جامعة آكلي محند أولحاج –البويرة–

كلية الحقوق والعلوم السياسية

قسم القانون العام

الجرائم الواقعة على بطاقات الدفع الإلكتروني

مذكرة تخرج لنيل شهادة ماستر في القانون العام

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالب: –بوسعيد أسامة

تحت إشراف: الأستاذ(ة) د/ لعشاش محمد

لجنة المناقشة

الأستاذ(ة):.....رئيسا

الأستاذ(ة): الدكتور لعشاش محمد.....مشرفا ومقررا

الأستاذ(ة):.....ممتحنا

السنة الجامعية: 2021/2020

شكر وتقدير

أحمد الله تعالى الذي وفقنا لإنجاز هذا العمل الجاد، متقدما بالشكر الكبير أولا وأخيراً للمولى عزّ وجل الذي يقول في محكم تنزيله:

﴿ لَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ ﴾ سورة إبراهيم، الآية07.

كما أتقدم بالشكر الجزيل لأستاذي المشرف الدكتور: "**لعشاش محمد**" على احتضانه لهذا البحث ورعايته له، وتشجيعه المتواصل لي طيلة إنجاز هذا العمل، وعلى مد يد العون بنصائحه وتوجيهاته القيمة

كما أتقدم بشكري الخاص والخالص لأساتذتي الأفاضل

أعضاء لجنة المناقشة

لموافقتهم على مناقشة وتقويم هذا البحث

كما أشكر كل من مدّ لي يد المساعدة لإنجاز هذا العمل، ولم يبخلوا عليّ بالرأي السديد والنصيحة المخلصة

إلى كل هؤلاء الشكر الجزيل

الطالب: أسامة بوسعيد

إهداء

إلى سيدنا وحبيبنا وقدوتنا ومرشدنا محمد صلى الله عليه وسل

وإلى نبع الحنان ومصدر العطاء التي طالما غمرتني بحنانها، فهي سر نجاحي وتوفيقي... أمي الحبيبة أطال الله في عمرها

وإلى رمز المثابرة والعمل الجاد والمتواصل... أبي العزيز، أطال الله في عمره

وإلى كل من كان سنداً وعوناً إخوتي أحباء قلبي

وإلى رفاق الدرب الطويل والمشوار الصعب أصدقائي

إلى كل هؤلاء أهدي هذا العمل

مقدمة

مقدمة

في ظل التطور التكنولوجي الذي نعيشه في عصرنا هذا، والذي مس جميع القطاعات، ومنها قطاع البنوك الذي طور وسائل الدفع، واعتمد الطريقة الإلكترونية منها كبديل عن وسائل الدفع التقليدية، حيث ظهرت بطاقات الدفع الإلكترونية، والتي تعد من أهم الوسائل الحديثة التي أصبحت تستخدم في شتي المعاملات المصرفية والتجارية لإصدار كروت البنكية لمختلف شرائح المجتمع، وتوزيع نهائيات الدفع وموزعي الأوراق النقدية قصد تحقيق نجاعة ومسايرة القوانين الدولية.

ومع دخول الحاسوب والأنترنت إلى مجتمعنا، وفي كافة جوانب حياتنا، بدأ يظهر نوع جديد من الجرائم تسمي بـ: "الجرائم الإلكترونية"، وهي جرائم متعددة ومتنوعة، وعلى رأسها جرائم بطاقة الدفع الإلكترونية المرتكبة من قبل حاملها والغير والتاج، وبالتالي أصبحت هناك حاجة لتعريف هذا النوع من الجرائم والتوعية ومتابعة ما تحدثه من خسائر مادية ومعنوية كبيرة، فهي تهدد الذمة المالية للمتعاملين بالبطاقة الإلكترونية، بالإضافة إلى ما تقتضي إليه من عدم استقرار في المعاملات المالية المحلية والعالمية، الأمر الذي يقودنا بالضرورة إلى محاولة الإحاطة بالأحكام القانونية لهذه البطاقات التي تشكل دعامة لعدة عمليات قانونية، وكذا الآثار المترتبة عن استخدام هذا البطاقات استخداما غير مشروع وما ينطوي عليه من زعزعة للمعاملات المالية.

بدأ ظهور بطاقات الدفع الإلكترونية في الدول الغربية وفي أمريكا تحديدا، ثم امتدت وانتشرت في باقي الدول الأوربية الأخرى، إلى أن وصلت إلى الدول العربية وإلى الجزائر سنة 1994، وذلك عن طريق البنك الفلاحة والتنمية الريفية وقد كانت مقتصرة علي الوكالات الخاصة، ثم أصدر نفس البنك بطاقة أطلق عليها اسم: "**زيبزارب**" خصصت لزبائن معينين فقط، وفي سنة 1997 أصدرت مؤسسة "**ساتيم**"

المالية بطاقة مصرفية تمكن أصحابها من سحب أموالهم عبر أي صراف إلى في الجزائر، لكنها لم تلقى رواجا كبيرا إلى غاية سنة 2005.

أصبحت الجزائر اليوم تتوفر علي العديد من بطاقات الدفع الإلكترونية، التي تستعمل في الدفع والسحب علي رأسها البطاقة الذهبية لبريد الجزائر، بالإضافة إلى الدفع الخاص بالمصارف المحلية، وكمثال على ذلك: القرض الشعبي الجزائري، وبنك الفلاحة والتنمية الريفية، والصندوق الوطني للتوفير والاحتياط، والبنك الخارجي، وبنك البركة، وبطاقات الدفع العالمية كبطاقة "**فيز كارد**"، وبطاقة "**ماستر كارد**"، والسماح للبنوك الخارجية ذات السمعة العالمية والتي تعمل بنظام الدفع الإلكتروني بنسبة كبيرة في معاملاتها.

لم يعرف المشرع الجزائري بطاقات الدفع الإلكترونية، ولكنه أشار إليها كآلية للدفع في مجموعة من القوانين، كقانون القرض والنقد، والقانون التجاري المعدل سنة 2005. بحيث كل بطاقة صادرة عن البنوك والمؤسسات المالية والمصرفية، تمكّن صاحبها من إجراء مختلف معاملات المالية، من سحب أو تحويل للأموال في حين أن فقهاء القانون، ورغم اختلاف تعريفاتهم لها، إلا أن مواقفهم تصب في مجرى واحد، مفاده أنها أي بطاقة صادرة من الجهة المصدرة لمصلحة شخص معين يحصل بموجبها علي احتياجاته من سلع وخدمات.

وبالرغم من المزايا العديدة التي تقدمها هده البطاقة للمتعاملين بها، إلا أن ذلك صاحبه الكثير من السلبيات التي أثرت على المعاملات المالية والمصرفية، حيث أصبحت هذه البطاقات محلا للعديد من الجرائم من طرف أشخاص تتوفر لديهم الخبرة في المجال المعلوماتي، ما جعلهم يحترفون هذا النوع من الأعمال الإجرامية، وهوما انعكس سلبا علي مصداقية هذه البطاقات والجهات المصدرة لها والأطراف المتعاملين بها، ومن ثم كان لابد من تطوير التشريعات على الصعيد الوطني بما يتلاءم

وخصوصية هذا النوع من الجرائم، إضافة إلى تكثيف جهود التعاون على الصعيد الدولي نظرا لطبيعة هذه الجرائم العابرة للحدود.

أهمية الدراسة

تبرز أهمية دراسة هذا الموضوع في أنه موضوع يتسم بالحداثة والمعاصرة، حيث نسلط الضوء على واحدة من أهم جرائم هذا العصر في مجال المعاملات المصرفية الإلكترونية، والتي تتم بطريقة تقنية غير تلك الطريقة التقليدية المعهودة، وهي في تزايد مستمر ومذهل، وهوما أصبح يشكل خطرا على المعاملات التي تتم بواسطتها أيضا وعلى المتعاملين.

أسباب اختيار موضوع البحث

1- الأسباب الشخصية

تعود أسباب اختياري لهذا الموضوع الهام، إلى رغبتي الملحة في البحث في مثل هكذا مواضيع تقنية وحديثة وعصرية، لمعرفة خبايا وخفايا هذا النوع من الجرائم التي تفشت في عصرنا هذا وطريقة اكتشافها.

2- الأسباب الموضوعية

تعود الأسباب الموضوعية لاختيار هذا الموضوع نظرا لأنه أصبح التعامل ببطاقات الدفع الإلكتروني يعرف انتشارا واسعا في المجال المصرفي، حيث أن مختلف المؤسسات المالية والمصرفية الجزائرية بادرت بإصدار بطاقات الدفع الإلكتروني والخاصة بها، وهذا ما دفعنا للبحث في هذا الموضوع الذي يكتسي أهمية كبيرة في وقتنا الحالي، ومدى ملائمة النصوص التشريعية في مكافحة هذه الجرائم.

أهداف البحث

يهدف هذا البحث إلى محاولة الإلمام بجميع الجرائم وأنواعها الواقعة على بطاقات الدفع الإلكتروني، ومعرفة العقوبات التي أقرها المشرع الجزائري على الجاني،

والتدابير الوقائية والإجراءات الردعية التقليدية منها والمستحدثة من خلال الاطلاع على التشريعات ذات الصلة.

صعوبات البحث

من الصعوبات التي واجهتنا في إعداد هذا البحث هي صعوبة الإلمام بكافة الإجراءات والتمييز بينها، خاصة وأن منها التقليدية والمستحدثة، والتي تجمع بين الجانب الإجرائي والجانب التقني، إضافة إلى نقص المراجع لاسيما الأجنبية منها، وكذلك ندرة الأحكام القضائية الخاصة بهذا النوع من الجرائم.

إشكالية البحث

إلى أي مدى وفّق المشرع الجزائري في حماية بطاقات الدفع الإلكتروني من شتى أنواع الاعتداءات والجرائم الواقعة عليها، وما هي الإجراءات المتخذة ؟

وقد اتبعنا لمعالجة هذه الإشكالية مناهج البحث المناسبة وهي: المنهج الوصفي وهذا لوصف الاعتداءات الواقعة على بطاقات الدفع الإلكتروني، وعرضها عرضا منهجيا وبأسلوب علمي وقانوني بحت، وعلى المنهج التحليلي كذلك وهذا لأهميته في مثل هذه الدراسات القانونية.

وللإجابة على هذه الإشكالية فقد تم تقسيم هذا البحث إلى فصلين، حيث تناولت في **الفصل الأول:** مفهوم جرائم الدفع الإلكتروني والاعتداءات الواقع عليها، حيث تناولته في ثلاثة مباحث، تعرضت من خلالهم إلى مفهوم الدفع الإلكتروني، ووسائل الدفع الإلكتروني، وإلى إساءة استخدام البطاقة من قبل المصدر والتاجر والغير.

وأما في **الفصل الثاني:** فقد تناولت بالبحث والتحليل الإجراءات المتخذة في مواجهة الاعتداءات الواقعة علي بطاقات الدفع الإلكتروني، وذلك في مبحثين تناولت من خلالهما الإجراءات الوقائية، والإجراءات الردعية، وأنهيت بحثي بخاتمة للموضوع استعرضت من خلالها النتائج التوصل إليها.

الفصل الأول:

مفهوم الدفع الإلكتروني والاعتداءات الواقعة عليها

الفصل الأول

مفهوم الدفع الإلكتروني والاعتداءات الواقعة عليها

شهد العصر الحديث ثورة تكنولوجية والتي مست جميع مناحي الحياة، ولم تكن المعاملات المالية في مناي عن ذلك بحيث أفرزت هذه التغيرات نوع جديد من التعاملات يعرف بالتعاملات الإلكترونية، أين تتم مختلف عمليات السحب أو الوفاء بطريقة الإلكترونية عن طريق الدفع الإلكتروني، وبقدر ما سهلت هذه التطورات إجراء مختلف المعاملات المالية إلا أنها لم تمنع من ظهور اعتداءات عديدة جراء الاستخدام غير الشرعي لهذه البطاقة الإلكترونية.

وبذلك سنحاول في هذه الفصل تسليط الضوء: الدفع الإلكتروني، ومختلف الاعتداءات الواقعة عليها من خلال تحديدها، حيث تم تقسيم هذه الفصل إلى ثلاثة مباحث، **(المبحث الأول)** خصص لمفهوم الدفع الإلكتروني، في حين نعرج بالدراسة في **(المبحث الثاني)**: إساءة استخدام البطاقة من قبل صاحبها، و**(المبحث الثالث)** نخصصه لدراسة إساءة استخدام البطاقة من قبل المصدر والتاجر والغير.

المبحث الأول

المقصود بالدفع الإلكتروني

تعتبر شبكة الاتصالات العالمية البيئة التي تنمو فيها المعاملات الاقتصادية الحديثة والدفع الإلكتروني علي وجه الخصوص، فعرفت سرعة انتشارها مذهلة حيث استغرقت فقط أعوام لكي يصل مستخدميها إلى خمسون مليون مستخدم، وذلك باستعمال برامج الحواسيب وتبادل البيانات التي ترسل عبر قنوات وعناوين الإلكترونية يمتلكها كل متعامل علي هذه الشبكة.

وأختلف الفقه حول تسمية هذه البطاقة، فسماها فريق بالبطاقة البلاستيكية وفريق ثاني سماعا البطاقة الدائنية أما فريق الثالث فسماها ببطاقة الوفاء، والبطاقة البنكية وبطاقة الائتمان وغيرها من التسميات. ولكل بطاقة وضيفتاها الخاصة بها علي أساس الاتفاق بين العميل والجهة المصدرة للبطاقة.

من خلال هذا المبحث سنتناول ثلاث مطالب، في **(المطلب الأول)** مفهوم الدفع الإلكتروني، وفي **(المطلب الثاني)** إساءة استخدام البطاقة من قبل صاحبها، وفي **(المطلب الثالث):** الاستخدام غير الشرعي للبطاقة خارج فترة صلاحيتها.

المطلب الأول

مفهوم الدفع الإلكتروني

بطاقة الدفع أو محفظة المقود، الإلكترونية هي وسيلة دفع افتراضية تستخدم في سداد المبالغ قليلة القيمة بشكل مباشر أو غير مباشر.

وتستخدم هذه المحفظة للوفاء سواء عن طريق شبكة الانترنت أوعن غير شبكة الانترنت، وتعرف أيضا بطاقة الدفع البلاستيكية : يطلق اصطلاح البطاقة البلاستيكية علي تلك البطاقات التي تتم معالجتها إلكترونيا لاستخدامها في أغراض متعدد من

خلال معلومات مخزنة عليها والدخول بها علي الآلات المعدة لذلك بغية تحقيق أغراض معينة ومن أهم هذه البطاقات ما يلي[1]:

-بطاقة الدفع الفوري.

-بطاقة الدفع المؤجل أو بطاقة اعتماد النفقات.

-بطاقات التحويل الإلكتروني.

-بطاقات الصرف الآلي.

-بطاقات ضمان الشيكات [2].

وانطلاقا من هذا المطلب قمنا بتقسيمه إلى فرعين ففي **(الفرع الأول)** تعريف الدفع الإلكتروني، وأما في **(الفرع الثاني)** خصائص الدفع الإلكتروني.

الفرع الأول: تعريف الدفع الإلكتروني

تقتضي الدراسة لهذا الفرع بيان معنى بطاقة الدفع الإلكتروني، والتي سنحدد لها أربع جوانب، التعريف اللغوي لبطاقة الدفع **(أولا)**، ثم التعريف التشريعي للدفع الإلكتروني **(ثانيا)**، وبعدها إلى تعريف بطاقة الدفع من حيث الشكل **(ثالثا)**، وأخيرا تعريف بطاقة الدفع من حيث المضمون **(رابعا)**.

أولا: التعريف اللغوي لبطاقة الدفع

هي الرقعة الصغيرة من الورق وغيره يكتب عليها بيان ما تعلق عليه، وكلمة وفاء هي من الفعل وفي، وفي الشيء، يفي، ووفيا، ثم يقال وفي ريش الجناح وفي الشيء وفيا: كثره، وفي فلان نذره وفاء: أداء وفي بعهده: عمل به، وفي فلان حقه أوفاه إياه.

[1]- كميت طالب البغدادي، الاستخدام الغير المشروع لبطاقة الائتمان، دار الثقافة، عمان، 2008، ص ص 52، 53.

[2]- جهاد رضا الحباشئة، الحماية الجزائية لبطاقة الوفاء، رسالة ماجيستير، دار الثقافة، عمان، 2008، ص 22، 24.

