جامعة أكلي محند أولحاج – البويرة

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

الجرائم الواقعة على بطاقات الدفع الإلكتروني

مذكرة لنيل شهادة المـاستر في الحقوق

تخصص: قانون أعمال

إعداد الطالبتين:

– نايلي ادواودة رزيقة

– مدانـــــي شهرة

إشراف الأستاذة:

– د / بركات كريمة

لجنة المناقشة

الأستاذ(ة).....رئيسا

الأستاذ(ة):د. بركات كريمة.....مشرفا ومقررا

الأستاذ(ة):.....ممتحنا

السنة الجامعية: 2021/2020

كلمة شكر

أحمد الله عــز وجل أولا وأخرا على نعمة العقل، والصحة، وقوة الإرادة، وأن وفقني إلى إنجاز هذا العمل

وأتوجه بخالص الشــكر إلى الدكتورة بركات كريمة، لتفضله بالإشراف علي هذه المذكــرة، وعلى كل المجهودات التي بذلتها، من أجل إنجاز هذا العمل

كما لا يفوتني أن أتقدم بالشكــر الجزيــل للجنة المناقشة الموقرة لتحملها عبء قراءة هذه المذكــرة ومناقشتها.

إن أي بحث لا يخلو من النقائص وإن الكمــال لله عــز وجــل، وأسأل الله العلــي العظيــم أن يوفقــني، وأن ينتفع ببحثي هذا كل قارئ له

إهـــــداء

قال تعالى: "وأخفض لهما جناح الذل من الرحمة وقل رب ارحمهما كما ربياني صغيرا"

قد أنسى التعب، قد تغفل ذاكرتي في لحظة عما عانيت.....

ولكن لن أنسى شقائهم في سبيل أن أكون دائما الأفضل.....

أهدي ثمرة جهدي إلى:

من حملتني وهنا على وهنا والتي وضعت الجنة تحت قداميها.....

أمي النور الذي أضاء ويضيء دروب حياتي.....

أرجو من المولى عز وجل أن يمدها الصحة والعافية، ويطيل عمرها.....

إلى من جعل تعبه وجهده دربا أسير عليه من علمني أن الحياة أولها كفاح واخرها نجاح

إلى الذي لا يمكن للكلمات أن توفى حقه ولا للأقلام أن تحصي فضائله والدي العزيز حفظه الله لي.....

إلى من أشد بهم أزري وأقوي بهم عضدي إخوتي وأخواتي وعمتي حفظهم الله وأطال في عمرهم.....

إلى أسمى معاني الصداقة والمحبة G ,S,4" وإلى كل زميلاتي وزملائي في الدراسة والحياة

، إلى كل من سعتهم ذاكرتي ولم تسعهم مذكرتي

شهـــــرة

إهـــــــــداء

إلهي لا يطيب الليل إلا بشكرك..... ولا يطيب النهار إلا بطاعتك

ولا تطيب اللحظات إلا بذكرك.....ولا تطيب اللحظات إلا بعفوك

إلى من بلغ الرسالة وأدى الأمانة

إلى المعلم الأول، صاحب العلم الحق، سيدنا محمد عليه الصلاة والسلام

لأن حياتي لا تطيب إلا بك

إلى رمز الحب وبلسم الشفاء.....إلى والدي أطال الله في عمره

إلى بسمة الحياة وسر الوجود.....إلى والدتي حفظها الله

إلى من أرى التفاؤل بأعينهم.....والضحكة في وجوههم

إخوتي وأخواتي

إلى من تميزو بالوفاء.....إلى أساتذتي وزملائي وزميلاتي

إليكم جميعا أهدي جهدي المتواضع

-رزيقـــة-

قائمة المختصرات

ص : صفحة

ص ص: من الصفحة إلى الصفحة

ج ر ج ج : جريدة رسمية للجمهورية الجزائري

د ذ س ن : دون ذكر سنة النشر.

مقدمة

في ظل التطور التكنولوجي الحالي، يعيش العالم موجه من الابتكارات والاختراعات اللامتناهية، حيث شملت هذه التغيرات على وجه الخصوص المجال المصرفي، الذي شهد تحولات وتغييرات سريعة وهامة على الصعيد التكنولوجي، فأصبحنا نعيش في زمن ثورة تكنولوجيا المعلومات والتي نتج عنها ظهور شبكات اتصال عالمية، وفكرة التجارة الالكترونية والتي بدورها ترتب عنها ظهور ما يعرف بالنقود الالكترونية والصرافة الالكترونية التي يمكن عن طريقها تحويل مبالغ مالية لحسابات أخرى ودفع فواتير لجهات أخرى خارج البنوك عن طريق الوسائل الالكترونية والمتمثلة في بطاقات الدفع الالكتروني.

ويتم استخدام بطاقات الدفع الإلكتروني كوسيلة للدفع، أو أداة للإبراء، ووسيط للتبادل، فقد دخلت حيز التداول في الفترة ليست بالبعيدة والتي لاقت رواجا وقبولا في الدول التي تسمح باستخدامها، لاسيما أن هذه البطاقات يمكنها القيام بغالبية الوظائف التي تقوم بها النقود العادية. وقد ظهرت لأول مرة مطلع القرن العشرين بالولايات المتحدة الأمريكية، كما أنها مرت بمراحل تطور عديدة حيث ظلت مستعملة محليا إلى غاية السبعينات أين اتفقت بعض البنوك الأمريكية على إصدار بطاقة جديدة سميت "بطاقة فيزا" وعام 1977 سمحت لمختلف البنوك في أنحاء العالم بالانضمام إلى نظام "بطاقة فيزا"ومنه أصبحت بطاقة الدفع الإلكتروني أكثر انتشارا في جميع دول العالم بداية من الدول الأوروبية وصولا إلى الدول العربية.

الجزائر لم تعرف بطاقة الدفع الالكتروني، إلا في السنوات الأخيرة حيث كان أول ظهور لها عام 1994 حين تم فتح بنوك خاصة ولكنها لم تلقى رواجا كبيرا إلى غاية سنة 2005، ونجد أن المشرع الجزائري لم يسن القواعد القانونية التي تواكب التطور التقني المستمر بالنسبة لإتمام الأعمال التجارية إلكترونيا إلا مؤخرا، فحاول تكريس جهوده لإثراء المنظومة التشريعية بخصوص مجال التعامل التجاري الالكتروني وتحديث أنظمة الدفع المتاحة في ظله، بحيث أن

المشرع اعترف ضمنيا بتقنية الدفع الالكتروني، ولكن من دون أن يقدم تعريفا لها وتجلى ذلك من خلال الأمر 03-11 المتعلق بالنقد والقرض[1].

كما استعمل المشرع الجزائري مصطلح وسائل الدفع الالكتروني في المادة 3 من الأمر 05-06 المتعلق بمكافحة التهريب[2]، حيث اعتبرها المشرع من التدابير والإجراءات الوقائية لمكافحة التهريب، ثم أضاف المشرع بموجب القانون 05-02 المعدل والمتمم لقانون التجاري فصلا ثالثا بعنوان بطاقات الدفع والسحب [3].

في حين أن فقهاء القانون ورغم اختلاف تعريفاتهم لبطاقات الدفع إلا أنها تصب في مجرى واحد مفاده أنها بطاقة صادرة من الجهة المصدرة لمصلحة شخص معين يحصل بموجبها على احتياجاته من سلع وخدمات مع التزامه بتسديد قيمة مشترياته في مدة محددة الآجال.

وقد ترتب على صدور بطاقة الدفع الإلكتروني،شأها في ذلك شأن أي وسيلة تطور جديدة، عدة أثار إيجابية وأخرى سلبية، ومن الآثار السلبية هو الاعتداء عليها بالقيام بتصرفات غير مشروعة، مثل السرقة والتزوير والاحتيال، وهو ما انعكس سلبا على مصداقية هذه البطاقة والجهات المصدرة لها والأطراف المتعاملين بها.

وعليه فنظام الدفع الالكتروني يحتاج إلى وسائل حماية فنية وأخرى قانونية، تعزز من وجود بيئة آمنة في عالم التجارة الالكترونية، إضافة إلى ضرورة تطوير التشريعات على الصعيد الوطني بما يتلاءم وخصوصية هذا النوع من الجرائم مع تكثيف جهود التعاون على الصعيد الدولي نظرا لطبيعة هذه الجرائم العابرة للقارات.

---

(1) أمر رقم 03-01 مؤرخ في جمادى الثانية 1424الموافق ل 26 أوت 203 المتعلق بالنقد والقرض، ج. ر العدد 52 الصادرة في 27 أوت 2003 المعدل والمتمم.

(2) أمر رقم 05-06 مؤرخ في 18 رجب 1426 الموافق ل 23 أوت 2005 المتعلق بمكافحة التهريب المعدل والمتمم ج.ر العدد 59 ، الصادرة في 24 أوت 2005.

(3) قانون رقم 05 -02 مؤرخ في 06 فبراير 2005 المعدل والمتمم لأمر 75-59 المتضمن القانون التجاري، ج.ر العدد11، الصادرة في 07 فبراير 2005 .

أهمية الموضوع:

تبرز أهمية الموضوع محل الدراسة في دور بطاقات الدف الإلكتروني في مسايرة التطور المصرفي والتكنولوجي، وإن هذا الموضوع يتسم بالحداثة، حيث يسلط الضوء على بعض من الجرائم العصرية في مجال المعاملات الالكترونية والتي قد تكون خطيرة على مصالح المجتمع والاقتصاد القومي، مما يستدعي ضرورة التصدي العلمي لها بما يتناسب مع تقنياتها.

أسباب اختيار الموضوع:

- حداثة الموضوع والرغبة الملحة في دراسته والتعمق فيه.
- إمكانية توجه الجزائر إلى تحديث أنظمتها القانونية والمصرفية تماشيا مع ما هو موجود في العالم المتطور.
- الحث على وضع قوانين تحدد عقوبات للاستخدام الغير شرعي لهذه البطاقات وحمايتها جنائيا.
- جهل المتعاملين بها حول حقيقة خطورتها في التعامل.

إشكالية موضوع البحث:

- فيما تتمثل الاعتداءات التي يمكن أن تقع على بطاقات الدفع الالكتروني وما هي آليات الحماية الجنائية المقررة له؟

أهداف موضوع البحث:

- يهدف هذا البحث إلى الإلمام بجميع الجرائم الواقعة على بطاقات الدفع الالكتروني.
- التعرف على طرق حماية البطاقات الالكترونية من الاستخدام الغير المشروع لها.
- البحث عن الآليات الفعالة والمبتكرة لمكافحة الجرائم الواقعة على بطاقات الدفع الالكتروني.
- معرفة ما مدى اهتمام المشرع الجزائري بهذه الوسيلة عن طريق تدخله في تنظيمها وحمايتها وإنشاء نصوص قانونية تحارب هذه الجرائم.

الصعوبات:

- نقص الكتب والمراجع التي تتناول موضوع الجرائم الواقعة على البطاقات.
- قلة الكتابات في هذا المجال نظرا لحداثة الموضوع.
- ضيق الوقت.
- انتشار فيروس كورونا الذي أعاق عملية البحث والتنقل لحصول على المعلومات والمراجع لهذا الموضوع.

المنهج المتبع:

اعتمدنا في دراستنا لهذا الموضوع على المنهج التاريخي الذي يبين التطور التاريخي للدفع الإلكتروني، بالإضافة إلى المنهج التحليلي وذلك خلال تحليلنا لنصوص القانونية المتعلقة بالجرائم الواقعة على بطاقات الدفع الالكتروني، إلى جانب المنهج التحليلي والتاريخي اعتمدنا على المنهج المقارن لمقارنة التشريعات الوطنية والدولية المتعلقة بحماية بطاقة الدفع الالكتروني

هيكل البحث:

للوصول إلى حل الإشكالية المطروحة ارتأينا تقسيم هاته الدراسة إلى فصلين على النحو التالي:

تناولنا في (الفصل الأول) طرق الاستخدام الغير مشروع بطاقات الدفع الالكتروني والذي قسمناه إلى مبحثين، حيث تضمن المبحث الأول الاستخدام الغير مشروع لبطاقة الدفع الالكتروني من قبل أطرافها، أما المبحث الثاني فتناولنا الاستخدام الغير مشروع لبطاقة الدفع الالكتروني من قبل الغير، في حين خصصنا (الفصل الثاني) إلى الحماية القانونية لبطاقات الدفع الالكتروني من الاستخدام الغير مشروع والذي بدوره قسمناه إلى مبحثين فتناولنا في المبحث الأول الإجراءات الوقائية والأمنية المتبعة لحماية بطاقات الدفع الالكتروني أما المبحث الثاني فجاء بعنوان قواعد الحماية القانونية الوطنية والدولية لبطاقات الدفع الالكتروني.

الفصل الأول
طرق الاستخدام غير المشروع لبطاقات الدفع لإلكتروني

إن استخدام وسائل الدفع الإلكتروني كوسيلة وفاء مستحدثة ذات تقنية تكنولوجية عالية بل وفائقة التطور، أدى إلى إقبال كبير من طرف المتعاملين بها في تسوية معاملاتهم المالية نظرا لسهولة التعامل بها، وكذا الحماية من مخاطر حمل النقود وبطاقات الدفع الإلكتروني حالها حال أي اختراع جديد قد يتعرض إلى اعتداءات وتصرفات غير مشروعة تفقدها ثقتها الائتمانية، فهذه الاعتداءات متعددة ومتطورة من حيث النوع يصعب حصرها فهي ذات أشكال وأساليب متنوعة تهدد مستخدمي وسائل الدفع الإلكتروني. فيمكن أن تكون هذه الاعتداءات من طرف الأشخاص المتدخلين في الصفقات أو من الغير، وتكون حتى من قبل التاجر والمصدر، وكما قد تنجم هذه المخاطر عن طبيعة هذه الوسائل التي يمكن أن تكون عبارة عن خدمات مالية تعتمد التكنولوجية الحديثة في أداء مهامها، والتي تكون في كثير الأحيان في بيئة مفتوحة كالانترنت وبالإضافة إلى المخاطر الأمنية التي يمكن أن تحدث بهدف تحقيق أهداف غير مشروعة هناك أيضا مخاطر قانونية ومخاطر متعلقة بأنظمة الدفع نفسها.

لذلك سنحاول في هذا الفصل تسليط الضوء على هذه الاعتداءات من خلال تحديدها، حيث نقسم هذا الفصل إلى مبحثين نتناول في المبحث الأول الاستخدامات الغير مشروعة من قبل حامل البطاقة وكذلك التاجر والمصدر لها، نتناول في المبحث الثاني الاستخدام الغير مشروع للبطاقة من قبل الغير.

المبحث الأول

الاستخدام غير المشروع لبطاقات الدفع الإلكتروني من قبل أطرافها

في أغلب الحالات يتم الاستخدام غير المشروع لبطاقات الدفع الإلكتروني من طرف حاملها الشرعي، كما قد يتم من طرف التاجر أو المصدر، أو بالاتفاق بين أكثر من طرف.

وعليه سنقوم بتقسيم هذا المبحث إلى مطلبين، فنتطرق في المطلب الأول إلى إساءة استخدام بطاقة الدفع الإلكتروني من قبل حاملها، وفي المطلب الثاني إلى إساءة استخدام بطاقة الدفع الإلكتروني من قبل التاجر والمصدر.

المطلب الأول

إساءة استخدام بطاقة الدفع الإلكتروني من قبل حاملها

يقصد بحامل البطاقة (card holder): الشخص الذي صدرت البطاقة له، سواء كانت البطاقة رئيسية أم تابعة، ويكون له كل الحق في التصرف في بطاقته ومع ذلك يمكن أن يستخدمها خارج إطارها المشروع والمتفق عليه في العقد المبرم بينه وبين الجهة المصدرة للبطاقة[1]، حيث يمكن أن يكون هذا الاستخدام غير مشروع خلال فترة صلاحيتها وهذا ما سنتناوله من خلال (الفرع الأول)، أو يكون خارج فترة صلاحيتها سواء بانتهاء تلك الفترة أو بعد إلغاء تفعيل البطاقة من طرف الجهة المصدرة لها وهذا ما سنفصل فيه من خلال (الفرع الثاني)، كما سنتطرق للاستخدام المقنع لها من خلال (الفرع الثالث).

الفرع الأول:الاستخدام غير المشروع للبطاقة خلال فترة صلاحيتها

من خلال هذا الفرع سنحاول الوقوف أمام المقصود بحصول الحامل على البطاقة عن طريق النصب وذلك باستعمال بيانات مزورة (أولا)، وكذلك إساءة استخدامها يتجاوز السقف المسموح به سواء في عمليات السحب أو الوفاء (ثانيا).

(1) أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، الطبعة الأولى، دار الميسرة للنشر والتوزيع والطباعة، عمان، 2010، ص128.

أولا: الحصول على بطاقة الدفع الإلكتروني بطريقة غير شرعية

إن فتح الحساب البنكي يعني إقامة علاقة مالية بكل ما ينتج عنها من حقوق والتزامات بين العميل والبنك، لذلك يجب أن تتوفر بعض الشروط القانونية والتنظيمية لهذه العملية وهي تلك التي حددتها النصوص والتنظيمات الجزائرية[1].

ومن أجل حصول المشروع على بطاقة الدفع الإلكتروني، يقوم العميل باستيفاء البيانات الخاصة بطلب البطاقة من الجهة المصدرة لها، وذلك عن طريق ملء نموذج يشتمل عدة بيانات ضرورية، إذ يتعين على العميل أن يفصح عن اسمه، عنوانه، حالته المهنية والمادية، ويقوم بالتوقيع، ويجب أن تكون هاته البيانات صحيحة ومن ثمة تعود السلطة التقديرية إلى الجهة المصدرة للبطاقة بإصدار البطاقة من عدم إصدارها[2].

وقد يحدث وأن يتقدمطالب البطاقة بيانات كاذبة وأسماء منتحلة وعناوين وهمية تعرض البنك لخسائر مادية نتيجة استخدام البطاقة في شراء السلع والخدمات بمبالغ كثيرة، حيث لن تتمكن الجهة المصدرة العثور على صاحب البطاقة نتيجة بياناته الوهمية[3]، ويكيف فعله الإجرامي على أنه جريمة نصب استنادا لنص المادة 372 من قانون العقوبات الجزائري[4].

1-تعريف جريمة النصب

نظم هذه الجريمة قانون العقوبات الجزائري في المادة 372 التي جاء فيها: "**كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها شرع في ذلك وكان ذلك**

(1) سليمان ناصر، التقنيات البنكية وعمليات الائتمان، ديوان المطبوعات الجامعية، الجزائر، 2012، ص15.

(2) علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكترونية (دراسة مقارنة)، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2011، ص280.

(3) بن تركي ليلى، الحماية الجنائية لبطاقات الائتمان الممغنطة، رسالة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، 2017، ص148.

(4) انظر المادة 372 من قانون رقم 04-15 المؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر ج ج ، العدد 71 ، الصادرة بتاريخ 10 نوفمبر 2004.

بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار".

1- أركان جريمة النصب:

منخلال النص المذكور أعلاه نجد أن جريمة النصب تقوم على ركنين هما:

أ- الركن المادي

يتحقق الركن المادي لجريمة النصب في الحصول على بطاقة دفع غير مشروعة باتخاذ الحامل اسما كاذبا أو صفة غير صحيحة، بانتحال شخصية لغيره أو اسم الغير مستعملا بذلك طرق التدليس والاحتيال، بحيث ينخدع الطرف المتعامل معه والذي يتم إقناعه بأوراق مزورة أو أعمال مادية أو مظاهر خارجية وليس مجرد إدعاءات وأقوال، بغية الاستيلاء على شيء ملموس مادي منقول ذو قيمة مالية والمتمثل في وسيلة الدفع الإلكتروني[1].

ب- الركن المعنوي

يتطلب الركن المعنوي لجريمة النصب توافر القصد الجنائي العام المتمثل في إرادة المتهم حامل البطاقة في تحقيق الجريمة بأركانها الكاملة وهو عالم بذلك، وتوافر القصد الجنائي الخاص المتمثل في نيته في الاستيلاء على مال الغير باستعمال بطاقة إلكترونية مزورة[2].

ثانيا: تجاوز الحامل لسقف البطاقة

يرتب العقد المبرم بين الحامل والمصدر التزاما على البنك بإصدار بطاقات دفع لتسهيل عمليات صرف المبالغ المالية في أي وقت بواسطة أجهزة الصراف الآلي، والتزاما على الحامل بعدم تجاوز السقف المحدد في البطاقة، وفي حال عدم تطبيق الحامل لهذا الالتزام يعد

(1) أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة إحدى والعشرون، دار هومة، الجزائر، 2019، ص ص 314، 322.

(2) نفس المرجع السابق، ص ص 322، 323.

مستخدما البطاقة في إطار غير مشروع، ويكون هذا التجاوز في صورتين إما تجاوز الحامل لرصيده في السحب أو تجاوزه لرصيده في الوفاء بثمن السلع والخدمات[1].

1- تجاوز الحامل لرصيده في السحب:

يحدث هذا التجاوز عند قيام حامل البطاقة باستعمالها في تنفيذ عمليات سحب النقود من الموزعات الآلية للأوراق أو الشبابيك الآلية في البنوك متجاوزا رصيده المزود به في حسابه البنكي أو الحد الأقصى المصرح له به[2].

اختلف كل من الفقه والقضاء حول التكييف القانوني لجريمة تجاوز الحامل لرصيده في السحب وذلك على النحو التالي:

أ- **الاتجاه الأول:** مساءلة حامل البطاقة جزائيا إما عن جريمة "سرقة" أو "احتيال" أو "إساءة ائتمان".

اتجه البعض من الفقهاء إلى أن التكييف الصحيح لهاته الجريمة هو جريمة خيانة أمانة، لأن البنك أصدر لجاني البطاقة على سبيل الائتمان إلا أن هذا الأخير استعملها بطريقة غير مشروعة للحصول على أموال غيره بغير وجه حق وقد نص المشرع على جريمة خيانة الأمانة في نص المادة 376 من قانون العقوبات[3].

في حين يرى البعض الآخر أنها جريمة احتيال لأن الجاني يعلم أن رصيده غير كاف ورغم ذلك يقوم بإيهام البنك عند القيام بإدخاله للبطاقة في جهاز الصراف الآلي بأن بحوزته مبلغ من المال في رصيده، وقد نص عليه المشرع الجزائري من خلال المادة 372 من قانون العقوبات[4].

لكن هذا الاتجاه تم انتقاده على أساس أن البطاقة استعملت من طرف حاملها الشرعي حيث أن الحامل لم يستعمل أسماء أو صفات كاذبة وهذا يبعد كون أن صاحب البطاقة قد

(1) أمجد حمدان الجهني، المرجع السابق، ص ص 129، 130.

