

جامعة إِمحمد بوقرة- بومرداس-



كلية الحقوق والعلوم السياسية- بودواو-

قسم القانون الخاص

حماية البنوك من مخاطر الدفع الالكتروني

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في القانون

تخصص قانون أعمال

إشراف الدكتورة:

مرشيشي عقيلة

من إعداد الطالبتين:

- حمودي سارة

- بن مالك فضيلة

لجنة المناقشة

عمورة راج	أستاذ محاضر (ب)	كلية الحقوق - إِمحمد بوقرة- بومرداس	رئيسا
- مرشيشي عقيلة	أستاذ محاضر (ب)	كلية الحقوق - إِمحمد بوقرة- بومرداس	مشرفا ومقررا
- دومة نعيمة	أستاذ محاضر (ب)	كلية الحقوق - إِمحمد بوقرة- بومرداس	ممتحنا

السنة الجامعية 2019 - 2020

الشكر

في البداية نحمد الله تعالى على نعمه الجليلة، وأنه تبارك وتعالى أمدنا بالصحة والقوة وكان لنا عوناً ودعماً، نحمده -عز وجل- أنه وهبنا التوفيق والسداد ومنحنا الرشد والثبات لإعداد هذا البحث ونرجو أن يكون ذخراً في ميزان الحسنات يوم القيامة.

ونشكر كل من تلقينا منه علماً صالحاً أو عملاً مفيداً لمواصلة مشوارنا، كما نشكر الأستاذة المشرفة "مرشيشي عقيلة" على توجيهاتها القيمة ونصائحها النفيسة، وكل الأساتذة الذين تدرسنا على أيديهم، كما لا ننسى أعضاء لجنة المناقشة كل باسمه.

وفي الختام نشكر كل من ساعدنا طيلة فترة إعداد المذكرة من قريب أو بعيد، بالكثير أو بالقليل حتى ولو كلمة طيبة أو ابتسامة عطرة.

إلى كل هؤلاء نقول لهم:

"بارك الله فيكم وجعلها في ميزان حسناتكم"

الإهداء

الحمد لله فائق الأنوار، وجاعل الليل والنهار والصلاة والسلام على نبينا محمد المختار.
إلى من ربّني وأنارت دربي وأعانتني بالصلوات والدعوات إلى أعلى إنسانة في هذا
الوجود إلى القلب الناصع بالبياض إليك أُمي الحبيبة أطل الله في عمرها.
إلى من كان السند القوي والشمعة التي تضيء دربي وغرس في نفسي معاني الصدق
والتربية إلى أبي الغالي -حفظه الله-
إلى من لم يكتب لهم القدر أن يشاركوني فرحتي إلى من وافتهم المنية:
إلى زوج أختي، إليك أخي الغالي "محمد" رحمك الله وأنارك بالجنة -إن شاء الله-.
إلى من كانوا يضيئون لي الطريق ويساندوني ويتنازلون عن حقوقهم لإرضائي،
والعيش في هناء، أخواتي كلهن بأسمائهن وأخي الغالي "شمس الدين".
إلى من عمل معي بكد بغية إتمام هذا العمل إلى صديقتي "بن مالك فضيلة".
إلى من تشرفت بمعرفتهم رفيقاتي وصديقاتي خاصة "أسماء وزينب".
إلى من أحببتهم وأحبوني.

أهدي هذا العمل

سارة

الإهداء

الحمد لله فائق الأنوار، وجاعل الليل والنهار والصلاة والسلام على نبينا محمد المختار.

إلى من ربّني وأنارت دربي، إلى الغالية على قلبي، إلى الصدر الحنون إلى أعز ما
أملك في الدنيا إلى أُمي الغالية أطال الله عمرك.

إلى من كان السند القوي والشمعة التي تضيء دربي وغرس بي معاني الصدق
والتربية إلى أبي العزيز.

إلى أخي الغالي إبراهيم وزوجته ياسمين وأختي الغالية مريم.

إلى كل أفراد عائلتي وإلى رفيقاتي، وإلى كل من عمل معي بكد بغية إتمام هذا العمل
إلى صديقتي حمودي سارة.

إلى الذين بذلوا كل الجهد والعطاء لكي أصل إلى هذه اللحظة أساتذتي الكرام.

إلى من أحببتهم وأحبوني.

أهدي هذا العمل

فضيلة

الملخص:

يعتبر تطوير القطاع المصرفي واستحداث نظام الدفع من المشاريع التي تمكن من قياس درجة التطور في التجارة والمعاملات المصرفية، ما جعل العديد من البنوك في مختلف دول العالم تسعى إلى تطوير أنظمة الدفع. ومن أجل توفير الأمان، السهولة والسرعة في التعامل، استحدث نظام يسمى " نظام الدفع الالكتروني" والذي اتخذته البنوك كتقنية في إجراء المعاملات البنكية. ولقد كان الهدف من الدراسة التعرف على وسائل الدفع الالكتروني والآثار المترتبة على استعمالها استعمالا غير مشروع على البنوك، والحماية المقررة لهذه الأخيرة. ومن أهم النتائج المتوصل إليها هي أن المشرع الجزائري لم يخص الدفع الالكتروني بنظام مستقل، بل نجد أن المشرع الجزائري تصدى للأفعال غير مشروعة والجرائم المرتكبة الكترونيا استنادا إلى النصوص التقليدية العامة وبعض النصوص الخاصة.

مقدمة

مقدمة:

شهد العالم تطورات تكنولوجية معلوماتية في مراحل زمنية مختلفة ما أحدث تغيرات جذرية في التعاملات الاقتصادية على العموم، وعلى القطاع المصرفي على الخصوص لتتماشى مع متطلبات التجارة الالكترونية، وهذا ما أدى إلى ظهور البنوك الالكترونية والتي تتجاوز نمط الأداء الاعتيادي ولا تتقيد بمكان وزمان معينين، وتعرف على أنها "عبارة عن بنوك افتراضية تنشئ لها مواقع الكترونية على الانترنت لتقديم خدمات وهي خدمات موقع البنك من سحب ودفع وتحويل دون انتقال العميل إليها"¹.

اهتمت البنوك الالكترونية بتقنيات المعلومات والاتصالات والحواشيب الآلية، وتطوير كفاءاتها وابتكار خدمات مصرفية مستحدثة ومتنوعة وبتكاليف منخفضة، على عكس البنوك التقليدية التي لم تعد فعالة باعتمادها تقنيات بسيطة أصبحت تثير عدة مشاكل من عمليات حسابية معقدة وجرائم السرقة وضياع النقود عند إجراء صفقات ضخمة، والنظم والوسائل التي تستعملها أصبحت تسمى بنظم الدفع التقليدية أو وسائل الدفع الكلاسيكية، أما البنوك الالكترونية اعتمدت على وسائل ونظم دفع حديثة يطلق عليها أنظمة "الدفع الالكتروني"، والتي تعرف على أنها "عبارة عن تقنية للمعلومات والاتصالات، تسهل عملية نقل ومتابعة حركة الأموال والأوراق التجارية المتداولة بين البنوك، وهي أنظمة ذات فعالية وشفافية عالية، كما تستجيب لمعايير المعدة من طرف لجنة أنظمة الدفع والتسوية على مستوى بنك التسويات الدولية"².

ساعدت التطورات التكنولوجية في الانتشار الواسع لأنظمة الدفع الالكترونية المستخدمة من طرف المتعاملين في جميع أنحاء العالم، وتحديثها وتطويرها المستمر والمتلاحق الذي كان له أثر على سهولة اللجوء إليها، لتمكين المتعامل من إبرام صفقات وخدمات قانونية في أوقات زمنية قياسية، وتتمثل أنظمة الدفع الالكتروني في السندات الالكترونية والتي تتضمن سندات تجارية الكترونية كالشيك الالكتروني، السفتجة والسند

¹ شوبوب نصيرة، الإدارة البنكية الالكترونية في الجزائر، دراسة ميدانية حول أنظمة النقد الآلي، مذكرة لنيل شهادة ماجستير، تخصص مجتمع معلومات، كلية العلوم السياسية، جامعة الجزائر 3، (2012-2013)، ص54.

² حدوم ليلي، أنظمة الدفع ما بين البنوك، أطروحة لنيل درجة دكتوراه، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر 1، (2011-2012)، ص2.

لأمر الالكترونيين، البطاقات الالكترونية، كما تتضمن عمليات الدفع الالكترونية والمتمثلة في المقاصة الالكترونية، التحويل الالكتروني والاعتماد المستندي الالكتروني. ونتج عن تضخم حجم المعاملات التجارية الالكترونية وتعدد مجالاتها، تزايد حجم المخاطر التي تواجهها البنوك، فأصبحت تتعرض لمخاطر سرقة الحسابات الالكترونية عن طريق اختراق قاعدة البيانات الخاصة بالبنك، وسرقة الأرقام السرية لحسابات العملاء، مع وضع نظام تتبع للحساب في حال تغيير مكانه أو إقامة أي حركات مصرفية على الحساب سواء كان إيداع أو سحب، وهذا ما يمكن السرقة بواسطة السحب الفوري أو تحويل الأموال من الحسابات. وعدم قدرة حاملي البطاقات الالكترونية سداد الديون المستحقة عليهم، ما يؤدي بالبنك تحمل نفقات ضياع البطاقة الالكترونية، كما سهل الدفع الالكتروني أن تكون وسيلة ارتكاب جرائم تبييض الأموال، التهرب الضريبي، القرصنة المعلوماتية وجريمة انتهاك الخصوصية.

وجميع هذه المخاطر والجرائم التي تتعرض لها البنوك لم تكن معروفة في ظل التعاملات التي كانت تعتمد على الوسائل التقليدية، فهي تقل وتزداد حسب توافر الأنظمة الخاصة لاكتشافها والوقاية منها، وهذا ما دفع بمختلف الدول بالمسارعة في إصدار تشريعات لمكافحة الاستخدام غير المشروع لوسائل الدفع الالكتروني والحد من الجرائم المرتكبة بواسطتها، واعتبارها كضمان لحماية عمليات الدفع الالكتروني ووسائلها.

فعلى الصعيد الوطني قام المشرع الجزائري بتطوير المنظومة القانونية، وذلك بإدخال تعديلات على القوانين العامة والمتمثلة في قانون العقوبات، قانون الإجراءات الجزائية، والقانون التجاري، أو بإصدار قوانين خاصة المتمثلة في القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، قانون النقد والقرض، النظام المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، القانون المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، قانون الملكية الفكرية الجزائري، وحتى قانون التجارة الالكترونية الجزائري، والغرض من إصدار هذه الأنظمة هو تشديد العقوبات ومنع الجناة من ارتكاب جرائم باستعمال هذه الوسائل.

أما على الصعيد الدولي فقد تم إصدار عدة معاهدات كمعاهدة بودابست بشأن جرائم الحسابات في حماية وسائل الدفع الالكتروني، من طرف منظمات عالمية كالمنظمة

الدولية للأمم المتحدة وانضمام جميع دول العالم إلى هذه المعاهدات من أجل الحد من هذه المخاطر والجرائم.

تتجلى أهمية موضوعنا من عدة جوانب من بينها التطور التكنولوجي الذي عرفه القطاع المصرفي واستعمال شبكة الانترنت في نظم الدفع، التعاقد والتسارع في تغيير بيئة الأعمال، والانتشار الواسع والاستعمال المتكرر لهذه الوسائل وانتشار البنوك الالكترونية في العالم.

ويعود سبب اختيارنا لهذا الموضوع لنقص الأبحاث القانونية والدراسات التي تطرقت له، بالإضافة إلى حدائته في الجزائر نظرا لحدثة ظهور البنوك الإلكترونية والبحث في المخاطر التي واجهتها جراء استعمالها لوسائل وتقنيات دفع حديثة.

للتفصيل في هذه الأفكار نطرح الإشكالية التالية: في ظل الانتشار الواسع لوسائل الدفع الإلكتروني ما هي السبل الكفيلة للحد من المخاطر التي تترتب عن الاستعمال غير المشروع لها والتي تواجهها البنوك؟

للإجابة عن هذه الإشكالية ارتأينا تقسيم موضوع الدراسة إلى فصلين: يتعلق الفصل الأول بمخاطر الدفع الإلكتروني على البنوك، يتضمن بحثين في؛ الأول نتطرق إلى آليات الدفع الإلكتروني وفي الثاني إلى الآثار المترتبة عن الاستخدام غير المشروع لوسائل الدفع الإلكتروني، أما الفصل الثاني فيتعلق بطرق مكافحة مخاطر الدفع الإلكتروني على البنوك، ويتضمن هذا الفصل أيضا بحثين؛ في الأول نتطرق إلى الحماية التقنية لمكافحة مخاطر الدفع الإلكتروني وفي الثاني إلى الحماية القانونية لمكافحة مخاطر الدفع الإلكتروني.

معتمدين في ذلك على المنهج الوصفي تارة في التعاريف وتحديد المفاهيم العامة، وتارة أخرى المنهج التحليلي في تكييف الأعمال غير المشروعة الناتجة عن استخدام وسائل الدفع الإلكتروني.

الفصل الأول

مخاطر الدفع الإلكتروني

على البنوك

الفصل الأول: مخاطر الدفع الالكتروني على البنوك

ساهم التطور التكنولوجي في تحسين النظام المصرفي، حيث تبنت البنوك نظام جديد في تسوية المعاملات المالية ما أدى إلى ظهور نظام يطلق عليه "نظام الدفع الالكتروني"، والذي يعتمد على وسائل وتقنيات حديثة بغرض تحقيق السرعة في المعاملات التي تقوم بها البنوك. وذلك بتحويل شكل النقود من مادية إلى نقود الكترونية محفوظة في بطاقات وسندات تجارية الكترونية بالإضافة إلى عمليات الدفع التي تكون الكترونيا بواسطة التحويل والمقاصة الالكترونيين.

ورغم أهمية هذا النظام في تسهيل المعاملات المالية على البنوك والمتعاملين معها إلا أن هذا الأخير قد تواجهه مخاطر عديدة ممن يستغلون هذا النظام في أعمال غير مشروعة تنجر عنها تكبدتها خسائر لم تكن متوقعة.

وللبحث في الآليات الحديثة التي تستعملها البنوك والمخاطر التي تواجهها من جراء ذلك، قسمنا هذا الفصل إلى مبحثين: نتناول في الأول آليات الدفع الالكتروني للبنوك، وفي الثاني الآثار المترتبة عن الاستخدام غير المشروع لهذه الآليات.

المبحث الأول: آليات الدفع الالكتروني للبنوك

عرف المشرع الجزائري آليات الدفع الالكتروني في المادة 69 من الأمر 03-11 التي تقضي بما يلي: "تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل الأموال مهما يكن السند أو الأسلوب التقني المستعمل"¹.

يتضح من هذا التعريف أن المشرع لم يحدد وسيلة دفع معينة ولم يحدد لها شكل معين فما يهم هو وظيفتها في تحويل الأموال، سواء كانت وسائل تقليدية للدفع أو كانت وسائل دفع حديثة والمتمثلة في السندات الالكترونية (المطلب الأول) وتقنيات الدفع الالكتروني (المطلب الثاني) التي تعتمد على البنوك في تسوية المعاملات المالية.

¹ المادة 69 من الأمر رقم 03-11 المؤرخ في 26 أوت سنة 2003، المتعلق بالنقد والقرض، معدل ومتمم، جريدة رسمية عدد 52 الصادرة في 27 أوت 2003.

المطلب الأول: السندات الالكترونية

عرف الفقهاء¹ السند الالكتروني "بأنه معلومات ترسل أو تسلم بوسائل الكترونية أيا كانت وسائل استخراجها في المكان المستلمة فيه"، فمجال السند الالكتروني واسع حيث لا يقتصر على تبادله عبر شبكة الانترنت فقط بل يكون باستعمال وسائل الكترونية أو أية وسائل تقنية متاحة.

الفرع الأول: السندات التجارية الالكترونية

تعتبر السندات الالكترونية وسائل مطورة لتلك الأوراق التجارية التقليدية، وتعرف بأنها محررات تمت معالجتها الكترونياً بصورة كلية أو جزئية، تمثل مبلغ من النقود تكون مستحقة الدفع وقابلة للتداول²، فهي تخضع لنفس أحكام ما يسري على الأوراق التقليدية إلا ما تعلق بأحكام قد ذكرت في قوانين خاصة، وتتمثل السندات التجارية الالكترونية³ فيما يلي:

أولاً/ الشيك الالكتروني:

يعتبر الشيك الالكتروني من أبرز أشكال النقود الالكترونية، فهو يحقق السرعة في إنجاز المعاملات الالكترونية ويعزز الثقة بين المتعاملين⁴، وهو أحد وسائل الدفع الالكتروني التي نشأت وتطورت عن الشيك التقليدي. لذلك نجد أن أغلب التشريعات لم تخصص أحكام قانونية جديدة للشيك الالكتروني رغم أن هذا الأخير يتمتع بخصوصية كبيرة في عدة نواحي بالمقارنة مع الشيك التقليدي⁵.

¹ نقلاً عن طمين سهيلة، الشكلية في عقود التجارة الالكترونية، مذكرة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2011، ص 68.

² بوعزة هداية، النظام القانوني للدفع الالكتروني-دراسة مقارنة-، أطروحة لنيل درجة دكتوراه، تخصص القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، (2018-2019)، ص 141.

³ حنان مليكة، بحث قانوني هام عن الشيكات الالكترونية، 2016، <https://www.mohamah.net/law> تم الاطلاع عليه بتاريخ 22 جوان 2020 على الساعة 22:00.

⁴ حنان مليكة، المرجع نفسه.

⁵ عامر محمد بسام أحمد مطر، الشيك الالكتروني، دار الجنان للنشر والتوزيع، الأردن، 2013، ص 17.

حاول بعض الفقهاء¹ إيجاد تعريف للشيك الالكتروني استنادا إلى الشيك العادي وبما يتناسب مع طبيعته الالكترونية، ولهذا تعددت التعريفات فذهب بعض الفقهاء إلى القول بأنه: "وثيقة الكترونية تحتوي على البيانات التالية: رقم الشيك، اسم الدافع، رقم حساب الدافع، اسم المصرف، اسم المستفيد والقيمة التي تدفع ووحدة العملة المستعملة، تاريخ الصلاحية والتوقيع الالكتروني". ذهب البعض الآخر من الفقهاء إلى تعريف الشيك الالكتروني بأنه وثيقة الكترونية تحمل التزاما قانونيا هو ذات الالتزام في الشيكات الورقية ويحمل نفس البيانات الأساسية ولكن يكتب بطريقة الكترونية.

يتضح من خلال هذين التعريفين أن الشيك الالكتروني يستغني عن التوقيع الكتابي الذي يضعه الأمر بسحبه فيحل الرقم السري محل التوقيع الكتابي المعتمد سابقا في الشيكات التقليدية، والذي يساعد في التعرف على هوية مصدر الشيك الالكتروني فيتم تحريره وتوقيعه وفقا لآليات معينة، حيث يستلزم أن يكون لكل من الساحب والمستفيد حسابات جارية في بنك واحد يقبل التعامل بالشيكات الالكترونية² وذلك على النحو التالي:

- الخطوة الأولى: اشتراك كلا من الساحب والمستفيد لدى جهة الدفع نفسها، وفتح حساب جاري ويتم تحديد لكل منهما توقيعها الكترونيا وتسجيله في قاعدة بيانات البنك.
- الخطوة الثانية: يختار الساحب السلعة أو الخدمة التي يرغب في شرائها، بعد أن يتم تحديد السعر الكلي والاتفاق على أسلوب الدفع. وهذا يتم بشكل الكتروني في مدة محددة ومعقولة³.

¹ نقلا عن بن تركي ليلي، الحماية الجنائية لبطاقة الائتمان المغنطة، تخصص قانون العقوبات والعلوم الجنائية، أطروحة لنيل درجة دكتوراه، جامعة الإخوة منتوري، قسنطينة، (2016-2017)، ص 67.

² هداية بوعزة، المرجع السابق، ص (101-102).

* الشيكات الالكترونية هي نوعين: الشيك الالكتروني المباشر على الانترنت والذي يميز بين حالتين، حالة إتمام العملية دون تدخل الوسيط، وحالة تدخل الوسيط لإتمام العملية، النوع الثاني للشيك الالكتروني هو الشيك الالكتروني المغنط. كردي نبيلة، (الشيك الالكتروني)، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، الجزء الثاني، العدد الثالث عشر، 2017، ص (253-254).

³ الخامس فاضيلي، (الشيك الالكتروني من الوجهة القانونية: خطوات استخدام الشيك الالكتروني)، 2017 <http://juris.ma/ar/annuaire/fadili-el-khamis/publication.juin> اطلع عليه بتاريخ 25 جوان 2020 على الساعة 23:03.

- الخطوة الثالثة: يقوم الساحب بتحرير الشيك وتوقيعه بشكل الكتروني متضمنا جميع البيانات المطلوبة في الشيك الالكتروني، ثم ينتقل الشيك من الساحب إلى المستفيد بواسطة بريده الالكتروني أو أية وسيلة الكترونية أخرى.
- الخطوة الرابعة: يستلم المستفيد الشيك الالكتروني على بياناته ويتحقق من الساحب والمبلغ، يوقع المستفيد على الشيك الالكتروني ثم يرسله للبنك ليتحقق هذا الأخير من صحة البيانات والأرصدة، فإذا كانت صحيحة يحول قيمة الشيك من رصيد الساحب إلى رصيد المستفيد¹.

ثانيا/ السفتجة الالكترونية:

يطلق على السفتجة مصطلح "الكمبيالة"، وهي تلك الورقة التجارية التي تتضمن أمرا صادرا من شخص يسمى الساحب إلى شخص يسمى المسحوب عليه بأن يدفع لأمر شخص ثالث هو المستفيد مبلغا معينا في ميعاد معين².

بدأ العمل بالسفتجة الالكترونية في 2 جويلية سنة 1983 في فرنسا، نتيجة جهود لجنة (GILLET) المتعلقة بتخفيض ائتمان قصير الأجل، وهي عبارة "عن محرر شكلي، ثلاثي الأطراف معالج الكترونيا، بصورة كلية أو جزئية، يتضمن أمرا من شخص يسمى الساحب إلى شخص آخر يسمى المسحوب عليه بأن يدفع مبلغا من النقود لشخص ثالث يسمى المستفيد لدى الإطلاع أو في تاريخ معين".

وتشتمل السفتجة الالكترونية على بيان اسم بنك المسحوب عليه، رقم حسابه، أو اسم الفرع الذي يوجد به الحساب ورقمه³.

¹ هداية بوعزة، المرجع السابق، ص102.

² لوصيف عمار، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين مع الإشارة إلى التجربة الجزائرية، مذكرة لنيل شهادة ماجستير، تخصص التحليل و الاستشراف الاقتصادي، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، (2008-2009)، ص21.

³ واقد يوسف، النظام القانوني للدفع الالكتروني، مذكرة لنيل شهادة ماجستير، تخصص قانون التعاون الدولي، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2011، ص54.

* نصت المادة 390 من الأمر 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن للقانون التجاري، جريدة رسمية عدد 101 الصادرة في 19 ديسمبر 1975 المعدل والمتمم بالقانون 05-02 المؤرخ في 6 فبراير 2005 جريدة رسمية عدد

تستخدم السفتجة الالكترونية كأداة للوفاء لأن إجراءات الحصول على الدين الثابت فيها بسيطة، وغالبا ما تتضمن شرط الرجوع بلا مصاريف أو بدون احتجاج ويعفى حامل من مراعاة إجراءات الاحتجاج ومواعيده للمحافظة على الحق في الرجوع، وهذا لا يعفيه من مطالبة المسحوب عليه بقيمة السفتجة في ميعاد استحقاقها، لا يعتبر حامل السفتجة الالكترونية مهملا. كما نجد أنها لا تتعرض لمخاطر الضياع والسرقة أو التزوير هذا قد ساهم بشكل كبير في التعامل بهذه السندات التجارية الالكترونية. فيما تعلق بمجال الوفاء بالديون التجارية¹.

ثالثا/ السند لأمر الالكتروني:

تضمن القانون التجاري الجزائري أحكام السند لأمر في المواد من 465² إلى 471 منه واعتبره ورقة مكتوبة يلتزم الساحب فيها بأن يدفع لمستفيد معين أو لأمره في تاريخ معين مبلغ محدد فالأطراف المتعاملة بالسند لأمر تتمثل في الساحب والمستفيد³، أما السند لأمر الالكتروني فقد عرفه الفقهاء⁴ على أنه: "عبارة عن محرر شكلي ثنائي الأطراف معالج الكترونيا بصورة كلية أو جزئية يتضمن تعهدا من محرره بدفع مبلغ من النقود في تاريخ معين لإذن شخص آخر يسمى المستفيد".

11 الصادرة في 9 فيفري 2005، على البيانات الواجب توافرها في السفتجة التقليدية وتتمثل في: "تسمية السفتجة في متن السند نفسه أو باللغة المستعملة في تحريره، أمر غير معلق على قيد أو شرط بدفع مبلغ معين...".
*ظهر نوعين للسفتجة الالكترونية يمكننا التمييز بين: السفتجة الورقية أو المقترنة بكشف والتي تحرر على دعامة ورقية وبعدها يقوم البنك بنقل البنك البيانات الأساسية الموجودة في السفتجة الورقية إلى السفتجة الممغنطة. أما النوع الآخر فهي السفتجة الالكترونية الممغنطة والتي تحرر على دعامة ممغنطة مباشرة، يتم تحرير وتداول هذا النوع من السفتجة في كل مراحلها بالطرق الالكترونية. حابت آمال، التجارة الالكترونية في الجزائر، أطروحة لنيل درجة دكتوراه، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2015، ص(73-74).

