش، المرجع السابق، ص ص 66-69.

² عوسات تكلت، "تقنية البلوك تشين دراسته في المفهوم"، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 7، العدد 2، جوان 2022، ص 945.

أولاً: تعريف الإحتيال في المصارف الرقمية:

الاحتيال المصرفي الرقمي هو كل عملية غير قانونية تتم عبر الوسائل الإلكترونية بهدف الاستيلاء على الأموال أو البيانات المالية الخاصة بالعملاء أو المؤسسات المصرفية باستخدام تقنيات رقمية مختلفة. ويشمل ذلك اختراق الحسابات البنكية، وسرقة البطاقات الإلكترونية، والتصيد الاحتيالي، وانتحال الهوية الرقمية.¹

-تعريف الاحتيال المصرفي.

أ/لغة:

يعني مصطلح الاحتيال: الإسم مشتق من escroquer المأخوذ عن الإيطالية décrocher, Scroccare ، فك، من Crocco، كلاب . وهو: جريمة تؤدي إلى الإضرار بملكية الغير بالحصول من هذا الأخير الذي يملكها على النقل الإرادي لمال (شيء، نقود، مستندات لها قيمة بيعية وشرائية أو قانونية) عن طريق خدعة تتصف (وهي ناتجة عن اتخاذ اسم كاذب أو صفة كاذبة، أو استخدام مناورات غش)، قارن بالسرقة vol، إساءة الاستعمال abus، إساءة الائتمان (abus de confiance) اختلاس filouterie، إساءة استعمال أموال الشركة abus de bien sociaux²

¹ مريم عبد الكافي - صورية بورباية، "جريمة الإحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية"، مجلة القانون والعلوم السياسية، جامعة النعامة الجزائر، المجلد 8، العدد 1، أبريل 2022، ص ص 408 414.

² -خلود صلجة -مروة شيل، "جريمة الإحتيال الإلكتروني في التشريع الجزائري"، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 - سكيكدة، الجزائر 2025-2024، ص 13، 14.

ب/اصطلاحا:

الاحتيال هو: "الاستيلاء على مال الغير وملكيته بالخداع مما يدفع الضحية إلى تسليم أمواله".¹

كما يعرف الاحتيال على أنه "استخدام وسيلة من وسائل التدليس التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا المملوكا لغيره".²

ثانيا: مسؤولية المصارف الرقمية في تحديث أساليب الكشف عن الإحتيال:

إن المصارف الرقمية من أكثر المؤسسات عرضة لمحاولات الاحتيال الإلكتروني، لذلك أصبحت مسؤولة عن تطوير وتحديث وسائل وأساليب الكشف عن الاحتيال بشكل مستمر. ومن أبرز التقنيات الحديثة التي تعتمد عليها هذه المصارف: الذكاء الاصطناعي، والأمن السيبراني، وتقنية البلوكشين، لما لها من دور فعال في حماية المعاملات والبيانات المالية.

1/الذكاء الاصطناعي :

هو تقنية حديثة تمكّن الأنظمة والبرامج من محاكاة الذكاء البشري، مثل التعلم والتحليل واتخاذ القرارات، ويُستخدم في كشف العمليات المشبوهة والاحتيال بسرعة ودقة.

أ/تعريفه:

يشير الذكاء الاصطناعي إلى "قدرة كمبيوتر أو روبوت مدعم بكمبيوتر، على معالجة المعلومات والوصول الى نتائج بطريقه مماثله لعملية التفكير لدى البشر في التعلم واتخاذ القرارات وحل

1- حياة هراكي، "واقع جريمة الإحتيال لإلكتروني في التجارة الإلكترونية، مجلة التغيير الاجتماعي، جامعة بسكرة -الجزائر، المجلد 8، العدد 2، 2023، ص 50.

2- سهيرة بولحية- دنيا زاد سويح، " الإحتيال الإلكتروني"، مجلة الدراسات القانونية والإقتصادية، جامعة باتنة، الجزائر، مجلد 2، عدد 2، 2019، ص 38.

المشكلات، وبالتالي فإن هدف الذكاء الاصطناعي هو تطوير أنظمة قادرة على معالجة المشكلات المعقدة بطريقة مشابهة للعمليات المنطقية والإستدلالية عند البشر".¹

ب/ تقنية الكشف عن الاحتيال بالذكاء الاصطناعي:

حل المشكلات: يعتمد الذكاء الاصطناعي على تصميم خوارزميات قادرة على تحليل المعطيات وتقديم حلول فعالة، بما يساهم في تسهيل مختلف جوانب الحياة وتحسين الأداء في القطاعات المتعددة.²

-التصنيف الائتماني :

تعتمد البنوك على تقنيات الذكاء الاصطناعي والنماذج الإحصائية الحديثة في تقييم الجدارة الائتمانية للعملاء، وذلك من خلال تحليل البيانات المالية وسلوك المعاملات للتعرف بمخاطر التعثر في السداد. وتساعد هذه التقنيات في تحسين دقة قرارات منح القروض وتقليل المخاطر الائتمانية، كما تساهم الشبكات العصبية وأنظمة التعلم الآلي في معالجة كميات كبيرة من البيانات بسرعة وكفاءة، مما يعزز فعالية إدارة المخاطر داخل المؤسسات المصرفية.³

-فهم العملاء وخدمتهم :

يساعد الذكاء الاصطناعي البنوك على فهم احتياجات العملاء وسلوكهم من خلال تحليل البيانات المستخرجة من التطبيقات الرقمية ووسائل الاتصال المختلفة. ويساهم ذلك في تقديم خدمات مصرفية أكثر تخصيصاً وسرعة، إضافة إلى تحسين جودة التواصل مع العملاء والاستجابة

1- هدى بوحنيك، "أثر تبني البنوك لتقنيات الذكاء الاصطناعي -دراسة حالة بنك " مجلة للدراسات والبحوث الإنسانية، جامعة العربي التبسي تبسة، الجزائر المجلد 08، العدد 04، جانفي 2024، ص 171.

2- بن علي سمية، "مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي باستخدام تطبيق الأمن السيبراني بنك daske الدنماركي النموذجي"، مجلة أبعاد إقتصادية، جامعة محمد بوقرة، بومرداس، الجزائر، المجلد 03، العدد 02، 2023، ص 46

3- نورة سداوي، "تطبيقات الذكاء الاصطناعي في المصارف العربية تجربة الإمارات العربية المتحدة"، مجلة إضافات اقتصادية، جامعة غرداية، الجزائر، المجلد 08، العدد 01، 2023، ص 214.

الفورية لاستفساراتهم. كما تلعب تقنيات معالجة اللغة الطبيعية دورًا مهمًا في تطوير خدمات الدعم الرقمي والرد الآلي، مما يؤدي إلى رفع مستوى رضا العملاء وتحسين جودة الخدمة المصرفية.¹

-الإستشارات المالية:

أصبحت تقنيات الذكاء الاصطناعي تُستخدم بشكل واسع في مجال الاستشارات المالية والاستثمارية، حيث تعتمد على الخوارزميات وتحليل البيانات لتقديم حلول مالية تتناسب مع احتياجات العملاء وأهدافهم المستقبلية. كما تساعد هذه الأنظمة في إدارة الأصول والتخطيط المالي وتحسين كفاءة القرارات الاستثمارية، من خلال استخدام تقنيات مثل التعلم الآلي والحوسبة المعرفية والنظم الخبيرة.²

2/الأمن السيبراني :

هو مجموعة من الوسائل والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الاختراق والهجمات الإلكترونية، لضمان أمن المعلومات وسلامتها.

أ/تعريفه:

الأمن السيبراني (cybersecurity) هو مجموعة من الوسائل التقنية والتنظيمية والإدارية التي تستخدم لحماية المعلومات والأنظمة الإلكترونية من الاستخدام غير المصرح به أو الإستغلال السيء بهدف يهدف الأمن السيبراني إلى ضمان استمرارية عمل نظام المعلومات من خلال:

-منع الوصول الغير المصرح به الى البيانات والأنظمة.

-الحفاظ على سرية البيانات وضمان خصوصيتها مما يعني منع تسريب أو التلاعب بالمعلومات

1- بن علي سمية، المرجع السابق، ص 50.

2- هدى بوحنيك، المرجع السابق، ص 175.

-استعادة البيانات والأنظمة في حال حدوث هجمات أو خلل، لضمان استمرارية العمل وعدم تأثر العمليات المهمة.¹

ب/ تقنية الأمن السيرياني في الكشف عن الإحتيال:

تعتمد المؤسسات الحديثة على مجموعة من تقنيات الأمن السيرياني لحماية بياناتها وأنظمتها، ومن أبرزها:

انعدام الثقة (Zero Trust): يقوم على مبدأ عدم منح الثقة التلقائية لأي مستخدم أو تطبيق، وفرض إجراءات تحقق ومراقبة مستمرة داخل المؤسسة.

تحليلات السلوك: تعتمد على مراقبة حركة البيانات وسلوك المستخدمين والأجهزة للكشف عن الأنشطة غير المعتادة التي قد تشير إلى تهديدات أمنية.²

أنظمة كشف التسلل: تستخدم لرصد محاولات الاختراق والاستجابة السريعة لها، بما يساعد على الحد من الأضرار واكتشاف مصدر الهجوم.

التشفير السحابي: يهدف إلى حماية البيانات عبر تشفيرها قبل تخزينها في البيئات السحابية، مما يمنع الوصول غير المصرح به إليها.³

3/تقنية البلوك تشين :

تعتبر تقنية البلوك تشين (Blockchain) من أبرز التقنيات الحديثة التي ساهمت في تعزيز الأمان والشفافية داخل المصارف الرقمية، خاصة في مجال الكشف عن الاحتيال المالي والحد من

1- فاطمة الزهراء حشروف - وحيدة صديقي «الأمن السيرياني في البنوك الجزائرية التحديات والاستراتيجيات»، مجلة الدفاتر الإقتصادية، جامعة زيان عاشور - الجلفة، الجزائر، مجلد 16، عدد 01، 2025، ص 669

2- بن علي سمية، المرجع السابق، ص 53

3- فاطمة الزهراء حشروف -، وحيدة صديقي، المرجع السابق، ص 673.

الجرائم الإلكترونية. وتعتمد هذه التقنية على سجل رقمي موزّع وغير قابل للتعديل، يسمح بتسجيل جميع المعاملات بطريقة آمنة وشفافة.

أ/تعريفه:

إن تقنية البلوك تشين هي أكبر بيانات رقمية آمنة شفافة فائقة السرعة لا مركزية تدار بواسطة مستخدميها بلا وسيط غير قابلة للتعديل أو الإزالة irréversibilité تتولى إدارة قائمة متزايدة من الكتل التي تحتوي منها على عدة من البيانات والمعلومات وهذه التقنية تقوم على تجميع البيانات والمعلومات بكل ما يتم من معاملات داخل كتل سلسلة زمنية من الأقدم إلى الأحدث وهو السجل يهدف إلى إثبات وجود هذه المستندات وتتبع المعاملات التي تتم نشأها.¹

ب/ تقنية البلوك تشين في الكشف عن الإحتيال:

تؤدي تقنية ال Blockchain ثلاث وظائف أساسية تتمثل في: الإرسال، الحفظ، والأتمتة.

1/ الإرسال (Transmission)

أتاحت تقنية ال Blockchain تنفيذ نوعين رئيسيين من العمليات، هما:

تحويل العملات المشفرة (monnaie-Crypto).

تحويل الأصول (Transfert des actifs).

ويقصد بالعملية المشفرة أنها أصل رقمي غير مادي، يُمثّل برموز إلكترونية قابلة للتداول عبر شبكة الإنترنت دون الحاجة إلى وسيط، ومن أبرز أمثلتها: البيتكوين والإيثريوم.

كما تسمح تقنية ال Blockchain بإجراء عمليات تحويل الأصول الرقمية وتنفيذ المعاملات المالية بطريقة آمنة وشفافة، وهو ما ساهم في توسيع نطاق استخدامها في المجالات الاقتصادية والتجارية.²

2/ الحفظ (Conservation)

1- عوسات تكليت، المرجع السابق، ص 945.

2- نوري جهاد- رحيمة شتوح رحموني، "تطبيقات تقنية البلوك تشين"، مجلة القانون والعلوم الاجتماعية، جامعة زيان عاشور -الجلفة، الجزائر، المجلد 7، العدد 2، سنة 2022، ص 952.

تتمثل وظيفة الحفظ في تخزين البيانات والسجلات الرقمية بطريقة آمنة ومنظمة، بما يضمن سهولة الوصول إليها وتبادلها وإدارتها في أي وقت، وذلك بالاعتماد على العقود الذكية (Smart Contracts) وقواعد البيانات الموزعة.

3/ الأتمتة (Automatisation)

تعتمد الأتمتة على استخدام العقود الذكية (Smart Contracts)، وهي برامج رقمية تُنفذ تلقائيًا عند تحقق شروط معينة. كما ساهمت هذه التقنية في دعم أنظمة الذكاء الاصطناعي (Artificial Intelligence) من خلال تسهيل التكامل مع البيانات الرقمية المخزنة على الشبكة، الأمر الذي جعلها من أبرز التطبيقات الحديثة لتقنية ال Blockchain.¹

الفرع الثاني: تطوير المنصات الرقمية لتحقيق الدقة والفعالية في التحقق والإمثلة:

إستجابة للتغيرات المصرفية الحديثة، أصبح من الضروري مواكبة هذه التغيرات عن طريق الإعتماد على آليات تكنولوجية حديثة تهدف إلى تقديم خدمات مصرفية أكثر تطوراً، تمتاز عن المصارف التقليدية من حيث السرعة والتكلفة، هذا ما أدى بالمصارف الرقمية والمؤسسات المالية إلى إعتماد منصات تعمل بتكنولوجيا مالية عالية من أجل تحقيق كفاءة القطاع المصرفي، ومن أبرز هذه المنصات نجد: واجهة برمجة التطبيقات ApLs ومنصة Netinfo والخدمات المصرفية الرقمية.

ومنه يمكننا دراسة هذا الفرع من خلال بيان النقاط التالية: تعريف المنصات الرقمية (أولاً)، دور المنصات الرقمية في القطاع المصرفي (ثانياً)، الإنتقال نحو المنصات الرقمية الحديثة كآلية لتطوير الخدمات المصرفية (ثالثاً).

أولاً: تعريف المنصات الرقمية:

1- عوسات تكليت، المرجع السابق، ص951.

تعد المنصات الرقمية تجسيدا للتطبيقات التكنولوجية المعاصرة التي تعمل على نقل المحتوى وتبادله عبر قنوات إتصالية متعددة، مما يتيح سهولة الوصول إلى المعرفة دون مواجهة القيود المكانية والزمانية، ومنه سوف نتطرق إلى التعريف التشريعي والتعريف الفقهي:

1-التعريف التشريعي: تباينت موقف التشريعات الوطنية والدولية بشأن تعريف المنصات الرقمية نذكر منها ما يلي:

-تعريف المشرع المصري: "نموذج أعمال قائم على استخدام الوسائل التكنولوجية في مزاوله الأنشطة المالية غير المصرفية وفي عرض المنتجات والخدمات المرتبطة بها على الأشخاص الراغبين في الحصول عليها، ويسمح تبادل البيانات والمعلومات اللازمة للإتمام هذه التعاملات." ¹

المشرع- الكويتي فنجد أنه لم يتطرق لتعريف المنصات الرقمية بشكل مباشر، وإنما ذكرها في إطار تعريف البنوك الرقمية بنصه: "البنك سواء التقليدي أو الإسلامي الذي يزاول المهنة المصرفية عن طريق القنوات الرقمية". ²

أما بالنسبة للمشرع الجزائري فنلاحظ أنه لم يقدم تعريفا للمنصات الرقمية وإنما أشار إليها في تعريف البنوك الرقمية في المادة 24-04: " بأنه كل بنك يقدم خدمات ومنتجات حصريا عبر قنوات أو منصات أو دعائم رقمية." ³

2-التعريف الفقهي: تعددت التعريفات التي تطرقت إلى تعريف المنصات الرقمية، نذكر منها:

1- المادة 1 من القانون رقم 5 لسنة 2022، المؤرخ في 8 فيفري 2022، المتضمن تنظيم وتنمية استخدام التكنولوجيا المالية في الأنشطة المالية غير المصرفية، ج ر، العدد 5، الصادرة في 8 فبراير 2022.