(2) بن تركي ليلى، المرجع السابق، ص77.

(3) انظر المادة 376 من قانون العقوبات الجزائري.

(4) انظر المادة 372 نفس المرجع السابق.

تجاوز المبلغ المتفق عليه ودون علم الجهة المصدرة أو رضاها، إلا أن هذا الرأي لم يسلم من الانتقاد أيضاحيث أن البنك قام بكل طواعية بتسليم الأموال للجاني[1].

ب-الاتجاه الثاني: عدم انطواء هذه الواقعة على جريمة احتيال أو أي جريمة أخرى في ضوء نصوص قانون العقوبات:

على عكس الاتجاه الأول يرى أصحاب هذا الاتجاه أن هذه الواقعة لا تكيف جريمة من الجرائم المدروسة (احتيال، سرقة أو خيانة أمانة) في ضوء نصوص قانون العقوبات وإنما مجرد إخلال بالتزام تعاقدي بين العميل والبنك أو استعمال تعسفي صادر عن حامل البطاقة، وبالتالي تتم مساءلة الجاني في الشق المدني دون الجزائي[2].

2- تجاوز الحامل لرصيده في الوفاء

تسمح بطاقة الدفع الإلكتروني لصاحبها الحصول على السلع والخدمات من التاجر المعتمد دون دفع قيمتها نقدا، إذ يكفي تقديم البطاقة لتحل الجهة المصدرة محله في الوفاء، لكن يمكن للحامل أن يسيء استخدام بطاقة الدفع إذا ما علم أن رصيده في البنك غير كاف لإجراء هذه العملية ورغم ذلك يقوم باستخدامها للوفاء بقيمة السلع والخدمات للتاجر[3].

اختلفت آراء الفقهاء حول التكييف القانوني لجريمةتجاوز الحامل لرصيده في الوفاء، فاتجه الرأي الأول لاعتبار أن الحامل الذي يوفي بقيمة السلع والخدمات التي يقتنيها بالرغم من عدم وجود رصيد كافي في البطاقة، يعتبر مرتكب لجريمة النصب ويخضع للمساءلة الجزائية، أما الرأي الثاني فقط أسقط المسؤولية الجزائية عن الحامل لعدم انطواء الفعل على أي جريمة

(1) خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة مكملة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2018، ص9.

(2) ميهوبي فطيمة، جرائم بطاقات الدفع الإلكتروني، مذكرة لنيل شهادة الماستر في القانون الإداري، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة،2016، ص33.

(3) مرباح صليحة، الحماية القانونية المدنية والجزائية لبطاقة الائتمان، رسالة لنيل شهادة دكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2019، ص 190.

واعتبر مجرد إخلال بالتزام الحامل اتجاه البنك المصدر، وفي هذه الحالة تترتب عليه المسؤولية العقدية لتعويض الضرر[1].

ثالثا: استخدام الحامل البطاقة في عمليات غسل الأموال

لقد أثار استخدام بطاقة الدفع الإلكتروني كبديل للتعامل بالنقود الورقية العديد من المشكلات ومنها غسل الأموال، فقد أصبح أصحاب الدخول غير المشروعة يلجؤون إلى استعمالها لإضفاء صفة المشروعية على أموالهم، وبذلك تكون الوسيلة المتمثلة في بطاقة الدفع الإلكتروني والمستخدمة من قبل حاملها الشرعي صحيحة إلا أن الغاية التي استخدمت من أجلها غير مشروعة.

ويتم اللجوء لهذه الوسيلة نظرا إلى أن هذا النوع من التعامل المالي لا يكون من المستطاع تعقب أثره، فضلا على أن التعامل بهذه البطاقات يتم مباشرة بين شخصين ولا يقتضي تدخل من المؤسسة المالية كما أن هذه التعاملات تتم بسهولة وبسرعة إذ تكفل تحويلا فوريا للمال من وإلى أي مكان في العالم، ويكون المتعامل فيها مجهول الشخصية ودون حواجز أو قيود قانونية[2].

1-طرق استخدام الحامل للبطاقة في عمليات غسل الأموال:

يوجد طريقتين هما:

أ- غسيل الأموال بواسطة استخدام البطاقة في أجهزة الصراف الآلي:

حيث يقوم العميل بتقديم طلبات متتالية للبنك من أجل إصدار بطاقات الوفاء له ولأفراد عائلته ولموظفيه، بضمان ودائع الشركة النقدية أو العينية، ويتم تحويل الأموال التي تصل من الخارج باستخدام هذه البطاقات عن طريق أجهزة الصراف الآلي، ويتم سحبها قبل أن تستقر، ثم يتم تجميعها وتحويلها بمبالغ كبيرة إلى الخارج. ويقوم العميل بصرف المبلغ عن طريق البطاقة من أجهزة الصراف الآلي باستخدام رقمه السري ثم يقوم الفرع الذي صرف منه بتحويل المال

(1) خولة بوقديرة، المرجع السابق، ص10.

(2) أمجد حمدان الجهني، المرجع السابق، ص134.

إليه من الفرع مصدر البطاقة الذي يقوم بدوره بالتحويل تلقائيا، وخصم القيمة من حساب عملية وبهذه الطريقة يكون قد تهرب من القيود المعروضة على التحويلات وسهلت عليه عملية تهريب الأموال المشبوهة[1].

ب- غسيل الأموال بواسطة الوفاء بالبطاقة:

وتتم هذه العملية عبر ثلاث مراحل:

- **المرحلة الأولى: الإيداع**

حيث يتم توظيف الأموال المنهوبة الناتجة عن جريمة أو عمل غير مشروع عن طريق إيداعها في أحد البنوك سواء المحلية أو الخارجية، من أجل إدخالها إلى النظام المالي والحصول بموجبها على بطاقات دفع إلكترونية سقف يعادل الرصيد المودع[2].

- **المرحلة الثانية: التغطية**

تقوم هذه المرحلة على تضليل الجهات الرقابية على المصدر غير المشروع للأموال المودعة عن طريق سلسلة متتابعة من العمليات المصرفية والتحويلات سواء الداخلية أو الخارجية باستخدام وسيلة الدفع الإلكتروني، التي تمكنه من إيداع أمواله الغير مشروعة في الدورة المالية وإضفاء صفة المشروعية[3].

- **المرحلة الثالثة: الدمج:**

من خلال هذه المرحلة يتم دمج الأموال والمتحصلات ذات المصادر الإجرامية الغير مشروعة في النظام المصرفي المشروع، وبالتالي خلط تلك الأموال المشبوهة بالأموال المشروعة حتى تبدو وكأنها آتية من أنشطة عادية[4].

---

(1) وسام فيصل محمود الشواورة، الاستخدام غير المشروع لبطاقات الوفاء، الطبعة الأولى، دار وائل للنشر، الأردن، 2013، ص ص 80،81.

(2) أمجد حمدان الجهني، المرجع السابق، ص136.

(3) يزيد بوحليط ، السياسة الجنائية في مجال تبييض الأموال في الجزائر، دار الجامعة الجديدة، 2014،ص66.

(4) أحمد سيفر، جرائم غسل الأموال وتمويل الإرهاب في التشريعات العربية، المؤسسة الحديثة للكتاب طرابلس، لبنان، 2006، ص36.

2-أركان جريمة غسل الأموال:

عالج المشرع الجزائري جريمة تبييض الأموال في المادة 389 مكرر من قانون العقوبات الجزائري ونص على العقوبة المقررة لها في نصوص المواد من 389 مكرر1 إلى المادة 389 مكرر7[1].

أ- الركن المادي:

يتمثل الركن المادي لجريمة تبييض الأموال في كل فعل يساهم في إخفاء أو تمويه مصدر الأموال غير المشروعة سواء تعلق الأمر بتحويل الأموال أو إخفاء طبيعتهم، أو حيازة واستخدام هذه الأموال، ويكون الغرض من هذه الأفعال إضفاء طابع الشرعية عليهم، بحيث تشمل هذه الأموال محل الجريمة كافة العائدات الناتجة عن الجريمة الأصلية غير الشرعية مثل جريمة التهريب، المخدرات، الاتجار بالأسلحة بغض النظر عن نوع هذه العائدات أو أيا كانت طبيعتها[2].

ب- الركن المعنوي:

جريمة تبييض الأموال هي جريمة قصدية تتوفر فيها عناصر العلم والإرادة، إذ يفترض علم الجاني بالمصدر غير المشروع لأموال غير المشروعة، كما تنصرف إرادة الجاني إلى ارتكابها بإرادته الحرة رغم أنه يعلم بأنه يمارس نشاطا إجراميا[3].

الفرع الثاني: الاستخدام غير المشروع للبطاقة خارج فترة صلاحيتها

إن أهم الالتزامات التي تترتب نتيجة العقد المبرم بين العميل حامل البطاقة والبنك المصدر لها، هو أن يتم استخدامها خلال مدة صلاحيتها، والتي تكون غالبا مدة سنة واحدة قابلة للتجديد، وإذا ما انتهت هذه المدة فإن على الحامل أن يقوم بردها إلى الجهة التي أصدرتها، وعليه فإن استمرار الحامل في استعمالها على الرغم من انتهاء المدة المحددة لها

(1) انظر المادة 389 مكرر إلى 389 مكرر 7 من قانون لعقوبات الجزائري.

(2) خلوفي خدوجة "أركان جريمة تبييض الأموال في التشريع الجزائري"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد الثاني، العدد8، المسيلة، ديسمبر 2017، ص، ص 602،607.

(3) مرباح صليحة، المرجع السابق، ص 190.

سوف يعرضه للمساءلة الجنائية، كما أن استخدامها في إطار غير مشروع قد يدفع الجهة المصدرة إلى إلغائها أو سحبها من الحامل رغم عدم نفاذ مدتها[1].

أولا: استخدام الحامل للبطاقة الملغاة في الوفاء أو سحب لأموال

نشير أولا أنه يحق للمصدر وفي أي وقت إلغاء البطاقة دون إبداء أية أسباب ومبررات، أو لأسباب فنية أو أمنية، ويستمد المصدر هذه السلطة بصفته مالكا للطاقة الدفع الإلكتروني وسلمها إلى الحامل على أساس الأمانة، إلا أنه حدد بعض حالات الإلغاء على سبيل المثال لا الحصر: كعجز الحامل عن الدفعأو إشهار إفلاسه بحكم قضائي، أو وفاة الحامل أو سرقة البطاقة وهذا إتباعا لما ينتهجه من وسائل لحماية البطاقة[2].

ويتم سحب البطاقة الملغاة من التعامل إما بطلبها من المصدر وتوجيه إشعار بذلك إلى الحامل، أو باحتفاظ جهاز الصراف الآلي بها وعدم إرجاعها أو عن طريق سحبها من قبل التاجر[3].

وتظهر إساءة استخدام البطاقة الملغاة من قبل الحامل إما في الوفاء للتاجر بطرق احتيالية أو استخدامها لسحب الأموال من أجهزة الصراف الآلي وذلك على النحو التالي:

1-استخدام الحامل البطاقة الملغاة في الوفاء

يمكن أن يستخدم الحامل الشرعي للبطاقة الملغاة للوفاء بثمن السلع والخدمات للتاجر عن طريق استخدام طرق احتيالية في إيهام التاجر بقبول بطاقة ائتمان منتهية الصلاحية، مرتكبا بذلك جريمة احتيال، وبناء عليه يلتزم المصدر بالوفاء بهذا المبلغ للتاجر مادام هذا الأخير لا يعلم إلغائه البطاقة، خاصة إذا قصر المصدر في أداء واجبه والمتمثل في إعطاء التاجر نشرة

(1) حسينة شرون، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الدفع الإلكتروني، **مجلة الباحث لدراسات الأكاديمية**، المجلد6، العدد2، جامعة بسكرة، الجزائر،2019، ص134.

(2) أمجد حمدان الجهني، المرجع السابق، ص 139.

(3) نفس المرجع السابق، ص140.

دورية تحذيرية بأرقام البطاقات التي جرى إلغائها، أو عند حصول التاجر على الإذن من المصدر بقبول الوفاء بالبطاقة بالرغم من أنها ملغاة[1].

2-استخدام الحامل البطاقة الملغاة في السحب

يمكن للحامل استعمال البطاقة الملغاة في سحب الأموال من أجهزة الصراف الآلي، في حين أن البنك لم يقم بإعادة برمجة ذاكرة الموزع الآلي، ومن ثم لم يقم بالاحتفاظ بالبطاقة أو حجزها في الآلة، مما يساعد العميل بالحصول على مبالغ نقدية دون وجه حق، وفي هذه الحالة يسأل الحامل عن جريمة الشروع في السرقة في حالة عدم وجود رصيد له في البنك، لأن إرادة الحامل اتجهت إلى الاستيلاء على ثروة الغير وهي أموال البنك في تلك الأجهزة[2].

ثانيا: استخدام البطاقة منتهية الصلاحية

يتم تدوين تاريخ انتهاء صلاحية البطاقة على وجهها وبأحرف بارزة، وعند انتهاء صلاحية البطاقة يتم تجديدها تلقائيا، إلا إذا أبدى المصدر عدم رغبته في تجديد الطاقة، وهنا يلتزم الحامل بتسليم البطاقة للمصدر[3].

ويمكن أن يقوم الحامل باستخدام البطاقة منهية الصلاحية بصفة غير مشروعة كأن يقوم الحامل بمحو ثم تعديل مدة صلاحية بطاقة الائتمان بعمل أرقام وبيانات جديدة طباعة خاصة بواسطة آلة طباعة معينة على الشريط الممغنط بواسطة جهاز تشفير، بعد محو ما عليه من بيانات قديمة ثم يتعمد بعدها شراء السلع والخدمات بواسطتها من التاجر ويحتج على الوفاء للمصدر وهنا يكون بصدد ارتكاب جريمة مرتبطة باحتيال[4].

---

(1) وسام فيصل محمود الشواورة، المرجع السابق، ص 83.

(2) عباسي حمزة، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر، مذكرة الماستر في الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، سنة 2019، ص50.

(3) زرقان هشام، النظام القانوني لبطاقات الدفع الإلكتروني، مذكرة الماستر في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016، ص37.

(4) راشد بن صالح بن سفيان الراشدي، الحماية الجزائية لبطاقات الائتمان في التشريع، رسالة للحصول على درجة ماستر، قسم الحقوق، كلية الحقوق، جامعة الشرق الأوسط العماني، حزيران2020، ص104.

قد يقوم الحامل باستخدام البطاقة منتهية الصلاحية بصورة غير مشروعة وذلك في حالتين:

- **الحالة الأولى:**

حالة اتفاقه مع التاجر على قبول البطاقة على قبولها في الوفاء إضرار بالمصدر، حيث يوم التاجر بتزوير تاريخ انتهاء صلاحية البطاقة على إشهار البيع أو يقوم بالإعلان– معتمدا– عن تاريخ غير صحيح لانتهاء صلاحية البطاقة عند طلب التفويض بالبيع من المصدر، وهنا نكون بصدد جريمة احتيال يسأل فيها الحامل جزائيا باعتباره فاعلا أصليا ويسأل التاجر باعتباره شريكا[1].

- **الحالة الثانية:**

إذا قبل التاجر حسن النية الوفاء بوسيلة الدفع المنتهية الصلاحية وذلك بإغفاله لتاريخ انتهاء صلاحية البطاقة بسبب خطأ فني في أجهزة الاتصال بينه وبين البنك الذي أعطى جهاز نقطة البيع لدى التاجر إشارة موافقة على إجراء عملية الوفاء، مع أن وسيلة الدفع منتهية الصلاحية وتاريخ انتهاء صلاحيتها مزور، فيكون هنا حاملها في صدد ارتكاب جريمة احتيال باعتبار البطاقة منتهية الصلاحية وسيلة من وسائل النصب المنصوص عليها في نص المادة 372 من قانون العقوبات الجزائري[2].

(1) أمجد حمدان الجهني،المرجع السابق، ص142.

(2) هداية بوعزة، النظام القانوني للدفع الإلكتروني(دارسة مقارنة)، رسالة مقدمة لنيل شهادة في القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2017، ص ص534،535.

ثالثا: الامتناع عن رد البطاقة الملغاة أو المنتهية الصلاحية

إذا ما انتهى عقد بطاقة الدفع الإلكتروني سواء بانتهاء مدة صلاحيتها أو إلغائها وقام البنك بإخطار المرسل إليه (العميل) بردها، التزم هذا الأخير بردها لأنها سلمت إليه كعارية استعمال، فإذا رفض ردها يعتبر خائنا للأمانةحتى وإن لم يستعمل البطاقة أو يتصرف فيها[1].

1-تعريف جريمة خيانة الأمانة:

نص المشرع الجزائري على جريمة خيانة الأمانة في المادة 376 من قانون العقوبات والتي تنص على ما يلي[2]: "**كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة ويعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة مالية من 500 إلى 20.000 دج**"

2-أركان جريمة خيانة الأمانة:

تتمثل أركان فذه الجريمة في:

أ- الركن المادي:

يتحقق الركن المادي لجريمة خيانة الأمانة في هذه الحالة في استغلال الحامل للبطاقة الإلكترونية بسوء قصد خلافا للغرض الذي عهد به إليه أو سلم له من أجله، مع اقترانه بنية الحامل في تملك البطاقة التي سلمت له على أساس عارية الاستعمال، وبذلك إذا امتنع الحامل عن رد البطاقة إلى المصدر فقد أفصح عن نيته في تغيير حيازته على البطاقة من حيازة

(1) حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، رسالة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2015، ص513.

(2) انظر المادة 376 من قانون العقوبات الجزائري.

ناقصة إلى حيازة كاملة والتي تظهر فيها صور التعدي محققا بذلك الركن المادي لجريمة خيانة الأمانة[1].

ب- الركن المعنوي:

يتحقق الركن المعنوي لجريمة خيانة الأمانة بتوافر عنصري العلم والإرادة، أي علم الحامل باحتفاظه ببطاقة منتهية الصلاحية أو ملغاة، وأنه ملزم بردها بموجب الاتفاق الوارد في العقد بينه وبين المصدر، وأنه يريد برفضه إلحاق الضرر بمصدرها[2].

الفرع الثالث: الاستخدام المقنع للبطاقة

من خلال هذا الفرع سوف نتطرق إلى الاستخدام المقنع لبطاقة الدفع الإلكتروني من قبل حاملها والتي يظهر في ثلاث حالات:

أولا: الإبلاغ غير الصحيح عن فقد أو سرقة البطاقة

تفرض عقود استخدام بطاقات الدفع الإلكتروني على الحامل الالتزام بالإخطار عن فقد أو ضياع بطاقة الدفع أمام الجهة المصدرة لها، فيجب أن يتم هذا الإخطار في وقت مناسب وبوسيلة سريعة كالهاتف أو الفاكس أو الايمايل، مع ضرورة تأكيده كتابةً إلى جهة الإصدار حتى ينتج أثره، فتقوم جهة الإصدار بغلق أداة الدفع وتسقط مسؤولية الحامل اتجاه أي تصرف يحدث بها بعد ذلك[3].

وقد يحدث أن يبلغ الحامل البنك المانح للبطاقة والجهات المختصة عن فقدها أو سرقتها رغم أنها لا تزال في حوزته، ويقوم باستعماله قبل قيام البنك باتخاذ الإجراءات اللازمة وإعادة برمجة ماكينات السحب والبيع الإلكترونية بعدم قبول هذه البطاقة المسروقة أو المفقودة في السحب، أما الحامل فيقوم باستخدامها للوفاء لدى التجار المزودين بآلة الطباعة اليدوية مرتكبا

(1) احمدي بوزينة أمنة، "المسؤولية الجزائية عن الاستعمال غير المشروع لبطاقة الائتمان"، **مجلة اقتصاديات شمال إفريقيا**، العدد13، جامعة الشلف، الجزائر، د س ن ، ص154.

(2) هداية بوعزة، المرجع السابق، ص 545،

(3) لوسي عقيلان أبو عقيل، التنظيم القانوني للنقود الإلكترونية كأحد وسائل الدفع، الطبعة الأولى، دار الأيام للنشر والتوزيع، عمان، 2018، ص ص115،116.

جريمة الغش والسرقة، وذلك من أجل استفادته من الإعفاء من المسؤولية عن فقد أو ضياع البطاقة بالإعلان الكاذب وإيهام البنك المصدر أنه تم استخدامها غير المشروع من قبل الغير[1].

ثانيا: الإدعاء غير الصحيح بعدم استخدام البطاقة

في هذه الحالة يقوم حامل البطاقة باستخدامها في السحب أو الوفاء أثناء سفره إلى بلد ما، حيث يستفيد مما يقدمه ذلك البلد من خدمات كشراء مختلف السلع من المتاجر والمحلات خلال فترة مكوثه هناك وعند عودته لبلده ينكر سفره ويدعي عدم استخدام بطاقته ويعتمد في إثبات ذلك على جواز سفر آخر[2].

ثالثا: التواطؤ ما بين الحامل والغير

يتم التواطؤ ما بين الحامل الشرعي والغير بقصد التحايل على المصدر، وذلك إما عن طريق إعطاء الحامل بطاقته للغير لاستخدامها في السحب وتزوير توقيعه مقابل حصة معينة من المال، وبعده يعترض على عمليات السحب ويقوم بالطعن بتزوير توقيعه، حتى لا يتم خصم المبلغ المسحوب من حسابه كما يمكن أن يتم التواطؤ عن طريق إعطاء بيانات البطاقة ورقمها للغير، بهدف تزوير بطاقة أخرى على غرارها الاستيلاء على أموال المصدر والتاجر[3].

المطلب الثاني

إساءة استخدام بطاقة الدفع الإلكتروني من قبل التاجر والمصدر

لا يقتصر الاستخدام غير المشروع لبطاقة الدفع الإلكتروني على الحامل فقط، بل قد يمتد لموظفي المصدر القائمين على إدارته، والتاجر قابل الوفاء باستخدام هذه الوسيلة وعليه سنفصل من خلال هذا المطلب في إساءة استخدام بطاقة الدفع الإلكتروني من قبل موظفي المصدر والتاجر كل على حدى في فرعين متتاليين على النحو التالي:

(1) مرباح صليحة، المرجع السابق، ص 235.

(2) أمجد حمدان الجهني، المرجع السابق،145.

(3) وسام فيصل محمود الشواورة، المرجع السابق، 86.

الفرع الأول: إساءة استخدام بطاقة الدفع الإلكتروني من قبل المصدر

باعتبار أن المصدر شخص معنوي يباشر صلاحياته بواسطة الأشخاص القائمين على إدارته، وبحكم موقعهم الوظيفي قد يقومون بإساءة استخدام هذه السلطة والاعتداء على وسيلة الدفع الإلكتروني بالاتفاق والتواطؤ مع الحامل أو التاجر أو الغير، بغية تحقيق مصلحة أو الحصول على فائدة أو مزية.

