

أثر تكنولوجيا الاعلام والاتصال على جريمة تبييض الأموال *The impact of ICT on the money laundering crime*



بعجي عبد النور^{*}،

كلية الحقوق جامعة الجزائر-1، (الجزائر)

تاريخ الاستلام: 2022/03/24 تاريخ القبول للنشر: 2022/05/18 تاريخ النشر: 2022/06/30



ملخص:

تعد التكنولوجيا أداة هامة في حياة الفرد التي تضمن تبادل المعلومات عبر مختلف وسائل الاتصال، وامتدت ثورة التكنولوجيا الى مجال القطاع المالي لتركز المعاملات المالية على الفضاء السيبراني، وفي ظل هذه التطورات التي تغذيها العولمة المالية ظهر نوع جديد من المجرمين يسعون لارتكاب الجرائم المالية عبر ما توفره التكنولوجيا من فرص سهلة وعديدة عن ما هو موجود في العالم الواقعي، لتأخذ جريمة تبييض الأموال التقليدية شكل جديد من خلال استخدام الوسائط الالكترونية، إن الهدف الرئيسي من هذه الورقة هو دراسة جريمة تبييض الأموال السيبراني، ومعرفة أساليب ارتكابها لمواجهة هذا الإجرام والحد منه.

الكلمات المفتاحية: العولمة، تبييض الأموال السيبراني، أنظمة الدفع الإلكتروني، الوسائل الالكترونية، الجريمة المالية الإلكترونية.

Abstract:

The technology is an important tool in the individual's life, its ensures the exchange of information through various ways of communications and information systems, as a result the financial sector based on cyber financial transactions, these developments fueled by financial globalization, there is a new kind of criminal commit a financial crimes through the easy opportunities offered, it has emerged from what exists in the real world.

The main objective of this paper is to study the crime of cyber-laundering as a modern crime at the stage of development, as well as an assessment of the methods of its commission, also proposing adequate solutions to counter and reduce this crime.

Keywords: globalization; cyber-laundering; electronic payment systems; electronic means; electronic financial crime.

مقدمة:

لقد شهد العالم تطور في استعمال تكنولوجيا المعلومات والاتصالات، وأدى إدخال الوسائل التكنولوجية في بيئة الأعمال التجارية إلى تحسين كبير في العمليات التجارية، هذا الاستخدام المتزايد لأجهزة الابتكار التكنولوجي مثل الحواسيب والهواتف النقالة والإنترنت وغيرها أسفر عن نتائج إيجابية وسلبية على حد سواء، فمن الناحية الإيجابية، ساهم في تطوير القطاع المالي الذي أصبح يقدم خدمات مالية سريعة وسهلة نظرا لما تمنحه أنظمة الدفع الإلكتروني وشبكة الأنترنت والبطاقات النقدية الذكية من ميزات في ظل العولمة المالية، بل أصبح الحديث مؤخرا عن القطاع المالي الذكي الذي يعتمد على تكنولوجيا الذكاء الاصطناعي في التنبؤ والاحصاء والرصد للتحويلات المالية الإلكترونية.

وفي الجانب السلبي من هذا التطور ظهر للوجود اجرام جديد يتجلى في ظاهرة غسيل الأموال السيبراني (cyber money laundering) والتي أخطر الجرائم المستحدثة في عصر الاقتصاد الرقمي، وتمثل تحدي للمؤسسات المالية والقطاعات المصرفية في العالم، لاسيما فعالية القواعد القانونية في مواجهة هذه الأنشطة الجرمية التي تتطور طرق ارتكابها بشكل متسارع.

وساهم التطور التكنولوجي الرهيب في تحفيز غاسلي الأموال على الاستفادة منه من أجل إضفاء الشرعية على العائدات الإجرامية والذي يمنحهم فرص أكثر من العالم الحقيقي ويمكنهم من إخفاء هويتهم، وبالتالي تشكل جريمة تبييض الأموال السيبراني تهديدا خطيرا لجميع جوانب النشاط الاقتصادي لأي دولة، وهذا التهديد أكثر وضوحا في المؤسسات المالية، لاسيما مع تطور الوباء covid-19 الذي أسفر عن تغييرات في السلوكيات المالية مثل السلوك عبر الإنترنت المشتريات والتفاعلات المصرفية وزيادة التقلبات المالية التي سببت الخسائر بالملايين في الوظائف وعمليات اغلاق الشركات¹، ومن هذا نطرح الإشكالية التالية: كيف تساهم ظاهرة استخدام تكنولوجيات الاعلام والاتصال من قبل غاسلي الأموال في عولمة جريمة تبييض الأموال؟

وفي هذا الصدد اعتمدت على المنهجين الاستقرائي والوصفي من أجل تحليل مختلف النصوص القانونية المتعلقة بتبييض الأموال عبر الوسائط الإلكترونية، وبيان الأساليب التقنية لارتكاب هذا الاجرام.

وللإجابة على هذه الإشكالية، تم تقسيم الموضوع إلى قسمين، القسم الأول تبييض الأموال السيبراني اجرام مستحدث، ثم مفهوم تبييض الأموال السيبراني، وتقنيات تبييض الأموال السيبراني، أما القسم الثاني تجريم تبييض الأموال السيبراني، ثم تبييض الأموال السيبراني جريمة في القانون الجزائري، وتطبيق المعايير الدولية في مواجهة تبييض الأموال السيبراني، وبعدها التطرق في الخاتمة إلى نتائج الدراسة وبعض التوصيات.

¹ . Financial Action Task Force. COVID-19-Related Money Laundering and Terrorist Financing: Risks and Policy Responses. 2020. p08.

المبحث الأول

تبييض الأموال السيبراني اجرام مستحدث

يعد تبييض الأموال السيبراني بمثابة اجرام مستحدث يصنف ضمن الجرائم الاقتصادية الالكترونية، وهو نتاج للتطور التكنولوجي في مجال المعاملات المصرفية والمالية، ويشير هذا الاجرام الى خصوصية طبيعته المعقدة بحيث يجمع بين نوعين من الاجرام، تبييض الأموال كجريمة تقليدية والجريمة السيبرانية، هذه الأخيرة تمنح لغاسلي الأموال أساليب تقنية مبتكرة عبر مختلف الوسائل الالكترونية.

وهناك تعقيد في وضع مفهوم لجريمة تبييض الأموال السيبراني (مطلب أول)، ويعزز ذلك استخدام أساليب حديثة من نتاج التكنولوجيا وافرزات العولمة الاقتصادية أي تقنيات تبييض الأموال السيبراني (مطلب ثان).

المطلب الأول: مفهوم تبييض الأموال السيبراني

يجب أن يعكس تعريف تبييض الأموال عنصري أساسين، تبييض الأموال كجريمة تقليدية والجريمة السيبرانية، كما يستمد من هذه الأخيرة مميزات الإجرام الذي يتعدى حدود الدولة الواحدة.

الفرع الأول: محاولة وضع تعريف لتبييض الأموال السيبراني

تبييض الأموال السيبراني هو نتاج نوعين من الإجرام يتمثل في تبييض الأموال التقليدي من جهة، والجريمة السيبرانية من جهة أخرى، ونوضح مفهوم العنصر الأول: تبييض الأموال التقليدي وبنفس الكيفية نستكشف مفهوم العنصر الثاني: الجريمة السيبرانية بإيجاز، كل هذا من أجل الوصول لوضع تعريف لظاهرة "تبييض الأموال السيبراني".

أولاً: تحديد تعريف تبييض الأموال التقليدي

تعد جريمة تبييض الأموال من الجرائم المركبة ذات الطبيعة المعقدة وتقوم على عدة مراحل من أجل غسل المال الفذر وإكسابه صفة الشرعية، ويكون للمجرم الإعلان عن هذا المال وانفاقه في إطار رسمي¹، ويعد أحد أقدم تعريف لتبييض الأموال في المادة 03 (ب) "1" من اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية، بنصها: "تحويل الأموال أو نقلها، مع العلم بأنها مستمدة من أية جريمة أو جرائم منصوص عليها في الفقرة الفرعية (أ) من هذه الفقرة [الاتجار بالمخدرات]، أو من فعل من أفعال الاشتراك في مثل هذه الجريمة أو الجرائم، بهدف إخفاء أو تمويه الأصل غير المشروع للأموال أو قصد مساعدة أي شخص متورط في ارتكاب مثل هذه الجريمة أو الجرائم على الإفلات من العقاقب القانونية لأفعاله"، ويستنتج من هذا التعريف أن جريمة تبييض الأموال تكون تابعة لجرائم الاتجار بالمخدرات التي حددتها الاتفاقية، ويكون للمجرم

¹. محسن أحمد الخضيرى، غسل الأموال: "الظاهرة - الأسباب - العلاج"، مجموعة النيل العربية، القاهرة، سنة 2003، ص 58.