¹ واقد يوسف، المرجع السابق، ص74.

* نصت المادة 465 من التقنين التجاري على البيانات اللازمة التي يتضمنها السند لأمر و تتمثل في: "شرط الأمر أو تسمية السند مكتوبة في نفس النص وباللغة المستعملة لتحريره، الوعد بلا قيد ولا شرط بأداء مبلغ معين...".

³ زماموش ندير، آليات الدفع الالكترونية، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق، جامعة الجزائر 1، (2017-2018)، ص100.

⁴ نقلا عن عامر محمد بسام مطر، المرجع السابق، ص33.

يلاحظ من خلال هذا التعريف أن العلاقة تقوم بين طرفين فقط وفي الغالب يكونان طبيعيين، ولكن يمكن للبنك أن يكون طرفاً في هذه العلاقة وذلك في حالتين: في حالة ما إذا تدخل البنك بطريقة مباشرة عن طريق القروض البنكية، أو في حالة ضمان السند حيث يكون البنك ضامناً أمام المستفيد¹، أما فيما يتعلق بتحرير السند لأمر الالكتروني فهو كما كان سابقاً في السند لأمر التقليدي، أي أنه بعد تحريره من طرف المحرر في صورة ورقية يسلمه إلى مصرفه، وهذا الأخير ينقل البيانات على الشريط الممغنط ثم يحتفظ به ويتم تداول هذا الشريط الممغنط الذي يحتوي على بيانات السند من بنك المستفيد إلى المقاصة بواسطة الحاسب الآلي ثم إلى بنك المحرر الملتزم بالوفاء².

الفرع الثاني: البطاقات الالكترونية

تعتبر البطاقات الالكترونية من بين وسائل الدفع الأكثر انتشاراً في الفترة الأخيرة، نظراً لاستعمالاتها الكثيرة ولما توفره من سرعة في المعاملات، وهذا ما تقتضيه التطورات التكنولوجية والتجارة الالكترونية، لذلك كان لزاماً علينا التطرق لمفهوم هذه البطاقات في النقاط التالية:

أولاً/ تعريف البطاقات الالكترونية:

تعرف البطاقات الالكترونية من الناحية الشكلية أنها عبارة عن قطعة بلاستيكية أو معدنية مستطيلة الشكل، مكتوب عليها بحروف نافرة اسم حاملها، تاريخ إصدارها، تاريخ انتهاء صلاحيتها، رقم تسلسلها، توقيع حاملها وغيرها من البيانات الخاصة بهذه البطاقة³. وتعرف من الناحية الفقهية¹ على أنها: "عقد يتعهد بمقتضاه مصدر البطاقة لفتح اعتماد بمبلغ معين لمصلحة شخص آخر هو حامل البطاقة الذي يستطيع بواسطتها الوفاء

¹ عبد الله ليندة، النظام القانوني لبطاقة الدفع، مذكرة لنيل شهادة ماجستير، تخصص قانون خاص، كلية الحقوق، جامعة جيجل، 2007، ص 27.

² بحماوي الشريف وسليمان مصطفى، (خصوصية وسائل الوفاء الالكتروني ودورها في المعاملات التجارية)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية، أدرار، المجلد الأول، العدد السابع، 2017، بدون صفحة.

³ عبد الحكيم أحمد محمد عثمان، أحكام البطاقات الائتمانية في القانون والآراء الفقهية الإسلامية، دار الفكر الجامعي، الإسكندرية، 2007، ص 19.

بمشتريات حاملي البطاقات الصادرة عن الطرف الأول على أن تتم التسوية النهائية بعد مدة معينة".

وأما قانونا فقد أشار المشرع الجزائري إلى البطاقات الالكترونية في القانون التجاري في الفصل الثالث منه بعنوان "في بطاقات السحب والدفع" من الباب الرابع المعنون ب "في بعض وسائل وطرق الدفع" من الكتاب الرابع "السندات التجارية" في المادة 543 مكرر 23 من التقنين التجاري على أنها: "تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو بتحويل أموال، وتعتبر بطاقة سحب كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب أموال".

حصر المشرع الجزائري صلاحية إصدار بطاقات الدفع الالكتروني في البنوك دون سواها، وهذا ما نصت عليه المادة 71 من الأمر 03-11 المتضمن قانون النقد والقرض على أنه: "لا يمكن للمؤسسات المالية تلقي الأموال من العموم، ولا إدارة وسائل الدفع أو وضعها تحت تصرف زبائنهم. وبإمكانها القيام بسائر العمليات الأخرى".

نلاحظ من خلال التعريفات السابقة للبطاقات الالكترونية أنه تنتج عنها علاقة تعاقدية ثلاثية، وبالتالي تستوجب وجود الأطراف الثلاثة المتمثلين في كل من مصدر البطاقة وهو البنك أو المؤسسة المالية المتعاقدة مع "المركز العالمي للبطاقات"²، وحصولها على ترخيص لإصدارها، والتاجر المتمثل في كل من الشركات أو المؤسسات صاحبة السلع ومحلات البيع، ونجد حامل البطاقة طرفا في هذه العلاقة وهو الشخص الذي حصل على

¹ نقلا عن عديدان مرزوق عبد الله إنصافي، التنظيم القانوني لبطاقات الائتمان الصادرة عن البنوك-دراسة مقارنة بين التشريعين الأردني والكويتي، مذكرة لنيل شهادة ماجستير، تخصص قانون، جامعة آل البيت، (2015-2016)، ص19.

² يتولى المركز العالمي إنشاء البطاقات الالكترونية ومنح التراخيص للبنوك الموجودة في جميع أنحاء العالم بالموافقة على دخولها في عضوية هذه الأداة، نجد مؤسسة فيزا العالمية، ماستر كارد، ويسترن يونين، أمريكان إكسبرس. مصطفى يوسف كافي، النقود والبنوك الالكترونية في ظل التقنيات الحديثة، دار مؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2011، ص51.

البطاقة الالكترونية بناء على طلب تقدم به إلى الجهة المصدرة مع حصوله على الموافقة¹.

ثانيا/ العلاقات التعاقدية الناشئة عن البطاقات الالكترونية:

تنشأ عن البطاقات الالكترونية علاقات تعاقدية وبالتالي تخضع للنظرية العامة للعقد "مبدأ سلطان الإرادة"، وذلك لعدم وجود أي تشريع ينظمها، فالعلاقة الأولى تجمع كل من مصدر البطاقة وحاملها، فهي تقوم على أساس عقد مكتوب يحدد التزامات الطرفين استنادا إلى قاعدة العقد "شريعة المتعاقدين"، حسب المادة 106 من التقنين المدني الجزائري التي تقضي على أنه: "العقد شريعة المتعاقدين، فلا يجوز نقضه، ولا تعديله إلا باتفاق الطرفين، أو بالأسباب التي يقررها القانون"²، ويسمى هذا العقد من الناحية القانونية بعقد الانضمام، أشار إليه الدكتور نادر شافي حين يقول "عقد الانضمام هو عقد يبرمه مصدر البطاقة مع حاملها، وهو يسمى عقد الانضمام لأن الحامل ينظم إلى نظام البطاقة والتي تصدر عن الهيئة الدولية أو عن مصرف أو شركة بترخيص من تلك الهيئة الدولية"³، وعادة ما يأخذ عقد الانضمام صورة عقد الإذعان، أي أن شروطه مطبوعة مسبقا على نموذج يوقعه العميل، وطالب البطاقة ليس له الحق في مناقشة بنود العقد⁴.

أما العلاقة الثانية فهي تربط كل من مصدر البطاقة الالكترونية مع التاجر المعتمد، والذي سمي بعقد التوريد، وفي هذا الشأن يقول الدكتور محمد شكري التباي: "الاتفاق بين

¹ خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، مذكرة لنيل شهادة ماجستير، تخصص قانون أعمال، جامعة محمد بوضياف، مسيلة، 2016، ص71.

*ظهرت عدة أنواع للبطاقات الالكترونية منها بطاقات الدفع التي تسمح لحاملها بتسديد ثمن السلع والخدمات التي يحصل عليها. بن عمير أمينة، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة لنيل شهادة ماجستير، تخصص قانون أعمال، كلية الحقوق، جامعة الاخوة منتوري، قسنطينة، (2004-2005)، ص20.

² المادة 106 من الأمر 75-58 المؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني الجزائري، جريدة رسمية عدد 78 الصادرة في 30 سبتمبر 1975، معدل ومتمم.

³ عن رضوان غنيمي، بطاقة الائتمان بين الوضع القانوني المصرفي و التأصيل الفقهي، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2012، ص100.

⁴ خشة حسيبة، المرجع السابق، ص71.

المؤسسة المصدرة والتاجر المنخرط يطلق عليه عقد التوريد أو التموين¹، فهو عقد يلتزم بموجبه أحد الأطراف وغالبا ما يقوم البنك بتسديد قيمة المشتريات والخدمات التي يقدمها الطرف الآخر وهو التاجر لحامل البطاقة الصادرة من البنك كوسيلة وفاء. وعقد التوريد هو عقد إذعان يبرم لمدة غير محددة إلا إذا اتفق الطرفان عكس ذلك، وهو قابل للتجديد ضمنيا ويخضع للقواعد العامة في القانون المدني من أهلية، رضا، محل وسبب².

فيما يخص العلاقة التعاقدية الثالثة فهي قائمة بين حامل البطاقة والتاجر المعتمد على أساس عقد البيع، وهو عقد مسمى وهو من عقود المعاوضة، ويسمى **عقد التوريد** يلتزم فيه التاجر المعتمد بنقل ملكية المشتريات لحامل البطاقة مقابل تنفيذ هذا الأخير لالتزامه وهو الدفع بالبطاقة الالكترونية وتوقيع الفاتورة عن طريق البنك، ففي هذه الحالة ينوب البنك عن الحامل في الوفاء للتاجر باعتبار الحامل مدين والتاجر دائن والبنك هو النائب³.

تكون العلاقة الرابعة والأخيرة قائمة بين البنك والمركز العالمي للبطاقات الالكترونية وهي علاقة تعاقدية إلزامية بحيث لا يمكن للبنك إصدارها دون رخصة من المركز العالمي للبطاقات، وهذا نسبة لدورها الفعال في العلاقات بين البنوك على مستوى تحصيل الديون وتسهيل عمل البطاقة الالكترونية بين التاجر والبنك والحامل وبين التاجر والبنك، فالعلاقة التي تجمع بينهما هي علاقة وساطة⁴.

ثالثا/ الطبيعة القانونية للبطاقات الالكترونية:

تقوم الطبيعة القانونية للبطاقات الالكترونية على أساس آراء فقهية مختلفة⁵، فهناك من يكتفيها على أساس طبيعة العلاقات التعاقدية بين أطرافها وذلك بإسقاطهم لأحكام العقود المسماة المعروفة على العلاقة العقدية التي تخلقها هذه البطاقات، فهناك من الفقهاء من

¹ رضوان غنيمي، المرجع السابق، ص105.

² مرشيشي عقيلة، بطاقات الائتمان في القانون الجزائري -دراسة مقارنة-، أطروحة لنيل درجة دكتوراه، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2017، ص(108-109).

³ بن عميور أمينة، المرجع السابق، ص(63-64).

⁴ رضوان غنيمي، المرجع السابق، ص112.

⁵ نقلا عن بن عميور أمينة، المرجع السابق، ص(35-36).

يراهنا على أساس أسلوب سداد الديون وعلى فكرة حوالة الدين وهناك من كيّفها على أساس عقد الكفالة إلا أنها لا تتماشى ولا تتفق مع نظام التعامل بالبطاقات الالكترونية. أما الجانب الآخر من الفقه قد كيّف هذه البطاقات الالكترونية على أنها نقود الكترونية وذلك لتشابهها مع النقود الورقية غير أنها بلاستيكية وهناك جانب من الفقه من كيّفها على أنها شيك باعتبارهما أداة وفاء، انتقدت هذه التكيّفات الفقهية¹ نظرا لما تتميز به البطاقات الالكترونية بنظام قانوني خاص بها و قائم بذاته، يحكمه العقد المبرم بين أطراف البطاقة الالكترونية والذي ينتج عنه علاقات عقدية متشابكة تختلف وتستقل عن العلاقات الناشئة عن باقي العقود المسماة في إطار القانون المدني الجزائري.

المطلب الثاني: عمليات الدفع الالكتروني

تعتبر عمليات الدفع أنظمة استفادت منها البنوك باعتبارها وسائل لنقل النقود بطريق القيود الحسابية بواسطة الأجهزة الالكترونية من حساب الأمر إلى حساب المستفيد، وعلى البنك تنفيذ الالتزام على أساس عقد فتح الحساب، وتقسم هذه الأنظمة إلى المقاصة الالكترونية، التحويل الالكتروني والاعتماد المستندي الالكتروني².

الفرع الأول: المقاصة الالكترونية

تتميز المقاصة الالكترونية بأنها عملية معقدة باعتبارها عملية مركبة من جهة، وتنشئ علاقات قانونية متشابكة من جهة أخرى، فهي بمثابة منعرج هام في تطوير القطاع المصرفي لما تتسم به من سرعة و دقة في المعاملات³.

أولا/ تعريف المقاصة الالكترونية:

تعرف المقاصة الالكترونية بأنها: "نظام يسمح بالمعالجة عن بعد لجميع أوامر الدفع التي يتم تبادلها بصفة مجردة بين البنوك والمؤسسات المالية، وتعرف بنظام الدفع الشامل

¹ نقلا عن بن عميور أمينة، المرجع السابق ، ص46.

² طارق محمد عودة الله الشقيرات، مسؤولية البنوك في التحويل الالكتروني للأموال-دراسة في التشريع الأردني-، مذكرة لنيل شهادة ماجستير، تخصص قانون، الجامعة الأردنية، 2005، ص10.

³ مسيدري سيد أحمد، النظام القانوني للمقاصة في المعاملات البنكية -دراسة مقارنة-، أطروحة لنيل درجة دكتوراه، تخصص قانون خاص، جامعة أبو بكر بلقايد، تلمسان، (2017-2018)، ص131.

للمبالغ الصغيرة، بحيث تتم المقاصة بصورة آلية بين البنوك بالاعتماد على الربط الشبكي فيما بينها وهذا تحت إشراف وإدارة البنك المركزي¹.

تطرق المشرع الجزائري لعملية المقاصة الالكترونية من خلال النظام رقم 05-06 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى في المادة الثانية منه التي تقضي بأنه: "ينجز بنك الجزائر نظام المقاصة الالكترونية الذي يدعى نظام الجزائر للمقاصة المسافية ما بين البنوك-أتكي-(ATCI). ويتعلق الأمر بنظام ما بين البنوك للمقاصة الالكترونية للصكوك والسندات والتحويلات والاقتطاعات الأوتوماتيكية السحب والدفع باستعمال البطاقة المصرفية.

لا يقبل هذا النظام إلا التحويلات التي تقل قيمتها الاسمية عن مليون (1) دينار. يجب أن تنفذ أوامر التحويل، التي تفوق أو تساوي قيمتها الاسمية هذا المبلغ، ضمن نظام التسوية الإجمالية الفورية للمبالغ الكبير والدفع المستعجل.

يشتغل نظام أتكي(ATCI) وفقا لمبدأ المقاصة المتعددة الأطراف لأوامر الدفع التي يقدمها المشاركون في هذا النظام².

تتمتع أيضا بعدة خصائص فهي أداة وفاء مزدوجة، آمنة وسرية في نقل البيانات وذلك باعتماده على مزايا أمنية متوفرة في النظام من تشفير البيانات المرسله وتوثيقها وتنفيذ المقاصة بواسطة وسائل الكترونية تتمثل في الأجهزة الكهربائية وغيرها³.

ثانيا/ إجراءات المقاصة الالكترونية:

يتضمن نظام المقاصة الالكترونية إجراءات:

¹ دحية رباب، دراسة تحليلية لأداء أنظمة الدفع - حالة نظام الدفع المكثف بالجزائر -، مذكرة لنيل شهادة ماجستير، تخصص مالية بنوك وتأمينات، جامعة مسيلة، (2011-2012)، ص56.

² المادة 2 من النظام 05-06 المؤرخ في 15 ديسمبر 2005 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى، جريدة رسمية عدد 26 مؤرخ في 23 أبريل 2006.

³ هند فالح محمود وصون كل عزيز عبد الكريم، (المقاصة الالكترونية والمسؤولية المدنية التي تنجم عنها)، مجلة الراصد للحقوق، المجلد 18، العدد 23، 2020، ص51.

- إجراء المقاصة الواردة: تتضمن تقديم الشيك من المستفيد إلى البنك الذي بدوره يقوم بتنفيذ مجموعة من الإجراءات للتأكد من البيانات الواردة، بعد ذلك يتم إدخال الشيك في النظام¹.
- إجراء المقاصة الصادرة: وتكون في مرحلة تلقي البنك للشيك فيقوم باستيفاء كافة المعلومات المتعلقة به، ثم يرسلها إلى البنك المسحوب عليه فيتأكد نظام الرسائل الالكترونية من قبل البنك المرسل لمطابقة المواصفات الفنية، فيحول فوراً الصور المختومة للشيكات، السفاتج، السندات لأمر، ثم إرسالها إلى المرسل إليه².

ثالثاً/ أنواع المقاصة الالكترونية:

تنقسم المقاصة الالكترونية إلى عدة أنواع؛ النوع الأول يتمثل في المقاصة الالكترونية التي تتم على مستوى غرفة المقاصة الموجودة في البنك المركزي للدولة، لتشمل نظام التسوية الإجمالية الفورية ويطبق لتسوية المدفوعات المحلية كبيرة القيمة والتي تتطلب درجة عالية من السيولة والسرعة لإجرائها³، ونظام الجزائر للمقاصة المسافية بين البنوك⁴.

أما النوع الثاني يكون خارج غرفة المقاصة عن طريق اتفاق البنوك⁵، ويتفرع عنه المقاصة الالكترونية البسيطة، وتكون بين حسابين لشخص واحد أو حسابين لشخصين مختلفين وتكون على مستوى نفس البنك، ونجد أيضاً المقاصة الالكترونية الثنائية تتم بين حسابين مفتوحين في بنكين مختلفين سواء كان الحسابان لنفس الشخص أو لشخصين

¹ مسيدري سيد أحمد، المرجع السابق، (ص241-ص243).

² حدوم ليلي، المرجع السابق، ص(106-107).

³ مسيدري سيد أحمد، المرجع السابق، ص148.

⁴ حدوم ليلي، المرجع السابق، ص3.

⁵ مسيدري سيد أحمد، المرجع السابق، ص139.

مختلفين، يتضمن هذا النوع أيضا المقاصة الالكترونية المركبة وهي أن يشترك في عملية المقاصة أكثر من بنكين¹.

الفرع الثاني: التحويل الالكتروني للأموال

يعد نظام التحويل الالكتروني إحدى أهم العمليات المصرفية التي تنفذها البنوك الكترونيا، وذلك من خلال شبكات الاتصال العالمية على الانترنت.

أولا/ تعريف التحويل الالكتروني للأموال:

يعتبر التحويل الالكتروني للأموال عملية قانونية استنادا لما تقتضيه المادة 51 من الأمر 03-11 المتعلق بالنقد والقرض التي تنص على أنه: "يمكن بنك الجزائر أن يجري كل العمليات المصرفية مع البنوك والمؤسسات المالية العاملة في الجزائر ومع كل بنك مركزي أجنبي. ولا يمكنه أن يتعامل مع البنوك العاملة بالخارج، إلا في عمليات بالعملات الأجنبية". وباستقراء المادة 543 مكرر 19 من التقنين التجاري نجد أن المشرع الجزائري لم يعرف التحويل الالكتروني وإنما أورد الإجراءات الشكلية التي يجب أن تتقيد بها البنوك لإتمام هذه العملية والمتمثلة في الأمر الذي يوجهه صاحب الحساب إلى ماسك الحساب لتحويل الأموال والقيم والسندات المحددة القيمة، بيان الحساب الذي يتم الخصم منه، بيان الحساب الذي يتم إليه التحويل وصاحبه، تاريخ التنفيذ وتوفير الأمر بالتحويل².

وعملية التحويل الالكتروني هي الإجراء الذي يقوم به البنك بنقل مبلغ من المال من حساب عميل إلى حساب عميل آخر وهو المحول إليه أو يقوم الأمر بإيداع هذا المبلغ في حساب آخر له في البنك نفسه، ونلاحظ أن البنك قد سهل عملية النقل المادي للأموال ويكون ذلك بشكل الكتروني دون حضور الأمر³.

¹ صفاء يوسف القواسمي، المسؤوليات القانونية الناشئة عن عمليات المقاصة الالكترونية للشبكات في القانون الأردني، مذكرة لنيل شهادة ماجستير، تخصص قانون خاص، جامعة الشرق الأوسط للدراسات العليا، الأردن، 2009، صص (30-32).

² غزالي نزيهة، المسؤولية الجزائية عن استخدام وسائل الدفع الالكتروني في القانون الجزائري، أطروحة لنيل شهادة دكتوراه، جامعة محمد لمين دباغين، سطيف، 2017-2018، صص (76-77).

³ يوسف بوهدون، الجوانب القانونية لوسائل الوفاء الالكترونية، ص27، [https:// drive.google.com](https://drive.google.com)، اطلع عليه يوم 28 جوان 2020 على الساعة 16:43.

ثانيا/ إجراءات عملية التحويل الالكتروني:

تتخذ عملية التحويل الالكتروني بتوقيع العميل نموذجا معتمدا لصالح الجهة المستفيدة(التاجر)، ويمكن اقتطاع القيمة المحددة من حساب العميل عن طريق هذا النموذج وفق ترتيب زمني معين، ولإتمام عملية التحويل المالي الكترونيا¹ يجب أن تمر بمرحلتين:

✓ **مرحلة إصدار الأمر بالتحويل:** تبدأ عملية التحويل الالكتروني للأموال بإصدار أمر من الأمر يوجهه إلى البنك، يطلب فيه تحويل مبلغ مالي من حسابه إلى حساب آخر، فهو الوسيلة التي يستعملها الأمر لتحريك حسابه وهذا الأمر لا يشترط فيه أن يكون صادرا ممن يملك الحق في إصداره أي ممن يملك سلطة تحريك الحساب².

✓ **مرحلة إصدار تنفيذ الأمر بالتحويل:** يمر تنفيذ الأمر بالتحويل بمرحلتين:

- **القيد بالخصم من حساب الأمر:** نص المشرع الجزائري في خلال المادة 543 مكرر 20 من التقنين التجاري بأنه:"يكون الأمر بالتحويل غير قابل للرجوع فيه ابتداء من تاريخ الاقتطاع من حساب الأمر بالتحويل..."، يتبين من هذا النص أن الرصيد يبقى في حيازة الأمر بالتحويل حتى لحظة القيد بالخصم في حسابه لدى المصرف، أي أنه قبل إجراء القيد بالخصم يكون للأمر السيطرة التامة على الرصيد ومن حقه الرجوع في الأمر بالتحويل، لكن الرجوع يكون قبل اقتطاع البنك للمبلغ المحدد في الأمر.

- **القيد بالإضافة في حساب المستفيد:** يقوم المصرف بعد إتمام عملية التحويل بتسليم النقود القيدية والتي تعرف بعملية القيد بالإضافة في حساب الدائن للمستفيد وتبرأ ذمة الأمر بالتحويل، وفي هذه الحالة لا يمكن لهذا الأخير الرجوع عن أمره بالتحويل لأنه أصبح نهائي، ولا يمكن للبنك استخراج النقود من حساب المستفيد لأن البنك مؤتمن على أدراج العملاء ولا تغيير محتوياتها دون رضاهم. أما في حال تم التحويل بين حسابين في

¹ نوال بن عمارة، وسائل الدفع الالكتروني (الأفاق والتحديات)، كلية الحقوق والعلوم الاقتصادية، جامعة ورقلة، ص12، <https://dSPACE.univ-ouargla.dz> اطلع عليه يوم 28 جوان 2020 على الساعة 17:08.

² طارق محمد عودة الله الشقيرات، المرجع السابق، ص32.

مصرفين مختلفين فذلك يتطلب إجراء عدد من القيود المحاسبية بين الأمر والمستفيد وتكون عن طريق تسوية بين البنوك¹.

الفرع الثالث: الاعتماد المستندي الالكتروني

تطور الاعتماد المستندي من تقليدي إلى الكتروني نظرا لاتساع مجال استعمال التكنولوجيا الحديثة، فاهتمت به البنوك والمؤسسات المالية وأصبحت تعتمد عليه في مجال التجارة الدولية للحصول على تمويل وتحسين نوعية الخدمات المقدمة لزيائنها، ومواكبة المنافسة في العمليات التجارية الدولية التي لم تكن متوفرة من قبل.