أولا: تواطؤ موظفو البنك مع العميل

قد يتفق موظف البنك مع العميل على الاعتداء على نظام وسيلة الدفع الإلكتروني، ويكون هذا الاعتداء في عدة صور: كأن يقوم الموظف باستخراج بطاقة دفع إلكترونية سليمة ببيانات أو مستندات مزورة لصالح العميل حتى يستفيد من الربح (المال) الذي تنطوي عليه البطاقة.

كما يمكن أن يحدث التواطؤ في حالة سماح موظف البنك للعميل بالصرف بموجب بطاقة الدفع الإلكترونية منتهية الصلاحية أو بعد صدور أمر إلغائها، وكذلك عند سماحه له بتجاوز الحد الأقصى المسموح بموجب هذه الوسيلة[1].

وفي هذا الإطار نجد أن الجرائم التي يسأل عنها الموظف جزائيا في حالة اتفاقه غير المشروع مع الحامل تتمثل في جريمة الاشتراك في التزوير أو استعمال مزور وجريمة الرشوة.

1-جريمة الاشتراك في التزوير أو استعمال مزور

هي جريمة تقوم على تغيير حقيقة المحررات أو استعمالها من طرف موظف البنك للصالح غير المشروع للعميل.

أ- تعريفها:

يمكن اعتبار موظف البنك شريكا في جريمة التزوير واستعمال المحررات المزورة لمساعدة العميل في استخراج بطاقة دفع مزورة، قصد الاستيلاء على أموال البنك دون وجه

(1) هداية بوعزة، المرجع السابق، ص 592.

حق[1]، فتطبق عليه أحكام جريمة التزوير طبقا لما ورد في قانون العقوبات الجزائري، ويعاقب عقوبة الفاعل الأصل يوفقا لنص المادة 221 من قانون العقوبات الجزائري[2].

ب- **أركان جريمة التزوير أو استعمال مزور**

وتتمثل في ركنان هما:

- **الركن المادي**

يتمثل الركن المادي في جريمة تزوير المحررات في تغيير حقيقة المحرر تغييرا من شأنه أن يسبب ضررا بإحدى الطرق التي نص عليها القانون، حيث يستعمل موظف المحررات المزورة في استخراج وسيلة دفع مشروعة للعميل[3].

- **الركن المعنوي**

جريمة التزوير في المحررات من الجرائم القصدية التي تلزم لقيامها القصد والنية والغاية التي يتوخاها الموظف من جراء ارتكابه الركن المادي للتزوير أو استعمال المحررات المزورة[4].

2- جريمة الرشوة

هي جريمة تقوم في حق موظفي البنك، في حالة اتفاقه مع العميل، على تلقي مبلغ مالي مقابل جريمة الاشتراك في التزوير أو استعمال المزور.

أ- تعريفها:

جاء في نص المادة 25 فقرة2 من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته أنه يعاقب بعقوبة الحبس وغرامة مالية[5]: "**كل موظف عمومي طلب أو قبل، بشكل مباشر أو**

---

(1) عبد الكريم الردايدة، الجرائم المستحدثة وإستراتيجية مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2013، ص228.

(2) أنظر المادة 221 من قانون العقوبات الجزائري.

(3) أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، دار هومة، الجزائر، 2003، ص239.

(4) نفس المرجع السابق، ص 245.

(5) القانون 06-01 المؤرخ في 21 محرم 1427 الموافق لـ20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، ج ر ج ج ، عدد 14، الصادرة بتاريخ 8 مارس2006.

غير مباشر، مزية غير مستحقة سواء لنفسه أو لصالح شخص آخر أو كيان آخر لأداء عمل أو الامتناع عن أداء عمل من واجباته". وهذا إضافة إلى العقوبات التكميلية المنصوص عليها في المادة 09 من قانون العقوبات الجزائري[1].

واستنادا لنص هذه المادة فإن جريمة الرشوة تقوم في حق موظف البنك باعتباره موظف عمومي، في حال اتفاقه مع العميل من أجل انجازه لأفعال واعتداءات غير مشروعة بواسطة بطاقة الدفع الإلكتروني وذلك مقابل فائدة أو مبلغ مالي يمنحه العميل للموظف جزاء هذه الخدمات[2].

ب- أركانها: وهي الركن المادي والركن المعنوي.

- **الركن المادي:**

فيما يتعلق بالركن المادي لجريمة الرشوة يجب التمييز بين الرشوة السلبية والرشوة الإيجابية، ففيما يخص الركن المادي للرشوة الإيجابية يتعلق الأمر بعرض الراشي وهو حامل بطاقة الدفع الإلكتروني مزية غير مستحقة على موظف البنك نظير حصوله على منفعة بإمكان ذلك الشخص توفيرها له بالقيام بعمل من أعمال وظيفته أو الامتناع عن أدائه[3].

أما فيما يخص الركن المادي لجريمة الرشوة السلبية من خلال استقراء المادة 2/25 من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، يظهر في جريمة الموظف المرتشي حيث يتحقق هذا الركن بطلب موظف البنك أو قبوله مزية غير مستحقة والتي تمثل محل الجريمة، نظير قيامه بعمل من أعمال وظيفته أو الامتناع عن القيام به[4].

(1) أنظر المادة 9 من قانون العقوبات.

(2) عبد الكريم الردايدة، المرجع السابق، ص229.

(3) أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص(جرائم الفساد، جرائم المال والأعمال، جرائم التزوير)، الطبعة 13، الجزء الثاني، دار هومة، الجزائر، 2013، ص85.

(4) نفس المرجع السابق، ص85.

- **الركن المعنوي:**

يشترك الركن المعنوي لجريمة الرشوة في كلتا صورتي الرشوة الإيجابية والسلبية فتتطلب توافر القصد الجنائي العام لدى مرتكبيها، والذي يتحقق بثبوت توافر عنصري العلم والإرادة، فيتعين أن يحيط علم الموظف المرتشي أن العمل الذي يطلب منه أداؤه أو الامتناع عنه داخل في اختصاصه، وأن المقابل الذي يقدم إليه جزاء القيام بهذا العمل غير مشروع فإن انتفى عنده العلم انتفى عنه القصد الجنائي[1].

ثانيا: تواطؤ موظفو البنك مع التاجر

قد يحدث وأن يتواطؤ موظف البنك مع التاجر في التاجر ارتكاب الاعتداء على نظام وسيلة الدفع الإلكتروني وذلك بارتكاب الأفعال الآتية:

-تجاوز حد السحب في صرف قيمة سندات البيع.

- اعتماد سندات بيعصدرت استنادا إلى بطاقات وهمية، أو مزورة، أو منتهية الصلاحية.

- السماح للتاجر بإدخال رقم البطاقة على الجهاز الإلكتروني يدويا مما يسمح له بإدخال رقم البطاقة على الفواتير دون وجود البطاقة عنده أصلا[2].

وتكيف جريمة تواطؤ موظفو البنك مع التاجر عند إقدام الموظف على ارتكاب هذه الأفعال بالاتفاق مع التاجر، فإنه تتم مساءلته جزائيا، وبالرجوع إلى القانون06-01 نجد أن أركانها قد تتحقق بالفعل الغير مشروع المرتكب من طرف الموظف على بطاقة الدفع الإلكتروني، فنجد أن ركنها المادي يتوافر من خلال المزية أو الفائدة التي يتلقاها موظف البنك مقابل اتفاقه مع التاجر والسماح له بتجاوز سقف السحب في صرف قيمة سندات البيع، أما الركن المعنوي فيظهر في نية الموظف في القيام بهذا الفعل على الرغم من إدراكه أنه مخالف للنظام العام الداخلي ومنه تترتب عليه المسؤولية الجزائية لهذا الفعل غير المشروع[3].

---

(1) حليمة غوباش، جريمة الرشوة في ظل القانون06-01 المتعلق بالوقاية من الفساد ومكافحته، مذكرة لنيل شهادة الماستر، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2014، ص23.

(2) أمجد حمدان الجهني، المرجع السابق، ص154.

(3) عبد الكريم الردايدة، المرجع السابق، ص 231.

ثالثا: تواطؤ موظفو البنك مع الغير

قد يتفق موظف البنك مع الغير اتفاقا غير مشروع مقابل الحصول على فائدة أو مقابل مالي، ويقصد بالغير هنا أفراد العصابات الإجرامية، والتي تحصل على بطاقات الوفاء الصحيحة عن طريق التقليد والاصطناع والتزوير وغير ذلك من أفعال غير مشروعة، وذلك من أجل الاستيلاء على المبالغ النقدية من خلالها، وتستهدف جرائمهم عادة البطاقات ذات القيمة المرتفعة وأفراد ذو سمعة تجارية عالية[1].

وتكيفالجرائم الواقعة عند تواطؤ موظف البنك مع العميل، على أنها جريمة إفشاء السر المهني، وجريمة رشوة.

1-جريمة إفشاء السر المنهي:

نص المشرع الجزائري على جريمة إفشاء السر المهني في المادة 60 من المرسوم التشريعي رقم 93-10 المتعلق ببورصة القيم المنقولة حيث جاء في متنها[2]: "**يعاقب بالحبس من 6 أشهر إلى خمس سنوات وبغرامة مالية قدرها 30000 دج، ويمكن رفع مبلغها إلى أكثر من ذلك حتى يصل أربعة أضعاف المبلغ المغتنم المحتمل تحقيقه، دون أن تقل هذه الغرامة على المبلغ المغتنم نفسه، أو يعاقب بإحدى العقوبتين فقط كل شخص تتوفر له بمناسبة ممارسة مهنته أو وظيفته معلومات إمتيازية عن منظورية تطور قيمة منقولة ما، فينجز بذلك عملية أو عدة عمليات في السوق أو يعتمد السماح بانجازها، إما مباشرة أو عن طريق شخص مسخر لذلك قبل أن تنتهي تلك المعلومات إلى الجمهور، تعد العلميات التي تنجز على هذا الأساس عمليات باطلة**".

(1) منال بتة، الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2019، ص58.

(2) مرسوم تشريعي رقم 93-10 مؤرخ في 2 ذي الحجة عام 1413 الموافق ل23 مايو سنة 1993، يتعلق ببورصة القيم المنقولة، ج ر ج ج، العدد 34، الصادرة بتاريخ 30 مايو1993، المعدل والمتمم.

إضافة إلى هذا عاقب المشرع على جريمة إفشاء الأسرار بمقتضى نص المادة 01/301 من قانون العقوبات الجزائري[1]، حيث أن موظف البنك المصدر للبطاقة تعمد إطلاع الغير على أسرار ائتمن عليها بمقتضى عمله، وقام بتزويد أفراد العصابات ببيانات دون علم أصحابها ما يهيئ الطريق لأفراد العصابات لسحب أموال الغير عن طريق التزوير وهذا ما يمثل الركن المادي لجريمة إفشاء الأسرار[2].

كما أن هذا الموظف يعلم أنه مؤمن على أسرار العملاء، والبيانات المتعلقة بوسائل دفعهم و رغم ذلك يقوم بإفشائها للغير رغم منع القانون لذلك وهذا ما يشكل الركن المعنوي للجريمة[3].

3- جريمة الرشوة

يكون الدافع وراء قيام موظف البنكلإفشاء أسرار بيانات وسيلة الدفع الإلكتروني الخاصة بعميل ما هو الحصول على مقابل مالي أو فائدة معينة، حيث يظهر الركن المادي في هذه الجريمة في فعل الموظف المتمثل في طلب أو قبول أخذ فائدة مادية أو غير مادية مقدمة من الغير نظير، إفشاء بيانات وسيلة الدفع الإلكتروني تخص العملاء، أما الركن المعنوي لهذه الجريمة فيظهر في نية الموظف في الإخلال بواجبات وظيفته وعلمه بأنه يدلي بيانات عملائه وهنا يتحقق القصد الجنائي للركن المعنوي لجريمة الرشوة[4].

الفرع الثاني: الاستخدام الغير المشرع من قبل التاجر

للتاجر دور كبير في استكمال عمليات البيع، وتقديم الخدمات والسلع للعملاء باستخدام بطاقات الدفع الإلكتروني فيقوم بفحص هذه البطاقات والتأكد من صلاحياتها ويتأكد أيضا من الشخصية الحاملة لها وتوقيعه، وذلك باعتماد على مجموعة من الوسائل والأساليب المسلمة لها وكما يمكن أن يستخدم هذه الوسائل في استعمالات غير مشروعة بتزوير هذه الطاقة أو التلاعب بها من خلال الأجهزة المخصصة لها.

(1) أنظر المادة 01/301 من قانون العقوبات الجزائري.

(2) منال بتة، المرجع السابق، ص58.

(3) هداية بوعزة، المرجع السابق، 604.

(4) نفس المرجع السابق، ص604.

أولا: التجاوزات التي يقوم بها التاجر باستخدام للآلة اليدوية

من خلال استخدام الآلة اليدوية يقوم التاجر بعدة تصرفات غير مشروعة وهي:

-قيام التاجر سيء النية بتزوير التواقيع الخاصة لديه على فواتير تضمن المشتريات وبعد قيام التزوير يقدمها التاجر إلى البنك من أجل استيفاء قيمتها من رصيد صاحب البطاقة.

-كما يمكن أن يقوم بطباعة أرقام العملاء المتعاملين معه على إشعارات فارغة وخالية ويقوم بإرسالها إلى تجار آخرين منتمين أيضا لدى البنك المصدر[1].

-ادعاء التاجر بتعطيل الآلة الإلكترونية وبعد ذلك يقوم بكتابة أرقام وهمية على المستندات ليتمكن من استيفاء قيمتها لاحقا[2].

-قبول بعض التجار التعامل بالبطاقة المزورة أو الملغاة أو منتهية الصلاحية باتفاق مع حاملها الشرعي لإجراء عمليات وهمية وتحصيل قيمتها، إضافة إلى ذلك تقديم الفواتير أكثر من مرة باستخدام الأصل مرة والصورة مرة أو تقديم صورته مرة وصورة المشتري مرة أخرى بالتواطؤ معه، وفي بعض الأحيان يستكمل التجار العمليات على الرغم من عدم وجود موافقة عليها[3].

-وقد يستخدم التاجر إشعاراتمطبوعة بأرقام بطاقات عملاء وتواريخ على الرغم من التبليغ بسرقة البطاقة أوفقدها بتاريخ سابق على عملية البيع[4].

ثانيا: التجاوزات التي يقوم بها التجار بواسطة الجهاز الإلكتروني

يقوم التاجر بالعبث بالجهاز الإلكتروني من خلال الطرق التالية:

-يقوم التاجر بوضع جهاز قارن على جهاز البيع الإلكتروني بحيث يقوم نسخ المعلومات والبيانات على بطاقة أخرى لاستعمالها في عمليات بيع وهمية دون علم الحامل.

---

(1) محمد توفيق سعودي، بطاقات الائتمان والأسس القانونية للعلاقات الناشئة عن استخدامها، دار الأمير، بيروت، لبنان، 2002، ص 44.

(2) عبد الفتاح بيومي حجازي، جرائم الكمبيوتر الآلي في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 584.

(3) محمد توفيق سعودي، المرجع السابق، ص 45.

(4) نفس المرجع السابق، ص45.

– يقوم التاجر التلاعب في البرامج الخاصة بالآلة الإلكترونية لتعطيل العمل بها أثناء قراءة البطاقة حتى لا يتم اكتشاف البطاقة المزورة، ومن ثم استخدامها في تحصيل القيمة التي تمت بموجب البطاقة المزورة[1].

–وقد يقوم التاجر بتعطيل نظام تشغيل الآلة الإلكترونية في سبيل استخدام بطاقة مسروقة أو موقوفة، أو في سبيل استعمالها في عمليات بيع وهمية للحصول على مبالغ مالية دون وجه الحق.

– كما يمكن أن يلجأ التاجر إلى تشغيل الآلة الالكترونية يدويا ثم يقوم بتزوير توقيع أصحاب البطاقات على الإشعارات وإرسالها إلى البنك المصدر لتحصيل قيمتها[2].

–قيام بعض التجار باستخدام البطاقات التي ليس لها أرصدة كافية للصرف، وذلك عن طريق إجراء عمليات بيع مختلفة ومتنوعة بمبالغ صغيرة وأخذ الموافقة عليها وصرفها من البنك، ثم يتضح بعد ذلك عدم وجود رصيد كافي لأصحاب هذه البطاقات.

–إجراء اتصالات دولية وتحميل القيمة على بطاقات الدفع الإلكتروني المنفصلة الخاصة بالغير [3].

(1) حوالف عبد الصمد، المرجع السابق، ص335.

(2) نفس المرجع السابق، ص 335.

(3) أسماء بوعقال، الحماية الجنائية لبطاقات الدفع الإلكتروني، مذكرة لنيل شهادة الماستر في قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بالمهيدي، أم البواقي، 2017/2016، ص 22.

المبحث الثاني

الاستخدام الغير مشروع لبطاقات الدفع الإلكتروني من قبل الغير

الغير هو كل شخص أجنبي على الأطراف المتعاقدة المتعاملة بالبطاقة ولا يخضع لالتزامات العلاقة التعاقدية، ورغم ذلك فقد يصادف أن تقع البطاقة في يده فيستخدمها في أعمال غير مشروعة وهو ما يشكل خطرا على أطرافها سواء من خلال جريمة التزوير (المطلب الأول)، أو من خلال استخدام البطاقة المسروقة أو المفقودة (المطلب الثاني).

المطلب الأول

استعمال الغير لبطاقة ائتمان غير صحيحة(مزورة)

ويكون تزوير بطاقات الدفع الالكتروني، إذا كانت البطاقة البلاستيكية المصنوعة تشبه إلى حد قريب جدا البطاقة الحقيقية بغرض توليد الشيفرة، وإتمام العملية وهذا بإرسال المبلغ إلى حساب آخر.

الفرع الأول:جريمة تزوير بطاقة الائتمان الالكتروني

تعد جريمة التزوير الإلكتروني من أخطر طرق الغش التي ظهرت في مجال المعاملات الإلكترونية على أساس نشر هذه الأخيرة في مختلف المجالات، مثل عمليات طلب البضائع والوفاء بقيمتها، وتحويل الأموال من بنك إلى آخر، ومما يزيد من خطورة الجريمة هو صعوبة اكتشاف وإثبات التزوير في هذا المجال[1].

يمكن الاعتداء على بطاقة الدفع الإلكتروني من قبل شخص غير صاحب البطاقة الأصلي،حيث أنه في بعض الأحيان يمكن أن تفقد البطاقة أو تسرق من العميل وتقع عند الغير الذي يقوم باستخدامها استخداما غير مشروع ومن هذه الاستخدامات التزوير[2].

(1) الذهبي خدوجة، الحماية الجزائية للمعاملات الإلكترونية(دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2019/2018، ص59.

(2) جلال عايد الشورة، وسائل الدفع الإلكتروني، دار الثقافة للنشر والتوزيع، الجزائر، 2008، ص102.

أولا: أركان جريمة التزوير

هي جريمة نص عليها قانون العقوبات الجزائري في نص المادة 394 مكرر1، فقرر لها عقوبات أصلية، سواء تعلق الأمربالشخص الطبيعي أو الشخص المعنوي إضافة إلى عقوبات تكميلية[1].

تجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بتزوير المعلومات فقد حذا حذو المشرع الفرنسي الذي أخضع تزوير المعلومات إلى النصوص العامة في التزوير، وهي نصوص قانون العقوبات، وذلك بعد التعديل الذي قام به بجعل موضوع التزوير هو أي دعامة مادية وليس فقطالمحرر وهذا هو الفرق في قانون العقوبات الجزائري فالنصوص الخاصة بالتزوير، تجعل التزوير يقع على المحرر، وعليه لا يمكن إخضاع أفعال التزوير المعلوماتي إلى النصوص العامة للتزوير، وإنما يستدعي ذلك تدخلا تشريعيا إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي[2].

والجريمة بشكل هي أي فعل أو ترك، رتب له القانون عقوبة بنص إذ لا جريمة إلا بنص[3]، وبهذا فإن لجريمة التزوير ركن مادي وركن معنوي وهما:

- **الركن المادي:**

وهو تغيير الحقيقة في محرر بإحدى الطرق المنصوص عليها قانونا، وهذا الركن يتكون من ثلاثة عناصر وهي المحرر و تغيير الحقيقة المسجلة فيه، والوسيلة التي نص عليها المشرع:

أ-**المحرر**: هو كل ما هو مكتوب بحروف أو أرقام أو علاماتمادية ظاهرة للعيان، ويتمتع بالثبات أو الاستقرار ومن شأنه التعبير عن الأفكار، والمحافظة على بقائها والسماح بالرجوع

(1) انظر المادة 394 مكرر1 من قانون العقوبات الجزائري.

(2) عمراني مصطفى، "جريمة تزوير البطاقات البنكية"، **مجلة الدراسات والبحوث القانونية**، العدد 07، كلية الحقوق، ، جامعة جيلالي اليابس، سيدي بلعباس، 2012، ص ص322،323.

(3) باسم الفقير، التزوير الإلكتروني، دار اليراع للنشر والتوزيع، الجزائر، 2007، ص21.

إليها سواء من طرف أصحابها أو من طرف الغير، وهذه الكتابة لم يحددها القانون المدني شكلا وبذلك فهي متعددة ومختلفة المصادر لنقل المعلومات والاحتفاظ بها واستعمالها، ويجب أن تمتاز هذه الكتابة بالثبات لمدة غير محددة وإلا فإنها لا تصلح بأن تكون عرضة للتزوير وعليه فالنشاط الإجرامي في جريمة التزوير يقوم على عنصرين أساسين هما:

- أن تكون كتابةً أي صكا ومخطوطا.
- أن تكون له قوة في الإثبات بالنسبة للبيانات التي انصب عليها تحريف الحقيقة[1].

ب- تغيير الحقيقة المسجلة فيه: ويعد تحريف الحقيقة جوهر جريمة التزوير بحيث لا تقوم هذه الجريمة إذا لم يقم هذا التغيير في مضمون المحرر، فإذا انتفى هذا العنصر انتفى معه التزوير حتى ولو توهم الفاعل أنه يغير الحقيقة إذ لا قيام لجريمة بغير فعل جرمي.

وتحريف الحقيقة لا يعني أن تكون كل البيانات المدرجة في المحرر كاذبة بل إن القانون يكتفي بأقل نصيب يقع عليه التزوير[2].

ج- الوسيلة التي نص عليها القانون: والتي يتحقق بها النشاط الإجرامي للفاعل وهي طرق التزوير التي حددها القانون على سبيل الحصر، وعليه لا قيام للتزوير إلا إذا كان تغيير الحقيقة بإحدى هذه الطرق، ويعلل جانب من الفقه حول هذا الحصر في حرص المشرع على أن توضع للتزوير الحدود المعقولة له وعلى تفادي أن يدخل في نطاق هذه الجريمة والعقاب عليها حالات من تحريف الحقيقة لا تقتضي المصلحة العقاب عليها[3].