ثانيا: التعريف التشريعي للدفع الإلكتروني

عرفها المشرع الفرنسي بأنها: أداة تصدر من احدي مؤسسات الائتمان أو احدي الجهات المنصوص عليها في المادة الثامنة من القانون رقم (84 -16) الصادر في 1984/01/24) والخاص بنشاط ورقابة مؤسسات الائتمان، تسمح لحاملها بسحب أو تحويل النقود من حسابه.

أم المشرع الجزائري فقد انتهج طريق التشريعات العربية التي أرست معالم النظام القانوني لبطاقة الوفاء.

فقام المشرع الجزائري بإيراد تعريفا " لبطاقة السحب والدفع " في التعديل الأخير لقانون التجاري في عام 2005، في الفصل الثالث من الباب الرابع من الكتاب الرابع من القانون التجاري وفي المادة 543 مكرر 23 من القانون التجاري المعدل والمتمم بموجب قانون رقم 05-02 والتي تنص علي ما يلي: في تعريفها لبطاقة الوفاء تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال "[1].

إذا المشرع الجزائري اقتصر في تعديله الأخير للقانون التجاري والمادة 543 مكر 23 من القانون 05-02 علي تعريفه للبطاقة الوفاء فقط ولم يحدد نصوص قانونية أمرة لها، وهذا لتتماشي هذه البطاقة مع الساحة التجارية الحالية كونها جديدة المنشأ في الجزائري[2].

إذا المشرع الجزائري اقتصر في تعديله الأخير للقانون التجاري والمادة 543 مكر 23 من القانون 05-02 علي تعريفه للبطاقة الوفاء فقط ولم يحدد نصوص قانونية

[1]- جهاد رضا الحباشئة، المرجع السابق، ص ص 53، 54.

[2]- أنظر: المادة 23 من القانون 05-02، المؤرخ في 6 فبراير 2005، يعدل ويتمم الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون التجاري، ج ر، العدد 11، سنة 2005.

أمرة لها، وهذا لتتماشي هذه البطاقة مع الساحة التجارية الحالية كونها جديدة المنشأ في الجزائر.

وهناك من عرفها علي أنها، بطاقات تصدر بواسطة مؤسسة مالية باسم أحد الأشخاص وتقوم تلك البطاقة بوظيفتي الوفاء والائتمان، أي أن حاملها يملك أمكانية تتابع سداد المبالغ التي استخدمها من الاعتماد المفتوح من الجانب مصدر البطاقة.

ثالثا: تعريف بطاقة الدفع من حيث الشكل

عرفت بطاقة الائتمان من حيث الشكل أنها " بطاقة مستطيلة من البلاستيك تحمل اسم وشعار المؤسسة العالمية الراعية لها واسم البنك المصدر لها واسم حساب العميل، وأحيانا صورته وتاريخ صلاحيته، ومثبت علي خليفتها شريط مغناطيسي يحمل جميع البيانات المشفرة والخاصة بالبنك المصدر وحامل البطاقة "[1].

وعرفها الدكتور عمر سالم بأنها "بطاقة تمنح بناء علي تعاقد خاص بين أحد الهيئات المالية القائمة علي تسهيل الائتمان وأحد الأشخاص بموجب هذا التعاقد تقوم هذه الهيئة بفتح اعتماد بمبلغ محددا من المال، فإذا أرد حاملها شراء سلعة أو الحصول علي خدمة من أحد المحال المعتمدة لدي تلك الهيئة المصدرة يقوم بتقديم البطاقة إليه، حيث تقوم الجهة المصدرة بتسوية العملية ثم تسترد مقابلها من حامل البطاقة وفقا لشروط فتح الاعتماد "[2].

تعني بطاقة الائتمان في اللغة: الورقة أو الرقعة الصغيرة من الورق وغيره يكتب عليها بيان ما تعلق عليه، وقيل أنها عبارة عن رقعة صغير يثبت فيها مقدار ما تجعل فيه فان كان عينا فوزنه أو عدده، وان كان متاعا فقيمته.

[1]– صلاح الدين حسين السيسي، اقتصاد الفساد، دار الكتاب الحديث، القاهرة، 2012، ص 175.

[2]– ناظم محمد نوري الشعري وعبد الفتاح زهير عبدالات، الصيرفة الإلكترونية، دار وائل للنشر، الأردن، 2008، ص 47.

والمفهوم الأساسي لمعني الائتمان هو التسليم الفوري للسلعة أو الخدمة مقابل الوفاء المؤجل سواء أكان هذه الوفاء بالخصم الفوري أو بالخصم نهاية كل فقرة، وهو معني أشمل من معني الوفاء أو الخصم لذا فكل بطاقة وفاء هي بطاقة اعتماد، أو خصم فوري والعكس غير صحيح[1].

رابعا: تعريف بطاقة الدفع من حيث المضمون

يختلف تعريفها بالاختلاف الجانب الذي يتم تعريفة فيعرف تعريف مصرفيا علي النحو التالي:

" هي عبارة عن صك اسمي يصدره البنك لمصلحة عملية يعطيه الحق في الحصول علي ما يلزمه من سلع أو خدمات تجاه هذه المشروعات، مقابل الوفاء بقيمة السلع والخدمات التي حصل عليها العميل حامل البطاقة استنادا علي الشروط المتفق عليها بينهما "، لكن يعيب علي هذا التعريف أنه حصر إصدارها علي البنوك فقط الأن إصدارها لا يقتصر فقط علي البنوك فقط تصدرها الشركات أو المجموعات الاقتصادية أو المحلات التجارية الكبيرة أو المنظمات المختصة "[2].

الفرع الثاني: خصائص الدفع الإلكتروني

يعد الدفع الإلكتروني بيئة غير مادية للمعاملات المالية النقدية، ونظر لدولية شبكة الانترنت، فالوسائل المستعملة من خلالها تكون ذات طبيعة دولية، بمعني أن تكون مقبولة من طرف جميع الدول، حيث أن عقد الاشتراك في بنوك المعلومات يتم عبر فضاء الإلكتروني مفتوح بين مستخدمين من طرف مختلف الأقطار.

هذا الفرع حدثنا عن خصائص الدفع الإلكتروني من حيث الجهة التي تقوم بخدمة الدفع الإلكتروني **(أولا)**، ثم من حيث وسائل الأمان الفنية **(ثانيا)**.

---

[1]– صلاح الدين حسين السيسي، المرجع السابق، ص 176.

[2]– ناظم محمد نوري الشعري وعبد الفتاح زهير عبدالات، المرجع السابق، ص 47.

أولا: من حيث الجهة التي تقوم بخدمة الدفع الإلكتروني

يترتب علي هذه الطبيعة تواجد نظام مصرفي مسبق لدي طرفي التعامل يتيح الدفع بهذه الوسيلة، أي توفر بإدارة مثل هذه العمليات التي تتم عن بعد ومن شأنها أن توفر الثقة المتعاملين بهذه الوسيلة، فيرتبط هذا الدور بصفة أصلية بالبنوك وغيرها من المنشاة التي تقوم لهذا الغرض، حيث أن إدارة وسائل الدفع في البلاد الأوربية، عدا فرنسا، غير مقتصر علي البنوك، لتسهيل تبادل وتقديم هذه الخدمة بين البلدان الأوروبية[1].

ثانيا: من حيث وسائل الأمان الفنية

يتم الدفع الإلكتروني من خلال فضاء معلوماتي مفتوح، فإن فرصة السطور علي أرقام الكروت أثناء الدفع الإلكتروني قائمة، فيزداد الخطر في الدفع عبر الانترنت عن غيرها من الشبكات باعتبارها فضاء يستقبل جميع الأشخاص من جميع البلدان بمختلف مقاصدهم ونواياهم[2].

المطلب الثاني

إساءة استخدام البطاقة من قبل صاحبها

صاحب البطاقة هو الملك الأصلي لبطاقة الدفع التي صدرت لأجله، وله خالص الحق في التصرف في بطاقة ومع ذلك فقد يقع أن تجاوز حدود استخداماته المتفق عليها في العقد المبرم مع الجهة المصدرة للبطاقة كأن يستخدمها خلال فترة صلاحياتها يتجاوز السقف المسموح به في عمليات السحب والوفاء، وكذا عدم استخدامه لها بعد انتهاء صلاحياتها سواء بانتهاء تلك الفقرة أو بعد إلغاء تفعيل البطاقة من طرف الجهة المصدرة لها.

---

[1]– فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الأنترنت، دار الجامعة الجديدة للنشر، دون طبعة، 2002، ص 100.

[2]– ناظم محمد نوري الشعري وعبد الفتاح زهير عبدالات، المرجع السابق، ص 101، 102.

ومن خلال هذا المطلب تناولنا فيه فرعين، الحصول علي بطاقة الدفع بطريقة غير شرعية **(الفرع الأول)** ، الاستخدام غير الشرعي للبطاقة في عملية السحب والوفاء. **(الفرع الثاني)**

الفرع الأول: الحصول علي بطاقة الدفع بطريقة غير شرعية

الأصل في الحصول علي بطاقة الدفع هو تقديم طلب من طرف العميل إلى الجهة المصدرة للبطاقة وإبداء رغبته في الحصول عليها، يحتوي علي البيانات المطلوبة من العميل، حيث يقوم بالاقتصار علي اسمه ولقبه وعنوانه، والمهنة المادية وتوقيعه، ومن ثم تقرر الجهة المصدرة للبطاقة إصدارها من عدمه.

في ضوء هذا الفرع تحدثنا عن التكيف القانوني للجريمة **(أولا)**، ثم أركان جريمة النصب **(ثانيا)**.

أولا: التكيف القانوني للجريمة

يكيف هذه الفعل الإجرامي علي أنه جريمة نصب، وذلك بموجب المادة 372 قانون العقوبات الجزائري والتي تصب علي أنه " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو عود أو مخالصات إبرام من التزامات أو إلى الحصول علي أي منها، أو شرع في ذلك وكان ذلك بالاختيار لسلب كل ثروة أو بعضها أو الشروع فيه إما بالاستعمال أسماء أو صفات كاذبة أو سلطة خيالية، أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أوفي وقوع حادث أو أية واقعة آخرة وهمية أو الخشية من وقوع شيء منها...علي الأكثر "[1].

ثانيا: أركان جريمة النصب

تتمثل أركان جريمة النصب فيما يلي: الركن المادي **(1)** ، الركن المعنوي **(2)** ، الركن الشرعي **(3)**.

[1]– أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، الطبعة الثالثة، الديوان الوطني للأشغال التربوية الجزائر،2001، ص 146.

1-الركن المادي: يتمثل الركن المادي لهذه الجريمة حسب نص المادة 372 من القانون العقوبات الجزائري في الغش والخداع وتقديم بيانات كاذبة أدت إلى تغير الحقيقة، وعلي أساسها قامت الجهة المصدرة بمنع البطاقة للعميل[1]، كذلك من قام بالاحتيال بواسطة تقديم مستندات مخالفة للحقيقة، والتي تحدث الأصيل في الفوز بالثروة التي سيطلقها إزاء تعامله بالبطاقة.

العلاقة السببية بين الفعل المجرم والنتيجة المتمثلة في استعمال وسائل الاحتيال التي أدت إلى وقوع الضحية في الخدعة وتسليم المال للجاني.

2-الركن المعنوي: جريمة النصب من الجرائم العمدية المعدية التي تقوم علي القصد الجنائي العام والخاص معا، فأما القصد الجنائي العام فيتمثل في العلم والإرادة في ايتانها وتحقيق نتيجتها وأما القصد الجنائي الخاص فيتمثل في الاستعلاء علي مال الغير[2].

3-الركن الشرعي: الركن الشرعي لجريمة النصب هو نص القانوني المجرم لهذه الفعل، بالرجوع إلى نص المادة 372 من قانون العقوبات الجزائري والتي جاء فيها الحبس من سنة علي الأقل إلى خمس سنوات علي الأكثر، وبغرامة من 500 إلى 20000 دينار جزائري بالإضافة لذلك يمكن أن يحكم علي الجاني بالحرمان من جميع الحقوق الواردة في المادة 14 من القانون العقوبات الجزائري أومن بعضها وبالمنع من الإقامة لمدة سنة علي الأقل وخمس سنوات علي الأكثر[3].

---

[1]- أمين طالب البغدادي، الإستخدام الغير مشروع لبطاقة الإئتمان المسؤولية الجزائية والمدنية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 189.

[1]- أسامة حمدان الرقيب، جرائم النصب والاحتيال (الأساليب -المظاهر -العلاج)، الطبعة الأولي، دار ياقا العلمية للنشر والتوزيع، عمان،2012، ص 27.

[1]- القانون رقم 09-01 المؤرخ في 29 صفر 1430هـ الموافق ل 25 فبراير 2009، يعدل يتمم الأمر 66-156 المؤرخ في 28 صفر 1386هـ الموافق ل 08 يونيو 1966، المتضمن قانون العقوبات، ج ر، العدد 15، سنة 1946، الصادر بتاريخ 08 مارس 2009.

الفرع الثاني: الاستخدام غير الشرعي للبطاقة في عملية السحب والوفاء

سنتعرض من خلال هذا الفرع إلى الاستخدامات الغير شرعي إبان فترة صلاحية البطاقة الإلكترونية، سنتناول تجاوز الحاصل للسقف المسموح به للبطاقة **(أولا)**، استخدام البطاقة في عمليات غسيل الأموال **(ثانيا)**.

أولا: تجاوز الحاصل للسقف المسموح به للبطاقة

يقوم البنك بإصدار بطاقات الدفع لعملائه لتسهيل عملية صرف المبالغ المالية في أي وقت بواسطة أجهزة الصرف الآلي، ولكن بطاقة سقف محدد لا يمكن تجاوزه سواء في عملية الدفع أو الوفاء وذلك تماشيا مع النظام المعمول به في البنك.

ودوره ينقسم تجاوز الحاصل للسقف المسموح به للبطاقة إلى تجاوز الحامل لرصيده في لسحب **(1)** ، تجاوز الحامل لرصيده في الوفاء **(2)**.

1-تجاوز الحامل لرصيده في السحب: وتكون البطاقة، صحيحة من الوظائف التي تمنحها بطاقة الدفع لحاملها، ويتم السحب بواسطة أجهزة الصرف الآلي وذلك بتقديم البطاقة ورقمها أو بواسطة أحد فروع البنوك المصدرة للبطاقة، والأصل في سحب المبلغ بأن ليجاوز الرصيد الموجود في البطاقة، وإذا قام الحامل بذلك يتغير قيامه بسلوك غي شرعي في مجال المعلوماتي[1].

أما في ما يخص مدي انطباع النصوص التقليدية علي هذه الجريمة فقد اختلف الفقه والقضاء ذلك علي نحو الآتي:

الرأي الأول: يري جانب من الفقه أن هذه الفعل الذي قام به صاحب البطاقة يخضع للنصوص التجريمية اختلفوا حول التكيف الصحيح له وانقسموا بدورهم إلى ثلاثة أراء كالآتي[2]:

---

[1]- عبد الكريم الرديدة، جرائم بطاقة الإئتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013، ص 59.

[2]- علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكتروني (دراسة مقارنة)، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2011، ص 33.

يري البعض منهم أنها خيانة أمانة لأن الجاني تحصل علي بطاقة من بنك علي سبيل الائتمان واستعملها بطريقة تعسفية في الحصول علي أموال بغير وجه حق، في حين يري البعض الأخر أنها جريمة سرقة، لكن الرأي لم يسلم من الانتقاد علي أساس أن البنك هومن سلم الأموال للجاني.

وذهب فريق ثالث إلى أنها جريمة احتيال، وهذا الرأي أيضا لم يسلم من الانتقاد لأن البطاقة استعملت من طرف حاملها الشرعي.

وفي الوقت الحالي فأن كل هذه الآراء أصبحت فروض نظرية، ولم يعد لهذا السلوكيات في الوقت العملي وجود علي الأغلب، وذلك بالنظر إلى تطور التقنيات في المجال الإلكتروني في مجال الأجهزة الآلية لسحب النقود في الأماكن المتعامل بها بالبطاقة حيث تعطي هذه الأجهزة بيان لحال البطاقة فيما اذا كانت تحتوي علي رصيد كافي أم لا، ومن ثم فأن هذه الفعل لا يعد جريمة في القوانين الحالية[1].