التتصل من تبييض الأموال إذا لم يكن إجرامه متعلقا بالمخدرات، وعليه يجب توسيع مجال الجرائم الأصلية التي تكون محلا لتبييض الأموال، وهذا ما ذهبت إليه اتفاقية مكافحة الجريمة المنظمة عبر الوطنية ليشمل تبييض الأموال الجرائم الخطيرة والمنظمة، وتبنت مجموعة العمل المالي¹ تعريفا لتبييض الأموال بأنه "معالجة العائدات الإجرامية لإخفاء مصدرها غير القانوني من أجل إضفاء الشرعية على عائدات الجريمة غير مشروعة"²، ومن هنا أخذ الفقه الجنائي معظم التعريفات التي تم صياغتها والتي يكون المال هو موضوع لها، واستعملت مصطلحات للدلالة على احتفاظ المجرمين على أموالهم غير المشروعة، وهي "غسل" و"تبييض" و"تمويه" و"إخفاء" و"تحويل الأموال القذرة"، ومع ظهور العولمة المالية تطور مفهوم المال بحيث لا يقتصر مفهوم "المنافع" على المال وحده الذي يشكل موضوع جريمة تبييض الأموال التقليدية، بل يشتمل على الأشياء الأخرى ذات القيمة المستمدة من الأنشطة الإجرامية، وبالتالي يمكن القول بأن الخدمات التجارية الالكترونية أو البرامج المسروقة أو الأموال الالكترونية وغيرها تصلح لأن تكون عائدات إجرامية.

ثانيا: تحديد تعريف الجريمة السيبرانية

تعد مصطلحات "الجريمة الإلكترونية" و"جرائم الكمبيوتر" و"إساءة استخدام الكمبيوتر"، و"جرائم المعلوماتية"، مرادفات لكلمة واحدة، حتى أن التسميات تتوسع أكثر لتشمل تسمية "جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال"، ويسمى آخرون جرائم الكمبيوتر والانترنت³، ويرجع ذلك إلى أن الفقه الجنائي لم يتفق على تسمية موحدة، وفيما يتعلق بمفهوم الجريمة الالكترونية بذلت محاولات عديدة لتعريفها، ولعل أقدم تعريف يعود إلى الفقيه "دون باركر" الذي يستخدم مصطلح "إساءة استخدام الكمبيوتر"، ويعرفه بأنه "أي حادث ينطوي على فعل متعمد يلحق ضررا بالضحية، أو يحتمل أن يلحقه ضرر من ذلك، ويحصل الجاني على مكسب مرتبط بالاستخدام السيء لأجهزة الكمبيوتر"⁴، وبعدها ظهرت عدة تعريفات حديثة تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجريم، وتعرف بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"⁵، والبعض بالنظر إلى وسيلة ارتكاب الجريمة أنها: "الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسوب" وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابياً أكثر منه سلبياً⁶، ومع ذلك تظل مفهوم سيئ التعريف على حد قول الفقيه "francis fortin"، بأنه: "سيء التعريف ومعقد، بحيث أخذ مكان له

¹. مجموعة العمل المالي: هي منظمة حكومية دولية مقرها في العاصمة الفرنسية باريس، أسست سنة 1989، وتهدف مجموعة العمل المالي لمحاربة تزوير العملات وتمويل الإرهاب.

². Financial Action Task Force. Money laundering. Policy Brief July 1999, p03.

³. CHAWKI, Mohamed, et al. Cybercrime, digital forensics and jurisdiction. Springer, 2015. p03.

⁴. PARKER, D. B.; PARKER, D. Crime by computer: Scribner New York. 1976, p25.

⁵. هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، سنة 1992، ص 20.

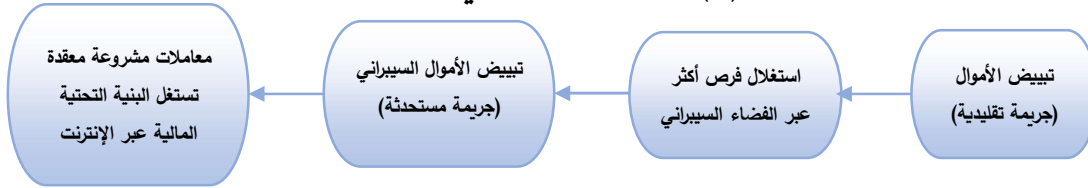
⁶. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، سنة 2000، ص 24.

في اللغة والخيال الجماعي، وبعدها تم تحويله إلى واقع ملموس ثقافيا، وتحليليا تغذية مصادر مختلفة مثل وسائل الإعلام الصحفية وخبراء الكمبيوتر والتمثيل السينمائي والخيالي، ويعد هذا المصطلح أساس ضعيف للبحث وجمع البيانات والتدخل في الواقع بحكم طبيعته غير الدقيقة والصحيحة، ويمثل هذا الافتقار في الوضوح مشكلة كبيرة لأنه يؤثر على جميع جوانب منع الجريمة الإلكترونية وتنظيمها¹، ونؤيد الطرح الذي يعتبر الجرائم الإلكترونية بمثابة سلوكيات إجرامية يتم تغييرها أو التوسط فيها عن طريق الإنترنت مما يميزها عن الأشكال التقليدية للسلوك الإجرامي²، وبالتالي تسمح الأنترنت بظهور جرائم تقليدية في الوسط السيبراني لتستغل المزيد من الفرص التي لا يوفرها الواقع الحقيقي التي وجدت فيه.

ثالثا: جريمة تبييض الأموال السيبراني تزوج بين نوعين من الإجرام

تعد جريمة تبييض الأموال السيبراني نتاج تزوج بين جريمة تبييض الأموال التقليدية والجريمة السيبرانية، فهو بمثابة اجرام حديث من إفرازات العولمة المالية والتطور التكنولوجي المتسارع الذي شمل جميع مناحي الحياة، ومما سبق بيانه يتضح بأن تبييض الأموال جريمة تقليدية في الأصل لكن بفعل التكنولوجيا وجدت فرص فيما يعرف بـ"العالم الافتراضي"، ويبين المخطط التالي ذلك.

المخطط (1): تبييض الأموال في عصر التكنولوجيا



وبالتالي أصبح المجرم الإلكتروني يلجأ الى تبييض الأموال الكترونيا عبر ما توفره مختلف الوسائط الإلكترونية، ويتشكل بذلك نوع جديد من الجرائم الإلكترونية المالية تظهر أهميته أكثر في المستقبل، ويتم تبييض الأموال بالمفهوم التقليدي للجريمة عن طريق إخفاء الأصل الإجرامي الذي تتأتى منه الأموال القدرة لتضفي عليها صفة الشرعية من خلال اتباع مجموعة من العمليات الاحتمالية، وعلى النقيض من ذلك يعد تبييض الأموال السيبراني ذو بعد تقني لان العمليات التي يجب أن يجتازها لإضفاء الشرعية على المال تكون في العالم الافتراضي، كما تتطلب ذكاء ومهارة المجرم الإلكتروني.

ويمكن أن تعرف جريمة تبييض الأموال السيبراني بأنها: "استخدام الأنترنت في إضفاء الشرعية على معاملات أو ممتلكات أو منافع سواء كانت مادية أو معنوية، والتي يكون مصدرها نشاط إجرامي".

¹ DU QUÉBEC, Sûreté; FORTIN, Francis. *Cybercriminalité: Entre inconduite et crime organisé*. Presses inter Polytechnique, 2013, p03.

² WALL, David S. Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, 2007, 8.2, p187.

الفرع الثاني: خصائص جريمة تبييض الأموال السبيرياني

تشتمل جريمة تبييض الأموال السبيرياني على العديد من العناصر المميزة لها، نظرا لأنها تجمع بين نوعين من الإجرام، بحيث تتركب من جريمة اقتصادية تتمثل في تبييض الأموال التي تهدد اقتصاديات الدول والتنمية المحلية فيها، والمركب الثاني الجريمة الالكترونية التي تعد ظاهرة ناتجة عن العولمة والتكنولوجيا، وهذا ما جعل منها نوع من الاجرام الحديث والمعقد يندرج تحت طائفة الجريمة الاقتصادية الالكترونية.