- **الركن المعنوي:**

تعد جريمة تزوير بطاقات الدفع الإلكتروني من الجرائم العمدية التي تقتضي توافر القصد الجنائي لدى الجاني الذي ينبغي أن يكون معاصرا لارتكاب الفعل المادي الذي تقوم به جريمة

(1) نجيمي جمال، جرائم التزوير في قانون العقوبات الجزائري، دار الهومة للنشر والتوزيع، الجزائر، 2013، ص ص 388، 389.

(2) عماد علي الخليل، الحماية الجزائية لبطاقات الوفاء(دراسة تحليلية مقارنة)، الطبعة 1، درا وائل للطباعة والنشر، الأردن، سنة2000، ص54.

(3) نفس المرجع السابق، ص ص54،55.

التزوير، فإذا لم يتوفر القصد الجنائي بعناصره وقت ارتكاب الفعل فلا تتحقق جريمة التزوير في هذه الحالة والقصد الجنائي يمكن أن يكون عاما ويمكن أن يكون خاصا[1].

أ- القصد العام: يتوفر القصد العام عندما يقوم الشخص بتزوير بطاقة الائتمان وهو يعلم بأنه يغير الحقيقة في المحررات الرسمية والتي تلحق ضرر محتم واحتمالي على الأشخاص، وينتفي القصد العام لانتفاء إرادة تغيير الحقيقة، وبالتالي لا تقوم الجريمة في حالة موظف البنك أو أي مؤسسة مخول لها القانون إصدار البطاقات البنكية الذي يثبت رسميا البيانات الكاذبة التي يدلي بها الجاني مقترفا جريمة تزوير البطاقة البنكية طالما لم يكن الموظف عالما بما تتضمنه هذه البيانات في تغيير الحقيقة[2].

ب-القصد الخاص: هو اقتران العلم بالجريمة بنية استعمال المحرر فيما زور من أجله، واستعماله استعمالا غير مشروع، فالجاني،هنا انصرفت إرادته إلى تغيير الحقيقة في المحرر واستعماله فيما زور من أجله، حتى لو لم يستخدمه فعلا بل لو حتى أصبح مستحيلا استخدامه فيما زور من أجله كأن تبرمج الأجهزة الآتية لتوزيع النقود على كشف البطاقة المزورة أو أن يعدل من زورها عن استعمالها[3].

ثانيا: التزوير ببطاقات الدفع الإلكتروني

عادة ما نؤمن بطاقة الدفع الإلكتروني بعدة وسائل ضد التزوير، ولعل أهم هذه الوسائل الحروف البارزة، الطباعة الدقيقة، العلامات ثلاثية الأبعاد، الطباعة الغير مرئية التي يتم قراءتها بالأشعة فوق بنفسجية وغيرها، إلا أن هذا لا يمنع من تزويرها واستعمالها في الاحتيال على البنوك، وقد يكون التزوير كليا أو يكون تزويرا جزئيا.

(1) ممدوح بن راشيد الرشيد العتري، "الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير"، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 31، العد62، الرياض، سنة2015، ص 65.

(2) نفس المرجع السابق، ص66.

(3) عمراني مصطفى، المرجع السابق، ص 316.

1-التزوير الكلي:

إن التزوير الكلي يبدأ بعمل بطاقة بلاستيكية بالكامل تبدأ بتقليد الطباعةوالنقوش والرسوم علي البلاستيك، ثم تغليف البطاقة ولصق الهلوجرام ولصق الشريط الممغنط وشريط التوقيع، ثم اصطناع شريط ممغنط إما بالنسخ أو بالتشفير، ثم عمل الطباعة البارزة عن طريق إنشائها بمعلومات تم الحصول عليها بطريقة غير شرعية ثم تداول البطاقة واستخدامها في عمليات الشراء. أما إذا توفر للمزور الرقم السري المتوافق مع بطاقة ما فإنه يمكن عمل بطاقة بلاستيكية خالية من البيانات ويضع عليها شريط بتشفيره أو استنساخ بيانات صاحب البطاقة وعمل نسخ عديدة منها[1].

وهناك صور أخرى للتزوير الكلي عن طريق سرقة بطاقات كاملة التجهيز ومن الظواهر الدالة على التزوير الكلي للبطاقة:

- اختلاف مواصفات شكل وحجم البيانات المطبوعة طباعة بارزة بالبطاقة المصطنعة عند مقارنتها بنظيرتها الصحيحة.
- عدم دقة لصق الشريط الممغنط وشريط التوقيع بظهر البطاقة حيث من الممكن نزعها بسهولة بواسطة اظفر الأصابع.
- الميل إلى إهمال طلاء رؤوس البارزة للطباعة النافرة وهي على عكس الطباعة البارزة، فتتم باستخدام أسطوانة نحاسية محفور عليها الكلام، أو الصور أو الأشكال المرطبة طباعتها بحفار ميكانيكي أو بأشعة الليزر.
- إمكانية عدم تطابق البيانات المشفرة على الشريط الممغنط وبين البيانات المقروءة بصريا والمطبوعة طباعة نافرة.

(1) مهند فايز دويكات، حسين محمد الشبلي، "صور الاحتيال والتزوير في بطاقات الائتمانية"، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 29، العدد 58، الأردن، ص 63.

- خلو البطاقة المصطنعة من الخواص المميزة للطباعة المجهرية نتيجة لنقص في الإمكانيات في آلات التصوير التجارية التي يستخدمها المزورون[1].

2- التزوير الجزئي لبطاقات الدفع الإلكتروني

يستفيد المزور في هذه الحالة من جسم البطاقة الحقيقية من هولجرام ونقوش والطباعة وكتابة آمنة ليقوم بتزوير البطاقة، ويكون بالقيام بحذف أرقام الحقيقية أو المنتهية الصلاحية أو إعادة كتابةحساب جديد أو حساب آخر يتم الحصول عليه بسرقة المعلومات الخاصة بطريقة غير مشروعة أو تقليد الشريط الممغنط بمحو بياناته وإعادة تشفيره بمعلومات جديدة وصحيحة مسروقة، أو إجراء العمليتين معا أو نزع الصورة الموجودة على البطاقة الخاصة بالعميل ووضع صورة شخص آخر مكانه ومن المظاهر الدالة على التزوير الجزئي للبطاقة:

- انهيار بعض المواضيع من شريط التوقيع وظهور سطح البطاقة أسفل مواضع الانهيار نتيجة المحو الآلي والكيميائي.
- التشوه أو التقطع الظاهر على أسفر الحافة للهولجرام.
- وجود بقع سوداء في مناطق الكتابة النافرة أو عدم انتظام الرؤوس البارزة لهذه الكتابة.
- الاختلاف في المسافات الأمنية للتشكيل الطباعي للأرقام والحروف والصور والأشكال
- المثبتة على البطاقة المزورة من البطاقة الأصلية[2].

3- تزوير الإشعارات والمستندات الخاصة ببطاقة الائتمان

أ- تزوير الإشعارات:

- **من قبل موظف البنك:**قد يحصل اتفاق بين موظف البنك وأفراد عصابة إجرامية على إعطائهم بيانات بطاقة ائتمان صحيحة ومتداولة من أجل استخدامها في تزوير وإنشاء بطاقة جديدة فينحصر هنا دور موظف البنك في منح المعلومات والبيانات، أما دور أفراد العصابة

(1)مهند فايز دويكات، حسين محمد الشبلي ، المرجع السابق، ص 64.

(2) ميهوبي فطيمة، المرجع السابق، ص، ص42 43.

فهو إنشاء بطاقة جديدة، فيشكل ذلك عدة جرائم متداخلة من حيث أمداد المعلومات عن حساب العملاء وتزوير البطاقة والاستيلاء على الأموال دون وجه الحق[1].

وقد يعتمد أيضا موظف البنك إشعارات ببيع صدرت استنادا على بطاقة وهمية أو مزورة أو منتهية الصلاحية أو ملغاة وإذا أثبت علمه بوجود حالة من هذه الحالات فإن الأمر يشكل جريمة تزوير، وكما يمكن لوظف البنك أن يتلاعب شخصيا ببطاقة الدفع الإلكتروني في حالة تقدم حامل البطاقة من أجل سحب أو إيداع فيقوم بتزوير قيمة المبلغ الموجود برصيد البطاقة حيث يشتمل هذا الاعتداء جريمة سلب الأموال والاستيلاء عليها وتزوير المستندات والبيانات[2].

- **تواطؤ حامل البطاقة مع التاجر:** ويتم ذلك من خلال قيام حامل البطاقة بإجراء عملية شراء وهمية حيث يقوم بالاتفاق مع التاجر، مقابل نسبة معينة من قيمة الفاتورة لصالح التاجر، ويتم ذلك في الغالب عند استيفاء الرصيد الشهري للبطاقة وبعدها يقوم التاجر بالحصول على قيمة الفاتورة من البنك المصدر للبطاقة[3].
- **تزوير الإشعارات والفواتير الناتجة عن عملية البيع:** وتحصل في الغالب مع كبار السن بمغافلة التاجر له، بعد استعماله بطاقة الائتمان في شراء بعض السلع فيحصل على بصمته على إشعار حال من البيانات ثم يقوم بتسجيل المبلغ الذي يريده أو يقوم التاجر بتزوير مبالغ الإشعارات بإضافة مبالغ وهمية على الإشعارات[4].
- **تلاعب التاجر في ماكينات البيع الإلكترونية:** كأن يقوم التاجر باستغلال الماكينة اليدوية في الحصول على أكثر من إشعار دون علم صاحب البطاقة، بحيث يكون مطبوع غليها بيانات البطاقة وثم تقليد توقيع صاحب البطاقة على تلك الإشعارات من أجل أن يتم تحصيل

(1) نوال الحاج مخناش، رشيد شميشم، "التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني"، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01، ص 1122.

(2) نوال الحاج مخناش، رشيد شميشم، المرجع السابق، ص 1123.

(3) مهند فايز دويكات، حسين محمد شبلي، المرجع السابق، ص66.

(4) نفس المرجع السابق، ص67.

قيمتها من البنك فيما بعد بأن يقوم بالتلاعب بتلك الإشعارات مرة والصورة مرة أخرى، كما يقوم باستخدام بطاقة مسروقة أو منتهية الصلاحية عن طريق العبث بماكينة البيع الإلكتروني المسلمة إليه والقيام بعملية البيع الوهمية، وقيامه بتزوير توقيعات أصحاب البطاقات والاستفادة منها بتحصيل قيمتها مرة أخرى من البنك[1].

ب-إصدار بطاقات صحيحة بمستندات مزورة: حيث يقوم المحتالون في هذه الحالة بالتقدم إلى فروع البنك بمستندات إثبات الشخصية مزورة للحصول على بطاقات ائتمان بعناوين وهمية وأسماء منتحلة، من أجل القيام بعمليات سريعة ومتتالية وتستهدف هذه العملية الاستيلاء على أكثر من بطاقة من بنك بأسماء منتحلة وبيانات منتحلة مستغلين بذلك ضعف خبرة بعض موظفي البنك في كشف التزوير المستندات والوثائق[2].

ثالثا: أدوات التزوير

تختلف أدوات التزوير حسب دور كل منهما:

1-**جهاز المسح:** يستعمل لاستنساخ معلومات الحساب من الشريط الممغنط، وهو جهاز صغير يمكن حمله في راحة اليد ويستطيع تخزين ما يقارب مئة رقم حساب منسوخ من البطاقة الأصلية.

2-منظم سايون: هو جهاز يدوي يستقبل المعلومات ويخزنها من الجهاز الممغنط الموصول برأسه ليتمكن من قراءة البيانات الموجودة على الشريط المغناطيسي في البطاقة البلاستيكية[3].

3-المشفرة: وهو جهاز يستخدم لتشفير البطاقات المسروقة أو المفقودة أو المزورة، ويمكن شراءه من المتاجر الإلكترونية ويحتويعلى رأس للكتابة على الشريط الممغنط عند تمرير البطاقة من خلال الفتحة.

(1)مهند فايز دويكات، حسين محمد شبلي، المرجع السابق، 67.

(2) نفس المرجع السابق، ص67.

(3) خولة بوقديرة، المرجع السابق، ص35.

4-جهاز التسجيل المغناطيسي: يقوم هذا الجهاز بتسجيل المعلومات التي تم الحصول عليها من الأشرطة الممغنطة للبطاقة المزورة أو المسروقة أو المفقودة، بحيث يتم توصيله بجهاز الكومبيوتر على الشريط الممغنط وتسجيل أرقام الحساب التي تم نسخها سابقا حيث أن هذه العملية تظهر البطاقة الحقيقية على الجهاز الإلكتروني عند تمريرها فيه.

5-جهاز الطبع بحروف نافرة أو اطلاعها: ويستعمل لطباعةرقم الحساب والمعلومات حروف نافرة على الوجه الأمامي للبطاقة يتم طلائها باللون الفضي والذهبي والأسود، وهذا الجهاز يحتوي على جميع الأرقام التي تم طلائها[1].

الفرع الثاني: استعمال وسائل الدفع الإلكتروني المزورة

جرمت التشريعات الجزائية العربية عامة والجزائرية خاصة تزوير المحررات واستعمالها سواء في الدفع أو الوفاء حتى ولو لم يكن المستعمل للمحرر المزور هو نفسه من زوره.

أولا: استعمال البطاقة المزورة من قبل الغير

ولقد أجمعا الفقه والقضاء على المساءلة الجزائية لكل من استعمل بطاقة ائتمان إلكترونية مزورة سواء بالسحب أو بالوفاء، إلا أنهم اختلفوا فيما بينهم حول نوع الجريمة التي يسأل حسبها المستعمل.

1- **الرأي الأول:** تم تكييف هذه الجريمة على أنها "جريمة السرقة باستعمال مفتاح مصطنع" استنادا إلى المادة 07/353 من قانون العقوبات الجزائري[2]، لأن المال خرج عن حيازة المجني عليه حامل البطاقة دون رضاه واعتبروا أن البطاقة المزورة تعد من قبيل المفتاح المصطنع في جريمة السرقة وما يدعم هذا الرأي أن البطاقة حسبهم ليست محررا للإثبات وإنما أداة ائتمان فليس ثمة تزوير في الأمر، لذلك لا يمكن الحديث عن استعمال محرر مزور[3].

(1) خولة بوقديرة، المرجع السابق، ص 35،36.

(2) أنظر المادة 07/353 من قانون العقوبات .

(3) منال بتة، أمال قبلي، المرجع السابق، ص 85.

إلا أن هذا الرأي تعرض للنقد من طرف غالبية الفقهاء مستندين في أن تسليم النقود قد تم إراديا من قبل الجهاز الآلي لتوزيع النقود بمجرد إدخال البطاقة الإلكترونية في الجهاز وكتابة الرقم السري لها، كما أن هذه البطاقة الائتمانية الإلكترونية لا تعد ولو حكما مفتاحا مصطنعا، لأن المفتاح المصطنع يعرف على أنه تلك الأداة المستخدمة من قبل الجاني لفتح الباب الخارجي للمكان، كما أن هذا المفتاح يستخدم إلى الدخول إلى المكان الذي سوف تقوم فيه عملية السرقة، وهو ما لا يتحقق في بطاقة الائتمان الإلكترونية فهي لا تستعمل لدخول إلى مثل هذا المكان بل هي أداة الجريمة نفسها، أضف إلى ذلك المبادئ العامة في القانون الجنائي تمنع القياس في النصوص القانونية التجريمية[1].

2- **الرأي الثاني:** تم تكييف هذه الجريمة على أنها "جريمة النصب" إذا قام أحد الأفراد باستعمال بطاقة إلكترونية مزورة سواء في السحب أو في الوفاء فإنه يعد مرتكب لجريمة الاحتيال والدليل على ذلك هو استخدام طرق احتيالية لخداع الجهاز الآلي الذي يقوم بدوره بسحب النقود وإيهام التاجر بوجود ائتمان بهدف الحصول على السلع والخدمات[2].

3- **الرأي الثالث:** تم تكيف هذه الجريمة على أنها "جريمة استعمال محرر مزور": يرى هذا الرأي بأن استعمال بطاقة ائتمان إلكترونية مزورة يشكل جريمة استعمال محرر مزور وذلك لتوافر أركان هذه الجريمة، لأن موضوع الجريمة يرد على محرر مزور وهو هنا بطاقة الائتمان الإلكترونية المزورة، لما يشترط في النشاط المادي لجريمة استعمال المحرر المزور أن يحتج بالمحرر المزور على أنه صحيح وهو ما حدث في هذه الواقعة، كما يشترط أن ينخدع التاجر أو الجهاز الآلي بها وهو ما حدث بالفعل حيث تمكن من السحب أو الوفاء بعد الاستعانة بالبيانات التي تضمنتها البطاقة المزورة للتأثير على التاجر من أجل قبول البطاقة في الوفاء[3].

(1) منال بتة، المرجع السابق، ص 86.

(2) راشد بن صالح بن سفيان الراشدي، المرجع السابق، ص 127.

(3) نفس المرجع السابق، ص128.

ثانيا: جريمة استعمال بطاقة ائتمان إلكترونية مزورة من قبل مزورها

في معظم الأحيان من يقوم بتزوير بطاقة الائتمان الإلكترونية هو نفسه من يقوم باستعمالها سواء في السحب أو الوفاء، وفي هذه الحالة نكون أمام مجموعة من جرائم وهي ارتكاب جريمة تزوير محرر زائد ارتكاب الجريمة استعمال محرر مزور[1]،وهذا التعدد للجرائم قد يكون تعددا معنويا، وذلك إذا تم التزوير والاستعمال بفعل واحد كأن يوقع المتهم على الفواتير لدى أحد التجار. فقد تم تزوير توقيع واستعمال للبطاقة في آن واحد وفي هذه الحالة يعاقب الجاني على الفعل الأشد، كما يمكن أن يكون هذا التعدد إذ ما ارتكبت الجريمة بفعلين مستقلين، وهذا التعدد قد يكون مرتبطا ارتباطا غير قابل للتجزئة في حالة ارتكاب جريمتين لغرض واحد، كما يمكن أن يكون ارتباطا بسيطا إذا لم يكن للجريمتين لغرض واحد[2].

المطلب الثاني

استخدام الغير لبطاقة الدفع الإلكتروني صحيحة "المسروقة أو المفقودة"

من بين أهم المشاكل التي تعترض التعامل ببطاقات الدفع الإلكتروني سرقة هذه الأخيرة أو ضياعها ومن ثم استخدامها من قبل سارقها أو واجدها استخداما غير مشروع في السحب من الموزعات الآلية كما يستخدمها في الوفاء لدى التجار المعتمدين بدلا من أن يقوم بتسليمها إلى المصدر، أو الحامل الشرعي لها[3].

الفرع الأول: جريمة سرقة بطاقة الدفع ورقمها السري

من الاعتداءات التي تقع على البطاقة الائتمانية باعتبارها محل للحقوق مالية سرقة البطاقة فالسارق سواء استعمل البطاقة أو لم يستعملها فهو يعد مرتكبا لجريمة السرقة لمجرد توافر أركان هذه الجريمة.

(1) منال بتة، أمال قبلي، نفس المرجع السابق، ص 87.

(2) راشد بن صالح بن سفيان الراشدي، المرجع السابق، ص 129.

(3) رزقان هشام، المرجع السابق، ص 41.

أولا: جريمة سرقة البطاقة

عرفها المشرع الجزائري في نص المادة 350 منه بأنها: اختلاس مال منقول مملوك للغير بنية تملكه[1]، ومنه فجريمة السرقة تقوم على ركنان سنقوم بتفصيلهما على النحو التالي:

1- الركن المادي: ويقوم هذا الركن على الفعل الأخر كنشاط إجرامي يؤدي إلى حيازة السارق للشيء محل السرقة بأخذه من مالكه دون رضاه أو علمه أو بعلمه، ولكن دون رضاه إذا تعرض للإكراه والتهديد من قبل السارق[2]، فهذا التعريف يبرز عنصرين عنصر الحيازة وعنصر مادي وهو عملية النزع والاستيلاء فلا يكتمل الاختلاس إلا بالحيازة ولا تكتمل الحيازة إلا بالفعل المادي[3].

1- **الركن المعنوي:** ويتمثل في عنصري الإرادة والعلم معا أي العلم بكافة عناصر الجريمة والمتمثلة في المال المسروق مملوك للغير المأخوذ بإرادة حرة وسليمة خالية من أي عيب يعدمها أو يعيبها وبهذا يتوفر القصد العام[4]، إضافة إلى القصد الخاص وهو نية الشخص في تملك الشيء المختلس والتصرف فيه بصفة المالك الأصلي[5].

ثانيا: سرقة الرقم السري لبطاقة الدفع الإلكتروني

يقوم الغير بجريمة الاعتداء على البطاقة الإلكترونية فيسرق رقمها السري إلا أن هذا الأمر لا يكون وليد الصدفة بل وجب توفر عدة عوامل -وهذا ما يسأل عنه جزائيا- بحيث يقوم باستخدامه في مختلف العمليات المصرفية.

1-عوامل الحصول على الرقم السري

(1) لعليلي زوبيدة، الحماية الجنائية لبطاقة الائتمان المصرفية، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، تخصص قانون عام للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق سنة 2014/ 2015، ص 11.

(2) منال بتة، المرجع السابق، ص 79.

(3) لعليلي زوبيدة، المرجع السابق، ص 12.

(4) منال بتة، نفس المرجع السابق، ص 79.

(5) لعليلي زوبيدة، نفس المرجع السابق، ص16.

أ-إهمال الحامل: ويحصل هذا الإهمال في حالة كتابة الرقم السري على وجه البطاقة من قبل حاملها وتركه عرضة لأعين الغير الذي يتمكن من معرفته بكل سهولة كما يمكن أن يقوم الحامل الشرعي بقراءة وتكرار الرقم السري على مسمع الغير أثناء قيامه بعملية سحب النقود[1].

ب- التجسس: وتتم هذه العملية وفق طريقتين:

- وضعكاميرات المراقبة على أجهزة الصراف الآلي التي تقوم بتصوير الأرقام السرية عند إدخالها.
- وضع جهاز إلكتروني في مكان ما على الصراف الآلي حيث يقوم بنقل الرقم السري لجهاز في آخر لحظة إدخاله من قبل حامله[2].

ج-القرصنة: وذلك من خلال الدخول إلى أجهزة الكمبيوتر التي يتم فيها حفظ بيانات العملاء وأرقام بطاقاتهم وذلك بصورة غير قانونية[3].

