مجلة طبنـــة للدراسات العلمية الأكاديميةISSN 2661-7633 / EISSN 2716-8883

السنة: 2021 المجلد: 04 العدد: 03 ص.ص: 1218-1240

آليات مواجهة المخاطر القانونية المترتبة عن استخدام وسائل الدفع الالكتروني

Mechanisms to address the legal risks arising from the use of electronic payment methods

سماح محمودي، المركز الجامعي بريكة ، (الجزائر)، mahmoudisamah@yahoo.fr

تاريخ إرسال المقال: 21-08-2021 تاريخ قبول المقال: 03-10-2021

ملخص:

يترتب على المعاملات الالكترونية استخدام وسائل لعل أهمها وسيلة الدفع الالكتروني، وتعد المخاطر القانونية أهم ما يمكن أن يواجه الدفع الالكتروني والتي تنشأ عن الاستغلال غير المشروع لهذه الوسيلة أو ما قد يقوم به بعض المتعاملين من أعمالا احتيالية و متعسفة.

توصلت الدراسة إلى أن وقوع المخاطر القانونية المترتبة عن استخدام وسائل الدفع الالكتروني مرده قصور النصوص القانونية مع ووجود ثغرات بها وعدم مواكبة التشريعات والقوانين للتطورات التكنولوجية الفائقة والتي لا يمكن استيعابها بشكل مطلق في هذا المجال، وذلك رغم الجهود الوطنية والدولية لجعل وسيلة الدفع الالكتروني أكثر أمانا مع محاولة وضع خطط واستراتيجيات وتدابير للتغلب عليها ومواجهتها.

الكلمات المفتاحية: الدفع الالكتروني ـ المخاطر القانونية ـ التكنولوجية ـ تبييض الاموال.

Abstract :

Electronic transactions result in the use of means, perhaps the most important of which is electronic payment, and legal risks are the most important that can be faced by electronic payment arising from the illegal exploitation of this method or the fraudulent and abusive actions that some dealers may carry out.

The study found that the legal risks arising from the use of electronic payment methods are due to the lack of legal texts with gaps in them and the failure to keep pace with legislation and laws for high-tech developments that cannot be fully absorbed in this area, despite national and international efforts to make the electronic payment method safer while trying to develop plans, strategies and measures to overcome and confront them.

Keywords: Electronic payment - technology - legal risks- money laundering.

مقدمة:

أصبحت المعاملات في مجال التجارة في عصرنا هذا تتم عبر الوسائط الإلكترونية التي تعبر عن ممارسة تجارة جديدة التجارة الإلكترونية، ونظرا لما تتطلبه هذه الأخيرة من سرعة وأمان في التعامل، فقد استفاد المتعاملين الاقتصاديين من هذه التكنولوجيات والتقنيات الحديثة التي وفرت لهم السرعة في التعامل و الآمان.

وعلى ذلك لجأت البنوك والمؤسسات المالية إلى استعمال التقنيات والوسائط الإلكترونية وقامت بابتكار خدمات مصرفية مستحدثة تتمثل في وسائل ونظم دفع حديثة، حيث قامت هذه المؤسسات المالية باستحداث عدة وسائل وأدوات جديدة متطورة للدفع والتي من شأنها السماح لعملائها بالقيام بعمليات الدفع والسحب بواسطة وسائل الدفع الإلكترونية بمختلف أنواعها، وذلك بتسخير كل ما لديها من إمكانيات بشرية ومادية لتطوير هذه الوسائل من أجل تقديم خدمات ذات جودة عالية لزبائنها وعملائها، وقد تزايد حجم التعامل بوسائل الدفع الالكتروني كوسيلة حديثة للوفاء حيث أقبل عليها العديد من العملاء في تسوية معاملاتهم المالية نظرا لما توفره من عن تجنب الأضرار التي تترتب على حمل النقود.

ومع ذلك فإنه تعتري وسائل الدفع الالكتروني بعض المخاطر بحكم البيئة الرقمية المفتوحة التي تمارس فيها بلا حدود مكانية ولا زمانية، غير أنه تزايدت هذه الأخطار وأثارت اهتمام المجرمين والقراصنة الذين حققوا منها أرباحا جد خيالية من عمليات النصب والاحتيال على المتعاملين بها، وهذا ما أدي بالقانونيين والباحثين و القائمين في المجال التكنولوجي بالتصدي لتوفير اكبر قدر من الحماية والأمان لوضع برامج و أنظمة تقنية لمنع كافة المخاطر التي تشوب استعمال وسائل الدفع الالكترونية.

ومن ذلك تنقسم المخاطر الى نوعين من المخاطر، مخاطر أمنية والتي يمكن أن تحدث بهدف تحقيق أهداف غير مشروعة تتعلق بالأنظمة التقنية لوسائل الدفع نفسها وتتعلق بالجانب الوظيفي لها، وهناك المخاطر القانونية التي يمكن أن تنشأ على الرغم من مراعاة الجوانب التقنية لهذه الوسائل من خلال انتهاك القوانين والتشريعات مثل جرائم غسيل الاموال و إفشاء أسرار العميل وانتهاك السرية والخصوصية من خلال استغلال ما قد ينشأ من ثغرات في النصوص القانونية أو حتى غياب هذه النصوص، وما يندرج ضمن ذلك من ضرورة اتخاذ تدابير للوقاية وسبل مواجهتها، وهي الجوانب من المخاطر القانونية التي تهمنا بالدراسة.

يكتسي الموضوع أهميته من شيوع التعامل بوسائل الدفع الالكتروني، وما صاحب هذا الانتشار من محاولات للاعتداء اللامشروع من قبل المجرمين في هذا المجال بسلب الاموال والاعتداء على خصوصية المتعاملين، وما يستدعي ذلك من ضرورة اقرار التشريعات نظاما قانونيا متميزا وخاصا يضفي حماية خاصة لهذه التعاملات، ذلك تجنبا لأي استخدام غير مشروع يؤدي الى خسائر مالية فادحة. الامر الذي يحتاج الى وسائل فنية واخرى قانونية تعزز من وجود بيئة آمنة يشجع كل من الافراد والمؤسسات على التعامل بهذا النوع من الوسائل الالكترونية ويبعث الثقة والطمأنينة للتعامل بها.

وانطلاقا من ذلك نطرح **اشكالية الدراسة** كما يلي: فيما تتمثل المخاطر القانونية التي تترتب على استخدام وسائل الدفع الالكتروني وكيف تتم مواجهتها؟

يهدف الموضوع الى معرفة المبادئ والقواعد القانونية التي تحكم الدفع الالكتروني باعتباره موضوعا حديثا، وتسليط الضوء على بعض الجوانب التي تشكل مخاطر قانونية من أجل ايجاد الحلول التي توفر مزيدا من الامان للمتعاملين في هذا المجال، حيث أن وسائل الدفع وتحديثها له أهمية كبيرة في تطوير النظام المصرفي والتقدم به نحو الامام.

يتبع في الدراسة المنهج التحليلي وذلك بتحليل مختلف المبادئ والقواعد التي تخضع لها وسائل الدفع الالكتروني وعرضها لمعرفة مدى كفالتها لمواجهة المخاطر الناشئة عنه، كما نتبع المنهج الوصفي بوصف مختلف القواعد والاوضاع والحالات التي يكون عليها الدفع الالكتروني.

سوف تتم معالجة الموضوع من خلال تقسيمه الى مباحث ومطالب وفروع، وذلك بعرض الجوانب المتعلقة بمواجهة المخاطر الناشئة عن استخدام وسائل الدفع الالكتروني في المبحث الاول، مواجهة المخاطر القانونية المترتبة عن حالات استخدام وسائل الدفع الالكتروني في المبحث الثاني.