1./ **جريمة مستحدثة:** يعد تبييض الأموال السبيرياني من الجرائم المالية الالكترونية الناشئة والتي ينتظر منها الكثير في ظل التطور الرهيب للتكنولوجيا واتصاله باقتصاد الدول والعمليات المصرفية.

2./ **عابرة للحدود الوطنية:** تستغل جريمة تبييض الأموال العالم الافتراضي مما يجعلها عالمية، ويكون للمجرم ان يمارس اجرامه المالي باستعمال الكمبيوتر او الهاتف او اجراء تحويلات مالية الكترونية مشبوهة، فلا يمكن حصر هذا الاجرام في رقعة جغرافية محددة، فهو يستعير صفة الجريمة الالكترونية التي تتميز بأنها عابرة للحدود الوطنية، فهي تتخطى الحدود الجغرافية وتكتسب طبيعة دولية عن طريق القدرة التي تتميز بها الحاسبات الآلية في نقل وتبادل المعلومات بين أنظمة يفصل بينها الآلاف من الأميال في سرعة هائلة، وأن حجم تلك المعلومات يميزها عن الجريمة التقليدية بصورة كبيرة¹.

3./ **تهديد الاقتصاد الوطني:** تعد جريمة تبييض الأموال السبيرياني من الصور الإجرامية المستحدثة ذات البعد الاقتصادي والتي تتعدى حدود الدولة، فهي من الجرائم الاقتصادية الدولية لما لها من اتصال وثيق بالأنشطة الاقتصادية غير المشروعة، وتسبب تغير مفاجئ في قوى السوق في الدولة، مما يصيب الاقتصاد بفقدان التوازن والتخبط بين دورتي التضخم تارة والانكماش تارة أخرى لأسباب غير متوقعة وغير معلومة، ويصعب على صاحب القرار في الدولة مواجهتها وعلاجها، بسبب دخول وخروج المال غير المشروع بمقادير كبيرة معتمدا على أساليب التحايل والخفاء².

4./ **استعمال الوسائط الالكترونية:** تأثير العولمة المالية أدى الى استعمال تكنولوجيات الاعلام والاتصال في القطاع المالي، فأصبحت التحويلات المالية تتم عبر الأنترنت أو الهواتف النقالة بفعل التكنولوجيا، وفي نفس الوقت تطور الإجرام المالي متأثرا بما تتيحه الجريمة الالكترونية، ومن هنا تطورت وسائل تبييض الأموال لتعتمد أكثر على الأنترنت لما توفره من سهولة وفرص أكثر.

¹. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، سنة 2004، ص 47.

². أحمد محمد العمري، جريمة غسل الأموال: نظرة دولية لجوانبها الاجتماعية والنظامية والاقتصادية، العيكان للنشر، الرياض، سنة 2000، ص 69.

المطلب الثاني: تقنيات تبييض الأموال السيبراني

يقوم تبييض الأموال السيبراني على أساليب حديثة من نتاج التكنولوجيا وافرارات العولمة الاقتصادية، ونبين التقنيات التي يلجأ إليها غاسلي الأموال التي لا تتوافر في الواقع كما أنها تمنح لهم فرص أكبر في الواقع الخيالي، وبذلك نزيل الغموض على هذا الاجرام المستحدث الذي تأثر فعلا بالتقدم التكنولوجي.

الفرع الأول: الأساليب الشائعة في تبييض الأموال السيبراني

هناك وسيلتين تستخدمان على نطاق واسع في تبييض الأموال السيبراني، ونجد في مقدمتها أنظمة الدفع الإلكتروني التي يتم تطوير مجموعة كثيرة منها حالياً، والوسيلة الثانية والتي تعد من ضمن أنظمة الدفع التي تستند إلى الإنترنت -بمعنى تختلف عن الدفع الإلكتروني-، ويندرج ضمنها: النقد الإلكتروني والبطاقات الذكية ذات القيمة المخزنة¹، والتي تسجل استعمالاً شائع في معظم عمليات تبييض الأموال السيبراني.

أولاً: أنظمة الدفع الإلكتروني

أنظمة الدفع الإلكتروني "E-payment systems" لوضع تعريف له نبين معنى لـ"الدفع" وهو تحويل للقيمة النقدية ولهذا فإن "نظام الدفع" ليس أكثر من ترتيب منظم لتحويل القيمة النقدية بين المشاركين فيه، وتكون أنظمة الدفع أساسية لعمل جميع الاقتصادات النقدية، إذا كان المال هو شريان الحياة للاقتصادات النقدية الحديثة، فإن أنظمة الدفع هي نظام التداول الذي يشير إلى مختلف الوسائل التي يمكن من خلالها إجراء الدفع عبر الإنترنت، وتؤدي حالات الفشل في نظام التداول هذا إلى خطر حدوث توقف في المعاملات الحقيقية والمالية التي تدعمها، مما قد يؤدي إلى تكاليف اجتماعية كبيرة محتملة².

وتتطوي أنظمة الدفع الإلكتروني على تبادل مالي عادة ما يكون في شكل أداة مالية مشفرة، مثلاً رقم بطاقة الائتمان المشفرة أو العملة الإلكترونية أو الشيك الإلكتروني التي عادة ما تكون مدعومة من قبل بنك أو وسيط أو مانح قانوني³، وتعتمد الجزائر على هذه الأنظمة التي عرفت في قانون التجارة الإلكترونية في المادة 06 بأن: "وسيلة الدفع الإلكتروني: كل وسيلة دفع مرخص بها طبقاً للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية"⁴.

¹. MOLANDER, Roger C.; MUSSINGTON, David; WILSON, Peter A. *Cyberpayments and money laundering: Problems and promise*. Rand Corporation, 1998, p11.

². HALDANE, Andrew G.; SAPORTA, Victoria (ed.). *The future of payment systems*. Routledge, 2008, p02.

³. O'MAHONY, Donal; PIERCE, Michael; TEWARI, Hitesh. *Electronic payment systems for e-commerce*. Artech, 2001, p05.

⁴. قانون رقم 18-05 مؤرخ في 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، صادر في 16 مايو سنة 2018، ص 04.

وأكدت هيئة تجمع النقد الآلي (GIE) Monétique بأن المعاملات الإلكترونية في الجزائر خلال الفصل الأول من سنة 2021 واصلت ارتفاعها بفضل القفزة التي أحرزتها عمليات الدفع عبر الإنترنت (+247,80 بالمائة خلال سنة) وعمليات الدفع بواسطة أجهزة الدفع الإلكتروني (+384,34 بالمائة)، مع زيادة معتبرة في عدد البطاقات البنكية بأكثر من 10,7 مليون بطاقة¹، وتم مؤخرا تحت إشراف الوزير الأول التوقيع على اتفاقية إطلاق خدمة الدفع الإلكتروني عبر الإنترنت بين كل من تجمع النقد الآلي ومؤسسة بريد الجزائر، وكذا شركة النقد الآلي والعلاقات التلقائية بين البنوك "ساتيم"²، وبالتالي فإن القطاع المالي في الجزائر تأثر فعليا بالتقدم التكنولوجي في المجال الاقتصادي ليقتررب شيئا نحو العولمة المالية، كل هذا التطور الحاصل يمنح للمجرمين فرص من أجل الاجرام المالي الالكتروني في صورة تبييض الأموال السببراني.

ونعتبر أن أنظمة الدفع الالكتروني وسيلة جديدة للقيام بتبييض الأموال من خلال التحويلات المالية، والتي تكون من الأموال الإلكترونية غير الشرعية "القذرة" التي يتم الحصول عليها إما من الفضاء السببراني أو الأموال التي كانت في الأصل عبارة عن نقود غير شرعية، ولكن تم تحويلها إلى نقود إلكترونية غير قانونية مثلا يمكن تحويل النقود السائلة المتأتية من عائدات إجرامية إلى نقود إلكترونية شرعية من خلال استخدام أنظمة الدفع الإلكتروني.