2-سرقة أرقام بطاقات الدفع عبر الانترنت

من المعلوم أنه إلى جانب الاستعمال الواسع للبطاقات الإلكترونية خلال التعاملات العادية والمألوفة والتي تتم عند التواجد الفعلي للمتعاقدين من حيث المكان والزمان، هناك استعمال واسع أيضا لهذه البطاقة عبر شبكة الانترنت والتي تستعمل فيها البطاقة الإلكترونية بطرق غير مباشرة تقوم على أساس التعاقد عن بعد، وهنا تكمن سهولة التحايل من قبل الغير عبر شبكة الانترنت في كون عملية التعريف بالبطاقة تتم عن طريق المشتري عند السداد، أيضا يكون عبر خطوط اتصال بالانترنت، وهنا بالذات تتعرض المعلومات السرية الخاصة بالبطاقة ورقمها السري لعملية الكشف عنها، وبالتالي استخدام هذه المعلومات من قبل الغير للحصول على أموال دون وجه حق[4].

(1) وسام فيصل محمود شواورة، المرجع السابق، ص 100.

(2) عبد الكريم ردايدة ، المرجع السابق، ص 70.

(3) خولة بوقديرة، المرجع السابق، ص 39.

(4) حوالف عبد الصمد، المرجع السابق، ص 338.

أ- مفهوم الاستخدام الغير شرعي لوسيلة الدفع الإلكتروني عبر الانترنت

يضع بعض الفقهاء تعريفا للاستخدام الغير مشروع لوسيلة الدفع الإلكتروني عبر الانترنت بأنه: "عندما يخل الحامل بشروط عقد إصدار البطاقة مما يؤدي إلى فسخ هذا العقد أو قفل الحساب الذي تقوم البطاقة بتشغيله حيث يسأل الحامل لمجرد امتناعه عن ردها أو استمراره في استخدامها بعد إلغائها من البنك المصدر لها أو استمراره في استخدامها بعد انتهاء مدة الصلاحية[1].

يشوب هذا التعريف عيب من حيث المحدودية حيث أنه تناول حالة واحدة من حالات الاستخدام غير المشروع لبطاقة الدفع الإلكتروني وهو حالة استخدامها من قبل الحامل، فقد استبعد حالات التاجر والغير والمصدر في بعض الأحيان لها فإنه من الصعب وضع تعريف للاستخدام الغير مشروع لبطاقة الدفع الإلكتروني وتحديد ماهيته تحديدا دقيقا، حيث أن هذا الاستخدام الغير مشروع هو عبارة عن حالة أو حالات تختلف باختلاف الشخص أو الجهة التي قامت بمزاولته، كما أن هذه الحالات تختلف بتطور وسائل حماية البطاقة فقد تظهر حالات استخدام غير مشروعة في المستقبل غير معروفة في الوقت الراهن[2].

ب- صور الاعتداء على نظام بطاقة الائتمان من خلال شبكة الانترنت

تقوم عملية الدفع الإلكتروني من خلال شبكة الانترنت بعد أن يدخل العميل عن طريق تلك الشبكة التي تعرض منتجاتها وعند رغبته في الشراء يقوم بملء نموذج مطبوع على أعلى تلك الصفحة بحيث يقوم بتدوين جميع بيانات البطاقة والعنوان التي ترسل إليه، فهذا النوع من الشراء يطلق عليه اسم التجارة الإلكترونية وقد يحدث بعض تلاعب من مستخدمي هذه الشبكة في مثل هذه العمليات بهدف حصولهم على البيانات الخاصة بالبطاقة بأساليب احتيالية نذكر منها:

(1) حوالف عبد الصمد، المرجع السابق ، ص 339.

(2) نفس المرجع السابق ، ص 339.

1- **أسلوب الخداع:** عن طريق إنشاء مواقع وهمية على شبكة الانترنت بحيث يظهر الموقع وكأنه حقيقي لإحدى الشركات الكبرى ويبدأ باستقبال تعاملات الموقع الأصلي وبعد حصوله على الأموال يقوم بغلقه.

2- **أسلوب التجسس:** حيث يقوم قراصنة الانترنت بوضع برامج تتيح لهم الإطلاع على للبيانات ومعلومات الشركات الكبرى للحصول على أرقام بطاقة الائتمان ويعد طريقة غير مشروعة.

3- **أسلوب تفجير الموقع المستهدف:**بتزويد الحاسب بمعلومات فوق طاقته التخزينية الأمر الذي يؤدي إلى تبعثر البيانات المخزنة فتنقل إلى الجهاز الخاص بالفاعل وترتكب هذه الطريقة الإجرامية على مواقع المؤسسات المالية والفنادق والشركات الكبرى[1].

4- **الاختراق الغير مشروع لمنظومة خطوط الاتصالات العالمية:** وهي الخطوط التي تربط الحاسب الآلي للمشتري بذلك الخاص بالتاجر، ويقوم الجاني هنا بالتصنت على المكالمات الهاتفية، وهذا أخطر أسلوب يهدد التجارة الإلكترونية لأن الدافع الأساسي من وراءه هو رغبة مخترقي إجرام التقنية وقراصنة البطاقات هو قهر النظم التقنية والتفوق على الحماية المقررة لها بحيث تقوم هذه العصابات الإجرامية بنشر هذه المعاملات وبيان كيفية الحصول على الأرقام الخاصة ببطاقات الوفاء المملوكة للغير وذلك عبر مواقعهم على شبكة الانترنت.

5- **تخليق أرقام البطاقة:** يعتمد هذا الأسلوب على الأسس الرياضية في تبديل وتوفيق لأرقام حسابية تؤدي في النهاية لناتج معين وهو الرقم السري لبطاقة الوفاء المتداولة، ويتم استخدامها في المعاملات غير المشروعة عبر شبكة الانترنت ومن هنا تأتي خطورة أن يكون رمز البطاقة أو رقمها السري هو الضمان الوحيد لعدم اختراقها أو إساءة استعمالها[2].

(1) مونية معروف، جرائم بطاقات الائتمان الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر شعبة حقوق، تخصص قانون جنائي للأعمال، كلية الحقوق العلوم السياسية، جامعة العربي بن مهيدي، أم البواقي2015/2014، ص 49.

(2) حوالف عبد الصمد، المرجع السابق، ص 343.

6- **أسلوب الإيهام:** هو تحصيل البيانات والمعلومات للأشخاص مع أرقام بطاقاتهم الائتمانية عن طريق إرسال رسائل إلى زبائن أحد المواقع الإلكترونية بحجة أن الموقع بحالة تحديث وبعد ذلك يقوم المجرمون باستخدام تلك الأرقام في الشراء عبر شبكة الانترنت[1].

7- **تبادل المعلومات:** تبادل المعلومات هي أفضل طريقة بين قراصنة الكمبيوتر من أجل الدخول الغير مشروع للحصول على المعلومات والبيانات فيما بينهم من أجل التوسع في استخدام الأرقام، ويكون هذا لاستخدام صادر من بلدان مختلفة وفي سبيل التقليل من الاستخدام الغير مشروع لهذه البطاقات من قبل الغير قامت العديد من الشركات بتطوير خدمات الدفع الإلكتروني لتلاءم التعامل مع شبكة الانترنت، كما قامت بعض البنوك أيضا بإصدار بطاقات خاصة للاستعمال عبر شبكة الانترنت مدفوعة مقدما بحيث إذا تعرضت المعلومات السرية إلى السرقة أو الكشف وتم الاستيلاء على النقود كانت الخسائر محدودة، غير أن هذا يبقى نسبي الفعالية بالنظر إلى آلاف العمليات التي تتم يوميا عبر شبكة الانترنت والمقدرة بمئات الملايين[2].

ثالثا: استخدام البطاقة المسروقة

يقصد بهذا الاستخدام أن يقوم الشخص الذي سرق البطاقة بتسليمها إلى الغير من أجل استعمالها ونفرق بين حالتين من الاستعمال:

1- **استلام الجاني للبطاقة المسروقة مع عمله برقمها السري:** يسأل الجاني جنائيا عن جريمة النصب مع استعمال البطاقة المسروقة أو المفقودة في سحب النقود أو الوفاء للتاجر، لأنه في حالة استخدام البطاقة المسروقة قد انتحل اسما كاذبا على أساس أنه اسم صاحب البطاقة الحقيقي وهو أحد طرق النصب[3].

---

(1) مونية معروف، المرجع السابق، ص 49.

(2) حوالف عبد الصمد، نفس المرجع السابق، ص 344.

(3) محمود أحمد طه، المسؤولية الجنائية غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، كلية الشريعة والقانون غرفة الصناعة، دبي، جامعة الإمارات العربية المتحدة، أيام 13 و12 مايو 2003، ص 115.

كما يمكن أن يسأل عن جريمة اختفاء الأشياء لأنه على دراية بأن البطاقة مسروقة وقام بالاحتفاظ بها[1]، وفقا لنص المادة 387 من قانون العقوبات[2]، كما يمكن أن يسأل عن جريمة التزوير عند استعماله للبطاقة في الوفاء لأنه يقوم بالتوقيع باسم صاحب البطاقة حتى يدفع البنك ثمن مستحقاته[3].

2- **استلام البطاقة المسروقة دون معرفة رقمها السري:** في هذه الحالة فإن الجاني يسأل عن جريمة اختفاء الأشياء لأنه على دراية بأن البطاقة مسروقة، ولا يمكن أن يسأل عن جريمة استخدام البطاقة لأنه لا يعرف رقمها السري وفي حالة إذا حاول استخدامها في السحب والوفاء فإنه يسأل في حدود جريمة الشروع في عملية الاحتيال، فإذا قام الجاني بإدخال الرقم السري خاطئ أكثر من ثلاث مرات فتسحب البطاقة منه لأن بهذه الصراف الآلي ذاكرة مبرمجة على سحب البطاقة في مثل هذه الحالات[4]. أما بالنسبة لسارق البطاقة الذي قدمها للغير ولا تقع عليه أي مسؤولية إذا سلم البطاقة للغير على أنه حاملها الشرعي، أما إذا سلمها للغير مع علمه بأنه ليس مالكها، فهنا يسأل عن جريمة السرقة كما يسأل أيضا عن جريمة الاحتيال والتزوير باعتباره شريكا في الجريمة[5].

الفرع الثاني: جريمة استعمال بطاقة الدفع المفقودة

في هذه الجريمة لم يقم الغير بالاعتداء على بطاقة الدفع الإلكتروني بالسرقة من صاحبها بل عثر عليها، فقد تكون هذه البطاقة إما مسروقة أو مفقودة ولم يقم بإرجاعها إلى صاحبها الشرعي أو الجهة المصدرة لها.

أولا: حالات استخدام البطاقة المفقودة

(1) علي عدنان الفيل، المرجع السابق، ص 59،60.

(2) أنظر المادة 387 من قانون العقوبات الجزائري.

(3) خولة بوقديرة، المرجع السابق، ص 43.

(4) أمجد حمدان الجهني، المرجع السابق. ص181.

(5) علي عدنان الفيل، المرجع السابق، ص 61.

في غالب الأحيان يصادف الغير أن يحصل على بطاقة ائتمان مفقودة أو ضائعة فيقوم باستعمالها وهنا نميز بين حالتين:

1- **استعمال البطاقة من طرف الشخص الذي عثر عليها:** في حالة احتفاظ الشخص الذي عثر على البطاقة واستخدمها لمصلحته الشخصية فإن يعاقب على جريمة الاحتيال لأنه انتحل لصفات كاذبة واستخدم البطاقة في الحصول على ما يريد من السلع والخدمات وكما يمكن أن يسأل على جريمة التزوير إذا قام بالتوقيع على سندات البيع[1].

2- **عدم استعمال البطاقة من طرف الشخص الذي عثر عليها ومنحها لشخص آخر:** قد يقرر من عثر على البطاقة الإلكترونية بأن لا يحتفظ بها ويسلمها للغير، وهنا هذا الأخير أن يكون مالكا أو قد يكون غير ذلك.

أ-**تسليم البطاقة لشخص يدعي أنه مالكها:** يعتقد الشخص الذي عثر على البطاقة أنه قد سلمها إلى الشخص الصحيح وهو مالكها، ولكنه قد يقع ضحية إدعاءات كاذبة من قبل شخص آخر من أجل الحصول عليها بغرض الاستيلاء عليها وفي هذه الحالة لا تقع عليه أي مسؤولية لأنه حسن النية[2].

ب-**تسليم البطاقة لمالكها مع العلم بذلك:** في هذه الحالة يعتبر الشخص الذي يسلم البطاقة شريك في الجريمة لأنه سيء النية، أما الغير الذي استلم البطاقة فتقع عليه مسؤولية ويعاقب عن جريمة السرقة كما يسأل عن جريمة الاحتيال في مواجهة من عثر على البطاقة وسلمها إياه على أساس أنه صاحبها وأيضا في مواجهة التاجر عندما يقدم له الخدمات والسلع على أساس أنه الحامل الشرعي ويسأل عن جريمة التزوير في حالة استخدام التوقيع الشخصي[3].

ثانيا: استخدام بطاقات الائتمان المسروقة أو المفقودة في السحب أو الوفاء

(1) عبد الكريم الردايدة، المرجع السابق، ص ص244،245.

(2) علي عدنان الفيل، المرجع السابق، ص60.

(3) عبد الكريم الردايدة، المرجع السابق، ص246.

يمكن أن تستخدم البطاقات المسروقة أو المفقودة في سحب النقود من أجهزة السحب أو في الوفاء بقيمة المشتريات أو الخدمات التي حصل عليها المستخدم الغير شرعي من التجار.

1-استخدام البطاقات المسروقة أو المفقودة في سحب النقود: من أجل استخدام البطاقات المسروقة أو المفقودة في الصراف الآلي فإنه يجب توفر الرقم السري لهذه البطاقات وإلا لا تتم عملية السحب، وفي حالة إدخال الرقم السري خاطئ أكثر من ثلاث مرات فتسحب البطاقة من مستخدمها[1].

إن الاستخدام الغير مشروع للبطاقة المسروقة أو المفقودة يعد جريمة احتيال وليس جريمة السرقة لأن التسليم النقود بواسطة هذه الأجهزة يكون إراديا مما ينفي وجود أركان السرقة، ولكن يمكن أن تنسب إلى الفاعل جريمة سرقة البطاقة ذاتها والشفرة الخاصة بها فبذلك يرتكب جريمتين مستقلتين عن بعضهما البعض وهما السرقة (جريمة الوسيلة) أو الاحتيال (جريمة الغاية) ويتطبق في هذه الحالة العقوبة الأشد[2].

2-استخدام بطاقة الائتمان المسروقة أو المفقودة كأداة وفاء: كما تستخدم بطاقة الائتمان في سحب النقود فإنها تستخدم أيضا كأداة وفاء من قبل حاملها الغير شرعي، ويتم استخدام البطاقة في هذه الحالة كأداة وفاء لدى التجار الذين يستخدمون الآلة اليدوية أي أنه لا حاجة إلى الرقم السري الخاص بالبطاقة إذ يكتفي بتوقيع حاملها على الفاتورة وهذا ما سهل استخدامها من قبل الحامل الغير شرعي لها لأنه يصعب على التاجر معرفة إذا تم توقيع هذه البطاقة أم لا، كما يصعب عليه أيضا معرفة ما إذا كان التوقيع الموجود على البطاقة مخالف للتوقيع الموجود على الفاتورة وهذا راجع لنقله خبرة التاجر، وفي هذه الحالة يكون الفاعل مرتكبا لجريمة الاحتيال باتخاذه الصفة الغير صحيحة وانتحال الاسم الكاذب، وكذلك تقوم جريمة التزوير

(1) جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقة الائتمان الممغنطة(دراسة تطبيقية في القضاء الفرنسي والقانون المصري)، دار النهضة العربية مصر، 1999، ص91.

(2) عبد الجبار الحنيص، "الاستخدام غير مشروع لبطاقات الائتمان الممغنطة من وجهة نظر القانون الجزائي"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، المجلد 26، العدد الأول، سنة 2010، ص82 .

أيضا بتوقيع الفاعل على الفاتورة وبذلك يكون قد قلد توقيع الحامل الشرعي وهنا يقتضي تطبيق العقوبة الأشد لقيام جريمتين في آن واحد[1].

(1) ن عبد الجبار الحنيص ، المرجع السابق، ص ص84،83.

الفصل الثاني
الحماية القانونية لبطاقات الدفع الالكتروني من الاستخدام الغير مشروع

تعتبر جرائم بطاقات الدفع الالكتروني باختلاف صورها وأساليبها من الجرائم المستحدثة في العصر الحالي، والتي أصبحت تمس كيان الدول والمجتمعات على المستويين المحلي والدولي مما أدى بالبعض إلى تصنيفها من بين الجرائم المنظمة العابرة للحدود، وجراء المخاطر التي يمكن أن تترتب على إساءة استخدام باقات الدفع الالكتروني كان لابد من البحث عن السبل الكفيلة لإخراج هذه الوسائل الجديدة من دائرة الخطر الذي يمكن أن تعيق تطورها وتقف عائقا أمام توجه المستهلكين نحو استخدامها وهذا الأمر يتطلب البحث عن الحلول وإتباع آليات وإجراءات مختلفة من قبل محيطها، إضافة إلى تكريس نوعين من الحماية، حمايةداخلية عن طريق سن مختلف الدول بما فيها الجزائر قوانين وتشريعات تحمي مستعملي بطاقات الدفع الالكتروني، وأخرى دولية لحماية المعاملات المالية الالكترونية وعليه ارتأينا تقسيم هذا الفصل إلى مبحثين، حيث تضمن (المبحث الأول) الإجراءات الوقائية والأمنية المتبعة لحماية بطاقة الدفعالكتروني، أما (المبحث الثاني) يندرج تحت عنوان قواعد الحماية القانونية الداخلية والدولية لبطاقات الدفع الالكترونية.

المبحث الأول

الإجراءات الوقائية والأمنية المتبعة لحماية بطاقات الدفع الالكتروني

إن جرائم بطاقات الائتمان الالكترونية من أخطر المشكلات التي تواجه الأنظمة الاقتصادية، وقد شهدت في الآونة الأخيرة تزايدا ملحوظا في عمليات الاستخدام غير المشروع لها، هذا ما دفع بأطراف البطاقة والجهاز الأمني إلى انتهاج أساليب وقائية وأخرى أمنية، للحد من هذه الاعتداءات وعليه سنفصل في (المطلب الأول) الإجراءات الوقائية المتخذة من قبل أطراف البطاقة، أما في (المطلب الثاني) فسنتناول الإجراءات الأمينة المتخذة لمواجهة مخاطر بطاقة الدفع الالكتروني.

المطلب الأول

الإجراءات الوقائية المتبعة من قبل أطراف بطاقة الدفع الإلكتروني

من أجل ضمان سلامة وأمن المعاملات المصرفية ببطاقة الدفع الإلكتروني ووقف الممارسات الغير مشروعة عليها، كان لابد من إتباع وسائل وقائية من طرف الجهة المصدرة للبطاقة (الفرع الأول)، إضافة إلى الحامل والمستفيد من البطاقة (الفرع الثاني)، ولا تقتصر هذه الإجراءات على هذين الطرفين فقط،بل يجب أن تتضافر جميع الجهود بن أطراف البطاقة، لتمتد بذلك إلى التاجر (الفرع الثالث) وسنفصل في ذلك على النحو التالي:

الفرع الأول: الإجراءات الوقائية المتخذة من قبل المُصدّر

تتمثل الإجراءات التي يقوم بها المصدر من أجل حماية البطاقات من الاستخدامات الغير مشروعة المصاحبة لها، إما بتطويرها تقنيا أو القيام بإجراءات أخرى، وسوف نتناول الإجراءات التقنية (أولا) ثم الإجراءات الإدارية (ثانيا) وطرق الحماية والرقابة الأخرى (ثالثا).

أولا: الإجراءات التقنية

سوف نقوم بمحاولة إيجاز أهم الإجراءات التقنية المتخذة لمواجهة إساءة استخدام بطاقة الدفع الالكتروني:

1-أول حلقات هذا التطور كان باختراع بطاقة ذات دوائر الكترونية، من مزاياها أنها غير قابلة لتأثير عيها، أو اختراقها أو تزويرها حيث تحتفظ في ذاكرتها بآخر العمليات المنفذة عليها، وتعد من الناحية التقنية غير قابلة للتزوير ومثالها صورة الحمامة في بطاقة الفيزا[1].

2-وثاني حلقات التطوير تتمثل في إدخال البطاقة الالكترونية الذكية "smart card"، وهي عبارة عن بطاقة بلاستيكية من حجم بطاقة الدفع الالكتروني، وتضع شرائح ذات دوائر متكاملة قادرة على تخزين البيانات ومعالجتها[2].

3-وكذلك من بين الإجراءات التقنية المتبعة نجد النموذج التقني الموحد الذي أعلنت عنه شركتي فيزا "visa" وماستر كارد "master card" بتاريخ 1996/2/1 والمسمى نظام الصفقات الالكترونية الآمنة وبعد ذلك انضمت لهذا المشروع شركة أمريكية أخرى[3].

4-وقد ابتكرت منظمة فيزا الدولية بطاقة ذكية حديثة، تحتوي على ذاكرة الكترونية ومعالج صغير جدا (micro processon)، حيث يمكن لهذه البطاقة تخليق أرقام سرية مختلفة، عقب كل عملية شراء يتم استخدام البطاقة فيها بمجرد الضغط بالأصبع على المعالج، وذلك لتأمين عمليات التعامل بالبطاقة سواء كانت العمليات مباشرة مع التاجر أو من خلال الهاتف أو البريد الالكتروني [4].

(1) مونية معروف، المرجع السابق، ص76.
(2) أمجد حمدان الجهني، المرجع السابق، ص112.
(3) علي عدنان الفيل، المرجع السابق، ص77.
(4) بن تركي ليلى، المرجع السابق، ص313.

5-وتتأهب حاليا شركة أمريكية وهي شركة (ابلايد ديجيتال سوليوشينز) (lds) والتي عرفت بتطوير رقائق تزرع تحت الجلد لتحديد الهوية الشخصية للتعرف على موقع حامليها، لتأمين طريقة موثوقة لزبائنها لتفادي الغش، بتوظيف الرقائق في تعاملات الدفع ببطاقة الائتمان الالكترونية، وأسمتها (رقيقة فيبريتشيب)[1].