المبحث الأول: الجوانب المتعلقة بمواجهة المخاطر الناشئة عن استخدام وسائل الدفع الالكتروني

بالإضافة الى مجموعة المخاطر التي قد تثيرها وسائل الدفع الالكترونية و منها المخاطر الأمنية المتعلقة بالجانب الأمني والتقني، تثار بعض المخاطر القانونية التي تسببها وسائل الدفع الالكتروني والتي تنشأ من خلال مخالفة النصوص القانونية والتنظيمات كجرائم غسيل الاموال وإفشاء أسرار العميل وانتهاك السرية، وقد تتولد هذه المخاطر القانونية أيضا عندما تنص القوانين على حقوق و التزامات الاطراف المتعاقدة بطريقة غامضة، ومن ذلك فإن موضوع حماية العملاء والزبائن يعد من أهم المخاطر القانونية التي يمكن أن يفرزها التعامل بهذه الوسائل الالكترونية.

ومن المتوقع أيضا ان يصاحب انتشار الدفع الالكتروني تزايد في جرائم التهرب الضريبي، حيث سيكون من الصعب على الجهات الحكومية المكلفة بتحصيل الضرائب القيام بربط الضريبة على تلك الصفقات التي تتم بواسطة الدفع الالكتروني، نظرا لان تلك الصفقات تتم خفية عبر شبكة الانترنت[1] .

وعليه فان توسع استخدام وسائل الدفع الالكترونية مرهون بوجود حماية قانونية محكمة، وأيضا حماية تقنية فعالة باستعمال وسائل تقنية معينة مما يمكن من مواجهة كل المخاطر المحتملة التي تحصل للمتعاملين بوسائل الدفع الالكتروني من حيث أدائها لوظائفها مثلا أو إساءة استخدامها بمحاولة تقليدها أو التعديل في بياناتها.

لذا ولدراسة الاجراءات الخاصة بمواجهة المخاطر الناشئة عن استخدام وسائل الدفع الإلكترونية، يقتضي الأمر التعرف على تدابير مواجهة و مكافحة مخاطر أمن المعلومات، ثم معالجة الاجراءات الخاصة ووسائل مكافحة المخاطر القانونية، فالآليات المؤسساتية لمكافحة الجرائم المتعلقة بالدفع الالكتروني في الجزائر، نقوم بعرض هذه المسائل من خلال المطلبين المواليين:

المطلب الاول: مواجهة مخاطر أمن المعلومات المتعلقة بالدفع الالكتروني

يعرف أمن المعلومات بأنه حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها والأجهزة التقنية المستعملة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة ويتم بها سلامة المعلومات وهي

[1] محمد ابراهيم محمود الشافعي: النقود الالكترونية، الهيئة العليا لتطوير الرياض، المال والاقتصاد مقال منشور على الموقع: www.amadh.com!:(

الامر المهم الذي وجبت المحافظة عليه، ومن خلال ذلك يمكن اكتشاف امكانية حدوث عمليات احتيالية وتحديد مصدرها[1].

وهناك ما يعرف بتدابير الاحتواء فهي ترمي إلى الحد من نطاق النصب المرتكب عقب اكتشافه، كما أنه لتدابير الكشف والاحتواء مهمة رادعة أيضا تساعد في منع الغش، و يضاف الى ذلك أن بعض الاجراءات الأمنية لا سيما تقنيات التشفير أو الترميز التي تعتبر ذات صفة حساسة بالنسبة لأمن منتجات وسائل الدفع الالكتروني طوال مراحل الوقاية والكشف والاحتواء [2].

وسيتم دراسة هذه المظاهر بعرض التدابير الوقائية للحماية التقنية في الفرع الاول، ليتم عرض آليات الحماية التقنية للدفع الالكتروني في الفرع الثاني.

أولا: تدابير الحماية التقنية لاستخدام وسائل الدفع الالكتروني

إن استعمال وسائل الدفع الالكتروني يمكن أن يعترضه العديد من المخاطر ذات الطابع الامني وهو ما يؤثر على ثقة المتعاملين به، لذلك فإن اغفال معالجة هذه المخاطر من شأنه تهديد مستقبل العمل بوسائل الدفع الحديثة، وفي سبيل ذلك تقوم معظم الهيئات والمؤسسات المصدرة لهذه الوسائل بعملية إجراء تقييم للمخاطر بصورة كافية وسريعة لمنع تفاقمها والعمل على ابتكار تقنيات و آليات تكنولوجية متطورة للعمل على معالجة تلك المخاطر الأمنية المتعلقة بحصول اختراقات النظام و مقاومة العمليات الاحتيالية.

وهو ما يعرف ايضا بالحماية التقنية للدفع الالكتروني، والتي يقصد بها جميع وسائل الحماية والتدابير التقنية التي نستهدف حماية نظام الدفع الالكتروني من أي اعتداء على انظمة المعلومات الخاصة به بحماية المواقع الالكترونية والبرمجيات ومصنفات الحاسب الآلي، وكذلك حماية قاعدة البيانات ببنك المعلومات.

كما يقصد بالحماية التقنية أو الفنية للدفع الالكتروني ايضا ذلك الاجراء الوقائي الذي يتخذه مصدر وسيلة الدفع الالكتروني او صانعها اثناء وضعه لها للحد من الاعتداءات الخارجية التي تقع عليها[3]،

[1] محمد دباس الحميد، ماركة ابراهيم نينو، حماية أنظمة المعلومات، دار الحامد للنشر و التوزيع، عمان 2007، ص: 34.

[2] حوالف عبد الصمد: حوالف عبد الصمد: النظام القانوني لوسائل الدفع الالكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2015/2014.ص: 435.

[3] خثير مسعود: الحماية الجنائية لبرامج الكمبيوتر . أساليب وثغرات . دار الهدى، الجزائر 2010، ص: 111.

حيث تعمل هذه الحماية الفنية التقنية على ايجاد انظمة آمان لحماية نظم المعلوماتية وتقنية المعلومات المتداولة عن طريق الشركات المنتجة للبرامج[1] . وعموما تتمثل التدابير في العمل على مقاومة العبث في الأجهزة ، ثم تشفير البيانات كوسيلة لتأمين الدفع الالكتروني ، فكيفية الحصول على الترخيص بالاستعمال.

وكان لزاما على مختلف الدول وكذا المؤسسات المصدرة لوسائل الدفع الالكتروني إجراء تقييم لهذه المخاطر بصورة كافية وسريعة لمنع تفاقمها والعمل على ابتكار تقنيات و آليات تكنولوجية متطورة للعمل على معالجة تلك المخاطر الامنية عن طريق أدوات القرصنة التي تهدد الامن المعلوماتي وتستوجب الحماية التقنية، حيث نجد ان الكثير من نظم الكمبيوتر التي تعتمد عليها انظمة الدفع الحديثة لا تزال غير مؤمنة بشكل مثير للدهشة حيث يلجأ المخزنين والقراصنة الى استخدام مجموعة متنوعة من الادوات والتقنيات للتغلب على مشكل الامن [2].

وما يمكن قوله من الناحية العملية ان كثير من النظم المعلوماتية التي تعتمد عليها أنظمة الدفع الحديثة لاتزال غير مؤمنة بشكل مثير للدهشة، لان المجرمون والقراصنة المعلوماتيون يلجأون إلى استخدام مجموعة من الأدوات والتقنيات للتغلب على البرامج الأمنية المعدة.