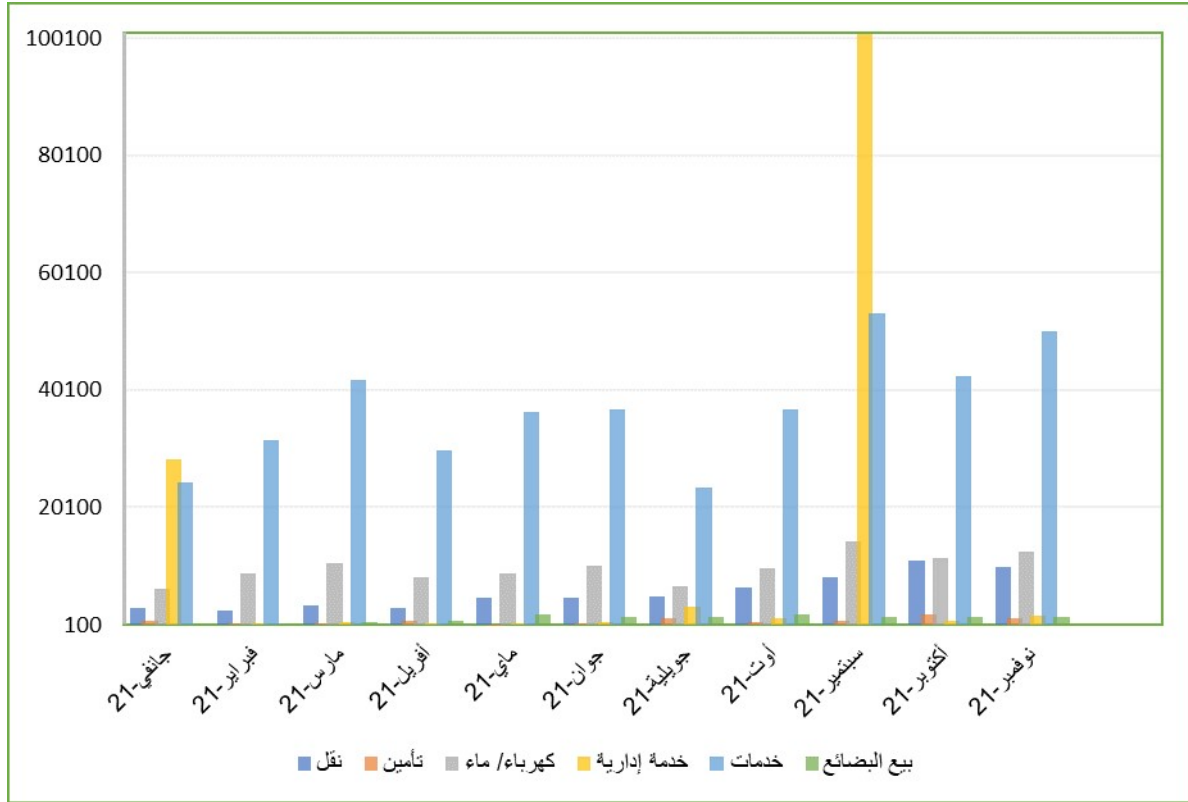
وتعد النقود الإلكترونية بمثابة السلاح الذي يتم استخدامه لأغراض تبييض الأموال عبر الإنترنت، ويمكن وصف النقود الإلكترونية بأنها قيمة نقدية أو ما يعادلها يتم تمثيلها في شكل إلكتروني، ولا تعد نقودا إلكترونية الوسائل الحديثة للوصول إلى الحساب المصرفي من بطاقات الدفع المصرفية والخدمات المصرفية عبر الإنترنت، لأنها تسمح ببساطة بالعمليات بأموال حقيقية محفوظة في الحسابات المصرفية، بمعنى آخر لا توفر هذه المنتجات سوى وسائل الوصول إلى الأموال، ويمكننا القول إن "النقود الإلكترونية" الحديثة هي مرحلة طبيعية في تطور وسائل الدفع الإلكتروني³، فالنقود الإلكترونية نظام يسمح للشخص بالدفع مقابل سلع أو خدمات عن طريق إرسال رقم من جهاز كمبيوتر إلى آخر، وتعد الأرقام النقدية الرقمية فريدة من نوعها، ويتم إصدار كل واحد من قبل البنك ويمثل مبلغا محدداً من المال الحقيقي، وتتمثل إحدى السمات الرئيسية للنقد الرقمي في أنه مثل النقود الحقيقية تكون مجهولة المصدر وقابلة لإعادة الاستخدام، ويبين المخطط التالي تطور عمليات الدفع الالكتروني في سنة 2021.

¹. وكالة الأنباء الجزائرية (APS)، ارتفاع عدد أجهزة الدفع الإلكتروني بنسبة تقارب 30 بالمائة إلى غاية الفصل الأول من 2021، في 01 أكتوبر 2021، تم الاسترداد من وكالة الأنباء الجزائرية: <https://www.aps.dz/ar/economie/106428-30-2021>

². المؤسسة العمومية للتلفزيون الجزائري (ENTV)، الوزير الأول يشرف على مراسم توقيع اتفاقية إطلاق خدمة الدفع الإلكتروني عبر الإنترنت، في 30 ديسمبر 2021، تم الاسترداد من: <https://www.entv.dz/117928-2>

³. VLASOV, A. V. The Evolution of E-Money, "European Research Studies", 20(1), 2017, p217.

المخطط (2): نشاط الدفع الآلي في الجزائر سنة 2021



المصدر: موقع تجمع النقد الآلي **GIE monetique**، جدول احصائيات حول "نشاط الدفع الآلي"، الرابط:
<https://giemonetique.dz/ar/qui-sommes-nous/activite-paiement-sur-internet>

ثانيا: البطاقات النقدية الذكية

بطاقات القيمة المخزنة تُعرف أيضًا باسم "البطاقات الذكية" أو المحفظة الإلكترونية، وهي عبارة عن قطع بلاستيكية عادة ما تكون بحجم بطاقة الائتمان، تحتوي على رقاقة (شريحة ذاكرة) يمكن تشفير القيمة إليها، ويمكن تحميل هذه البطاقات أو القيمة المضافة عبر ماكينة الصرف الآلي والهواتف النقالة وأجهزة الكمبيوتر الشخصية ومن بطاقات القيمة المخزنة الأخرى باستخدام جهاز يمكنه نقل القيمة مباشرة، ومن الناحية النظرية يمكن برمجتها لتخزين مليارات الدولارات، ومع ذلك فإن معظم برامج بطاقات القيمة المخزنة الحالية تضع حدًا لمقدار القيمة التي يمكن تحميلها على أي بطاقة فردية¹، وقد تسهل البطاقات الذكية على الشخص الذي يقوم بغسيل الأموال تحويل الأموال غير المشروعة بدون الكشف عنه من طرف السلطات العامة والمؤسسات المالية²، لأن القيمة النقدية يتم تخزينها على البطاقة فلا داعي للاتصال ببنك أو شركة بطاقة ائتمان للحصول على الموافقة على المعاملة، وما هو مفيد لغاسلي الأموال إمكانية نقل الأموال من بلد إلى آخر بشكل آمن عن رقابة المؤسسة المالية، واستخدام بطاقة صادرة في دولة ما لسحب الأموال في دولة أخرى، كما يمكن

¹. Financial Action Task Force. GAFI. Report on New Payment Methods. Paris: FATF. 2006, p04.

². MOLANDER, Roger C, Op. Cit., p18.

للمستخدمين حمل العديد من البطاقات مما يسمح للمجرمين بتحريك مليارات الدولارات دون استخدام البنوك على الإطلاق.

الفرع الثاني: استغلال هشاشة البنية الإلكترونية

تستغل البنية الإلكترونية في المجال المالي من طرف مجرمي تبييض المال عبر الخدمات المالية عبر الإنترنت والمزادات عبر الإنترنت والألعاب عبر الإنترنت، وهي ميزة بارزة في صفة غاسلي الأموال لاستغلال الخدمات التجارية المشروعة لأغراض تبييض الأموال، ونحدد بعض هذه الخدمات التي يوفرها الفضاء السيبرانية، ونكشف عن بعض التقنيات المستخدمة حاليًا لأغراض تبييض المال السيبراني.