ثانيا: الإجراءات الإدارية

تتمثل هذه الإجراءات إما بتحديد حد أقصى لاستخدام البطاقة، أو سحبها، أو إعداد كشف بأرقام البطاقات الممنوع قبولها على النحو التالي:

1-تحديد الصعوبات ضمن سقف البطاقة:

إن الهدف من وضع سقف للبطاقة يمكن تجازوه في حالات معينة وهي الحد من الإفراط في المشتريات من قبل الحامل، والتقليل من الخسائر التي يمكن أن تنتج عند وقوع البطاقة في يد الغير، بالإضافة إلى تحديد الحد الأقصى لاستخدام البطاقة والذي يكون في حالتين[2]:

أ-الحد الأقصى لاستخدام البطاقة في الوفاء: وهنا نفرق بين الجهاز اليدوي لطباعة، و جهاز البيع الالكتروني:

*عند استخدام البطاقة في الجهاز اليدوي يكون السقف صفر، ويجب الحصول على ترخيص من المصدر عند كل عملية، كما يتوجب على التاجر حفظ رقم التفويض على الفاتورة لأنه لا يعلم برصيد البطاقة.

(1) علي عدنان الفيل، المرجع السابق، ص78.

(2) أمجد حمدان الجهني، المرجع السابق، ص115.

*عند استخدام البطاقة في الجهاز الالكتروني يظهر على الشاشة إذا ما كان الرصيد كافي لإتمام عملية أم لا، وإذا تجاوز الرصيد الحد يرفض الجهاز إتمام العملية إلا بعد حصول التاجر على الموافقة من المصدر[1].

ب-الحد الأقصى لاستخدام البطاقة في السحب:

يتم تحديد السقف الأقصى للبطاقة عند السحب من أجهزة الصراف الآلي، حسب المبلغ المسموح به من الرصيد، ففي بطاقة الدفع الإلكتروني العادية يكون بمقدار نصف سقف البطاقة، وفي بطاقات الصراف الآلي التي تستخدم في الوفاء، يكون بمقدار الرصيد المتوافر في الحساب وبالنسبة للحد الأقصى في المقدار اليومي فهو يختلف من بنك لآخر ويتراوح هذا المقدار ب (500-1000) دينار، ويحق لهذه البنوك أن تسمح لحامل بطاقة الصّراف الآلي بتجاوز رصيده في السحب وفق حالات معينة ووفق ضمانات[2].

2-سحب البطاقة:

تسحب البطاقة من الحامل من أجل محافظة المصدر على حقوقه، ولضمان عدم استعمالها بطريقة غير مشروعة بعد إلغائها، ويكون السحب لأسباب جوهرية، وإلا عد المصدر متعسفا ووجب عليه التعويض[3].

أ-سحب البطاقة عن طريق المُصدر

إن سحب البطاقة يكون إما بالطلب من المُصدر بالطرق العادية، كما يمكن أن يكون بالطرق الفنية كبرمجة الصراف الآلي على سحب البطاقة في الحالات التالية:

(1) خولة بوقديرة، المرجع السابق، ص50.

(2) أمجد حمدان الجهني، المرجع السابق، ص116.

(3) منال تبة، أمال قبلي، المرجع السابق، ص39.

-إذا تم إدخال الرقم السري خاطئ ثلاث مرات.

-أذا لم يقم الحامل باستلام البطاقة بعد إعادتها له من جهاز الصراف الآلي بحوالي 30 ثانية.

-إذا تم الإبلاغ عن السرقة أو فقدان البطاقة، يقوم البنك ببرمجة الصراف الآلي على عدم قبول البطاقة وسحبها وعدم إعادتها[1].

ب- سحب البطاقة من قبل التاجر

وتسحب البطاقة في هذه الحالة ما إذا اتفق موظفي المُصدر لها مع التجار مقابل دفع علاوة، بحيث تصادر البطاقة من أصحابها إذا كانت أرقامها مدرجة ضمن قائمة المعارضة أو إذا كانت مزورة، أو كأن تستخدم من قبل الغير مع معرفة التاجر بالمالك الأصلي للبطاقة فينتابه الشك عن كيفية وصول الغير إليها[2].

3- المعارضة في قبول البطاقة:

المعارضة هي عبارة عن إجراء وقائي يعمل على عدم قبول البطاقة في عمليات الوفاء وهذا في حالات عديدة منها السرقة أو الفقد، وعملية المعارضة قد تصدر من قبل صاحبها، أو من قبل الجهة المصدرة عندها يتم إلغائها.

ويكمن تعريف المعارضة على أنها نظام يعمل على توزيع رقم البطاقة عن طريق نشرات تحذيرية تقدم للتجار الذين يتعاملون بها في الوفاء، سواء بالجهاز اليدوي أو الجهاز الالكتروني pos، أو جهاز الصراف الآلي[3].

(1) منال بتة، نفس المرجع السابق ، ص39.

(2) صونية مقري، المسؤولية المدنية عن الاستخدام الغير مشروع لبطاقات الدفع الالكتروني، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2015، ص107.

(3) خولة بوقديرة، المرجع السابق، ص51.

أ-المعارضة لدى التجار المزودين بالجهاز اليدوي:

يتم نشر هذه المعارضة من خلال تزويدهم بقوائم تتضمن أرقام البطاقات الغير مقبولة في الوفاء، وإذا لم يقم التاجر بإجراء المطابقة وقبل الوفاء، وكانت ضمن البطاقات الواردة أرقامها في قائمة المعارضة فإنه يتعرض لرفض صرف الفاتورة من قبل المصدر.

ب-نشر المعارضة للتجار المزودين بجهاز البيع الإلكتروني (p.o.s):

في هذه الحالة المصدر لا يقوم بتسليم التاجر قائمة تحمل أرقام بطاقات الدفع الالكتروني غير مقبولة في الوفاء، وإنما يتم ذلك بشكل إلكتروني فبمجرد تمرير البطاقة على الجهاز الموصول بالكومبيوتر المصدر المزود بأرقام البطاقات الغير مقبولة يقوم هذا الأخير تلقائيا بقبول أو رفض البطاقة[1].

ج- نشر المعارضة من خلال جهاز الصراف الآلي:

ويكون ذلك ببرمجة جهاز الصراف الآلي الموصول بكمبيوتر البنك على رفض البطاقة خلال عمليات السحب وفي حالة ما إذا كانت البطاقة المسروقة أو المفقودة فالجهاز يقوم بسحبها وعدم إعادتها[2].

ثالثا: طرق الحماية والرقابة الأخرى

يجب على المصرف المتعامل عبر الانترنت إتباع مجموعة من الإجراءات لتوفير عنصر الأمان والرقابة السليمة للحفاظ على سمعة الجهاز المصرفي ونذكر منها:

(1) أمجد حمدان الجهني، المرجع السابق، ص120.

(2) نفس المرجع السابق ، ص121.

1-توجد نسبة 70% من المهاجمين الذين يحاولون الدخول والعبث بشبكة الموظفين العاملين لدى المصرف، بحيث أن شبكة والنظم المعلومات الداخلية لدى الموظفين على توفير معلومات أعلى من المهاجمين، عليه يجب على إدارة المصرف أن تحرص على توفير معلومات عن الشبكة الداخلية ونظم المعلومات الموظفين المعينين بذلك عند الحاجة فقط.

2-استخدام نظام إلكتروني معقد لتكوين الكلمات السرية المقابلة لمفاتيح الدخول الالكترونية (ID_S) ، بحيث يجب أن تكون كلمة السر مكونة على الأقل من 6-7 حروف أو أرقام، وأن يتم وضعها بطريقة يصعب تخمينها من قبل الغير.

3-يجب أن يقوم المصرف المتعامل عبر شبكة الانترنت بتحديد وحصر كافة النقاط والأجهزة الداخلية مع الفضاء الخارجي، وأن يقوم بمراقبة هذه النقاط ومنع استخدام أية جهاز آخر من قبل الموظفين[1].

4- انتهاج أسلوب رقابة وتدقيق داخلي يتناسب مع طبيعة ومستوى خطرة العمل المصرفي عبر الانترنت.

5-العمل على توعية مستخدمي هذه البطاقات بمخاطرها، وذلك بعقد اللقاءات والندوات وبرامج تلفزيونية توعوية.

6-إخضاع العاملين في مجال المكافحة إلى برامج تدريبية. وتأهيل التقني ذات الصلة بالإجراءات الوقائية لتحقيق المكافحة لهذه الجرائم.

7-مراقبة أصحاب السوابق مثل هذه الجرائم من أجل وضعهم في دائرة أمينة للمراقبة المستمرة، لتفادي تكرار مثل لهذه الجرائم[2].

(1) حليمة حمودي، المرجع السابق، ص ص41، 42.

(2) علي عدنان الفيل، المرجع السابق، ص80، 81.

8-تكثيف الدوريات الأمنية في المواقع والمناطق التي يتم التعامل فيها بالبطاقات، بحيث أن التواجد الأمني يبعث الطمأنينة في نفوس المواطنين، وردع الجناة، فيحد من فرص ارتكابهم للجريمة.

9-العمل على إيجاد إطار شرطي متخصص في مواجهة جرائم البنوك بشكل عام، وتأهيلية تقنيا حيث يصبح قادرا على عمل أرشيف لمثل هذه الجرائم، من حيث أسلوب الارتكاب، وأشخاص المرتكبين، وبالتالي القدرة على التحقيق الفني والتقني والتعامل مع مثل هذه القضايا[1].

10-يجب أن يقوم المصرف بكافة إجراءات الرقابة والحماية المادية للأجهزة، حيث يجب حفظ هذه الأجهزة في أماكن آمنة، لا يسمح لأحد بالدخول ما عدى الموظفين المخول لهم بالدخول إليها[2].

الفرع الثاني: الإجراءات الوقائية المتخذة من قبل حامل البطاقة

وتتمثل الإجراءات التي يقوم بها حامل البطاقة والمستفيد الأول من خدماتها في جملة من الوسائل والتدابير الوقائية، وذلك لتفادي الجرائم التي يمكن أن تقع على البطاقة وحمايتها من الضياع أو السرقة، والمحافظة على الرقم السري، وتفادي أي تجاوز أو استخدام غير مشروع لها من قبل الغير، فتتجلى هذه الإجراءات في إجراءات وقائية (أولا) وأخرى متخذة عند الشراء من المحلات التجارية (ثانيا) وأخرى متخذة عند الشراء عن طريق الانترنت (ثالثا):

(1)علي عدنان الفيل ، المرجع السابق، ص81.

(2) حليمة حمودي، المرجع السابق، ص42.

أولا: إجراءات وقائية

هنالك جملة من الوسائل الوقائية التي يجب على الحامل إتباعها لحماية بطاقة الدفع الالكتروني، والمحافظة على بياناتها تتمثل في:

1-أن يقوم الحامل بإهمال البطاقة أو وضعها في مكان غير آمن فتسهل سرقتها أو ضياعها.

2- أن يقوم الحامل بتسليم البطاقة لأي شخص لو كان أحد أقربائه أو عائلته.

3- أن لا يقوم الحامل بالإفصاح عن رقمه السري أو ترديده أمام الغير، كتابته على جسم البطاقة، أو على ورقة منفصلة على البطاقة، بل يجب أن يحفظ الرقم السري عن ظهر قلب ويحرص على إدخاله في جهاز الصراف الآلي بكل خصوصية وسرية، أما الوثيقة التي يكون بها الرقم السري فيقوم بإتلافها، حتى لا تقع في يد الغير[1].

4- يجب على الحامل أن يحتفظ بالنسخة التي يعطيها التاجر له لأنها تحتوي على رقم البطاقة.

5- يجب على الحامل أن يقوم باستخدام بطاقته في الأماكن الموثوقة والآمنة وتفادي المحلات الصغرى، أو المطاعم المشكوك فيها، وخاصة الملاهي ودور القمار.

6- يجب على الحامل عند الشك بأن الرقم السري للبطاقة قد عرف،أو عند فقده لبطاقته أو سرقتها إبلاغ المصدر فورا بواسطة الهاتف، فتقوم الجهة المصدرة على هذا الأساس بإلغاء البطاقة، على أن يقوم الحامل لاحقا بتعزيز هذا الإبلاغ بخطاب مكتوب.

7- أن يحرص الحامل على شحن حساب بطاقته بمبالغ قليلة حتى لا تكون الخسائر كبيرة أن تم السحب بواسطة الغير[2].

(1)علي عدنان الفيل، المرجع السابق، ص83.

(2) أمجد حمدان الجهني، المرجع السابق، ص122.

8- على الحامل عند اختيار الرقم السري أن يختار أرقاما وحروفا غامضة وعشوائية وأن لا تكون ذات علاقة بالحامل وبحياته الشخصية حتى لا يصبح من السهل كشفها[1].

ثانيا: الإجراءات المتخذة عند الشراء من المحلات التجارية

من أهم الإجراءات التي يجب أن يتخذها الحامل قبل إجراء أي عمل بشراء هي:

1-يجب على حامل البطاقة أن يحرص على التسوق من محلات تجارية آمنة، ورفقة أشخاص ذو موثوقية.

2-التحقق من هوية ومصداقية التاجر، كما يتحقق من وصل الشراء قبل التوقيع عليه، والاحتفاظ به، ونسخة من أي وثيقة لها حجية إثبات على إجراء المعاملة.

3-في حال ما إذا قام الحامل بالسحب باستعمال البطاقة في جهاز الدفع الآلي ولم يستطيع استردادها أو لاحظ وجود أجهزة غير مألوفة متصلة بها فعليه إبلاغ البنك أو الشرطة لتفادي تجاوزات عليها لاحقا[2].

ثالثا: الإجراءات المتخذة عند الشراء عن طريق الانترنت

بما أن التعامل بالانترنت يكون قائما على عالم افتراضي فإن ذلك يشكل خطوة أكبر في حال التعامل الواقعي، لذا يجب على الحامل اتخاذ بعض الإجراءات المتمثلة في:

1-على حامل البطاقة استخدام برامج كمبيوتر مشفرة مثل برنامج (PGP) لضمان خصوصية البريد الالكتروني وبعد إتمام العملية يجب أن يطبع الصفحة التي يحتوي على مختصر للعملية، التي قام بها حتى يدرك الحامل ماله وما عليه.

(1) بن تركي ليلى، المرجع السابق، ص314.

(2) خولة يوقديرة، المرجع السابق، ص56.

2-التأكد من وجود اتصال آمن وذلك بالتأكد من وجود كلمة (Rttps://)،بدلا من (Rttp://)، كما يمكن التأكدمن وجود القفل المغلق غفي أسفل نافذة المتصفح على يمين الشاشة.

3- على الحامل التأكد من أن الموقع الذي يتعامل معه محل ثقة، فيتجنب لمواقع الصغيرة والمجهولة.

4-تفادي إرسال معلومات شخصية مثل عنون الشخص، رقم الضمان الاجتماعي، رقم بطاقة الائتمان وغيره من المعلومات الشخصية عبر الشبكة، إلا بطريقة آمنة ومشفرة.

5-الحرص على المحافظة على كلمة السر وعدم حفظها على الجهاز أو السماح للمتصفح بذكرها واستخدام النسخ الحديثة التي لا تتضمن ثغرات أمنية فيها والتي تصعب سرقة البيانات السرية المتعلقة بالبطاقة.

6-على الحامل التأكد من جميع المبالغ المسجلة على البطاقة عند وصول كشف حساب بطاقة الائتمان، وعند اكتشاف أي تلاعب لابد من رفع شكوى إلى البنك المصدر الذي يقوم بدوره بالتحقيق على ماهية الشخص أو الجهة التي استخدمت البطاقة دون تصريح وإذن من الحامل[1].

الفرع الثالث: الإجراءات الوقائية المتخذة من قبل التاجر

لا تقتصر إجراءات حماية بطاقة الدفع الالكتروني على البنك المصدر والحامل فقط، فتمتد المسؤولية بذلك إلى التاجر الذي قد يكون ضحية التلاعب والاحتيال التي قد يتم بواسطة بطاقة الدفع الالكتروني، والتي تحمله خسائر مادية وحتى دعاوي قانونية، و للوقاية من الاستخدام الغير مشروع لها يجب عليه أن:

(1) بن تركي ليلى، المرجع السابق، ص ص316، 317.

أولا: أثناء تنفيذ عملية الوفاء بواسطة بطاقة الدفع الالكتروني

1-يجب على التاجر التأكد من هوية مقدم البطاقة فإن لم يكن حاملها الشرعي فعليه أن يرفض التعامل معه.

2-بعد التأكد من هويته يجب عليه أن يطلب التوقيع على البطاقة في حال غياب التوقيع عليها عند الشراء.

3-عدم تجزئة العملية الشرائية الواحدة إلى أكثر من تمريرة واحدة على البطاقة، وفي حالة إظهار الجهاز لعبارة "راجع الجهة المصدرة" فلا يجب أن يحاول تمرير البطاقة وإنما عليه إيقاف العملية مباشرة والاتصال بالجهة المصدرة.

4-عدم اعتماد رمز التفويض على المعاملة إلا من خلال الجهاز الذي لدى التاجر أو مركز التفويض لدى المصدر.

5-في حالة عدم تمكن التاجر من تمرير البطاقة على الجهاز فعليه أن يقوم البطاقة بواسطة الجهاز اليدوي أو رفض البطاقة وإلغاء العملية كليا[1].

ثانيا: على التاجر التأكد من الأمور التالية

يجب على التاجر أن يتأكد من أن البطاقة صحيحة وسارية المفعول، وأن الشريط المخصص للتوقيع على البطاقة سليم ولم يتعرض لأي تزوير، كما يجب أن يتأكد من صحة البيانات المسجلة على البطاقة وأنها مطابقة لبيانات حاملها، كما يجب أيضا التأكد من سلامة رقمها والتوقيع الموقع عليها[2].

(1) أمجد حمدان الجهني، المرجع السابق، ص ص124، 125.

(2) نفس المرجع السابق، ص125.

ثالثا: على التاجر رفض البطاقات التالية

على التاجر أن يرفض التعامل بالبطاقات غير الصالحة، كأن تكون البطاقة مقدمة من قبل الغير، أو أنه تم التعديل فيها أو إتلافها، إضافة إلى تفادي البطاقات العالمية التي لا تتضمن علامات الضمان كبطاقة فيزا[1].

رابعا: على التاجر رفض التعامل مع حامل البطاقة

على التاجر أن يأخذ الحيطة والحذر من الأشخاص الذين تدور حولهم الشكوك، كالأشخاص الذين يقومون بإخراج البطاقة من الجيب بدل المحفظة، أو يظهر عليهم سلوك مريب، أو الذين يقومون بالشراء بشكل عشوائي بدون معاينة المنتوجات أو الاهتمام بجودتها أو سعرها، والاقتناء بكميات محدودة.

وهنا يتوجب على التاجر إخبار البنك المصدر لتفادي أن يقع ضحية لهؤلاء الأشخاص ويتفادى أن تجاوز قد يحدث من قبلهم، كالسرقة والاحتيال والتزوير[2].

المطلب الثاني

الإجراءات الأمنية المتخذة لمواجهة مخاطر بطاقة الدفع الإلكتروني

يوجد في عديد من دول العالم أجهزة متخصصة في مكافحة جريمة الاعتداء على بطاقة الدفع الإلكتروني، إلا أن هناك دول تفتقر لهذا النوع من الأجهزة، وتعتمد على رجال الشرطة في حال وجود بلاغات من قبل البنوك والمؤسسات المالية الكبرى وهذا ما سنتناوله في (الفرع الأول)، وكما تعتمد أيضا على برمجة الحاسب الآلي الذي سوف نتناوله في (الفرع الثاني).

(1) علي عدنان الفيل، المرجع السابق، ص125.

(2) وسام فيصل الشواورة، المرجع السابق، ص 108.

الفرع الأول: الإجراءات الأمنية المتخذة من قبل الشرطة لحماية بطاقة الائتمان

يقع على عاتق جهاز الشرطة حماية اقتصاد الدولة من الاعتداءات التي يمكن أن يتعرض لها، لذلك حماية بطاقة الائتمان من الاعتداءات يندرج في نطاق حماية الأمن الاقتصادي، فحماية هذه البطاقات يحقق الأمن سواء للفرد أو الدولة[1].

حيث يمكن لجهاز الشرطة اتخاذ بعض الإجراءات للحد من وقوع مثل هذه الجرائم والمتمثلة في:

1-تأمين البنوك ومراكز التعامل المالي بالحراسات الأمنية لمتابعة ومراقبة كل من يحاول إساءة استخدام تلك المراكز، أو مراقبة العملاء لمعرفة أرقام بطاقتهم، وتأمين البنوك والمراكز المالية يزرع الرعب والخوف في نفوس المقيمين لهذه الجرائم.

2-العمل على إجراءات تفتيشات دورية فنية، لشركات المرخص لها إصدار مثل هذه البطاقاتلتأكد بأنها تتقيد بالمواصفات التقنية العالية[2].

3-إعطاء توجيهات وتعليمات لحاملي البطاقات على كيفية التصرف عند فقدها أو سرقتها[3].

4-إخضاع أفراد الشرطة إلى برامج تدريبية وتأهيلية ذات صلة بالإجراءات الوقائية لتحقيق مكافحة هذه الجرائم.

5-ضرورة إنشاء معمل متخصص يحتوي على أجهزة متطورة تستخدم في عملية فحص الوثائق والمستندات، ويتولاها ضباط ذات كفاءة عالية[4].

---

(1) إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان الالكترونية، الطبعة 1، الأردن، دار المسيرة للنشر والتوزيع، سنة 2002، ص383.

(2) عبد الكريم الردايدة، جرائم بطاقات الائتمان (دراسة تطبيقية ميدانية)،الطبعة1، الأردن، دار حامد للنشر والتوزيع، 2013، ص ص129، 130.

(3) إيهاب فوزي السقا، المرجع السابق، ص387.

(4) عبد الكريم الردايدة، المرجع السابق، ص ص130، 131.

الفرع الثاني: الحماية الأمنية لبطاقات الدفع الالكتروني من خلال الحاسب الآلي

يعتبر الحاسب الآلي تقنية بالغة الأهمية في استعمال بطاقة الدفع الالكتروني، إلا أن خطورته تكون بالغة، حيث أن الجرائم الواقعة بواسطته تقع على أشياء غير ملموسة مثل البرامج والبيانات التي تزيل الآثار المادية للجريمة، وتصعب عملية البحث والتحري على الشرطة[1] وعليه يجب اتخاذ العديد من الإجراءات الأمنية التي يكون الحاسب الآلي محورها تتمثل في:

1-انتهاج أسلوب نظام حفظ المعلومات بجهاز الشرطة، وإدراج الحاسب الآلي وتطوير برامجه وتقنياته، وإدخال مختلف المعلومات المتعلقة بالجرائم الاقتصادية ومرتكبيها، وبهذا يصبح لدى الشرطة قاعدة حفظ جميع الملفات.

2-ربط الحاسب الآلي بوسيلة آلية تحدد عدد معين من محاولات الوصول إلى الحاسب الآلي في حالة استعمال الهاتف، الانترنت...

3-التأكد من توفر الاحتياطات الأمنية على نطاق المعلومات في الحاسب الآلي.