2- قرار بنك الكويت المركزي لسنة 2022، بإصداره دليل متطلبات تأسيس البنوك الرقمية في دولة الكويت، المصدر السابق، ص 3.

3- المادة 2 من النظام رقم 04.24، المؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، المصدر السابق، ص 30.

يمكن تعريف المنصات الرقمية على أنها: «فضاءات رقمية بعيدة المدى تتأسس على البنية التحتية لشبكات الأنترنت، وترجم إلى منظومة متكاملة ذات بعدين تقني وتجاري متداخلين، تمكن المستخدم من النفاذ إلى فضاءات خدماتية متنوعة تفاعلية كانت أو غير تفاعلية، تقدم عبر الأنترنت إما بمقابل مالي أو مجانا مع إختلاف درجات الإتاحة من المحدودة إلى المفتوحة».¹

كما تعرف على أنها: "هي أجهزة أو برامج تستخدم تطبيق أو خدمة ما ، تعمل وفق نظام تشغيل تنسيق البرامج التي تستخدم مجموعة من التعليمات لمعالج معين".²

ثانيا: دور المنصات الرقمية في القطاع المصرفي:

تلعب المنصات الرقمية دورا محوريا هاما في تطوير القطاع المصرفي من خلال الخدمات التي تتيحها، والتي تتجلى فيما يلي:

1-إدارة الحسابات : تتيح المنصات الرقمية للعملاء إمكانية مراقبة حساباتهم المصرفية ، و القيام بمعاملاتهم المالية في أي مكان و في أي وقت ، إضافة إلى إمكانية الإطلاع على أرصدهم و تحويل الأموال بين حساباتهم بكل سهولة مع مراجعة تحركاتهم المالية.³

2-خدمة الدفع الإلكتروني : تضع المنصات الرقمية تحت تصرف العملاء خدمة الدفع الإلكتروني (e-paiement) تمكنهم من سداد الفواتير و الخدمات عبر مواقع إلكترونية تتعامل مع هذه الوسيلة ، ويتم ذلك عن طريق البطاقة البنكية ، وتمتاز هذه الخدمة بمجموعة من الميزات منها :

1- ابتسام نوري - خالد بن الوليد نهار، "المنصات الرقمية كآلية تسويقية للخدمات المالية المصرفية: دراسة حالة منصة LENPO الرقمية للتمويل الإسلامي في المملكة العربية السعودية"، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، جامعة المسيلة، المجلد 18، العدد 02، ديسمبر 2025، ص 51.

2- محمد بوعتلي - سامي ليلية، "واقع المنصات الرقمية وتأثيرها على التنمية المستدامة في الجزائر: دراسة ميدانية وقياسية، مجلة المدير، المدرسة العليا للتسيير والاقتصاد الرقمي - القليعة، الجزائر، المجلد 9، عدد خاص، أكتوبر 2022، ص 14.

3- فاتح مرزوق - ياسين عطاء الله، " الخدمات المصرفية الرقمية ودورها في تسهيل التجارة الخارجية -دراسة حالة بنك الجزائر الخارجي BEA»، مجلة الجغرافيا الاقتصادية، المركز الجامعي مرسل عبد الله - تيبازة، الجزائر، المجلد 2، العدد 1، جانفي 2025، ص 66.

-توفير الوقت و الراحة.

-توفير حماية مؤمنة لضمان حقوق العملاء.

-تتسم بالسهولة و البساطة و إمكانية الولوج في أي وقت و أي مكان.¹

3-تحويل الأجور عن طريق خدمة تبادل المعطيات الآلية : حيث تعمل المنصة الرقمية على وضع خدمة تبادل المعطيات الآلية BDI تحت تصرف زبائنها ، والتي تمكن أصحاب المؤسسات من تحويل أجور موظفيها بصفة آلية لربح الوقت و سير المعاملات المالية ، بإستخدام تكنولوجيا الإتصال الحديثة بحيث تتميز بالعصرية و المصداقية.²

4-التمويل الإلكتروني : تقدم المنصات الرقمية تسهيلات فيما يخص تقديم القروض ، إذ تمكن الشركات التي نحتاج إلى تمويل مشاريعها التجارية أو عملياتها اليومية، بتقديم طلب الحصول على تمويل دون أن يكلفها ذلك اللجوء إلى الفروع البنكية ، حيث يتم قبول الطلب إلكترونيا مما يوفر الوقت و السرعة.³

5-تعزيز الشمول المالي : تعمل المنصات الرقمية بشكل كبير على تعزيز الشمول المالي ، وذلك عن طريق تقديم خدمات مصرفية للأفراد في المناطق النائية و المناطق التي يصعب الوصول فيها إلى الفروع التقليدية ، و بالتالي تمكنهم من الانضمام إلى النظام المالي و الإستفادة من الخدمات المالية.

6-تعزيز التجارة الخارجية : من خلال الخدمات التي تقدمها المنصات الرقمية تحقق تسهيلات في التجارة الخارجية ، و ذاك عن طريق تسريع العمليات المالية و تحقيق الأمان ، مما يساهم في تقليل المخاطر المرتبطة بالتجارة الدولية.⁴

1- مصطفى صايم - محمد بوفناديل، "مساهمة الإدارة الإلكترونية في تطوير أساليب العمل المصرفي: إشارة الخدمات الإلكترونية التي يقدمها البنك الوطني الجزائري BNA، مجلة إضافات إقتصادية، جامعة غرداية، المجلد 3، العدد 2، أكتوبر 2019، ص 122.

2- مصطفى صايم - محمد بوفناديل، المرجع السابق، ص 122.

3- فاتح مرزوق -ياسمين عطاء الله، المرجع السابق، ص 67.

4- فاتح مرزوق -ياسمين عطاء الله، المرجع السابق، ص 62.

ثالثا: الإنتقال نحو المنصات الرقمية الحديثة كآلية لتطوير الخدمات المصرفية:

سعت المصارف الرقمية والمؤسسات المالية إلى سد الثغرات والفجوات التي تعترض النظام المصرفي من إختراقات وإعتداءات تمس البيانات الشخصية للعملاء، عن طريق تطوير منصات الرقمية متبعة في ذلك إبتكارات تقنية مالية توظفها في العديد من مجالاتها المصرفية، والتي تهدف إلى تقديم خدمات بأقل تكلفة، وتحقيق الدعم المالي والتي لا يمكن تحقيقها على مستوى المصارف التقليدية.

- نماذج المنصات المصرفية الرقمية الحديثة:

نعمد في دراستنا على نموذجين: واجهة برمجة التطبيقات ApLs، منصة Netinfo

أ- واجهة برمجة التطبيقات ApLs:

تعد من أبرز الإبتكارات التي تعمل على تعزيز الخدمات المالية الرقمية، ونظرا لحدائته فقد تنوعت التعريفات الخاصة بهذا النموذج، حيث يعرفها البعض على أنها " مصطلح حديث الإستعمال في عالم الأعمال والمنظومة المصرفية الخاصة، وهو عبارة عن مجموعة مكاتب إلكترونية تشمل قواعد وبيانات جاهزة للإستعمال، تساعد مطورين الويب على تصميم التطبيقات ومواقع الويب المتخصصة، بحيث تكون هذه المكاتب موجودة على خوادم عالية التقنية، تستضيفها منصات شبكية خاصة تتيح لمستخدميها تصميم البرامج دون الحاجة إلى تخزينها".¹

تهدف واجهة برمجة التطبيقات ApLs إلى تطوير الخدمات المصرفية من خلال:

- إعادة التوازن للخدمات المصرفية، وتحقيق ميزة تنافسية للبنوك والمؤسسات المالية.²

¹ - أيمن بوزانة -وفاء حمدوش، " منصات التكنولوجيا المالية كآلية لتعزيز الخدمات المصرفية المفتوحة -واجهة برمجة التطبيقات ApLs

نموذجاً"، مجلة المدير، المدرسة العليا للتسيير والإقتصاد الرقمي - القليعة، الجزائر، المجلد 9، عدد خاص، أكتوبر 2022، ص 158.

² - أيمن بوزانة -وفاء حمدوش، المرجع السابق، ص 161-170.

- تعمل على ربط قاعدة بيانات البنك (معلومات العملاء) بتطبيقات أو برامج مختلفة ، مما يساهم في تشجيع الخدمات و المدفوعات.

- تلعب دورا أساسيا في تمكين الأعمال الرقمية من خلال توفير خدمات مبتكرة تتمحور حول العملاء.

- حيث أفادت الشركة الرائدة Axway و Ap ldays أن 88% من المديرين في القطاع المصرفي وشركات التكنولوجيا المالية يرون أن إدارة واجهات برمجة التطبيقات ضرورية للتفوق في هذا القطاع.¹ هناك ثلاث نماذج خاصة بواجهة برمجة التطبيقات ApLs تتجلى في:

-النموذج العام : يستخدم من قبل الأطراف الخارجية و المطورين الذين يعملون على إبتكار تطبيقات لتسهيل المعاملات المصرفية ، حيث يعمل هذا النموذج على تقليل كلفة الشركة و تحقيق الأمن.

-النموذج القائم على الشراكة : يستخدم من قبل شركاء العمل لتحقيق الشراكة في العمل للوصول إلى السوق المستخدم.

-النموذج الداخلي : نموذج خاص يستخدم من قبل المطورين من الداخل ، يعمل على تحقيق الكفاءة التشغيلية و تقليل التكلفة.²

ب- منصة Netinfo للخدمات المصرفية الرقمية:

تعد نظاما مصرفي رقمي شامل، تعمل على توحيد قنوات الإتصال المتعددة في القطاع المصرفي، يمكن تعريفها على أنها: " حلا شاملا متعدد القنوات يمكن المؤسسات المالية من تحقيق التحول الرقمي وتطوير إستراتيجية مصرفية رقمية عبر قنوات متعددة، حيث تتميز بأنها طبقة قابلة للتخصيص توفر تجربة عملاء سلسلة، مما يزيل العوائق التي قد تعترضها وتعمل على دعم مجموعة واسعة من الوظائف والخدمات التي تغطي الحاجيات المصرفية ".

1 - Mohammed BEN Moussa, ApI « AppLication p'ogramming Interface » : Apromising Future For Financial Institutions CInternational Experience, Revue Des sciences commerciales, vol 18, N°2, Décembre 2019, pp 35-36.

2- أيمن بوزانة -وفاء حمدوش، المرجع السابق، ص 159-ص160.

تعمل منصة الخدمات المصرفية Netinfo على توفير ميزات رقمية عالية، تساعد في تطوير المؤسسات المالية، حيث تمكنها من الإستجابة الفعالة لمتطلبات وتوقعات عملائها، يمكن حصرها في النقاط التالية:

-تمكن العملاء من دمج تفاعلاتهم المصرفية بسلسلة عبر قنوات متعددة ، مما يوفر تجربة مستخدم إستثنائية.

-تمكين العملاء من إجراء الأنشطة المالية في بيئة سريعة الإستجابة و سهلة الإستخدام و آمنة.

-تعمل على توفير عنصر الراحة و السرعة لكل من البنك و العميل ، بإتاحة إمكانية التسجيل عبر الأنترنت دون الحاجة إلى الأعمال الورقية

-تمكين البنك من إطلاق حملات تسويقية مستهدفة و الترويج لعدد من المنتجات و الخدمات المصرفية.

-إحتوائها على نظام مراسلة داخلي ثنائي الإتجاه يتيح التواصل الآمن بين العملاء و المصرف ، مما يتيح سرية البيانات الشخصية للعملاء.

-إدارة خدمات التنبيهات و ذلك من خلال تمكين المستخدمين من إعداد تنبيهاتهم و إشعاراتهم الخاصة سواء كانت رسائل نصية قصيرة أو بريد إلكتروني.¹

المبحث الثاني: الفجوات والثغرات التي تهدد مهام المصارف الرقمية في مكافحة غسل الأموال:

نتيجة للتطورات التكنولوجية المالية المعاصرة التي شهدتها المصارف الرقمية في الآونة الأخيرة، أحدثت تحولا جوهريا في القطاع المصرفي من خلال الخدمات الرقمية المتكاملة التي تقدمها عبر الوسائط الإلكترونية، إلا أنها رغم ما توفرها من سرعة و كفاءة في القيام بالمعاملات المالية ، فإنها أصبحت في الوقت ذاته عرضة لجملة من الفجوات و الثغرات التي أصبحت تستغلها الشبكات الإجرامية لإرتكاب جرائم غسل الأموال ، و إخفاء المصادر الغير مشروعة للأموال . و تتجلى أهم

¹ منصة الخدمات المصرفية الرقمية». «Platform DiGital Banking-NETinfo» متاح على الرابط: <https://netinfo.eu> ، أطلع عليه بتاريخ 23ماي 2026 على الساعة 11:50.

هذه الفجوات في التهديدات الإجرامية الرقمية التي تستهدف تقنيات المعلومات لسرقة البيانات باستخدام تقنيات رقمية ، كالمساس بأنظمة التحقق و إستعمال الوثائق المزورة ، فضلا على التحديات المرتبطة بالطابع العابر للحدود للمعاملات الرقمية و ما يترتب عليه من صعوبات أبرزها المعايير الرقابية بين الدول ، و زيادة الإعتماد على مزودي الخدمات دون تراخيص ، إضافة إلى غياب الآليات الأمنية التي تعمل على حفظ تبادل البيانات الشخصية ، هذا ما أدى إلى ضرورة الحد من الفجوات بإضعاف الجهود الرامية إلى مكافحة جرائم غسيل الأموال.

وبناء عليه نقسم هذا المبحث إلى مطلبين نتناول: **المطلب الأول:** التهديدات الإجرامية الرقمية .
المطلب الثاني: الفجوة الرقابية.

المطلب الأول: التهديدات الإجرامية الرقمية .

تواجه المصارف الرقمية متوسطة الحجم العديد من التهديدات الإجرامية التي تستهدف أمن عملياتها وخدماتها الإلكترونية، ومن أبرزها المساس بأنظمة التحقق من الهوية واستخدام الوثائق المزورة لفتح الحسابات أو تنفيذ المعاملات المالية بطرق احتيالية. وتزداد خطورة هذه التهديدات مع التوسع في الخدمات الرقمية، مما قد يؤدي إلى خسائر مالية وإضعاف ثقة العملاء. لذلك، أصبح تعزيز أنظمة التحقق والرقابة الأمنية ضرورة أساسية لحماية المصارف الرقمية وضمان سلامة معاملاتها .

وبناء عليه نقسم هذا المطلب إلى فرعين: نتناول في **الفرع الأول:** المساس بأنظمة التحقق، و**الفرع الثاني:** الوثائق المزورة.

الفرع الأول: المساس بأنظمة التحقق:

يعد المساس أو الإعتداء على أنظمة التحقق من بين الإعتداءات التي شهدت إنتشارا واسعا نتيجة تزايد استخدام تكنولوجيا المعلومات، والتي تهدف إلى إختراق آليات التحقق كالرقم السري والتوقيع الإلكتروني ورموز التحقق للوصول للبيانات الشخصية وإستهدافها، والمساس بأنظمة التحقق

يصنف ضمن الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات التي تستهدف الأنظمة المعلوماتية والبيانات المعالجة إلكترونيا.

ومنه يمكن دراسة هذا الفرع من خلال التقسيم الآتي: تعريف المساس بأنظمة المعالجة الآلية للمعطيات أولا، صور المساس بأنظمة التحقق ثانيا، الآليات المستعملة في المساس بأنظمة التحقق ثالثا.