أولاً: البنوك الإلكترونية

البنوك الإلكترونية تختلف عن البنوك التقليدية التي تمارس الخدمات التقليدية وخدمات الصيرفة الإلكترونية، فلا يوجد لها واقع على الأرض وإنما موجودة في شبكة الأنترنت¹، ويعود انتشار البنوك الإلكترونية إلى تطور دور الوساطة في حركة التدفقات المالية والنقدية نتيجة عولمة الأسواق، وتطور المعلوماتية وتكنولوجيا الإعلام والاتصال أو ما يعرف بالصدمة التكنولوجية²، وتستخدم البنوك الإلكترونية لأداء أنشطة مصرفية منتظمة مثل الاستفسارات عن الحساب ودفع الفواتير وتحويل الأموال، ومع ظهور البنوك الإلكترونية يشعر العملاء بمستوى جديد من الراحة، لأنه يمكن لهم إبرام بعض المعاملات المصرفية الأساسية دون تواجدهم فعلياً في البنك، وتعد من الثمار المفيدة للإنترنت التي بفعلها أصبح العالم مركز إلكتروني وقرية عالمية، وبادرت البنوك الجزائرية في تطوير الخدمات المالية عبر استعمال التكنولوجيا من خلال تطوير شبكات الكترونية للدفع والتسديد عبر نقاط في التراب الوطني مثل: CPA، BEA، BNA، CNMA، ALBARAKA، CNEP، BDL، BADR وغيرها من البنوك.

ويعد النقد الإلكتروني الذي تحتفظ به معظم البنوك القائمة على الإنترنت لا يندرج في نطاق النقد الثابت الذي يخضع للتنظيم والرقابة، كما أن مبدأ "اعرف عميلك" الذي يكرسه المشرع بفرضه واجب على الخاضعين للالتزام باليقظة والحذر أثناء ممارسة مهنتهم وذلك بالتحقق من هوية الزبائن وفقاً لما تنص عليه المادة 07 من القانون 01/05 المعدلة بمقتضى المادة 04 من الأمر 12-02 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم، حيث جاء فيها أنه: "يجب على الخاضعين أن يتأكدوا من موضوع وطبيعة النشاط وهوية زبائنهم، كل فيما يخصه قبل فتح أي حساب أو دفتر، أو حفظ سندات أو قيم أو إيصالات، أو تأجير صندوق أو القيام بأي عملية أو ربط أي علاقة أعمال أخرى"، والذي يتطلب من البنوك الأرضية الإبلاغ عن المعاملات المشبوهة، فلا يمكن تطبيقه مباشرة على البنوك عبر الإنترنت لأنه لا يتم التحقق من هوية العميل المحتمل على

¹. طارف طه، إدارة البنوك في بيئة العولمة والأنترنت، دار الجامعة الجديدة، مصر: الإسكندرية، سنة 2007، ص 120.

². عبد العزيز خنفوسي، قانون الدفع الإلكتروني، مركز الكتاب الأكاديمي، سنة 2018، ص 129.



عكس البنوك الأرضية (التقليدية)، هناك لقاء وجهاً لوجه في البنك، حيث يُطلب من العملاء المحتملين تقديم مستندات إثبات الهوية، والتي يتم التحقق منها قبل فتح الحساب، بينما في البنوك عبر الإنترنت، تم تصميم استراتيجية التسويق لمعظم البنوك عبر الإنترنت للسماح لأي شخص بفتح حساب، بغض النظر عن مكان تواجد الشخص، وبالتالي فإن أي معلومات يتم توفيرها لفتح الحساب هي فقط الأدلة التي يراها البنك فقط، وتبقى الهوية الحقيقية للمجرم الجالس وراء الكمبيوتر غير معروفة¹.

ثانياً: البيع بالمزاد العلني عبر الإنترنت

البيع بالمزاد الإلكتروني من نتائج الثورة التكنولوجية في مجال الاقتصاد، ويعرف بأنه البيع والشراء الذي يتم في موقع من المواقع الإلكترونية على شبكة الأنترنت بطريقة المزايمة²، ولم يضع المشرع قواعد تشريعية تنظم البيع بالمزاد العلني الإلكتروني في القانون رقم 05-18 الذي يتعلق بالتجارة الإلكترونية مع أن نصوص القانون المدني وقانون الإجراءات المدنية والإدارية نظمت البيوع بالمزايدات في المنقول والعقار، وفي المزاد الإلكتروني يقوم فيه البائع بعرض السلعة المراد بيعها بعد أن يقوم بتسعيرها ويتم وضع سعر يفتح به المزاد الإلكتروني، ثم يقوم صاحب المزاد بعملية التوسط في البيع والشراء من خلال الموقع الإلكتروني الذي يملكه، ويقوم كل مزاد بتقديم عطائه، بسعر أعلى من العطاء السابق، حتى يتم الوصول إلى السعر النهائي الذي يرسو به المزاد، ويترتب عليه آثار من خلال قيام المستهلك بالوفاء الإلكتروني لثمن البضاعة، وقيام صاحب المزاد بتوريد السلعة إلكترونياً أو بطريقة عادية، وبوصولها إلى يد المستهلك خالية من العيوب ووصول العملة إلى صاحب المزاد، تنتهي المزايمة الإلكترونية³.

وبالنظر إلى أن شركات المزادات عبر الإنترنت شرعية، تكمن الثغرة بالنسبة للمجرمين في عملية تقديم المزايدات، أين يمكن للمجرم استغلال هذا الطريق من خلال توظيف مزايد يمكنه الاستمرار في تقديم عطاء بمبالغ كبيرة حتى يتم بيع العنصر له، وعلى سبيل المثال: يقدم تاجر مخدرات على تحويل أموال التي لديه المكتسبة من الجريمة لإضفاء الشرعية على ثروته، ويقوم بشراء بطاقة نقدية لشحنها بالأموال غير المشروعة تحضيراً للمشاركة في مزاد علني عبر الأنترنت، يضع قطعة أثرية في المزاد العلني ويقوم بالمزايد الذي اتفق معه مسبقاً بتقديم أكبر عطاء ليرسو المزاد على الأنترنت وينتج آثاره، والذي يدفع الأموال في الحساب المصرفي لـ "الموقع الإلكتروني للمزاد العلني"، وفي الوقت نفسه يرسل تاجر المخدرات القطعة الأثرية (البائع) إلى المزايد الذي توقف عليه المزاد (المشتري)، وبعد ذلك يتم إجراء عمليات التحقق اللازمة ودفع الأموال إليه، وفي هذه المرحلة تم دمج المال بالكامل في العالم التجاري أي تم "تنظيفه".

¹ . LESLIE, Daniel Adeoyé. *Legal principles for combatting cyberlaundering*. Springer, 2014, p77.

² . أحمد عبد التواب محمد بهجت، *إبرام العقد الإلكتروني "دراسة مقارنة"*، دار النهضة العربية، مصر، سنة 2009، ص36.

³ . ثامر عبد الجبار عبد العباس السعيد، *التنظيم القانوني للمزاد الإلكتروني، دراسة مقارنة*، المركز العربي للنشر والتوزيع، مصر، سنة 2018، ص12.

ثالثا: لعب القمار عبر الأنترنت

تدخل ألعاب الرهان أو القمار عبر الأنترنت ضمن مجال تبييض الأموال والتهرب الضريبي، ويصنفها الخبراء كخدمة مثالية قائمة على الويب لإضفاء الشرعية على المكاسب غير المشروعة، وتستخدم الكازينوهات في العالم الحقيقي لغسل الأموال القذرة، ويمكن القيام بنفس الشيء عن طريق مواقع القمار عبر الأنترنت، وهناك احتمالان لغاسلي الأموال عبر استغلال خدمة شرعية قائمة على الويب أو القيام بإنشاء شركة قمار عبر الأنترنت من أجل تنظيف الأموال¹.

ويعد من السهل إنشاء موقع ويب للقمار عبر الأنترنت، للميزة اللامحدودة التي يمنحها العالم السيبراني، وتمثل المقامرة عبر الأنترنت لغسيل الأموال أحد الجوانب السلبية في وجود فضاء سيبراني يجعل تنظيم ومراقبة مواقع المقامرة عبر الأنترنت شبه مستحيل، خصوصا عندما تسمح قوانين البلد المعني بالمقامرة عبر الأنترنت، ويعد إنشاء موقع للمقامرة عبر الأنترنت مهمة خالية من المتاعب للمجرم².