الرأي الثاني: علي عكس من الرأي الأول فأن الرأي الأخر من الفقه يري بأن هذه الفعل لا ينطوي علي أنه جريمة، ولا يعتبر إلا مجرد إخلال بالالتزامات المتعاقدية بين الحامل والبنك وبالتالي تتم مساءلة الجاني في الشق المدني دون الجزائي.

2-تجاوز الحامل لرصيده في الوفاء: تمنع هذه البطاقة لحاملها تسديد ثمن مشترياته عن طريق تحويل مبلغها من حسابه لحساب التاجر عن طريق البنك[2]، وفي هذه الحالة يقوم الحامل باستخدام بطاقته حيث يقدمها للتاجر بغية الحصول علي خدماته علي أن يقوم البنك لاحقا بتسديد قيمتها بناء علي ما يوجد في رصيد الحامل، شرط أن لا تتعد هذه القيمة المبلغ الموجود في رصيد البطاقة وبعدها يقوم الحامل بتسديد المبلغ للبنك لكنه يتجاوز سقف البطاقة، وهذا ما يطرح السؤال حول قيام الجريمة من عدمه.

---

[1]- عبد الكريم الردايدة، المرجع السابق، ص 59.

[2]- أمجد حمدان الجهني، المسؤولية المدنية عن استخدام غير مشروع لبطاقة الدفع الإلكتروني، دار المسيرة، عمان، 2010، ص 131.

اختلفت أراء الفقهاء حول هذه المسألة فمنهم من يري بضرورة خضوع الجاني للمسألة الجزائية ومنه من رفض ذلك علي النحو التالي:

الرأي الأول: يري أصحاب هذا الرأي أن الحامل الذي يتحصل علي المشتريات بالرغم من عدم وجود رصيد في بطاقته يوفي قيمتها، فأنه يخضع للمسألة الجزائية عن جريمة النصب[1].

الرأي الثاني: يذهب أصحاب هذه الرأي إلى الدفع بعدم انطواء الفعل علي أي جريمة، ولا تعد وأنها إخلال بالتزامه تجاه البنك المتعامل معه، ويترتب عليه المسؤولية العقدية لتعويض الضرر[2].

ثانيا: استخدام البطاقة في عمليات غسيل الأموال

بالنظر لكون بطاقات الدفع أصبحت في الوقت الراهن تحتل مكان النقود، والتعامل بها من الصعب تعقبه فحتي ولو كانت صحيحة وتم استعمالها من قبل حاملها الشرعي فأنه قد يستعملها بطريقة غير شرعية في عمليات غسيل الأموال.

ويكون ذلك بطريتين كما يلي: استخدام البطاقة في أجهزة الصراف الآلي **(1)** ، غسيل الأموال بواسطة الوفاء بالبطاقة **(2)**.

1-استخدام البطاقة في أجهزة الصراف الآلي: وفي هذه الحالة يقوم الحامل باستصدار طلبات متتالية لبطاقة الدفع، لصالحه ولعائلته وكذلك لموظفيه ولمعاونيه قصد الاستخدام الوطني والدولي وذلك بضمان ودائع الشركة النقدية أو العينية ويتم استخدامها في مجال التحويلات المالية الإلكترونية بواسطة أجهزة الصراف الآلي في

[1]- وسام فيصل محمود الشواورة، المسؤولية القانونية عن الاستخدام غير المشروع لبطاقات الائتمان، الطبعة الأول، دار وائل للنشر، عمان، 2013، ص 79.

[2]- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، جرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2015، ص 195.

عمليات غسيل الأموال، ويتم إجراء التحويلات التي تصل إلى الخارج وقبل أن تستقر يتم سحبها وتجميعها وتحويلها بمبالغ كبير.

وبعد ذلك يقوم حامل البطاقة بصرف هذه المبالغ من أجهزة الصراف الآلي باستخدام رقمه السري ثم يقوم الفرع الذي صرف منه أو بواسطة أجهزته بطلب تحويل المال إليه من الفرع مصدره البطاقة، ليقوم هذ الأخير بعملية التحويل تلقائيا وخصم قيمة المبلغ من حساب عميله، وبهذه الطريقة يكون قد تهرب من الالتزامات علي التحويلات[1].

2-غسيل الأموال بواسطة الوفاء بالبطاقة

-**مرحلة التوظيف:** وفيها يتم إيداع الأموال المستعملة في أعمال مشبوهة في احدي البنوك الدولية أو المحلية من أجل الحصول علي بطاقة الدفع بقيمة الرصيد المودع[2].

-**مرحلة التغطية:** وفي هذه المرحلة يتم إخفاء مصدر الأموال المشبوهة فيتم استخدامها في شراء المعادن واللوحات الفنية الثمينة، سواء بطريقة مباشرة أو عن طريق الغير بواسطة بطاقة الدفع الإلكتروني أو الانترنت بالإضافة لاستخدام نظم الحماية والتشفير لضمان سرية هذه العمليات[3].

-**مرحلة الدمج:** وأخير في هذه المرحلة يتم دمج الأموال المشبوهة في النظام المالي واختلاطها بالأموال المشروعة فتصبح مثلها، وذلك من خلال وضع الأموال المشبوهة في الاقتصاد وتكون هذه المرة معلومة المصدر كبيع اللوحات نفسها التي اشتراها من قبل، ويتم بيعها نقدا أو لقاء شيك أو حوالة مالية مسحوبة علي بنك أخر.

---

[1]- وسام فيصل محمود الشواورة، المرجع السابق، ص ص، 81، 80.

[2]- أمجد حمدان الجهني، المرجع السابق، ص 136.

[3]- عبد الكريم الردايدة، المرجع السابق، ص 89.

المطلب الثالث

الاستخدام غير الشرعي للبطاقة خارج فترة صلاحيتها

كما وسبق أن تطرقنا في المطلب الأول إلى الاستخدام غير الشرعي للبطاقة خلال فترة صلاحيتها من قبل صاحبها، كذلك فأن هذه الأخير يقوم بإساءة استخدامها خارج فترة صلاحيتها عند انتهاء مدتها، أو بعد أن يتم إلغائها من قبل البنك المصدر لها ورغم ذلك يتم استخدامها خارج في عمليات السحب والوفاء.

سنتناول في هذا المطلب فرعين، الاستخدام غير الشرعي للبطاقة **(الفرع الأول)** سنتطرق ، إلى الاستخدام المقنع للبطاقة من صاحبها **(الفرع الثاني)**.

الفرع الأول: الاستخدام غير الشرعي للبطاقة

بناء علي العقد المبرم بين العميل حامل البطاقة والبنك المصدر لها، فأن التعامل بها يحدد بمدة معينة وغالبا ما تكون هذه المدة سنة واحدة، يبدأ سريانها من تاريخ إصدار البطاقة وتكون قابلة للتجديد دوريا، وتمتلك الجهة المصدرة لها الحق في إلغائها أو سحبها من الحامل اذا أساء استخدامها، ومنه فأن العمل بالبطاقة له وقت محدد كما ذكر آنفا لكن ورغم علم الحامل بذلك فأنه يتمتع عن ردها للبنك ويستمر في استخدامها، ويتجلى ذلك في ما يلي: استخدام البطاقة الملغاة **(أولا)**، إساءة استخدام بطاقة منتهية الصلاحية **(ثانيا)**.

أولا: استخدام البطاقة الملغاة

البطاقة الملغاة هي التي أقرت الجهة المصدرة لها أمرا بإيقاف العمل بها نتيجة تعسفه في استعمالها بموجب الوظائف التي تمنحها له، وإخلاله بالتزامه التعاقدي معها ومع ذلك ورغم علم الحامل بإلغائها يقوم باستعمالها. [1]

[1]– عبد الجبار الحنيص، "الاستخدام غير المشروع لبطاقات الائتمان الممغنطة في وجه نظر القانون الجزائي"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010.

وفيما سيأتي سنتناول هذه المسألة فيما إذا كانت تشكل جريمة من عدمها، الامتناع عن رد بطاقة الدفع الملغاة أو منتهية الصلاحية **(1)** ، طرق استخدام البطاقة الملغاة. **(2)**

1-الامتناع عن رد بطاقة الدفع الملغاة أو منتهية الصلاحية: عند انتهاء صلاحية بطاقة الدفع أو تم إلغائها من قبل البنك، فأن الحامل يلتزم بإرجاعها للبنك لأنها سلمت له كعارية استعمال، وعند رفضه إعادتها رغم علمه بإلغائها يعتبر خائنا للأمانة لأنه تسلمها بناء علي العقد الذي تم إبرامه بينه وبين الجهة المصدرة، ويتعين عليه إعادتها عند انتهاء مدة العقد أو إلغائه لأنها تبقى ملكا للجهة المصدرة وليست له[1].

-مدي انطباع النصوص القانونية التقليدية علي الجريمة: كما ذكر سابقا فأن البطاقة ملك وتسليم للحامل علي أنها عارية استعمال وإذا امتنع عن ردها يعتبر خائنا للأمانة، وقد عالج المشرع الجزائري هذه الجريمة في المادة 376 من القانون العقوبات الجزائري بقولها: " كل من اختلس أو بدد بسوء نية أوراق تجارية أو نقودا أو بضائع أو أورقا مالية أو الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر شرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل. معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبها لجريمة خيانة الأمانة.." [2].

أ-الركن المادي لجريمة خيانة الأمانة: يتمثل الركن المادي لجريمة خيانة الأمانة حسب نص المادة 376 من القانون العقوبات الجزائري في ثلاثة عناصر:

---

[1]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الطبعة الأولي، دار الفكر العربي، الاسكندرية، 2002، ص، 383.

[2]- خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، مذكرة مكملة لنيل شهادة الماجستير في الحقوق، بن صغير محفوظ، قسم الحقوق، كلية الحقوق، العلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016، ص111.

الاختلاس أو التبديد: يكون بنقل الشيء من حيازة مؤقتة إلى حيازة دائمة وفي نيته تملك هذا الشيء وعدم إرجاعه لصاحبه، وهذا ينطبق الأمر علي حامل البطاقة الذي رفض إرجاعها إلى الجهة المصدرة لها بعد انتهاء صلاحياتها أو إلغائها ويستمر العمل بها[1].

محل الجريمة: يتمثل المحل في جريمة خيانة الأمانة مال منقولا حسب نص المادة 376 من القانون العقوبات الجزائري، وهذ ينطبق علي بطاقة الدفع التي تتضمن مال بموجبه يتصرف به الحامل لتسهيل تعاملاته المالية، كذلك ينطبق عليها لفظ (أية محررات أخري) الدفع تعتبر محررات مصرفية[2].

تسليم الشيء: حتي تقوم جريمة خيانة الأمانة يلزم تسليم الشيء علي شكل حيازة مؤقتة كوديعة، أو إجازة أو وكالة أو رهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر شرط ردها، وهذا ينطبق علي بطاقة الدفع لأن الحامل تسليمها من الجهة المصدرة علي سبيل الحيازة المؤقتة وقد اتفق في العقد المبرم بينهما علي إرجاعها عند إلغائها أو انتهاء مدة صلاحيتها.

ب-الركن المعنوي لجريمة خيانة الأمانة: جريمة خيانة الأمانة من الجرائم العمدية التي يلزم لقيامها القصد الخاص والقصد العام كما سيأتي تباينه:

القصد العام: بعنصرية العلم والإرادة أي أن الجاني يعلم أن فعله يعتبر جريمة يعاقب عليه القانون، ورغم ذلك تتجه إرادته لإثباتها.

-**القصد الخاص:** ويتمثل في نية الجاني في الحيازة والتملك وحرمان مالكه الأصلي منه، الأمر الذي يسبب له ضرر وعندما تسقط هذا علي بطاقة الدفع فأن الحامل قد احتفظ بالبطاقة وامتنع عن ردها واستمر بالعمل بها علي الرغم من علمه بأنها ملك

[1]- خشة حسيبة، المرجع السابق، ص 42.

[2]- علي عدنان الفيل، المرجع السابق، ص 111.

للبنك وتسليمها بصفة مؤقتة، وقد انتهت مدة صلاحيتها أو تم إلغاؤها وهذا السلوك بسبب ضرر للبنك الذي لا يعلم بالاستمرار في استخدامها[1].

ج-الركن الشرعي لجريمة خيانة الأمانة: إن العقوبات المقررة لجريمة خيانة الأمانة نصت عليها المادة 376 من قانون العقوبات الجزائري، بحث خص المشرع عقوبات أصلية والأخرة تكميلية كالآتي:

-**العقوبات الأصلية:** الحبس من ثلاثة أشهر إلى 3 سنوات وغرامة مالية من 20000 إلى 100000 دينار جزائري.

-**العقوبات التكميلية:** بالرجوع إلى نص المادة 9 من القانون السابق الذكر فإن هذه العقوبات تتمثل في الحرمان من الحقوق الوطنية والمدنية، والمنع من الإقامة لمدة أقصاها 5 سنوات، كما يمكن للجهة القضائية المختصة أن تحكم عليه بعقوبات تكميلية اختيارية تتمثل في المنع من التعامل ببطاقة الدفع أقصاها 5 سنوات[2].

2-طرق استخدام البطاقة الملغاة: قد يتم استخدام البطاقة الملغاة في عملية السحب، حيث يقوم الحامل باستعمال بطاقته الملغاة في سحب النقود من أجهزة الصراف الآلي، في هذه الحال يقوم التساؤل هل يتساءل جزائيا عن ذلك أولا ؟

في هذا الصدد اختلفت أراء الفقه وكذلك القضاء حول هذه المسألة حيث يري فريق أول بأن الفاعل تتم مساءلته جزائيا عن جريمة الاحتيال، في حين ذهب فريق أخر إلى القول بأن الفاعل يتساءل عن جريمة خيانة الأمانة[3].

أما في وقتنا الحالي ومع التطور التكنولوجي الحاصل في استحداث برمجة الصراف الآلي، فقد أصبح هذه التصرف ليشكل أس جريمة لأن تلك البرامج كفيلة

---

[1]- خشة حسيبة، المرجع السابق، ص ص، 112، 113.

[2]- أنظر المادة 376 من قانون العقوبات.

[3]- بن شهرة شول، الحماية الجنائية للتجارة الإلكترونية، مذكرة مقدمة لنيل درجة دكتوراه في القانون، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2010، ص22.

باكتشاف ما إذا كانت هذه البطاقة صالحة للاستخدام، أو أنها منتهية الصلاحية أم تم إلغاؤها من قبل مصدرها[1].

إضافة إلى استخدام البطاقة الملغاة في عملية السحب فقد يتم استخدامها في عملية الوفاء أيضا لتسديد ثمن المشتريات، ومن المعلوم أنها تحمل ضمن البيانات الواردة عليها تاريخ انتهاء وجب علي التاجر أن يتحقق من مدة صلاحيتها ولا يقبلها، وعندما يهمل هذا الالتزام من قبل التاجر فأنه يتحمل تبعات تصرفه ولا يستطيع مطالبة البنك بتسديد ثمن المشتريات، كما تجدر الإشارة أيضا عند إخطار التاجر من قبل البنك أنها ملغاة قبل التعامل بها، فلا يحق له بعد ذلك الرجوع إلى البنك[2].

أما فيما يخص التكيف القانوني لهذه الواقعة فهناك رأيين بخصوص هذه المسألة كما يلي:

الرأي الأول: يري أن الفاعل مرتكب لجريمة خيانة أمانة كما سبق ذكرها وحجتهم في ذلك أن أصحاب البطاقة استمر في استعمال بطاقة وامتنع عن ردها فيعتبر إساءة الأمين استعمال الشيء إضافة لفعل الاختلاس أو التبديد المتمثل في الاستمرار في استعمال البطاقة علي نحو يجرده من كل قيمته أو جزء منها[3].

غير أن هذا الرأي لم يسلم من الانتقاد، كون جريمة خيانة الأمانة هو أن يستعمل الجاني المسلم إليه استعمالا لا يجوز أن يصدر عن غير المالك، ويظهر للناس علي أنه هو الملك الحقيقي للشيء وهذا لا يتوفر في حامل البطاقة الملغاة أو المنتهية الصلاحية، ومنه لا يعد مرتكبا لجريمة خيانة الأمانة.

الرأي الثاني: يري أن هذا الفعل يشكل جريمة احتيال لأنه يكون مصحوبا بأعمال احتيالية لإقناع التاجر بعدم إلغائها، ويوهمه بوجود ائتمان وهمي يهدف للحصول من

---

[1]– بن شهرة شول، المرجع السابق، ص23.