أولا: تعريف المساس بأنظمة التحقق:

أدت التطورات السريعة التي شملت تقنيات الإعلام والإتصال إلى زيادة مجالات الإستعانة بالبيانات، والتي أصبحت ضرورة لتعامل في مختلف القطاعات، وقد تكون هذه البيانات متعلقة إما بالأشخاص أو المؤسسات، إلا أن هذا الإنتشار في إستعمال هذه البيانات أدى إلى زيادة إمكانية الإعتداءات التي قد تمسها، ومنه سيتم التطرق إلى التعريف التشريعي والتعريف الفقهي للمساس بأنظمة المعالجة الآلية للمعطيات.

1-التعريف التشريعي :

سنتطرق إلى موقف كل من التشريع المصري والتشريع الجزائري حول تعريف المساس بأنظمة المعالجة الآلية للمعطيات:

أ-موقف المشرع المصري : نجد أنه لم يعرف لنا المساس بأنظمة المعالجة الآلية للمعطيات، وإنما إكتفى بتحديد الأفعال التي تشكل مساس بأنظمة و تحديد العقوبات المقررة لها من القانون رقم 175 لسنة 2018 المتضمن بيان مكافحة جرائم تقنية المعلومات¹، حيث خصص الفصل الأول المعنون : الإعتداء على سلامة شبكات و أنظمة و تقنيات المعلومات جريمة الإنتفاع بدون حق بخدمات الاتصالات و المعلومات و تقنياتها بتحديد صور المساس بأنظمة المعالجة الآلية للمعطيات و التي شملت كل من :

¹ القانون رقم 175 لسنة 2018، المؤرخ في 14 أغسطس 2018، المتضمن بيان مكافحة جرائم تقنية المعلومات، ج ر، عدد 32، صادرة في 14 أغسطس 2018.

جريمة الدخول الغير المشروع المادة 14 منه.

جريمة تجاوز حدود الحق في الدخول المادة 15 منه.

جريمة الإعتراض غير المشروع المادة 16 منه.

جريمة الإعتداء على سلامة البيانات والنظم المعلوماتية¹ المادة 17 منه.. إلخ.¹

ب- موقف المشرع الجزائري: نجد أنه لم يعرف لنا المساس بأنظمة المعالجة الآلية للمعطيات، إلا أنه تدخل في تجريم بعض الصور للسلوكيات التي تشكل مساسا بنظام المعالجة الآلية للمعطيات، حيث جدد في قانون العقوبات الجزائري رقم 06-24 المعدل والمتمم لقانون العقوبات الصادرة بموجب الأمر رقم 66-156²، صور المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 إلى المادة 394 مكرر²، وهي كالتالي:

- **جريمة الدخول والبقاء عن طريق الغش:** والتي عرفها بموجب المادة 394 مكرر ف2 على أنه: " كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك ». مع تحديد العقوبة المقررة لها في المادة 394 مكرر³.

- **جريمة الإعتداء على سلامة المعطيات وعلى نظام المعالجة:** والتي عرفتها المادة 394 مكرر 1 من قانون العقوبات: "كل من أدخل بطريق الغش المعطيات في نظام للمعالجة الآلية وأزال أو عدل بطريق الغش المعطيات التي يتضمنها". وقد حدد العقوبة المقررة لها من خلال نص المادة 394 مكرر 1 من قانون العقوبات⁴.

ج- جريمة التعامل مع المعطيات غير المشروعة: والتي تعرف على أنها: " كل أشكال وأنواع التعامل الواقعة والواردة على معطيات الحاسب الآلي السابقة لعملية إستعمال هذه المعطيات لإرتكاب جريمة

1- القانون رقم 175 لسنة 2018، المؤرخ في 14 أغسطس 2018، المتضمن بيان مكافحة جرائم تقنية المعلومات، المصدر السابق.

2- القانون رقم 06-24، المؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، ج ر ج ج، العدد 30، الصادرة في 30 أبريل 2024.

3- المادة 394 مكرر من القانون رقم 06-24، المؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، المصدر السابق، ص 20.

4- المادة 394 مكرر 1 من القانون رقم 06-24، المؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، المصدر نفسه، ص 20.

ما، بداية من تخطيط المعطيات والبحث فيها وتجميعها وصولاً إلى نشرها من أجل جعلها في متناول الغير أو الإتجار بها.¹

وقد أقر لها المشرع الجزائري نظراً لخطورتها النص القانوني في المادة 394 مكرر 2 من قانون العقوبات.²

2- التعريف الفقهي :

تعدد التعريفات الفقهية المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات نظراً لخطورتها على البيانات الشخصية، حيث نذكر من هذه التعريفات ما يلي:

عرف المساس بأنظمة المعالجة الآلية للمعطيات على أنه: " المساس بمجموعة العناصر المتداخلة والمتفاعلة والمندمجة مع بعضها البعض والتي البيانات والمعلومات ومعالجتها وتخزينها وتوزيعها، بهدف دعم صناعة القرارات والتنسيق وتأمين السيطرة على المنظومة، إضافة لتحليل المشكلات للموضوعات المعقدة."³

كما تم تعريفها على أنها: الدخول الغير مشروع إلى الشبكات الخاصة والعبث بالبيانات الرقمية التي يحويها، أو إتلافها أو محوها مما يلحق ضرر بالبيانات والمعلومات دائماً، وكذلك البرامج والأجهزة التي يحويها."⁴

ثانياً: صور المساس بأنظمة التحقق:

1- سمير بودواب - فؤاد لبيديوي، " جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة 20 ماي 1955-سكيكدة، جوان 2024، ص 31.

2- المادة 394 مكرر 2 من القانون رقم 06-24، المؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، المصدر السابق، ص 20.

3- سمير بودواب - فؤاد لبيديوي، المرجع السابق، ص 10.

4- نسيمة جدي، " جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، مذكرة ماجيستر، تخصص قانون جنائي، كلية الحقوق، جامعة وهران، الجزائر، 2013-2014، ص 8.

تعد أنظمة التحقق من أحدث الطرق التي تعمل على التحقق من هوية العملاء في المصارف الرقمية، لضمان سلامة المعلومات واستخدامها من الأشخاص المصرح لهم، إلا أنها لم تسلم من الإعتداءات والإختراقات الغير مشروعة والتي تشمل كلمات المرور والتوقيع الإلكتروني ورموز التحقق، نذكر منها مايلي:

1-الإعتداء على كلمات المرور :

تعد الحماية بواسطة كلمات المرور من أكثر الإجراءات المستعملة في المجال الرقمي في الوقت الحالي، على إعتبار أن إستعماله يسمح لصاحب البرنامج التعرف أو التأكد من هوية المستخدم الذي يحاول الولوج لذلك الحساب، حيث أنه لا يمكن تصفح البيانات السرية والشخصية إلا بتقديم الرقم السري الصحيح.

لذلك أصبح من الضروري الحرص على سرية كلمات المرور وعدم الإفصاح بها الغير والتغيير الدوري لها، إلا أنه ونظرا لإمكانية الإعتداء عليها وإختراقها بكل سهولة كالإستعانة بوسائل أو برامج تتيح التواصل إلى الرقم السري من خلال عدد المحاولات.¹

2-الإعتداء على التوقيع الإلكتروني :

والذي يعرف على أنه: " مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته".²

1- عزو سعدي، " الأمن التقني الدفع الإلكتروني أي فعالية "، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي بتندوف، العدد الثاني، ديسمبر 2017، ص 123.

2- خالد بروان، " جرائم الإعتداء على التوقيع الإلكتروني"، مذكرة ماستر في الحقوق، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور -الجلفة، 2019-2020، ص 10.

حيث أنه ونتيجة للتطورات التكنولوجية التي فرضت استخدام التوقيع الإلكتروني في المعاملات اليومية، إلا أنه وعلى الرغم من التسهيلات التي يقدمها أصبح يستغل من قبل المحترفين كالقيام بتزوير التوقيع لإلحاق الأضرار بالتمعاقدين، ومن بين الإعتداءات نجد:

الدخول الغير مصرح به على قاعدة بيانات المتعلقة بالتوقيع الإلكتروني: أي الدخول الغير مرخص به إلى نظام المعالجة الآلية للمعطيات الذي يشمل على المعطيات المخزنة دون رضا المستخدم.

الحصول على التوقيع الإلكتروني بالوسائل الإحتيالية: كإستخدام البرمجيات الخبيثة تعمل على سرقة التوقيع الإلكتروني أو كلمات المرور المرتبطة به.¹

3-الإعتداء على رموز التحقق :

وهي عبارة عن رموز تحقق قصيرة غالبا ما تتكون من 4 إلى 6 أرقام، يتم إنشائها تلقائيا لتأكيد تسجيل الدخول أو تنفيذ معاملة، تمتاز رموز التحقق OTP بأنها رقم تعريف شخصي مرقت يعمل على تعزيز الأمان ، كما تمتاز بأنها سهلة الإستخدام ، و تعمل على قنوات متعددة مثل الرسائل النصية القصيرة ، البريد الإلكتروني و الإشعارات على الهواتف، وتستعمل رموز التحقق لتأكيد تحويل الأموال سواء كان محليا أو دوليا، إلا أن رموز التحقق رغم ما توفرها من أمان إلا أنها معرضة للإعتداء بإستعمال أساليب الإحتيال : كإستدراج العميل بإستعمال برامج خبيثة ، أو إنتحال شخصية موظف في البنك و إقناع العميل بضرورة الإفصاح عن البيانات المتعلقة برمز التحقق كإجراء يتخذه البنك لتحديث البيانات .²

ثالثا: الآليات المستعملة في المساس بأنظمة التحقق:

1- المرجع نفسه، ص 34-39

2- دينا يوسف، الرموز المؤقتة OTP في القطاع المصرفي: كيف يتم إرسالها ولماذا هي مهمة، 14 مارس 2024، متاح على الرابط: <https://www.authentica.sa/ar>، أطلع عليه بتاريخ 23 ماي 2026 على الساعة 21:09

يعتمد المساس بأنظمة التحقق على جملة من الآليات الغير مشروعة التي تستعمل بغرض إستهداف هذه الأنظمة والمساس بالبيانات الشخصية التي تتضمنها، تذكر من بين هذه الآليات مايلي:

1-التصيد الإحتيالي :

وهو بشكل نشاط غير قانوني يهدف إلى الحصول على المعلومات والبيانات الشخصية والسرية مثل: إسم المستخدم، كلمة المرور، أرقام بطاقة الإئتمان.. إلخ، عن طريق إرسال رسالة بريد مزيفة تبدو في ظاهرها أنها مرسله من قبل المؤسسة المصرفية تطلب من عملائها الإلتحاق بالرباط، أو إستخدام الرسائل غير المرغوب فيها والتي تعمل على نشر البرامج الضارة التي تتضمن ترويج للحل الأمثل لمكافحة الفيروسات مع طلب زيارة تلك الصفحة لتمكن من الحصول على البيانات الشخصية.¹

2-البرمجيات الخبيثة :

وتعرف بأنها: " أي برمجية تستخدم لأغراض غير شريفة على سبيل المثال إلحاق الضرر، سرقة البيانات، الوصول غير المصرح به، تخطي الحواجز الأمنية."² وتشمل هذه البرمجيات الخبيثة:

1- سناء العايب، "تسيير المخاطر السيبرانية في القطاع المالي من المنظور الدولي"، مجلة الدراسات المالية والحاسبية و الإدارية، جامعة العربي بن مهيدي -أم البواقي، الجزائر، المجلد 8، العدد 3، ديسمبر 2021، ص 472.

2- عبد القادر صواق، " مساهمة الأمر السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية"، أطروحة دكتوراه، تخصص تسويق الخدمات، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة غرداية - الجزائر، نوقشت في 26 سبتمبر 2024، ص 66.

برامج التجسس spyware: وهي برمجيات خبيثة تم إبتكارها لتتبع المستخدمين والتجسس على بياناتهم الشخصية مثل: كلمات السر أو أرقام بطاقات الائتمان.

حصان طروادة، Trojan Hors: وهي برامج خبيثة تعمل على سرقة المعلومات السرية المخزنة والتي يتم معالجتها من خلال الأنظمة البنكية عبر الأنترنت.

برامج الإعلانات المتسللة Adware، يعمل على جمع البيانات الشخصية بغاية عرضها وتحقيق إيرادات.¹

3- هجمة الرجل كوسيط: Man in the Middle Attack

وهو بشكل مستخدم ضار يعمل على إعتراض البيانات التي نستخدم بين مقدم الخدمة والمستخدم، ويعمل على الإستدراج الإلكتروني لكافة المراسلات التي يرسلها المستخدم، كأن يقوم بإرسال بيانات بطاقة الائتمان الخاصة به لموقع ما فإنه يتم إستغلال تلك البيانات من قبل المتطفلين.

4- الهندسة الإجتماعية:

وهي فن وعلم التلاعب بالأشخاص والتأثير عليهم للحصول على معلومات سرية أو للقيام بأعمال غير قانونية أو ضارة، ونستخدم الهندسة الإجتماعية في العديد من المجالات مثل الإحتيال الإلكتروني والتجسس والقرصنة الإلكترونية، ويستخدم المهندسون الإجتماعيون ضعف المستخدمين والثقة الزائدة في الوصول إلى المعلومات الحساسة وإقناعهم بإتخاذ إجراءات غير مرغوب فيها.

وتعد الهندسة الإجتماعية من أبرز الأساليب التي يستخدم في الإعتداء على البيانات الشخصية للعملاء في المصارف، ويشمل هذا التهديد كل من:

1- سناء العايب، المرجع السابق، ص 470.

الإحتيال الهاتفي: كأن يتم خداع العميل والإدعاء بأنه موظف من البنك يطلب منه تحديث بياناته أو تأكيد هويته، أو يطلب منه إعطاء الرقم السري أو كلمة المرور ورقم البطاقة الائتمانية من أجل إستغلالها.

الإحتيال البريدي: يتم إرسال رسالة بريدية إلى المستخدم يطلب منه إدراج بياناته الشخصية والضغط على الرابط، حيث يتم تحويله إلى موقع مزيف يشبه موقع البنك، من أجل سرقة معلوماته واستغلالها.

الإحتيال الشخصي: عن طريق الإحاطة بالمستخدم ومحاولة الحصول على بياناته الشخصية من الرقم السري أو شكل التوقيع، بغاية التلاعب والإستغلال.¹

الفرع الثاني: الوثائق المزورة الإلكترونية

المصارف الرقمية هي مؤسسات مالية تقدم خدماتها البنكية عبر الوسائط الإلكترونية وباستخدام الإنترنت دون الحاجة إلى الحضور المادي للعميل إلى البنك. وتشمل هذه الخدمات: فتح الحسابات إلكترونياً، التحويلات المالية الرقمية، الدفع الإلكتروني، القروض الرقمية، المحافظ الإلكترونية، وقد أصبح التحول الرقمي عنصراً أساسياً في تطوير القطاع المصرفي الحديث. وهذا ما سنعالجه في هذا الفرع من خلال استعراض مفهوم الوثائق المزورة الإلكترونية أولاً، وبيان أنواع هذه الوثائق في المصارف الرقمية ثانياً.

أولاً: مفهوم الوثائق المزورة إلكترونياً.

الوثائق المزورة إلكترونياً هي مستندات رقمية يتم التلاعب بمحتواها أو إنشاؤها بطرق غير مشروعة بهدف استعمالها في عمليات احتيالية داخل الأنظمة المصرفية الرقمية مثل: تزوير بطاقات الهوية الرقمية، تزوير كشوف الحسابات البنكية، تزوير التوقعات الإلكترونية، إنشاء شهادات رقمية

¹ عبد القادر صواق، المرجع السابق، ص 70.