أولا/ تعريف الاعتماد المستندي الالكتروني:

يعرف الاعتماد المستندي الالكتروني بأنه عملية يتم من خلالها تبادل الوثائق والمستندات عن طريق البريد الالكتروني، ويتم الدفع فيه لمصلحة البائع بواسطة التحويل الالكتروني للأموال، ويساهم في تمويل التجارة الخارجية وتسهيل عمليات تبادل السلع والخدمات في الخارج، كما يخفف من العراقيل التي تواجهها البنوك.

والاعتماد المستندي الالكتروني هو إحدى صور المبادلات التجارية الدولية وأفضل ضمان للبائع والمشتري²، وذلك باعتماده لنظام "سويفت"³ الذي يقتصر على العلاقات بين البنوك فهي شبكة مزودة بنظام تشفير يصعب على الغير اختراقه⁴. ويختلف الاعتماد المستندي الالكتروني عن التقليدي في كونه دعامة الكترونية غير ملموسة على عكس التقليدي الذي يكون في شكل ورقي، أما من الناحية القانونية نجد أن لهما نفس القيمة القانونية، إلا أنه يضاف للاعتماد المستندي الالكتروني بعض الشروط المتمثلة في قابلية

¹ خشة حسية، المرجع السابق، ص(178-179)

² عبد الله ليندة، (تبييض الأموال عن طريق الاعتماد المستندي الالكتروني)، مداخلة في أعمال المؤتمر الدولي الرابع عشر بعنوان: الجرائم الالكترونية، جامعة محمد الصديق بن يحيى، جيجل، 2017، صص(2-4)،

www.jilrc.com

³ يعرف نظام السويفت بأنه: "نظام مركزي عالمي، يستخدم لتنفيذ الحوالات المالية المتبادلة بين البنوك العالمية الكترونيا وذلك باعتماد مقاييس دولية، من خلال رمز محدد لكل بنك يسمى سويفت كود". عبد الله ليندة، المرجع السابق، ص242.

⁴ سعدي عبد الحليم، (الأرضية القانونية للاعتماد المستندي الالكتروني)، مجلة الفكر، جامعة قسنطينة1، العدد9، ص89.

المعلومات للقراءة من خلال الحواسيب بلغة مفهومة وضرورة العمل على توفير الأمان لمستخدمي هذا النظام¹.

ثانيا/ إجراءات الاعتماد المستندي الالكتروني:

يتم إجراء الاعتماد المستندي بموافقة البنك على طلب يقدمه العميل، فيقوم البنك بإرسال الموافقة على نص الاعتماد عن طريق البريد الالكتروني، وقبل انتهاء الأجل المحدد يقوم المستفيد بإرسال كافة المستندات المتعلقة بموضوع فتح الاعتماد للحصول على قيمتها بواسطة البريد الالكتروني، ويطلب من كافة الأطراف المشاركة في إجراء عملية الاعتماد المستندي وأن يقوم بإرسال مستنداتهم للبنك عبر الانترنت. وفي حالة تدخل أكثر من بنك يقوم البنك صاحب الاعتماد بإرسال جميع الرسائل الالكترونية الواردة إليه إلى البنك المستفيد، وإذا كانت المستندات موافقة لما ورد في الاعتماد فإنه يقوم بتحويل المبلغ بصورة الكترونية².

المبحث الثاني: الآثار المترتبة عن الاستخدام غير المشروع لوسائل الدفع الالكتروني

تواجه البنوك العديد من المخاطر من جراء اعتمادها لآليات الدفع الالكتروني، بعضها مرتبط بوسيلة الدفع ذاتها والتي تشكل مخاطر أمنية (المطلب الأول) والبعض الآخر جرائم يرتكبها المتعاملين لهذه الوسائل باستخدامها غير مشروع مما أدى إلى توسع دائرة الجرائم المرتكبة باستخدام وسائل الدفع الالكتروني (المطلب الثاني).

المطلب الأول: المخاطر الأمنية لوسائل الدفع الالكتروني

تشمل المخاطر الأمنية المخاطر التقنية المرتبطة بالوسيلة والتي يقصد بها تلك المخاطر التي قد تعتري وسيلة الدفع الالكتروني جراء اختلالات أو حدوث تقصير في

¹ عبد الله ليندة، المرجع السابق، ص(4-5).

² شفارة عبد النور. حماية المستهلك في الخدمات المصرفية الالكترونية، مذكرة لنيل شهادة ماجستير، تخصص قانون خاص، جامعة الجزائر 1، (2014-2015)، ص18.

صيانتها والتي تتسبب في القصور الوظيفي لها، إلى جانب ذلك المخاطر المتعلقة بضياع وسيلة

وسيلة الدفع أو سرقتها من حاملها الشرعي ما يترتب عليه جرائم البطاقات الالكترونية.

الفرع الأول: القصور الوظيفي لوسيلة الدفع الالكتروني

تتعرض وسيلة الدفع الالكتروني لأعطال قد تكون ناتجة عن اختلال في تصميم أداة الدفع أو قصور في عملية الصيانة، هذا ما يؤدي بالأداة إلى عدم القيام بالعمل الذي وجدت لأجله.

أولا/ القصور الوظيفي لوجود عيب في أداة الدفع الالكتروني:

تسعى البنوك إلى اكتساب ثقة العملاء من خلال التكوين الجيد للموظفين وتوفير خدمات إضافية للعملاء¹، ولكن قد يتعرض العميل إلى أضرار في حالة وجود عيب في أداة الدفع الالكتروني، وتتعلق مخاطر القصور الوظيفي بأول مرحلة من مراحل النظام وهي مرحلة إدخال البيانات إلى النظام الآلي وتتمثل في الإدخال غير المتعمد لبيانات غير سليمة، أو الإدخال المتعمد لبيانات غير سليمة، التدمير غير المتعمد للبيانات، أو حتى التدمير المتعمد للبيانات والتي تكون بسبب الموظفين. فمخاطر القصور الوظيفي قد تؤثر على الموردين الآخرين للخدمات البنكية الالكترونية لذلك تقوم جهات الإشراف على البنوك بوضع إرشادات داخلية لمن يقومون بالفحص².

ويترتب عن هذه الأعطال في وسيلة الدفع فقدان العميل لأرصدة نقدية الكترونية أو حرمانه من الحصول على متطلباته نتيجة عدم تمكنه من إجراء مدفوعاته في الوقت المناسب³، هذا ما يستدعي مساءلة مؤسسات النقد الالكتروني عما لحق العميل من خسارة وما لحقه من أضرار جراء هذا العيب الموجود في الأداة، بغض النظر عن مصدرها وما إذا كانت ناتجة عن أعطال تقنية، هذا ما يساعد على إقبال العملاء على

¹ لعايب وليد، (تقييم تجربة نظام الدفع الالكتروني الجزائري في ظل ثورة التكنولوجيا المصرفية، دراسة مقارنة مع تجربة نظام الدفع الالكتروني الأوروبي)، مجلة أبحاث ودراسات التنمية، المجلد 4، العدد 2، 2018، ص 139.

² نوال بن عمارة، المرجع السابق، ص (16-17).

³ هداية بوعزة، المرجع السابق، ص 319.

وسائل الدفع الالكتروني دون الخشية من ضياع حقوقهم بسبب صعوبة إثبات ذلك العطل الموجود في أداة الدفع ويدفع أيضا الجهات المصدرة نحو تحديث وتطوير نظم الدفع الخاصة بها، لضمان عدم حدوث عطل أو أضرار للعميل لاستخدامه وسيلة دفع الكترونية.

ثانيا/ القصور الوظيفي لوجود تقصير في صيانة وسيلة الدفع الالكتروني:

تعتمد أنظمة الدفع الالكتروني على نظم المعلومات وتقنية شبكات الاتصال الالكترونية، فالعلاقة التي بينهما قد تزيد من حجم المخاطر أو قد تتشأ بسبب عدم كفاءة النظم المتبعة لمواجهة متطلبات العملاء أو قد يعود للسرعة في إجراء الصيانة الطارئة أو الدورية التي تتطلبها شبكات الاتصال¹.

وقد تستند أنظمة الدفع أيضا إلى تقنيات غير متطورة أو تقنية واحدة مشتركة للعديد من أنظمة التشغيل أو الأجهزة المستخدمة، ما يؤدي إلى إحداث عطل في هذه الأنظمة والشبكات المرتبطة بها، في حالة حدوث أي مشكلة تتعلق بالبرمجة أو البنية التحتية الالكترونية، وبالتالي يتم الاعتماد على مصادر تقنية لتقديم الدعم التقني، بشأن البنية الأساسية اللازمة لصيانة الشبكات وغيرها من الأجزاء المادية التي تصيب البنوك بواسطة استعمالها لوسائل الدفع الالكتروني².

ويتحمل البنك مسؤولية الأضرار التقنية الناتجة عن استعمال أداة الدفع سواء يرجع ذلك إلى سوء في العمل أو الوظيفة أو إلى التقنية المستعملة، فالمسؤولية المترتبة عن البنوك تعتبر حافز لها لتبني تكنولوجيا آمنة تعمل بشكل جيد وتفادي الأعطال التقنية وتجنب وقوع أي خسارة أو إضرار بالعميل³.

¹ حوالف عبد الصمد، النظام القانوني لوسائل الدفع الالكتروني، أطروحة لنيل درجة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، (2014-2015)، ص(319-320).

² هداية بوعزة، المرجع السابق، ص320.

³ علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، دار الجامعة الجديدة للنشر، الإسكندرية، 2012، ص(433-434).

الفرع الثاني: جرائم البطاقات الالكترونية

تعتمد البطاقة الالكترونية على تقنية تأمين ما يجعلها وسيلة توفر لحاملها الأمان لدى استعمالها، ولكن ما يعاب عنها هو إمكانية الاعتداء على نظامها واستخدامها بشكل خاطئ سواء صدر ذلك عن الحامل أو الغير.

أولا/ الاستعمال غير المشروع للبطاقات الالكترونية من قبل الحامل:

يتعسف الحامل الشرعي في استعماله للبطاقة الالكترونية باعتماده على طرق احتيالية، بهدف الاستفادة منها دون دفع ما عليه من مستحقات، خلال فترة صلاحية البطاقة أو بعد انتهاء صلاحيتها.

1/ الاستعمال غير المشروع للبطاقة الالكترونية أثناء فترة الصلاحية:

يكون الاستعمال غير المشروع للبطاقة الالكترونية في فترة صلاحيتها عن طريق تجاوز الحامل لرصيده¹، وهو عالم بأنه لا يملك رصيد كاف لتغطية السلع والخدمات، فيشتريها الحامل دون دفع قيمتها نقداً، فتلتزم الجهة المصدرة للبطاقة الالكترونية بالوفاء خلال فترة محددة بقيمة تلك المقتنيات².

كما تقوم جريمة أخرى عن الاستعمال غير الشرعي لهذه البطاقة وهو سحب الحامل مبلغ من جهاز السحب الآلي مع العلم بعدم وجود رصيد فعلي، ويكون في حالات نادرة عندما يصيب الجهاز عطل فني أو قصور التعليمات المعطاة له، فتخرج نقود متجاوزة للسقف المسموح به حسب طلب الحامل³.

وتقوم جريمة الحصول على البطاقة الالكترونية بطريقة غير شرعية بتقديم سندات مزورة، فيتوجب على الحامل تقديم بيانات صحيحة وغير مخالفة للحقيقة، ولا يجوز له تقديم أسماء وهمية أو منتحلة أو ضمانات غير حقيقية فيعتبر من الاعتداءات الأكثر شيوعاً،

¹ بن تركي ليلي، المرجع السابق، ص 77.

² عبد الكريم الردايدة، المرجع السابق، ص 212.

³ عبد الكريم الردايدة، المرجع نفسه، ص 209.

فيتحمل البنك الخسائر نتيجة هذا الغش وعدم قدرته للوصول إلى الحامل وذلك بسبب عدم صحة المعلومات التي قدمها¹.

يكيف جانب من الفقه² الاستعمال غير المشروع للبطاقات الالكترونية من قبل حاملها على أساس جريمة السرقة وهذا حسب ما جاء في المادة 350 من تقنين العقوبات الجزائري التي تنص على أنه: "كل من اختلس شيئاً غير مملوك له يعد سارقاً...".

يكيفها جانب من الفقه³ على أنها جريمة نصب (احتيال)، حسب المادة 372 من تقنين العقوبات الجزائري التي تقضي على أنه: "كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية... وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه...". وجانب آخر من الفقه⁴ كيفها على أساس جريمة خيانة الأمانة حسب المادة 376 من تقنين العقوبات الجزائري التي تنص على أنه: "كل من اختلس أو بدد بسوء نية أوراقاً تجارية أو نقوداً أو بضائع أو أوراقاً مالية أو مخالصات أو أي محررات أخرى تتضمن أو تثبت التزاماً أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجارة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجل أو بغير أجل بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضراراً أو واضعي اليد عليها أو حائزها يعد مرتكباً لجريمة خيانة الأمانة...".

2/ الاستعمال غير المشروع للبطاقة الالكترونية المنتهية الصلاحية:

تكون البطاقة الالكترونية منتهية الصلاحية، في حالتين، في حالة ما إذا انتهت صلاحيتها المحددة في الاتفاق بين الحامل والجهة المصدرة لها، فيستعملها الحامل ويمتنع عن ردها للبنك باعتباره مالهما، وفي حالة إلغائها نتيجة تعسف الحامل في استخدامها سواء في السحب أو الوفاء أو لعدم سداده لمدىونيته في المواعيد المتفق عليها⁵. وأغلب الفقه⁶ كيفها على أنها جريمة خيانة الأمانة وهذا طبقاً للمادة 376 من

¹ مرشيشي عقيلة، المرجع السابق، ص(239-240).

² نقلاً عن بن عمير أمينة، المرجع السابق، ص127.

³ نقلاً عن مرشيشي عقيلة، المرجع السابق، ص248.

⁴ نقلاً عن مرشيشي عقيلة، المرجع نفسه، ص250.

⁵ عبد الكريم الردايدة، المرجع السابق، ص60.

⁶ نقلاً عن مرشيشي عقيلة، المرجع السابق، ص(264-265).

تقنين العقوبات الجزائري - السالفة الذكر-، فبمجرد فسخ العقد أو انتهائه يجب رد البطاقة أو تصبح نية الحامل في نقل الحياة من مؤقتة إلى دائمة، كما نجد الحامل الذي استخدم بطاقة منتهية الصلاحية يكون قد ارتكب جريمة احتيال على أساس استخدامه لاسم كاذب.

ثانيا/ الاستخدام غير المشروع للبطاقة الالكترونية من قبل الغير:

يقصد بالغير هو الشخص الذي لم تصدر البطاقة الالكترونية باسمه من الجهة المختصة بإصدارها، فإذا استعملها الغير يعد هذا الفعل غير مشروع.

1/ تزوير الغير للبطاقة الالكترونية:

تحرص الجهة المصدرة للبطاقة الالكترونية على حمايتها من التزوير، غير أن التطور التكنولوجي ساهم في استخدامها استخداما غير مشروع من طرف الغير وذلك بتزويرها في إحدى صورتين، قد يأخذ صورة تزوير كلي، وذلك بتقليد الطباعة من رموز وبيانات والنقوش والرسوم على البطاقة الالكترونية، تغليف البطاقة ولصق الهولوجرام والشريط المغنط أو الشريحة الرقائقية وشريط التوقيع¹، كما تأخذ صورة تزوير جزئي عن طريق صهر البطاقة وما عليها من أرقام نافرة لبطاقة مسروقة أو انتهت صلاحيتها وإعادة قولبتها بأرقام جرى سرقة المعلومات الخاصة بطريقة غير مشروعة أو تقليد الشريط المغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة وصحيحة ومسروقة أو إجراء العمليتين معا، أو عن طريق الكشط المادي لشريط التوقيع ووضع آخر مكانه أو بطبع صورة أخرى².

وأشار المشرع الجزائري إلى جريمة التزوير في قانون العقوبات في الكتاب الثالث بعنوان الجنايات والجناح ضد الشيء العمومي في الفصل السابع تحت عنوان التزوير، في القسم المعنون بالتزوير في المحررات العرفية أو التجارية أو المصرفية في المادة 219 التي تقضي على أنه: "كل من ارتكب تزويرا بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو المصرفية أو شرع في ذلك..."

¹ مرشيشي عقيلة، المرجع السابق، ص282.

² بن تركي ليلي، المرجع السابق، ص203.

2/ استخدام الغير لبطاقة الكترونية مزورة:

يتمثل الهدف الأساسي للغير من استعماله بطاقة الكترونية مزورة هو الحصول على مال الآخرين بسحب النقود أو الوفاء بقيمة السلع والخدمات التي يحصل عليها، فتقوم هذه الجريمة على ركنين، الركن المادي يتمثل في استعمال البطاقة الالكترونية المزورة في عملية السحب أو الوفاء بقيمة المشتريات والخدمات، والركن المعنوي يتمثل في توافر القصد الجنائي في الحامل الشرعي بحيث يقوم باستعمال هذه البطاقة وهو يعلم بذلك.

تباينت الآراء الفقهية¹ حول التكييف القانوني لفعل استعمال بطاقة مزورة من طرف الغير، فهناك من يرى أنها جريمة سرقة وذلك في سحب النقود من الصراف الآلي باستعماله مفتاحاً مصطنعاً، في حين يجده الرأي الآخر أنه جريمة احتيال وذلك باعتماده على حجة أنه يجب استخدام طرق احتيالية من أجل خداع الجهاز الآلي في سحب الأموال وإيهام التجار من أجل الحصول على السلع والخدمات، أما الرأي الأخير يكتف بهذا الفعل على أنه جريمة استعمال محرر مزور، فأداة الجريمة هي البطاقة الالكترونية المستخدمة في سحب الأموال والوفاء لدى التجار، فيحتج بها الغير على أساس أنها صحيحة وهذا الرأي السليم، ويعد مرتكب لجريمة استعمال محرر مزور وجريمة احتيال باستعمال اسم كاذب².

3/ استخدام الغير لبطاقة الكترونية دون سرقتها:

أ/ استخدام بطاقة الكترونية ضائعة من قبل من عثر عليها:

يتوجب على من عثر على البطاقة الالكترونية في حالة ضياعها من صاحبها الحقيقي أن يردها إليه إذا كان يعرفه أو يسلمها إلى البنك المصدر أو الشرطة، وفي حالة استخدامها يعاقب الجاني عن جريمة النصب، لأنه قد استخدم اسماً كاذباً وصفة غير صحيحة، كما يمكن أيضاً معاقبته عن جريمة أخرى هي جريمة التزوير لأنه قام بتزوير توقيع الحامل الأصلي للبطاقة الالكترونية³. فيقوم عن استخدام بطاقة الكترونية ضائعة

¹ بن تركي ليلي، المرجع السابق، ص ص(211-213).

² بن تركي ليلي، المرجع نفسه، ص 213.

³ مرشيشي عقيلة، المرجع السابق، ص 301.

ركنين، الركن المادي يتمثل في احتفاظ الغير ببطاقة الالكترونية وعدم إعادتها لمالكها، والركن المعنوي يتمثل في القصد الجنائي وهو علم الغير بأن البطاقة ليست ملكا له واتجاه إرادته في تملكها واستعماله لاسم كاذب وخداعه للتاجر من أجل الحصول على منفعه¹.

ب/ عثور الغير على البطاقة الالكترونية وتسليمها لشخص آخر

قد يعثر الشخص على البطاقة الالكترونية فيقوم بتسليمها لشخص آخر غير مالكها الشرعي، ويرى الأستاذ كميث طالب البغدادي² بأن الشخص إذا كان لا يعلم بأن من سلمه البطاقة ليس مالكها الأصلي، ففي هذه الحالة لا يسأل عن الجريمة أما إذا كان يعلم بذلك فإنه يعد شريكا ما إذا استعملها ويسأل عن جريمة الاحتيال لأنه هدف إلى إقناع التاجر بوجود ائتمان وهمي من أجل الاستيلاء على الأموال أما إذا استخدم البطاقة الالكترونية في السحب من جهاز الصراف الآلي فيسأل عن جريمة السرقة لاستيلائه على أموال مالك البطاقة، كما يسأل على جريمة التزوير وذلك بتوقيعه على إشعار البيع، وهذا يعد تقليد لتوقيع الحامل الشرعي. ففي هذه الحالة يكون تعدد مادي لجرائم السرقة، الاحتيال والتزوير التي لا تقبل التجزئة، فترتكب تنفيذا للمشروع الإجرامي المتمثل في الحصول على السلع والخدمات من التاجر بموجب البطاقة الالكترونية المفقودة.

المطلب الثاني: توسع دائرة الجرائم المرتكبة باستخدام وسائل الدفع الالكتروني

تتميز وسائل الدفع الالكتروني بتقنية ونظام أمن عالي، مما يصعب معها ارتكاب جرائم، لكن مع التطورات التقنية الحاصلة أصبح مجال الجرائم واسع، هذا ما يثير أخطار قانونية وتقنية لا يستهان بها.

نتطرق في هذا المطلب إلى أهم الجرائم المرتكبة باستعمال وسائل الدفع الالكتروني والتي عززتها التكنولوجيا الحديثة.

¹ عبد الكريم الردايدة، المرجع السابق، ص244.

² كميث طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان (المسؤولية الجزائية والمدنية)، دار الثقافة، عمان، الأردن، 2008، ص(211-212).

الفرع الأول: القرصنة وجريمة انتهاك السرية المعلوماتية

تشكل القرصنة المعلوماتية وجريمة انتهاك السرية المعلوماتية فعل احتيالي يهدد وسيلة الدفع الالكتروني على النحو التالي:

أولاً/ جريمة القرصنة المعلوماتية:

تعرف القرصنة المعلوماتية على أنها اعتداء احتيالي لوسائل الدفع الالكتروني عن طريق التزوير أو الاحتيال، والنجاح في القيام بالمبادلات والحصول على منافع شخصية على حساب الحامل الشرعي¹.

1/ التزوير:

يعتبر التزوير من أخطر الجرائم خاصة مع ظهور التكنولوجيا الحديثة، هذا ما أدى إلى المساس بوسائل الدفع الالكتروني باعتبارها محركات الكترونية، وقد عرف الفقيه هيتي التزوير الالكتروني بقوله: "التزوير الالكتروني يختلف عن التزوير التقليدي، حيث يتضمن التزوير المعلوماتي إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو بالإضافة، إضافة أنه يتعلق بالكيان المادي للحاسب الآلي، أو البرامج ذاتها، وهو يندرج بصفة عامة تحت نطاق التزوير الالكتروني كسلوك غير مشروع يتعلق بمعالجة المعلومات ونقلها، فهو سلوك غير قانوني وغير مسموح به يتعلق بالتعامل الفوري مع المعلومات والبيانات أو انتقالها"².

يتضح من خلال التعريف أن أجهزة الكمبيوتر لها أهمية كبيرة وذلك بتسجيل كل البيانات والمعلومات في ذاكرتها أو تسجيلها على الأشرطة الممغنطة أو الأسطوانات المخزنة، فهي تشكل هدفاً للمجرمين³.

يتم تزوير البيانات بالدخول بطريقة مشروعة أو غير مشروعة لقاعدة البيانات الموجودة في نظم المعلومات وتعديلها سواء كان بإلغاء بيانات موجودة بالفعل أو بإضافة

¹ حوالف عبد الصمد، المرجع السابق، ص323.

² حفصي عباس، جرائم التزوير الالكترونية- دراسة مقارنة-، أطروحة لنيل درجة دكتوراه، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1، (2014-2015)، ص19.

³ عمر عبد السلام حسين الجبوري، جريمة التزوير الالكتروني في التشريع الأردني-دراسة مقارنة-، مذكرة لنيل شهادة ماجستير، تخصص قانون عام، جامعة الشرق الأوسط، الأردن، 2017، ص21.

بيانات لم تكن موجودة من قبل، أما تزوير التوقيع الالكتروني يكون بحصول الشخص على منظومة التوقيع الخاصة لشخص آخر بغرض استخدامها في توقيع مستندات الكترونية متحصل عليها بواسطة التجسس الالكتروني¹.

فلا تقوم جريمة التزوير إلا بقيام الركن المادي وهو تغيير الحقيقة بإحدى الطرق التي نص عليها المشرع الجزائري في المادة 216 من تقنين العقوبات التي تنص على أنه: "يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج، كل شخص، عدا من عينتهم المادة 215²، ارتكب تزويرا في محررات رسمية أو عمومية. 1- إما بتقليد أو بتزييف الكتابة أو التوقيع. 2- وإما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو إدراجها في هذه المحررات فيما بعد. 3- وإما بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو لإثباتها. 4- وإما بانتحال شخصية الغير أو الحلول محلها."، فلا يشترط أن يكون الضرر مادي أو معنوي بل يكفي أن يكون الضرر محتمل الوقوع، فالضرر المادي يتمثل في الانقاص من عناصر الذمة المالية للمتعاملين، أما الضرر المعنوي يتمثل في عدم وضع الثقة والأمان في وسائل الدفع الالكتروني، أما الركن المعنوي يتمثل في القصد الجنائي العام وهو إدراك الجاني بتغييره للحقيقة وأنه يترتب على ذلك ضررا حالا أو محتمل الوقوع لأحد المتعاملين، أما القصد الجنائي الخاص هو نية استعمال وسيلة الدفع المزورة استعمالا غير مشروع في الأغراض التي أعدت لأجله³.