ثانيا: آليات الحماية التقنية للدفع الالكتروني

تكتسي حماية المعلومات الالكترونية الخاصة بنظام الدفع الالكتروني والمتداولة عبر شبكة الانترنت أهمية كبيرة لما يشكله المساس بها من آثار على الذمة المالية لعملاء البنك وعلى سمعة هذا الاخير، وما يمكن ان ينتج عن ذلك من خسائر مالية[3].

إن أهم الوسائل المستعملة في تأمين الدفع الالكتروني هي الآليات التي تعمل على توفير أكبر قدر من الثقة والاطمئنان، حيث تستعمل تقنيات لأجل حماية وتحديد الهوية والتحقق منها وتتمثل في نظام

[1] طارق ابراهيم الدسوقي عطية: الموسوعة الامنية، الامن المعلوماتي، النظام القانوني لحماية المعلوماتية، درا الجامعة الجديدة، الاسكندرية، ص: 549.

[2] هداية بوعزة: النظام القانوني للدفع الالكتروني . دراسة مقارنة ـ أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2019/2018.ص: 372.

[3] يقصد بأمن المعلومات حماية أصول وموارد ومكتسبات أي نظام معلوماتي ما بطرق مشروعة. وهو ايضا اداة تتحكم في تنظيم البيانات والعلاقات والاتصالات وذلك دون ان يؤثر على قدرة مستخدمي هذا النظام على الاداء أو يعوق عملهم من حيث الكفاءة او التوقيت، راجع طارق ابراهيم الدسوقي، المرجع السابق، ص: 489.

الارقام والكلمات السرية ونظام التشفير. وعليه فإن العبث بمحتوى هذه المعلومات الالكترونية قد يتخذ منها انتحال الغير شخصية أحد العملاء عن طريق سرقة كلمات السر أو تسجيل أحد الرسائل وإعادة ارسالها، ناهيك عن امكانية اختراق الموقع والاستخدام غير المرخص به والعبث بمحتوياته.

غير انه مع التطور المسجل في وسائل ارتكاب الجريمة المعلوماتية وتنوع الوسائل التي قد يلجأ إليها المجرمون، أصبحت تقنيات التحقق من الشخصية غير كافية خاصة اذا قام المجرمون باستخدام طرق أخرى للسطو على الحسابات غير تلك القائمة على سرقة كلمات السر [1]. لذلك سعى العاملون في الميدان الالكتروني الى ابتكار وسائل حديثة لحماية أمن وسرية المراسلات والمعلومات عن طريق تشفيرها وبحماية المواقع الالكترونية والشبكات الداخلية عن طريق جدران الحماية.

والمقصود بتقنية التشفير هو فن حماية المعلومات عن طريق تحويلها الى رموز معينة غير مقروءة لا يمكن حلها الا من خلال مفتاح سري يقوم بتحويل تلك الرموز الى نص عادي مقروء، فهو تغيير لمظهر المعلومات بحيث يختفي معناها الحقيقي من خلال إخفائها عن كل من ليست له صفة الاطلاع عليها أو العبث بمحتوياتها بتغيير شكلها الى صورة لا يمكن فهمها إلا بعد ارجاعها إلى صورتها الأصلية، ولا يتحقق ذلك إلا باستخدام مفتاح معين لا يملكه الا صاحب الحق في الاطلاع على المعلومات[2].

كما تعتبر الحماية بواسطة الرقم السري الإجراء المؤمن الأكثر استعمالا في المجال الرقمي في وقتنا الحالي، إذ ان إجراءات فتح النافذة و استعمال الرقم السري الشخصي يسمح لصاحب البرامج التأكد من هوية المستعمل الذي يحاول الدخول الى العنوان الالكتروني أو جزء منه، وذلك عند محاولة الدخول لنافذة مؤمنة بحيث لا يسمح له بذلك الا عند تقديم الرقم السري الصحيح الذي بموجبه يمكن الولوج للمعطيات والبيانات السرية والشخصية[3].

ولكي يحقق هذا الاسلوب الهدف المرجو منه لابد من توعية المستخدمين بالاحتفاظ الشخصي لكلمات المرور وعدم الافصاح عنها امام الغير، غير انه ما يعاب على هذا الاسلوب إمكانية اختراق

[1] محمد عبد الصمد: الجريمة المعلوماتية والاحتساب عليها، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد الثالث 2000، ص: 875.
[2] طارق ابراهيم الدسوقي عطية: المرجع السابق، ص:398
[3] حسن طاهر داوود: الحاسب أمن المعلومات، معهد الادارة العامة، مكتبة فهد الوطنية، الرياض، ص: 23.

وكسر كلمات المرور بسهولة تامة بواسطة برامج خاصة يجعل عدد لا نهائي من المحاولات حتى يتم التوصل الى الكلمات الصحيحة[1] .

المطلب الثاني: الآليات التشريعية و المؤسساتية لمكافحة الجرائم المتعلقة بالدفع الالكتروني في الجزائر

في اطار الاستراتيجية الوطنية التي انتهجتها الجزائر لمكافحة الاجرام المعلوماتي والمساس بمنظومة المعلومات باستخدام اجهزة وهيئات متخصصة تهتم بتقصي الجريمة السيبيرانية ومكافحته، بالاضافة الى جملة من القواعد التشريعية الخاصة التي تضمنت مبادئ متعلقة بالدفع الالكتروني لمحاربة الجرائم الخاصة به، نستعرض أولا الآليات التشريعية ثم الآليات المؤسساتية في كل فرع مستقل.

أولا: الآليات التشريعية لمكافحة الجرائم المتعلقة بالدفع الالكتروني في الجزائر

هناك تشريعات عديدة استهدفت الاجرام المعلوماتي أو تضمنت قواعد تتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا بالاعلام والاتصال نذكر من بينها:

1- قانون البريد والاتصالات السلكية والاسلكية، حيث نص في المادة 187 منه على امكانية اجراء التحويلات المالية الكترونيا واستعمال حوالات الدفع العادية الالكترونية، كما نصت منه المادة 105 على احترام المراسلات[2] .

2- قانون التأمينات، كما اهتم التشريع المتعلق بالتأمينات على تنظيم الجريمة الالكترونية من خلال مؤسسات وهيئات الضمان الاجتماعي، وذلك في عدة نصوص تخص البطاقة الالكترونية، حيث قام المشرع الجزائري باعتماد البطاقات الالكترونية بموجب القانون رقم 01/08 الذي تمم القانون رقم 11/83 المتعلق بالتأمينات الاجتماعية [3].

3- القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

لقد بادر المشرع باصدار هذا القانون من أجل توفير البيئة الملائمة لتداول المعلومات الكترونيا وتأمينها من الاستخدام غير المشروع لتقنية المعلومات، حيث نص فيه على عدة قواعد خاصة بمكافحة

[1] سعيدي عزوز، راكول خالد: الامن التقني للدفع الالكتروني، أية فعالية؟ مقال منشور في مجلة معالم للدراسات القانونية والسياسية، العدد الثاني، ديسمبر 2017،ص: 123.

[2] القانون رقم 03/2000 الملغى المؤرخ في 5 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، جريدة رسمية عدد 48 لسنة2000.

[3] القانون رقم 01/08 المؤرخ في 23 يناير 2008 المتمم للقانون رقم 11/83 المؤرخ في 02 يوليو 1983 والمتعلق بالتأمينات الاجتماعية، جريدة رسمية عدد 04 لسنة 2008.

الجريمة الالكترونية والتي لها علاقة بالدفع الالكتروني كتحديده للحالات التي يسمح فيها باللجوء الى المراقبة الالكترونية.