4-عدم السماح للأشخاص غير المصرح لهم بدخول الحاسب الآلي[2].

5-تحديد عدد وأنواع الأجهزة المحتمل إدراجها ضمن عملية الاستيلاء للتعامل معها، والحصول على أجهزة وبرامج مختلفة للاستعانة بها في الفحص والتشغيل.

6-تهيئة خريطة للموقع محل المداهمة وتفاصيل المنى، وتحديد مواقع الأجهزة والخزائن والملفات السرية، ومواقع بطاقات الدفع الالكترونية[3].

إضافة إلى الإجراءات سابقة الذكر، يمكن الحد من عمليات الاعتداء الواقعة على البطاقة بواسطة الحاسب الآلي من خلال:

(1) حليمة حمودي، المرجع السابق، ص47.

(2) إيهاب فوزي السقا، المرجع السابق، ص 385.

(3)عبد الكريم الردايدة، المرجع السابق، ص136.

1-تحديد الدخول إلى غرفة الحاسب الآلي ببطاقة دخول.

2-وجوب وجود تصريح للسماح باستخدام الحاسب الآلي.

3-حصر فئة محددة يمكنها الولوج إلى بعض الملفات المعينة.

4-تحديد أرقام هواتف معينة، ولعدد محدود، وأوقات معينة بإمكانها دون غيرها، واستخدام الحاسب الآلي عن طريق الهاتف.

5-توفير احتياطات أمنية خاصة فعالة لحماية نظم المعلومات.

6-تهيئة وتصميم برامج أمنية خاصة، يجري اختيارها من وقت لآخر من قبل جهات معينة ومتخصصة، حماية للحاسب الآلي.

ومما سبق ذكره نستنتج أن الأخذ بهذه الاحتياطات قد يمكننا بصورة كبيرة من مواجهة الاعتداءات التي قد تقع على بطاقة الدفع الالكتروني من خلال الحاسب الآلي، أو على الأقل إتباع الجاني وتقديمه للعدالة [1].

(1) حليمة حمودي، المرجع السابق، ص ص48، 49.

المبحث الثاني

قواعد الحماية القانونية الوطنية والدولية لبطاقة الدفع الإلكتروني

نظرا لتعدد استخدام وسائل الدفع الالكتروني في المجال التجاري من قبل المستهلكين باستعمال بطاقات الدفع الالكتروني، أدى ذلك إلى التعدي عن تلك البطاقات، وهذا ما دفع بالتشريعات إلى توفير القدر الكافي من الحماية القانونية، لمثل هذه البطاقات، والتي سوف نتناولها بالتفصيل في المطالبين التاليين، حماية التشريعات الوطنية للدفع الإلكتروني (المطلب الأول) والجهود الدولية لحماية الدفع الالكتروني (المطلب الثاني).

المطلب الأول

حماية التشريعات الوطنية لدفع الإلكتروني

لقد تبنت الكثير من دول العالم تشريعات خاصة بحماية الدفع الالكتروني في التشريعات الداخلية وذلك من خلال سن قوانين تعاقب على مثل هذه الجرائم ومن أهمها[1]:

الفرع الأول: الحماية في القانون الفرنسي

مرت التجربة الفرنسية في معاملات الدفع الالكتروني بعدة مراحل منها:

أولا: المرحلة الأولى

كانت أولى المحاولات في قانون العقوبات، لحماية المال المعلوماتي بفرنسا من طرف وزير العدل سنة 1985، بإضافة الباب الرابع للكتاب الثالث منه بعنوان الجرائم على المادة المعلوماتية يتكون من ثمانية مواد من 1/307 إلى 8/307 تناولت الموضوعات التالية:

(1) دبابش عبد الرؤوف، "وسائل الدفع مابين الحماية التقنية والقانونية لمستهلك الالكتروني"، **مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع**، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، أفريل 2017، ص110.

1- التقاط البرامج أو المعطيات أو أي عنصر آخر من النظام المعلوماتي عمدا.

2-استخدام أو نقل أو إنتاج برامج أو معطيات أو أي عنصر من عناصر النظام بدون موافقة من لهم الحق.

3- تخريب أو تعييب كل أو جزء من نظام المعالجة الآلية للمعلومات أو عرقلة أدائه للوظيفة.

4- الحصول أو السماح بالحصول على فائدة غير مشروعة عن طريق الاستخدام غير المشروع لنظام المعالجة الآلية للمعومات[1].

ولكن هذا المشروع لم يجد سيلا للتطبيق.

ثانيا: المرحلة الثانية

وهذه المرحلة هي التي توجت بنجاح وكانت في الخامس من أوت 1986 عندما تقدم النائب "jacqwegodfrain" باقتراح مشروع قانون الغش المعلوماتي" fraude informatique"، وهذا الاقتراح يشمل الجرائم التقليدية كالسرقة وخيانة الأمانة والتزوير، كما شمل الاعتداء على المال المعلوماتي، وقد تعرض هذا المشروع إلى عدة مناقشات في البرلمان وتم الوصول في الأخير إلى قانون مختلف تماما عن الذي قدم أول مرة، والذي يشابه المشروع الأول الذي تقدم به وزير العدل سنة 1985[2].

وجاء هذا المشروع في الباب لثالث ، من القسم الثاني من الكتاب المتعلق بالجنايات والجنح الماسة بالأشخاص، وأصبح الباب الثالث متعلق بالجرائم المعلوماتية، وذلك في المواد من 4/462 إلى 9/462 وتضمن الجرائم التالية:

(1) واقد يوسف، النظام القانوني للدفع الالكتروني، مذكرة لنيل درجة ماجستير في القانون، فرع قانون عام، نخصص قانون التعاون الدولي، كلية الحقوق ، مدرسة دكتوراه القانونية والسياسية، جامعة تيزي وزو، سنة 2011، ص172.

(2) نفس المرجع السابق، ص ص173، 174.

1-الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه.

2-إدخال المعطيات في نظام أو المحو أو التعديل للمعطيات الموجودة فيه عمدا أو بدون مراعاة حقوق الغير، سواء بطريقة مباشرة أو غير مباشرة.

3-كل فعل من شأنه أن يعرقل أو يفسد أداء النظام لوظيفته.

4-تزوير المستندات المعالجة آليا.

5- الشروع في ارتكاب الجرائم السابقة.

6- الاتفاق الجنائي على ارتكاب الجرائم السابقة[1].

كما جرمت المادة 11 من القانون 91-1382 الصادر في 30 ديسمبر 1991 بعض الاستعمالات الغير مشروعة لبطاقة الدفع الالكتروني، وهي التقليد أو تزوير، استعمال أو محاولة استعمال البطاقة المقلدة أو المزورة[2].

ثالثا: المرحلة الثالثة

تم تعديل قانون العقوبات الفرنسي سنة 1994 وجاء في هذا التعديل مصطلح الغش في الجرائم السابقة، واستغنى عن مصطلح "دون مراعاة حقوق الغير" كما أدخل تغيير على المادة 1/441، فطور من جريمة التزوير المعلوماتي لتصبح جريمة تزوير المستندات المعالجة آليا فحسب، كما ضم هذا التعديل المواد من 1/323 إلى 7/323، ونجد أنه في نص المادة 3/322 لا يحكم المشرع الفرنسي بهذا النص النظام من الناحية المادية لكنه يوفر بهذا النص حماية البيانات الموجودة في النظام من أي نشاط إجرامي، وتتضمن هذه الجريمة ثلاثة صور وهي: الإدخال، المحو، التعديل، ولا يشترط أن تتوفر هذه الصور جميعا بل يكفي لتحقيق

(1) واقد يوسف، المرجع السابق، ص174.

(2) Loi, n° 91,1382 du 30 décember 1991 relative a la sécurité des cléques et des cartes de paiement.

الجريمة توافر إحداها[1]، وبعد عشر (10) سنوات من هذا التعديل جاء تعديل آخر لقانون العقوبات سنة 2004 وقد أضاف فيه المشرع نوع جديد من الجرائم وهي التعامل في الوسائل التي يمكن أن ترتكب بها الجريمة، وقد نصت على هذه الجريمة المادة 3/323-1 [2].

وتنص المادة 1/323 من القانون رقم 275/2004 المعدل لقانون العقوبات، على أنه بمجرد الدخول أو البقاء بصفة غير قانونية في كل أو جزء من نظام المعالجة الالكترونية للبيانات، فإنه يعاقب بسنتين حبس وب (30.000 اورو) غرامة عندما ينتج من جراء ذلك، وتشدد العقوبة في حالة عرقلة سير النظام.

كما نصت المادة 3/323 من نفس القانون السابق المعدل لقانون العقوبات الفرنسي، على أن مجرد إضافة أو إدخال بطريقة غير شرعية بيانات في نظام المعالجة الرقمية أو المحو أو التغيير غير شرعي للبيانات التي يحتويها، تتم المعاقبة عليها، ب5 سنوات و(750.000 اورو) غرامة، ونصت المادة 5/323 كذلك على العقوبات الإضافية إلى جانب العقوبات الأصلية ، فالأشخاص الطبيعية تحرم من الحقوق المدنية والعائلية في هذا النوع من الجرائم لمدة 5 سنوات[3].

ويتم حجز كل الوسائل التي استخدمت في الجريمة، كما يمكن إقصاءه من الصفقات العمومية لنفس المدة، واعتبرت المادة 7/323 أن محاولة اقتراف المخالفات أو الجرائم التي نصت عليها في المواد 1/323 و 3/3232-1 معاقب عليها بنفس العقوبة.

([1])voir le code pénal françaias, crée par la loi n° 96- 392 du 13 mai 1996 jorf, mai 1996 in http://droit.finance.commentcamarche.net/legifrance/37.code .penal

(2) خنفوسي عبد العزيز، قانون الدفع الالكتروني، الطبعة 1، مركز الكتاب الأكاديمي لنشر وتوزيع، عمان، 2018، ص44.

(3) واقد يوسف، المرجع السابق، ص175.

رابعا: المرحلة الرابعة

نجد القانون 2001-1062 المؤرخ في 5 نوفمبر 2001 والمتعلق بالحماية الدائمة، والتي أدخلت في القانون النقدي والمالي نصوصا جديدة قصد ضمان حماية الدفع، والتي تمنح لنبك فرنسا مهمة ضمان حماية وسائل الدفع[1].

لذلك يجب أن تحظى بطاقات الدفع بحماية قانونية مثلها مثل الشيك ويمكن تحديد الأفعال التي تعد تجريما فيما يلي:

1- تقليد وتزوير بطاقات الدفع واستعمالها.
2-صناعة أو بيع أدوات وآلات يتم استعمالها في تصنيع البطاقات بغير ترخيص قانوني.
3-عرض للبيع أو حيازة أدوات خاصة بنظام الدفع بعير تصريح قانوني.
4-استخدام بطاقة غير صحيحة أو ملغاة أو المنتهية في سحب مبلغ تجاوز الرصيد أو في الوفاء لدى اتجار مع عدم وجود رصيد[2].

الفرع الثاني: الحماية في القانون الألماني

تعتبر معظم النصوص الخاصة بضمان المعاملات الإلكترونية بواسطة بطاقات الدفع في التشريع الألماني، عبارة عن قواعد عامة جاءت في قانون العقوبات، بحيث يعتبرها البعض مرنة بالقدر الكافي، لتشمل بعض الحالات من بينها العلاقة بين حامل البطاقة من جهة والتجار والمؤسسات المالية من جهة أخرى.

([1])Document du service des études juridiques du Senat (RF.)La sécurité des transactions réalisées par carte bancaire , in http://www.senat.fr/lc/lc/lc125.html octobre 2003, p01.

(2) خنفوسي عبد العزيز، المرجع السابق، ص45.

وبدخول قانون الشراء عن بعد حيز التنفيذ سنة 2000، الذي نصت عليه العديد من إجراءات الحماية الخاصة لاستعمال بطاقات الدفع، والذي تم إلغاءه مباشرة بعدما تم إدخال قواعده في القانون المدني الألماني.

وقد نص قانون العقوبات الألماني في المادة 152A أنه بمجرد استعمال بطاقة مزورة أو حيازتها أو إعطاؤها لشخص آخر، يعاقب بمدة حبس تتراوح ما بين سنة إلى 10 سنوات، وعندما ترتكب هذه الجريمة من قبل جماعة فإن العقوبة تكون أقل بسنتين، وكما نصت المادة 266 B على الاستعمال المفرط لبطاقات الدفع، وكيفتها بأنها جريمة ذات خصوصية ومعاقب عليها بغرامة مالية أو الحبس، وكما تم النص على الاستعمالات التعسفية الأخرى بموجب المادة 263 A الخاصة بالتزوير الرقمي (الجريمة المعلوماتية) والتي يعاقب عليها بغرامة مالية و5 سنوات حبس على الأكثر.

اتخذت البنوك منذ أفريل 2001 إجراء يلزم المستهلكين بتقديم للبائعين عددا يتكون من ثلاثة أرقام والمتواجدة على ظهر البطاقة عند دفعه لسلع والخدمات التي اقتناها، وكما قام البائعون ومقدمو الخدمات إلى فرض مراقبات عديدة، منها تقديم الهوية عند استعمال بطاقة الدفع لالكتروني، كما يوجد تعاون داخلي بين أجهزة الشرطة والمتعاملين بهذه الطريقة وذلك بتقديم الأرقام المسروقة من قبل المعاملات المزورة[1].

الفرع الثالث: الحماية في القانون الجزائري

جاء تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات[2]، والذي خصص القسم السابع

(1)Document du service des études juridiques du Senat (RF.)La sécurité des transactions réalisées par carte bancaire , op. cit, p02.

(2) القانون رقم04-15 مؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات ج ر العدد 71 الصادرة في 10 نوفمبر 2004.

مكرر منه، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" والذي تضمن ثمانية مواد من المادة 394 مكرر إلى 394مكرر 7.

نصت المادة 394 مكرر المضافة بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 206 على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى2000.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من ستة أشهر إلى سنتين، وبغرامة مالية من 50.000 دج إلى 300.000 دج، وكما أضافت المادة 394 مكرر1 من القانون نفسه "يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج..."

كما نص هذا التعديل أيضا على عقوبة مصادرة وسائل ارتكاب الجريمة وإغلاق المواقع أو المحلات التي تكون محلا لها أو التي ارتكب فيها وذلك وفق المادة 394 مكرر6[1].

أصدر بنك الجزائر تنظيم داخلي رقم 05-07 بتاريخ 28 ديسمبر 2005، يتعلق بأمن أنظمة الوفاء، من أجل ضمان عملية الوفاء الالكتروني، وهذا التنظيم هو عبارة عن إجراءات وطنية أو دولية تنظم العلاقات بين طرفين على الأقل تتوف فيهم صفة البنك أو المؤسسة المالية[2].

(1) المواد 394 مكرر و394 مكرر 1 و394 مكر6 من القانون 04-15 المؤرخ في 2004 المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات.

(2) واقد يوسف، المرجع السابق، ص181.

كما تضمن القانون رقم 09-04 المؤرخ في 5 غشت سنة 2009 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وحصر هذا القانون في مادته الثانية الفقرة "أ" الجرائم الماسة بأنظمة لمعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى يسهل ارتكابها عن طريق المنظومة المعلوماتية أو نظام الاتصالات، وكما انشأ هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها في الفصل الخامس منه، وخولت لها المادة 14 المهام التالية:

1-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
2-مساعدة السلطات القضائية ومصالح الشرطة القضائية في تحريات ذات صلة بهذه الجريمة.
3-تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعلومات التي تساعد في التعرف على مرتكبي جرائم تكنولوجيا الإعلام والاتصال وتحديد مكانهم[1].

كما نص القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة في الفصل الخامس على الخدمات المحمية، وأخص المادة الرابعة الفقرة 1 التي نصت على برامج الحواسيب، التي تدخل ضمن نطاق الملكية الفكرية المحمية والتي يعاقب على التعدي عليها[2].

استنتاجا مما سبق يمكن القول أن المشرع الجزائري وسع في دائرة الحماية إلى أن يشمل كافة الجرائم، سواء كانت ماسة بأمن الدولة، والماسة بالاقتصاد الوطني، من خلال عبارة "أي جريمة أخرى".

(1) المادة 2 و14 من القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 5 غشت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر العدد 47- الصادرة في 25 شعبان 130 الموافق ل 10 غشت 2009.

(2) المادة 1/4 من الأمر 03-05 المؤرخ في 19 جويلية 2003 المتعلقة بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44 الصادرة في 2003/07/23.

المطلب الثاني

الجهود الدولية لحماية بطاقات الدفع الالكتروني

لم تقتصر حماية بطاقات الدفع الالكتروني على التشريعات الداخلية فقط، وإنما امتدت إلى ضرورة تضافر الجهود الدولية نظرا للانتشار الواسع لاستخدام بطاقات الدفع الالكتروني عبر العالم، مما يستدعي وضع نظام قانوني صارم يتفق وطبيعة الجرائم المستحدثة، إضافة إلى انتهاج وسائل مختلفة وذلك لضمان حماية فعالة لمختلف المعاملات الالكترونية، وعليه سنعرض في(الفرع الأول) بعض النماذج الدولية لحماية بطاقات الدفع الالكتروني، إلى جانب وسائل التعاون الدولي المختلفة لمكافحة جرائم بطاقات الدفع الالكتروني في(الفرع الثاني).

الفرع الأول: هيئات التعاون الدولي

التعاون الدولي هو تبادل البحوث وتضافر الجهود المشتركة بين جميع الدول، حيث أثبت الواقع العلمي أن الدولة لا تستطيع بمجهودها المنفرد القضاء على هذا النوع الحديث من الجريمة، ولهذا السبب تم إنشاء مجموعة من المنظمات بهدف تفعيل التعاون الدولي على أوسع نطاق والتي بدورها انبثقت عنها عدة اتفاقيات في مكافحة جرائم بطاقات الدفع الالكتروني، وسنفصل فيها على النحو التالي:

أولا: الحماية القانونية في ظل الاتحاد الأوروبي

يتجسد الاهتمام الأوروبي بالحماية التشريعية للمعاملات الإلكترونية للمجموعة الاقتصادية الأوروبية، من خلال التوصية رقم (598/87) حول القانون الأوروبي للسيرة الحسنة الخاصة بالدفع الإلكتروني[1]، هذه التوصية تضمنت دعوة جميع المتعاملين لتطبيق واحترام هذا القانون

(1) Recommondation N°87/598/ CEE de la commission européenne du 8 décombre 1987 protant sur un code européen de bonne conduite en matiére de paiement électronique, JOL365,24 décombre 1987.

من أجل حماية الدفع الالكتروني، وترقية الحماية والضمان للمستهلكين، كما نصت هذه التوصية على إضفاء الطابع الشخصي والسري للمعطيات والبيانات المقدمة، من طرف المستهلك، مع ضمان حق الدخول المتعادل إلى جميع خدمات مقدمي مختلف خدمات الدفع الالكتروني، وإلزام المستهلك أو حامل البطاقة على ضرورة الأخذ بالعناية اللازمة لطريقة استعمال بطاقة الدفع الالكتروني[1].

أصدر الاتحاد الأوروبي توصية ثانية تحت رقم (489/97) تتضمن المعاملات التي تتم بواسطة وسائل الدفع الالكتروني وخاصة في إطار تنظيم العلاقة بين مصدر البطاقات والحامل، فخصت هذه التوصية المعاملات التي تتم عن طريق وسائل الدفع الالكتروني عن بعد منها:

1- استخدام وسائل الدفع الالكتروني في نقل الأموال.
2- سحب الأموال السائلة بواسطة بطاقات الدفع الالكتروني باستخدام جهاز السحب الآلي للأوراق. [2]

كما جاءت هذه التوصية مؤكدة على ضرورة استخدام وسائل الدفع الالكتروني استخداما صحيحا، وفقا للشروط المتفق عليها، سواء في إصدار أو استعمال هذه الوسائل، مع ضرورة أخذ كافة الإجراءات.

(1) ليندة بلحارث ، آلية تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري، الملتقى الوطني الثامن حول آلية تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري، الجزائر، يومي 13-14 مارس 2017، ص8.

(2) Recommondation N°97/489/ CE du 30 jullet 1997 concernant les opérations effectuées au moyens d'intruments de paiment déctronique, relation entre émetteur et titulaire JOL 208, du 2 Aout 1997.

ثانيا: المنظمة الدولية لضباط الجرائم المالية

هي منظمة تم إنشائها عام 1986، عن طريق التعاون بين 68 محقق دولي مختص في جرائم الأموال، وهي منظمة دولية غير ربحية، هدفها توفير الخدمات والبيئة التي من خلالها يتم جمع المعلومات حول الاحتيال المالي وطرق التحقيق والحماية المالية، ومن خلال هذه المنظمة تم إنشاء منظمة دولية لضباط جرائم بطاقات الائتمان[1].

ومنذ عام 1996 فإن هذه المنظمة تمنح عضويتها العادية لضباط الشرطة ومحققي مؤسسات إصدار البطاقات، وخبراء مكافحة الاحتيال، وهذا من خلال إتباع شروط خاصة بها، كما تتيح هذه المنظمة لأعضائها إمكانية الحصول على المعلومات السرية الخاصة بالجرائم المالية الدولية والمجرمين الدوليين، كما تقوم بإرسال إنذارات لأعضائها بالأماكن المعرضة لهذه الجرائم، وتسمح للعضو الدخول على شبكات الحاسب الآلي التي تخص الجرائم المالية[2].

ومن اختصاصات هذه المنظمة أيضا أنها تعمل على تبادل المعلومات بين أعضائها بهدف الإنذار المبكر لأحدث أساليب ارتكاب الجريمة المالية، وتسعى أن تكون على علم بالعصابات المتخصصة في النشاط الإجرامي المتعلق بجرائم الأموال، ورصد المحتالين ووضعهم تحت المراقبة في حالة دخولهم لبلادهم، وضبطهم طبقا لتشريع كل دولة وذلك من أجل ردع ومواجهة المخاطر المتوقعة الحدوث[3].

(1) إيهاب فوزي السقا، المرجع السابق، ص508.

(2) نوال حاج مخناش، المرجع السابق، ص1125.

(3) نفس المرجع السابق، ص1125.

ثالثا: الحماية القانونية في ظل صدور اتفاقية المجلس الأوروبي الخاصة بالجريمة المعلوماتية (بودابست)

هي اتفاقية جاءت بهدف بناء سياسية جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في مختلف أنحاء العالم، تم التوقيع عليها سنة 2001[1]، تقوم على مبدأ تنسيق وانسجام التشريعات الوطنية مع بعضها البعض، والتعزيز من قدرات القضاء والتشديد في تطبيق القانون، إضافة إلى تقوية وتحسين التعاون الدولي في هذا الإطار، وكذا العمل على تحديد العقوبات من جرائم المعلوماتية في إطار قوانينهم المحلية[2].