2/ الاحتيال:

يعتبر الاحتيال المعلوماتي من بين الجرائم القانونية الحديثة، فهو سلوك خداعي منظم ومخطط له مسبقا مرتبط بالكومبيوتر، يهدف بواسطته شخص إلى كسب فائدة أو مصلحة مالية، فهي تعتمد على قصد الجاني للاعتداء على المعلومات بالاستعانة على

¹ حفصي عباس، المرجع السابق، ص 97.

² تقضي المادة 215 من تقنين العقوبات على أنه: "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية أثناء تحريه محررات من أعمال وظيفته بتزييف جوهرها...".

³ حوالف عبد الصمد، المرجع السابق، ص (554-555).

جهاز الكمبيوتر¹، وذلك باستخدام بعض المعلومات الالكترونية أو التواصل مع الأشخاص بغرض الاحتيال عليهم، خاصة مع كثرة التداول المالي الالكتروني واستخدام الانترنت، وأهم ما يتميز به الاحتيال الالكتروني هو النطاق الواسع لممارسة عمليات الاحتيال عبر الانترنت بسبب حجم استخدامها، واعتمادها من طرف البنوك في جميع أنحاء العالم².

ينتشر الاحتيال الالكتروني في الكثير من الدول، فنجد الاحتيال الذي يكون عن طريق البيانات المدخلة التي يلجأ إليها بعض الموظفين في القطاع المصرفي، عن طريق إدخال معطيات مصنعة، أو عن طريق التلاعب في البرامج التي تتم أثناء تطوير البرنامج أو صيانتها، كما يمكن أن يكون الاحتيال بواسطة التلاعب في المعطيات عن بعد من قبل أشخاص خارجين وذلك من خلال اعتراض المعلومات المتبادلة عبر الشبكات وتحليلها واستعمالها من أجل اختلاس الأموال المرتبطة بها³، ويكون الاحتيال كذلك بعدم تسليم البطاقة الالكترونية لصاحبها وذلك باستعمال جهاز قارئ للبطاقة، فتسرق معلومات البطاقة الموجودة على الشريط المغنط وبعدها يصدر المخترق بطاقة مزيفة كما لو كانت بطاقة أصلية. كما يأخذ الاحتيال صورة أخرى دون وجود بطاقة الكترونية، فيأخذ صور طلبات احتيالية تكون باستحواذ المجرمون على معلومات الحساب بطريقة غير مشروعة واستخدامها في طلبات الشراء في الانترنت أو في البريد الالكتروني⁴، فيكون بإرسال رسالة الكترونية إلى البريد الالكتروني عن طريق عروض غير شرعية من أجل الحصول على المعلومات الخاصة بالحساب المصرفي كتشجيع المتعاملين على شراء سلع وخدمات بأسعار منخفضة مع عدم وجود أي نية لتسليم هذه المشتريات⁵.

¹ زيدان محمد وحمو محمد، (أمن المعلومات المصرفية كمطلب لتبني التسويق الالكتروني في البنوك الجزائرية)، مجلة رؤى اقتصادية، كلية الحقوق والعلوم السياسية، جامعة الشهيد محمد خيضر، بسكرة، العدد 8، 2015، ص 170.

² طرق الاحتيال الالكتروني، كتاب السطور، www.sotor.com تم الاطلاع عليه في 8 جويلية 2020 على الساعة 10:46.

³ زيدان محمد وحمو محمد، المرجع السابق، ص 170.

⁴ شايب محمد، (آليات الحماية من الغش في وسائل الدفع الالكترونية في الاقتصاد الفرنسي 2002-2016 "حالة البطاقة المصرفية")، مجلة نماء للاقتصاد والتجارة، جامعة سطيف 1، الجزائر، العدد الثاني، 2017، ص 9.

⁵ أنواع الاحتيال، <https://ar.bkon time.com> تم الاطلاع عليه يوم 22 أوت 2020 على الساعة 14:41.

يمكن للاحتيال الالكتروني أن يأخذ نوعين، النوع الأول يكون دون استهداف مباشر بغرض سرقة الأموال، أما النوع الثاني يعتبر أكثر خطورة والأكثر تقدماً فهو يستهدف فرد أو كيان معين للحصول على معلوماته الخاصة للاستفادة منها في أنشطة غير قانونية¹.

ثانياً/ جريمة انتهاك السرية المعلوماتية:

يقصد بالسرية المعلوماتية التزام البنك اتجاه المتعاملين بالسرية المصرفية، وذلك بأن لا يقدم أي تفصيل شأن الحساب المصرفي أو أي معلومة مصرفية أو شخصية دقيقة إلى أي طرف آخر لكسب ثقة المتعاملين، كما تعتبر السرية المعلوماتية من أهم الضمانات الممنوحة للعميل وذلك بجمع البيانات ومعالجتها، والالتزام بما تضمنته القوانين والأنظمة والتعليمات النافذة بخصوص السرية المعلوماتية².

وتقتضي السرية المعلوماتية معرفة طبيعة هذه المعلومات، حيث حاول بعض الفقهاء³ تحديد المعلومات التي تدخل ضمن السرية المعلوماتية، وذلك باعتماده على ضابطين:

✓ **الضابط المادي:** يتعلق بالمعلومات التي ترتبط ارتباطاً وثيقاً بمباشرة المصرف لنشاطه، فأى تفصيل يتحصل عليه البنك تعد من الأسرار المصرفية ولا يجوز إفشاءها.

✓ **الضابط الشخصي:** يعتمد على الجانب الشخصي للعميل فالمعلومات التي تعد سرا هي تلك المعلومات التي يحددها العميل في علاقته مع المصرف.

ويعتبر انتهاك السرية المعلوماتية جريمة في حالة استعمالها بشكل غير صحيح أو جراء الاعتداءات التي تحدث بواسطة الانترنت وعدم توفير الحماية الكافية لتتقل المعلومات⁴، وهذا ما أشار إليه المشرع الجزائري في الكتاب السادس تحت عنوان مراقبة البنوك والمؤسسات المالية في الباب الرابع المعنون بالسرية المهنية من قانون النقد والقرض في

¹ الاحتيال الالكتروني، التخلف التقني للقطاع المصرفي اللبناني يمنع تفاقم القرصنة، عبد الرحمان عرابي، <http://www.alaraby.couk> تم الاطلاع عليه في 8 جويلية 2020 على الساعة 11:02.

² حقوق ومسؤوليات العميل، البنك المركزي الأردني، <https://www.cbj.gov.jo> تم الاطلاع عليه في 8 جويلية 2020 على الساعة 11:55.

³ إياد خلف محمد جويعد، (المسؤولية الجزائية عن إفشاء السرية المصرفية)، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 23، 2010، ص 246.

⁴ حوالف عبد الصمد، المرجع السابق، ص 375.

المادة 117 التي تقتضي بأنه: "يخضع للسِر المهني، تحت طائلة العقوبات المنصوص عليها في قانون العقوبات:- كل عضو في مجلس إدارة، وكل محافظ حسابات وكل شخص يشارك أو شارك بأي طريقة كانت في تسيير بنك أو مؤسسة مالية أو كان أحد مستخدميها.- كل شخص يشارك أو شارك في رقابة البنوك والمؤسسات المالية وفقا للشروط المنصوص عليها في هذا الكتاب. تلزم بالسِر، مع مراعاة الأحكام الصريحة لجميع السلطات ماعدا: - السلطات العمومية المخولة بتعيين القائمين بإدارة البنوك والمؤسسات المالية.- السلطة القضائية التي تعمل في إطار إجراء جزائي...".

تقوم السرية المصرفية على مجموعة من الاعتبارات فهي تستند إلى حماية الحرية الشخصية للفرد، فذمة العميل تعد من الأمور المتصلة بحياته الخاصة التي يحرص على عدم اطلاع الغير عليها، وهذا لما فيها مساس بكيان المتعاملين المالية والتجارية، فلا يجوز لأي شخص كان أن يطلع على المعلومات السرية الخاصة بالعميل إلا للأشخاص المخول لهم قانونا، فالسرية المصرفية هي مظهر من مظاهر حماية الحرية الشخصية للأفراد، وهي تستند إلى حماية مصلحة المصرف في كتمان أعماله فازدهار وتطور البنك يكون بتزايد عدد المتعاملين معه وحركة معاملاتهم، لأن البنوك تعتمد اعتمادا كلياً على زبائنهم، لذلك فمن مصلحة البنك بقاء أعماله سرية لارتباطه بمصلحة الزبون ولتدعيم الثقة بين البنوك والمتعاملين، فإفشاء الأسرار المصرفية يترتب عنها خسارة البنوك على الصعيد المالي والتجاري وتعويض الأضرار التي لحقت بالمتعاملين¹.

الفرع الثاني: استخدام وسائل الدفع في جريمة تبييض الأموال والتهرب الضريبي

تطور القطاع البنكي بتطور التكنولوجيا المصاحبة للعلوم، هذا ما زاد من جرائم تبييض الأموال عن طريق الوسائل الخاصة بنقل الأموال وتحويلها، وجريمة التهرب الضريبي أيضا.

أولا/ جريمة تبييض الأموال باستعمال وسائل الدفع الالكتروني:

تعرف جريمة تبييض الأموال وفقا للمفهوم المصرفي على أنها: "استخدام القنوات

¹ خوجة جمال، (أثر السرية المصرفية على مكافحة جريمة تبييض الأموال)، المجلة الجزائرية للحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة تلمسان، العدد 3، 2017. ص(14-15).

المصرفية والمؤسسات المالية في تنفيذ بعض العمليات المالية والتحويلات المصرفية للأموال الناتجة عن دخول غير مشروعة بغرض تغيير صفة هذه الأموال أو صعوبة التعرف على مصادرها وإعادة هذه الأموال إلى أصحابها مغايرة لحقيقتها الأولى".¹

تستخدم وسائل الدفع الالكتروني في عمليات تبييض الأموال، كون أن العمليات الالكترونية تتميز بصعوبة ملاحقتها نظرا لسرعة حركتها، وبالتالي يلجأ الجاني إلى الطرق التي قد تعجز أجهزة المراقبة عن كشفها أو رصدها.² وحيث يستغل الجناة وسائل الدفع في ارتكاب هذه الجريمة لأنها تمثل وسيلة مثالية لاختزان قيمة نقدية لأموال متحصل عليها من مصدر غير مشروع تمهيدا لتبييض هذه الأموال، فهنا يبرز الجانب السلبي لوسائل الدفع الالكتروني على اعتبار أن مراقبتها مسألة في غاية الصعوبة.³

يقع على عاتق البنوك التزام مراقبة حسابات المتعاملين ومتابعة العمليات الواردة عليها بشكل دائم ومستمر، خاصة تلك المتضمنة للمخاطر وتكون هذه المراقبة من خلال المتابعة للعمليات التي تنفذ بواسطة حسابات المتعاملين وحركاتها والحرص على أن تكون العمليات مناسبة مع المعلومات التي تمتلكها على المتعاملين، ومنع متعاملها من إيداع مبالغ مالية في حسابه غير مشروعة كتجارة المخدرات أو أية أفعال أخرى، بهدف تبييضها، ويستوجب على البنوك أن تراقب حركات أوامر الدفع بغرض اكتشاف العمليات والتحويلات غير الاعتيادية أو تلك التي تكون بدون مبرر اقتصادي⁴، لهذا أوجدت البنوك مؤشرات إرشادية للتعرف على العمليات التي يشتبه فيها أنها تتضمن تبييض، مثل قيام أحد العملاء بشراء سندات لوضعها في إحدى الخزائن في البنك، وهذا لا يبدو مناسباً

¹ العبد سعيدة، المسؤولية الجزائية للبنك عن جريمة تبييض الأموال، أطروحة لنيل درجة دكتوراه، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2016، ص47.

² صقر بن هلال المطيري، جريمة غسل الأموال-دراسة حول مفهوما ومعوقات التحقيق فيها وإشكاليات تنسيق الجهود الدولية لمواجهتها-، مذكرة لنيل شهادة ماجستير، تخصص التشريع الجنائي الإسلامي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص49.

³ سلاي بوبكر، أثر النقود الالكترونية على إدارة السياسة النقدية، دراسة استشرافية على الجزائر، أطروحة لنيل درجة دكتوراه، تخصص علوم اقتصادية، جامعة محمد بوضياف، المسيلة، 2019، ص38.

⁴ عبد الله ليندة، المرجع السابق، ص227.

لوضع المتعامل، أو حدوث إيداعات نقدية متكررة لا تتناسب مع نشاط المتعامل خلال فترة معينة¹.

يستعين الجاني بالوسائل الالكترونية في جريمة تبييض الأموال ويظهر ذلك من خلال المراحل التي تمر بها هذه الجريمة:

- **مرحلة الأموال المشروعة:** يتعرف الجاني على المصادر الأصلية للأموال عن طريق استخدام الوسائل الالكترونية الحديثة والدخول إلى أنظمة المعلومات وبرمجيات البنوك ومحاولة فك الشفرات السرية للأموال والتخطيط لكيفية سرقتها.
- **مرحلة إدارة الأموال غير المشروعة:** يستخدم الجاني الشفرات السرية لأرقام حسابات البنوك والمؤسسات الأخرى وعملائهم لسحب الأموال بطرق غير مشروعة عن طريق الأجهزة الالكترونية.
- **مرحلة التوظيف:** يتم توظيف الأموال غير المشروعة عن طريق التحويل الالكتروني للأموال إلى حسابات مصرفية خارجة أو تحويلها إلى نقود الكترونية أو الدخول الالكتروني إلى الأسواق المالية لشراء الأسهم والسندات².
- **مرحلة التغطية:** تكون مرحلة التغطية عن طريق إخضاع الأموال غير المشروعة المدخلة في النظام البنكي لسلسلة من العمليات البنكية المتعقدة والمعقدة، بهدف قطع صلة الأموال عن مصدرها غير المشروع لإخفاء المصدر الإجرامي للأموال موضوع التبييض³.
- **مرحلة الدمج:** تعتبر مرحلة الدمج هي المرحلة الأخيرة لجريمة تبييض الأموال، حيث يقوم الجاني في هذه المرحلة بدمج الأموال غير المشروعة في نظام مالي ومصرفي شرعي كأموال مصدرها⁴.

¹ سلالي بوبكر، المرجع السابق، ص114.

² حوالف عبد الصمد، المرجع السابق، ص(375-376).

³ تدريست كريمة، دور البنوك في مكافحة تبييض الأموال، أطروحة لنيل درجة دكتوراه، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2014، ص(83-84).

⁴ علي حبش، أثار الإصلاحات المصرفية في مكافحة تبييض الأموال في الجزائر، مذكرة لنيل شهادة ماجستير، تخصص نقود مالية وبنوك، جامعة سعد دحلب، البليدة، 2006، ص(22-23).

يترتب عن استعمال وسائل الدفع الالكتروني سهولة ارتكاب جريمة تبييض الأموال لأن التعامل بهذه الوسائل يتم دون الحاجة إلى ظهور الهوية الحقيقية للمتعاملين وأحيانا دون إظهار الهوية إطلاقا، ما سمح بارتكاب هذه الجريمة ويجع السلطات المختصة بمراقبة جريمة تبييض الأموال، يصعب عليها مراقبة السجلات والعمليات المالية والمصرفية التي تتم باستعمال وسائل الدفع الالكتروني، وتعتمد هذه الوسائل على استخدام أجهزة الكمبيوتر والأنظمة الالكترونية وقد تتعطل هذه الأجهزة والأنظمة التي تحفظ النقود باستخدام الدفع الالكتروني، سواء كان العطل مقصود أو عطل تلقائي، وبالتالي يستحيل مراقبة العمليات التي تتم باستخدام هذه الوسائل بعد ذلك يسهل ارتكاب جرائم تبييض الأموال¹.

ثانيا/ جريمة التهرب الضريبي باستعمال وسائل الدفع الالكتروني

تشكل وسائل الدفع الالكتروني أداة للتهرب الضريبي، حيث انتشرت هذه الجريمة بكثرة في الدول المتقدمة المتعاملة بوسائل الدفع الالكتروني، لذلك يتعين على الإدارة الجبائية مراقبة الحسابات لأن أصحابها قد يتعمدون إخفاء عدد معتبر من الأموال في البلدان المعروفة بالجناة الجبائية، كما تصعب عملية المراقبة في حالة استخدام وسائل دفع مزورة².

ولأن انتشار وسائل الدفع الالكتروني صاحبه تزايد في جرائم التهرب الضريبي، كان من الصعب على الجهات الحكومية المكلفة بتحصيل الضرائب للقيام بربط الضريبة على تلك الصفقات التي تكون بواسطة هذه الوسائل³.

وتكون وسائل الدفع الالكتروني وسيلة للتهرب الضريبي أيضا، حيث تساعد النقود الالكترونية في تأمين الأموال غير المشروعة الناتجة عن ارتكاب الجرائم والتي تحتاج إلى تبييض، هذا ما يصعب على الجهات المكلفة بتحصيل الضرائب ومراقبة الصفقات التي تتم عبر شبكة الانترنت باستخدام وسائل الدفع الالكتروني، فرض الضرائب عليها ولا شك

¹ حوالف عبد الصمد، المرجع السابق، ص378.

² هداية بوعزة، المرجع السابق، ص354.

³ لوصيف عمار، المرجع السابق، ص117.

أن الأموال التي تنتج عن التهرب الضريبي تعد أموال غير مشروعة¹.

¹ بسام أحمد الزلمي، (دور النقود الالكترونية في عمليات غسل الأموال)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010، ص 558.

الفصل الثاني

طرق مكافحة مخاطر الدفع

الالكتروني على البنوك

الفصل الثاني: طرق مكافحة مخاطر الدفع الالكتروني

تسعى البنوك جاهدة لتوفير نظم الحماية بغرض مكافحة المخاطر التي تصاحب استعمال وسائل الدفع الالكتروني والتي قد تفقدها ثقة المتعاملين معها، ولأن معظم البنوك أصبحت تعتمد نظام الدفع الالكتروني في المعاملات البنكية والخدمات التي تقدمها للمتعاملين تتم عبر شبكة الانترنت، حاول قراصنة الانترنت التعدي على هذا النظام باستعمالهم له استعمالا غير المشروع.

لذلك حاولت البنوك مكافحتها بواسطة إجراءات تقنية لاستقرار المعاملات المصرفية الالكترونية التي تقوم بها، إضافة إلى الحماية التي أقرتها التشريعات للتصدي لمختلف أساليب الاستعمال غير المشروع لوسائل الدفع الالكتروني. وعليه ندرس هذا الفصل في مبحثين: نتناول في الأول الحماية التقنية لمكافحة مخاطر الدفع الالكتروني وفي الثاني الحماية القانونية لمكافحة مخاطر الدفع الالكتروني.

المبحث الأول: الحماية التقنية لمكافحة مخاطر الدفع الالكتروني

ظهرت عدة جرائم الكترونية بظهور الانترنت، هدفها تدمير مخازن المعلومات وسرقة أموال المتعاملين، لهذا فإن العديد من الدول¹ سعت جاهدة لإيجاد حلول لهذه الجرائم والحد منها²، ولأجل ذلك سعت البنوك إلى اعتماد آليات تقنية لمكافحة مخاطر الدفع الالكتروني (المطلب الأول) وعملت على تأمين العمليات الالكترونية (المطلب الثاني).

المطلب الأول: الآليات التقنية المعتمدة لمكافحة مخاطر الدفع الالكتروني

تعتبر الآليات التقنية من أهم الوسائل المعتمدة لمواجهة المخاطر الناشئة عن وسائل الدفع الالكتروني، فهي مجموعة من الحماية والتدابير التقنية على المواقع الالكترونية

¹ هناك العديد من الدول التي سعت جاهدة للحد من جرائم المعلوماتية من خلال العديد من التوصيات والقوانين كالولايات المتحدة الأمريكية على مستوى الدول الغربية، تونس والإمارات المتحدة العربية على مستوى الدول العربية. حوالف عبد الصمد، المرجع السابق، ص12.

² فاطمة الزهرة خبازي، (جرائم الدفع الالكتروني وسبل مكافحتها)، مداخلة في ملتقى وطني بعنوان: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، جامعة الجليلي بونعامة، خميس مليانة، 2017، ص40.

وبرمجيات الكمبيوتر، فتم الاستغناء على الكتابة والتوقيع التقليدي، والاعتماد على الطابع الالكتروني لهذه الوسائل، حيث يتم استعمالها كوسيلة إثبات في المعاملات¹.

الفرع الأول: الكتابة الالكترونية

تعتبر الكتابة الالكترونية من أفضل طرق الإثبات، وأكثر الأدلة استعمالا في الحياة المعاصرة، فهي مثبتة على دعائم غير مادية لهذا تسمى "بالإثبات الالكتروني"، وهي رسالة بيانات يتبادلها طرفي العلاقة والتي تثبت التصرف القانوني الذي أبرم الكترونيا². نص المشرع الجزائري على الكتابة الالكترونية من خلال المادة 320 مكرر من التقنين المدني التي تقضي على أنه: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أي علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها"، وتعتبر هذه المادة أول نص اعترف من خلاله المشرع الجزائري بالكتابة الالكترونية لاستعمالها كوسيلة إثبات³.

تمر الكتابة الالكترونية بمراحل هي كالتالي:

- **مرحلة تدوين الكتابة وحفظها:** تتم بإدخال البيانات إلى الكمبيوتر، ثم معالجتها عن طريق برامج في الحاسوب، فيدخل البيانات وفقا للتعليمات التي تلقاها من المستخدم لتصبح معلومات مقروءة، بعد ذلك يتم حفظها وتخزينها.
- **مرحلة إظهار الكتابة للاطلاع عليها:** تظهر في هذه المرحلة الكتابة على شكل مخرجات ووحدات ملحقة في الكمبيوتر.
- **مرحلة الإرسال والتبادل الالكتروني للكتابة:** يتم إرسال الكتابة بين الحواسيب عبر شبكة الانترنت فيكون على شكل صفحات الكترونية⁴.

¹ هداية بوعزة ويوسف فتيحة، (الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الالكتروني)، مجلة الدراسات والبحوث القانونية، جامعة وهران 2، العدد 4، المجلد 3، 2018، ص23.

² دنيا زراد، (إبرام العقد الالكتروني)، <https://www.marocdroit.com>، تم الاطلاع عليه بتاريخ 13 جويلية 2020، على الساعة 00:40.

³ فوغالي بسمة، إثبات العقد الالكتروني وحجته في ظل عالم الانترنت، مذكرة لنيل شهادة ماجستير، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف2، (2014-2015)، ص8.

⁴ بلقاسم حمدي، إبرام العقد الالكتروني، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، (2014-2015)، ص183.

وتقبل الكتابة الالكترونية كدليل إثبات، باستيفاء الشروط التي وضعها المشرع الجزائري المتمثلة في:

✓ **إمكانية قراءة الكتابة:** تكون عن طريق إعداد برامج خاصة تحول الرموز والإشارات إلى حروف مقروءة وواضحة، وإذا كانت المستندات مشفرة وجب فك التشفير حتى تصبح بيانات واضحة¹، وهذا ما نص عليه المشرع الجزائري في المادة 323 مكرر من التقنين المدني التي تقضي بأن: "...أن تكون الرموز أو الحروف أو غيرها من عناصر الكتابة ذات معنى مفهوم...".

✓ **التأكد من هوية الشخص الذي أصدرها:** ويكون بتأكد المتعاقد من هوية المتعاقد معه، عن طريق اسمه، عنوانه، بريده الالكتروني، وغيرها من المعلومات. نص المشرع الجزائري على هذا الشرط في المادة 323 مكرر 1 من التقنين المدني بقولها: "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها...".

✓ **إمكانية الحفظ وعدم القابلية للتعديل:** فيما يخص قابلية الحفظ، نص المشرع الجزائري على هذا الشرط في المادة 323 مكرر 1 من التقنين المدني التي جاء فيها أنه: "...أن تكون الكتابة معدة ومحفوظة في ظروف تضمن سلامتها". أما عدم القابلية للتعديل يكون بخلوها من العيوب المؤثرة في صحتها، والهدف منه هو أن يجعل الكتابة تتمتع بالثقة والأمان من طرف مستخدميها².

تصبح للكتابة الالكترونية حجية في الإثبات المعطاة للكتابة على الدعامة الورقية بمجرد توافر هذه الشروط، ولكلاهما نفس قوة الإثبات القانوني، حتى في حالة عرض أدلة مزدوجة أمام القضاء، أي أدلة ورقية والكترونية، فالقاضي لا يعطي الأولوية لأن لكلاهما نفس المرتبة والحجية، بل يعتمد على الدليل الذي يكون أكثر صلة بالموضوع³.

¹ مصطفى هنشور وسيمة، النظام القانوني للتجارة الالكترونية في التشريع الجزائري والمقارن، أطروحة لنيل درجة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، (2016-2017)، صص (289-291).

² مصطفى هنشور وسيمة، المرجع نفسه، ص 293.

³ سعيد السيد قنديل، التوقيع الالكتروني (ماهيته، صورته، حجيته في الإثبات بين التداول والاقتباس)، دار الجامعة للنشر، الطبعة الثانية، الإسكندرية، 2006، ص 16.