[2]– عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص548.

[3]– المرجع نفسه، ص ص 44، 45.

البنك علي الوفاء بقيمة مشترياته من الجار، مما يشكل استيلاء علي ثروة الغير، بالإضافة لذلك فقد اعتمد الجاني علي صفات كاذبة للحصول علي مبتغاه لأنه صفة حامل البطاقة كانت له وثم زالت عنه بإلغائها أو انتهاء صلاحيتها، كذلك ادعاء بأنه وكيل عن الشخص طبيعي أو المعنوي، وهذه الأسباب مما تقوم عليها جريمة الاحتيال، وهكذا فانه بمجرد أن يقدم الجاني بطاقة الائتمان للتاجر الذي لا يعلم بإلغائها ولم يتم إخطاره بذلك فأنه تقوم جريمة احتيال القائمة علي استعمال صفات كاذبة للحصول علي أموال الغير[1].

ثانيا: إساءة استخدام بطاقة منتهية الصلاحية

الأصل أنه عند انتهاء مدة صلاحية بطاقة الدفع، يقوم الحامل بتجديدها فيسلم بطاقته القديمة ويستلم الجديدة، لكنه في بعض الأحيان يحتفظ بها ويستمر في استخدامها سواء في الوفاء لدى التاجر أو عند سحب النقود من أجهزة الصراف الآلي[2].

وفي هذا الصدد يثور التساؤل حول ما مدى إمكانية مساءلته جزائيا ؟ وعن أي جريمة يسأل ؟، استغلال استخدم بطاقة منتهة الصلاحية في حالتين استخدام بطاقة الدفع منتهية الصلاحية في السحب **(1)** ، استخدام بطاقة الدفع منتهية الصلاحية في الوفاء. **(2)**

1-استخدام بطاقة الدفع منتهية الصلاحية في السحب: في الغالب وطبقا لنظام البرمجة في أجهزة استخدام بطاقة الدفع في السحب النقود، تقوم الماكنة بابتلاعها أو رفضها وذلك إشعارا من البنك بتجديدها، ولكن أحيانا يتم صرف القيمة من طرف الجهاز وتصدر مديونية علي العميل دون أن يتعرض لأنه لم يقصد، ومن خلال ذلك نميز بين حالتين:

[1]- علي عدنان الفيل، المرجع السابق، ص 47.

[2]- عبد الكريم الردايدة، المرجع السابق، ص 215.

فأما أولاهما فهي استخدام الحامل بطاقته منتهية الصلاحية في سحب النقود خطأ، وهذا يكون الحامل ليعلم بانتهاء صلاحيتها عندئذ تتم مساءلته جزائيا عن جريمة خيانة أمانه ويخضع لأحكامها[1].

وأما في الحالة الثانية فهي استخدام الحامل لبطاقته في السحب مع علمه بانتهاء صلاحيتها، وفي هذا الحالة نميز بين نوعين من المساءلة الجزائية، فقد يقوم الحامل بعملية سحبه للنقود بطريقة المعتادة وبذلك يسأل عن جريمة خيانة الأمانة[2]، كما قد يقوم الحامل بعملية سحبه للنقود معتمدا علي الطرق الاحتيالية، فيسأل عن جريمة احتيال.

وكما تجد الإشارة إلى أن هذه الآراء تبقي مجرد نظريات في الوقت الحالي الذي يتميز بالنجاح التكنولوجي في الإلكترونيات، ومن بينها أجهزة الصراف الآلي الخاص ببطاقة الدفع الإلكتروني والتي تكون مبرمجة للامتناع عن صرف نقود البطاقة منتهية الصلاحية.

2-استخدام بطاقة الدفع منتهية الصلاحية في الوفاء: يمكن هذا الاستخدام عندما يقوم الحامل بتقديم بطاقته منتهية الصلاحية للتاجر للوفاء بقيمة الخدمات المقدمة له من طرف البنك[3].

اعتبر الفقه أن هذا الفعل لا ينطوي تحت أي جريمة لأنه عند القيامّ بالوفاء للتاجر بواسطة بطاقة منتهية الصلاحية، فهو فعل ساذج ويمكن كشفه بسهولة فهو أمر يلتزم به تعاقديا، حيث يجب عليه الاطلاع علي تاريخ صلاحية البطاقة الظاهر علي

[1]- علي عدنان الفيل، المرجع السابق، ص30.

[2]- المرجع نفسه، ص42.

[3]- عبد الحكيم أحمد محمد عثمان، أحكام البطاقات الائتمانية في القانون والآراء الفقهية الإسلامية، الطبعة الأولي، دار الفكر الجامعي، الاسكندرية،2007، ص338.

الوجه الأمامي لها، ومنه فان التاجر هو من يتحمل مسؤولية الضرر المترتب عليه لأنه قبل الوفاء ببطاقة منتهية الصلاحية، أخل بالتزاماته التعاقدية[1].

كذلك في هذه الحالة قد يسأل التاجر عن الجريمة احتيال بصفته شريك إلى جانب الحامل الفاعل الأصلي، وذلك عند قبوله التعامل ببطاقة منتهية الصلاحية إضرارا بالبنك كأن يقوم بتزوير تاريخ انتهاء صلاحية البطاقة علي الفاتورة، أو يقوم بالإعلان عمدا عن تاريخ كاذب لانتهاء صلاحية البطاقة[2].

الفرع الثاني: الاستخدام المقنع للبطاقة

نتطرق في الاستخدام المقنع لبطاقة الدفع من قبل حاملها والذي يكون في ثلاث حالات، الإبلاغ غير الصحيح عن فقدان البطاقة أو سرقتها **(أولا)**، التواطؤ ما بين الحامل والغير **(ثانيا)**، الادعاء غير الصحيح بعد استخدام البطاقة **(ثالثا)**.

أولا: الإبلاغ غير الصحيح عن فقدان البطاقة أو سرقتها

في هذه الحالة يقوم صاحب البطاقة بإبلاغ الجهة المصدرة لها عن فقدان بطاقته أو سرقتها في الوقت الذي لاتزال في حوزته، ويستمر باستعمالها سواء في السحب أو الوفاء فأما عملية السحب فأن أجهزة الصراف الآلي الحديثة مبرمجة لرفض البطاقة المفقودة أو المسروقة، وأما بالنسبة لعملية الوفاء فأن الحامل وخوفا من اكتشاف أمره يقوم باستخدامها عند التاجر الذي يتعاملون بألة الطباعة اليدوية التي لا يمكن اكتشاف وضعية البطاقة من خلالها، علي العكس من التاجر الذي يستعملون الجهاز الإلكتروني الذي يكتشف حالات الغش بسهولة، وهذا يشكل احتيال علي التاجر الغرض منه تحصيل قيمة البضاعة من البنك بدلا منه، والاستيلاء علي مال البنك دون وجه حق. [3]

---

[1]– أمين طالب البغدادي، المرجع السابق، ص174.

[2]– علي عدنان الفيل، المرجع السابق، ص44.

[3]– أمجد حمدان الجهني، المرجع السابق، ص 142.

ثانيا: التواطؤ ما بين الحامل والغير

إن تواطؤ ما بين الحامل الشرعي للبطاقة والغير التحايل علي المصدر يقوم ذلك بأن يقوم الحامل بإعطاء بطاقة للغير لكي يستعملها في عملية السحب وتزوير وتوقيعه، بعدما يقوم الحامل بالاعتراض عن عمليات السحب يطعن بتزوير وتوقيعه لا كيلا يتم خصم المبلغ المسحوب من لأجله.

وكذلك يتم إعطاء بيانات البطاقة ورقمها بهدف تزوير بطاقة أخري من خلالها، للتحايل علي المصدر والتجار الآخرين وللحصول علي أموالهم[1].

ثالثا: الادعاء غير الصحيح بعد استخدام البطاقة

هذه الحالة يقوم صاحب البطاقة باستعمالها في السحب أو الوفاء أثناء سفره إلى بارما، بحيث ينتفع بما تقدمه من خدمات كشراء السلع المختلفة من التاجر والمحلات خلال فترة مكونة في هذه البلد وبعد عزته لبلده يدعي عدم سفره، وعدم استخدام بطاقة، ويعتمد في إثبات ذلك علي جواز سفر إثبات ذلك علي جواز سفر أخر[2].

[1]– أمجد حمدان الجهني، المرجع السابق، ص 142.

[2]– لبني عمر سقاوي، المسؤولية المصرفية في الاعتماد المالي، الطبعة الأول، منشورات الحلبي للحقوقية، بيروت، 2006، ص 252.

المبحث الثاني

إساءة استخدام البطاقة من قبل المصدر والتاجر والغير

تعتبر الجهة المصدرة والتاجر اطراف في العلاقة التعاقدية لبطاقة الدفع الإلكترونية، وما ترتبه هذه العلاقة من التزامات، فالجهة المصدرة، هي البنك الذي يمنحها للعمل وفق عقد بينهما، وأما التاجر هو الجهة التي تقبل العمل بالبطاقة من طرف حاملها للوفاء بثمن السلع والخدمات التي يقدمها له بناء علي توقيعه علي فاتورة الشراء بعد التأكد من هويته والتأكيد من صحة البطاقة، أما الغير فهو خارج العلاقة التعاقدية للبطاقة ولا يترتب علي أي التزامات وهو أي شخص من العامة قد يتصادف أن تقع البطاقة في يده في حالة ضياعها.

قمنا بتقسيم هذا المبحث إلى مطلبين، الاستخدام غير الشرعي للبطاقة من قبل المصدر والتاجر **(المطلب الأول)** ، الاستخدام غير الشرعي للبطاقة من قبل الغير. **(المطلب الثاني)**

المطلب الأول

الاستخدام غير الشرعي للبطاقة من قبل المصدر والتاجر

له استخدامات عديدة بالنسبة الغير شرعية الواقعية علي بطاقات الدفع الإلكتروني من قبل الجهة المصدرة لها، باعتبارها شخص معنوي فإن موظفوها هم المرتبون لهذه الجرائم، بإضافة إلى ذلك فقد ترتكب هذه الجرائم من قبل التاجر.

نستعرض من خلال هذا المطلب ، الاستخدام غير الشرعي من قبل المصدر **(الفرع الأول)** ، الاستخدام غير الشرعي من قبل التاجر **(الفرع الثاني)** ، مسؤولية موظفو البنك والتاجر عن الأعمال غير الشرعية. **(الفرع الثالث)**

الفرع الأول: الاستخدام غير الشرعي من قبل المصدر

الحدود الممنوح للبنك لا يعطيه صلاحية الانحراف عن مهامه، حيث يعتبر الجهة المصدرة لبطاقة الدفع الإلكتروني وبما أن شخص معنوي يقوم بالاعتداء علي البطاقة بواسطة موظفيها حيث يتم ذلك من خلال تواطؤهم مع صاحب البطاقة أو مع الغير.

في ضوء هذا الفرع سنتناول فيه تواطؤ موظفي البنك مع العميل **(أولا)**، تواطؤ موظف البنك مع التاجر **(ثانيا)**، تواطؤ موظف البنك مع الغير **(ثالثا)**.

أولا: تواطؤ موظفي البنك مع العميل

يقوم موظفي البنك باستخراج بطاقة دفع الإلكتروني تسليمه لكن بيانات مزورة، بحيث يتفق موظف البنك مع العميل وذلك باستخدام بطاقة كل أوراقها ومستنداتها ضرورية، أو يتم استخدامها لعميل ليس له وجود مع علمه بذلك حتي يستنفذ هو وذلك العميل بالمبالغ التي تنطوي تحت رصيد البطاقة، وتكيف هذه الواقعة علي أنها جريمة للاستلاء علي أموال البنك دون وجه حق وتزوير للمستندات[1].

ثانيا: تواطؤ موظف البنك مع التاجر

يتجلى هذا التواطؤ من خلال عدة عمليات، كأن يتفق الموظف مع التاجر فيصرف قيمته إشعارات البيع وهذا بدافع الاستلاء علي الأموال، أو يقوم موظف البنك باعتماد إشعارات بيع تتسبب إلى بطاقة مزورة أو وهمية أو منتهية الصلاحية أو مشحونة وهو يعلم بذلك، فيكون بذلك أمام جريمة التزوير[2].

[1]– لبني عمر سقاوي، المرجع السابق، ص 252.

[2]– عبد الكريم الردايدة، المرجع السابق، ص 61.

ثالثا: تواطؤ موظف البنك مع الغير

اتفاق موظفي مع أفراد العصابات، ومنحهم بيانات بطاقات الدفع الإلكتروني الصحيحة، وذلك لتقليدها أو اصطناعه أو لاستعمالها في عمليات السحب والوفاء لدي التجار، أومن خلال أجهزة الصرف الآلي[1].

ومن خلال ذلك يصبح موظف البنك شريك مع افراد العصابات في جريمة منظمة، وهذا الفعل يعتبر مجموعة جرائم متداخلة من حيث امتداد معلومات عن حسابات العملاء وتزوير بطاقات الدفع الصحيحة والصادرة لحاملها، والاستلاء علي الأموال بدون وجه حق.

الفرع الثاني: الاستخدام غير الشرعي من قبل التاجر

التاجر يعتبر العلاقة تعاقدية لبطاقة الدفع بصفته الجهة التي تقبل البطاقة من حاملها وذلك للدفع بواسطتها مقابل السلع والخدمات المقدمة من خلالها للعمل، بشرط توقيعهم علي إشعارات البيع وشرط وجود تعاقد من أحد المصدرين للبطاقة حتي يتم تزويد التاجر بالأجهزة قد تكون يدوية أو إلكترونية مع مستلزمات التشغيل الخاصة بها، حيث يقوم التاجر فيما بعد بتحصيل ثمن سندات البيع من المصدر المتعاقد معه[2].

من خلال هذا فأن التاجر دور كبير في استكمال عمليات البيع، وتقديم الخدمات والسلع للعملاء باستخدام بطاقات الدفع الإلكتروني فيقوم بفحص للبطاقة والتأكيد من صلاحيتها، والتأكيد من شخصية حاملها وتوقيعه والحصول علي الموافقة لإجراء العملية وذلك بالاعتماد علي الأجهزة المسلمة له، وبذلك فأن مجال عملية الواسع قد يدفعه لارتكاب بعض الافعال الغير الشرعية كتزوير هذه البطاقات أو التلاعب من خلال استخدام الأجهزة المخصص لذلك مواد يدوية كانت أو إلكترونية.

---

[1]– وسام فيصل محمود الشواورة، المرجع السابق، ص 91.

[2]– أمجد حمدان الجهني، المرجع السابق، ص 148.

من خلال هذا الفرع نستعرض التجاوزات التي تتم بواسطة الأجهزة اليدوية **(أولا)**، التجاوزات التي يقدم بها التجار بواسطة الجهاز الإلكتروني **(ثانيا)**.

أولا: التجاوزات التي تتم بواسطة الأجهزة اليدوية

-شراء بعض التجار من بعض الأفراد لسندات بيع مطبوع عليها أرقام بطاقات مزورة حتي ولو كانت بياناتها صحيحة، وبذلك تم تقليدها بواسطة بطاقات فعلية، ثم يقوم هؤلاء التجار بطابعته رقم أجهزته عليها وبذلك لتحصيل ما تم التعامل به من خلالها من أنهم لم يقوموا ببيع أو تأدية أية خدمات لأصحاب تلك البطاقات، هذه الفعل يمثل جريمة احتيال واستلاء علي أموال الغير وبدون وجه حق[1].

-قيام التاجر بطباعة بيانات بطاقة الدفع الخاصة بالعملاء لديهم علي سندات فارغة وبيعها لتجار أخرين للتعامل بها وتحصيل قيمتها بعد اخذ موافقة عليها.

-تزوير البيع، وبالتالي فإن هؤلاء التجار قاموا بشراء هذه بطاقات المسروقة أو المزورة أو المفقودة والتعامل بها بطريقة وهمية لتحصيل قيمتها دون وجه حق[2].

-ادعاء التاجر بتعطيل الآلي الإلكتروني وبعد ذلك يقوم بكتابة ارقام موافقات وهمية علي السندات ليتمكن بعد ذلك من صرف قيمتها[3].

ثانيا: التجاوزات التي يقدم بها التجار بواسطة الجهاز الإلكتروني

-قيام التاجر بوضع جهاز قارئ يتم النسخ بواسطته علي جهاز البيع الإلكتروني حتي يقوم بطباعة هذا البيانات علي بطاقة أخري لاستعمالها في عمليات بيع وهمية دون علم الحامل[4].