مزيفة، التلاعب بالبيانات البنكية. وقد اعتبرت الدراسات القانونية أن التزوير الإلكتروني صورة من صور الفساد الرقمي الذي يهدد أمن المعلومات والثقة في المعاملات الإلكترونية.¹

1/تعريف الوثائق المزورة الإلكترونية

أ/لغة:

"لفظ مشتقة من الزور وهو الكذب والباطل، وقيل الشهادة الباطل وكلام مموه مزور بالكذب والتزوير هو محاولة تزيين الكذب وطمس الحقيقة والبأس الباطل بثوب الحق، فجوهر التزوير الكذب الذي يهدف إنشاء حقيقة مخالفة أو تحريف حقيقة قائمة".²

ب/إصطلاحا:

"إظهار الكذب في محرر على أنه حقيقة بعد خداع لعقيدة الآخرين والتزوير هو تقليد شيء ما مع التظاهر بأن هذا التقليد هو النسخة الأصلية رغم أنه ليس كذلك".³

ج/التعريف التشريعي لجريمة التزوير.

1- مريم تومي، صدراي وفاء، تزوير بطاقات الائتمان صورة خاصة في جريمة التزوير الإلكتروني، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، الجزائر، المجلد 5، العدد 02، 2021، ص 966.

2- المرجع نفسه، ص 966.

3- أحمد محمد محروس عبد العال، "التزوير الإلكتروني بين التشريع التقليدي وآليات المواجهة الحديثة"، المجلة الأكاديمية للأبحاث والنشر العلمي، جامعة طنطا، مصر، المجلد 6، العدد 02، 2025، ص 48.

يقصد بالتزوير قانوناً كل تغيير للحقيقة يتم بإحدى الوسائل التي يحددها القانون ويترتب عليه ضرر للغير. وقد نصت المادة 441 من قانون العقوبات الفرنسي المعدلة بتاريخ 14 ماي 1993 على أن التزوير هو كل تغيير للحقيقة من شأنه إحداث ضرر، يتم في محرر أو أي دعامة للتعبير عن الفكر بهدف إثبات حق أو واقعة ذات آثار قانونية.

ويُفهم من هذا النص أن التزوير لا يقتصر على المحررات الورقية، بل يمتد ليشمل المحررات الإلكترونية. كما عرفت المادة 07 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التزوير المعلوماتي بأنه كل إنشاء أو تعديل غير مشروع للبيانات المسجلة بما يؤثر في صحتها ويؤدي إلى خداع الغير.¹

أما في التشريع الجزائري، فقد نظم المشرع جرائم التزوير في المواد 222 إلى 229 من قانون العقوبات الجزائري، كما تناول بعض صور التزوير في الوثائق والشهادات بموجب المواد 219 و220 و222 من القانون ذاته.

وعليه، يمكن تعريف التزوير الإلكتروني بأنه كل تغيير غير مشروع للحقيقة في البيانات أو المحررات الإلكترونية عن طريق الإنشاء أو التعديل أو الحذف، بقصد استعمالها لإثبات حق أو واقعة على خلاف الحقيقة، بما يترتب عليه ضرر للغير.²

ثانياً: أنواع وثائق التزوير في المصارف الرقمية.

تتنوع صور وأساليب تزوير الوثائق في المصارف الرقمية بحسب الوسائل التقنية المستخدمة، حيث يلجأ المجرمون الإلكترونيون إلى اختراق الأنظمة المعلوماتية، واستعمال برامج التعديل الرقمي، وتقنيات الذكاء الاصطناعي، والتصيد الاحتيالي للحصول على بيانات العملاء أو إنشاء وثائق مزيفة يصعب اكتشافها، كما ازدادت خطورة هذه الجرائم مع انتشار الخدمات البنكية عبر الإنترنت والتطبيقات الذكية، مما جعل المصارف الرقمية هدفاً رئيسياً للهجمات الإلكترونية المنظمة.

¹ - ريم تومي، صدارتي وفاء، المرجع السابق، ص 996، 997.

² - عبد الفتاح بيومي حجازي، الدليل الجزائري والتزوير الجرائم الكمبيوتر والأنترنت، دار الكتب القانونية دون طبعة، مصر، 2000، ص 184.

1/ تزوير شهادة التصديق الإلكتروني:

- لم يتضمن القانون رقم 04-15 نصاً صريحاً يعرّف تزوير شهادة التصديق الإلكتروني، مما يستوجب الرجوع إلى القواعد العامة في قانون العقوبات.
- وتتمثل صور التزوير الممكنة في:¹
- تضمين الشهادة بيانات أو توقيعات إلكترونية مزورة.
 - انتحال صفة مؤدي خدمات التصديق الإلكتروني. وذلك حسب نص المادة 70 من نفس القانون.
 - تعديل بيانات الشهادة أو حذفها أو تزويرها بعد إصدارها.
 - استعمال بيانات شخصية لأغراض غير مشروعة، حسب نص المادة 72 من نفس القانون.
 - الإدلاء ببيانات كاذبة للحصول على شهادة تصديق إلكتروني، وذلك وفق نص المادة 68 من نفس القانون.

قد ترتكب جرائم التزوير الإلكتروني من مؤدي خدمات التصديق الإلكتروني، طالب الشهادة أو من الغير أو القراصنة الإلكترونيين. أما بالنسبة للقراصنة فقد يقوموا عادة باختراق أنظمة التصديق والاستيلاء على مفاتيح التشفير والتوقيعات الإلكترونية، مما يسمح لهم بإصدار شهادات مزورة أو استعمال بيانات الغير بصورة غير مشروعة.

رغم أن المشرع الجزائي جرم بعض الأفعال المرتبطة بالتصديق الإلكتروني، مثل: ممارسة خدمات التصديق دون ترخيص، إفشاء البيانات السرية، الإدلاء بتصريحات كاذبة للحصول على الشهادة، إلا أن العقوبات الواردة في نصوص المواد 68، 70، 72 من نفس القانون غير كافية مقارنة بخطورة الجرائم المرتكبة، خاصة إذا ما قورنت بالعقوبات المقررة في النصوص العامة المتعلقة بتزوير المحررات الرسمية،

1- القانون رقم 04/15 المؤرخ في 11 ربيع الثاني 1436 هـ الموافق لاول فبراير سنة 2015، يحدد القانون المتعلق بالتوقيع والتصديق الإلكتروني، ج ر، ج، ج، عدد 06، الصادر في 20 ربيع الثاني 11/36 هـ الموافق ل 10 فبراير سنة 2015.

حيث أن النصوص الحالية لا تغطي جميع صور التزوير الإلكتروني، خاصة ما يتعلق بالتلاعب بالبيانات الإلكترونية أو اختراق أنظمة التشفير.¹

2/تزوير بطاقات الائتمان:

بطاقة الائتمان هي بطاقة إلكترونية تصدرها مؤسسة مالية أو بنك، تخول لحاملها شراء السلع والخدمات أو سحب الأموال دون الدفع الفوري، على أن يتم تسديد المبالغ لاحقاً وفقاً للشروط المتفق عليها مع الجهة المصدرة. وتحتوي هذه البطاقة على مجموعة من البيانات المهمة مثل اسم حاملها ورقمها وتاريخ صلاحيتها والشريط المغنط والرقم السري.²

قد يتم تزوير بطاقات الائتمان بالتلاعب في محتوياتها سواء تعلق الأمر بالمعلومات المرئية الموجودة عليها أو المعلومات المشفرة المخزنة في الشريط المغنط، وتنقسم صور التزوير إلى نوعين رئيسيين: التزوير الكلي والتزوير الجزئي.

يتم التزوير الكلي عن طريق إنشاء بطاقة مزورة بالكامل تحاكي البطاقة الأصلية من حيث الشكل والمضمون، بحيث يتم تقليد جميع عناصرها الأساسية، ومن أبرز العلامات التي تكشف التزوير الكلي: عدم دقة أو ثبات الشريط المغنط أو شريط التوقيع وإمكانية نزعه بسهولة، اختلاف شكل أو حجم البيانات المطبوعة عن البطاقة الأصلية أو عدم تطابق البيانات المطبوعة مع البيانات المخزنة في الشريط المغنط.

أما التزوير الجزئي لبطاقة الائتمان فيقوم على وجود بطاقة أصلية وصحيحة، تم إجراء تعديلات على بعض بياناتها أو عناصرها دون إعادة تصنيع البطاقة كاملة. ويستغل المزور الجسم الحقيقي للبطاقة وما يحتويه من علامات أمنية، ومن المؤشرات التي تساعد على اكتشاف التزوير الجزئي: ظهور آثار محو أو

1- عبد الحليم بوقرين - إيمان بوناصر، "تزوير شهادة التصديق الإلكتروني بين جمود النصوص وتطور التقنية"، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الاغواط، الجزائر، مجلد 3، العدد 2، 2019، ص ص 6-9.

2- فارس خطايي - ديلة مباركي، "تزوير التوقيع الإلكتروني في البطاقات الائتمان -دراسة على ضوء القانون 15/ 04 المتعلق بالتوقيع والتصديق الإلكتروني"، المجلة الجزائرية للأمن الإنساني، جامعة الحاج لخضر 1 باتنة، الجزائر، مجلد 5، عدد 2، 2020، ص 657.

تلف في مواضع التوقيع، وجود بقع داكنة أو مصفرة نتيجة استعمال مواد كيميائية لإزالة البيانات وعدم دقة تثبيت شريط التوقيع الجديد أو ظهور آثار لاصق وخدوش حوله.¹

المطلب الثاني: الفجوات الرقابية:

يشهد القطاع المصرفي الرقمي تطورًا متسارعًا صاحبه ظهور فجوات رقابية، خاصة مع الاعتماد على مزودي خدمات غير مرخصين وتزايد مخاطر القرصنة وتسريب البيانات والمعلومات الشخصية. وتكمن أهمية الأنظمة الرقابية في تنظيم الأنشطة المصرفية الرقمية، وفرض متطلبات الترخيص والامتثال، وتعزيز أمن المعلومات وحماية العملاء، بما يساهم في الحد من المخاطر وضمان استقرار وثقة النظام المصرفي وبناءا عليه نقسم هذا المطلب الى 3 فروع: **الفرع الأول:** الإعتماد على مزودي خدمات رقمية دون تراخيص، **الفرع الثاني:** تباين أنظمة الرقابة على المستوى العالمي، **الفرع الثالث:** غياب آليات أمانة لتبادل المعلومات والبيانات الشخصية.

الفرع الأول: الإعتماد على مزودي خدمات رقمية دون الحصول على تراخيص:

أصبح الاعتماد على مزودي الخدمات المالية وتقنية خيارًا شائعًا لدى العديد من المؤسسات لتقديم خدمات الدفع والتحويلات المالية بسرعة وكفاءة، غير أن ممارسة بعض الأنشطة المصرفية أو المالية دون الحصول على التراخيص القانونية اللازمة من الجهات الرقابية المختصة قد يعرض المؤسسات لمخاطر قانونية وتنظيمية كبيرة، كما قد يؤثر ذلك على مستوى الثقة والأمان وحماية حقوق العملاء، مما يجعل الالتزام بالمتطلبات التنظيمية والحصول على التراخيص المناسبة عنصرًا

1- رياض فتح الله بصله، "جرائم بطاقات الإئتمان"، دارالشروق، الطبعة الاولى، بيروت لبنان، 1995، ص 108.

أساسيًا لضمان استمرارية النشاط ومشروعيته. وهذا ما سنعالجه في هذا الفرع: مفهوم مزودي خدمات المصرفية أولاً، العلاقة بين مزودي الخدمات دون تراخيص وجريمة غسل الأموال ثانياً.

أولاً: مفهوم مزودي الخدمات المصرفية.

يقصد بمزود الخدمات المصرفية بأنهم المؤسسات أو الجهات المالية التي تتولى تقديم الخدمات البنكية والمالية للأفراد والمؤسسات، مثل إدارة الحسابات، تحويل الأموال، خدمات الدفع، الإقراض، والعمليات المصرفية الإلكترونية.

1/تعريف الخدمات المصرفية الإلكترونية المرخصة :

تُعرّف الخدمات المصرفية الإلكترونية بأنها: "مجموعة الخدمات والعمليات البنكية التي تُقدّم للعملاء باستخدام وسائل وتقنيات الاتصال الحديثة، سواء السلكية أو اللاسلكية، بما يتيح إنجاز المعاملات المصرفية عن بُعد دون الحاجة إلى التواجد الفعلي داخل البنك.¹"

2/تعريف الخدمات المصرفية دون تراخيص :

"كل نشاط أو عملية مصرفية تمارسها جهة أو شخص طبيعي أو معنوي دون الحصول مسبقاً على الاعتماد أو الترخيص القانوني الصادر عن السلطة المختصة، متى تعلق الأمر بتلقي أموال الجمهور أو منح الائتمان أو تقديم خدمات الدفع أو غيرها من العمليات التي حصر القانون ممارستها في البنوك والمؤسسات المالية المعتمدة.²"

1- هاجر ديدوش -عبد الغني حريري، "واقع الخدمات المصرفية الإلكترونية بالبنوك الجزائرية"، مجلة إستراتيجية للتحقيقات الاقتصادية، جامعة تيبازة، الجزائر، مجلد 4، عدد 1، 2022، ص 23.

2- أمينة سماعين فراقي، "الأحكام الخاصة بجرائم القانون النقدي والمصرفي رقم 09/ 23 على ضوء التوجيهات الحديثة للسياسات الجنائية"، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، الاغواط، الجزائر، مجلد 8، عدد 1، 2024/03، ص 252.

ثانيا: العلاقة بين مزودي الخدمات دون تراخيص وجريمة غسل الأموال:

إن العلاقة بين مزودي الخدمات المالية غير المرخصين وغسل الأموال ليست علاقة مباشرة دائماً، لكنها علاقة استغلال، أي أن هذه الجهات قد تكون في الأصل تقدم خدمات تحويل أو وساطة مالية، لكن غياب الرقابة يجعلها بيئة مناسبة لاستغلالها في عمليات غير قانونية ويتم ذلك من خلال: الضعف الرقابي وغياب التقارير المالية.

1/ مفهوم ضعف الرقابة

يقصد بضعف الرقابة في المجال القانوني والمالي عدم قدرة الأجهزة الرقابية الداخلية أو الخارجية على القيام بوظائفها بشكل فعال، سواء في الكشف عن الانحرافات أو منع المخالفات أو تصحيح الاختلالات داخل المؤسسات، ويظهر هذا الضعف في غياب المتابعة الدقيقة، أو تأخر التدخل الرقابي، أو عدم فعالية أدوات التفتيش والمحاسبة.¹

أ- أسباب ضعف الرقابة:

- تتعدد الأسباب المؤدية إلى ضعف الرقابة، ويمكن إجمالها فيما يلي:
- قصور الإطار التنظيمي أو القانوني رغم وجود نصوص قانونية، إلا أن تطبيقها قد يكون غير فعال.
- ضعف الكفاءة والخبرة البشرية لدى القائمين على أجهزة الرقابة.
- غياب الاستقلالية للهيئات الرقابية، مما يؤثر على موضوعية قراراتها.
- تضارب المصالح داخل المؤسسات المالية والإدارية.

1- نجا طباعة، "عن أزمة ضعف الرقابة في تفعيل الإدارة الرشيدة للبنوك العمومية"، مجلة الدراسات حول فعالية القاعدة القانونية، جامعة عبد الرحمن ميرة- بجاية، الجزائر، المجلد 8، العدد 1، 2024، ص 18.