ولتعزيز ذلك منع المشرع الجزائري إدخال معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بالغش في المعطيات التي يتضمنها في قانون العقوبات في الكتاب الثالث المعنون بالجنايات والجرح وعقوباتها في الفصل الثالث بعنوان الجنايات والجرح ضد الأموال في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المادة 394 مكرر إلى المادة 394 مكرر 7. إذ تنص المادة 394 مكرر 1 على أنه: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 4.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تضمنها".¹

الفرع الثاني: التوقيع الالكتروني

يعتبر التوقيع الالكتروني في مجال الأعمال والتجارة الالكترونية أهم جانب قانوني، فهو عبارة عن تقنية حديثة معترف بها من قبل الدولة، وهي شهادة رقمية تحتوي على بصمة الكترونية للشخص الموقع مع بيان هوية صاحبها، ومجموعة من الرموز والأرقام والحروف الالكترونية الخاصة بها.²

عرف المشرع الجزائري التوقيع الالكتروني في القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني في الباب الأول المعنون بأحكام عامة في الفصل الثاني بعنوان تعاريف، في المادة الثانية الفقرة الأولى التي تنص على أنه: "بيانات في شكل الكتروني مرفقة أو مرتبطة منطقياً ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق". كما نصت المادة الثانية في فقرتها الثالثة من نفس التقنين على بيانات إنشاء التوقيع الالكتروني التي تقضي بأنه: "بيانات فريدة، مثل الرموز أو مفاتيح التشفير، الخاصة التي يستعملها الموقع لإنشاء التوقيع الالكتروني".³

يأخذ التوقيع الالكتروني إحدى الصور التالية:

¹ مصطفى هنشور وسيمة، المرجع السابق، ص 294.

² عرورة فتيحة، وسائل التبادل المصرفي في القانون الجزائري، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق، جامعة الجزائر 1، (2016-2017)، ص 198.

³ القانون 15-04 مؤرخ في 1 فبراير 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، جريدة رسمية عدد 6 مؤرخ في 10 فبراير 2015.

- التوقيع بالخواص الذاتية أو البيومتري: يتميز بتحديد هوية كل شخص وأنه لكل شخص صفات خاصة، من خصائصه البصمة الشخصية، مسح العين البشرية، التعرف على الوجه البشري، خواص اليد البشرية ونبرة الصوت، ويتم التأكد من هوية المتعامل بإدخال هذه المعلومات في الكمبيوتر وتخزينها ليقوم بعد ذلك بالمطابقة.
 - التوقيع الرقمي أو الكودي: يكون برقم سري لا يعرفه إلا صاحب التوقيع، فهو مجموعة من الأرقام أو الحروف يختارها صاحبها لتكون رقم سري ويعتمد على تشفير مماثل معلوما بين الحامل والجهاز، أو التشفير غير المتماثل يعتمد على مفتاح عام معروف لدى الجميع¹.
 - التوقيع بالقلم الالكتروني: يستعمل في الكتابة على شاشة الكمبيوتر، بواسطة برنامج هدفه هو خدمة التوقيع والتحقق من صحتها، تتمثل هذه الطريقة في نقل التوقيع المحرر بخط اليد عن طريق التصوير بالماسح الضوئي إلى رسالة الكترونية المراد منها إضافة هذا التوقيع إليها بإضفاء الحجية عليها².
- يحتج بالتوقيع الالكتروني عند استيفاءه الشروط اللازمة المنصوص عليها في المادة 7 من القانون 04-15 والتي ورد فيها: "التوقيع الالكتروني الموصوف هو التوقيع الالكتروني الذي تتوفر فيه المتطلبات الآتية:
- 1- أن ينشئ على أساس شهادة تصديق الكتروني موصوفة.
 - 2- أن يرتبط بالموقع دون سواه.
 - 3- أن يمكن من تحديد هوية الموقع.
 - 4- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني.
 - 5- أن يكون منشئ بواسطة وسائل تكون تحت التحكم الحصري للموقع.
 - 6- أن يكون مرتبطا بالبيانات الخاصة به، يمكن الكشف عن التغيرات اللاحقة بهذه

¹ عرورة فتيحة، المرجع السابق، ص(199-200).

² خالد ممدوح إبراهيم، إبرام العقد الالكتروني - دراسة مقارنة-، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2011، ص255.

البيانات."

كما أقر المشرع الجزائري بحجية التوقيع الالكتروني في المادة 8 من نفس التقنين التي تنص على أنه: "يعتبر التوقيع الالكتروني الموصوف وحده مماثلاً للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي."

رغم الحجية التي يتميز بها التوقيع الالكتروني والأمان والثقة التي يوفرها لدى المتعاملين بها، إلا أن هذا الأخير قد تواجهه مخاطر عديدة جراء ارتكاب الجناة لجرائم التزوير. والذي يعتبر من أكثر الجرائم التي تمس بالتوقيع الالكتروني، ويكون إما بتزوير التوقيع البيومترى عن طريق بصمة العين، الأصبع، معالم الوجه، خواص الصوت، أو بتزوير الرقم السري بسرقة البيانات من جهاز الكمبيوتر وتزويرها، كما قد يكون التزوير بالتوقيع الرقمي وذلك بواسطة حصول الجاني على منظومة التوقيع الرقمي لشخص آخر واستخدامها لتوقيع مستندات، والكشف عن الجريمة يكون بإثبات أن التوقيع صادر من شخص آخر غير مالك المنظومة¹. وقد قرر المشرع الجزائري عقوبات لجريمة التزوير في تقنين العقوبات من خلال المادة 219 التي تنص على أنه: "كل من ارتكب تزويراً بإحدى الطرق المنصوص عليها في المادة 216² في المحررات التجارية أو المصرفية أو شرع في ذلك، يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 20.000 إلى 100.000...".

ونظراً لأهمية التوقيع الالكتروني وجب تدخل هيئات التصديق الالكتروني لربط ذلك التوقيع مع صاحبه، حتى تضفى عليه المصادقية³.

¹ إبراهيم بن سطم بن خلف العنزي، التوقيع الالكتروني وحمايته الجنائية، أطروحة لنيل درجة دكتوراه، تخصص الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، 2009، ص ص (109-111).

² تنص المادة 216 من تقنين العقوبات الجزائري على أنه: "يعاقب بالحبس المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج، كل شخص، عدا من عينتهم المادة 215، ارتكب تزويراً في محررات رسمية أو عمومية: إما بتقليد أو بتزييف أو كتابة أو التوقيع..."

³ غزالي نزيهة، (الآليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري)، مجلة البحوث السياسية والإدارية، جامعة محمد لامين دباغين، سطيف 2، العدد 10، بدون سنة النشر، ص 289.

يعرف التصديق الالكتروني على أنه آلية تهدف إلى بناء الثقة في نظام الشهادات الرقمية وتشجيع المعاملات الالكترونية بإضفاء المصادقية عليها، أما المشرع الجزائري فهو لم يعرف التصديق الالكتروني وإنما عرف شهادة التصديق الالكتروني¹، في المادة 2 الفقرة 7 من القانون 04-15 المتعلق بالتوقيع والتصديق الالكترونيين التي تنص على أنه: "وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع."

الفرع الثالث: السجل الالكتروني

يعتبر السجل الالكتروني وسيلة لحفظ المعلومات المتبادلة الكترونيا لتوثيق البيانات فيه، فهو أمر لا يجب إغفاله في المجال الالكتروني للبيانات. ويعرفه الفقه² بأنه: "السجل الالكتروني سجل نشأ أو نتج أو اتصل أم تم تلقيه أو حفظه بوسيلة الكترونية"، ويرى جانب آخر من الفقه³ على أنه: "مجموعة من النصوص أو الرسومات أو البيانات أو الأصوات أو الصور أو غيرها من المعلومات تتمثل في صورة رقمية، ويتم إنشائها أو تعديلها أو حفظها أو فهرستها أو استرجاعها أو توزيعها بواسطة نظم الحاسب الآلي".

يتضح من خلال هذين التعريفين أن للسجل الالكتروني عدة مميزات وهي كالتالي:

✓ يأخذ السجل الالكتروني مكان وحيز أقل مقارنة بالسجلات الورقية، ونظرا لتبادل البيانات بالنظام الالكتروني، فإن تجميع كميات ضخمة من المعلومات في قرص أو أسطوانة لا تشغل مكان.

✓ يتميز بصعوبة تغييره أو تحريفه أو تزويره وذلك بتشفير البيانات، مما يصعب على أي شخص غير مرخص له بالوصول إلى هذه المستندات المحفوظة الكترونيا⁴.

نص المشرع الجزائري من خلال المادة 4 من القانون 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين -السالف ذكره- على دعامة الحفظ للسجل

¹ غزالي نزيهة، المرجع نفسه، ص 291.

² نقلا عن حدوم ليلي، المرجع السابق، ص 130.

³ نقلا عن حدوم ليلي، المرجع نفسه، ص 130.

⁴ مخلوفي عبد الوهاب، التجارة الالكترونية عبر الانترنت، أطروحة لنيل درجة الدكتوراه، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، (2011-2012)، ص (246-247).

الالكتروني التي تنص على أنه: "تحفظ الوثيقة الموقعة الكترونيا في شكلها الأصلي، ويتم تحديد الكيفيات المتعلقة بحفظ الوثيقة الموقعة الكترونيا عن طريق التنظيم"، كما أصدر المرسوم التنفيذي رقم 16-142 المحدد لكيفيات حفظ الوثيقة الموقعة الكترونيا في المادة 2 الفقرة 4 التي تقضي بأنه: "الحفظ: مجموعة تدابير تقنية التي تسمح بتخزين الوثيقة الموقعة الكترونيا في دعامة الحفظ".

للسجل الالكتروني حجية في الإثبات متى توفر على الشروط التي المنصوص عليها في المادة 6 من المرسوم 16-142 التي تنص على أنه: "يتم حفظ الوثيقة الموقعة الكترونيا على دعامة حفظ يسمح في أي وقت بالإنفاذ في كل محتواها واسترجاعها بواسطة الوسائل التقنية الملائمة"، وهذا ما جاء أيضا في المادة 8 من نفس المرسوم التي تقضي بأنه: "يجب أن تتضمن كل عملية تجرى على الوثيقة الموقعة الكترونيا والمحفوظة لدواعي فعالية و/ أو الأمن، استرجاعها في شكلها الأصلي".¹

كما يجب أن يتوفر شرط رقابة جهة ثالثة موثوقة للمعاملات الالكترونية التي تتم بين طرفين وتخزن وتحفظ بدقة، فإذا توفرت هذه الشروط قامت قرينة قانونية على صحة السجل الالكتروني إلا إذا أثبت العكس.²

المطلب الثاني: تأمين العمليات الالكترونية من قبل البنوك

تتم العمليات الالكترونية بواسطة فضاء الكتروني مفتوح مما يجعلها أكثر عرضة للجرائم الالكترونية، هذا ما ألزم البنوك على توفير وسائل أمان لتعزيز الثقة بين المتعاملين وضمان فعالية وسائل الدفع الالكتروني، وذلك عن طريق إجراءات تأمين العمليات الالكترونية.³

¹ المرسوم التنفيذي رقم 16-142 مؤرخ في 5 مايو 2016 يحدد كيفيات حفظ الوثيقة الموقعة الكترونيا، جريدة رسمية عدد 28 مؤرخ في 28 ماي 2016.

² حدوم ليلي، المرجع السابق، ص135.

³ لوصيف عمار، المرجع السابق، ص33.

الفرع الأول: إجراءات تأمين العمليات الالكترونية من قبل البنوك

ينتج عن استخدام الانترنت مخاطر عديدة كانتحال الشخصيات، أو اختراق المواقع أو استخدامها بطريقة غير مشروعة دون ترخيص، ولتوفير الحماية من هذه المخاطر استوجب تحديد أمن المعلومات وضمان أمن المراسلات من جهة أخرى¹.

أولاً/ أمن المعلومات:

تعتمد تقنية امن المعلومات على تحديد هوية المتعاقدين والتأكد منها واعتمادها على كلمة السر، وتستخدمه البنوك في المعاملات الالكترونية، وتسيير وسائل الدفع الالكتروني.

1/ نظام هوية المستخدم وكلمة السر:

يستوجب على المستخدم عند استعماله لموقع البنك على الانترنت للاستفادة من خدماته الالكترونية، أن يدخل هويته وكلمة السر الخاصة به، فهي وسيلة للتحقق من شخصية العميل، وتجرى العمليات بمجرد إدخال الهوية وكلمة السر، حيث يشكل ذلك دليلاً على اتجاه إرادة العميل في الالتزام بالعملية التي أجراها².

وتحقق معرفة هوية الأطراف المصادقية في المعاملات الالكترونية، إمكانية تعيين القانون الواجب التطبيق. وتعتمد البنوك هذه التقنية للتأكد من مشروعية الاستفادة من خدماتها³، وهذا ما ورد في المادة 29 من النظام 08-11 المتعلق بالرقابة الداخلية للبنوك والمؤسسات المالية⁴ التي تقضي بأنه: "...السهر على التحديد الدقيق لهوية الأمر بالعملية والمستفيد من التحويلات الالكترونية، بالإضافة إلى عنوانيهما مهما كانت الوسيلة المستعملة...".

¹ حابت أمال، المرجع السابق، ص(273-274).

² هداية بوعزة ويوسف فتيحة، المرجع السابق، ص(27-28).

³ حابت أمال، المرجع السابق، ص274.

⁴ النظام رقم 08-11 مؤرخ في 28 نوفمبر 2011 يتعلق بالرقابة الداخلية للبنوك والمؤسسات المالية، جريدة رسمية عدد 36 مؤرخ في 29 أوت 2012.

أما بالنسبة لكلمة السر هي أداة تخول لصاحبها إمكانية الوصول لحسابه فهي تثبت للنظام هوية صاحب الحساب وتحمي بيانات هامة ومعلومات خاصة¹.

تعتبر كلمة السر خط الحماية الأول الذي تم اعتماده من قبل مستخدمي أجهزة الكمبيوتر، لذلك فأول خطوة يقوم بها قراصنة الانترنت هي اختراق كلمة السر وانتحال شخصية أخرى لتنفيذ جرائمهم²، وللحفاظ على كلمة السر يستوجب على صاحبها أن يختار كلمة سر معقدة وأن يحافظ عليها بعيدا عن أعين الغير، وأن يعمل على تغييرها دوريا³.

ويمثل نظام هوية المستخدم وكلمة السر أحد الوسائل التأمينية لأنظمة الدفع الالكتروني، التي تسمح للبنوك والمؤسسات المالية المصدرة لوسائل الدفع بالكشف عن هوية القراصنة، وأماكن دخولهم لشبكة المؤسسة الداخلية بحيث تمنع من اقتحامها أو اقتحام نظام المعلومات⁴.

2/ نظام كلمة السر التي لا تتكرر:

تهدف كلمة السر التي لا تتكرر إلى صلاحية كلمة السر لمرة واحدة، بمجرد إتمام العملية تصبح غير صالحة للاستعمال، وتستخدم من طرف البنوك عند إجراء عمليات تتضمن أوامر الدفع ويعتمد على اشتراك العميل مع البنك للتوصل لكلمة السر التي لا تتكرر، حيث يتم تزويد كل منها في البداية بنفس جملة المرور وعدد مرات إدخال بيانات لخوارزمية القيمة الاختيارية⁵، فيرسل العميل رسالة للبنك برقم عشوائي يستخدمه لإخراج كلمة سر لا تتكرر وهي تمر بثلاث مراحل:

¹ خالد بن سليمان الغنبر ومحمد بن عبد الله القحطاني، أمن المعلومات، مكتبة الملك فهد الوطنية للنشر، الطبعة الأولى، الرياض، 2009، ص43.

² هداية بوعزة، المرجع السابق، ص378.

³ خالد بن سليمان الغنبر ومحمد بن عبد الله القحطاني، المرجع السابق، ص43.

⁴ هداية بوعزة، المرجع السابق، ص 378.

⁵ خوارزمية القيمة الاختيارية: "تتمثل في مجموعة من العمليات الحسابية التي يتم من خلالها توليد مجموعة من الحروف ذات طول معين مستنتجة رياضيا من مجموعة من الحروف أطول بكثير والتي تمثل الرسالة المراد تشفيرها، كما تستخدم هذه العملية لاكتشاف تزوير البيانات، فأى تغيير في الرسالة الأصلية يؤدي إلى تغيير في القيمة الاختيارية". هداية بوعزة، المرجع السابق، ص380.

- المرحلة التمهيدية: تتمثل في إدخال العميل جملة مرور وتضاف إلى الرقم العشوائي ثم ترسل إلى البنك.
- مرحلة التوليد: يتم من خلالها تنفيذ خوارزمية القيمة الاختيارية عدة مرات على جملة المرور وذلك لإنتاج كلمة سر.
- مرحلة العرض: تأخذ كلمة السر المنتجة في المرحلة السابقة وتعرض بصورة مقروءة للعميل الذي يستخدمها مرة واحدة فقط بعد تأكد البنك من صلاحيتها¹.

ثانيا/ تقنيات أمن المراسلات والمواقع الالكترونية:

تعتمد البنوك لتأمين المراسلات والمواقع الالكترونية على تقنياتي جدران الحماية والتشفير، ذلك لحماية شبكة المؤسسة الداخلية والوسائل التقنية المشتغلة فيها ومنع اختراقها².

1/ جدران الحماية:

يقصد بجدران الحماية مجموعة الأنظمة التي توفر وسيلة أمنية بين الانترنت وشبكة المؤسسة الداخلية والخروج منها للمرور عبر هذه الجدران، والتصدي لجميع الأخطار القادمة من شبكة الانترنت إلى الشبكة الداخلية الخاصة بالبنوك، كما يمنع جميع محاولات الدخول لهذه الشبكة بدون صفة³.

ويطلق أيضا على جدران الحماية مصطلح "الحائط الناري"، لأن هذا النظام يمنع التلصص على المعلومات الشخصية وما يحتفظ به على الكمبيوتر ويسمح بحمايته، ويقوم أيضا بتصفية المعطيات المتنقلة عبر شبكة المؤسسة ويعالج ويحلل كل المعلومات المتبادلة بين المتعاملين المحليين والدوليين عبر هذه الشبكة، ولا يسمح للأشخاص غير المسموح بهم للتعرض أو معرفة المعلومات الخاصة كأرقام البطاقات الالكترونية، أو أرقام الحسابات أو كافة البيانات الأخرى التي تتميز بالسرية⁴.

¹ حابت آمال، المرجع السابق، ص(275-276).

² شايب محمد، المرجع السابق، ص20.

³ هداية بوعزة، المرجع السابق، ص396.

⁴ واقد يوسف، المرجع السابق، ص170.

وتتجسد الحماية باستخدام جدران الحماية بإدارة عملية النفاذ إلى الموقع أو الشبكة من خلال ثلاث طرق أساسية وهي كالآتي:

✓ **طريقة إتاحة العام وغلق الخاص:** تقسم المؤسسة بياناتها إلى بيانات عامة توضع على خادم يقع خارج جدران الحماية، لتمكين جميع الأشخاص من الإطلاع عليها، كما تقسم البيانات أيضا إلى سرية توضع على خادم آخر يقع على جدران الحماية لمنع جميع محاولات الوصول إليها.

✓ **طريقة جدران المنع المزدوجة:** يتم وضع خادم الملفات العام بعد جدران الحماية الأول، ويوضع خادم الملفات الخاص بعد جدران الحماية الثاني لترشيح وتصفية كل الرزم الداخلة والخارجة من الشبكة.

✓ **طريقة الفصل المطلق للخدمات:** يتم الفصل التام بين كل من خادم الملفات العام والخاص، ويكون الخادم الأخير بمثابة حاسب آلي مستقل بذاته يعمل بنظام تشغيل آمن يحول دون الدخول إلى الملفات الخاصة بالمنظمة¹.

2/ التشفير:

يطلق على التشفير مصطلح التعمية أو الكتابة السرية، فكلها تدل على وسيلة تقنية لحماية أمن المعلومات ضد أعمال قرصنة واختراق وبث فيروسات والاعتداء على المعلومات الاسمية وبيانات وسائل الدفع الالكتروني². وتختلف تقنية التشفير باختلاف الوسائل المستعملة في تنفيذها لكنها تتفق في الهدف من التشفير وهو ضمان تأمين العمليات الالكترونية وتتمثل طرق التشفير فيما يلي:

- **التشفير بالمفتاح المتماثل:** يستطيع كل من المرسل والمستقبل في التشفير بالمفتاح المتماثل فك شفرة المعلومات بنفس المفتاح السري، لكن هذا النوع يطرح مشكلة الأمان وعدم التحقق من الهوية لذلك تراجع استخدام هذا النوع من التشفير³.

¹ سمية ديمش، التجارة الالكترونية حقيقتها وواقعها في الجزائر، مذكرة لنيل شهادة ماجستير، تخصص تحليل واستشراف اقتصادي، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الإخوة منتوري، قسنطينة، (2010-2012)، ص94.

² هداية بوعزة، المرجع السابق، ص382.

³ فاطمة الزهرة خبازي، المرجع السابق، ص38.

- يقوم المنشئ بعد كتابة الرسالة وتشفيرها بتزويد المرسل إليه بذات المفتاح المتماثل، ليتسنى له تلقي الرسالة المشفرة حلها واستعادة محتوى الرسالة في صورتها الأصلية¹.
- **التشفير غير المتماثل:** يستخدم في هذه الطريقة مفتاحين، مفتاح عام ومفتاح خاص، يستعمل المفتاح العام لغرض تشفير المعلومات المرسله للحاسوب الذي يملك صاحبه مفتاح خاص يتمشى معه المفتاح العام، فيستعمل المفتاح الخاص لفك تشفير البيانات التي تلقاها من الحاسوب الذي يملك مفتاح عام². يطلق على هذا النوع من التشفير أيضا بالمفتاح العلني لأنه يمكن أن ينشر أحد المفتاحين ويسمى بالمفتاح العلني، ويحتفظ بالآخر سريا ويسمى المفتاح الخاص أو السري³.
 - **المرج بين نظامي المفتاح المتماثل والمفتاح العام:** يعتبر هذا النظام مختلط، لأنه يقوم بالمرج بين النظامين، حيث يقوم المنشئ بعد كتابة الرسالة بتشفيرها بالمفتاح المتماثل وتشفير المفتاح المتماثل بالمفتاح العام، وإرسالها بعد ذلك للمستقبل الذي سيقوم بحل شفرة المفتاح العام عن طريق مفتاحه الخاص، ليحصل بذلك على المفتاح المتماثل المستخدم في تشفير الرسالة التي تم استلامها، وبعد ذلك يقوم بحل الشفرة بالمفتاح المتماثل⁴.

الفرع الثاني: كفاءات تأمين عمليات الدفع الالكتروني

يعتبر تأمين البنوك من مخاطر الدفع الالكتروني جزء رئيسي من أمن المعلومات، والنظم التقنية العالية⁵. تتم عمليات الدفع الالكتروني بوسائل الكترونية عبر شبكة مفتوحة تزيد من مخاطر الاختراق والاطلاع على البيانات التي تخص المتعاملين، كما يمكن أيضا التلاعب بحساباتهم، ما استوجب على البنوك⁶ توفير وسائل الأمان لتعزيز الثقة بين المتعاملين وضمان فعالية وسائل الدفع الالكتروني، وذلك من خلال

¹ هداية بوعزة، المرجع السابق، ص389.

² واقد يوسف، المرجع السابق، ص164.

³ حوالف عبد الصمد، المرجع السابق، ص446.

⁴ هداية بوعزة، المرجع السابق، ص390.

⁵ يوسف مسعداوي، (البنوك الالكترونية)، مداخلة في ملتقى بعنوان: المنظومة المصرفية الجزائرية والتحول الاقتصادي- واقع وتحديات-، جامعة البليدة، بدون سنة النشر، ص236.

⁶ زهير زواش، المرجع السابق، ص22.

برنامج غرضه تشفير العمليات التي تتم بوسائل الكترونية، بحيث لا يظهر الرقم البنكي على الشبكة ويتم عمل أرشيف يسهل الرجوع إليه للمبالغ التي يتم سحبها بهذه الطريقة، وهذا ما يعرف بنظام المعاملات الالكترونية الآمنة¹.

كما تتم حماية المتعاملين وتأمين عمليات الدفع الالكتروني التي يقومون بها عبر شبكة الانترنت، حيث نجد مصلحة المشتري هي حماية دفعه للثمن عن طريق الشبكة. وحماية البائع بتأمين استحقاقه لدينه، لأن أغلب الأشخاص يستعملون وسائل الدفع لسحب الأموال من الموزع الإلكتروني، ما يستوجب توفير حماية تقنية كافية لمواجهة المخاطر التي قد تتعرض لها وسيلة الدفع الالكتروني.