---

[1]- وسام فيصل محمود الشواورة، المرجع السابق، ص 88.

[2]- أمجد حمدان الجهني، المرجع السابق، ص 148.

[3]- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والحاسب الآلي في القانون العربي نموذج، المرجع السابق، ص 584.

[4]- وسام فيصل محمود الشواورة، المرجع السابق، ص 89.

-التلاعب بالماكنة الإلكترونية الخاصة بعمليات البيع ونظام تشغيلها، وبذلك يهدف الاحتيال علي البنك باستخدام بطاقات دفع تم التبليغ عن سرقتها أو ضياعها بعد أن تم العبث بنظام التشغيل الخاصة بها[1].

-التلاعب بالماكنة الإلكترونية الخاصة بعمليات البيع ونظام تشغيلها، وبذلك يهدف الاحتيال علي البنك باستخدام بطاقات الدفع تم التبليغ عن سرقتها أو ضياعها بعد أن تم العبث بنظام التشغيل الخاصة بها.

-قيام بعض التجار بالحصول علي أرقام بطاقات الدفع الخاص ببعض العملاء، وذلك لإجراء الاتصالات الدولية من طرف بعض مراكز خدمة رجال الأعمال، وبعد ذلك يقومون بتحميل قيمه المكالمات علي هذه البطاقات حيث تتم هذه المكالمات تقدم من طرف بعض العملاء، ولويتم سدادها للجهة المعنية بذلك، كما قد يقوم التاجر بالاتفاق مع الحامل الشرعي للبطاقة باستخدامها لنفاذ رصيدها الشهري في اجراء عمليات البيع بهدف اقتسام قيمة الفاتورة المحصلة من المصدر[2].

الفرع الثالث: مسؤولية موظفو البنك والتاجر عن الأعمال غير الشرعية

وعلي غرار الحامل الذي يتساءل عن جرائمه ضد بطاقات الدفع الإلكتروني وكذلك فأن موظفو البنك التجار يتساءلون عن أفعالهم غي الشرعية.

نستعرض في هذا الفرع مسؤولية موظفي البنك **(أولا)**، المسؤولية الجزائية للتاجر **(ثانيا)**.

أولا: مسؤولية موظفي البنك

تتم مساءلة موظفي البنك عن مجموعة من الجرائم، كل جريمة حسب الفعل المترتب لها، **(1)** مسؤولية موظفي في حالة اتفاقه مع حامل البطاقة، **(2)** مسؤولية موظف البنك في حال اتفاقه مع التاجر.

[1]- عبد الكريم الرديدة، المرجع السابق، ص 65.

[2]- أمجد حمدان الجهني، المرجع السابق، ص 152.

1-مسؤولية موظفي في حالة اتفاقه مع حامل البطاقة:

أ-جريمة الاشتراك في تزوير واستعمال المزور: يسأل كشريك في التزوير واستعمال المحررات المزورة لمساعدة العميل في استخدام بطاقة الدفع المزورة وذلك عندما يقل المستندات المزورة لاستخراج البطاقة وبالتالي فهو سهل من مهمة الجاني مع علمه المسبق بأن تلك المستندات مزورة[1].

وبالنسبة للعقوبات وحسب نص المادة 221 قانون العقوبات، فأن الشيك فالجريمة تزوير المحررات واستعمال المزور يعاقب بنفس عقوبة الفاعل الأصلي[2].

ب-جريمة الرشوة: هذه جريمة الرشوة تقوم بحق موظف البنك في حال اتفاقه مع العميل في حال إنجازه للأفعال غير شرعية المذكورة سابقا، وذلك مقابل مبلغ مالي يمنحه العميل للموظف لقاء هذه الخدمات[3].

وبالتطبيق علي بطاقة الدفع، فالموظف البنك هو موظف عمومي يعلم أن المزية التي سيتقاضاها غير مستحقة وذلك مقابل أن يقوم أو يمتنع عن عمل ضمن وظائفه.

وجريمة الرشوة كما نص عليها المشرع الجزائري في قانون العقوبات، وأحالها إلى القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، وذلك بموجب المادة 25 والتي نص علي أنه يعاقب بالحبس من سنتين (02) إلى (10) سنوات، وبغرامة من 200.000 إلى 1.000.000 دج.

1-كل من وعد موظفا عموميا بمزية غير مستحقة وأعرضها عليه ومنحه إياها، بشكل مباشر أو غير مباشر، سواء كان ذلك لصالح الموظف نفسه أو لصالح شخص أخر أو كيان اخر لأداء عمل أو الامتناع عن عمل من واجباته.

---

[1]- عبد الكريم الردايدة، المرجع السابق، ص 282.

[2]- أنظر المادة 221 من القانون العقوبات الجزائري.

[3]- عبد الكريم الردايدة، المرجع السابق، ص 289.

2-كل موظف عمومي طلب أو قيل، بشكل مباشر أو غير مباشر، مزية مستحقة، سواء لنفسه أو لصالح شخص أخر أو كيان أخر، لأداء عمل أو الامتناع عن أداء عمل من واجباته[1].

أما فيما يخص أركان جريمة الرشوة فلها صورتان، الأولي وتتمثل في صورة السلبية من خلال ما ذكر في المادة 2/25 حيث أن الركن المفترض وهو صفة الجاني يجب أن تكون موظف عمومي، أما **الركن المادي** فهو القيام بسلوك الطلب أو القبول المزية وهي محل الجريمة وتكون هذه المزية بصور عديدة قد تكون مادية كما قد تكون معنوية صريحة أو ضمنية وذلك مقابل قيامه وامتناعه عن القيام بعمل في وظيفته.

أما **الركن المعنوي** لهذه الجريمة والذي يشمل عنصري العلم والإرادة، حيث يجب أن يكون موظف البنك علي علم بأن هذه السلوك يمثل جريمة رشوة عنه يدخل ضمن واجباته الوظيفية ويعلم أن هذه المزية غير مستحقة عند الطلب والقبول.

إضافة إلى أركان جريمة الرشوة في صورتها السلبية، فأن لها أركانها في صورتها الإيجابية ويتمثل ركنا المادي في قيام شخص ما بوعد الموظف العمومي بمزية غير مستحقة وأن يكون هذه الوعد صادق من أجل إغراء الموظف العمومي وحمله علي القيام بما يطلب منه، بأن يقوم بعمل أو امتناع عن أداء عمل في إطار وظيفته[2].

أما بالنسبة للركن المعنوي فتشترك الصورتين في الركن المعنوي، وأما **الركن الشرعي** لهذه الجريمة فقد نص عليها المشرع الجزائري بموجب المادة 25 من القانون السالف الذكر، المتعلق بالوقاية من الفساد ومكافحته، حيث أن العقوبات الأصلية لهذه الجريمة تشمل الحبس من سنتين إلى 10 سنوات وغرامة مالية من 200.000 إلى 1.000.000دج[3].

---

[1]- عبد الكريم الردايدة، المرجع السابق، ص 230.

[2]- أحسن بوسقيعة، المرجع سابق، ص ص، 94، 95.

[3]- أنظر: المادة 25 من القانون المتعلق بالوقاية من الفساد ومكافحته.

إضافة إلى ذلك فهناك العقوبات التكميلية المنصوص عليها في المادة 09 من القانون العقوبات الجزائري[1].

2-مسؤولية موظف البنك في حال اتفاقه مع التاجر: هذه المسؤولية تكون من خلال عدة أفعال يقوم بها الموظف لمساعدة التاجر علي أفعاله المجرمة مقابل الحصول علي مصلحة معينة من طرف التاجر، من بين هذه الأفعال قبول التعامل بمستندات بيع لبطاقة دفع مزورة أو وهمية أو منتهية الصلاحية، وأيضا في حالة السماح بعملية التعامل في مستندات للبيع وصرف قيمتها متجاوزة السقف المحدد للسحب[2].

وبالرجوع لجريمة الرشوة المذكورة في قانون 01/06 المشارة إليه سابقا، وبالتطبيق علي الفعل الواقع علي بطاقة الدفع، فنجد أن ركنها المادي يتوافر هنا من خلال الفائدة التي يتلقاها موظف البنك من أجل اتفاقه مع التاجر والسماح له بعملية الصرف التي تتجاوز سقف السحب، وتوافر الركن المعنوي يتمثل في نية الموظف في إتمام هذه الفعل من علمه أنه مخالف لنظام العمل الداخلي، وبالتالي فهو فعل مجرم ومعاقب قانونا.

عصابات تمتهن الإجرام، ومن بين عملياتها الإجرامية ما تقوم به ضد بطاقات الدفع الإلكتروني، عن طريق تزويرها وأخذ ما تحتويه من مبالغ مالية، وحتي تتم عملية التزوير تسعي هذه العصابات من أجل الحصول علي بيانات وارقام البطاقات الصحيحة، وحتي تسهل من مهمتها نعتمد علي موظفي البنك لتزويدهم بالبيانات اللازمة مقابل مبالغ مالية[3].

أ-جريمة الرشوة: تقوم هذه الجريمة في حق الموظف عن هذا الفعل بقيام أركانها المادية والمعنوية والشرعي، فإما الركن المادي المتمثل في تقديم الخدمة من طرف

---

[1]- أنظر المادة 9 من القانون العقوبات.

[2]- عبد الكريم الردايدة، المرجع السابق، ص 231.

[3]- المرجع نفسه، ص، 231.

موظف عمومي، هو موظف البنك مقابل مزية غير مستحقة وهي ما يمنحه أفراد العصابات للموظف لقاء البيانات الخاصة ببطاقات الدفع، والركن المعنوي المتمثل في العلم والإرادة حيث أن الموظف يعلم أن هذه الفعل مجرم ومعاقب عليه قانونا، إلا أن إرادته تتجه لإثباته، إضافة إلى الركن الشرعي الذي تم الإشارة له في تعريف الرشوة[1].

ب-جريمة إفشاء الأسرار: تقوم هذه الجريمة في حق موظف البنك، لأنه سمح للغير بالاطلاع علي أسرار منتهية، التي وكلت إليه بمناسبة وظيفته المتمثلة في تزويد أفراد العصابات بيانات البطاقات التي تعود كامليها يقوم بذلك دون علمهم، بهدف تسمي الأفعال الإجرامية[2].

وقد نص المشرع الجزائري علي جريمة إفشاء السر المهني في المرسوم التشريعي رقم 93-10 المتعلق ببورصة القيم المنقولة، بموجب المادة 60 منه والتي نصت أنه "يعاقب بالحبس من 6 اشهر إلى خمس سنوات وبغرامة مالية قدرها 30000 دج، ويمكن رفع مبلغها إلا أكثر من ذلك حتي يصل إلى اربعة أضعاف مبلغ المقدم المحتمل تحقيقه، دون أن تقل هذه الغرامة علي المبلغ المقدم نفسه، أو يعاقب بأحد العقوبتين فقط كل شخص تتوفر له بمناسبة ممارسة مهنته أو وظيفته معلومات امتيازية عن منظوريه مصدر سندات أو منظورية تطور قيمة منقولة ما، فينجر بذلك عملية أو عدة عمليات السوق أو يعتمد السماح بإنجازها إما مباشرة أو عن طريق شخص مسخر لذلك، قبل أن تنتهي تلك المعلومات إلى الجمهور.

وجريمة إفشاء السر المهني علي غرار بقية الجرائم لها أركان الآتي:

الركن المادي: يتمثل هذه الركن في أن يقوم الموظف بإفشاء السر المهني الذي وصل إليه بمناسبة تأدية وظيفته وفعل الإفشاء هو الكشف عن المعلومات وإيصالها للغير

[1]- عبد الكريم الردايدة، المرجع السابق، ص ص 233، 234.

[2]- محمد عبد الودود أبو عمر، المسؤولية الجزائية عن إفشاء السر المهني، الطبعة الأولي، دار وائل للنشر والطباعة، عمان، 1999، ص 110.

بأية طريقة دون مبرر قانوني بحيث يكون ما تم إفشاؤه سرا وفق النظام الداخلي للوظيفة[1].

كما يجب ايضا أن تصدر الجريمة عن شخص ذو صفة معينة، التي يكون قد تحصل عليها من خلال وظيفته التي يمارسها، ومن خلال تلك فهو ملزم بالمحافظة علي السير لمهنة وقيامه بفعل الإفشاء بعد إخلالا بأحكام مهنته.

وتطبيقا لذلك فإن موظف البنك يحصلون علي أسرار عملائهم بمناسبة تأدية مهامه، وهم ملزمون بكتمانها حفاظا علي المصلحة العامة والسير الحسن للبنك، وايضا علي الثقة المتبادلة بين البنك والعميل وما قد يسببه هذه الفعل من أضرار للطرفين[2].

الركن المعنوي: هي جريمة عمدية التي تتطلب القصد العام، والذي يتمثل في العلم والإرادة حيث يجب ان يكون الفاعل عالما بأن محل فطته سر مهني وانه حصل عليه يحكم وظيفته، ولذلك فإن إفشاء هذه السر يعد مخالفة للأحكام والقواعد لأن العميل صاحب السر غير راضي عن، إفشاء ومع ذلك تتجه إرادة الموظف إلى فعل الإفشاء والذي يؤدي إلى علم الغير بهذه السر.

النص القانوني المجرم لفعل إفشاء السر المهني: بالرجوع لنص المادة 60 من المرسوم التشريعي 09-10 المتعلق ببورصة القيم المنقولة فأن العقوبات تشمل الحبس من 06 اشهر إلى 05 سنوات وبغرامة مالية قررها 30000 دج ويمكن رفعها إلى 4 أضعاف المبلغ المحتمل تحصيله دون أن تقل عن المبلغ المقدم نفسه، أو إحدى العقوبتين فقط[3].

---

[1]- محمد عبد الودود أبو عمر، المرجع السابق، ص ص 111، 141.

[2]- المرجع نفسة، ص 115، 116.

[3]- أنظر: المادة 60 من المرسوم التشريعي المتعلق ببورصة القيم المنقولة.

ثانيا: المسؤولية الجزائية للتاجر

يعتبر شريكا في جريمة التزوير أو السرقة وتقوم مسؤولية الجزائية لعلمه بأن البطاقة مسروقة أو مزورة، ومع ذلك قبل التعامل بها يسأل عن جريمة خيانة الأمانة عند علمة بأن البطاقة ملغاة أو منتهية الصلاحية ومع ذلك قبل التعامل بها.

ومن خلال هذا نتطرق، مسؤولية التاجر عند استخدامه غير الشرعي **(1)** للماكنات اليدوية، مسؤولية التاجر عند استخدامه غي الشرعي للماكنات الإلكترونية. **(2)**

1-مسؤولية التاجر عند استخدامه غير الشرعي للماكنات اليدوية: يسأل عند شرائه خواتيم وإشعارات عليها أرقام مزورة، وهو يعلم بذلك يقوم بطباعة رقم ماكنة عليها بغرض الحصول علي قيمتها دون تقديمة للخدمة، ويسأل عن جريمة النصب لأن الأموال المحصل عليها ليس من حقه، وكذلك يسأل عن جريمة إخفاء الأشياء المسروقة عند قبوله لبطاقة مسروقة رغم علمه بذلك ويعتبر شريك في جريمة السرقة عندما يوقع علي فاتورة غي صحيحة، ويسأل عن جريمة النصب عند قيامه بتبعته أرقام بطاقات عملائه علي فواتير فارغة دون علمهم، ويقوم بتغير مبالغتهم المتحصل عليها مقابل البضائع[1].

2-مسؤولية التاجر عند استخدامه غير الشرعي للماكنات الإلكترونية: يسأل عن جريمة إتلاف بتعين الشيء ما يفقده قيمته الجزائية، وجريمة الإتلاف نص عليه المشرع الجزائري في المادة 394 من قانون العقوبات، وتطبيق علي التاجر لأن عطل الماكنة الإلكترونية وهذا ما يمثل الركن المادي وقصد جنائي يتمثل في الحصول علي أموال من البنك بدون حق[2].

[1]- أمين طالب البغدادي، المرجع السابق، ص216.

[2]- عبد الكريم الردايدة، المرجع السابق، ص 224.