- ضعف أنظمة المعلومات والتدقيق الداخلي مما يؤدي إلى بطء أو عدم دقة التقارير.
- غياب الشفافية وعدم الإفصاح الكامل عن العمليات المالية والإدارية.¹

ب- آثار ضعف الرقابة:

يترتب عن ضعف الرقابة مجموعة من النتائج السلبية الخطيرة، خاصة في القطاع المالي والمصرفي، أهمها:

- انتشار الفساد المالي والإداري داخل المؤسسات.
- ارتفاع مخاطر غسل الأموال والاحتيال المالي نتيجة غياب المتابعة الفعالة.
- ضعف الثقة في النظام المصرفي والمؤسسات المالية.
- تدهور الأداء الاقتصادي للمؤسسات العامة والخاصة.
- عدم كشف الانحرافات في الوقت المناسب، مما يؤدي إلى تفاقم الأزمات المالية.²

ج- العلاقة بين ضعف الرقابة وغسل الأموال:

تعد الرقابة الضعيفة بيئة خصبة لارتكاب جرائم غسل الأموال، حيث تسمح بتمرير العمليات المالية المشبوهة دون تدقيق كافٍ، خاصة عند غياب آليات مثل التحقق من هوية العملاء (KYC) والإبلاغ عن العمليات المشبوهة، وضعف التدقيق الداخلي والخارجي.³

2/ غياب التقارير المالية:

يعتبر الإفصاح المالي من الركائز الأساسية لضمان الشفافية والمساءلة في الأنشطة الاقتصادية والمالية، حيث تسهم التقارير المالية في توفير معلومات دقيقة حول المركز المالي للمؤسسات ونتائج أعمالها. ويؤدي غياب هذه التقارير أو عدم إعدادها بصورة منتظمة إلى إضعاف فعالية الرقابة المالية وتقليل قدرة الجهات المختصة على متابعة حركة الأموال والتحقق من مشروعيتها. كما يترتب على

1- آسيا خليفة، "أساليب الرقابة البنكية الإحترازية خلال فترة 2014-2018"، مجلة استراتيجيات التحقيقات الإقتصادية والمالية، جامعة تيبازة، الجزائر، مجلد 3، عدد 2، 2021، ص 68-89.

2- نجا طباعة، المرجع السابق، ص 12، 13.

3- آسيا خليفة، المرجع السابق، ص 19.

ذلك انخفاض مستوى الشفافية، الأمر الذي يخلق بيئة ملائمة لإخفاء المعاملات المالية غير المشروعة وصعوبة اكتشاف المخالفات المالية.¹

- العلاقة بين غياب التقارير المالية وجريمة غسل الأموال:

تتجلى العلاقة بين غياب التقارير المالية وجريمة غسل الأموال في أن ضعف الإفصاح المالي أو انعدامه يحدّ من قدرة الجهات الرقابية على كشف العمليات المشبوهة وتتبع التدفقات المالية غير المشروعة، فالتقارير المالية المنتظمة تمثل وسيلة فعالة لرصد المعاملات غير الاعتيادية والكشف عن التناقضات المالية التي قد تشكل مؤشرات على وجود عمليات غسل أموال. ومن ثم، فإن تعزيز نظم التقارير المالية والالتزام بالإفصاح الدقيق والشفاف يُعدّ من أهم الآليات القانونية والرقابية للحد من مخاطر غسل الأموال وحماية نزاهة النظام المالي.²

الفرع الثاني: تباين أنظمة الرقابة على المستوى العالمي:

إن توحيد المعايير الرقابية يعد من أهم الركائز الأساسية التي تقوم عليها الجهود الدولية، لتمكين المصارف الرقمية من مكافحة الجرائم المالية التي تستهدفها ومن أبرزها جرائم غسيل الأموال التي تتسم بطابعها العابر للحدود، إلا أن تباين الأنظمة الرقابية بين مختلف الدول من شأنه أن يولد فجوات وثغرات تنظيمية ورقابية يمكن استغلالها من قبل مرتكبي جرائم غسيل الأموال، للقيام بتحويل الأموال و مصادرها غير المشروعة عبر أنظمة قانونية أقل صرامة، الأمر الذي يحد من قدرة و فعالية

1- فادي شوشان، "التحول الرقمي وآثاره في تعزيز الكفاءة والشفافية في إدارة المالية العامة"، المجلة الجزائرية للمالية العامة، جامعة أبو بكر بلقايد- تلمسان، الجزائر، مجلد 15، عدد 1، 2025، ص 6.

2- فادي شوشان، المرجع السابق، ص 9.

المصارف الرقمية في مكافحة أو تتبع هذه الأنشطة الغير مشروعة، وبالتالي فإن توحيد أنظمة الرقابة على المستوى العالمي أصبح من الحلول الرائدة لمواجهة جرائم غسيل الأموال.

ومن هذا المنطلق يمكننا دراسة هذا الفرع من خلال بيان المعايير المساهمة في تباين أنظمة الرقابة على المستوى العالمي، والتي يمكن حصر أهمها في النقاط التالية: تباين التشريعات المتعلقة بمكافحة جريمة غسيل الأموال أولاً، غياب التوافق الدولي في مجال مكافحة جرائم غسيل الأموال ثانياً، ضعف التعاون الدولي بسبب عقبة السرية المصرفية ثالثاً، ضعف أجهزة الرقابة ووجود إشكاليات قانونية بداخلها رابعاً

أولاً: تباين التشريعات المتعلقة بمكافحة جريمة غسيل الأموال:

حيث نجد أن ما يشكل جريمة في تشريع ما قد يعتبر أمراً متاحاً في تشريع دولة أخرى، مثلاً نرى أن بعض تشريعات الدول تجرم تجارة المخدرات إلا أنها لا تحرم استهلاكها أو تعاطيها وتعتبرها من الحرية الشخصية، في حين أن بعض التشريعات الأخرى تجرم كل من التجارة و الإستهلاك، هذا ما ينتج عنه تباين كبير فيما بين التشريعات بشأن الأحكام القانونية المنظمة لمكافحة جريمة غسل الأموال، والذي من شأنه أن يولد ثغرات في التشريعات ويتيح فرص لمرتكبي هذه الجريمة من أجل استغلالها في ارتكاب مختلف العمليات المرتبطة بغسل عوائدهم غير المشروعة أو الإجرامية، هذا التباين قد يؤدي إلى ضعف التنسيق الدولي في مجال مكافحة هذا النوع من الجرائم.¹

ثانياً: غياب التوافق الدولي في مجال مكافحة جرائم غسيل الأموال:

تعد هذه المسألة من أبرز التحديات التي تواجه فعالية الجهود الدولية في التصدي لجرائم غسيل الأموال عبر البيئة الرقمية، حيث نجد تباين بين الدول التي تسعى إلى وضع أنظمة رقابية صارمة و بين دول ذات ضعف رقابي، وتعد مجموعة العمل المالي من أبرز الهيئات الحكومية التي تسعى إلى تحقيق التوافق الدولي لمكافحة جرائم غسيل الأموال، وهي تمثل هيئة مستقلة متعددة الحكومات تعمل على

1- عبد العزيز منصور الميل، المرجع السابق، ص 845.

تعزيز حماية النظام المالي العالمي ضد الحرائم المالية، و تتألف هذه الهيئة الحكومية من خبراء في مجال الإقتصاد و المال و المصارف و سياسين و رجال أعمال و قضاة و موظفي جمارك ، تهدف إلى :

-نشر رسالة مكافحة جرائم تبييض الأموال في أنحاء العالم.

-زيادة يقظة المؤسسات المالية.

-المساعدة الدولية المتبادلة في تسليم المجرمين.

-إصدار سياسات الحد من سرية البنوك لعدم عرقلة كشف جرائم تبييض الأموال.

-تعزيز دور النظام المالي في مكافحة تبييض الأموال بإلزام البنوك بفحص هوية العملاء مع الإبلاغ عن المعاملات المشتبه فيها.¹

إلا أنه يلاحظ وجود تفاوت بين التشريعات الدولية في الأخذ بتوصيات مجموعة العمل المالي، مما يؤدي إلى وجود دول ملتزمة وهي الدول الأعضاء والتي عملت على دمج التوصيات بقوانينها الوطنية بهدف تكثيف الرقابة على جرائم غسيل الأموال، كما توجد دول خاضعة للمتابعة المتزايدة تدرج ضمن (القائمة الرمادية) وهي الدول التي تعاني نظمها التشريعية و الرقابية من ضعف في مكافحة غسيل الأموال و تمويل الإرهاب، لكنها قدمت التزاما رفيع المستوى بخطة عمل لمجموعة العمل المالي، وتخص هذه الدول إلى متبعتها إلى حين استيفاء و تنفيذ الخطة ضمن إطار زمني محدد.

إلى جانب المجموعتين السابقتين، نجد الدول عالية المخاطر والمدرجة في (القائمة السوداء): وهي الدول التي تدعو مجموعة العمل المالي إلى اتخاذ إجراءات بشأنها، حيث تعاني هذه الدول من اختلالات ونقص إستراتيجية والتي يتم يجب تطبيق تدابير مضادة تجاهها، كما لم تحرز هذه الدول تقدما لمعالجة النقائص أو التي لم تقدم تعهدا لتنفيذ خطة عمل مع مجموعة العمل المالي². وبالتالي فإن

1- غنية آيت بن أعر، " دور مجموعة العمل المالي في نطاق مواجهة جرمي تبييض الأموال وتمويل الإرهاب، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس -مستغانم، الجزائر، المجلد6، العدد 2، جوان 2021، ص 238-242.

2- مذكرة توضيحية بخصوص الدول عالية المخاطر والدول محل المتابعة المتزايدة، صادرة عن اللجنة التونسية لتحليل المالية، تونس، 25 ماي 2025، ص 1، ص 2.

هذا التفاوت يعجل من مرتكبي جرائم غسيل الأموال في استغلال تلك الثغرات، خاصة بالنسبة الدول التي تفتقر لقوانين صارمة لمكافحة غسيل الأموال.

ثالثا: ضعف التعاون الدولي بسبب عقبة السرية المصرفية:

تعد السرية المصرفية من أبرز القواعد الأساسية التي تربط البنك وصاحب الحساب، والتي تفرض عليه عدم الإفصاح بأسرار العميل لما لها من دور في بناء الثقة والائتمان المصرفي، إلا أن هذا المبدأ يشكل عائقا أمام مكافحة جرائم الأموال، حيث إستغل مرتكبي جرائم غسيل الأموال السرية المطلقة لبيانات الحسابات البنكية التي تفترضه بعض الدول للقيام بعملياتها الإجرامية.¹

من منطلق أن السرية المصرفية تؤدي إلى إخفاء وتحويل المصادر غير المشروعة للأموال، خاصة وأن المصارف تعد المكان الملائم لتحقيق جريمة غسيل الأموال، بالتالي تؤدي إلى عرقلة تتبع مصدر وحركة الأموال ومحل غسيل الأموال لاسيما في الدول التي تأخذ بالسرية المطلقة الحسابات.²

رابعا: ضعف أجهزة الرقابة ووجود إشكاليات قانونية بداخلها:

عملت الدول على وضع نظام رقابي يهدف إلى رصد الصفقات المشبوهة والتصدي لعمليات غسيل الأموال، إلا أنه من الملاحظ وجود تباين بين الدول في التزام البنوك والمؤسسات المالية بتأهيل الإطارات المسؤولة العاملة في القطاع المصرفي، إضافة إلى ازدواجية المسؤوليات وتداخل الصلاحيات التي أصبحت تشكل عائقا أمام مكافحة غسيل الأموال، ذلك أن المؤسسات المالية تتشكل أرباحها أساسا من الأموال المودعة لديها، مما أدى ببعض المصارف إلى وقوعها بشكل مباشر أو غير مباشر، في تسهيل عمليات غير مشروعة لتحقيق نكتسب مالية ضخمة.³

1- كمال فراحتية، "التعاون الدولي ودور البنوك في مكافحة جريمة تبيض الأموال"، أطروحة دكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، الجزائر، نوقشت في 26 سبتمبر 2017، ص 222.

2- محمد حميش، "معوقات مكافحة جرمي تبيض الأموال وتمويل الإرهاب، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس -مستغانم، الجزائر، المجلد 5، العدد2، ديسمبر 2020، ص 404.

3- عبد العزيز منصور الميل، المرجع السابق، ص 847.

الفرع الثالث: غياب آليات أمنية لتبادل البيانات الشخصية:

أصبحت البيانات الشخصية من أهم الأصول في العصر الرقمي، حيث تُستخدم في مختلف المعاملات الإلكترونية والخدمات الرقمية، ومع التوسع الكبير في استخدام الإنترنت وتبادل المعلومات عبر الشبكات، برزت الحاجة إلى توفير آليات آمنة لحماية هذه البيانات من الوصول غير المصرح به. إلا أن غياب هذه الآليات أو ضعفها يؤدي إلى زيادة احتمالية تعرض البيانات الشخصية للاختراق والقرصنة الإلكترونية، مما يشكل تهديدًا حقيقيًا لخصوصية الأفراد وأمنهم الرقمي.

وهذا ما سنعالجه في هذا الفرع، من مفهوم البيانات الشخصية أولاً، أثر غياب الآليات الآمنة على زيادة مخاطر القرصنة الإلكترونية ثانياً، سبل تعزيز أمن البيانات الشخصية ثالثاً.

أولاً: مفهوم البيانات الشخصية:

تشير البيانات الشخصية إلى جميع المعلومات التي يمكن من خلالها التعرف على هوية شخص معين بشكل مباشر أو غير مباشر، مثل الاسم، ورقم الهاتف، والعنوان، والبريد الإلكتروني، والبيانات البيومترية، والمعلومات المالية والصحية، وتكتسب هذه البيانات أهمية كبيرة نظراً لارتباطها المباشر بحقوق الأفراد وخصوصيتهم.¹

- أما بالنسبة **المشرع المصري** عرف البيانات الشخصية في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 في المادة الأولى: عرفت البيانات الشخصية بأنها البيانات المتعلقة بشخص طبيعي محدد أو يمكن تحديده بصورة مباشرة أو غير مباشرة من خلال الربط بينها وبين بيانات أخرى، كما اعتبر قانون حماية البيانات الشخصية لسنة 2020 البيانات الشخصية هي كل بيانات تتعلق بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى.²

1- رحمانى إيمان، لعطار زين العابدين، **حماية البيانات الشخصية في العصر الرقمي**، مجلة طلبة للدراسات العلمية الأكاديمية المركز الجامعي سي الحواس بركة، الجزائر، مجلد 8 العدد 2، 2025، ص 406.

2- المادة الأولى من القانون رقم 175 لسنة 2018 المتعلق بقانون حماية البيانات الحساسة، الجريدة الرسمية، عدد 28، الصادر بتاريخ 14 أوت 2018.

- كرسّ المشرّع الجزائري حماية البيانات الشخصية على المستوى الدستوري والتشريعي. فقد نصّ التعديل الدستوري لسنة 2016 على حماية المعطيات الشخصية بموجب المادة 46، ثم أكد دستور 2020 هذا الحق من خلال المادة 47، مما يعكس الأهمية التي أولتها الدولة لحماية الحياة الخاصة للأفراد في البيئة الرقمية.

كما جاء القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ليضع تعريفاً قانونياً للبيانات الشخصية، حيث نصّ على أنّها كل معلومة، بغضّ النظر عن دعامتها حفظها، تتعلق بشخص طبيعي معرّف أو قابل للتعرف عليه بصورة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

وعليه، يتضح أن المشرّع الجزائري تبنى مفهوماً واسعاً للبيانات الشخصية، يشمل جميع المعلومات التي تسمح بتحديد هوية الشخص الطبيعي، سواء بشكل مباشر أو عن طريق الربط بينها وبين بيانات أخرى، بما ينسجم مع التوجهات الحديثة في مجال حماية المعطيات الشخصية.¹

ثانياً: أثر غياب الآليات الأمنية على زيادة مخاطر القرصنة الإلكترونية:

مع التوسع المتسارع في استخدام التقنيات الرقمية والاعتماد المتزايد على الأنظمة المعلوماتية، أصبحت حماية البيانات والأصول الرقمية ضرورة ملحة. غير أن غياب الآليات الأمنية الفعّالة، مثل أنظمة الحماية والتشفير والمراقبة المستمرة، يفتح المجال أمام الجهات الخبيثة لاستغلال الثغرات الأمنية. ويؤدي ذلك إلى زيادة مخاطر القرصنة الإلكترونية وما يترتب عنها من سرقة للبيانات، وتعطيل

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

للخدمات، وخسائر مادية ومعنوية للأفراد والمؤسسات. لذلك يُعدّ تعزيز الأمن السيبراني وتطوير آليات الحماية الآمنة من أهم السبل للحد من التهديدات الإلكترونية المتزايدة.