كما نص على مجموعة من القواعد الاجرائية التي تتماشى وطبيعة الجرائم الالكترونية مثل القواعد الاجرائية المتعلقة بتفتيش المنظومة المعلوماتية وحجز المعطيات المعلوماتية[1] .

4- قانون التوقيع والتصديق الالكترونيين[2] ، فقد اعترف بموجب هذا القانون بحجة التوقيع الالكتروني في اثبات المعاملات الالكترونية واثبات هوية الموقع وذلك بموجب المادة 6 منه. ومن خلال هذا القانون حاول المشرع إرساء الثقة وحماية البيانات الشخصية وتأمينها في البيئة الافتراضية وتجسيد التجارة الالكترونية، وكذا الدفع الالكتروني لانه يستمد منه أحكاما عديدة.

5- قانون التجارة الالكترونية [3]، يحدد هذا القانون القواعد العامة المتعلقة بالتجارة الاكترونية للسلع والخدمات وتضمن مجموعة من المفاهيم حول الدفع الالكتروني حيث عرفه في المادة 6 منه على انه كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب او عن بعد عبر منصة الكترونية.

ونظم في الفصل السادس منه عملية الدفع في المعاملات الالكترونية التي تتم إما عن بعد و إما عند تسليم المنتوج او عن طريق وسائل الدفع المرخص بها قانونا (المادة 1/27).

كما نظم هذا القانون طريقة الدفع الالكتروني التي تتم بين المستهلك الالكتروني والمورد لأجل أمن المعاملة، و اوجب أن يكون وصل موقع الانترنت الخاص بالمورد الالكتروني بمنصة الكترونية مؤمنا بواسطة نظام التصديق الالكتروني، كما اخضع هذه المنصات لرقابة بنك الجزائر وجوبا لضمان استجابتها لمتطلبات الامن البيئي وسرية البيانات وسلامتها و امن تبادلها[4] .

---

[1] المادتين 5 و6 من القانون رقم 04/09 المؤرخ في 5 اوت 2009، جريدة رسمية عدد 47 لسنة 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال و مكافحتها.

[2] القانون رقم 04/15 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فبراير 2015، الجريدة الرسمية عدد 6 لسنة 2015- يحدد القواعد العامة الماعلقة بالتوقيع والتصديق الالكترونيين.

[3] القانون رقم 05/18 المؤرخ في 24 شعبان 1439 الموافق لـ 10 ماي 2018، الجريدة الرسمية عدد 28 لسنة 2018، يتعلق بالتجارة الالكترونية.

[4] المادتين 28 و 29 من قانون التجارة الالكترونية رقم 05/18 السابق الاشارة اليه.

ثانيا: الآليات المؤسساتية لمكافحة الجرائم المتعلقة بالدفع الالكتروني في الجزائر:

وتتمثل هذه الاجهزة في ما يلي:

1- مركز الوقاية من جرائم الاعلام الآلي وجرائم المعلوماتية للدرك الوطني

أنشأ هذا المركز سنة 2008 لأجل تأمين منظومة المعلومات لخدمة الامن العمومي، ويعد بمثابة مركز نوثيق يقوم بتحليل المعطيات والبيانات للجرائم الالكترونية المرتكبة، وقد استطاع الجهاز معالجة عدد كبير من الجرائم الالكترونية بفضل التركيبة البشرية المؤهلة التي يتوفر عليها من التكوين المستمر والملتقيات الدولية و الوطنية وتبادل الخبرات مع الدول الاخرى.

2- المعهد الوطني للادلة الجنائية وعلم الاجرام

تقوم دائرة الاعلام الآلي والالكتروني التابعة للمعهد و المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة مع تقديم المساعدة للمحققين في جرائم المعلوماتية.

يضم المعهد عدة تجهيزات تتمثل في محطة ترميم وتصليح الاجهزة والحوامل المعطلة، الشبكات الاعلامية والتجهيزات البيانية، بالإضافة الى محطة محمولة وثابتة لإجراء خبرات الإعلام الألي، ويحتوي على قاعات مختلفة كلها تتعلق بمختلف انظمة الاعلام الالي.

3- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني

حيث قامت مصالح الامن بإنشاء المصلحة المركزية للجريمة الالكترونية استجابة لمتطلبات الامن السيبيراني ومكافحة التحديات الامنية الناجمة عن جرائم الكترونية وقد تم انشاؤه سنة 2011 وأضيف الهيكل التنظيمي في سنة 2015 [1]

4- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

استحدثت هذه الهيئة وفقا للقانون 04/09 السابق الذكر حيث تتولى هذه الهيئة طبقا لمادة 14 من هذا القانون مجموعة كبيرة من المهام[2].

[1] حوالف عبد الصمد: المرجع السابق،ص: 460.

[2] القانون رقم 04/09 السابق الذكر و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال و مكافحتها

حيث صدر فيما بعد المرسوم الرئاسي رقم 172/19 ليحدد تشكيلة الهيئة الوطنية وتنظيمها وكيفيات سيرها[1].

وقد اعتبر هذا المرسوم ان الهيئة مؤسسة عمومية ذات طابع اداري تتمتع بشخصية عمومية والاستقلال المالي موضوعة تحت سلطة وزارة الدفاع الوطني[2] .

وتنص المادة 9 من المرسوم اعلاه على ان تتولى المديرية العامة السهر على حسن سير الهيئة وتضطلع بمهمة إعداد مشروع ميزانية الهيئة واعداد وتنفيذ برنامج عمل الهيئة وتنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة، كما تعمل على تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما، كما تقوم بتبادل المعومات مع مثيلاتها الاجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم الالكترونية والتعرف عليهم، كما تعمل على تحضير اجتماعات مجلس التوجيه واعداد التقرير السنوي لنشاط الهيئة.

وكخلاصة حول دور وعمل المؤسسات في مواجهة المخاطر الالكترونية يمكن القول انه توجد وسائل ادارية لاحتواء الاعمال الاحتيالية بواسطة اجراءات خاصة ووضع تدابير لمنع حدوث أعمال احتيالية تخترق انظمة الدفع الالكترونية، لكنها تبقى غير كافية لمواجهة مثل هذه المخاطر، لذلك تقوم التدابير المعتمدة من قبل هذه الانظمة بضبط الاعمال والمحاولات الاحتيالية، وتتخذ من أجل ذلك عددا من التدابير التي تهدف الى احتوائها محاولة في ذلك الحد من أثرها.

وتنطوي تدابير الاحتواء على عدد من الاجراءات التي تشمل القيود على القيم المخزنة على وسائل الدفع الالكتروني، وتسجيل هذه الوسائل باسم مستعملها الشخصي، كما يمكن أن يقوم النظام بوضع لوائح بوسائل الدفع التي شابها اختراق امني، وقد يصل الامر الى تعليق النظام برمته في حال فشل جميع التدابير المتخذة في منع اختراقه[3].

[1] المرسوم الرئاسي رقم 172.19 المؤرخ في 3 شوال 1440 الموافق لـ6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر عدد 37 مؤرخة في 06 يونيو 2019 (ص05 الى 07).

[2] المادة 02 من المرسوم الرئاسي رقم 172.19 المؤرخ في 06 يونيو 2019 سالف الذكر

[3] لمزيد من التفاصيل راجع: أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، طبعة 1، دار الميسرة 2010، الاردن، ص: 115 وما بعدها.

المبحث الثاني: مواجهة المخاطر القانونية المترتبة عن حالات استخدام وسائل الدفع الالكتروني.