إلى جانب الأدوات التقنية المستخدمة في تأمين الشبكات، يوجد للتأمين عدة برامج وأنظمة عبر شبكة الانترنت هدفها تأمين عمليات الدفع الالكتروني نذكر منها:

✓ **بروتوكول الطبقات الآمنة:** يعرف بروتوكول الطبقات الآمنة بأنه برنامج مخصص للتحقق من وصول البيانات اللازمة بطريقة آمنة²، ويسمى بروتوكول الطبقات الآمنة نظام SSL اختصار ل (SECURE SOCKET LAYER)، هذا البروتوكول يقوم بتأمين المعلومات بين البائع والمشتري، حيث يتم تشفير بيانات الرسالة المرسلة من المشتري إلى البائع وإرسالها عبر الانترنت أو البريد الالكتروني، كما يمكن لهذا النظام أن يندمج داخل قناة الاتصالات الالكترونية بطريقة تسمح بضمان شفاف لمستعمل تشفير المعطيات بهدف ضمان السرية، حتى لا يتمكن قراصنة الانترنت من التقاط أرقام البطاقات ولا تزوير المحررات الالكترونية³.

✓ **بروتوكول الحركات المالية الآمنة:** يسمى بروتوكول الحركات المالية الآمنة بنظام SET اختصار ل (Secure Electronic Transation)، ويعتبر من أهم بروتوكول لأمن المعاملات الالكترونية لتحقيقه ضمان الحفاظ على أمن البيانات كالخصوصية، السلامة، والتحقق من وصولها إلى الجهة المطلوبة، أثناء إجراء الحركات المالية عبر شبكة مفتوحة، ويستخدم هذا النظام برمجيات تسمى "المحفظة الالكترونية".

¹ لوصيف عمار، المرجع السابق، ص33.

² حوالف عبد الصمد، المرجع السابق، ص464.

³ واقد يوسف، المرجع السابق، ص165.

وتحتوي هذه المحفظة الالكترونية على رقم حامل البطاقة الالكترونية والشهادة الرقمية التابعة له.

أما التاجر فتكون له شهادة رقمية صادرة عن أحد البنوك المعتمدة، ويستخدم كل من حامل البطاقة والتاجر الشهادة الرقمية التابعة له مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الانترنت، ولا يمكن للتاجر مشاهدة رقم البطاقة الالكترونية حيث ترسل الصيغة المشفرة لهذا الرقم إلى الجهة المصدرة، للموافقة على إجراء الحركة المالية مع التاجر وتضمن هذه الطريقة عدم عرض رقم البطاقة كما تمنع أي تعديل غير مرخص به أثناء إرسال هذه البيانات¹.

ولتأمين عمليات الدفع الالكتروني يشترط توافر بعض الشروط وهي إضفاء الصفة الرسمية على الأمر بالدفع، إلى جانب حفظ المعلومات الخاصة بعملية الدفع وكذا تحديد التاريخ الالكتروني لعملية الدفع على النحو التالي:

- **الصفة الرسمية على الأمر بالدفع:** يتم إبرام الصفقات في التجارة الالكترونية على دعائم الكترونية، ويتم التوقيع عليها من قبل أطراف الصفقة الالكترونية، وهذا التوقيع بحاجة إلى من يوثقه ويصادق عليه، وبالتالي ليس من السهل الرجوع إلى المستندات الالكترونية والتحقق من صحة ونسبة صدور التصرف إلى موقعه².
- **حفظ المعلومات الخاصة بعملية الدفع الالكتروني:** تتوقف الحجية القانونية للكتابة الالكترونية على عملية حفظ هذه الكتابة بما يكفل ضمان الحفاظ على نفس محتواها. يتم حفظ المعلومات والمعطيات على دعائم الكترونية ضد التلف أو التعديل، ويلتزم مقدمي خدمات التصديق أن يقوموا بعملية تسجيل وحفظ المعلومات المتعلقة بالشهادات التي يصدرونها خلال المدة التي تبقى دائماً الشهادة صالحة لأن تقدم إلى العدالة³.

¹ مسعداوي يوسف وسعيد جميل، (وسائل الدفع الالكترونية)، مداخلة في الملتقى العلمي الدولي الرابع بعنوان: عصرنه نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الالكترونية في الجزائر -عرض تجارب دولية-، كلية الحقوق والعلوم السياسية، جامعة البليدة، بدون تاريخ النشر، بدون صفحة.

² حابت أمال، المرجع السابق، ص(280-281).

³ السيد سعيد قنديل، المرجع السابق، (103-104).

- **تحديد التاريخ الالكتروني:** يعتبر تحديد التاريخ الالكتروني لعملية الدفع الالكتروني مهم بالنظر لتاريخ الاستحقاق للدفع ولعدم ترتيب فوائد التأخير إلى غير ذلك، ولإسناد تاريخ محدد للسند الالكتروني يمكن إتباع إحدى الطريقتين:
 - وضع التاريخ في صلب رسالة البيانات.
 - تدخل شخص ثالث يتولى توثيق التاريخ والساعة التي يتم فيها التصرف الالكتروني¹.

المبحث الثاني: الحماية القانونية لمكافحة مخاطر الدفع الالكتروني

عمل المشرع الجزائري على حماية البنوك من المخاطر التي قد تواجهها من استعمالها لوسائل الدفع الالكتروني، وذلك بسن جملة من النصوص القانونية بعضها عامة وأخرى خاصة، هذا على الصعيد الوطني، أما على الصعيد الدولي فقد سعت مختلف الدول للحد من المخاطر التي تتعرض لها البنوك وذلك بتوحيد الجهود ووضع نظام صارم هدفه حماية نظام الدفع الالكتروني لذلك نتناول حماية البنوك من مخاطر الدفع الالكتروني في ظل التشريع الجزائري (مطلب أول) ثم الحماية القانونية الدولية لها (مطلب ثان).

المطلب الأول: حماية البنوك من مخاطر الدفع الالكتروني في ظل التشريع الجزائري

تولد عن تكنولوجيا الإعلام والاتصال استخدامات غير مشروعة لوسائل الدفع الالكتروني، ما أوجب وضع قواعد قانونية لتحديد شروط استعمالها، وضرورة سن نصوص جزائية لحماية هذه الأنظمة ومعاينة الجاني، سواء كان ذلك بتطبيق نصوص تقليدية على هذا النوع من الأنظمة المعلوماتية، أو بتطبيق نصوص خاصة والتي ظهرت نتيجة تطور المنظومة التشريعية².

¹ حابت أمال، المرجع السابق، ص282.

² درياد مليكة، (المساس بأنظمة المعالجة الآلية للمعطيات)، مجلة حوليات الجزائر¹، كلية الحقوق، جامعة الجزائر 1، الجزء الأول، العدد 33، 2019، ص237.

الفرع الأول: الحماية المكرسة في التشريعات العامة

ساير المشرع الجزائري التشريعات المقارنة فيما يخص تطوير النصوص التقليدية لتحديد الجرائم المعلوماتية وكل اعتداء على أنظمة المعالجة الآلية على النحو التالي:

أولاً/ الحماية المقررة في قانون العقوبات:

نظم المشرع الجزائري جرائم أنظمة المعالجة الالكترونية والعقوبات الواردة عليها في قانون العقوبات، في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" من الفصل الثالث المعنون "بالجنايات والجنگ ضد الأموال" من الكتاب الثالث بعنوان "الجنايات والجنگ ضد الأموال" في المواد من 394 مكرر إلى المادة 394 مكرر 7.

وفيه قسم المشرع جرائم أنظمة المعالجة الآلية إلى جرائم ترتكب من طرف الشخص الطبيعي، نص عليها في المادة 394 مكرر وذلك بالدخول عن طريق الغش إلى النظام الآلي، وهو ما يشكل الركن المادي للجريمة وهذا الأخير متمثل في النشاط الإجرامي وهو تحقيق فعل الدخول إلى النظام المعلوماتي دون أي ترخيص وهذا يعتبر سلوك غير مشروع، أما الركن المعنوي يستلزم إرادة الجاني في الدخول إلى النظام المعلوماتي بكل علم وإرادة¹.

وتنص المادة 394 مكرر، من نفس التقنين على العقوبات في حالة ارتكاب هذه الجريمة، وتقسّم إلى عقوبات أصلية والمتمثلة في الحبس من 3 أشهر إلى سنة وغرامة من 50 ألف دينار إلى مئتي ألف دينار، وتنص المادة 394 مكرر 1 على أنه: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 4.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"²، يتضح من خلال المادة أن الجريمة ركن مادي يتمثل في الاعتداء العمدي في إحدى الأفعال التالية: الإدخال، المحو والتعديل، فالنشاط الإجرامي

¹ أحمد بن مسعود، (جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري)، مجلة الحقوق والعلوم الإنسانية، كلية الحقوق والعلوم السياسية، جامعة الجلفة، المجلد 10، العدد الأول، 2017، ص484.

² القانون رقم 06-23 المتضمن قانون العقوبات مؤرخ في 20 ديسمبر 2006 معدل ومتمم للأمر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات الجزائري، جريدة رسمية عدد 84 المؤرخ في 24 ديسمبر 2006.

يرد على محل وموضوع محدد وهو المعلومات المعالجة آلياً، سواء كانت إشارات أو رموز وليست المعلومات باعتبارها أحد عناصر المعرفة¹.

كما قرر المشرع الجزائري حماية جزائية من المساس العمدي للمعطيات خارج النظام، من خلال المادة 394 مكرر 2 التي تقتضي على أنه: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج كل من يقوم عمداً أو عن طريق الغش بما يأتي: 1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم. 2- حيازة أو إفشاء أو إنشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم في هذا القسم." يتضح من هذا النص أن محل الجريمة تكون في معطيات مخزنة سواء على أشرطة أو أقراص وغيرها، ما دامت أنها وسيلة لارتكاب هذه الجريمة، أما في الفقرة الثانية من ذات النص فقد جرم المشرع الجزائري أفعال الحيازة، الإفشاء والنشر كما اشترط توافر نية الغش².

وأقر المشرع الجزائري إلى جانب العقوبة الأصلية عقوبات تكميلية تتمثل في المصادرة، وهذا حسب المادة 394 مكرر 6 التي تنص على أنه: "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة..."، حسب هذه المادة فإن المصادرة تتعلق بكل وسيلة استخدمت في ارتكاب الجريمة مهما كان نوعها وطبيعتها. أما العقوبة الثانية تتمثل في الغلق كعقوبة تكميلية وجوبية المنصوص عليها في المادة 394 مكرر 6 التي تنص على أنه: "...مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها."

بالنسبة للعقوبات المطبقة على الشخص المعنوي نص عليها المشرع في المادة 394 مكرر 3 وقد استثنى الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية

¹ هداية بوعزة، المرجع السابق، ص 449.

² هداية بوعزة، المرجع السابق، ص (450-451).

فالعقوبة مشددة، ويطبق الحد الأقصى للغرامة المساوي لخمس أضعاف¹. وبخصوص حماية البطاقات الالكترونية، نص المشرع الجزائري في المادة 387 من تقنين العقوبات على أنه: "كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة في مجموعها أو في جزء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 20.000 إلى 100.000 دج، ويجوز أن تجاوز الغرامة 20.000 دج حتى تصل إلى ضعف قيمة الأشياء المخفاة ويجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 من هذا القانون لمدة سنة على الأقل وخمس سنوات على الأكثر وكل ذلك مع عدم الإخلال بأية عقوبات أشد إذا اقتضى الأمر في حالة الاشتراك في الجناية..."، فحسب المادة تقوم هذه الجريمة على ركن مادي يتمثل في الإخفاء والركن المعنوي يتمثل في الإخفاء عمدا أي العلم بالقصد الجرمي للأشياء المخفية².

خص جريمة السرقة بعقوبات صارمة نص عليها في المادة 350 تقنين العقوبات التي تقضي على أنه: "كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100.000 دج إلى 500.000 دج..."، حسب هذه المادة فإن المشرع اشترط أن يكون المال مملوك للغير سواء كان المتهم شخص طبيعي أو شخص معنوي³. وبإسقاط أركان جريمة السرقة على البطاقات الالكترونية يتضح أنها محققة لأنها تعتبر من الأموال المنقولة التي تكون محلا لجريمة السرقة، فالعقوبة المقررة لجريمة سرقة البطاقات الالكترونية هي نفسها العقوبات المنصوص عليها في قانون العقوبات على جريمة السرقة⁴.

¹ حديدان سفيان، (الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، المجلد 2، العدد 8، 2017، ص(683-684).

² عقوبة جريمة إخفاء أشياء في قانون العقوبات الجزائري، أمل المرشدي، <https://www.mohamah.net/law/> تم الإطلاع عليه في 27 جويلية 2020 على الساعة 16:16.

³ عاشور نصر الدين، (جريمة السرقة في ظل التعديلات قانون العقوبات 2006)، مجلة المنتدى القانوني، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 5، بدون سنة، ص230.

⁴ مرشيشي عقيلة، المرجع السابق، ص297.

تنص المادة 372 تقنين العقوبات على أنه: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو مخالصات أو إجراء من الالتزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي أو بإحداث الأمل في الفوز أو في وقوع حادث أو أية أخرى واقعة وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 20.000 إلى 100.000 دج..."، طبقا لهذه المادة فإن الجريمة تقتضي توافر الركن المادي الذي يقوم على استعمال وسائل التدليس باستعمال صفات كاذبة أو مناورات احتيالية والاستيلاء على مال الغير، والعلاقة السببية تكون الوسائل الاحتياطية من شأنها تسليم المال نتيجة خداع، أما الركن المعنوي يتمثل في القصد الجنائي العام وهو انصراف إرادة المتهم إلى تحقيق الجريمة بأركانها والقصد الجنائي الخاص وهي نية المتهم في الاستيلاء¹. ويتبين من ذات النص أن العقوبات المقررة لجريمة الاحتيال في قانون العقوبات الجزائري هي نفسها المطبقة على جريمة الاحتيال في البطاقات الالكترونية².

كما نص المشرع الجزائري على جريمة خيانة الأمانة في المادة 376 تقنين العقوبات التي تقتضي بأنه: "كل من اختلس أو بدد بسوء نية أوراق تجارية أو نقودا أو بضائع... أو أوراقا مالية... يعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 20.000 إلى 100.000 دج ويجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة وذلك لمدة سنة على الأقل وخمس سنوات على الأكثر..."، وتكمن أركان جريمة خيانة الأمانة في موضوع ينصب عليه نشاط الجاني، يتمثل الركن المادي في الاختلاس أو الاستعمال أو التبديد، أما الركن المعنوي يتخذ صورة القصد الجنائي العام وذلك باتجاه إرادة المتهم وانصرافها لارتكاب الجريمة بكامل أركانها، وقصد جنائي خاص يتمثل في نية المتهم في التملك وحرمان

¹ لجنة النصب في قانون العقوبات الجزائري، المكتبة القانونية الجزائرية، <https://law-dz.net/>، تم الإطلاع عليه

في 27 جويلية 2020 على الساعة 16.48.

² بن تركي ليلي، المرجع السابق، ص 100.

المالك الحقيقي للمال منه¹، وطبقا لهذا النص يعتبر حامل البطاقة الالكترونية الذي امتنع عن ردها للجهة المصدرة لها متى طلبتها منه، مرتكبا لجريمة خيانة الأمانة، ويعاقب بنفس العقوبات المقررة على مرتكب جريمة خيانة الأمانة الواردة في ذات النص².

ثانيا/ الحماية المقررة في قانون الإجراءات الجزائية:

تتابع الجريمة الإلكترونية بنفس الإجراءات التي تتابع بها الجريمة التقليدية المتمثلة في التفتيش، المعاينة، الاستجواب، الضبط وغيرها، إلا أن قانون الإجراءات الجزائية³ يتضمن بعض المستجدات الإجرائية وتتمثل في استحداث الأقطاب الجزائية المتخصصة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حسب المادتين 37 و 40 من تقنين الإجراءات الجزائية، وتتمثل أيضا في إمكانية قيام المحاكم الجزائية بالنظر في الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال في الخارج حتى وإن كان الجاني أجنبيا، وتوسيع صلاحية الضبطية القضائية وهذا ما نصت عليه المادة 16، واعتماد أساليب تحري خاصة كاعتراض المراسلات الالكترونية، التسرب وتفتيش المنظومة المعلوماتية وهذا حسب المواد 47، 65 مكرر 5، 65 مكرر 11 من تقنين الإجراءات الجزائية⁴.

ثالثا/ الحماية المقررة في القانون التجاري:

نص المشرع الجزائري في القانون التجاري الجزائري على بطاقات الدفع والسحب في المادة 543 مكرر 23 التي تقتضي بأنه: "تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال. تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب أموال."، كما نصت المادة 543 مكرر 24 على أنه: "الأمر أو الالتزام بالدفع المعطى بموجب بطاقة الدفع غير قابل للرجوع فيه، ولا يمكن الاعتراض

¹ بن تركي ليلي، المرجع السابق، ص 104.

² مرشيشي عقيلة، المرجع السابق، ص 265.

³ الأمر رقم 02-11 المؤرخ في 23 فيفري 2011، جريدة رسمية عدد 12 مؤرخ في 23 فيفري 2011، معدل ومتمم للأمر رقم 66-155 المؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية.

⁴ هداية بوعزة، المرجع السابق، ص (451-452).

على الدفع إلا في حالة ضياع أو سرقة البطاقة المصرح بهما قانونا، أو تسوية قضائية أو إفلاس المستفيد."

اكتفى المشرع الجزائري بتعريف البطاقة الالكترونية كما حدد الوظيفة التي تقوم بها هذه البطاقات وهي الوفاء بالتزامات وسحب النقود، وحدد أيضا الجهات المخول لها إصدار هذه البطاقات وهي البنوك والمؤسسات المالية هذا من خلال المادة 543 مكرر 23 من التقنين التجاري، وأشار في المادة 543 مكرر 24 أن الدفع المعطى بالبطاقة غير قابل للرجوع فيه، والحالات الواردة للاعتراض على الدفع، يتضح من المادتين أنه لا يوجد نص صريح ينظم العمليات المصرفية الالكترونية¹ ولا حماية قانونية للبنوك من المخاطر التي تتعرض لها جراء استعمالها للدفع الالكتروني بالبطاقة وفقا لما ورد بالمادتين.

الفرع الثاني: الحماية المكرسة للدفع الالكتروني في التشريعات الخاصة

شرع المشرع الجزائري في سن تشريعات خاصة بغرض حماية الدفع الالكتروني، من خلال وضع نصوص قانونية صريحة تعاقب على الجرائم المعلوماتية باستغلال المعاملات المصرفية التي تتم في فضاء انترنت مفتوح. ونجد أن الجزائر تأخرت في سن قوانين لحماية وسائل الدفع الالكتروني، والسبب يعود إلى السرعة في التقدم التكنولوجي وانتشار وسائل الدفع الحديثة، أدى إلى ظهور أشكال جديدة للجرائم ما استوجب ضرورة توفير حماية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات²، على النحو التالي:

¹ مرشيشي عقيلة، المرجع السابق، ص26.

² بلحارث ليندة ووالي نادية، (الحماية القانونية لوسائل الدفع الالكتروني)، مداخلة في الملتقى الوطني الثامن حول: آلية تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري، كلية الحقوق والعلوم السياسية، جامعة البويرة، المنعقد في يومي 13 و 14 مارس 2017، ص(3-4).

أولاً/ الحماية القانونية للدفع الالكتروني من خلال قانون الملكية الفكرية الجزائري:

يتضح أن الحماية المقررة للجريمة المعلوماتية من خلال النصوص التقليدية في قانون العقوبات الجزائري هي غير كافية، هذا ما تطلب البحث في مدى إمكانية الحماية من خلال نصوص أخرى ومنها تلك الخاصة بالملكية الفكرية.

1- مكافحة الجريمة المعلوماتية من خلال قانون الملكية الصناعية:

نصت المادة 2 من الأمر 03-06¹ المتعلق بالعلامات على تعريف العلامات الجماعية بأنها: "كل علامة تستعمل لإثبات المصدر والمكونات والإنتاج أو كل ميزة مشتركة لسلع أو خدمات مؤسسات مختلفة عندما تستعمل هذه المؤسسات العلامة تحت رقابة مالكيها"، يتبين من تعريف العلامة أنه يمكن لبرامج الحاسب الآلي الاستفادة من الحماية، لأن كل برنامج يحمل اسماً خاصاً به لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية لبرنامج الحاسب الآلي، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الاسم مقترناً به²، ويتضح أنه لا توجد حماية قانونية للدفع الالكتروني وإنما حماية لبرامج الحاسب الآلي من خلال الأمر 03-06 المتعلق بالعلامات.

2- مكافحة الجريمة المعلوماتية من خلال قانون حقوق المؤلف والحقوق المجاورة

نصت المادة 151 من الأمر 03-05³ المتعلق بحقوق المؤلف والحقوق المجاورة على أنه: "يعد مرتكب جنحة التقليد كل من يقوم بالأعمال التالية: - الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف. - استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة..."، وأشار المشرع الجزائري إلى العقوبة المقررة لمرتكب جنحة التقليد في المادة 153 التي تقضي على أنه: "يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين

¹ الأمر رقم 03-06 المتعلق بالعلامات مؤرخ في 19 جويلية 2003، معدل ومتمم للأمر 67-223 مؤرخ في 19 أكتوبر 1967 المتضمن أحكام العلامات التجارية، جريدة رسمية عدد 44 صادرة في 23 جويلية 2003.

² حابت آمال، المرجع السابق، ص 402.

³ الأمر رقم 03-05 المؤرخ في 19 جويلية 2003 يتعلق بحقوق المؤلف والحقوق المجاورة، جريدة رسمية عدد 44 مؤرخ في 23 جويلية 2003.

151 و 152 أعلاه، بالحبس من ستة(6) أشهر إلى ثلاث(3) سنوات وبغرامة من خمسمائة ألف دينار(5000.000دج) إلى مليون دينار(1.000.000دج) سواء كان النشر قد حصل في الجزائر أو في الخارج".

يتضح من الأمر أن المشرع الجزائري وسع قائمة المصنفات المحمية التي تمكن من القيام بأي نشاط أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم الكترونيا بالحاسوب¹. أما بخصوص مسألة الحماية المخولة للدفع الالكتروني فالمشرع الجزائري لم يخصه بنصوص خاصة، باستثناء حماية البرامج الالكترونية في قانون حقوق المؤلف والحقوق المجاورة².

ثانيا/ الحماية القانونية للدفع الالكتروني من خلال القانون 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين:

يعتبر تنظيم المشرع الجزائري لمسألة التوقيع والتصديق الالكترونيين مسألة مهمة، فالقانون 04-15 يسعى إلى إرساء جو من الثقة وحماية البيانات الشخصية وتأمينها، وكذا تسهيل المعاملات عبر الانترنت عن طريق تجسيد التعامل عن بعد في شتى الميادين كعمليات التجارة الالكترونية، وتعميم استعمال الدفع الالكتروني عبر الانترنت³. يعتبر التوقيع الالكتروني أحد أهم مكونات الجانب القانوني والتشريعي في مجال الأعمال والتجارة الالكترونية، ويستند عليه في تنظيم التعاقدات الالكترونية وأعمال الدفع الالكتروني، عبر البطاقات الالكترونية⁴.

تتجسد الحماية القانونية للتوقيع الالكتروني من خلال المادة 68 من نفس التقنين التي تقضي بأنه: "يعاقب بالحبس من ثلاثة(3) أشهر إلى ثلاث(3) سنوات وبغرامة من مليون دينار(1.000.000دج) إلى خمس ملايين دينار(5.000.000دج)، أو بإحدى هاتين العقوبتين، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني

¹ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص107.

² حابت أمال، المرجع السابق، ص406.

³ هداية بوعزة، المرجع السابق، ص(456-457).

⁴ غزالي نزيهة، المرجع السابق، ص289.

موصوف خاصة بالغير"، ويتضح من المادة أن المشرع اكتفى بحماية التوقيع الالكتروني باعتباره من أساليب التأمين والحماية التقنية لعمليات الدفع الالكتروني ووسيلة إثبات لها¹، ولا توجد حماية قانونية مقررة للبنوك من مخاطر الدفع الالكتروني.

ثالثا/ الحماية القانونية للدفع الالكتروني من خلال قانون التجارة الالكترونية الجزائري:

تضمن القانون 18-05² المتعلق بالتجارة الالكترونية أحكام متعلقة بالدفع الالكتروني في الفصل السادس المعنون بالدفع في المعاملات الالكترونية، وقد نصت المادة 27 الفقرة الأولى من نفس القانون على أنه: "يتم الدفع في المعاملات التجارية الالكترونية إما عن بعد أو عند تسليم المنتج، عن طريق وسائل الدفع المرخص بها وفقا للتشريع المعمول به..."، ويتضح من هذا النص أن المشرع الجزائري لم يشترط أن يكون الدفع الكترونيا، بل يمكن أن يتم بأية وسيلة كانت يشترط أن تكون مرخص بها ومعترف بها قانونا³. واشترط المشرع الجزائري في حالة الدفع الالكتروني، أن يتم من خلال منصات دفع مخصصة لهذا الغرض، منشأة ومستغلة حصريا من طرف البنوك المعتمدة من قبل البنك الجزائر وبنك الجزائر وموصولة بأي نوع من أنواع محطات الدفع الالكتروني عبر شبكة المتعامل العمومي للمواصلات السلكية واللاسلكية⁴، كما اشترط المشرع من خلال المادة 28 من نفس القانون أنه من الواجب أن يكون وصل موقع الانترنت الخاص بالموارد الالكتروني بمنصة الدفع الالكترونية مؤمنا بواسطة نظام تصديق الكتروني.