يسأل التاجر عن الجريمة النصب والاحتيال لأن التصرف الذي قام به هو إتلاف وتعطيل الماكنة الإلكترونية هدف منه تظلل البنك وإيهامه بوجود سند دين[1]، يسأل كذلك عن جريمة التزوير عند قيامه بفعل السابق بهدف إيهام البنك بعمليات بيع لاوجود لها تمت بواسطة البطاقات المسروقة مع تزوير توقيع الحاصل الأصلي للبطاقة، أنه أشرف علي هذه المعاملة وتنطبق عليه عملية التزوير لأنه قام بتحرين الحقيقة وهما ما يمثل الركن المادي للجريمة، وهذا يضر بمصالح البنك، نظر الاستلاء علي أموال بغير حق الركن المعنوي[2].

المطلب الثاني

الاستخدام غير الشرعي للبطاقة من قبل الغير

الغير هو كل شخص دون الأطراف المتعاقدة للتعامل بالبطاقة، ولا يخضع للالتزامات العلاقة التعاقدية، رغم ذلك يصادف أن تقع البطاقة في يده فيستغلها بأعمال غير شرعية.

سنتحدث في هذا المطلب، جريمة التزوير واستعمال المزور **(الفرع الأول)** ، جريمة سرقة بطاقة دفع أو رقمها السري **(الفرع الثاني)** ، جريمة استعمال بطاقة دفع مفقودة. **(الفرع الثالث)**

الفرع الأول: جريمة التزوير واستعمال المزور

تقع جريمة التزوير أو جريمة استعمال المزور علي بطاقات الدفع الإلكتروني من قبل الغير في حال ضياعها أو سرقتها، حيث يقوم هذه الأخير بتحريف حقيقتها وذلك باستبدال البيانات التي تحملها باخرة مزورة، هذه يتمثل جريمة ضد حاملها والجهة المصدرة.

[1]– أمين طالب البغدادي، المرجع السابق، ص 216.

[2]– عبد الكريم الردايدة، المرجع السابق، ص 224.

في هذا الفرع سنتحدث عن جريمة تزوير بطاقة الدفع الإلكتروني **(أولا)**، جريمة استعمال بطاقة الدفع مزورة من طرف الغير **(ثانيا)**.

أولا: جريمة تزوير بطاقة الدفع الإلكتروني

لمعرفة جريمة تزوير بطاقة الدفع الإلكتروني نتناول **(1)**: تعريف التزوير، **(2)**: أركان جريمة التزوير، **(3)**: أساليب تزوير بطاقات الدفع الإلكتروني.

1-تعريف التزوير: ويعرف بأنه تغير الحقيقة في المقررات الرسمية والسندات، ويقصد بها الغش بالأساليب المحددة قانونا والتي تلحق ضررا بالضحية[1].

2-أركان جريمة التزوير: نص المشرع علي جريمة العقوبات في المواد من: 214 إلى 299، هو كأن جريمة تلزم لقيامها أركان، المحددة كالآتي[2]:

أ-**الركن المادي**: يتجلى في جريمة تزوير المحررات من خلال تغير الحقيقة بأحدي الطرق التي نص عليها القانون والتي تسبب ضررا، ومنه كانت عناصر هذه الركن كالآتي:

محل التزوير: بالرجوع إلى المواد من 214 إلى 229 قانون العقوبات فأنه يجب ان يقع التزوير علي المحررات التي تشكل سندات بما في ذلك المحررات العمومية والرسمية والعرفية، وكذلك المحررات التجارية تنطوي ضمن المحررات المصرفية، وبذلك تكون محلا للتزوير[3].

-**تغير الحقيقة**: حتي تقوم جريمة التزوير لبد أن يحدث تغير لحقيقة المحرر واستبدال بياناته باخري غير حقيقة، وقد يكون هذا التغير كلي أو جزئي.

---

[1]- حسين محمد الشيلي، محمد فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولي، دار مجلاوي للنشر والتوزيع، عمان، 2009، ص57.

[2]- أنظر المادة قانونية المواد 214 إلى 299.

[3]- أحسن بوسقيعة، المرجع السابق، ص 540.

-**طرق تزوير:** يكون الأسلوب المتبع في عملية التزوير أسلوب نص عليه القانون، وحددها المشرع الجزائري في قانون العقوبات علي سبيل الحصر في المادة 216 من هذه القانون حيث يكون بتقليل أو بتزييف الكتابة أو التوقيع، وإما باصطناع اتفاقات أو نصوص والتزامات.

-**الضرر:** حتي تقوم جريمة التزوير يجب أن يترتب عليه ضرر، وهذ الضرر لا يشترط فيه أن يمسي الشخص الذي يقصده المزور، بل يكفي ان يقع علي اي شخص كان، قد يكون هذه ضرر ماديا أو معنوي، وبالإسقاط ذلك بطاقات الدفع الإلكتروني فان عنصر الضرر محتمل الوقوع علي الجهة المصدرة للبطاقة وحاملها الشرعي[1].

ب-الركن المعنوي: هي من الجرائم العمدية التي تستوجب القصد الجنائي العام والخاص

-**القصد الجنائي العام:** يقصد به العلم والإرادة وذلك أن تتجه إرادة الجاني إلى تغير الحقيقة مع علمه أن هذه التغير فعل مجرم قانونا يترتب عليه ضرر محتمل.

-**القصد الجنائي الخاص:** اتجاه نية الجاني لاستعمال المحرر فيما زور من أجله أو دفع مضرة عن الغير أو عن نفسه[2].

ج-النص القانوني المجرم لفعل التزوير: نص المشرع الجزائري علي عقوبة جريمة التزوير في المحررات التجارية أو المصرفية أو الشروع بموجب نص المادة 219 قانون العقوبات الجزائري، " فإن العقوبة الأصلية فهي الحبس من سنة إلى خمس سنوات، وبغرامة مالية من 500 إلى 20000 دينار ويمكن أن يضاعف الحد الأقصى، إذا تعلق الأمر بمديري الشركات أو أحد رجال المصارف أو أي من الأشخاص يلجؤون للجمهور قصد إصدار أسهم أو حصص سواء لشركة أو مشروع تجاري أو صناعي.

---

[1]- خشة حسيبة، المرجع السابق، ص 125.

[2]- أحسن بوسقيعة، المرجع السابق، ص ص 541، 542.

أما العقوبة تكميله فهي الحرمان من الحق أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة من سنة إلى 5 سنوات على الأكثر"[1].

3-أساليب تزوير بطاقات الدفع الإلكتروني: صنف الخبراء الكشف عن التزوير أساليب إلى أسلوبين:

أ-الأسلوب التزوير الكلي: يتم أولا باصطناع بطاقة كاملة، ثم تقليد الرسوم الخاصة علي الحسم البطاقة وتغليفها وتلصيق شريط الممغنط وشريط التوقيع كل حسب مكانه، ثم القيام بالطباعة النافرة وتشغيلها بواسطة اشباعها بالمعلومات التي تحصل عليها المزورون من البطاقة الصحيحة، وبعد ذلك يتم استخدامها في عمليات الشراء، وفي حالة ما إذا تحصيل المزور على الرقم السري للبطاقة ما فإنه يقوم باستغلالها باصطناع بطاقة بلاستيكية فارغة من البيانات ويلصق عليها الشريط الممغنطة ونسخ بيانات صاحب هذه البطاقة، ويقوم باستخدام نسخ عديدة منها لاستخدامها في الحصول علي الأموال من أجهزة الصراف الآلي.

وكذلك يتم التزوير الكلي عن طريق سرقة بطاقات كاملة التجهيز من الشركات المنتهية لها، عن طريف شركات بداخل الشركات أو المصارف ثم بيعها أو تزويرها كما سبق ذكره كما قد يتم اخذ البيانات من قوائم حجوزات الفنادق، ووكالات السفر، وفي الفواتير التي رميها[2].

ب-أسلوب التزوير الجزئي: هذه الحالة يتم استغلال جسم البطاقة الحقيقي، وما تحمله من رسوم خاصة وحروب بارزة والكتابات أمنية بغرض، تزويرها بواسطة مهرها عليها من أرقام بارزة لبطاقة صحيحة انتهت صلاحيتها، أو إعادة قولية رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب أخر يتم الحصول عليه بالطريقة السابقة الذكر، كذلك

[1]- أنظر المادة 219، من قانون العقوبات.

[2]- وسام فيصل محمود الشواورة، المرجع السابق، ص، 94.

يتم محوها على الشريط الممغنطة من بيانات وإعادة برمجته بمعلومات صحيحة تمت سرقتها، أو كشف التوقيع ووضع شريط توقيع أخر[1].

ج-أدوات التزوير:

جهاز المسح: والذي يستعمل لاستنساخ معلومات الحساب من الشريط الممغنط علي البطاقة الصحيحة وهو جهاز الصغير يمكن حمله في راحة اليد، ويستطيع تخزين ما يقارب مئة رقم حساب، حيث يتم نسخها من بطاقات أصلية، عندما يحصل الجاني علي مبتغاه من الشريط الممغنط، يقوم بتخزينها في الحساب الآلي الخاص به[2].

منظم سايون: جهاز يدوي يستقبل المعلومات ويخزنها من الجهاز الممغنط الموصول براسه ليتمكن من قراءة بيانات الشريط المغناطيسي في البطاقة البلاستيكية، وعند تمرير البطاقة في الفتحة يقوم منظم سايون بتخزين المعلومات علي حساب الآلي.

المشفر: جهاز يستخدم لتشفير البيانات التي تكون علي الشريط الممغنط علي البطاقة ضرورية أو المسروقة أو المفقودة والذي تمت مصادرتها لاعتقال المجرمين في عمليات احتيال علي البطاقات الدفع الإلكتروني، كما يمكن شراؤه من المتاجر الإلكترونية، ويحتوي علي رأس للكتابة علي شريط الممغنط عند تمرير البطاقة من خلال الفتحة، ويستخدم بالاشتراك مع الحاسب الآلي وبرامج مناسبة.

جهاز الطبع بحروف نافرة: جهاز يستخدم لطباعة رقم الحساب وأيضا المعلومات بحروف نافرة علي الوجه الأمامي للبطاقة، وهو يستخدم أيضا للأغراض شرعية ومن السهل الحصول عليه[3].

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص 157.

[2]- وسام فيصل محمود الشواورة، المرجع السابق، ص 94.

[3]- المرجع نفسه، ص 166.

جهاز طلاء الحروف: جهاز يستخدم لطلاء الأرقام المطبوعة بحروف نافرة علي البطاقة المزورة، حيث يتم طلاؤها بالون الفضي أو الذهبي أو الأسود، وهذا الجهاز يحتوي علي جميع الأرقام التي تم طلاؤها.

ثانيا: جريمة استعمال بطاقة الدفع مزورة من طرف الغير

تصبح جريمة استعمال بطاقة دفع ضرورية ضمن جريمة استعمال المحررات المزورة، وتعتبر جريمة قائمة بذاتها ونص عليه المشرع الجزائري بموجب المادة 221 قانون العقوبات، تطرقنا، إلى أركان الجريمة. **(1)**

1-أركان الجريمة: تتمثل أركان الجريمة في الركن المادي وفي الركن المعنوي وكذا في النص القانوني المجرم لاستعمال المحرر المزور.

أ-الركن المادي: الركن المادي لجريمة استعمال المحررات المزورة يتمثل في استعمال ورقة مزورة، حيث أن المشرع الجزائري لم يبين ما المقصود باستعمال ورقة المزورة، وتعرف علي أنها التمسك والاحتجاج بمحرر مقدم لفرد أو جهة من الجهات سواء شخص المحتج أو من الغير[1].

ب-الركن المعنوي: يتمثل الركن المعنوي لجريمة استعمال المحرر المزور في أن يكون الجاني عالما عند استعمالها للمحرر بأنه مزور والفاعل لا يعلم بذلك، اكتشف لاحق بأنه مزور ولكنه استمر بالتمسك به فهنا تقوم الجريمة من يوم علمه بالأمر، ويخضع لأحكامها ويدون هذه العلم في حكم الإدانة وإلا كان معيبا بالقصور[2].

ج-النص القانوني المجرم لاستعمال المحرر المزور: العقوبة المقررة لجريمة استعمال المحرر المزور هي نفسها عقوبة جريمة التزوير المشار إليها سابقا، سواء العقوبات الأصلية منها أو تكميلية.

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص 158.

[2]- أحمد أبو الروس، قانون جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية الموسوعة الجنائية الحديثة، المجلد الخامس، المكتب الجامعي الحديث، الاسكندرية، 1997، ص 89.

الفرع الثاني: جريمة سرقة بطاقة دفع أو رقمها السري

تعتبر جريمة سرقة بطاقة دفع أو رقمها السري أحد الجرائم التي يتعرض لها صاحب بطاقة الدفع، سنقوم من خلال هذا الفرع بالتعرف على جريمة سرقة البطاقة **(أولا)**، ثم نتطرق إلى جريمة سرقة الرقم السري لبطاقة الدفع الإلكتروني **(ثانيا)**.

أولا: جريمة سرقة البطاقة

نص المشرع الجزائري علي جريمة السرقة بموجب المادة 350 قانون العقوبات الجزائري حيث جاء فيها كل من اختلس شيء غير مملوك له بعد سارق[1].

سوف نتطرق من خلال هذا الفرع الركن المادي **(1)** ، الركن المعنوي **(2)**.

1-الركن المادي: يتمثل الركن المادي لجريمة السرقة في فعل الإخلاس الذي يعرف علي انه أخذ مال الغير بدون رضا مالكه أو حائزه، ومن هذه التعريف يتبين أن الفعل الاختلاس يتكون من عناصر أساسية، فالعنصر المادي يتمثل في الاستلاء علي الشيء المملوك للغير، وأما العنصر المعنوي فهو عدم رضا صاحب هذه الشيء علي هذه الفعل المجرم، كذلك فيما يتعلق بمحل الجريمة فأن فعل السرقة يقع علي الشيء مملوك للغير وتقع علي المنقولات دون العقارات.

2-الركن المعنوي: تقوم جريمة السرقة علي القصد الجنائي العام والخاص، القصد الجنائي العام فهو العلم ولإرادة، إي أن الجاني يعلم أن الشي ملك الغير، ولاستيلاء عليه فعل مجرم قانونا، ومع ذلك تتجه إرادته لأثباته، وفيها يخص بطاقة الدفع فالجاني يعلم أنها مالك لصاحبها ولا يجوز التصرف فيها، وهذه الفعل يعد سرقة ومع ذلك تتجه إرادته لسرقتها[2].

[1]- أنظر المادة 350 من القانون 14-01 المتضمن القانون العقوبات.

[2]- عبد الفتاح بيومي الحجازي، جرائم الكمبيوتر والحاسب الآلي في القانون العربي النموذجي، المرجع السابق، ص 587.

أم القصد الجنائي الخاص يقصد به نية التملك، ولكن مع تطور القضاء أصبح لا يؤخذ به كشرط لقيامه جريمة السرقة، وإنما تقوم بمجرد الاستلاء علي الشيء واستخدامه، وبالتطبيق علي بطاقة الدفع الإلكتروني فأن جريمة السرقة تقوم بمجرد استلاء الغير عليها، مع علم هذا الأخير بأن هذا الفعل يعد جريمة يعاقب عليها القانون، حتي ولولم تكن نية تملكها، والدفع يعد باطلا[1].

ثانيا: جريمة سرقة الرقم السري لبطاقة الدفع الإلكتروني

تعد جريمة سرقة الرقم السري لبطاقة الدفع الإلكتروني، وسنتناول فيه المقصود بسرقة الرقم السري للبطاقة **(1)** ، ثم إلى سرقة أرقام بطاقات الدفع عبر الأنترنت **(2)**.

1-المقصود بسرقة الرقم السري للبطاقة: يسأل الغير عن جريمة السرقة عندما يقدم بسرقة الرقم السري لبطاقة الدفع الإلكتروني، بحيث يستطيع الفاعل الحصول عليه واستخدامه في مختلف العمليات المصرفية[2].

أ-إهمال الحامل: تحصيل نتيجة تدوين الرقم السري علي وجه البطاقة من قبل حاملها الشرعي، وتركها عرضة لمرأي الغير الذي يتمكن من معرفة بكل سهولة، كذلك قد يقوم حاملها بتكرار الرقم السري على مسمع أو أنظار الغير أثناء قيامه بعملية سحب النقود دون أخذ الحيطة اللازمة[3].