يثير الدفع الالكتروني الكثير من المشكلات القانونية وذلك ناتج عن طبيعته الناشئ فيها وهي البيئة الالكترونية، فهل هي كافية القواعد القانونية لتنظيم هذه الآلية؟ ومن هنا تظهر مدى الحاجة الى قواعد قانونية خاصة تحكمها، فعلى سبيل المثال تثير بطاقات الدفع العديد من الاشكالات القانونية بدءا من حماية المعلومات الشخصية الى تنظيم مختلف الاستعمالات التي يمكن أن تقوم بها، وهذا يتطلب مواجهة قانونية معينة لهذه المخاطر عن طريق تنظيم دقيق يحافظ على مصالح كل المتعاملين في هذا الخصوص.

ويتعين أن يكون واضحا أن ازدهار التجارة الإلكترونية عموما ووسائل الدفع الالكتروني خصوصاً، يتوقف على جريانها في وسط قانوني يكفل الأمن للمعاملات ويحمي حقوق وحريات الأطراف [1].

هذا وقد تتم سرقة الحاسب الشخصي للعميل ويكون المفتاح الخاص مندمجا على الجهاز مما يسمح بسرقة المفتاح دون أن يشعر العميل بذلك، بالاضافة الى ذلك تطرح اشكالية كيفية مواجهة جرائم غسيل الاموال وإفشاء أسرار المستهلك الالكتروني وانتهاك السرية، ناهيك عن امكانية حدوث تهرب ضريبي لصعوبة ربط الضريبة بالصفقة التي تتم عبر الانترنت.

كما يمكن أن تنطوي هذه المخاطر على ما يسمى بخصوصية المتعاملين بالدفع الالكتروني، والمتعلقة بالمعلومات التي يعطيها المستهلك أو المتعامل للمؤسسة المصدرة للدفع الإلكتروني والمتعلقة بالخصوصية الشخصية، ضف الى ذلك استغلال البعض لنقاط ضعف التي يمكن أن تشوب وسائل الدفع هذه خاصة المتطورة منها كالنقود الإلكترونية، ويمكن أن تشمل هذه الأعمال استثمار أموال غير مشروعة في مشاريع ذات صبغة مشروعة فيما يعرف بتبييض الأموال، دون أن ننسى مشكلة التهرب الضريبي، مستغلين الطابع الدولي لهذه الوسائل[2].

[1] إبراهيم أحمد سعيد زمزمي، القانون الواجب التطبيق في منازعات عقود التجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة عين الشمس، كلية الحقوق، قسم الدراسات العليا، مصر،2015، ص500.

[2] حوالف عبد الصمد: المرجع السابق، ص: 475.

لذلك سوف نركز الحديث من خلال هذا المطلب، على حماية الخصوصية في الفرع الاول، ثم التطرق لمسألة الحماية في مواجهة تبييض الأموال بواسطة وسائل الدفع الالكترونية ومشكلة التهرب الضريبي في الفرع الثاني.

المطلب الاول: مواجهة مخاطر وسائل الدفع الالكتروني على حماية الخصوصية

نتناول ماهية مخاطر وسائل الدفع الالكتروني التي تهدد الخصوصية وكيفياتها، لنتطرق بعدها لعلاقتها وتأثيرها على الخصوصية.

أولا: ماهية المخاطر التي تهدد الخصوصية الشخصية

منذ ان عرف نظام الدفع الالكتروني عبر الانترنت ظهر معه المتسللون من أجل الاستيلاء على اموال الغير، ويعد السطو على وسائل الدفع الالكتروني والارقام السرية الخاصة بها من المخاطر التي تهدد الحق في الحياة الخاصة صورة من صور الاعتداء على الخصوصية.

ومن ذلك يجب احترام سرية البيانات الخاصة بالعملاء بوصفهم المستهلكين وكذلك احترام حقهم في الخصوصية، ويقتضي ذلك الإلتزام بعدم نشر أو بث أي بيانات تتعلق بشخصياتهم أو حياتهم الخاصة وكذلك البيانات المصرفية الخاصة بهم[1].

فالبيانات الإسمية أو الشخصية التي تتعلق بالتعاقد الإلكتروني[2]، هي البيانات المتعلقة بالأشخاص أطراف التعاقد ومنهم المستهلكين، وذلك عندما يتعلق الأمر بطلب السلع والخدمات، وكذلك هناك بيانات تتعلق برغبات المستهلك وميوله، وهي تلك التي يمكن تتبعها من جانب الشركات على شبكة الإنترنت، وفي مرحلة لاحقة يتم إغراق المستهلكين بالدعاية لمنتجات هذه الشركات، على نحو قد يؤدي لإعاقة شبكة الإتصالات[3].

فخصوصية العميل يجب أن تكون موضع حماية فيما يتعلق بمعلوماته الشخصية والمالية الموجودة على السجلات الالكترونية أو على وسائل الدفع المختزنة القيمة، وخلال جميع العمليات التي تهدف الى اجراء صفقات مالية في ظل عمليات الصيرفة الالكترونية، والقانون وحده لا يكفي ليحمي خصوصية المعلومات والاستراتيجيات التنظيمية وسياسات الحماية، لخصوصية المعلومات أو حماية

[1] هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت. ط 8، دار النهضة العربية، مصر ،5111، ص27.

[2] – Les Principes de Base de la Protection du Consommateur dans le Commerce (Electronique), guide pour les commerçants et des conseils, pour les consommateurs, sont offerts par voie électronique sur le Web

[3] – محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، الإسكندرية،5110، ص 822.

قطاعات الأعمال من احتمالات المساءلة والوسائل التقنية مهما بلغت فعاليتها لا تكفي وحدها لحماية خصوصية المعلومات من المخاطر التي تهددها وتهدد الثقة بالانترنت والتجارة الالكترونية.

وعليه يعتبر موضوع حماية الخصوصية الحلقة الرئيسية في اطار حماية المتعاملين في مجال الدفع الالكتروني و في أثناء ابرام صفقاتهم بواسطة وسائل الدفع الالكتروني، وهذا الأمر دفع بالعديد من الدول الى التعامل معه عن طريق سن عدد من التشريعات، التي أخذت بعين الاعتبار ضرورة مراعاة المصلحة العامة في تسيير عملية التجارة الالكترونية مع عدم اغفال حق المتعامل في صون خصوصيته في أثناء اجراء الصفقات.

وتتمثل مخاطر وسائل الدفع الالكتروني على الحياة الخاصة والتي تؤدي الى المساس بالحق في الحياة الخاصة للأفراد المتعاملين بهذه الوسائل في الاعتداء على البيانات والمعلومات والمعطيات السرية والمحمية للعملاء المتعاملين بوسائل الدفع الالكتروني، والذي سيؤدي حتما إلى الاعتداء على البيانات الشخصية المتصلة بالحياة الشخصية.

وبالنسبة لوسائل الدفع الالكتروني كبطاقات الائتمان مثلا تعد أموالا الكترونية والاستيلاء عليها يعد استيلاء على أموال الغير وانتهاكا لخصوصيتهم، اضافة الى ما يصاحب ذلك من عمليات الابتزاز حيث يقوم المجرمون باختراق الاجهزة الشخصية والعبث بما تحتويه من معلومات وذلك نظرا لإمكانية أو سهولة تعلم برامج الاختراق وكثرتها.

كما يقوم بعض المخترقين بالتعرض الى البيانات الشخصية السرية اثناء انتقالها والتعرف على شفرتها أن كانت مباشرة وهي الطريقة المستخدمة في كشف ارقام بطاقات الائتمان، والكشف عن الارقام السرية للبطاقات البنكية. لذلك ينبغي في هذا السياق عدم كشف ارقام بطاقات الائتمان لمواقع التجارة الالكترونية الا بعد التأكد بالتزام تلك المواقع بالسرية والامان، غير أن البعض لا يأخذون هذا الامر مأخذ الجدية فعندما يستخدمون بطاقة السحب الالي من أجهزة البنوك النقدية لا ينتظرون خروج السند الصغير المرفق بعملية السحب[1].