1/ مظاهر ضعف حماية البيانات الشخصية:

يظهر ضعف حماية البيانات الشخصية من خلال عدة ممارسات، منها: استخدام شبكات اتصال غير آمنة، عدم تشفير البيانات أثناء نقلها، استخدام كلمات مرور ضعيفة، غياب التحديثات الأمنية للأنظمة والبرمجيات، ضعف الوعي الأمني لدى المستخدمين.¹

2/ مخاطر القرصنة الإلكترونية الناتجة عن ضعف الحماية:

عندما تغيب الآليات الأمنية المناسبة، تصبح البيانات الشخصية عرضة للعديد من المخاطر، أبرزها:

أ- تزويد البيانات أو المعلومات الخاصة بالحكومة الإلكترونية:

تقوم الحكومة الإلكترونية على قاعدة بيانات رقمية مترابطة بين مختلف المؤسسات، الأمر الذي يفرض تحديات تتعلق بأمن وسلامة هذه البيانات. إذ يمكن أن تتعرض للاختراق أو التلاعب أو التسريب، سواء عبر شبكات الإنترنت أو من خلال أنظمة المعلومات المرتبطة بها.

1- ليلي بن برغوث، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي: التهديدات، التقنيات، التحديات، والآليات التصدي"، المجلة الدولية للاتصال الاجتماعي، جامعة عبد الحميد بن باديس - مستغانم، الجزائر، المجلد 10، عدد 1، 2023، ص 449.

كما أن تبادل المعلومات بين الجهات الإدارية يتم عبر وسائط إلكترونية قد تكون عرضة للتجسس أو الاعتراض، مما يستدعي اعتماد تقنيات حماية متقدمة لضمان سرية البيانات وسلامتها وتكاملها، مثل التشفير وأنظمة الحماية السيبرانية.¹

ب- جرائم الأموال في نطاق التجارة الإلكترونية:

يبرز هذا النوع من التحديات باعتباره من أخطر الجرائم المرتبطة بالبيئة الرقمية، حيث تتخذ الجرائم المالية عبر الإنترنت صوراً متعددة، مثل الاحتيال الإلكتروني، التلاعب بالبطاقات البنكية، سرقة البيانات المالية، أو الاستيلاء غير المشروع على الأموال.

وتتميز هذه الجرائم بصعوبة التتبع لكونها تُرتكب عبر شبكات عابرة للحدود، مما يفرض على الحكومات تطوير أطر قانونية وتقنية متقدمة لمكافحتها وتعزيز التعاون الدولي في هذا المجال.

ج- مسؤولية مقدمي الخدمات الوسيطة في نطاق شبكة الانترنت والاتصالات:

تتعلق هذه الإشكالية بتحديد المسؤولية القانونية لمقدمي خدمات الإنترنت والاتصال، مثل مزودي خدمة الوصول أو التخزين أو نقل البيانات.

ويتمحور الإشكال القانوني حول مدى مسؤوليتهم عن المحتوى أو البيانات التي تمر عبر شبكاتهم، وما إذا كانوا يُعدّون مسؤولين مباشرة عن الأضرار الناتجة عن الاستخدام غير المشروع، أم أن مسؤوليتهم

1- بجاوي محمد، مخاطر القرصنة المعلوماتية على الحكومة الإلكترونية، مجلة البحوث والدراسات العلمية، جامعة يحي فارس -المدية، الجزائر، العدد 5، يوليو 2011، ص ص 10-11.

تبقى محدودة في إطار الوساطة التقنية فقط، مع ضرورة وضع ضوابط قانونية واضحة تحدد نطاق هذه المسؤولية.¹

د- جرائم الاعتداء على بيانات الحكومة الإلكترونية:

تُعد هذه الجرائم من أخطر التهديدات التي تواجه أنظمة الحكومة الإلكترونية، وتشمل كل فعل غير مشروع يستهدف الوصول إلى البيانات الحكومية أو تعديلها أو إتلافها أو تعطيلها. وتتعدد صورها بين الاختراق، نشر البرمجيات الخبيثة، تعطيل الأنظمة، أو التلاعب بالمعلومات الرسمية، وهو ما يستوجب تشريعات صارمة لحماية البنية المعلوماتية للدولة وضمان استمرارية الخدمات العامة.²

ثالثا: سبل تعزيز أمن البيانات الشخصية:

1- الحلول التقنية:

اعتماد تقنيات تشفير قوية للبيانات استخدام أنظمة الحماية المتقدمة لتحديث البرمجيات بشكل دوري تفعيل المصادقة متعددة العوامل مراقبة الشبكات واكتشاف الأنشطة المشبوهة.³

- كما يركز الجانب التقني لأمن المعلومات على مجموعة من الوسائل والإجراءات الفنية التي تهدف إلى حماية الأنظمة والبيانات من الاختراق أو التلف أو الاستعمال غير المشروع. ومن أهم هذه الإجراءات استخدام برامج الحماية ومكافحة الفيروسات، وتأمين الملفات الحساسة بكلمات مرور وتقنيات التشفير، إضافة إلى حذف المعلومات بطرق تمنع استرجاعها. كما يشمل ذلك الحذر أثناء استعمال الإنترنت والبريد الإلكتروني، وتجنب فتح الروابط أو الملفات المجهولة، وعدم حفظ كلمات

1- يحياوي محمد، المرجع السابق، ص 12

2- المرجع نفسه، ص 451

3- ساره جريش واخرون المواجهة الجنائية للقرصنة الرقمية للبطاقات المصرفية وسبل الوقاية منها بالتشريع المغربي، المجلة العربية الألمانية للعلوم الشرعية والقانونية، المجلد 3، العدد 1، ألمانيا، 2024، ص 68-69.

المرور على الأجهزة أو المتصفحات. كذلك تُلزم المؤسسات بتحديث برامج الحماية والأنظمة بشكل دوري لضمان مواجهة التهديدات الإلكترونية الحديثة والحفاظ على سلامة المعلومات وسريتها.

2-الحلول التنظيمية والقانونية:

مع تزايد التهديدات الإلكترونية وتطور أساليب الهجمات السيبرانية، أصبح من الضروري مواجهة مخاطر القرصنة الإلكترونية من خلال اعتماد حلول تنظيمية وقانونية فعالة. فإلى جانب الوسائل التقنية، تسهم القوانين والتشريعات المنظمة للفضاء الرقمي والإجراءات التنظيمية داخل المؤسسات في تعزيز أمن المعلومات والحد من الجرائم الإلكترونية، وذلك من خلال:

- وضع سياسات وإجراءات واضحة لأمن المعلومات داخل المؤسسات.
- توعية المستخدمين وتدريبهم على الممارسات الآمنة.
- سنّ قوانين تجرم القرصنة الإلكترونية وتحدد العقوبات المناسبة.
- تعزيز التعاون بين الجهات المختصة لمكافحة الجرائم الإلكترونية.
- حماية البيانات الشخصية من خلال تشريعات خاصة بالأمن الرقمي والخصوصية.
- تعزيز ثقافة حماية البيانات لدى المستخدمين.¹

1- ليلي بن برغوث، المرجع السابق، ص 452-455.

خلاصة الفصل:

تعد المصارف الرقمية أحد أهم الفاعلين في القطاع المالي، نظرا لدورها المحوري في تطوير الخدمات المصرفية، غير أن هذا التطور التكنولوجي جعل منها فضاءا لإرتكاب جرائم غسيل الأموال، ومنه تترتب مسؤولية تقع على عاتق المصارف الرقمية منها قانونية وتنظيمية، تتمثل في مراقبة العمليات المصرفية بتطبيق الأنظمة الحاكمة والرقابية، وحسن إستعمال التقنيات الرقمية الحديثة بما يضمن الكشف المبكر عن الأنشطة المرتبطة بشكل مباشر أو غير مباشر بجرائم غسل الأموال. ورغم أهمية هذه المسؤوليات إلا أن المصارف الرقمية تواجه جملة من التحديات التي قد تحد من فعالية جهودها في مكافحة غسيل الأموال، ومن أبرزها التهديدات الإجرامية الرقمية التي تستهدف أنظمة التحقق الرقمية وإستغلال البيانات الشخصية للعملاء، كما تبرز الفجوة الرقابية كأحد أهم الإشكاليات التي تعاني منها البيئة المصرفية الرقمية نتيجة التباين في الأطر التنظيمية والرقابية بين الدول، الأمر الذي يخلق ثغرات يمكن إستغلالها من قبل الشبكات الإجرامية.

الختامة

الخاتمة:

أصبحت المصارف الرقمية خطوة مهمة في تطوير القطاع المصرفي وتعزيز الشمول المالي، لما توفره من خدمات سريعة وفعالة تعتمد على التكنولوجيا الحديثة، غير أن طبيعتها الرقمية تثير تحديات قانونية وأمنية، خاصة فيما يتعلق بحماية البيانات ومراقبة المعاملات المالية ومكافحة غسل الأموال. ولمواجهة هذه التحديات، يتعين على جميع الدول تعزيز الأطر القانونية والرقابية المتحكمة في عمل هذه المؤسسات المالية الرقمية، وتطوير آليات التحقق من هوية العملاء وتتبع العمليات المشبوهة، مع دعم الأمن السيبراني والتعاون بين الجهات المختصة، وبذلك يمكن تحقيق التوازن بين الاستفادة من المزايا التي توفرها المصارف الرقمية وضمان حماية النظام المالي من مخاطر غسل الأموال والجرائم المالية الإلكترونية.

أولاً: النتائج:

خلصت دراستنا لموضوع المصارف الرقمية وتحدياتها القانونية في مكافحة جرائم غسل الأموال إلى استخلاص مجموعة من النتائج نذكر فيما يلي:

1- تجسد المصارف الرقمية أهم التحولات الرقمية التي شملت القطاع المصرفي والتي تعتمد على التكنولوجيا المتقدمة لتقديم خدمات مصرفية أكثر كفاءة وسرية مقارنة بالمصارف التقليدية بما يتناسب من الاحتياجات المتنامية للعملاء.

2- لقد قامت المصارف الرقمية باستغلال الوسائل الرقمية المستحدثة في تسهيل خدماتها المالية، إلا أنه في المقابل تم إستخدامها كسلاح لإرتكاب الجرائم المالية المنظمة، والتي من أبرزها جريمة غسل الأموال الإلكترونية.

3- تتجسد مسؤولية المصارف الرقمية في الحد من جرائم غسل الأموال في حماية البيانات الشخصية للعملاء ومراقبة العمليات المصرفية لإمكانية الكشف المبكر عن أي نشاط مشتببه به.

- تعترض المصارف الرقمية في مكافحة جريمة غسل الأموال جملة من الثغرات التي تعمل على خلق بيئة ملائمة تستغل من قبل الشبكات الإجرامية.

ثانياً: الاقتراحات:

من خلال النتائج المتوصل إليها، فإننا نقدم الاقتراحات التالية، والتي تتمثل في:

- 1- ضرورة مواكبة المصارف التقليدية للنظم الحديثة والمتقدمة مع الاعتماد على الخدمات المصرفية المبتكرة نظراً لما تقدمه هذه الأخيرة من تسهيلات وفوائد ربحية.
- 2- نشر التوعية وضرورة تكوين كفاءات في مجال مكافحة جرائم غسل الأموال التي تتم عبر الوسائط الإلكترونية للحد من انتشارها.
- 3- ضرورة تطوير الأنظمة الرقابة على مستوى المصارف الرقمية لتعزيز ثقة العملاء وتحقيق الإمتثال.
- 4- ضرورة تعزيز الجهود الدولية وتوحيد المعايير الرقابية لتحقيق الإنسجام الدولي في مكافحة جرائم غسل الأموال.

قائمة المصادر والمراجع

1- قائمة المصادر:

أ: النصوص القانونية:

1. الأمر رقم 03-11، المؤرخ في 26 غشت 2003، يتعلق بالنقد والقرض، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 52، الصادرة 27 أوت 2003
2. الأمر رقم 05-06، المؤرخ في 23 غشت 2005، يتعلق بمكافحة التهريب، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 59، الصادرة في 28 غشت 2005
3. القانون رقم 05-01، المؤرخ في 6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج ر، العدد 11، الصادرة في 9 فبراير 2005.
4. القانون رقم 05-02، المؤرخ في 6 فيفري 2005، المعدل والمتمم للأمر رقم 75-59 المتضمن القانون التجاري الجزائري، ج ر ج ج، العدد 11، سنة 2005.
5. القانون رقم 08-09، المؤرخ في 25 فبراير 2008، يتضمن قانون الإجراءات المدنية والإدارية، ج ر ج ج، العدد 21.
6. القانون رقم 04/15 المؤرخ في 11 ربيع الثاني 1436 هـ الموافق لاول فبراير سنة 2015، يحدد القانون المتعلق بالتوقيع والتصديق الإلكتروني، ج ر، ج، ج، عدد 06.
7. القانون رقم 07/18 المؤرخ في 10 جوان سنة 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد 34.
8. القانون رقم 23-09، المؤرخ في 21 يونيو 2023، المتضمن القانون النقدي والمصرفي، ج ر ج ج، العدد 43، الصادرة في 27 يونيو 2023.
9. القانون رقم 24-06، المؤرخ في 28 أبريل 2024، المتضمن قانون العقوبات، ج ر ج ج، العدد 30، الصادرة في 30 أبريل 2024.

ب/ النصوص التنظيمية:

1. المرسوم التنفيذي رقم 02-127، المؤرخ في 7 أبريل 2002، يتضمن إنشاء خلية معالجة الإستعلام المالي وتنظيمها وعملها، ج ر ج ج، عدد 23، الصادرة في 7 أبريل 2002.
2. المرسوم رقم 06-05، المؤرخ في 9 يناير 2006، يتضمن شكل الإخطار بالشبهة ونموذجه ومحتواه ووصل إستلامه، ج ر ج ج، العدد 2، الصادرة في 15 يناير 2006.
3. النظام رقم 08-03، المؤرخ في 21 يوليو 2008، المتضمن تحديد شروط الترخيص بإقامة تعاونيات الإدخار والفرص وإعتمادها، ج ر ج ج، عدد 15.
4. النظام رقم 24-01، المؤرخ في 6 فبراير 2024، يتضمن تحديد شروط الترخيص بتأسيس بنك ومؤسسة مالية وإعتمادها، ج ر ج ج، عدد 18، صادرة في 13 مارس 2024.
5. النظام رقم 24-02، المؤرخ في 6 فبراير 2024، المتعلق بالحد الأدنى لرأس المال البنوك والمؤسسات المالية العاملة في الجزائر، ج ر ج ج، عدد 18.
6. النظام رقم 24-04، المؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي، ج ر ج ج، العدد 77، صادرة في 19 نوفمبر 2024.
7. النظام رقم 25-01 المؤرخ في 12 مارس 2025، يتضمن تحديد شروط إعتماد مسيري المؤسسات الخاضعة، ج ر ج ج، العدد 23، الصادرة في 22 أبريل 2025.
8. مرسوم بقانون إتحادي رقم 34، المؤرخ في 20 سبتمبر 2021، المتضمن مكافحة الشائعات والجرائم الإلكترونية، ج ر، عدد 712.

ج/ القرارات والتعليمات الصادرة عن البنك

1. التعليم رقم 25-02، المؤرخة في 2 مارس 2025، المتعلقة بالشروط الخاصة بالترخيص بتأسيس وإعتماد وممارسة نشاط البنك الرقمي
2. قرار البنك المركزي السعودي لسنة 2020، بشأن الإرشادات والمعايير الإضافية لطلب منح الترخيص للبنوك الرقمية في المملكة السعودية.
3. قرار بنك الكويت المركزي لسنة 2022، بإصداره دليل متطلبات تأسيس البنوك الرقمية في دولة الكويت.