ب-التجسس: يتم هذه الطريقة إما بمراقبة أجهزة الصراف الآلي بوضع كمرات عليه، ومن ثم رؤية الأرقام السرية عند إدخالها، أومن خلال وضع جهاز إلكتروني في مكان ما علي الصراف الآلي، حيث يقوم بنقل الرقم السري لجهاز أخر لحظة إدخاله من قبل حاملها.

---

[1]- فيصل محمود الشواورة، المرجع السابق، ص ص 96.

[2]- المرجع نفسه، ص 100.

[3]- عبد الكريم الردايدة، المرجع السابق، ص 70.

ج-القرصنة: يتم ذلك بالدخول إلى موقع الكمبيوتر التي فيها حفظ بيانات العملاء وأرقام بطاقتهم وذلك بصورة غير قانونية عبر البنوك المصدرة لها.

2-سرقة أرقام بطاقات الدفع عبر الأنترنت: تتم هذه العملية من ذوي الخبرة والمحترفين في مجال شبكات الأنترنت، وهي من ضمن أعمال القرصنة للحصول علي أرقام بطاقات الدفع يتم ذلك بعدة أساليب وتقنيات نذكر من بينها.

أ-اختراق منظومة الاتصالات العالمية: تلك الخطوط التي تربط بين الحاسب الآلي للمشتري والحاسب الآلي للتاجر، وتتم عملية القرصة بالتنصت علي الاتصالات بهدف اختراعها والتغلب على نظام حمايتها، تم الوصول إلى بطاقات الدفع الإلكتروني[1].

ب-أسلوب الخداع: يتجلى هذه الاسلوب في إنشاء مواقع إلكترونية وهمية، شبيعة بالمواقع الأصلية علي شبكة الأنترنت مثال ذلك مواقع المؤسسات التجارية، حيث تظهر هذه المواقع للغير علي أنها فعلية، وتتم هذه العملية من خلال قيام القراصنة من الجناة بجميع معلومات كافية متعلقة بمواقع أصلي علي الشبكات الأنترنت وبعدها يتم إنشاء موقع وهمي بواسطة تلك البيانات المحصل عليها من الموقع الأصلي حيث يبدو وكأنه نفسه الموقع ليتم استخدامها بعد ذلك من قبل القراصنة في استقبال جميع المعاملات الخاصة بالموقع الأصلي في مجال التجارة الإلكترونية، ومن بينها المعاملات التي تتم بواسطة بطاقات الدفع الإلكتروني لتنتهي هذه العملية بالاستلاء علي البيانات وأرقام هذه البطاقات[2].

ج-أسلوب الإبهام: يتمثل في قيام القراصنة بانتحال صفة الجهة المصدرة للبطاقة الدفع، ومن ثم إرسال رسالة إلكترونية لعملائهم أصحاب البطاقة، والهدف منها تجديد

[1]- أمجد حمدان الجهني، المرجع السابق، ص 190.

[2]- عبد الكريم الردايدة، المرجع السابق، ص 71.

معلوماتهم وبيانات بطاقاتهم عبر الموقع الإلكتروني، ليتسنى لهم التعرف على أرقامها وبياناتها[1].

د-أسلوب تخليق رقم بطاقات الدفع: يتم هذه الأسلوب في إيجاد الرقم السري للبطاقة عن طريق القيام بعمليات حسابية ومعادلات، وذلك بتبديل وتوثيق الأرقام حسابية، ومن ثم التعرف على هذا الرقم واستخدامه في العمليات الإجرامية للجناة.

ذ-أسلوب تبادل المعلومات: يقوم هذه الأسلوب علي التعاون القائم بين القراصنة المجرمين عبر مختلف الدول، من خلال تبادل الأرقام المتحصل عليها فيما بينهم، وذلك لتوسيع نشاطهم الاجرامي باستخدام تلك الأرقام عبر مختلف الدول[2].

الفرع الثالث: جريمة استعمال بطاقة دفع مفقودة

مفادها هذه الجريمة أن الغير لم يسرق بطاقة الدفع من صاحبها بل عثر عليها، فقد تكون هذه البطاقة مسروقة أو مفقودة ولم يقم بإرجاعها لصاحبها الشرعي أو الجهة المصدرة لها.

تطرقنا في هذا الفرع إلى استخدام البطاقة المفقودة **(أولا)**، استخدام البطاقة المسروقة **(ثانيا)**.

أولا: استخدام البطاقة المفقودة

قد يحصل أن يتم العثور علي بطاقة دفع ضائعة، وهنا يمكن التميز بين حالتين: استعمال البطاقة من طرف الشخص الذي عثر عليها **(1)** ، عدم استعمال البطاقة من طرف الشخص الذي عثر عليها ومنحها لشخص أخر **(2)**.

[1]- عبد الكريم الردايدة، المرجع السابق، ص 100.

[2]- جعفر حسين جاسم الطائي، جرائم التكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البداية للنشر والتوزيع، عمان، 2010، ص 192.

1-إستعمال البطاقة من طرف الشخص الذي عثر عليها: يقد هذه الأخير عدم إرجاع البطاقة واستخدامها لمصلحة الشخص هنا يسال عن جريمة احتيال لأنه استعمل صفات كاذبة عندما أدعى أنه المالك للبطاقة.

2-عدم استعمال البطاقة من طرف الشخص الذي عثر عليها ومنحها لشخص أخر: قد يقرر من عثر علي البطاقة عدم الاحتفاظ بها، وكذلك عدم استعمالها ليسلمها لشخص أخر هذه الأخير الذي قد يكون مالك أوقد يكون غير ذلك كما يلي :

تسلم البطاقة لشخص يدعي أنه مالكها: يعتمد الشخص الذي عثر علي البطاقة أنه قد سلمها لمالكها الحقيقي، لكن في الحقيقة هو ادعاء كاذب من قبل الشخص المسلمة إليه بغرض الاستلاء عليه، وفي هذه الحالة لا يخضع مسلم البطاقة لأي مسائلة جزائية لأنه فعل ذلك بحسن نية[1].

ثانيا: استخدام البطاقة المسروقة

يقصد بها الاستخدام أن يقوم الشخص الذي سرق بطاقة دفع بتسليمها للغير قصد استعمالها، استلام البطاقة المسروقة مع علمه برقمها السري **(1)** ، استلام البطاقة المسروقة دون معرفة رقمها السري **(2)**.

1-إستلام البطاقة المسروقة مع علمه برقمها السري: إذ قام من استخدام بطاقة الدفع مع علمه برقمها السري، سواء في عمليات السحب أو الوفاء فأنه يسأل عن عدة جرائم، فيسأل عن جريمة إخفاء الأشياء المسروقة لأنه يعلم أن البطاقة مسروقة ومع ذلك احتفظ بها[2].

كذلك يسأل عن جريمة احتيال عند تعامله مع التاجر في الوفاء أوفي السحب النقود لأنه استعمل صفات كاذبة، والتي علي أساسها تحصل علي النقود والخدمات،

[1]- عبد الكريم الردايدة، المرجع السابق، 244.

[2]- علي عدنان الفيل، المرجع السابق، ص ص 59، 60.

كما أنه يسأل أيضا عن جريمة التزوير عندما يستعمل البطاقة في الوفاء نتيجة توقيعه باسم صاحب البطاقة حتي يدفع البنك ثم مستحقاته[1].

2-استلام البطاقة المسروقة دون معرفة رقمها السري: الفاعل يسأل عن الجريمة إخفاء أشياء مسروقة، أما بالنسبة لاستخدام وإما أنه يعرف رقمها السري فأنه لا يستطيع استخدامها في عمليات السحب والدفع، وفي حالة ما إذا حاول ذلك فأنه يسأل عن الشروع في جريمة احتيال وأن تحقق النتيجة بسبب خارجي وهو عدم معرفته للرقم السري وكذلك فأن أجهزة الصراف الآلي مبرمجة على سحب البطاقة عند الإدخال المتكرر لثلاث مرات لرقم سري خاطئ أما بالنسبة المسؤولية سارق البطاقة الذي قدمها للغير فانه إذا سلم البطاقة للغير على اعتبار أنه حاملها الشرعي، فهنا لا يسأل على أنه جريمة لأنه يعتبر إعارة للبطاقة وأما إذا سلمه إياها مع علمه بأنه ليس لمالكها فهنا يسأل عن جريمة السرقة، كما يسأل أيضا بصفته شريك في الجريمة احتيال أو تزوير التي قام بها من سلمها[2].

[1]- علي عدنان الفيل، المرجع السابق، ص 60.

[2]- أمجد حمدان الجهني، المرجع السابق، ص 181.

الفصل الثاني:

الإجراءات المتخذة في مواجهة الاعتداءات الواقعة على بطاقات الدفع الإلكتروني

الفصل الثاني

الإجراءات المتخذة في مواجهة الاعتداءات الواقعة على بطاقات الدفع الإلكتروني

تشكل الاعتداءات على بطاقات الدفع الإلكتروني خطورة بالغة لما تسببه من خسائر في مجال التعاملات المالية، خاصة وأن هذه الجرائم ذات طبيعة تقنية لكونها ترتبط بأجهزة إلكترونية ولذلك نجد ان مرتكبي هذه الجرائم يتصفون بالفطنة والذكاء في المجال، وعليه وجب تبني استراتيجية لمكافحة هذه النوع من الجرائم للحد منها وردع مرتكبيها.

ولأن جرائم بطاقات الدفع الإلكترونية تمتاز بالحداثة، فهي تفتقد إلى قوانين خاصة بها تكون كفيلة بالحد من وقوعها، وذلك ما دفع إلى اتخاذ إجراءات خاصة بذلك سواء علي المستوي المحلي من خلال تبني أطراف العلاقة التعاقدية ولأن جرائم بطاقات الدفع الإلكترونية تمتاز بالحداثة، فهي تفتقد إلى قوانين خاصة بها تكون كفيلة بالحد من وقوعها، وذلك ما دفع إلى اتخاذ إجراءات خاصة بذلك سواء علي المستوي المحلي من خلال تبني أطراف العلاقة التعاقدية إجراءات لحماية حقوقهم وداوم الثقة في تعاملاتهم، وكذلك على مستوى الأجهزة الأمنية المختصة في مكافحة هذه الجرائم، ومن جهة آخرة وعلى الصعيد الدولي أيضا يجب تفعيل آليات كفيلة بمحاربة هذه الجرائم ومتابعة مرتكبيها.

ومن خلال هذه الفصل سنستعرض مختلف الإجراءات المتبعة في مجال الجرائم الواقعة على بطاقات الدفع الإلكتروني، حيث نخصص منه لدارسة الإجراءات الوقائية، في حين سنخصص **(المبحث الأول)** ، الإجراءات الردعية **(المبحث الثاني)**.

المبحث الأول

الإجراءات الوقائية

أحد المحافظة على سلامة وأمن المعاملات المصرفية ببطاقات الدفع الإلكتروني، كان من دارم وضع إجراءات وقائية من قبل جهات مختلفة في المجتمع سواء الجهات المصدرة للبطاقة أو المتهمة بها إضافة إلى الأجهزة الأمنية المختصة، وذلك لمنع أي جرائم قد تقع على البطاقة من خلال الإحاطة بسيداتها ودوافعها التي تؤدي لارتكابها، ومحاولة معالجتها حتى لا تتكرر مجددا.

ولتسليط الضوء على ذلك فقد قمنا هذا المبحث إلى مطلبين، نتناول في الإجراءات الوقائية على صعيد الهيئات الدولية وكذلك البنوك **(المطلب الأول)** ، بينما خصصنا للإجراءات الوقائية على مستوى صاحب البطاقة والتاجر والجهاز الأمني. **(المطلب الثاني)**

المطلب الأول

دور الهيئات الدولية والبنوك في حماية بطاقة الدفع الإلكتروني

نظرا للتزايد الكبير للاعتداءات التي تستهدف بطاقات الدفع الإلكتروني، هذا ما دفع المعنيين في هذا المجال إلى التدخل والتصدي لهذه الظاهرة والحد منها من خلال إجراءات وقائية متخذة من طرف الهيئات والشركات العالمية وهو ما خصصنا له **(الفرع الأول)**، في حين خصصنا، للإجراءات المتخذة من قبل البنوك والمؤسسات المصرفية. **(الفرع الثاني)**

الفرع الأول: الإجراءات الوقائية المتخذة من قبل الهيئات الدولية

تتمتع الهيئات الدولية المنشئة لبطاقات الدفع الإلكتروني ومثال ذلك بطاقات فيزا كارد وماستر كارد، بالدور الكبير في حماية هذه البطاقات لكونها هي من يصنع هذه البطاقات ويضفي عليها صفة القبول دوليا، مما يسمح بتداولها والتعامل بها حتى عن طريق الأنترنت وفي حال وقوع أي تجاوزات أو مشاكل فهذه الهيئات هي من يتدخل

لحلها[1]، ولذلك فقد اتخذت العديد من الإجراءات بغية الاستعمال الأمثل لهذه البطاقة ومن أهمها الإجراءات التقنية لتطوير البطاقة (**أولا**) ، تصميم البرامج(**ثانيا**).

أولا: الإجراءات التقنية لتطوير البطاقة: لقد تم إنشاء بطاقة مكونة من دوائر إلكترونية تجعلها غير قابلة للاختراق وهذا بفضل المادة المصنوعة بها (pvc)، وكذلك عن طريق إدخال الهول جرام وهو عبارة عن أشعة الليز والتي من خلالها تنعكس الصورة المراد تصويرها على مكان معين، كما تحتوي أيضا هذه البطاقة على ذاكرة لها القدرة على حفظ العمليات الأخيرة التي تم إجراؤها، كذلك دمج البطاقة الذكية وهي بطاقة بلاستيكية حجمها كحجم بطاقات الدفع الأخرى، حيث تتميز هذه البطاقة بدوائر متكاملة تسمح لها بتخزين ومعالجة البيانات[2].

كذلك فقد تم استخدام الانترنت النموذجي التقني الموحد والمسمى بنظام الصفقات الإلكترونية الآمنة، والذي أعلنت عنه الشركتين العالميتين ماستر كارد وفيزا كارد سنة 1996، وانظم إليه لاحقا مجموعة من الشركات الأمريكية، ومن جهة أخرى فقد قامت شركة ماستر كارد العالمية بطرح بطاقة ماستر كارد باي اباس" وذلك عام 2002، وهي عبارة عن برنامج الدفع دون اتصال حيث يتم بواسطة تقنية متطورة، حيث يقوم الحامل بتمريرها قرب جهاز الكتروني مهيا لهذا الغرض وبعد ارسل هذه البطاقة معلومات الدفع لاسلكيا وبعد معالجة العملية يستلم الحامل إشارة بتأكيد الدفع[3].

إضافة إلى ذلك فقد قامت الشركات العربية بإصدار بطاقات مماثلة، حيث أعلنت شركة "دوت كوم عن إصدار البطاقة الإلكترونية المسمات" ماستر كارد، والتي توفر لحاملها خدمات البيع والشراء عبر الانترنت بثقة تامة وبصورة آمنة دون أي مخاطر[4].

---

[1]– عبد الكريم الردايدة، المرجع السابق، ص 179.

[2]– علي عدنان الفيل، المرجع السابق، ص ص، 76، 77.

[3]– المرجع نفسه، ص 77.

[4]– أمجد حمدان الجهني، المرجع السابق، ص115.

كانت إذا هذه نبذة عن بعض الإجراءات التقنية المتخذة من قبل بعض الشركات العالمية والعربية الناشطة في مجال البطاقات الإلكترونية بهدف تطويرها وجعلها آمنة للاستخدام.

ثانيا: تصميم البرامج: اقامت الهيئات المصدرة للبطاقة الإلكترونية بإنشاء برامج للحد من وقوع الاعتداءات على البطاقة ومن بينها على سبيل المثال ما يلي:

- **برنامج الشبكة العصبية:** ومن خلاله يتم رصد جميع التعاملات المنفذة بواسطة بطاقات الدفع، والكشف عن المشكوك في صحتها وإعادة فحصها.

- **برامج نظم المعرفة:** يعمل هذا البرنامج على عزل وإيقاف البطاقات التي يكتشف أن تعاملاتها غير شرعية، وذلك من خلال وسائلها الفعالة للكشف عن التهديدات من طرف المجرمين.

- **برامج نظم المعلومات الإرشادية:** والتي تعمل على مراقبة أساليب الغش والاحتيال التي قامت المؤسسية البنكية في بريطانيا بتطويرها[1].