كما توجد طرق وتقنيات أخرى لمحاولة المساس بخصوص العملاء عن طريق الحصول على معلومات وبيانات تتسم بالحساسية والسرية من العملاء، مستغلين بذلك أسلوب التفاعل في الاتصال مع العميل، ومن أهم الطرق المتبعة هناك محاولة الحصول على المعلومات السرية عن طريق الهاتف، حيث يدعي المحتال انه يمثل أحد البنوك او يقوم أو يقوم بمقابلة العميل وجها لوجه، كما يمكن

[1] بوعزة هداية: المرجع السابق. ص: 304.

الحصول على المعلومات السرية عن طريق البريد الالكتروني أو عن طريق المواقع المزيفة على الانترنت[1].

ثانيا: وسائل الدفع وعلاقتها بالمساس بالخصوصية.

إن البيع والشراء والدخول في المزادات في الواقع الحقيقي قد لا يتطلب اكثر من تحديد الدافع، وهي بذاتها تنطوي على سمات التخفي اكثر من وسائل الدفع السائدة تتمثل ببطاقات الدفع او النقود الالكترونية او الاوراق التجارية المطورة...الخ، فتتطلب عمليات الشراء وعمليات الاعلان وطلب الخدمات والمزادات في العالم الافتراضي –الانترنت– تقديم اسم الشخص ورقم هاتفه و عنوانه وبريده الالكتروني، وببساطة فإنها تتطلب معلومات تفصيلية يغيب فيها القدرة على التخفي خلافا للعام الواقعي.

ولهذا فإن حماية خصوصية التعاملات المالية في بيئة الانترنت احد اهم ضمانات وجود النشاط التجاري فيها وتطوره. وكما قيل، فان نظام الدفع المالي على الانترنت بدون نظام حماية للخصوصية سينقلنا من عالم الدفع النقدي المستتر الى عالم مليء بوسائل الكشف والتعريف، تتزايد فيه قدرة تتبع الاشخاص ومشترياتهم [2] .

لذلك ففيما يخص خصوصية احترام المستهلك في الدفع الالكتروني، فانه يستوجب احترام سرية البيانات الخاصة بالعملاء بوصفهم مستهلكين، وكذلك احترام حقهم في الخصوصية، ويقتضي ذلك الالتزام بعدم نشر او بث أي بيانات تتعلق بشخصياتهم او حياتهم الخاصة، خاصة اثناء عملية الدفع، وكذلك البيانات المصرفية الخاصة بهم على سبيل المثال.

لذلك ففيما يخص احترام خصوصية المستهلك في الدفع الالكتروني، فانه يستوجب احترام سرية البيانات الخاصة بالعملاء بوصفهم مستهلكين، وكذلك احترام حقهم في الخصوصية، ويقتضي ذلك الالتزام بعدم نشر او بث أي بيانات تتعلق بشخصياتهم او حياتهم الخاصة، خاصة اثناء عملية الدفع، وكذلك البيانات المصرفية الخاصة بهم على سبيل المثال.

[1] لمعلومات أكثر راجع سعيدي سليمة ومن معها، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي الاسكندرية 2017.ص: 95.

[2] يونس عرب: المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي/ ص:25 منشور على الموقع الالكتروني http://alyaseer.net/vb/showthread.php?t=19032

وعليه فان الاحتفاظ على بيانات المستهلك في التجارة الالكترونية، تورث الثقة في هذه التجارة طالما ان البيانات في مأمن من الاختراق والسرقة ومن ثم اساءة استعمالها. يؤثر ايجابا على هذه التجارة ويدفع الاشخاص للتعامل فيها[1] .

المطلب الثاني: مواجهة مخاطر وسائل الدفع الالكتروني بالنسبة لمشكلة تبيض الأموال ومشكلة التهرب الضريبي.

من المتوقع ايضا ان تثير وسائل الدفع الالكتروني بعض المخاطر القانونية والتي تتبع أساسا من خلال انتهاك القوانين واللوائح مثل جرائم غسيل الاموال وإفشاء أسرار العميل و انتهاك السرية، ومن ناحية أخرى فإن لهذه المخاطر ان تصاحب أنتشار الدفع الالكتروني في تزايد جرائم التهرب الضريبي ذلك نظرا للصعوبات التي تواجه الجهات المكلفة بتحصيل الضرائب في ربط الضريبة على تلك الصفقات التي تتم بواسطة الدفع الالكتروني، كونها تتم خفية عبر الانترنت.

من هذا المنطلق نعالج هذين النوعين من المخاطر كل على حدى في الفرعيين المواليين.

أولا: تبيض الأموال باستخدام ر وسائل الدفع الالكتروني.

لقد تطورت أساليب الدفع الالكتروني مع التطور التكنولوجي حيث أصبح المجرمون يستخدمون وسائل تقنيات حديثة ومتطورة لغسيل أمواهم إخفاء جرائمهم القذرة، حيث ارتقى القطاع المصرفي والمالي بخدماته البنكية و أصبح يوفر ميكانيزمات جديدة لأساليب الدفع.

وقد ساعدت التجارة الالكترونية على إجراء العديد من الصفقات المشبوهة وغير القانونية والتي تساهم في عمليات التبييض لأنه يصعب من خلالها التعرف على أصحاب البطاقات الشخصية وعناوين المتعاملين مع البنوك الالكترونية.

وقد تطرق المشرع الجزائري الى أحكام هذه الجريمة المادة 389 مكرر 07 من القانون رقم 15/04 المتضمن قانون العقوبات والتي نصت على حالات متعددة والتي تندرج في إطار التبييض[2].

ويقصد بالتبييض عموما كل استثمار أو تحويل آخر لتدفق الأموال من مصادر غير قانونية إلى قنوات غير شرعية، بحيث لا يمكن معه معرفة مصدرها الأصلي كما هو الحال في صفقات المخدرات واحتجاز الرهائن والقمار والاتجار بالبشر وتهريب الكحول والأدوية والتبغ والأسلحة والتهرب الضريبي

[1] حوالف عبد الصمد: المرجع السابق، ص: 355.

[2] أنظر الفصل الثالث من قانون العقوبات المتمم بالقانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية عدد 71 لسنة 2004، في القسم السادس مكرر بعنوان تبييض الاموال ويتضمن المواد من 389 مكرر الى المادة 389 مكرر7.

وغيرها من الأنشطة غير المشروعة، مما أدى إلى تنامي أسواق التهريب للعمالة غير الشرعية والقرصنة الالكترونية والاتجار بالبشر والأعمال الفنية الآثار والأسلحة والمواد السامة اليورانيوم [1].

ومن أهم وسائل الدفع والأدوات الالكترونية المستخدمة في تبييض الأموال: البنوك الالكترونية والنقود الالكترونية والبطاقات الذكية والتحويل الالكتروني للأموال.

وحيث تعد المؤسسات المصرفية والمالية الطريق المفضل لتنفيذ عمليات غسيل الأموال نظرا لكفاءتها وكلفتها المنخفضة في تنفيذ المعاملات المالية، ولما تتمتع به العمليات المصرفية من تعقيد وتشابك، ولعل أكثر ما سهل من اقتراف هذه الجريمة هو ارتكابها بواسطة وسائل الدفع الحديثة، هذه الأخيرة التي تخلف آثارا خطيرة تتمثل في علاقتها السلبية بالجريمة لانها تسهل ارتكابها وتقلل من فعالية الاجراءات المتخذة لمكافحتها.