رابعا/ الحماية القانونية للدفع الالكتروني من خلال قانون النقد والقرض:

نصت المادة 69 من الأمر 11-03 الصادر في 26 أوت 2003 المتعلق بالنقد والقرض المعدل والمتمم على الاعتراف باستعمال كافة وسائل الدفع التي تسمح للأشخاص تحويل الأموال مهما كانت الدعامة أو الطريقة المستعملة وهذا يعني أن

¹ هداية بوعزة، المرجع السابق، ص 457.

² القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، جريدة رسمية عدد 28 مؤرخ في 16 ماي 2018.

³ هداية بوعزة، المرجع السابق، ص 457.

⁴ منصوص عليها في المادة 27 فقرة 2 من القانون 18-05 المتعلق بالتجارة الالكترونية.

التشريع الجزائري تضمن إمكانية استعمال كافة تقنيات ووسائل تقليدية والكترونية وهو اعتراف ضمني لاستعمال الوسائل الالكترونية والتقنيات الحديثة في الدفع¹.
تقطن المشرع الجزائري إلى افتقار المنظومة التشريعية للقواعد القانونية التي تواكب التطور التقني المستمر بالنسبة لإتمام الأعمال التجارية الكترونيا، فحاول جاهدا لإثراء المنظومة التشريعية في مجال التعامل التجاري الالكتروني وتحديث أنظمة الدفع، فالمشرع الجزائري اعترف ضمنا بتقنية الدفع الالكتروني، لكن دون تقديم تعريف لتقنية الدفع الالكتروني ولا حماية للبنوك من المخاطر التي تتجر عن هذه التقنية².

خامسا/ الحماية القانونية للدفع الالكتروني من خلال النظام 12-03 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما:

تضمن الباب السادس المعنون بالتحويلات الالكترونية ووضع الأموال تحت التصرف، عملية من عمليات الدفع الالكتروني وهي التحويل الالكتروني والمنصوص عليها في المادة 17 من النظام 12-03 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما والتي تنص على أنه: "يتعين على المصارف والمؤسسات المالية لبريد الجزائر في إطار التحويلات الالكترونية مهما كانت الوسيلة المستعملة (ATCI و ARTS و SWIFT...الخ) و/أو وضع الأموال تحت التصرف أن تسهر على التحقق بدقة من هوية الأمر بالعملية والمستفيد بالإضافة إلى عنوانيهما. يجب أن يحوز مسيرو نظام الدفع والمتعاملون المباشرون أو غير المباشرين على جهاز آلي لاكتشاف الزبائن والعمليات ويتعلق الأمر بالهيئات أو الأشخاص المسجلين في القوائم المعدة مسبقا"³، ويتضح من المادة 17 من نفس النظام أن المشرع الجزائري لم يصرح بالدفع الالكتروني بل اكتفى بذكر عملية من العمليات التي تقوم بها البنوك وهي التحويل الالكتروني، بالرغم من الميزة التي يتميز بها التحويل الالكتروني إلا أنه لم يحظ بتنظيم تشريعي خاص.

¹ شبوب نصيرة، المرجع السابق، ص150.

² هداية بوعزة، المرجع السابق، ص14.

³ النظام رقم 12-03 مؤرخ في 28 نوفمبر 2012، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، جريدة رسمية عدد 12 مؤرخ في 27 فيفري 2013.

فالمشرع الجزائري لم يتبن تقنية التحويل، باعتباره أحد وسائل الدفع الالكتروني إلا من خلال آخر تعديل عرفه التقنين التجاري، وعليه وفي ظل غياب نظام تشريعي خاص يخضع له التحويل الالكتروني¹، وقصور التشريعات العقابية على الإحاطة بجريمة تبييض الأموال في نمطها التقليدي وضعف الآليات القانونية لتأطير الجرائم الالكترونية²، يتضح أن التحويل الالكتروني وجرائم تبييض الأموال المستخدمة بواسطته، تخضع إلى القانون رقم 04-15 المتضمن قانون العقوبات، طبقا للمادة 389 مكرر منه التي تحدد عقوبات لجريمة تبييض الأموال، المتمثلة في الحبس من خمس سنوات إلى عشر سنوات وغرامة من 1.000.000 دج إلى 3.000.000 دج وقد تصل في حالة ارتكابها في ظروف مشددة إلى 20 سنة حبسا نافذا، وبغرامة من 4.000.000 دج إلى 8.000.000 دج كما نصت على إمكانية توقيع عقوبات تكميلية على مرتكب جريمة تبييض الأموال، وعلى عقوبات تطبق على الشخص المعنوي مرتكب هذه الجريمة، يتضح أن المشرع الجزائري اكتفى بنسب جريمة تبييض الأموال المعاقب عليها في النصوص التقليدية إلى جريمة تبييض الأموال باستعمال التحويل الالكتروني باعتباره أحد وسائل الدفع الالكتروني³.

سادسا/ الحماية القانونية للدفع الالكتروني من خلال القانون 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

جاء القانون 09-04⁴ المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بغرض مكافحة الإرهاب الالكتروني، ضم في بابه الأول تعريف وتحديد الجرائم المعلوماتية، ثم انتقل إلى كيفية الحد منها بعدما أصبحت من النوع الذي يهدد أمن وسلامة المعاملات. يتضمن القانون عدة تعريفات وتسميات كالبيانات الالكترونية،

¹ عبد الله ليندة، المرجع السابق، ص36.

² العيد سعدي، المرجع السابق، ص238.

³ تدرست كريمة، المرجع السابق، ص133.

⁴ القانون رقم 09-04 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 مؤرخ في 16 أوت 2009.

الجريمة المعلوماتية وغيرها، وبالتالي فهو يطبق على كل التكنولوجيات الحديثة بما فيها الدفع الالكتروني¹.

تنص المادة 2 من نفس القانون على أنه: "أ- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية..."، ويتضح من المادة أن المشرع الجزائري وسع مجال الحماية القانونية إذ مست كافة الجرائم سواء الماسة بأمن الدولة أو الاقتصاد الوطني وذلك من خلال عبارة " أي جريمة أخرى"، ويمكن إدراج الاعتداء على شبكة الاتصالات الخاصة بمواقع البنوك ومختلف العمليات النقدية الالكترونية التي تتم بين المنشآت التجارية والاقتصادية ضمن الجرائم الماسة بالاقتصاد الوطني². وتتراوح العقوبات المنصوص عليها في هذا القانون في حق مرتكبي هذه الجرائم بين سنة واحدة و10 سنوات سجنا وغرامات مالية تصل إلى 5 ملايين دينار³.

المطلب الثاني: الحماية القانونية الدولية لمكافحة مخاطر الدفع الالكتروني

تسعى مختلف الدول لحماية الدفع الالكتروني وذلك من خلال وضع نصوص قانونية صريحة تعاقب على الجرائم المعلوماتية لحماية المتعاملين عبر شبكة الانترنت، وحماية الدفع الالكتروني من مختلف المخاطر التي تمسها⁴، بواسطة الجهود الدولية أو مختلف التشريعات المقارنة.

الفرع الأول: الجهود الدولية لمكافحة مخاطر الدفع الالكتروني

تضافرت الجهود الدولية لترقية التجارة الالكترونية بوضع نظام قانوني صارم يضمن حماية فعالة للمعاملات الالكترونية وبالتالي حماية الدفع الالكتروني⁵، ومن بين الجهود

¹ صغير يوسف، المرجع السابق، ص115.

² شبوب نصيرة، المرجع السابق، ص157.

³ شبوب نصيرة، المرجع نفسه، ص156.

⁴ بلحارث ليندة ووالي نادية، المرجع السابق، ص3.

⁵ واقد يوسف، المرجع السابق، ص184.

الدولية التي تسعى لحماية الدفع الالكتروني نقدم بعض النماذج المتمثلة في:

أولا/ الحماية القانونية في ظل الاتحاد الأوروبي:

يظهر اهتمام الاتحاد الأوروبي لحماية المعاملات الالكترونية من خلال توصية المجموعة الاقتصادية الأوروبية تحت رقم 87-598¹ حول القانون الأوروبي المتعلق بالسيرة الحسنة الخاصة بالدفع الالكتروني، حيث دعت هذه التوصية جميع المتعاملين لتطبيق هذا القانون من أجل ترقية الحماية والضمان للعملاء²، كما تنص على إضفاء الطابع الشخصي والسري للمعطيات أو البيانات المقدمة من طرف العميل وحق الدخول إلى كافة خدمات مقدمي خدمات الدفع الالكتروني، كما تلزم حامل البطاقة بضرورة الأخذ بالعناية اللازمة في استعمال البطاقة الالكترونية³.

صدرت توصية ثانية عن الاتحاد الأوروبي، تحت رقم 97-489⁴ والمتعلقة بالمعاملات التي تتم بواسطة وسائل الدفع الالكتروني، ركزت على مصدر البطاقة وحاملها فطبقت هذه التوصية على مختلف المعاملات التي تمت عن طريق وسائل الدفع الالكتروني عن بعد لاسيما:

- ✓ انتقال الأموال المتعلقة باستخدام وسائل الدفع الالكتروني.
- ✓ سحب الأموال السائلة بواسطة الدفع الالكتروني أو النقود الرقمية التي تتم في آلات السحب الآلي للأوراق.
- ✓ كما أكدت هذه التوصية على ضرورة استعمال وسائل الدفع الالكتروني بالطريقة الصحيحة حسب الشروط المتفق عليها، مع الأخذ بجميع الاحتياطات اللازمة لحمايتها⁵.

¹ Recommandation N° 87/598/CEE de la commission européenne du 8 décembre 1987 portant sur un code européen de bonne conduite en matière de paiement électronique, jOL 365, 24 décembre 1987.

² بلحارث ليندة ووالي نادية، المرجع السابق، ص8.

³ واقد يوسف، المرجع السابق، ص185.

⁴ Recommandation 97/489/CE du 30 juillet 1997 concernant les opération effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire, JOL 28, du 2 Août 1997.

⁵ بلحارث ليندة ووالي نادية، المرجع السابق، ص ص(6-8).

ثانيا/ جهود المنظمة الدولية للأمم المتحدة:

- توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الإجرام الدولي لمواجهة جرائم الانترنت يتطلب من الدول الأعضاء اتخاذ عدة إجراءات نذكر منها:
1. تحديث القوانين وأغراضها الجنائية، بما فيها التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة (التحقيق - قبول الأدلة) على نحو ملائم وإدخال التعديلات إذا دعت الضرورة.
 2. رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذا النوع من الجرائم بأهمية مكافحة هذه الجرائم ومحاكمة مرتكبيها¹.

ثالثا/ الاتحاد الدولي للاتصالات لحماية الفضاء الالكتروني:

وضع الاتحاد الدولي للاتصالات مجموعة من التوصيات التي تحدد السبل المسموح بها لاستعمال المعلومات وأنظمة الاتصالات الالكترونية، مع التشديد بوضعها لعدة مبادئ من بينها تأمين استمرارية الخدمة، خصوصية المعلومات والمعطيات وغيرها من المبادئ، فهي تهدف إلى حماية الاقتصاد بشكل عام والمعلومات المخزنة وأنظمة المعلومات وثقة المستخدمين بشكل خاص. ويدعو الاتحاد الدولي لمواجهة التحديات عبر تضافر جهود الأفراد وبالقوانين والأطر التنظيمية والإجراءات التكنولوجية، كما ألزم الأفراد إتباع الإجراءات الموضوعة من قبل المؤسسات المعنية².

رابعا/ المنظمة العالمية للملكية الفكرية:

تعد المنظمة العالمية للملكية الفكرية إحدى الوكالات التابعة للأمم المتحدة، اهتمت بالمجال المعلوماتي وذلك بتوفير حماية قانونية للبرامج المعلوماتية وقواعد البيانات. هذه الحماية لم تكن كافية في تشريعات براءات الاختراع، وبذلك تم الاتفاق على تطوير الحماية عن طريق اتفاقيات عالمية خاصة "التبرس وبرن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، خاصة تشريعات حق المؤلف، ووضع عقوبات

¹ صغير يوسف، المرجع السابق، ص(93-94).

² هداية بوعزة، المرجع السابق، ص(405-406).

على كل أعمال تزوير في المعاملات التجارية والقرصنة، ويعتبر الانترنت المكان المناسب لهذه التصرفات، والتي وصلت بموجبها الحماية القانونية لبرامج وقواعد البيانات المعلوماتية¹.

خامسا/ الحماية القانونية في ظل المنظمة العالمية للتجارة:

اهتمت المنظمة العالمية للتجارة بموضوع التجارة الالكترونية، وذلك بتحديد أهمية الحفاظ على تطور التجارة الالكترونية من خلال برنامج يراعي الاحتياجات الاقتصادية والفنية للدول النامية، وكذا عدم فرض رسوم جمركية على الوسائل الالكترونية لفترات مؤقتة، وتوفير الدعم المالي والفني لتمكين هذه الدول من إنشاء بنية أساسية تؤهلها من المشاركة في التجارة الالكترونية. يتمثل موقف الدول المتقدمة وخاصة الولايات المتحدة الأمريكية في ضرورة خضوع المنتجات الالكترونية لمبادئ المنظمة وتقنين عدم فرض الرسوم الجمركية على الرسائل الالكترونية².

سادسا/ الحماية القانونية من خلال المنظمة الدولية لضباط الجرائم المالية:

تتولى المنظمة الدولية لضباط الجرائم المالية مكافحة مختلف الجرائم والاعتداءات الحاصلة على البطاقات الالكترونية مع فرض الحماية على المنتجات الالكترونية التي تصنع منها.

تتيح عضوية هذه المنظمة لأعضائها الحصول على معلومات سرية تتعلق بالجرائم المالية الدولية والمجرمين الدوليين، كما ترسل إنذارات لأعضائها بالأعضاء المعرضة لهذه الجرائم، فتسمح لعضوها بالدخول على شبكات الكمبيوتر التي تخص مثل هذه الجرائم³.

سابعا/ معاهدة بودابست بشأن جرائم الحسابات في حماية وسائل الدفع الالكتروني:

تعتبر معاهدة بودابست معاهدة أوروبية، وأصبحت دولية بانضمام العديد من دول العالم إليها، وهي أول معاهدة دولية بشأن الأفعال الإجرامية، فهي تكافح جرائم الانترنت

¹ صغير يوسف، المرجع السابق، ص 98.

² واقد يوسف، المرجع السابق، ص 190.

³ بلحارث ليندة ووالي نادية، المرجع السابق، ص 11.

والحد منها خاصة بعد تطور الجرائم التي أصبحت تهدد الأشخاص والممتلكات، فتضمنت جوانب عديدة من بينها اتفاقيات الإرهاب الالكتروني، وعمليات تزوير البطاقات الالكترونية، تتضمن هذه المعاهدة 48 مادة مقسمة إلى أربعة فصول:

- الفصل الأول: تعريفات خاصة لبعض المصطلحات الفنية لتوحيد المفاهيم.
- الفصل الثاني: تركيبات لابد من اتخاذها على الصعيد المحلي.
- الفصل الثالث: مسائل التعاون الدولي وتسليم الجناة والمساندة المشتركة، الإجراءات، التعاون في التحريات وجمع بيانات المرور والحركة الخاصة بالبيانات.
- الفصل الرابع: يتعلق بالانضمام والانسحاب من المعاهدة وتعديلها وفض المنازعات والتشاور بين الأعضاء¹.

الفرع الثاني: موقف التشريعات المقارنة بشأن حماية الدفع الالكتروني

شرعت العديد من دول العالم في سن تشريعات خاصة بحماية الدفع الالكتروني، من خلال قوانين تعاقب على الجرائم المعلوماتية بهدف حماية المتعاملين عبر شبكات الانترنت².

أولا/ موقف بعض التشريعات الغربية بشأن حماية الدفع الالكتروني:

تتعدد الدول التي تطرقت إلى الدفع الالكتروني في تشريعاتها الداخلية نذكر منها:

1/ الحماية القانونية للدفع الالكتروني في التشريع الفرنسي:

سعى التشريع الفرنسي جاها لسن أول قانون مستقل، وذلك سنة 1985 بهدف حماية المعلوماتية، فتم إعداد كتاب كامل فيما تعلق بالجرائم المعلوماتية³، بعد ذلك صدر قانون 88-19 في 5 جانفي 1988 والخاص بالغش المعلوماتي، وقد نص هذا القانون بصفة غير مباشرة على الحماية الجزائية للبطاقة الالكترونية في المادة 462 الفقرة الخامسة والسادسة، وتتعلق المادة بتزوير المستندات المعالجة آليا واستعمالها، ويفهم من لفظ "المستندات" أنها تتضمن وسائل الدفع الالكترونية بما فيها البطاقات الالكترونية⁴.

¹ هداية بوعزة، المرجع السابق، (406-407).

² واقد يوسف، المرجع السابق، ص172.

³ بلحارث ليندة ووالي نادية، المرجع السابق، ص3.

⁴ هداية بوعزة، المرجع السابق، ص418.

وتدخل المشرع الفرنسي بموجب القانون 91-1382 الصادر في 30 ديسمبر 1991 في المادة 11 والتي تجرم بعض صور الاستعمال غير المشروع للبطاقة الالكترونية المقلدة والمزورة. كما جاء قانون العقوبات الفرنسي بتعديل آخر وذلك سنة 2004، أضاف بموجبه جريمة أخرى هي جريمة التعامل في وسائل يمكن أن ترتكب بها جريمة ويمكن استعمالها في التلاعب بالمعطيات أو إفساد أنظمة المعالجة الآلية للمعطيات¹.

إلى جانب قانون العقوبات تم سن العديد من القوانين لتدعيم هذه الحماية من أبرزها قانون رقم 2001-1062 المتعلق بالحماية الدائمة، والتي أدخلت في قانون النقد الفرنسي بهدف ضمان الدفع الذي يتم ببطاقة الدفع ومنح فرنسا صلاحية ضمان حماية وسائل الدفع².

2/ الحماية القانونية للدفع الالكتروني في التشريع الإيطالي:

تنص المادة 12 من القانون رقم 72 لسنة 1992 للعقوبات، على معاقبة كل من يسيء استخدام البطاقة الالكترونية أو ما شابهها من وسائل السداد، في حالة استخدامها بهدف سلب الأموال رغم أنه ليس بمالكها الشرعي أو استعمالها في السداد النقدي المقدم أو سداد قيمة بالسجن من سنة إلى 5 سنوات، أو بغرامة تتراوح بين 600 ألف وثلاثة ملايين ليرة إيطالية، وتطبق نفس العقوبة على كل من زيف جزئياً أو كلياً، البطاقات الالكترونية بغرض الاستيلاء على الأموال³.

ثانياً/ موقف بعض التشريعات العربية بشأن حماية الدفع الالكتروني:

نصت العديد من الدول العربية في تشريعاتها على حماية الدفع الالكتروني من بينها مصر والمغرب:

1/ الحماية القانونية للدفع الالكتروني في التشريع المصري:

تعدد تعديل قانون العقوبات المصري، إلا أنه يخلو من نصوص تعاقب على الأفعال غير المشروعة التي تصاحب نشاط وسائل الدفع الالكترونية، وقد لجأ القضاء المصري

¹ واقد يوسف، المرجع السابق، ص(174-175).

² بلحارث ليندة ووالي نادية، المرجع السابق، ص4.

³ هداية بوعزة، المرجع السابق، ص 421.

إلى تطبيق المواد التي تنص على عقوبات جرائم السرقة، الاحتيال، التزوير وخيانة الأمانة على الجرائم المعلوماتية.

صدر القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الالكتروني وحسم العديد من المشكلات القانونية التي كان يتصدى لها القضاء المصري، تضمن هذا القانون تعريفات واضحة ومحددة لماهية المحرر الالكتروني وغيرها من التعريفات¹، كتعريف التشفير الالكتروني بأنه منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونياً².

صدر مؤخراً القانون رقم 175 لسنة 2018 في 14 أغسطس 2018 المتعلق بمكافحة جرائم تقنية المعلومات³، والذي تضمن في الفصل الثالث على الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات، في المادة 23 بعنوان جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الالكتروني والتي تنص على ما يلي: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام بيانات البنوك والخدمات أو غيرها من أدوات الدفع الالكترونية... وتكون العقوبة مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين إذا توصل من ذلك الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير". فبصدور القانون الجديد منع المشرع المصري باب الاجتهاد بشأن المعاقبة على الأفعال غير المشروعة المصاحبة لنشاط البطاقات الالكترونية والتي كان يطبق عليها ما يطبق بشأن جرائم السرقة، الاحتيال، التزوير وخيانة الأمانة⁴.

¹ هداية بوعزة، المرجع السابق، ص 428.

² هداية بوعزة ويوسف فتيحة، المرجع السابق، ص 31.

³ القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، جريدة رسمية عدد 32 مكرر (ج)، الصادرة بتاريخ 14 أوت 2018.

⁴ هداية بوعزة، المرجع السابق، ص 429.

2/ الحماية القانونية للدفع الالكتروني في التشريع المغربي:

تضمن قانون العقوبات المغربي في الباب العاشر منه تعديلا بتاريخ 11 نوفمبر 2003، بإضافة المواد 607 فقرة 3 إلى غاية المادة 607 فقرة 11 لتجريم كافة الأفعال غير المشروعة المتعلقة بنظم المعالجة الآلية للمعلومات، ونص في قانون رقم 153-05 الصادر في 30 نوفمبر 2007 المتعلق بالتبادل الالكتروني للمعطيات القانونية².

¹ ظهير شريف رقم 129.1.07 صادر في 19 من ذي القعدة 1428 (30 نوفمبر 2007) بتنفيذ القانون رقم 53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونية.

² بن تركي ليلي، المرجع السابق، ص295.

الخلاصة

الخاتمة

عرف القطاع المصرفي في العالم قفزة نوعية في إطار المعاملات التجارية والبنكية وذلك بمواكبته للتطور التكنولوجي على إثر الانتشار الواسع لاستعمال الانترنت، ما أدى إلى ظهور وسائل دفع حديثة التي كانت وليدة البنوك الالكترونية، فحظيت بمكانة وأهمية ما ساعد في انتشارها وقبولها من طرف المتعاملين، والتي بدورها فاقت في أهميتها الوسائل التقليدية نظرا للسهولة التي توفرها في خدمات البيع والشراء بين المتعاملين والسرعة في المعاملات وتوفير الأمان، وهذا أدى إلى التحويل المادي لوسائل الدفع إلى وسائل حديثة غير ملموسة والتي لا يمكن استعمالها إلا عبر أجهزة الكمبيوتر وتقنياته الحديثة.

أثارت وسائل الدفع الالكترونية مشكلات بسبب الاستعمال غير المشروع لها، بحيث لم تكن مثالية كما توقعت البنوك لدى تبنيها للتكنولوجيا المعلوماتية، فكان لها الوضع السلبي حيث تعرضت البنوك للعديد من المخاطر منها التقنية وتكون في شكل اعتداءات بسرقة البطاقة الالكترونية، واستعمالها بطريقة غير مشروعة، واختراق أنظمة الدفع من أجل تحقيق مكاسب غير مشروعة، أو عن طريق ارتكاب جرائم تبويض الأموال والتهرب الضريبي أو القرصنة المعلوماتية، فيترتب عن هذه المخاطر خسائر للبنوك والمتعاملين معها ما دفع بالبنوك تبني مجموعة من التقنيات للحد من هذه المخاطر كالتوقيع والكتابة الالكترونيين، والاعتماد على التأمين والتشفير وغيرها من التقنيات، وتوفير حماية قانونية من طرف المشرع الجزائري من خلال بعض النصوص كقانون النقد والقرض، القانون التجاري، وفرض عقوبات على الجناة في قانون العقوبات، وسن قوانين خاصة لتوفير حماية فعالة لهذه الوسائل الالكترونية، كما حظيت بحماية دولية سواء من طرف التشريعات المقارنة أو من طرف الجهود الدولية.

نتائج الدراسة:

تتحصر أهم النتائج التي توصلنا إليها من خلال دراستنا في النقاط التالية:

- 1- يفترض على الجهاز المصرفي الاستجابة للتطورات الحاصلة في النشاط الاقتصادي لأن الجهاز المصرفي قطاع حساس و يتطلب السرعة في المعاملات والخدمات البنكية.

2- تعتبر البنوك الالكترونية مرحلة انتقالية ترتبت عنها وسائل الكترونية حديثة يجب أن تستعمل بشكل مشروع يمنع حصول جرائم بها.

3- أصبحت العديد من دول العالم تعتمد على وسائل الدفع الالكترونية في شتى المعاملات التجارية بما فيها الجزائر لكن عدم وجود حماية كافية في التشريع الجزائري لهذه الوسائل دفع المتعاملين على عدم وضع الثقة فيها وعدم إقبالهم على استعمالها.

التوصيات و الاقتراحات:

في ضوء النتائج المتوصل إليها من خلال هذه الدراسة ارتأينا تقديم التوصيات التالية:

1- إدخال وسائل الدفع الالكترونية وفرضها على أفراد المجتمع للتعامل بها والتخلي عن الوسائل التقليدية؛ مع ضمان حمايتهم من أي استخدام غير مشروع لها.