د /القوانين الأجنبية:

1. القانون رقم 80 لسنة 2002، المؤرخ في 22 مايو سنة 2002، يتضمن قانون مكافحة غسل الأموال، ج ر، العدد 20، الصادر في 22 مايو 2002.
2. القانون رقم 106 لسنة 2013، المؤرخ في 8 مايو 2013، المتعلق بمكافحة غسل الأموال وتمويل الإرهاب، ج ر، العدد 1137، الصادر 2 يونيو 2013.
3. القانون رقم 175 لسنة 2018، بشأن مكافحة جرائم تقنية المعلومات، ج ر، العدد 32، الصادرة 14 أغسطس 2008.
4. القانون رقم 194، المؤرخ في 15 سبتمبر 2020 المتضمن البنك المركزي والجهاز المصرفي، ج ر، العدد 37.
5. القانون رقم 5 لسنة 2022 المؤرخ في 8 فيفري 2022 المتضمن تنظيم وتنمية استخدام التكنولوجيا المالية ج ر العدد 5 الصادر في 8 فبراير 2022.

ثانياً: الكتب

1. بصله، رياض فتح الله، جرائم بطاقات الائتمان، دار الشروق، الطبعة الأولى، بيروت لبنان، 1995.
2. ثويني، فلاح حسين، المصارف الرقمية والوصول السهل الى التمويل قراءة في توسيع التمويل وقاعدة الزبائن المصرفيين من خلال المصارف، الطبعة الأولى، مركز البيان لدراسة والتخطيط ببغداد، سبتمبر 2024.
3. حجازي، عبد الفتاح بيومي، الدليل الجزائي والتزوير الجرائم الكمبيوتر والانترنت، دار الكتب القانونية دون طبعة، مصر، 2000.
4. شبير، محمد عثمان، المعاملات المالية المعاصرة في الفقه الإسلامي، الطبعة السادسة، دار النفائس، الأردن، 1427هـ 2007م.
5. فوضيل، نادية، شركات الأموال في القانون الجزائري، الطبعة الثالثة، ديوان المطبوعات الجامعية، الجزائر، 2008.

ثالثاً: المقالات

1. آيت بن أعمار، غنية، دور مجموعة العمل المالي في نطاق مواجهة جرمي تبويض الأموال وتمويل الإرهاب، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس مستغانم، الجزائر، المجلد 6، العدد 2، جوان 2021.
2. بدراني، أحمد - فروحات، سعيد، أحكام الإخطار بالشبهة المالية لمكافحة جريمة تبويض الأموال في التشريع الجزائري، مجلة الواحات البحوث والدراسات، جامعة غرداية، المجلد 14، العدد 1، نوفمبر 2020.

3. بلعور، خالد - منصوري، عبد الكريم، تأثير المخاطر البنكية على رأس المال في البنوك دراسة حالة مجموعة من البنوك العربية، مجلة المنهل الإقتصادي، جامعة الشهيد حمه لخضر الوادي، الجزائر المجلد 07، العدد 01، جوان 2024.
4. بن برغوث، ليلي، الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات، التحديات، والاليات التصدي، المجلة الدولية للاتصال الاجتماعي، جامعة عبد الحميد بن باديس مستغانم، الجزائر، المجلد 10، عدد 1، 2023.
5. بن تقي، سفيان، جريمة غسيل الأموال بين الوسائط الإلكترونية والمنصوص التجريبية، مجلة الأبحاث القانونية والسياسية، جامعة سطيف 2، الجزائر، المجلد 03، العدد 02، أفريل 2021.
6. بن علي، سمية، مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي باستخدام تطبيق الأمن السيبراني بنك daske الدغاركي النموذجي، مجلة أبعاد إقتصادية، جامعة محمد بوقرة، بومرداس، الجزائر، المجلد 03، العدد 02، 2023.
7. بن قايد علي، محمد الامين، الشيك الالكتروني امتداد وتطور الشيك التقليدي، مجلة بحوث في القانون والتنمية، جامعة أحمد بوقرة، بومرداس، الجزائر، المجلد 2، العدد 2، ديسمبر 2022.
8. بوالمرقة، رميساء - شويطر، رتيبة إيمان، الطوابط القانونية لإنشاء البنوك الرقمية في الجزائر، مجلة البحوث في العقود وقانون الأعمال، جامعة الإخوة منتوري قسنطينة 1، الجزائر، المجلد 10، العدد 01، جوان 2025.
9. بوحنيك، هدى، أثر تبني البنوك لتقنيات الذكاء الاصطناعي دراسة حالة بنك، مجلة للدراسات والبحوث الإنسانية، جامعة العربي التبسي تبسة، الجزائر المجلد 08، العدد 04، جانفي 2024.

10. بوزانة، أيمن - حمدوش، وفاء، منصات التكنولوجيا المالية كآلية لتعزيز الخدمات المصرفية المفتوحة واجهة برمجة التطبيقات ApLs نموذجاً، مجلة المدبر، المدرسة العليا للتسيير والإقتصاد الرقمي القليعة، الجزائر، المجلد 9، عدد خاص، أكتوبر 2022.
11. بوعتلي، محمد - ليلية، سامي، واقع المنصات الرقمية وتأثيرها على التنمية المستدامة في الجزائر دراسة ميدانية وقياسية، مجلة المدبر، المدرسة العليا للتسيير والإقتصاد الرقمي القليعة، الجزائر، المجلد 9، عدد خاص، أكتوبر 2022.
12. بوقرين، عبد الحليم - بوناصر، إيمان، تزوير شهادة التصديق الإلكتروني بين جمود النصوص وتطور التقنية، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، الجزائر، المجلد 3، العدد 2، 2019.
13. بولحية، سهيرة - سويح، دنيا زاد، الإحتيال الإلكتروني، مجلة الدراسات القانونية والإقتصادية، جامعة باتنة، الجزائر، المجلد 2، عدد 2، 2019.
14. تهامي، محمد رضا - سعيدي، يحي، دور البنوك في عملية غسيل الأموال بين مبدأ السرية المصرفية ومبدأ اعرف عميلك، مجلة الباحث الاقتصادي، جامعة برج بوعرييج، الجزائر، المجلد 5، العدد 1، سبتمبر 2018.
15. تومي، مريم - صدراقي، وفاء، تزوير بطاقات الائتمان صورة خاصة في جريمة التزوير الإلكتروني، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، الجزائر، المجلد 5، العدد 02، 2021.
16. جريش، ساره واخرون، المواجهة الجنائية للقرصنة الرقمية للبطاقات المصرفية وسبل الوقاية منها بالتشريع المغربي، المجلة العربية الألمانية للعلوم الشرعية والقانونية، المجلد 3، العدد 1، ألمانيا، 2024.

17. حباش، جمال، صلاحيات خلية معالجة الإستعلام المالي في مواجهة تبييض الأموال، مجلة الإدارة والتنمية للبحوث والدراسات، جامعة البليدة 2، المجلد 10، العدد 2، ديسمبر 2021.
18. حشروف، فاطمة الزهراء - صديقي، وحيدة، الأمن السيبراني في البنوك الجزائرية التحديات والاستراتيجيات، مجلة الدفاتر الاقتصادية، جامعة زيان عاشور الجلفة، الجزائر، مجلد 16، عدد 01، 2025.
19. حميل، عبد الحق - مسيردي، سيد أحمد، مظاهر إستقلال خلية معالجة الإستعلام المالي قراءة في المرسوم التنفيذي رقم 22-36، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي الأغواط، الجزائر، المجلد 7، العدد 01، ماي 2023.
20. حميش، محمد، معوقات مكافحة جرمي تبييض الأموال وتمويل الإرهاب، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس مستغانم، الجزائر، المجلد 5، العدد 2، ديسمبر 2020.
21. حوالف، عبد الصمد، شركة المساهمة بين النظامية والتعاقدية، مجلة القانون والعلوم السياسية، جامعة النعامة، الجزائر، المجلد 09، العدد 01، أفريل 2023.
22. خرباش، جميلة، الشيك الإلكتروني أداة وفاء عن بعد في التجارة الإلكترونية، مجلة البيان للدراسات القانونية والسياسية، جامعة برج بوعرييج، الجزائر، المجلد 3 العدد 1، جوان 2018.
23. خطاي، فارس - مباركي، دليلة، تزوير التوقيع الإلكتروني في البطاقات الائتمان دراسة على ضوء القانون 04 / 15 المتعلق بالتوقيع والتصديق الإلكتروني، المجلة الجزائرية للأمن الإنساني، جامعة الحاج لخضر 1 باتنة، الجزائر، مجلد 5، عدد 2، 2020.

24. خليفة، آسيا، أساليب الرقابة البنكية الإحترازية خلال فترة 2014-2018، مجلة استراتيجيات التحقيقات الإقتصادية والمالية، جامعة تيبازة، الجزائر، مجلد 3، عدد 2، 2021.
25. دريد، حنان - غريب، طاوس، الصيرفة الرقمية كتوجه حديث لبنوك الجزائرية دراسة إحصائية، المجلة العلمية المستقبل الاقتصادي، جامعة محمد بوقرة بومرداس، الجزائر، للمجلد 10، العدد 1، جوان 2022.
26. دغبوج، تقي الدين، النظام القانوني لتأسيس البنوك الرقمية في الجزائر، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة الشيخ العربي التبسي، تبسة، المجلد 10، العدد 02، ماي 2025.
27. ديدوش، هاجر - حريري، عبد الغني، واقع الخدمات المصرفية الإلكترونية بالبنوك الجزائرية، مجلة إستراتيجية للتحقيقات الاقتصادية، جامعة تيبازة، الجزائر، مجلد 4، عدد 1، 2022.
28. رحمان، ايمان - لعطار، زين العابدين، حماية البيانات الشخصية في العصر الرقمي، مجلة طلبة للدراسات العلمية الأكاديمية المركز الجامعي سي الحواس بركة، الجزائر، مجلد 8 العدد 2، 2025.
29. الزلمي، باسم أحمد - السراج، عبود، دور النقود الإلكترونية في عمليات غسل الأموال، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، جامعة دمشق، المجلد 26، العدد الأول، 2010.
30. زيتوني، هند - بوعاية، ذهبية ريمة، حلول الهوية الرقمية في معرفة العميل ودورها في تعزيز الشمول المالي، مجله التمويل والإستثمار والتنمية المستدامة، جامعة فرحات عباس بسطيف 1، الجزائر المجلد 08، العدد 01، جوان 2023.

31. زيدان، سميرة - عصماني، سفيان، دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية دراسة حالة بنك بنكسي الجزائر، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، جامعة محمد بوضياف المسيلة، المجلد 17، العدد 02، ديسمبر 2024.
32. سداوي، نورة، تطبيقات الذكاء الاصطناعي في المصارف العربية تجربة الإمارات العربية المتحدة، مجلة إضافات اقتصادية، جامعة غرداية، الجزائر، المجلد 08، العدد 01، 2023.
33. سعيدي، عزو، الأمن التقني الدفع الإلكتروني أي فعالية، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي بتندوف، العدد الثاني، ديسمبر 2017.
34. سعيود، محمد الطاهر، إجراءات تأسيس البنك الرقمي في التشريع الجزائري، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد 18، العدد 1، مارس 2026.
35. سلطاني، حميد، البنوك الرقمية شروط الترخيص بإنشائها واعتمادها في ظل القانون رقم 09./23، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي بالشلف، الجزائر، المجلد 11، العدد 1، جوان 2025.
36. شريف، هنية، الأساليب الحديثة للإجرام المنظم تبيض الأموال نموذجاً، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجزائر، المجلد 12، العدد 2، سبتمبر 2019.
37. شوشان، فادي، التحول الرقمي وآثاره في تعزيز الكفاءة والشفافية في إدارة المالية العامة، المجلة الجزائرية للمالية العامة، جامعة أبو بكر بلقايد تلمسان، الجزائر، المجلد 15، عدد 1، 2025.
38. صايم، مصطفى - بوفناديل، محمد، مساهمة الإدارة الإلكترونية في تطوير أساليب العمل المصرفي إشارة الخدمات الإلكترونية التي يقدمها البنك الوطني الجزائري BNA، مجلة إضافات اقتصادية، جامعة غرداية، المجلد 3، العدد 2، أكتوبر 2019.

39. طباعة، نجاة، عن أزمة ضعف الرقابة في تفعيل الإدارة الرشيدة للبنوك العمومية، مجلة الدراسات حول فعالية القاعدة القانونية، جامعة عبد الرحمن ميرة بجاية، الجزائر، المجلد 8، العدد 1، 2024.
40. طبائية، رمزي، الهوية الرقمية المصرفية كتوجه حديثي تحسين الخدمات المصرفية الإلكترونية نظام Aadhaar الهندي نموذجا، المجلة الجزائرية للعلوم الاجتماعية الإنسانية، جامعة الجزائر 3، الجزائر، المجلد 11، العدد 02، نوفمبر 2023.
41. العايب، سناء، تسيير المخاطر السيبرانية في القطاع المالي من المنظور الدولي، مجلة الدراسات المالية والمحاسبية والإدارية، جامعة العربي بن مهيدي أم البواقي، الجزائر، المجلد 8، العدد 3، ديسمبر 2021.
42. عبد الرحيم، نادية - بن سعيد، أمين، جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية، مجلة الدراسات الاقتصادية والمالية، جامعة الشهيد حمه لخضر الوادي، الجزائر، العدد 10، الجزء 2، 2017.
43. عبد العال، أحمد محمد محروس، التزوير الإلكتروني بين التشريع التقليدي وآليات المواجهة الحديثة، المجلة الأكاديمية للأبحاث والنشر العلمي، جامعة طنطا، مصر، المجلد 6، العدد 02، 2025.
44. عبد الكافي، مريم - بوربابة، صورية، جريمة الإحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية، مجلة القانون والعلوم السياسية، جامعة النعامة الجزائر، المجلد 8، العدد 1، أبريل 2022.
45. عوسات، تكليت، تقنيه البلوك تشين دراسه في المفهوم، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 7، العدد 2، جوان 2022.

46. **فراقي، أمينة سماعين**، الأحكام الخاصة بجرائم القانون النقدي والمصرفي رقم 23/ 09 على ضوء التوجيهات الحديثة للسياسات الجنائية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، الاغواط، الجزائر، مجلد 8، عدد 1، 2024.
47. **قعموسي، هواري**، تجريم العملات الافتراضية الرقمية بقانون تبييض الأموال 10/25 بالجزائر، المجلة الجزائرية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، المجلد 10 العدد 02، ديسمبر 2025.
48. **كباهم، سامي**، خصوصية شروط ممارسة نشاط البنك الرقمي دراسة في القانون الجزائري، مجلة الدراسات القانونية والإقتصادية، المركز الجامعي بريك، الجزائر، المجلد 08، العدد 02، نوفمبر 2025.
49. **كردي، نبيلة**، الشيك الالكتروني، مجلة العلوم الاجتماعية والسياسية، جامعة العربي التبسي، الجزائر، المجلد 10، العدد 2، جوان 2017.
50. **لبزة، هشام - ضيف الله، محمد الهادي**، واقع وتحديات وسائل الدفع الإلكترونية في الجزائر، مجلة الدراسات والبحوث الاجتماعية، جامعة الشهيد حمه لخضر الوادي، الجزائر، العدد 24، ديسمبر 2017.
51. **لعجال، ذهبية - سي يوسف، قاسي**، الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي، مجلة الإجتهد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد 13، العدد 1، جانفي 2021.
52. **لعور، عبد الله - كبوط، عبد الرزاق**، العلاقة بين النقود الإلكترونية، العملات الرقمية، العملات الافتراضية، والعملات المشفرة البحث في المفهوم، مجلة الاقتصاد الصناعي خراتك، جامعة الحاج لخضر 1 باتنة، الجزائر، المجلد 11، العدد 02، 2021.
53. **ماينو، جيلالي**، الاستخدام الإجرامي للعملات المشفرة، مجلة القانون والعلوم السياسية، جامعة النعامة، الجزائر، المجلد 06، العدد 10، أوت 2020.