تتضمن هذه الاتفاقية ديباجة تنصب في إطار الجرائم المعلوماتية، إضافة إلى 48 مادة تنقسم إلى ثلاثة أقسام كبرى.

حيث تناول القسم الأول مجوعة من الجرائم التي يمكن أن تتعرض لها نظم المعلوماتية وقسمت بدورها إلى أربعة أصناف رئيسية، حيث اشتمل الصنف الأول على جريمة الدخول غير المشروع، جريمة المراقبة أو الاعتراض غير المشروع، جريمة التشويش على البيانات، جريمة إتلاف نظام الحاسب كما تضمن النصف الثاني جريمة التزوير أو الاحتيال المرتبطة بالحاسوب[3]، هذا إضافة إلى صنفين آخرين، ومنه نستنتج أن القسم الأول قد جرم كل شكل من أشكال الاعتداء على وظيفة الحاسب بنية الغش المعلوماتي أو أية إجرامية من أجل الحصول دون وجه حق على منفعة اقتصادية وهذا ما تضمنته المادة 8 من الاتفاقية[4].

(1) اتفاقية بودابست، المتعلقة بالجريمة المعلوماتية، تم الاعتماد عليها وتقريرها في 8 نوفمبر 2001 والتوقيع عليها 23 نوفمبر 2001.

(2) خنفوسي عبد العزيز، المرجع السابق، ص53.

(3) انظر المادة 2، 3، 4 من اتفاقية بودابست، المرجع السابق.

(4) انظر المادة 8 من اتفاقية بودابست، المرجع السابق.

أما القسم الثاني فقد تضمن الإجراءات التي يمكن أن تتخذ في مواجهة هذا النوع من الجرائم، خاصة فيما يتعلق بتفتيش وضبط البيانات المخزنة في الحاسوب، وهذا ما نصت عليه المادتين 16 و17 من هذه الاتفاقية[1].

أما القسم الثالث فقد أدرج موضوع التعاون الدولي بين الأعضاء الموقعة على الاتفاقية، وهذا نظرا لشمولية جرائم الحاسوب والانترنت لجميع أرجاء العالم، ولهذا تعتبر اتفاقية بودابست من بين الاتفاقيات الدولية التي عالجت جريمة الاحتيال الالكتروني ووضحت الأسس المقررة من أجل التعاون الدولي قصد حماية النشاط الالكتروني وردع الجرائم التي تتم بالطرق الالكترونية[2].

رابعا: الحماية القانونية من خلال المنظمة الدولية للشرطة الجنائية (الأنتربول)

هي منظمة مقرها بباريس، تعتبر من أهم الوحدات المتخصصة في مكافحة جرائم الانترنت، تهدف إلى تأكيد ضرورة تكييف التعاون الدولي في مجال التحقيق في الإجرام الحديث الخاص بالمعاملات الالكترونية، وعليه قامت هذه الأخيرة بإتباع استراتجيات محكمة للحد من هذه الجرائم بالتعاون مع مجموعة الثمانية(G8) وذلك عن طريق:

1- إنشاء مركز اتصالات أمني بصفة دائمة ومستمرة مدة 24 ساعة متتالية، عبر الشبكة، على مستوى مصالح الشرطة للدول الأعضاء.

(1) انظر المادة 16 ،17 من اتفاقية بودابست، المرجع السابق.

(2) بزعيم نسرين، الحماية الجنائية للمستهلك الالكتروني، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد ابن باديس، مستغانم، ستة 2020، ص83.

2- الاستعانة بوسائل حديثة في مكافحة هذه الجرائم كاستخدام قاعدة من البيانات المركزية للدول الأطراف والتي بدورها تستخدم برامج مقاربة وتحليل لتلك البيانات المساعدة على كشف الجرائم والتحقيق فيها[1].

الفرع الثاني: وسائل التعاون الدولي مكافحة جرائم بطاقات الدفع الالكتروني

إلى جانب المنظمات الدولية والاتفاقيات والمعاهدات المنبثقة عنها والمقررة في إطار التعاون الدولي، وجب إتباع عدة وسائل للنهوض بمستوى مكافحة الجرائم المعلوماتية والمتمثلة في الوسائل الشرطية والوسائل الإدارية، والوسائل القانونية والتي سنفصل فيها على النحو التالي:

أولا: الوسائل الشرطية لمكافحة جرائم بطاقات الدفع الإلكتروني

تظهر جليا هذه الوسائل من خلال التعاون بين الشرطة الوطنية والشرطة المحلية، بخصوص كيفية اتصال الأجهزة مع بعضها البعض وعليه قامت الشرطة الجنائية الأنتربول بإنشاء كاتب مركزية وطنية في إقليم كل دولة عضو في الأنتربول، تحقيقا لفعالية التعاون الدولي لمكافحة الجرائم المعلوماتية، وتتمثل المهمة وتتمثل المهمة الرئيسية لهذه المراكز في تسهيل مرور الرسائل سواء من خلال نظام الاتصال المركزي الذي يسمح بإجراء الاتصالات العالمية لشركة من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، أو من خلال نظام الاتصال اللامركزي الذي يسمح بالاتصال المباشر بين أجهزة الشرطة ليتيح إمكانية القيام بمختلف الاتصالات عبر الحدود الدولية[2]).

---

[1] الذهبي خدوجة، المرجع السابق، ص ص210، 211.

[2] نوال حاج مخناش، المرجع السابق، ص1130.

ثانيا: الوسائل الإدارية لمكافحة جرائم بطاقات الدفع الالكتروني

تتم هذه الوسائل بتبادل الخبرات بين الدول في مجال جرائم بطاقات الدفع الالكتروني وذلك عن طريق القيام بالزيارات المنظمة وعقد الندوات والمناقشات مع الأجهزة المختصة لكل دولة، ليليها بعد ذلك تنظيم الدورات والندوات التدريبية، وكذا الاجتماعات والمؤتمرات الدولية لينتهي بعقد الاتفاقات والمعاهدات بين الأطراف، وكل ما تم ذكره يندرج تحت الرسائل الإدارية المتبعة لتحقيق التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، حيث أنه يترتب على كل أطراف المجتمع الدولي تطوير برامج خاصة بالعاملين في أجهزتها وتهيئتهم وتدريبهم لتحمل المسؤوليات، وإكسابهم خبرة فنية في مجال الجرائم المستحدثة والتي تشترط توافر الصلاحية العلمية والقدرات الذهنية والفنية لدى المتدرب[1].

ثالثا: الوسائل القانونية لمكافحة جرائم الاعتداء على بطاقات الائتمان

تدخل هذه الوسائل في إطار قانون إجراءات الجنائية، التي توفق بين مصلحتين المصلحة الفردية من جهة، وحكمان قانون العقوبات في حماية المصالح من جهة أخرى، وتختلف هذه الإجراءات من بلد إلى آخر تماشيا مع مبدأ إقليمية القانون الجنائي، واحتراما لسيادة الدول الأخرى، وبالتالي فإن الإجراءات القانونية هاته لا يمكن أن تتم إلا بموافقة كل دولة على إجراء الدولة الأخرى، بناءا على طلب أو اتفاق مسبق بينهما، وأي خروج عن هذا الاتفاق وعن قوانين الإجراءات الجنائية يكون باطلا وغير قابل لتنفيذ.

ومن أهم وابرز المعاهدات الدولية المنظمة للمساعدة الجنائية على النطاق الدولي ما يلي: المعاهدة النموذجية للمساعدة في الوسائل الجنائية، المساعدة النموذجية بشأن التسليم، المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، معاهدات بودابست بشأن مكافحة جرائم

(1) بن تركي ليلى، المرجع السابق، ص322.

نظم المعلومات والاتصالات، المعاهدة الأوروبية لمكافحة جرائم الانترنت، وكل هذه المعاهدات الغاية منها تسهيل إجراءات إقامة الدعوى الجنائية والحكم فيها وتسليم المجرمين[1].

(1) بن تركي ليلة، الرجع السابق، ص323.

الخاتمة

من خلال دراستنا لموضوع بطاقة الدفع الالكتروني اتضح لنا جليا الدور الرئيسي الذي تحققه هذه البطاقة خاصة في المجال المصرفي، وهذا ما ساهم في انتشارها وتزايد التعامل بها مما أدى بدوره إلى تنوع في الجرائم المصاحبة لاستخدامها، لذلك فإن جرائم بطاقات الدفع الالكتروني تهدد حامل البطاقة وجميع أطراف عمليات البطاقة في نفس الوقت دون اعتبار لحدود الدول، ويتم ذلك بالطرق العادية عبر مختلف الأجهزة الإلكترونية وعبر الانترنت وهذا ما يستوجب قيام المسؤولية الجزائية عن هذه الأفعال.

مقابل الجرائم التي تتعرض لها هذه البطاقات كان لابد من البحث عن السبل الكفيلة للحد من أثارها، وقد تبين أنه من الضروري العمل على مراعاة مجموعة من المبادئ والإجراءات المختلفة بهدف حماية استعمال وسائل الدفع الالكتروني، إلا أنه في إطار هذه الجرائم المستحدثة نجد عدم وجود قانون يحمي من جرائم الاحتيال المعلوماتي لطبيعتها الغير المادية، ومن ثم بقاء هذا النوع من القضايا مفتوحا ومعلقا في غياب قانون يكفل حماية أكيدة في مواجهة جرائم الاحتيال المعلوماتي.

إن تعدد المشاكل القانونية التي تعيق التعامل ببطاقات الدفع الالكترونية التي وضحتها الدراسة تتطلب حلولا فعالة وسريعة، وفي ظل هذه المشاكل، وكمحاولة للمساهمة في إنجاح نظام التعامل ببطاقات الدفع الالكترونية فإنه من المناسب التطرق إلى أهم النتائج المتوصل إليها وبعض التوصيات المقترحة:

النتائج

- بطاقة الدفع الالكتروني وسيلة حديثة من وسائل الدفع متعددة الأنواع والوظائف.
- جرائم بطاقات الدفع الالكتروني تدخل ضمن الجرائم المعلوماتية.
- الاستخدام الغير مشروع لبطاقات الدفع الالكتروني لا يقتصر على حاملها فقط بل يمتد إلى جميع محيطها، بداية بالمصدر والتاجر امتداد للغير.

- صعوبة الكشف عن هذه الجرائم نظرا لطبيعتها غير المادية وسهولة حذف البيانات وقابلية الإتلاف.
- ضعف الرقابة المركزية على المؤسسات المالية المصرفية له دور كبير في انتشار هذا النوع من الجرائم المستحدثة.
- قلة النصوص التشريعية المختصة لحماية هذه البطاقات والحد من المخاطر الناشئة عن الاستخدام الغير مشروع لها.
- المشرع الجزائري لم يسن لهذه البطاقات قانونا خاصا ينظمها بل نص على استعمالها ضمن القانون المدني ونص على المسؤولية الجنائية للجناة الذين يستخدمونها استخدام غير مشروع في قانون العقوبات.
- ضعف التعاون الأمني على المستوى الدولي رغم أهميته القصوى في مواجهة هذا النوع من الجرائم.

التوصيات:

- تشديد الرقابة على الأجهزة الالكترونية.
- تبني نظام خاص بوسائل الدفع الالكتروني لمواجهة الاعتداءات الواقعة عليها وسن نصوص سريعة وعدم الاكتفاء بالنصوص التقليدية.
- تشديد العقوبة في حالة كون المعتدي على البطاقة هو نفسه حاملها كذلك كونه أكثر إطلاعا عليها من الغير.
- ضرورة قيام المؤسسات المالية والبنوك المصدرة لبطاقات الدفع الالكتروني والشركات التجارية التي يعمل بها بتدريب العاملين فيها على جميع طرق التزوير التي يستخدمها الجناة.
- ضرورة انضمام الجزائر إلى الاتفاقيات الدولية التي تسعى إلى تحقيق الحماية الجنائية للمعلوماتية وبرامج الحاسب الآلي.

- تذليل الصعوبات والمعوقات التي تواجه التعاون الدولي عن طريق تحديث التشريعات المحلية المتعلقة بالجرائم العلوماتية العامة، وإبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم.

قائمـــــة المراجع

أولا : باللغة العربية

1- الكتب

1. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص(جرائم الفساد، جرائم المال والأعمال، جرائم التزوير)، الطبعة 13، الجزء الثاني، دار هومة، الجزائر، 2013.

2. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة إحدى والعشرون، دار هومة، الجزائر، 2019.

3. أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، دار هومة، الجزائر، 2003.

4. أحمد سيفر، جرائم غسل الأموال وتمويل الإرهاب في التشريعات العربية، المؤسسة الحديثة للكتاب طرابلس، لبنان، 2006.

5. أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، الطبعة الأولى دار الميسرة للنشر والتوزيع والطباعة، عمان، 2010.

6. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان الالكترونية، الطبعة 1، الأردن، دار المسيرة للنشر والتوزيع، سنة 2002 .

7. باسم الفقير، التزوير الإلكتروني، دار اليراع للنشر والتوزيع، الجزائر، 2007.

8. جلال عايد الشورة، وسائل الدفع الإلكتروني، دار الثقافة للنشر والتوزيع، الجزائر، 2008.

9. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقة الائتمان الممغنطة(دراسة تطبيقية في القضاء الفرنسي والقانون المصري)، دار النهضة العربية مصر، 1999.

10. خنفوسي عبد العزيز، قانون الدفع الالكتروني، الطبعة 1، مركز الكتاب الأكاديمي لنشر وتوزيع، عمان، 2018.

11. سليمان ناصر، التقنيات البنكية وعمليات الائتمان، ديوان المطبوعات الجامعية، الجزائر، 2012.

12. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر الآلي في القانون العربي النموذجي، الطبعة الأولى، الفكر الجامعي، الإسكندرية، 2006.

13. عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2013 .

14. عبد الكريم الردايدة، جرائم بطاقات الائتمان (دراسة تطبيقية ميدانية)،الطبعة1، الأردن، دار حامد للنشر والتوزيع، 2013.

15. علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكترونية (دراسة مقارنة)، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2011.

16. عماد علي الخليل، الحماية الجزائية لبطاقات الوفاء(دراسة تحليلية مقارنة)، الطبعة 1، درا وائل للطباعة والنشر، الأردن، سنة2000

17. لوسي عقيلان أبو عقيل، التنظيم القانوني للنقود الإلكترونية كأحد وسائل الدفع، الطبعة الأولى، دار الأيام للنشر والتوزيع، عمان، 2018.

18. محمد توفيق سعودي، بطاقات الائتمان والأسس القانونية للعلاقات الناشئة عن استخدامها، دار الأمير، بيروت، لبنان، 2002

19. نجيمي جمال، جرائم التزوير في قانون العقوبات الجزائري، دار الهومة للنشر والتوزيع، الجزائر، 2013.

20. وسام فيصل محمود الشواورة، الاستخدام غير المشروع لبطاقات الوفاء، الطبعة الأولى، دار وائل للنشر، الأردن، 2013.

21. يزيد بوحليط ، السياسة الجنائية في مجال تبييض الأموال في الجزائر، دار الجامعة الجديدة، 2014.

- **2- المذكرات والرسائل الجامعية**

أ- رسائل الدكتوراه

1. بن تركي ليلة، الحماية الجنائية لبطاقات الائتمان الممغنطة، رسالة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، 2017
2. حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، رسالة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2015
3. الذهبي خدوجة، الحماية الجزائية للمعاملات الإلكترونية(دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2019/2018.
4. مرباح صليحة، الحماية القانونية المدنية والجزائية لبطاقة الائتمان، رسالة لنيل شهادة دكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2019.
5. هداية بوعزة، النظام القانوني للدفع الإلكتروني(دارسة مقارنة)، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان،2017.

مذكرات الماجستير

1. واقد يوسف، النظام القانوني للدفع الالكتروني، مذكرة لنيل درجة ماجستير في القانون، فرع قانون عام، نخصص قانون التعاون الدولي، كلية الحقوق ، مدرسة دكتوراه القانونية والسياسية، جامعة تيزي وزو، سنة 2011.

ب – مذكرات الماستر

1.أسماء بوعقال، الحماية الجنائية لبطاقات الدفع الإلكتروني، مذكرة لنيل شهادة الماستر في قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بالمهيدي، أم البواقي، 2016-2017.

2.حليمة غوباش، جريمة الرشوة في ظل القانون06-01 المتعلق بالوقاية من الفساد ومكافحته، مذكرة لنيل شهادة الماستر، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2014.

3.خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة مكملة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2018.

4.راشد بن صالح بن سفيان الراشدي، الحماية الجزائية لبطاقات الائتمان في التشريع، رسالة للحصول على درجة ماستر، قسم الحقوق، كلية الحقوق، جامعة الشرق الأوسط العماني، حزيران2020.

5.زرقان هشام، النظام القانوني لبطاقات الدفع الإلكتروني، مذكرة الماستر في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016.

6.صونية مقري، المسؤولية المدنية عن الاستخدام الغير مشروع لبطاقات الدفع الالكتروني، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2015.

7.عباسي حمزة، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر، مذكرة الماستر في الحقوق والعلوم السياسية، جامعة أحمد درارية، أدرار سنة 2019.

8.لعليلي زوبيدة، الحماية الجنائية لبطاقة الائتمان المصرفية، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، تخصص قانون عام للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق سنة 2014، 2015.

9.منال بتة، الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2019.

10. مونية معروف، جرائم بطاقات الائتمان الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر شعبة حقوق، تخصص قانون جنائي للأعمال، كلية الحقوق العلوم السياسية، جامعة العربي بن مهيدي، سنة2015/2014.

11. ميهوبي فطيمة، جرائم بطاقات الدفع الإلكتروني، مذكرة لنيل شهادة الماستر في القانون الإداري، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة،2016.

المجلات والمقالات العلمية

1. خلوفي خدوجة "أركان جريمة تبييض الأموال في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الثاني،العدد8، المسيلة، ديسمبر 2017.

2. حسينة شرون، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الدفع الإلكتروني، **مجلة الباحث للدراسات الأكاديمية**، المجلد6، عدد2، جامعة بسكرة، الجزائر،2019.احمدي بوزينة أمنة، "المسؤولية الجزائية عن الاستعمال غير المشروع لبطاقة الائتمان"، مجلة اقتصاديات شمال إفريقيا، العدد13، جامعة الشلف، الجزائر.

3. –دبابش عبد الرؤوف، "وسائل الدفع ما بين الحماية التقنية والقانونية لمستهلك الالكتروني"، **مجلة الاجتهاد القضائي**، مخبر أثر الاجتهاد القضائي على حركة التشريع، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، أفريل 2017.

4. عبد الجبار الحنيص، "الاستخدام غير مشروع لبطاقات الائتمان الممغنطة من وجهة نظر القانون الجزائي"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، المجلد 26، العدد الأول، سنة 2010 .

5. عمراني مصطفى، جريمة تزوير البطاقات البنكية، كلية الحقوق، **مجلة الدراسات والبحوث القانونية**، ، جامعة جيلالي اليابس، سيدي بلعباس، 2012 .

6. ممدوح بن راشيد الرشيد العتري، الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 31، العد62، الرياض، سنة2015.

7. مهند فايز دويكات، حسين محمد الشبلي، "صور الاحتيال والتزوير في بطاقات الائتمانية"، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 29، العدد 58، الأردن، د س ن.

8. نوال الحاج مخناش، رشيد شميشم، التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01.

9. نوال حاج مخناش، "التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني"، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 1، جامعة يحي فارس، المدية، أفريل 2019.

المؤتمرات والملتقيات

1. ليندة بلحارث ، آلية تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري، الملتقى الوطني الثامن حول آلية تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري، الجزائر، يومي 13-14 مارس 2017.

2. محمود أحمد طه، المسؤولية الجنائية غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، كلية الشريعة والقانون غرفة الصناعة، دبي، جامعة الإمارات العربية المتحدة، أيام 13 و12 مايو 2003

3- النصوص القانونية

أ- الاتفاقيات الدولية

اتفاقية بودابست، المتعلقة بالجريمة المعلوماتية، تم الاعتماد عليها وتقريرها في 8 نوفمبر 2001 والتوقيع عليها 23 نوفمبر 2001.

ب- النصوص التشريعية

1. قانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج ، عدد 47 الصادرة في 25 شعبان 130 الموافق ل 10 غشت 2009 .

2. قانون رقم 04-15 مؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر ج ج ، عدد 71 ، الصادرة بتاريخ 10 نوفمبر 2004.

3. قانون رقم04-15 مؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات، ج ر ج ج ، العدد 71 الصادرة في 10 نوفمبر 2004 .

4. قانون 05 -02 مؤرخ في 06 فبراير 2005 المعدل والمتمم لأمر 75-59 المتضمن القانون التجاري، ج ر ج ج ، عدد11، الصادرة في 07 فبراير 2005 .

5. قانون 06-01 مؤرخ في 21 محرم 1427 الموافق لـ 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، ج ر ج ج ، عدد 14، الصادرة بتاريخ 8 مارس2006.

6. أمر رقم 03-01 مؤرخ في جمادى الثانية 1424الموافق لـ 26 أوت 203 المتعلق بالنقد والقرض، ج ر ج ج ، عدد 52 الصادر في 27 أوت 2003 المعدل والمتمم.

7. أمر رقم 03-05 المؤرخ في 19 جويلية 2003 المتعلقة بحقوق المؤلف والحقوق المجاورة، جريدة رسمية العدد 44 الصادرة في 2003/07/23

8. أمر رقم 05-06 مؤرخ في 18 رجب 1426 الموافق لـ 23 أوت 2005 المتعلق بمكافحة التهريب المعدل والمتمم ج رج ج ، عدد 59 ، الصادرة في 24 أوت 2005.

المراسيم التشريعية

المرسوم التشريعي رقم 93-10 المؤرخ في 2 ذي الحجة عام 1413 الموافق ل23 مايو سنة 1993، يتعلق ببورصة القيم المنقولة، ج رج ج، عدد 34، الصادرة بتاريخ 30 مايو1993، المعدل والمتمم.

ثانيا: باللغة الفرنسية

1 - Textes Juridiques

1- Recommandation N°87/598/ CEE de la commission européenne du 8 décombre 1987 portant sur un code européen de bonne conduite en matière de paiement électronique, JOL365,24 décombre 1987.

2- Recommondation N°97/489/ CE du 30 jullet 1997 concernant les opérations effectuées au moyens d'intruments de paiment déctronique, relation entre émetteur et titulaire JOL 208, du 2 Aout 1997.

Site Internet

Document du service des études juridiques du Senat)RF(.La sécurité des transactions réalisées par carte bancaire, in http://www.senat.fr/lc/lc/lc125.html octobre 2003, p01.

فهـــــرس
الموضوعات

11111