2- نشر إعلانات تتعلق بأهمية وسائل الدفع الالكتروني وضرورة الإبلاغ عن أي استخدام مشبوه لها، وبعث الثقة لدى المتعاملين بها وعن كيفية استعمالها والإجراءات المتخذة في حال ضياعها أو سرقتها.

3- خلق بيئة قانونية تساهم في التطورات الحاصلة على مستوى الجهاز المصرفي وتنظيم الدفع الالكتروني، وسن نصوص قانونية تجرم الاستخدام غير المشروع للوسائل الالكترونية.

4- نظرا لعدم وجود نصوص قانونية تعاقب الجناة على الاستعمال غير المشروع لوسائل الدفع وحماية مقررّة لهذه الوسائل، نقترح التعجيل في إصدار النصوص القانونية المتعلقة بتطبيق قانون التجارة الالكترونية فيما يتعلق بوسائل الدفع الالكترونية وطرق استخدامها وتجسيد الحماية المقررة لها.

بهذا نكون قد أنهينا دراستنا لموضوع مخاطر الدفع الالكتروني على البنوك.

قائمة

المصادر والمراجع

أولاً/ الكتب:

- 1- التميمي علاء، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، دار الجامعة الجديدة للنشر، الإسكندرية، 2012.
- 2- السيد سعيد قنديل، التوقيع الالكتروني (ماهيته، صورته، حججه في الإثبات بين التداول والاقتباس)، دار الجامعة للنشر، الطبعة الثانية، الإسكندرية، 2006.
- 3- الغصبر بن سليمان خالد والقحطاني بن عبد الله محمد، أمن المعلومات، مكتبة الملك فهد الوطنية للنشر، الطبعة الأولى، الرياض، 2009.
- 4- ردايدة عبد الكريم، جرائم بطاقات الائتمان، دراسة تطبيقية ميدانية، دار حامد للنشر والتوزيع، الطبعة الأولى، الأردن، 2013.
- 5- عامر محمد بسام مطر، الشيك الالكتروني، دار الجنان للنشر والتوزيع، الأردن، 2013.
- 6- عبد الحكيم أحمد محمد عثمان، أحكام البطاقات الائتمانية في القانون والآراء الفقهية الإسلامية، دار الفكر الجامعي، الإسكندرية، 2007.
- 7- غنيمي رضوان، بطاقة الائتمان بين الوضع القانوني المصرفي والتأصيل الفقهي، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2012.
- 8- كافي مصطفى يوسف، النقود والبنوك الالكترونية في ظل التقنيات الحديثة، دار مؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2011.
- 9- كميث طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان (المسؤولية الجزائية والمدنية)، دار الثقافة، عمان، الأردن، 2008.
- 10- ممدوح خالد إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2011.

ثانياً/ الأطروحات والمذكرات العلمية:

1- الأطروحات:

- 1- العنزي بن سطم بن خلف إبراهيم، التوقيع الالكتروني وحمايته الجنائية، أطروحة لنيل درجة دكتوراه، تخصص فلسفة العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

- 2- العيد سعدية، المسؤولية الجزائية للبنك عن جريمة تبييض الأموال، أطروحة لنيل درجة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016.
- 3- بلقاسم حمدي، إبرام العقد الإلكتروني، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، (2014-2015).
- 4- بن تركي ليلي، الحماية الجنائية لبطاقة الائتمان الممغنطة، أطروحة لنيل درجة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، (2016-2017).
- 5- بوعزة هداية، النظام القانوني للدفع الإلكتروني، دراسة مقارنة، أطروحة لنيل درجة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، (2008-2009).
- 6- تدريست كريمة، دور البنوك في مكافحة تبييض الأموال، أطروحة لنيل درجة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2014.
- 7- حابت أمال، التجارة الإلكترونية في الجزائر، أطروحة لنيل درجة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015.
- 8- حدوم ليلي، أنظمة الدفع ما بين البنوك، أطروحة لنيل درجة دكتوراه، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر 1، (2011-2012).
- 9- حفصي عباس، جرائم التزوير الإلكترونية، دراسة مقارنة، أطروحة لنيل درجة دكتوراه، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1، (2014-2015).
- 10- حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة لنيل درجة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، (2014-2015).
- 11- زماموش ندير، أليات الدفع الإلكترونية، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق، جامعة الجزائر 1، (2017-2018).

- 12- سلالي بوبكر، أثر النقود الالكترونية على إدارة السياسة النقدية، دراسة استشرافية على الجزائر، أطروحة لنيل درجة دكتوراه، تخصص علوم اقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد بوضياف، مسيلة، 2019.
- 13- عرورة فتيحة، وسائل التبادل المصرفي في القانون الجزائري، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق، جامعة الجزائر 1، (2016-2017).
- 14- غزالي نزيهة، المسؤولية الجزائية عن استخدام وسائل الدفع الالكتروني في القانون الجزائري، أطروحة لنيل درجة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، (2017-2018).
- 15- مخلوفي عبد الوهاب، التجارة الالكترونية عبر الانترنت، أطروحة لنيل درجة دكتوراه، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، (2011-2012).
- 16- مرشيشي عقيلة، بطاقة الائتمان في القانون الجزائري، دراسة مقارنة، أطروحة لنيل درجة دكتوراه، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2017.
- 17- مسيدري سيد أحمد، النظام القانوني للمقاصة في المعاملات البنكية، دراسة مقارنة، أطروحة لنيل درجة دكتوراه، تخصص قانون خاص، جامعة أبو بكر بلقايد، تلمسان، (2017-2018).
- 18- هنشور مصطفى وسيمة، النظام القانوني للتجارة الالكترونية في التشريع الجزائري والمقارن، أطروحة لنيل درجة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، (2016-2017).

2- المذكرات:

- 1- الجبوري عمر عبد السلام حسين، جريمة التزوير الالكتروني في التشريع الأردني، دراسة مقارنة، مذكرة لنيل شهادة ماجستير، تخصص قانون عام، جامعة الشرق الأوسط، الأردن، 2017.
- 2- الشقيرات طارق محمد عودة الله، مسؤولية البنوك في التحويل الالكتروني للأموال، دراسة في التشريع الأردني، مذكرة لنيل شهادة ماجستير، تخصص قانون، الجامعة الأردنية، 2005.

- 3- القواسمي صفاء يوسف، المسؤوليات القانونية الناشئة عن عمليات المقاصة الالكترونية للشيكات في القانون الأردني، مذكرة لنيل شهادة ماجستير، تخصص قانون خاص، جامعة الشرق الأوسط للدراسات العليا، الأردن، 2009.
- 4- بن عميور أمينة، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة لنيل شهادة ماجستير، تخصص قانون أعمال، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، (2004-2005).
- 5- بن هلال المطيري صقر، جريمة غسيل الأموال، دراسة حول مفهومها، ومعوقات التحقيق فيها وإشكاليات تنسيق الجهود لمواجهتها، مذكرة لنيل شهادة ماجستير، تخصص التشريع الجنائي الإسلامي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
- 6- حبيش علي، أثار الإصلاحات المصرفية في مكافحة تبييض الأموال في الجزائر، مذكرة لنيل شهادة ماجستير، تخصص نقود مالية وبنوك، كلية العلوم الاقتصادية وعلوم التسيير، جامعة سعد دحلب، البليدة، 2006.
- 7- خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، دراسة مقارنة، مذكرة لنيل شهادة ماجستير، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2017.
- 8- دحية رباب، دراسة تحليلية لأداء أنظمة الدفع، حالة نظام الدفع المكثف بالجزائر، مذكرة لنيل شهادة ماجستير، تخصص مالية بنوك وتأمينات، كلية الحقوق والعلوم السياسية، جامعة مسيلة، (2011-2012).
- 9- سمية ديمش، التجارة الالكترونية حقيقتها وواقعها في الجزائر، مذكرة لنيل شهادة ماجستير، تخصص تحليل واستشراف اقتصادي، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الإخوة منتوري، قسنطينة، (2010-2012).
- 10- شبوب نصيرة، الإدارة البنكية الالكترونية في الجزائر، دراسة ميدانية حول أنظمة النقد الآلي، مذكرة لنيل شهادة ماجستير، تخصص مجتمع معلومات، كلية العلوم السياسية، جامعة الجزائر 3، (2012-2013).
- 11- شفارة عبد النور، حماية المستهلك في الخدمات المصرفية الالكترونية، مذكرة لنيل شهادة ماجستير، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر 1، (2014-2015).

- 12- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.
- 13- طمين سهيلة، الشكالية في عقود التجارة الالكترونية، مذكرة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2011.
- 14- عبد الله ليندة، النظام القانوني لبطاقات الدفع، مذكرة لنيل شهادة ماجستير، تخصص قانون خاص، كلية الحقوق، جامعة جيجل، 2007.
- 15- عديدان مرزوق عبد الله إنصافي، التنظيم القانوني لبطاقة الائتمان الصادرة عن البنوك، دراسة مقارنة بين التشريعين الأردني والكويتي، مذكرة لنيل شهادة ماجستير، تخصص قانون، جامعة آل البيت، (2015-2016).
- 16- فوغالي بسمة، إثبات العقد الالكتروني وحجته في ظل عالم الانترنت، مذكرة لنيل شهادة ماجستير، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، (2014-2015).
- 17- لوصيف عمار، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين مع الإشارة إلى التجربة الجزائرية، مذكرة لنيل شهادة ماجستير، تخصص تحليل والاستشراف الاقتصادي، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، (2008-2009).
- 18- واقد يوسف، النظام القانوني للدفع الالكتروني، مذكرة لنيل شهادة ماجستير، تخصص قانون تعاون الدولي، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2011.

ثالث/ المداخلات:

- 1- بلحارث ليندة ووالي نادية، (الحماية القانونية لوسائل الدفع الالكتروني)، بحث مقدم في الملتقى الوطني الثامن حول: آلية تفعيل وسائل الدفع الحديثة بين النظام المالي والمصرفي الجزائري، كلية الحقوق والعلوم السياسية، جامعة البويرة، المنعقد في يومي 13 و14 مارس 2017.

2- خبازي فاطمة الزهرة، (جرائم الدفع الالكتروني وسبل مكافحتها)، بحث مقدم في الملتقى الوطني بعنوان: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، جامعة الجبالي بونعامة، خميس مليانة، 2017.

3- يوسف مسعداوي، (البنوك الالكترونية)، بحث مقدم في ملتقى المنظومة المصرفية الجزائرية والتحويلات الاقتصادية، واقع وتحديات، جامعة البليدة، بدون سنة النشر.

رابعاً/ المقالات:

1- أحمد بن مسعود، (جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري)، مجلة الحقوق والعلوم الإنسانية، كلية الحقوق والعلوم السياسية، جامعة الجلفة، المجلد 10، العدد 1، 2017.

2- الزلمي بسام أحمد، (دور النقود الالكترونية في عمليات غسل الأموال)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد 1، 2010.

3- بحماوي الشريف وسليمان مصطفى، (خصوصية وسائل الوفاء الالكتروني ودورها في المعاملات التجارية)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية، أدرار، المجلد 1، العدد 7، 2017.

4- جويعد إياد خلف محمد، (المسؤولية الجزائية عن إفشاء السرية المصرفية)، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 23، 2010.

5- حديدان سفيان، (الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، المجلد 2، العدد 8، 2017.

6- درياد مليكة، (المساس بأنظمة المعالجة الآلية للمعطيات)، مجلة حوليات الجزائر، كلية الحقوق، جامعة الجزائر 1، الجزء 1، العدد 33، 2019.

7- زيدان محمد وحمو محمد، (أمن المعلومات المصرفية كمطلب للتسويق الالكتروني في البنوك الجزائرية)، مجلة رؤى اقتصادية، كلية الحقوق والعلوم السياسية، جامعة الشهيد محمد خيضر، بسكرة، العدد 8، 2015.

8- سعدي عبد الحليم، (الأرضية القانونية للاعتماد المستندي)، مجلة الفكر، جامعة قسنطينة 1، العدد 9، بدون سنة.

- 9- شايب محمد، (آليات الحماية من الغش في وسائل الدفع الالكترونية في الاقتصاد الفرنسي 2002-2016 - حالة البطاقة المصرفية-)، مجلة نماء للاقتصاد والتجارة، جامعة سطيف 1، الجزائر، العدد 2، 2017.
- 10- عاشور نصر الدين، (جريمة السرقة في ظل تعديلات العقوبات 2006)، مجلة المنتدى القانوني، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 5، بدون سنة النشر.
- 11- غزالي نزيهة، (الآليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري)، مجلة البحوث السياسية والإدارية، جامعة محمد لمين دباغين، سطيف 2، العدد 10، بدون سنة النشر.
- 12- كردي نبيلة، (الشيك الالكتروني)، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، العدد 13، 2017.
- 13- لعايب وليد، (تقييم تجربة نظام الدفع الالكتروني الجزائري في ظل ثورة التكنولوجيا المصرفية دراسة مقارنة مع تجربة نظام الدفع الالكتروني الأوروبي)، مجلة أبحاث ودراسات التنمية، المجلد 4، العدد 2، 2018.
- 14- محمود هند فالح وصون كل عزيز عبد الكريم، (المقاصة الالكترونية والمسؤولية المدنية التي تتجم عنها)، مجلة الرافدين للحقوق، جامعة الموصل، المجلد 18، العدد 23، 2018.
- 15- يوسف فتيحة وهداية بوعزة، (الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الالكتروني)، مجلة الدراسات والبحوث القانونية، جامعة وهران 2، العدد 4، المجلد 3، 2018.

خامسا/ النصوص القانونية الجزائرية:

أ- النصوص التشريعية:

- 1- الأمر رقم 66-155 المؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 48 مؤرخ في 10 جوان 1966، معدل ومتمم.
- 2- الأمر رقم 66-156 المؤرخ في 8 جوان 1966 متضمن قانون العقوبات الجزائري، جريدة رسمية عدد 49 مؤرخ في 11 جوان 1966، معدل ومتمم.

- 3- الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن قانون المدني الجزائري، جريدة رسمية عدد 78 الصادرة في 30 سبتمبر 1975، معدل ومتمم.
- 4- الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن قانون التجاري الجزائري، جريدة رسمية عدد 101 الصادرة في 19 ديسمبر 1975، معدل ومتمم.
- 5- الأمر رقم 03-06 المؤرخ في 19 جوان 2003 يتعلق بالعلامات، جريدة رسمية عدد 44 الصادرة في 23 جوان 2003.
- 6- الأمر رقم 03-11 مؤرخ في 26 أوت 2003 المتضمن قانون النقد والقرض، جريدة رسمية عدد 52 الصادرة في 27 أوت 2003، معدل ومتمم.
- 7- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات الجزائري، جريدة رسمية عدد 71 الصادرة في 20 نوفمبر 2004، معدل ومتمم.
- 8- القانون رقم 05-02 المؤرخ في 6 فيفري 2005، جريدة رسمية عدد 11 الصادرة في 9 فيفري 2005، معدل ومتمم لقانون العقوبات الجزائري.
- 9- القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، جريدة رسمية عدد 84 مؤرخ في 24 ديسمبر 2006، معدل ومتمم لقانون العقوبات الجزائري.
- 10- القانون رقم 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 مؤرخ في 16 أوت 2009.
- 11- الأمر رقم 11-02 المؤرخ في 23 فيفري 2011، جريدة رسمية عدد 12 مؤرخ في 23 فيفري 2011 معدل ومتمم لقانون الإجراءات الجزائية.
- 12- القانون رقم 15-04 المؤرخ في 1 فيفري 2015 المتضمن للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية عدد 6 الصادرة في 10 فيفري 2015.
- 13- القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، جريدة رسمية عدد 28 المؤرخ في 16 ماي 2018.

ب- النصوص التنظيمية والمراسيم:

- 1- النظام رقم 05-06 المؤرخ في 15 ديسمبر 2005 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى، جريدة رسمية عدد 26 الصادرة في

23 أبريل 2006.

- 2- النظام رقم 08-11 مؤرخ في 28 نوفمبر 2011 يتعلق بالرقابة الداخلية للبنوك والمؤسسات المالية، جريدة رسمية عدد 36 الصادرة في 29 أوت 2012.
- 3- النظام رقم 03-12 مؤرخ في 22 نوفمبر 2012 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، جريدة رسمية عدد 12 الصادرة في 27 فيفري 2013.
- 4- المرسوم التنفيذي رقم 16-142 مؤرخ في 5 ماي 2016 يحدد كفايات حفظ الوثيقة الموقعة الكترونياً، جريدة رسمية عدد 28 الصادرة في 28 ماي 2016.

سادساً/ النصوص القانونية الأجنبية:

أ- العربية:

- 1- ظهير شريف رقم 129.1.07 صادر في 19 من ذي القعدة 1428 (30 نوفمبر 2007) بتنفيذ القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.
- 2- القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، جريدة رسمية عدد 32 مكرر (ج) الصادرة في 14 أوت 2018.

ب- الفرنسية:

- 1) Recommandation N° 87/598/CEE de la commission européenne du 8 décembre 1987 portant sur un code européen de bonne conduite en matière de paiement électronique, JOL 365, 24 décembre 1987.
- 2) Recommandation 97/489/CE du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire, JOL 28, du 2 Août 1997.

سابعاً/ المواقع الإلكترونية:

- 1- الاحتيال الإلكتروني، التخلف التقني للقطاع المصرفي اللبناني يمنع تفاقم القرصنة،

عبد الرحمان عرابي، <http://www.alaraby.couk>

- 2- الخامس فاضلي، (الشيك الإلكتروني من الوجهة القانونية: خطوات استخدام

الشيك الإلكتروني)، 2017.

<http://juris.ma/ar/annuaire/fadili-el-khamis/publication.juin>

- 3- بوهدون يوسف، الجوانب القانونية لوسائل الوفاء الالكترونية،
<https://drive.google.com>.
- 4- جنحة النصب في قانون العقوبات الجزائري، المكتبة القانونية الجزائرية،
<https://law-dz.net/>.
- 5- حقوق ومسؤوليات العميل، البنك المركزي الأردني، <https://www.cbj.gov.jo>.
- 6- حنان مليكة، بحث قانوني هام عن الشيكات الالكترونية، 2016،
<https://www.mohamah.net/law>
- 7- زراد دنيا، (إبرام العقد الالكتروني)، [https://www.maroc doit.com](https://www.maroc.doit.com).
- 8- طرق الاحتيال الالكتروني، كتاب السطور، www.sotor.com.
- 9- عبد الله ليندة، تبييض الأموال عن طريق الاعتماد المستندي الالكتروني، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، جامعة محمد الصديق بن يحيى، جيجل، [www. jilrc. com](http://www.jilrc.com).
- 10- نوال بن عمارة، وسائل الدفع الالكتروني (الأفاق والتحديات)، كلية الحقوق والعلوم الاقتصادية، جامعة ورقلة، <https://dspace.univ-ouargla.dz>.

فهرس

الموضوعات

الشكر.....	١
الإهداء.....	ب
الملخص.....	ث
مقدمة.....	1
الفصل الأول: مخاطر الدفع الالكتروني على البنوك.....	4
المبحث الأول: آليات الدفع الالكتروني للبنوك.....	4
المطلب الأول: السندات الالكترونية.....	5
الفرع الأول: السندات التجارية الالكترونية.....	5
أولا/ الشيك الالكتروني:.....	5
ثانيا/ السفتجة الالكترونية:.....	7
ثالثا/ السند لأمر الالكتروني:.....	8
الفرع الثاني: البطاقات الالكترونية.....	9
أولا/ تعريف البطاقات الالكترونية:.....	9
ثانيا/ العلاقات التعاقدية الناشئة عن البطاقات الالكترونية:.....	11
ثالثا/ الطبيعة القانونية للبطاقات الالكترونية:.....	13
المطلب الثاني: عمليات الدفع الالكتروني.....	13
الفرع الأول: المقاصة الالكترونية.....	13
أولا/ تعريف المقاصة الالكترونية:.....	13
ثانيا/ إجراءات المقاصة الالكترونية:.....	14
ثالثا/ أنواع المقاصة الالكترونية:.....	15
الفرع الثاني: التحويل الالكتروني للأموال.....	16

أولا/ تعريف التحويل الالكتروني للأموال:	16
ثانيا/ إجراءات عملية التحويل الإلكتروني:	17
الفرع الثالث: الاعتماد المستندي الالكتروني.....	18
أولا/ تعريف الاعتماد المستندي الالكتروني	18
ثانيا/ إجراءات الاعتماد المستندي الالكتروني:	19
المبحث الثاني: الآثار المترتبة عن الاستخدام غير المشروع لوسائل الدفع الالكتروني	19
المطلب الأول: المخاطر الأمنية لوسائل الدفع الالكتروني	20
الفرع الأول: القصور الوظيفي لوسيلة الدفع الالكتروني	20
أولا/ القصور الوظيفي لوجود عيب في أداة الدفع الالكتروني:	20
ثانيا/ القصور الوظيفي لوجود تقصير في صيانة وسيلة الدفع الالكتروني:	21
الفرع الثاني: جرائم البطاقات الإلكترونية.....	22
أولا/ الاستعمال غير المشروع للبطاقات الالكترونية من قبل الحامل:	22
ثانيا/ الإيستخدم غير المشروع للبطاقة الإلكترونية من قبل الغير	24
المطلب الثاني: توسع دائرة الجرائم المرتكبة باستخدام وسائل الدفع الالكتروني.....	26
الفرع الأول: القرصنة وجريمة انتهاك السرية المعلوماتية	26
أولا/ جريمة القرصنة المعلوماتية:	27
ثانيا/ جريمة انتهاك السرية المعلوماتية:	30
الفرع الثاني: استخدام وسائل الدفع في جريمة تبييض الأموال والتهرب الضريبي	31
أولا/ جريمة تبييض الأموال باستعمال وسائل الدفع الالكتروني:	32
ثانيا/ جريمة التهرب الضريبي باستعمال وسائل الدفع الالكتروني	30
الفصل الثاني: طرق مكافحة مخاطر الدفع الالكتروني	36

المبحث الأول: الحماية التقنية لمكافحة مخاطر الدفع الالكتروني	36
المطلب الأول: الآليات التقنية المعتمدة لمكافحة مخاطر الدفع الالكتروني	36
الفرع الأول: الكتابة الالكترونية	37
الفرع الثاني: التوقيع الإلكتروني	39
الفرع الثالث: السجل الالكتروني	42
المطلب الثاني: تأمين العمليات الالكترونية من قبل البنوك	43
الفرع الأول: إجراءات تأمين العمليات الالكترونية من قبل البنوك	44
أولا/ أمن المعلومات	44
ثانيا/ تقنيات أمن المراسلات والمواقع الالكترونية:	46
الفرع الثاني: كفاءات تأمين عمليات الدفع الالكتروني	48
المبحث الثاني: الحماية القانونية لمكافحة مخاطر الدفع الالكتروني	51
المطلب الأول: حماية البنوك من مخاطر الدفع الالكتروني في ظل التشريع الجزائري.	51
الفرع الأول: الحماية المكرسة في التشريعات العامة	52
أولا/ الحماية المقررة في قانون العقوبات:	52
ثانيا/ الحماية المقررة في قانون الإجراءات الجزائية:	56
ثالثا/ الحماية المقررة في القانون التجاري:	56
الفرع الثاني: الحماية المكرسة للدفع الالكتروني في التشريعات الخاصة	57
أولا/ الحماية القانونية للدفع الالكتروني من خلال قانون الملكية الفكرية الجزائري:	58
ثانيا/ الحماية القانونية للدفع الالكتروني من خلال القانون 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين:	59

ثالثا/ الحماية القانونية للدفع الالكتروني من خلال قانون التجارة الالكترونية الجزائري:.....	60
رابعا/ الحماية القانونية للدفع الالكتروني من خلال قانون النقد والقرض:	60
خامسا/ الحماية القانونية للدفع الالكتروني من خلال النظام 12-03 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافتهما:	61
سادسا/ الحماية القانونية للدفع الالكتروني من خلال القانون 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافتهما:	62
المطلب الثاني: الحماية القانونية الدولية لمكافحة مخاطر الدفع الالكتروني.....	63
الفرع الأول: الجهود الدولية لمكافحة مخاطر الدفع الالكتروني.....	63
أولا/ الحماية القانونية في ظل الاتحاد الأوروبي:	64
ثانيا/ جهود المنظمة الدولية للأمم المتحدة:	64
ثالثا/ الاتحاد الدولي للاتصالات لحماية الفضاء الالكتروني:	65
رابعا/ المنظمة العالمية للملكية الفكرية:	65
خامسا/ الحماية القانونية في ظل المنظمة العالمية للتجارة:	66
سادسا/ الحماية القانونية من خلال المنظمة الدولية لضباط الجرائم المالية.....	66
سابعا/ معاهدة بودابست بشأن جرائم الحسابات في حماية وسائل الدفع الالكتروني: ..	66
الفرع الثاني: موقف التشريعات المقارنة بشأن حماية الدفع الالكتروني.....	67
أولا/ موقف بعض التشريعات الغربية بشأن حماية الدفع الالكتروني.....	67
ثانيا/ موقف بعض التشريعات العربية بشأن حماية الدفع الالكتروني:	69
الخاتمة:.....	Error! Bookmark not defined.
قائمة المصادر والمراجع	75
فهرس الموضوعات.....	82