ويعتبر القمار عبر الأنترنت نشاطاً غير قانوني في الجزائر بموجب القانون رقم 05-18 المتعلق بالتجارة الالكترونية يمنع لعب القمار والرهان عبر الأنترنت في الفقرة الثانية من نص المادة 03 بأنه: "تمنع كل معاملة عن طريق الاتصالات الالكترونية تتعلق بما يأتي: -لعب القمار والرهان واليانصيب، .."، ويمكن تصور عملية تبييض الأموال عبر القمار أو الرهان في الأنترنت من خلال أن المقامر الذي عنده عائدات إجرامية "مال قذر" يقوم بفتح موقع للقمار عبر الأنترنت، ويقوم بتوظيف جيش من المقامرين في موقعه للوصول لهدفه، ويمكنه توزيع الأموال غير المشروعة بين هؤلاء المنضمين للمقامرة على الموقع، وليس من المهم ما إذا كان المقامر يفوز أو يخسر، لأنه ببساطة المجرم هو الذي يفوز بمجرد أن العائدات ستفوز وتصبح شرعية من ألعاب القمار عبر الأنترنت بعدما كانت غير مشروعة.

رابعا: محاكاة الحياة الافتراضية

يمكن تقسيم الفضاءات الافتراضية إلى ثلاثة أنواع أساسية، تتمثل في:

1/. فضاءات سيبرانية للألعاب الخيالية: مثل MMORPG التي تعني لعبة تقمص الأدوار كثيفة اللاعبين على الأنترنت اختصارا لـ "Massively Multiplayer Online Role-Playing"، ويجتمع فيها عدد هائل من اللاعبين ويتفاعلون فيما بينهم بداخل عالم اللعبة الافتراضي³ من خلال صوره الرمزية مع آلاف اللاعبين

¹. FILIPKOWSKI, Wojciech. Cyber Laundering: An Analysis of Typology & Techniques, *International Journal of Criminal Justice Sciences*, 2008, 3.1, p21.

². LESLIE, Daniel Adeoyé. Op. Cit., p82.

³. Wikipedia, the free encyclopedia, Massively multiplayer online role-playing game, available at: https://en.wikipedia.org/wiki/Massively_multiplayer_online_role-playing_game, (1 novembre 2021)

الآخرين، ويجمعون أشياء رقمية متنوعة الأنواع من أجل حل المهام وتنظيم أنفسهم في مجموعات للتغلب على تحديات معينة¹.

2/. فضاءات سيبرانية تعتمد على المحتوى: الذي ينشئه المستخدم والذي يديم الإنشاء المشترك للكائنات الافتراضية من قبل المستخدمين، مثلاً: SL(second life) بمعنى الحياة الثانية والتي تكون في العالم الافتراضي عبر الأنترنت، و"Entropia Universe" وهو عالم افتراضي متعدد اللاعبين عبر الأنترنت تم تصميمه ويحتوي على نموذج أعمال الدفع الأصغر، حيث يمكن للاعبين شراء عملة داخل اللعبة بأموال حقيقية يمكن استردادها مرة أخرى بالدولار الأمريكي بسعر ثابت، والعالم الافتراضي Active Worlds يعين المستخدمون أنفسهم اسماً، ويسجلون الدخول إلى كون رقمي، ويستكشفون العوالم والبيئات الافتراضية ثلاثية الأبعاد التي بناها الآخرون، وغيرها من البيئات الرقمية الواسعة الانتشار خصوصاً مع جائحة الكورونا.

3/. فضاءات سيبرانية التي تأخذ طابع أو ميزات مواقع الشبكات الاجتماعية: مثل Facebook أو Twitter، وتستضيف هذه العوالم الافتراضية تمثيلاً افتراضياً للعديد من الأفراد الحقيقيين، دون توفير بيئة مكانية افتراضية يمكن للمستخدمين التنقل فيها، فالروابط بين الملفات الشخصية الاجتماعية تجعل العلاقات الاجتماعية مرئية والعديد من الطرائق التي تخلق ديناميكيات اجتماعية وجاذبية، مثل المجموعات عبر الأنترنت.

ويمكن تصور تبييض الأموال السيبراني من خلال المثال الذي لم نشرحه سابقاً وهو SL اختصار لـ "second life" بمعنى الحياة الثانية التي تكون في العالم الافتراضي، وتم تطوير هذا الفضاء السيبراني في سنة 2003، ويسمح للمشاركين في SL الذين يضاف عليهم بـ "المقيمين"، ويمكنهم من خلال صورههم الرمزية استكشاف والتعرف على الآخرين المقيمين في البيئة الافتراضية والاختلاط والمشاركة في الأنشطة الفردية والجماعية، وحتى إنشاء وتداول الممتلكات والخدمات الافتراضية مع بعضها البعض أو السفر في جميع أنحاء العالم، وتعرف العملة المستخدمة في SL باسم (L \$) Linden Dollars.

كما هو الحال في العالم الحقيقي، تدور أنشطة جميع المقيمين حول المال (أي L \$)، حيث إنه ضروري لكسب لقمة العيش ولتدفق التجارة، يكون للسكان الأذكى تحقيق أرباح في الواقع من معاملاتهم الداخلية، ويمكن للمقيمين تحويل أموال العالم الحقيقي أي الواقعي إلى عملة العالم الافتراضي SL، ولديها خدمة تحويل الأموال المعروفة باسم Xstreet، ويمكن للمقيمين عمل أي شيء يرغبون فيه، بما في ذلك إنشاء أشياء افتراضية وشراء عقارات²، وبالتالي تكون القوانين غائبة في الفضاءات السيبرانية، وتأخذ القوانين الموجودة شكل شروط الاستفادة من الخدمة، والتي تحمي المقيمين أو اللاعبين من المضايقة والإفشاء والفحش والتعصب والاعتداء في اللعبة الإلكترونية.

¹. KLIMMT, Christoph. Virtual worlds as a regulatory challenge: A user perspective. In: *Virtual worlds and criminality*. Springer, Berlin, Heidelberg, 2011. p. 03.

². see SECONDLIFE, Available at: <https://www.secondlife.com> (22november2021)

المبحث الثاني

تجريم تبييض الأموال السبيرياني

يعد منع تبييض الأموال عبر الوسائط الإلكترونية أهمية بالغة نظرا لحدثة هذا الاجرام ولاسيما في اقتصاديات الدول النامية، ونحاول توضيح الإطار القانوني لمكافحة تبييض الأموال السبيرياني في القانون الجزائري انطلاقا من كونه جريمة كلاسيكية، ثم نوضح أهم المعايير الدولية في هذا المجال التي تشكل قانون غير ملزم على الدول وتبقى مجرد توصيات هامة لمواجهة هذا الاجرام على المستوى الوطني والدولي.

وهناك غموض في تجريم ظاهرة تبييض الأموال السبيرياني في القانون الجزائري (مطلب أول)، وضرورة تبني التدابير الدولية التي لا ترقى الى قانون ملزم إلا إذا تبنتها في قوانينها الداخلية، فهي نوع من الوقاية عبر تطبيق المعايير الدولية في مواجهة تبييض الأموال السبيرياني (مطلب ثان).

المطلب الأول: تبييض الأموال السبيرياني جريمة في القانون الجزائري؟

تتكون جريمة تبييض الأموال السبيرياني من شقين، الأول تبييض الأموال كجريمة في حد ذاتها بالمفهوم التقليدي التي اتفقت جميع التشريعات على التصدي لها، والثاني التقنيات المستعملة في ارتكابها التي تركز على التكنولوجيا مما جعل التصدي لها يكون عبر مكافحة الجريمة الإلكترونية.

الفرع الأول: تبييض الأموال من جرائم القانون العام

جرم المشرع الجزائري تبييض الأموال في المادة 389 مكرر من قانون العقوبات بأنه: "يعتبر تبييضاً للأموال: (1) تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلة، (2) إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصادرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها مع علم الفاعل أنها عائدات إجرامية، (3) اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية، (4) المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو التآمر على ارتكابها والمساعدة والتخريض على ذلك وتسهيله واسداد المشورة بشأنه"، كما أن القانون 05-01 الذي يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما في المادة الثانية منه جاءت مطابقة للصور السالف ذكرها، وبالتالي فالمشرع الجزائري في تجريمه لتبييض الأموال لم يقم بوضع تعريف للظاهرة، وإنما ساير الاتفاقيات الدولية في هذا الطرح، وعدد الأفعال الاجرامية التي تنطوي على تبييض للأموال على سبيل الحصر.