وتعتبر الانترنت من احدث الطرق لغسيل الاموال المشبوهة خاصة انها اسهل استخداما و أيسر في التعامل مع البنوك، وضغطة مفتاح تفتح له آفاق الدخول في حسابات وأنشطة مالية ومصرفية من أي جهة في العالم، فيقوم المجرمون بالاعتماد على عملية التحويل الالكتروني للاموال من خلال البنوك بايداع الاموال المسروقة في حسابات متعددة بالبنوك قم تحول الى عدة فروع في بلدان مختلفة[2] .

وتعتبر النقود الإلكترونية أهم الوسائل التي تسهل ارتكاب جريمة غسل الأموال لأنه يتم التعامل بالنقود الإلكترونية دون الحاجة إلى ظهور الهوية الحقيقية للمتعاملين و أحيانا دون ظهور هويتهم إطلاقاً، وهذا يخلق فرصة لدى غاسل الأموال لاستخدامها في ارتكاب جريمته، إذ لن يكون مضطراً للإفصاح عن شخصيته حتى لو كان له تاريخ حافل في ارتكاب جريمة غسل الأموال.

كما أن للنقود الإلكترونية طابعاً من السرية، يجعل مهمة السلطات المختصة بمراقبة جريمة غسل الأموال مهمة صعبة جد اً، حيث يصعب مراقبة السجلات و العمليات المالية و المصرفية التي تتم باستخدام هذه النقود [3].

---

[1] المادة 6 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية المحررة في بالقاهرة بتاريخ 21ديسمبر 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي 251.14 المؤرخ في 13ذي القعدة 1435 الموافق لـ 08 سبتمبر 2014، الجريدة الرسمية عدد56.

[2] عبد الرحيم وهيبة: تقييم وسائل الدفع الالكترونية ومستقبل وسائل الدفع التقليدية في حال وجودها، مجلة الاقتصاد الجديد العدد الثاني، جانفي 2010، ص: 198.

[3] توفيق شنبور، أدوات الدفع الإلكترونية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، الجزء الأول، الجديد في التقنيات المصرفية، الطبعة الأولى، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، منشورات الحلبي الحقوقية، بيروت 5115، ص882.

فضلاً عن أن استخدام هذا النوع من النقود، يعتمد بالدرجة الأولى على استخدام أجهزة الكمبيوتر والأنظمة الإلكترونية، وقد تتعطل هذه الأجهزة والأنظمة التي تحفظ هذه النقود سواء كان هذا العطل مقصوداً نتيجة أعمال جرمية أو عطلاً تلقائيا، وفي هذه الحالة يصبح من المستحيل مراقبة العمليات التي تتم باستخدام النقود الإلكترونية ومن ثم يخلق مجالا واسعا لارتكاب جريمة غسل الأموال [1].

ثانيا: التهرب الضريبي باستخدام وسائل الدفع الالكتروني.

أن وسائل الدفع الالكتروني بما فيها بطاقات الدفع الحديثة قد تشكل وسيلة للتهرب الضريبي، حيث أن هذه الظاهرة انتشرت بكثرة في الدول المتقدمة السباقة في التعامل بمثل هذه الوسائل، لذلك يتعين على الادارة الجبائية مراقبة الحسابات المتواجدة ببطاقات الائتمان لان أصحابها قد يتعمدون إخفاء عدد معتبر من الأموال في البلدان المعروفة بالجناة الجبائية، كما وان استخدام وسائل دفع مزورة قد يصعب نوعا ما من عملية المراقبة.

كما ان ممارسة التجارة الالكترونية واعتمادها على وسائل الدفع الالكتروني في نشاطاتها يواجهه صعوبات عملية تتعلق بمدى خضوع هذه النشاطات للضريبة، وهي تحديد النشاط وطبيعة المعاملة موضوع الوعاء الضريبي.

وتجدر الاشارة في هذا الصدد إلى ان المشرع الجزائري في قانون التجارة الالكترونية رقم 05/18 أخضع المعاملة الالكترونية الى الحقوق والرسوم التي ينص عليها التشريع والتنظيم المعمول بهما، بمعنى عدم الاخلال بالاعفاءات والمزايا الضريبية والجمركية المقررة بمقتضى قوانين الضرائب والجمارك وحوافز الاستثمار وغيرها من القوانين، ووضع الروط والأسس الخاصة بذلك.

وتعرف الجباية الالكترونية بأنها: التي تعنى بفرض الضرائب على التعاملات التي تتم على شبكة الانترنت[2] . والسؤال الاكثر أهمية هل يجب أن تفرض ضريبة على التجارة الالكترونية؟ وماهي الصعوبات التي تواجه فرض الضريبة على التجارة الالكترونية؟

ذلك أمام تزايد الاهتمام العالمي بالتجارة الالكترونية وفتح الاسواق والغاء القيود والحواجز الجمركية، وتزايد عائدات التجارة الالكترونية و أرباحها مما يؤدي الى ظهور فروض ضريبية جديدة ، وهذا بدوره يؤدي الى نشوء مخاطر التهرب الضريبي الالكتروني، فضلا عن حرمان الدول النامية ومنها الجزائر من

[1] نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس، لبنان 5117، ص 89.

[2] Frederic huet La fiscalite du commerce electronique Paris litec 2000 PP 23-25.

ايرادات ضريبية ناتجة عن التجارة الالكترونية حال عدم التنبه للموضوع وحصره واعادة تأهيل النظام الضريبي والبنية التحتية للادارة المالية.

ومع التطور الحاصل في هذا المجال ينادي الكثيرون بوجوب اخضاع التجارة الالكترونية للضريبة وذلك نظرا لاعتبارات متعددة من بينها انها تشكل حافزا لأصحاب المهن والاعمال لتقديم منتجاتهم وسلعهم على الخط المفتوح لان الاشخاص الذين يقبلون الشراء على الخط المفتوح يتهربون من دفع الضرائب، وهذا بدوره سيؤدي الى زيادة خسائر الدولة من العوائد الضريبية .

ويقابل ذلك عدة صعوبات قانونية وفنية تواجه ضريبة المبيعات على التجارة الالكترونية أهمها تحديد الدولة صاحبة الحق في فرض تلك الضريبة وثانيا تحديد آليات تحصيل تلك الضريبة ومدى جدواها.

ومهما يكن سواء ان قامت الضريبة على أساس دولة الوصول أم على أساس دولة المنشأ فان مسؤولية تحصيل الضريبة تقع على البائع، وللقيام بعملية التحصيل يمكن أن تدور بين طرق معينة، أولها التحصيل عن طريق طرف ثالث موثوق كالوسطاء الماليين ومزودي خدمة الانترنت أو التحصيل باستخدام وسائل تكنولوجية جديدة وهي البرامج المتخصصة في فرض الضريبة.

وهكذا يمكن القول، أن تطور الحياة المعاصرة قدم للإنسان وسائل جديدة تمكنه من إتمام معاملاته، و لاسيما المالية منها بكل يسر وسهولة، وتأتي النقود الإلكترونية في مقدمتها. لكن غاسل الأموال والمتهربين من الضرائب، لم يتوانوا عن استغلالها لارتكاب جريمة غسل الأموال وكذا جريمة التهرب الضريبي، لذلك يجب على السلطات المختصة بمكافحة هذه الجريمة أن تكون على درجة عالية من الحيطة والحذر لمنع غاسل الأموال والمتهربين ضريبياً، من الاستفادة من ميزات وسائل الدفع الإلكتروني لارتكاب جرائمهم، بحيث يتم الوصول إلى الحالة التي تصبح فيها هذه الوسائل ذات وجه إيجابي فقط، وهذا الأمر ينطبق على باقي المخاطر القانونية لوسائل الدفع الالكترونية من مسألة المساس بالخصوصية والدفع عبر الحدود.