54. مجدوب، حشيفة، تبييض الأموال عبر أساليب الوفاء الإلكترونية، مجلة القانون والعلوم السياسية، جامعة النعامة، المجلد 8، العدد 2، ماي 2022.
55. مرزوق، آمل، البتكوين نقود جديدة أم فعالية مالية؟، مجلة شعاع للدراسات الاقتصادية، جامعة تلمسان، الجزائر، المجلد 03، العدد 2، سبتمبر 2019.
56. مرزوق، فاتح - عطاء الله، ياسين، الخدمات المصرفية الرقمية ودورها في تسهيل التجارة الخارجية دراسة حالة بنك الجزائر الخارجي BEA، مجلة الجغرافيا الاقتصادية، المركز الجامعي مرسلبي عبد الله تيبازة، الجزائر، المجلد 2، العدد 1، جانفي 2025.
57. مزاجة، تواتية، العملات الرقمية في الجزائر بين الموقف الاحترازي والتحول الرقمي، مجلة المنتدى الدراسات والأبحاث الاقتصادية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد 09، العدد 02، أكتوبر 2025.
58. مشراوي، حدة - بالعبيدي، عايدة عبير، دور الهوية الرقمية المصرفية في رفع مستويات الشمول دراسة حالة بعض الدول العربية، مجلة الأقتصاد المالية البنكية إدارة الأعمال، جامعة محمد خيضر بسكرة، الجزائر، المجلد 12، العدد 01، أبريل 2023.
59. مطاي، عبد القادر - بن شنيعة، كريمة - صلاح، محمد، وسائل الدفع الإلكترونية ودورها في عصرنة المنظومة المصرفية الجزائرية، مجلة الإقتصاد الحديث والتنمية المستدامة، جامعة تيسمسيلت، المجلد 2، العدد 2، جوان 2020.
60. مهاوات، عبد القادر - حميدي، محمد طه، النقود المشفرة في الفقه الإسلامي، مجلة المدونة، مجمع الفقه الإسلامي بالهند، المجلد 7، العدد 26-27، أكتوبر 2010.
61. الميل، عبد العزيز منصور، جريمة غسيل الأموال عبر الفضاء الإلكتروني دراسة تشريعية مقارنة، مجلة البحوث القانونية والاقتصادية، العدد 93، سبتمبر 2020.
62. نوري، ابتسام - نهار، خالد بن الوليد، المنصات الرقمية كآلية تسويقية للخدمات المالية المصرفية دراسة حالة منصة LENPO الرقمية للتمويل الإسلامي في المملكة العربية

- السعودية، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، جامعة المسيلة، المجلد 18، العدد 02، ديسمبر 2025.
63. نوري، جهاد - رحمني، رحيمة شتوح، تطبيقات تقنية البلوك تشين، مجلة القانون والعلوم الاجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 7، العدد 2، سنة 2022.
64. هراكي، حياة، واقع جريمة الإحتيال إلكتروني في التجارة الإلكترونية، مجلة التغيير الاجتماعي، جامعة بسكرة الجزائر، المجلد 8، العدد 2، 2023.
65. الهاني، محمد طايح، جريمة غسل الأموال عبر الأنترنت في التشريع المصري والإماراتي، مجلة الدراسات القانونية، جامعة أسيوط، مصر، العدد 66، الجزء 02، ديسمبر 2024.
66. يحياوي، محمد، مخاطر القرصنة المعلوماتية على الحكومة الإلكترونية، مجلة البحوث والدراسات العلمية، جامعة يحي فارس المدية، الجزائر، العدد 5، يوليو 2011.

رابعاً: الرسائل والمذكرات:

أ/رسائل الدكتوراه:

1. بلعباس، نوال، بطاقة الإئتمان كوسيلة من وسائل الدفع الحديثة، أطروحة دكتوراه علوم في القانون، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر 1، 2016-2017.
2. صواق، عبد القادر، مساهمة الأمر السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية، أطروحة دكتوراه، تخصص تسويق الخدمات، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة غرداية الجزائر، نوقشت في 26 سبتمبر 2024.
3. فراحتية، كمال، التعاون الدولي ودور البنوك في مكافحة جريمة تبييض الأموال، أطروحة دكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، نوقشت في 26 سبتمبر 2017.

ب/مذكرات الماجستير:

1. جدي، نسيم، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة ماجستير، تخصص قانون جنائي، كلية الحقوق، جامعة وهران، الجزائر، 2013-2014.
2. الفليح، عاصم محمد طه، التنظيم القانوني للبنوك الرقمية في الأردن دراسة مقارنة، رسالة ماجستير، تخصص قانون خاص، جامعة الشرق الاوسط، الأردن، كانون الثاني 2025.

ج/مذكرات الماستر:

1. بروان، خالد، جرائم الإعتداء على التوقيع الإلكتروني، مذكرة ماستر في الحقوق، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، 2019-2020.
2. بودواب، سمير - لبيديوي، فؤاد، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة 20 ماي 1955 سكيكدة، جوان 2024.
3. بولالي، محمد - عطيط، زين الدين، النظام القانوني للبنك الرقمي في التشريع الجزائري، مذكرة ماستر في القانون، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي جيجل، الجزائر، 2024-2025.
4. خلاف، محمد أمين - كافي، إسماعيل أسامة، البنوك الإلكترونية، مذكرة ماستر، تخصص قانون شركات، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2017-2018.
5. الساييس، إبتسام - نيلي، صفاء، وسائل الدفع في التجارة الإلكترونية، مذكرة ماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2019-2020.

6. صلجة، خلود - شيل، مروة، جريمة الإحتيال الإلكتروني في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 سكيكدة، الجزائر 2024-2025.
7. قريول، عبد الرحيم - عزوزي، عبد القادر، النظام القانوني للرخص الإدارية في التشريع الجزائري، مذكرة ماستر في الحقوق، تخصص الدولة والمؤسسة، كلية الحقوق والعلوم السياسية، جامعة زياني عاشور، الجلفة، 2020-2021.
8. كبابي، صافية - تيخرباتين، مريم، النظام القانوني المعاملات البنكية الإلكترونية، مذكرة ماستر في الحقوق، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج البويرة، 2020-2021.
9. كرفاح، بختة، غسيل الأموال عبر الوسائط الإلكترونية، مذكرة ماستر في الحقوق، تخصص القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، جوان 2022.
10. مولاي علي، العربي - عاشي، هاجر، أثر النقود الإلكترونية على غسيل الأموال، مذكرة مقدمة لنيل شهادة الماستر، تخصص إدارة مالية، جامعة ابن خلدون تيارت، الجزائر، 2018-2019.

خامسا / المداخلات العلمية:

1. كحل الراس، سماح - شوايدية، منية، دور البنوك الالكترونية في تنشيط السوق المالي، الملتقى الوطني عن بعد الصيرفة الالكترونية والتنمية الإقتصادية، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، 3 جوان 2021.

سادساً: التقارير والدراسات

- مجموعة العمل المالي، المعايير الدولية لمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسليح، باريس، فرنسا، 12.2.2003.
- مذكرة توضيحية بخصوص الدول عالية المخاطر والدول محل المتابعة المتزايدة، صادرة عن اللجنة التونسية لتحاليل المالية، تونس، 25 ماي 2025.

سابعاً: المطبوعات الجامعية:

1. براني، عبد الناصر، محاضرات في مقياس المصارف الإسلامية، جامعة عبد القادر قسنطينة، الجزائر.

ثامناً: المواقع الإلكترونية

- دينا يوسف، الرموز المؤقتة OTP في القطاع المصرفي كيف يتم إرسالها ولماذا هي مهمة، 14 مارس 2024، متاح على الرابط: <https://www.authentica.sa/ar>، أطلع عليه بتاريخ 23 ماي 2026.
- منصة الخدمات المصرفية الرقمية NETinfo-DiGital Banking Platform، متاح على الرابط: <https://netinfo.eu>، أطلع عليه بتاريخ 23 ماي 2026.

2-المراجع باللغة الأجنبية

- Mohammed BEN Moussa, ApI AppLication programming Interface : Apromising Future For Financial Institutions CInternational Experience, Revue Des sciences commerciales, vol 18, N°2, Décembre 2019.

فهرس المحتويات

الصفحة	العنوان
	الشكر
	الاهداء
	قائمة المختصرات
11-9	مقدمة
13	الفصل الأول: الإطار المفاهيمي للمصارف الرقمية ومخاطر غسل الاموال
14	المبحث الأول: ماهية المصارف الرقمية
15-14	المطلب الأول: مفهوم المصارف الرقمية
15	الفرع الأول: تعريف المصارف لرقمية وخصائصها
18-15	أولاً: تعريف المصارف الرقمية
20-18	ثانياً: خصائص المصارف الرقمية
20	الفرع الثاني: التمييز بين المصارف الرقمية والبنوك التقليدية
20	أولاً: من حيث النشأة
21	ثانياً: من حيث الهيكل التنظيمي
21	ثالثاً: من حيث طبيعة المعاملات
22	رابعاً: من حيث التكاليف والتسيير
22	خامساً: من حيث الخدمات المقدمة
22	المطلب الثاني: اعتماد المصارف الرقمية
23	الفرع الأول: الشروط المطلوبة لانشاء المصارف الرقمية
27-23	أولاً: شروط التأسيس المتعلقة بالشخص المعنوي المصرف الرقمي
29-27	ثانياً: شروط التأسيس المتعلقة بالاشخاص الطبيعيين
29	الفرع الثاني: اجراءات منح الاعتماد للمصارف الرقمية
34-29	أولاً: الترخيص

فهرس المحتويات

38-35	ثانيا: طلب الاعتماد.
38	المبحث الثاني: تطور جرائم غسل الأموال في عصر البيئة الرقمية
39-38	المطلب الأول: مفهوم غسل الأموال الإلكتروني
39	الفرع الأول: تعريف غسل الاموال الإلكتروني
40	أولا: التعريف التشريعي لغسل الأموال الإلكتروني
42-41	ثانيا: التعريف الفقهي لغسل الأموال الإلكتروني
44-42	الفرع الثاني: نشأة وتطور غسل الأموال الإلكتروني
45-44	المطلب الثاني: الأدوات الحديثة المستخدمة في ارتكاب جريمة غسل الأموال
45	الفرع الأول: العملات المشفرة
46-45	أولا: تعريف العملات المشفرة:
46	ثانيا: خصائص العملات المشفرة
47	ثالثا: أنواع العملات المشفرة:
49-47	رابعا: العملة المشفرة كأداة لإرتكاب الجرائم
49	الفرع الثاني: الشيكات الإلكترونية وبطاقات الائتمان:
52-49	أولا: الشيك الإلكتروني:
56-52	ثانيا: بطاقة الائتمان الإلكترونية:
59	الفصل الثاني: التزام المصارف الرقمية بمكافحة غسل الأموال بين المسؤولية القانونية والفجوات العملية
60	المبحث الأول: المسؤولية القانونية للمصارف الرقمية في مكافحة غسيل الأموال.
60	المطلب الاول: المسؤولية عن تطبيق أنظمة الحاكمة والرقابة
61	الفرع الأول: التحقق من هوية العملاء ومن مصادر الأموال:

فهرس المحتويات

62-61	أولاً: مفهوم الهوية الرقمية المصرفية:
65-62	ثانياً: آليات الكشف عن هوية العملاء ومصادر الأموال
66	الفرع الثاني: الإبلاغ عن الأنشطة المشبوهة
68-66	أولاً: تعريف الإبلاغ عن الأنشطة المشبوهة
70-68	ثانياً: مؤشرات الإشتباه
73-71	ثالثاً: الجهة المكلفة بتلقي الإبلاغ عن الأنشطة المشبوهة:
74-73	المطلب الثاني: المسؤولية عن حسن إستعمال التقنيات الرقمية الحديثة:
74	الفرع الأول: تطوير الوسائل والأدوات التقنية لكشف محاولات الإحتيال:
75-74	أولاً: تعريف الإحتيال في المصارف الرقمية:
80-76	ثانياً: مسؤولية المصارف الرقمية في تحديث أساليب الكشف عن الإحتيال
81-80	الفرع الثاني: تطوير المنصات الرقمية لتحقيق الدقة والفعالية في التحقق والإمتثال
82-81	أولاً: تعريف المنصات الرقمية
84-82	ثانياً: دور المنصات الرقمية في القطاع المصرفي
86-84	ثالثاً: الإنتقال نحو المنصات الرقمية الحديثة كآلية لتطوير الخدمات المصرفية:
87	المبحث الثاني: الفجوات والثغرات التي تهدد مهام المصارف الرقمية في مكافحة غسيل الأموال
87	المطلب الأول: التهديدات الإجرامية الرقمية .
88	الفرع الأول: المساس بأنظمة التحقق
91-88	أولاً: تعريف المساس بأنظمة التحقق
93-91	ثانياً: صور المساس بأنظمة التحقق

فهرس المحتويات

95-93	ثالثا: الآليات المستعملة في المساس بأنظمة التحقق
95	الفرع الثاني: الوثائق المزورة الإلكترونية
97-96	أولا: مفهوم الوثائق المزورة إلكترونيا
100-97	ثانيا: أنواع وثائق التزوير في المصارف الرقمية
100	المطلب الثاني: الفجوات الرقابية
100	الفرع الأول: الإعتماد على مزودي خدمات رقمية دون الحصول على تراخيص
101	أولا: مفهوم مزودي الخدمات المصرفية
104-101	ثانيا: العلاقة بين مزودي الخدمات دون تراخيص وجريمة غسل الأموال
104	الفرع الثاني: تباين أنظمة الرقابة على المستوى العالمي
105	أولا: تباين التشريعات المتعلقة بمكافحة جريمة غسل الأموال
106-105	ثانيا: غياب التوافق الدولي في مجال مكافحة جرائم غسل الأموال
107-106	ثالثا: ضعف التعاون الدولي بسبب عقبة السرية المصرفية
107	رابعا: ضعف أجهزة الرقابة ووجود إشكاليات قانونية بداخلها
108-107	الفرع الثالث: غياب آليات أمنية لتبادل البيانات الشخصية
109-108	أولا: مفهوم البيانات الشخصية:
111-109	ثانيا: أثر غياب الآليات الآمنة على زيادة مخاطر القرصنة الإلكترونية
112-111	ثالثا: سبل تعزيز أمن البيانات الشخصية.
115-114	الخاتمة
132-117	قائمة المصادر والمراجع
	الملخص

ملخص:

تعد المصارف الرقمية نتاجا للتغيرات المالية والمصرفية التي شهدتها القطاع المصرفي، والتي أصبحت تحظى باهتمام كبير في الآونة الأخيرة، نظرا لما توفره من مزايا وتسهيلات التي تقدمها عبر الوسائل الحديثة في تقديم خدماتها المصرفية، إلا أنها ساهمت وبشكل غير مباشر في تطوير جرائم غسيل الأموال التي إتخذت منها فضاء إجراميا.

ومنه سعت المصارف الرقمية إلى الحد من إنتشار جرائم غسيل الأموال ومكافحتها، من خلال وضع إجراءات تكمن في تطبيقات الأنظمة الحاكمة والرقابية و سعيها منها لتطوير منصات الرقمية، إلا أنها واجهتها العديد من الفجوات التي ساهمت في خلق بيئة ملائمة تستغل في إرتكاب الجرائم المالية المنظمة.

الكلمات المفتاحية: المصارف الرقمية، غسيل الأموال الإلكتروني، الأنظمة الرقابية والحاكمة، الفجوات.

Abstract:

Digital banks are a product of the financial and banking changes witnessed by the banking sector, which have become of great interest recently, due to the advantages and facilities they provide through modern means in providing their banking services, but they have indirectly contributed to the development of money laundering crimes, which have taken a criminal space.

Digital banks have sought to reduce the spread of money laundering crimes and combat them by establishing procedures based on the applications of governing and regulatory systems and in an effort to develop their digital platforms, but they have faced many gaps that contributed to creating a favorable environment to be exploited in the commission of organized financial: crimes.

Key words : Digital banking، Electronic money laundering، Regulatory and governing systems،Gaps