كما لم يعرف "العائدات الاجرامية" الى غاية صدور القانون 06-01 الذي يتضمن قانون الوقاية من الفساد ومكافحته¹ (الجريدة الرسمية للجمهورية الجزائرية، 08 مارس 2006) في المادة الثانية البند (ز) بأنها: "كل الممتلكات المتأتية أو المتحصل عليها بشكل مباشر أو غير مباشر من ارتكاب الجريمة"، كما حددت بأن الجرم الأصلي هو كل جرم تتأتى منه عائدات يمكن أن تصبح موضوع تبييض للأموال وفقا للتشريع المعمول به ذي الصلة، وهذا المنهج الذي سلكه المشرع يتطابق مع مبدأ الشرعية الذي يقتضي تحديد الأفعال المجرمة بنصوص مكتوبة، ويبقى السؤال المطروح هل توجد جريمة تبييض الأموال السببراني في القانون الجزائري؟، وهذا ما سوف نحاول معالجته.

الفرع الثاني: تطبيق قواعد التجريم التقليدية على تبييض الأموال السببراني

عمل المشرع على تجريم مختلف الأفعال التي تستهدف أنظمة المعالجة الآلية للمعطيات من خلال القانون رقم 04-15 المتضمن تعديل قانون العقوبات في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات، ويكون بذلك قد اعتمد على معيار موضوع الجريمة ألا وهو المساس بأنظمة المعالجة الآلية للمعطيات، بعد ذلك صدر القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها²، والذي حددت المادة 02 منه مفاهيم بعض المصطلحات التي ترتبط بالجريمة الإلكترونية، وعرفت "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

ونستنتج بأن جريمة تبييض الأموال التقليدية في نص المادة 389 مكرر من الجرائم التي ترتكب أو يسهل ارتكابها عبر منظومة معلوماتية أو نظام للاتصالات الإلكترونية لتشكل نوع جديد من الإجرام تحت مسمى "تبييض الأموال السببراني"، وبالتالي يمكن القول بأن جريمة تبييض الأموال السببراني يتصور لها وجود قانوني من خلال القانون 09-04 في ظل تجريم تبييض الأموال التقليدي، ومن ناحية أخرى يستلزم مبدأ الشرعية المكرس في المادة الأولى من قانون العقوبات ضرورة أن يكون التجريم دقيقا وواضحا، وهذا محقق لأن جريمة تبييض الأموال التقليدية محددة الأركان في نص المادة 389 مكرر من قانون العقوبات، وانطلاقا من وجهة النظر هاته التي مفادها أن تبييض الأموال السببراني هو بالفعل غسيل أموال يظهر في شكل آخر، يمكن القول أن الأساس القانوني الذي يحكم تبييض الأموال التقليدي هو نفسه بالنسبة لتبييض الأموال السببراني، ومع ذلك

¹. قانون رقم 06-01 مؤرخ في 20 فبراير سنة 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 14، صادر في 08 مارس سنة 2006، ص 04.

². قانون رقم 09-04 مؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، صادر في 16 غشت سنة 2009، ص 05.

الإطار القانوني الحالي لتبييض الأموال ليس كافياً لقياس واحتواء معضلة تبييض الأموال السبيرياني، وذلك لعدم وجود قوانين لمكافحة تبييض الأموال تعالج هذا النوع المستحدث من الإجرام بشكل مباشر، وهذا التوجه أخذ به المشرع الإماراتي في معالجته لظاهرة تبييض الأموال السبيرياني في المادة 19 من القانون الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، بأنه: " مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالحبس مدة لا تزيد على سبع سنوات وبالغرامة التي لا تقل عن ثلاثين ألف ولا تزيد على مائتي ألف درهم، كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعا لارتكاب أي من هذه الأفعال".

المطلب الثاني: تطبيق المعايير الدولية في مواجهة تبييض الأموال السبيرياني

بذلت بعض المنظمات غير الحكومية وكيانات القطاع الخاص الدولية جهودا لفهم جريمة تبييض الأموال السبيرياني تأخذ شكل السياسات والتوصيات، فهي لا ترقى إلى إطار قانوني ضد الجريمة في حد ذاتها لأنها قوانين غير ملزمة، وتبقى مجرد تدابير وقائية للدول من الإجرام المستحدث.

الفرع الأول: تدابير في مجال الدفع الآلي

وضعت مجموعة العمل المالي العديد من التدابير التي يجب العمل بها من أجل مواجهة الخطر المتزايد عن استعمال التكنولوجيا في تبييض الأموال، حيث يجب على الدول والمؤسسات المالية تحديد وتقييم مخاطر تبييض الأموال التي تنشأ عن الممارسات التجارية الحديثة من طرق الدفع الإلكتروني وتنامي استخدام التقنيات الحديثة، واتخاذ التدابير المناسبة لإدارة هذه المخاطر والتخفيف من حدتها بالتأكد من أن مقدمي الخدمات الافتراضية منظمون لأغراض مكافحة غسل الأموال وتمويل الإرهاب¹، ويكون على المؤسسات المالية التي تصدر الأوامر أن تحتفظ بالمعلومات اللازمة لتحديد هوية جميع القائمين بالتحويلات المالية، واتاحتها عند الطلب للسلطات العامة، وأن تكفل عدم الدخول في معاملات مالية غير الاعتيادية حيثما يؤدي ذلك إلى زيادة خطر تبييض الأموال أو تمويل الإرهاب²، كما أن التطور التكنولوجي الحاصل أدى إلى ظهور قطاع مالي ذكي يشجع فيه استعمال ما توفره التكنولوجيا التي تيسر جمع البيانات وتجهيزها وتحليلها ومساعدة الجهات الفاعلة في تحديد وإدارة عمليات تبييض الأموال وبصورة فعالة وأقرب إلى الوقت الحقيقي، وتساهم في تسريع المدفوعات

¹. RECOMMENDATIONS, F. A. T. F, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 2012-2022, p17, available at: www.fatf-gafi.org/recommendations.html, (accessed 23november2021).

². Financial Action Task Force, Interpretative Note to Special Recommendation VII: Wire Transfers, 2004, p02, available at: <https://www.osce.org/files/f/documents/5/2/25888.pdf>, (accessed 24november2021).

والمعاملات من خلال نظم تحديد الهوية والرصد وحفظ السجلات وتبادل المعلومات، وفي نفس الوقت تتيح السلطات المختصة العديد من المزايا، فالحلول الرقمية لمكافحة تبييض الأموال تقوم على أساس الذكاء الاصطناعي¹.

الفرع الثاني: تدابير في مجال البطاقات الذكية

تتيح البطاقات النقدية تبييض الأموال السرياني كما تم تبيانها سابقا، ويمكن التخفيف من الفرص التي تمنحها عبر تقييم المخاطر المحتملة لتبييض الأموال من جراء برنامج البطاقات المسبقة الدفع، بالنظر في سمات كل برنامج، بما في ذلك القيود المفروضة على مصدر ومبلغ الأموال الموضوعة على البطاقات، وكيفية استخدامها، وعدد البطاقات التي يمكن أن يمتلكها شخص واحد²، هذا التحليل للسمات وغيرها من العوامل المادية تساعد في تحديد ومعرفة أن الاستخدام لغاية تبييض الأموال، كما أن الافتقار إلى المعلومات ذات الصلة عن حامل البطاقة مثل الاسم والعنوان وتاريخ الميلاد ورقم الهوية الفريد الذي تصدره الحكومة يشكل خطورة على جمع المعلومات وتوفيرها والتحقق منها في مجال الرقابة على التحويلات المالية، ويمكن أن تقلل المعلومات المتعلقة بحاملي البطاقات من توخي الحرص الواجب في معرفة نوع العملاء، وتساهم في معرفة الغرض من البطاقات ومستخدامها.

ويمكن تحديد استخدام البطاقة من خلال تصميم البرمجة للبطاقة المدفوعة مسبقا بحيث يقتصر استخدامها على نطاق معين سواء تاجر أو مؤسسة تسوق مثل "مركز تجاري"، ذلك أن البطاقة المفتوحة على جميع المعاملات تكون وسيلة ناجحة في تبييض الأموال السرياني³.

¹. FATF, Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, July 2021, p. 04., available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>, (accessed 25 November 2021).