خاتمة:

تقوم المعاملات الالكترونية على استخدام تقنيات ووسائل لعل أهمها وسيلة الدفع الالكتروني الذي توسع استخدامه بانتشار التكنولوجيا الحديثة وازدهار التجارة الالكترونية التي اعتمدت على هذه الوسائل الى حد كبير، استخلصنا أنه رغم ما يحققه الدفع الالكتروني من مزايا التي لم يوفرها الوفاء بصورته التقليدية فقد ظهرت معها عدة سلبيات ومخاطر، وتعد المخاطر أهم ما يمكن أن يواجه الدفع الالكتروني في إطار المعاملات البنكية والمالية أين تعد المخاطر القانونية الناتجة عن الاستغلال غير المشروع لهذه الوسيلة.

ووجدنا أن ذلك يكون سواء ما يتعلق منها بأمن المعلومات كالتهديد بالخصوصية الشخصية، أو ما قد يقوم به بعض المتعاملين من أعمالا احتيالية أو متعسفة كغسيل الاموال والتهرب الضريبي الذين يتم ارتكابهما بواسطة هذه الوسائل، فكان لزاما على الجهات المسؤولة اتخاذ كل تدابير الوقاية واتخاذ كل الاجراءات الخاصة لمواجهة هذه المخاطر.

توصلت الدراسة بصفة عامة إلى أن وقوع المخاطر القانونية المترتبة عن استخدام وسائل الدفع الالكتروني مرده قصور النصوص القانونية في تنظيم كل ما يتعلق بأحكام الدفع الالكتروني، مع ووجود ثغرات قانونية بها وعدم مواكبة التشريعات والقوانين للتطورات التكنولوجية الفائقة والتي لا يمكن استيعابها بشكل مطلق في هذا المجال، وذلك رغم الجهود الوطنية والدولية لجعل وسيلة الدفع الالكتروني أكثر أمانا مع محاولة وضع خطط واستراتيجيات للتغلب عليها ومواجهتها.

ومن أجل تدراك تلك الاشكالات القانونية وكمساهمة منا في محاولة إنجاح هذا النظام نتقدم بمجموعة من الاقتراحات نراها مناسبة،،

- على المتعاملين بوسائل الدفع الالكتروني، أن يكونوا واعيين بحجم المخاطر الناتجة عن الاستفادة من تلك الخدمات، وذلك بمراعاتهم لضوابط السلامة والامن، مع الاخذ بعين الاعتبار ما يقوم به البنك او مؤسسات الاصدار من معلومات حول كيفية الاستخدام.
- تعزيز الوسائل الكفيلة بإنجاح النظام الالكتروني للدفع.
- توفير الكوادر البشرية والادارية القادرة على ادارة العمليات المصرفية الالكترونية والتعامل مع النظم الحديثة للتجارة الالكترونية
- ضرورة وضع إطار تشريعي وتنظيمي يتلائم وطبيعة البيئة التي تتم فيها عمليات الدفع الالكتروني وتبني نظام.

ـ ضرورة انضمام الجزائر الى الاتفاقيات الدولية التي تسعى الى توفير حماية جنائية للمعلوماتية والتعامل ببرامج الأجهزة الالكترونية.

قائمة المراجع:

أولا: النصوص القانونية

1. القانون رقم 03/2000 الملغى المؤرخ في 5 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، جريدة رسمية عدد 48 لسنة 2000.
2. القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، الجريدة الرسمية عدد 71 لسنة 2004، المتمم لقانون العقوبات.
3. القانون رقم 01/08 المؤرخ في 23 يناير 2008 المتمم للقانون رقم 11/83 المؤرخ في 02 يوليو 1983 والمتعلق بالتأمينات الاجتماعية، جريدة رسمية عدد 04 لسنة 2008.
4. القانون رقم 04/09 المؤرخ في 5اوت 2009، جريدة رسمية عدد 47 لسنة 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال و مكافحتها.
5. القانون رقم 04/15 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فبراير 2015، الجريدة الرسمية عدد 6 لسنة 2015. يحدد القواعد العامة الماعلقة بالتوقيع والتصديق الالكترونيين.
6. القانون رقم 05/18 المؤرخ في 24 شعبان 1439 الموافق لـ 10 ماي 2018، الجريدة الرسمية عدد 28 لسنة 2018، يتعلق بالتجارة الالكترونية.
7. المرسوم الرئاسي رقم 19-172 المؤرخ في 3 شوال 1440 الموافق لـ6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر عدد 37 مؤرخة في 06 يونيو 2019 (ص05 الى 07).

ثانيا: الكتب

1. الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية المحررة في بالقاهرة بتاريخ 21ديسمبر 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي 251.14 المؤرخ في 13ذي القعدة 1435 الموافق لـ 08 سبتمبر 2014، الجريدة الرسمية عدد56.
2. محمد ابراهيم محمود الشافعي: النقود الالكترونية، الهيئة العليا لتطوير الرياض، المال والاقتصاد مقال منشور على الموقع: www.amadh.com
3. خثير مسعود: الحماية الجنائية لبرامج الكمبيوتر . أساليب وثغرات . دار الهدى، الجزائر 2010.

4. طارق ابراهيم الدسوقي عطية:الموسوعة الامنية، الامن المعلوماتي، النظام القانوني لحماية المعلوماتية، درا الجامعة الجديدة، الاسكندرية.

5. أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، طبعة 1، دار الميسرة 2010، الاردن.

6. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت. ط 8، دار النهضة العربية، مصر.

7. محمد حسين منصور، المسؤولية الالكترونية، دار الجامعةالجديدة، الإسكندرية،2015.

8. سعيدي سليمة ومن معها، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي الاسكنرية 2017.

9. نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس، لبنان 5117.

10. محمد دباس الحميد، ماركة ابراهيم نينو، حماية أنظمة المعلومات، دار الحامد للنشر و التوزيع، عمان 2007، ص: 34.

11. حسن طاهر داوود: الحاسب أمن المعلومات، معهد الادارة العامة، مكتبة فهد الوطنية، الرياض

12. Frederic huet La fiscalite du commerce electronique Paris litec 2000.

ثالثا: الرسائل والمذكرات

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

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

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

رابعا: المقالات

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

2. سعيدي عزوز، راكول خالد: الامن التقني للدفع الالكتروني، أية فعالية؟ مقال منشور في مجلة معالم للدراسات القانونية والسياسية، العدد الثاني، ديسمبر 2017.
3. عبد الرحيم وهيبة: تقييم وسائل الدفع الالكترونية ومستقبل وسائل الدفع التقليدية في حال وجودها، مجلة الاقتصاد الجديد العدد الثاني، جانفي 2010.

خامسا: أشغال الملتقيات

1. محمد عبد الصمد: الجريمة المعلوماتية والاحتساب عليها، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد الثالث 2000.
2. توفيق شنبور، أدوات الدفع الإلكترونية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، الجزء الأول، الجديد في التقنيات المصرفية، الطبعة الأولى، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، منشورات الحلبي الحقوقية، بيروت 5115.

سادسا: المواقع الإلكترونية

1. محمد ابراهيم محمود الشافعي: النقود الالكترونية، الهيئة العليا لتطوير الرياض، المال والاقتصاد مقال منشور على الموقع: www.amadh.com
2. يونس عرب: المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي/ ص:25 منشور على الموقع الالكتروني http://alyaseer.net/vb/showthread.php?t=19032