². Wolfsberg Group. (2011). *Wolfsberg Guidance on Prepaid and Stored Value Cards*, p05, Available at: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/11.%20Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14%2C_2011.pdf, (accessed 26 November 2021).

³. *Ibid.*, p. 07.

الخاتمة:

نستخلص من هذه الدراسة بأن جريمة تبييض الأموال السيبراني تعد فريدة من نوعها، فهي من الجرائم الخطيرة التي نتجت من تزاوج بين الجريمة الاقتصادية والجريمة الإلكترونية، وترقى في خطورتها للجريمة المنظمة، وتشكل تحدياً جديداً لاقتصاديات الدول لاسيما النامية منها وعائق نحو التنمية المحلية، ويكون على المشرع الجزائري معالجة الظاهرة وحصرها حتى يكون لرجال إنفاذ القانون التصدي لها ومكافحتها.

وتميزت جريمة تبييض الأموال السيبراني بطبيعة خاصة تجلت من خلال صعوبة تحديد مفهوم لها، ونظراً لكونها اجرام مستحدث يضم في شقه الثاني الاجرام الإلكتروني، ولتنوع أساليب الاجرام الذي يقوم على ما تقدمه التكنولوجيا من وسائل تتطور من يوم الى اخر، ونجد بأن المشرع الجزائري في تجريمه لتبييض الأموال السيبراني ظل يكتفه الغموض مما يعيق منع هذا الاجرام، وعليه نقترح بعض التوصيات، كالآتي:

1. إصدار قانون خاص بالجرائم الاقتصادية الإلكترونية وإدراج فيه الأفعال الإجرامية التي تتطوي على تبييض الأموال عبر الوسائط الإلكترونية، أو الاكتفاء صراحة بتجريم تبييض الأموال السيبراني في قانون العقوبات التزاماً بمبدأ الشرعية في المادة الأولى الذي يقتضي أن يكون التجريم دقيقاً وواضحاً.
2. ضرورة الاهتمام بالأدلة الجنائية الإلكترونية، ولا سيما داخل المؤسسات المالية، لأن القدرة على كشف وحفظ أدق الأدلة الإلكترونية هي الحد الأدنى المطلوب لاحتواء ظاهرة تبييض الأموال السيبراني بشكل ملائم.
3. ضرورة إنشاء مراكز لتحليل الأخطار الحاسوبية في جميع المؤسسات المالية، سواء في إطار ولاية وطنية أو دولية، ومن شأنها أن تمكن المؤسسات المالية من تبادل المعلومات الاستخبارية عن التهديدات الإلكترونية مع المؤسسات المالية الأخرى.
4. تكوين إطارات الأجهزة المعنية بمتابعة هذه الجرائم، وتخصيص فرق من الشرطة خاصة بالجرائم الاقتصادية الإلكترونية.
5. تعزيز التعاون الأمني والمخابراتي مع جميع الدول التي لها خبرة في هذا النوع من الجرائم، ولا سيما التعاون الشرطي في منظمة الإنتربول.
6. عقد مؤتمرات وندوات علمية لتبادل المعارف والتعريف بخطورة هذا النوع من الجرائم الاقتصادية الإلكترونية.

قائمة المراجع**باللغة العربية:****أولاً: الكتب**

- أحمد محمد العمري، جريمة غسل الأموال: نظرة دولية لجوانبها الاجتماعية والنظامية والاقتصادية، العبيكان للنشر، الرياض، سنة 2000.



- أحمد عبد التواب محمد بهجت، إبرام العقد الإلكتروني "دراسة مقارنة"، دار النهضة العربية، مصر، سنة 2009.
 - ثامر عبد الجبار عبد العباس السعيد، التنظيم القانوني للمزاد الإلكتروني، دراسة مقارنة، المركز العربي للنشر والتوزيع، مصر، سنة 2018.
 - طارق طه، إدارة البنوك في بيئة العولمة والانترنت، دار الجامعة الجديدة، مصر: الإسكندرية، سنة 2007.
 - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، سنة 2000.
 - عبد العزيز خنفوسي، قانون الدفع الإلكتروني، مركز الكتاب الأكاديمي، سنة 2018.
 - محسن أحمد الخضير، غسيل الأموال: "الظاهرة - الأسباب - العلاج"، مجموعة النيل العربية، القاهرة، سنة 2003.
 - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، سنة 2004.
 - هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، سنة 1992.
- ثانيا: مواقع الإنترنت**
- وكالة الأنباء الجزائرية (APS)، ارتفاع عدد أجهزة الدفع الإلكتروني بنسبة تقارب 30 بالمائة إلى غاية الفصل الأول من 2021. في 01 أكتوبر 2021، تم الاسترداد من وكالة الأنباء الجزائرية: <https://www.aps.dz/ar/economie/106428-30-2021>
 - المؤسسة العمومية للتلفزيون الجزائري (ENTV)، الوزير الأول يشرف على مراسم توقيع اتفاقية إطلاق خدمة الدفع الإلكتروني عبر الإنترنت، في 30 ديسمبر 2021، تم الاسترداد من: <https://www.entv.dz/117928-2>

رابعا: النصوص القانونية

- قانون رقم 18-05 مؤرخ في 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، صادر في 16 مايو سنة 2018.
- قانون رقم 06-01 مؤرخ في 20 فبراير سنة 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 14، صادر في 08 مارس سنة 2006.
- قانون رقم 09-04 مؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، صادر في 16 غشت سنة 2009.

باللغة الأجنبية:

1. Ouvrages :

- CHAWKI, Mohamed, et al. *Cybercrime, digital forensics and jurisdiction*. Springer, 2015.
- DU QUÉBEC, Sûreté; FORTIN, Francis. *Cybercriminalité: Entre inconduite et crime organisé*. Presses inter Polytechnique, 2013.
- Financial Action Task Force. *COVID-19-Related Money Laundering and Terrorist Financing: Risks and Policy Responses*. 2020.
- Financial Action Task Force. GAFI. *Report on New Payment Methods*. Paris: FATF. 2006.
- KLIMMT, Christoph. *Virtual worlds as a regulatory challenge: A user perspective*. In: *Virtual worlds and criminality*. Springer, Berlin, Heidelberg, 2011.
- LESLIE, Daniel Adeoyé. *Legal principles for combatting cyberlaundering*. Springer, 2014.
- O'MAHONY, Donal; PIERCE, Michael; TEWARI, Hitesh. *Electronic payment systems for e-commerce*. Artech, 2001.
- MOLANDER, Roger C.; MUSSINGTON, David; WILSON, Peter A. *Cyberpayments and money laundering: Problems and promise*. Rand Corporation, 1998.
- PARKER, D. B.; PARKER, D. *Crime by computer*. Scribner New York. 1976.
- HALDANE, Andrew G.; SAPORTA, Victoria (ed.). *The future of payment systems*. Routledge, 2008.

2. Article :

- Financial Action Task Force. *Money laundering. Policy Brief July 1999*.
- FILIPKOWSKI, Wojciech. *Cyber Laundering: An Analysis of Typology & Techniques*, *Internat-ional Journal of Criminal Justice Sciences*, 2008, 3.1.
- WALL, David S. *Policing cybercrimes: Situating the public police in networks of security within cyberspace*. *Police Practice and Research*, 2007, 8.2.
- VLASOV, A. V. *The Evolution of E-Money*, "European Research Studies", 20(1), 2017.

3. Documentation électronique:

- Wikipedia, *the free encyclopedia*, *Massively multiplayer online role-playing game*, available at: https://en.wikipedia.org/wiki/Massively_multiplayer_online_role-playing_game. (accessed 01 november 2021)
- SECONDLIFE, Available at: <https://www.secondlife.com> (22 november 2021)
- RECOMMENDATIONS, F. A. T. F, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris,



- France, 2012-2022, available at: www.fatf-gafi.org/recommendations.html, (accessed 23 november 2021).
- Financial Action Task Force, Interpretative Note to Special Recommendation VII: Wire Transfers, 2004, available at: <https://www.osce.org/files/f/documents/5/2/25888.pdf>, (accessed 24 november 2021).
 - FATF, Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, July 2021, available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>, (accessed 25 november 2021).
 - Wolfsberg Group. (2011). *Wolfsberg Guidance on Prepaid and Stored Value Cards*, Available at: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/11.%20Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14%2C_2011.pdf, (accessed 26 november 2021).