- **برنامج الاختيار:** يعمل على تطبيق المعايير الأولية على حساب حاملي بطاقات الدفع، حيث تظهر من خلاله الحسابات التي تستخدم هذه البطاقات بصفة غير شرعية ومن ثم عدم إتمام التعامل بالبطاقة.

- **برنامج التقييم:** يعمل على فحص حسابات حاملي بطاقات دفع العملاء بالاعتماد على تعليمات خبراء مكافحة الاحتيال المزودة بها ثم عزل الحسابات التي يثبت أنها تتبع طرق احتيالية[2].

الفرع الثاني: الإجراءات الوقائية المتخذة من قبل البنوك

القوم البنوك والمؤسسات المصرفية بتوفير الحماية التامة للحسابات التي تخص عملائهم لتحقيق الآمال ومنع التلاعبات التي تقع عليها من جهة، ولتعزيز الثقة بينها

[1]- أمجد حمدان الجهني، المرجع السابق، ص115.

[2]- عبد الكريم الردايدة، المرجع السابق، ص 180.

وبين عملائها من جهة أخرى، وذلك عن طريق إجراءات إدارية خاصة وكذلك إجراءات تقنية وأخرى رقابية[1].

نستعرض من خلال هذا الفرع الإجراءات الرقابية **(أولا)**، الإجراءات الإدارية **(ثانيا)**. إجراءات أخرى **(ثالثا)**.

أولا: الإجراءات الرقابية.

تخضع البنوك والمؤسسات المصرفية في أداء مهامها إلى قواعد تنظيمية داخلية يتولى تنظيمها البنك المركزي من حيث إجراءات الإشراف والرقابة والتوجيه، وهذا بهدف الاستقرار الداخلي للبنوك وللحفاظ على أموال العملاء، وتتجلى هذه الرقابة فيما يلي: الرقابة التوجيهية **(1)** ، الرقابة الداخلية **(2)** ، الرقابة الخارجية **(3)** ، الرقابة الزجرية **(4)** .

1- الرقابة التوجيهية: وتتمثل هذه الرقابة في إصدار التوصيات والتوجيهات للبنوك المشرف عليها وذلك الاهتمام بالمشاكل التي تواجهها هذه الأجهزة ومساعدتها على تجاوزها عن طريق دراستها ثم تقديم الاقتراحات المناسبة لها، وأيضا تحديد قواعد تسيير العمل المصرفي بما يتماشى مع التناسب بين الموجودات أو المطلوبات، كما أن للبنك المركزي سلطة توجيه التعليمات والمطالبة بالتقيد بمحتواها، وتوجه هذه التعليمات إلى كافة البنوك والمؤسسات المالية في الدولة وإلزامها بالتقيد باحترامها وتنفيذها[2].

2- الرقابة الداخلية: وتتم هذه الرقابة من خلال تحديد جزء من صلاحيات النظام الداخلي لأداء الرقابة على الحسابات التي تختص بحماية الأصول والسجلات لضمان دقة البيانات المحاسبية، كذلك تحديد جزء من النظام الداخلي للرقابة الإدارية وهي الإجراءات التي تنتهجها الإدارة بغرض تقييد هذه البنوك والمؤسسات، بالسياسة

[1]- أحمد سفر، أنظمة الدفع الإلكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008، ص 28.

[2]- حسين محمد الشلبي ومحمد فايز الدويكات، المرجع السابق، ص ص 100، 102.

الموضوعة من طرفها، والتأكد من الأداء الدقيق لعمل البيانات المالية ومنع الغش والخطأ، ويدوم بذلك أشخاص توظفهم الإدارة بعد التأكد من كفاءاتهم المهنية[1].

3- الرقابة الخارجية: وتتمثل هذه الرقابة في قيام أشخاص أو مؤسسات مستقلة بفحص ومراجعة البوابات الختامية للبنوك ومعرفة مدى صحتها ومصداقيتها بالاعتماد على القواعد المهنية المتبعة في ذلك، ومراقبة سلامة النظام الداخلي ومراجعة الرقابة الداخلية، تم إبلاغ إدارة البنك والسلطات المصرفية عن ملاحظة من شانها مخالفة القوانين المعمول بها[2].

4- الرقابة الزجرية: يمارس البنك المركزي رقابة زجرية عن طريق وضع قواعد وتعليمات، والمضاد بالالتزام التام بها ويتعرض كل من يخالفها إلى عقوبات مدنية أو جزائية، حيث يقوم بهذه الرقابة هيئات ولجان محددة لذلك تختص بالتأكد من التزام البنوك بما أقرته من أحكام، وتقوم هذه اللجان والهيئات الرقابية بهذه الوظيفة بصفة مباشرة أومن خلال موظفيها بقيامهم بدورات تفتيش مفاجئة للبنوك، وكذلك إجراء عمليات فحص للأوضاع الإدارية والمالية والتأكد من أن رأس المال مناسب للسيولة والتأكد أيضا من فعالية الوسائل المتبعة في الرقابة الداخلية ووسائل الإدارة، وما مدى قدرتها على المحافظة على سلامة البنك[3].

ثانيا: الإجراءات الإدارية

وتكون هذه الإجراءات عن طريق تعبين حد أقصى لاستخدام البطاقة أو سحبها أو المعارضة في قبولها وسنتناول فيما يلي كل عنصر على حدة: تحديد سقف لعمليات السحب بالبطاقة **(1)** ، سحب البطاقة **(2)**، المعارضة في قبول البطاقة **(3)**.

---

[1]- حسين محمد الشلبي ومحمد فايز الدويكات، المرجع السابق، ص103.

[2]- عبد الكريم الردادة، المرجع السابق، ص 101.

[3]- المرجع نفسه، ص 102.

1- تحديد سقف لعمليات السحب بالبطاقة: الأصل أن يتم تحديد سقف للبطاقة لا يمكن تجاوزه، واستثناءات قد يسمح بذلك في حالات معينة والهدف امن ذلك منع إفراط صاحب البطاقة في استعمال بطاقته خوفا من عدم إيفاءه بمصاريف المشتريات المترتبة عليه بتاريخ تسويتها المتفق عليه مع البنك، كذلك خوفا من وقوعها في يد الغير ولذلك وجب تحديد سقف الاستخدام البطاقة حيث يكون هذا التحديد سواء عند استخدامها في عمليات السحب أو الوفاء على حد سواء[1].

أ- الحد الأقصى لاستخدام البطاقة في الوفاء: في هذه الحالة نميز بين استخدامين:

- عند استخدام البطاقة في الجهاز اليدوي يكون السقف منعدم، ويتوجب الحصول على ترخيص من المصدر عند كل عملية، كما يتوجب على التاجر حفظ رقم التفويض في الخانة المخصصة له على الفاتورة لأنه لا يعلم برصيد البطاقة.

- عند استخدام البطاقة في الجهاز الإلكتروني يظهر خلال تمرير البطاقة في الجهاز على الشاشة م تحتوي رصيد كافي لإتمام عملية الوفاء أم لا، فإذا تجاوز حد الرصيد يرفض الجهاز إتمام هذه العملية إلا بعد حصول التاجر من المصدر على تفويض بالموافقة[2].

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 بطاقات الدفع العادية يكون نصف سقف البطاقة، وفي البطاقات التي تستخدم في الوفاء يكون نفس الرصيد المتوافر في الحساب، وفي حالة السحب اليومي فإن الحد

[1]- بيار إميل طوبيا، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، د ط، منشورات الحلبي الحقوقية بيروت، 2000، ص40.

[2]- أمجد حمدان الجهني، المرجع السابق، ص 116.

الأقصى للسحب يختلف من بنك لآخر حسب التسهيلات التي يمنحها كل بنك لعملائه[1].

2- سحب البطاقة: قد يتم سحب البطاقة من طرف المصدر أومن طرف التاجر من أجل الحفاظ على حقوق جميع الأطراف ومنع التجاوزات التي قد تتم عن طريق البطاقة.

أ- سحب البطاقة عن طريق المصدر: للبنك الحق في استرجاع البطاقة من صاحبها بالنص على ذلك في العقد بأن البطاقة ملك للمصدر، حيث استطيع هذا الأخير الطلب من صاحبها بإعادتها إليه أو إلغاءها وهذه العملية قانونية إذا كانت ناتجة الأب جوهرية ويخشي بقاؤها عند صاحبها، أما إذا انعدمت هذه الأسباب فهذا يعتبر تعسف من قبل المصدر ووجب التعويض، ويكون هذا السحب سواء بالطريقة العادية عندما يطلب المصدر إرجاع البطاقة بطريقة فنية في حالة برمجة الصراف الآلي على سحبها[2].

ب- سحب البطاقة عن طريق التاجر: ينشأ اتفاق بين المصدر بصفته مالك للبطاقة مع التاجر بصفته وكيل على القيام بسحب البطاقة وإرجاعها المصدر مقابل مكافأة على كل بطاقة مسحوبة، وذلك لتشجيعهم على مكافحة الجرائم الناتجة عنها، ويقوم التاجر يسحب البطاقة في حالات عدة كان تكون البطاقة ضمن قائمة البطاقات التي ورد رقمها في الكس الدوري التحذيري الذي تم توزيعه على التجار، أو كان يعرف التاجر صاحب البطاقة ولكن تم استخدامها من قبل الغير فشك في كيفية وصولها إليه[3].

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص 117

[2]- وسام محمود الشواورة، المرجع السابق، ص 116.

[3]- أمجد حمدان الجهني، المرجع السابق، ص ص، 118، 119.

3- المعارضة في قبول البطاقة: المعارضة عبارة عن إجراء وقائي يعمل على عدم قبول البطاقة في عمليات الوفاء، وهذا في حالة سرقتها أو فقدانها أو لسبب آخر غير عادي بهدف حمايتها من العمليات المشبوهة.

وعملية المعارضة قد تصدر من قبل صاحبها عندما يكون قد فقدها أو سرقت منه، كذلك قد تصدر من طرف الجهة المصدرة عندما يتم إلغاءها، ويمكن تعريف المعارضة على أنها نظام يعمل على توزيع رقم البطاقة عن طريق نشرات تحذير بصفة دورية، وتقديمها للتجار الذين يتعاملون بها في عمليات الوفاء، وهذا التقديم بغرض إعلامهم وتحذيرهم منها والطلب منهم عدم قبولها في معاملاتهم سواء المتعاملين بالجهاز اليدوي أو الجهاز الإلكترونيpos أو الصراف الآلي[1].

أ- نشر المعارضة لدى التجار المزودين بالجهاز اليدوي: يتم هذا النشر من خلال تزويد هؤلاء التجار بقوائم تحتوي على أرقام البطاقات المراد عدم قبولها في عمليات الوفاء حيث يقوم التاجر بمطابقة رقم البطاقة المقدمة له للتعامل بها، مع أرقام القائمة وبالتالي يتم قبولها إذا كانت مخالفة لهذه الأرقام، وفي حالة تطابقها مع أحد الأرقام يتم رفضها ويقوم بسحبها، وإذا ما خالف التاجر أمر البنك المصدر قبل التعامل بالبطاقة فإن المصدر يقوم برفض صرف الفاتورة، إلا إذا قامت هذه الحالة في شكل قانوني وذلك في حالة حصول التاجر على تفويض من المصدر لقبولها[2].

ب- نشر المعارضة لدى التجار المزودين بالجهاز الإلكتروني pos: يتم تزويد هؤلاء التجار بشكل الكتروني من خلال تزويد الجهاز الإلكتروني لدى التاجر والموصول بجهاز المصدر بأرقام البطاقات المرفوضة، حيث بمجرد تمرير البطاقة عليه بتحديد تلقائيا ما إذا كانت مقبولة أو مرفوضة في الوفاء[3].

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص 119.

[2]- المرجع نفسه، ص120.

[3]- علي عدنان الفيل، المرجع السابق، ص82.

ج- نشر المعارضة من خلال جهاز الصراف الآلي: ويكون ذلك برمجة جهاز الصراف الآلي الموصول بكمبيوتر البنك على رفض البطاقة خلال عمليات السحب وفي حالة ما إذا كانت البطاقة مسروقة أو مفقودة فالجهاز يقوم بسحبها وعدم إعادتها[1].

ثانيا: الإجراءات التقنية

اتجهت البنوك في مواجهة مخاطر بطاقة الدفع الإلكتروني إلى إجراءات تقنية بتطبيقها على الحواسيب الآلية والبطاقات، وذلك بهدف الكشف المبكر عن أي عملية مشبوهة ومن بين هذه الإجراءات:

- التحديث الدائم والمتجدد لشفرة بطاقات الدفع حتى يصعب على المحتالين التعرف عليها، واستحداث تقنيات للتعرف على هوية البطاقة الأصلي كإدخال صورته في البطاقة وتأمينها بحيث يصعب إزالتها وتزوير هاء واستخدام بصمات الصوت والعين والأصابع.

- استخدام نظام خدمة الرسائل القصيرة في الهواتف المحمولة الذي يعمل على وصول الإشعارات لأصحابها لتخبرهم فور إجراء أي عملية.

- استخدام تقنية الجدران النارية التي تعمل على مراقبة جميع عمليات الدخول إلى النظام الداخلي للبنك، ومن ثم اكتشاف العمليات المشبوهة الكترونيا

- استخدام كلمات سرية معقدة للدخول إلى الأنظمة الإلكترونية بحيث تكون مزيج من الأرقام والحروف يصعب تخمينها من الغير[2].

ثالثا: إجراءات أخرى

حتى تضمن البنوك الحماية التامة لتعاملاتها سواء مع عملائها أو مع التجار، وضمان إيفاء أموالها والوقت المناسب، ومنع التلاعبات تقوم بأداء مهامها على أكمل

[1]- أمجد حمدان الجهني، المرجع السابق، ص 121.

[2]- علي عدنان الفيل، المرجع السابق، ص82.

وجه من خلال إجراءات رقابية وتأهيلية خاصة إما بالموظفين أو العمال أو التجار، بالنسبة للموظفين **(1)** ، بالنسبة للعملاء **(2)** ، بالنسبة للتجار **(3)**.

1- بالنسبة للموظفين: وتشمل الإجراءات الرقابية الخاصة بالموظفين في:

- قيام المصرف بمنع الموظفين من استخدام أي أجهزة من دون تلك المحددة من طرف المصرف من خلال المراقبة المستمرة لها، وهذه الأجهزة والنقاط تعمل على ربط الشبكة والأنظمة الداخلية للمصرف مع الفضاء الخارجي[1].

- قيام البنك بمراقبة جميع الأجهزة وحمايتها وحفظها في أماكن آمنة لا يسمح لأحد بدخولها من غير الموظفين المخولين بالدخول، كما لا يسمح لغير الموظفين المعنيين من الاطلاع على معلومات الشبكة الداخلية حتى لا يقوموا بالعبث بالشبكة، لأن الكثير من الجرائم تتم من طرفهم أو بمساعدتهم نظرا لمعرفتهم بالنظام الداخلي أكثر من المجرمين خارج المصرف وأيضا بهدف عدم تسريب المعلومات وكذلك منع الموظفين من إفشاء السرية الخاصة بالحامل[2].

أما إجراءات التأهيل تتمثل في:

- إنشاء برامج تدريبية للموظفين في المصارف بهدف تعليمهم كيفية فحص بطاقات الدفع الإلكتروني ليتم اكتشاف التلاعب فيها بشكل فوري وتحديد السلوك المشبوه المتبع في ذلك.

- القيام بتدريب موظفي المصرف على طرح أسئلة معينة أثناء مكالماتهم الهاتفية للرد على طلبات التجار بالحصول على موافقات أو متابعة المعاملات الفورية، والمعاملات ذات المبالغ الكبيرة التي تتم على بطاقة أجنبية[3].

---

[1]- علي عدنان الفيل، المرجع السابق، ص 82

[2]- أمجد حمدان الجهني، المرجع السابق، ص 184.

[3]- عبد الكريم الردايدة، المرجع السابق، ص 183.

وهذه الإجراءات التأهيلية تشمل موظفي المتاجر والمحلات التي تتعامل ببطاقات الدفع من خلال قيام البنوك بدورات تدريبية لهؤلاء الموظفين لتدريبهم على كشف البطاقات المزورة بسهولة.

2- بالنسبة للعملاء: إن الاختيار الحسن العملاء المتقدمين للبنوك بنية الحصول على بطاقات الدفع الإلكترونية، حيث يتم إخضاعهم لمعايير خاصة بغرض دراسة مركزهم القانوني والمهني والمالي، والتأكد من صحة البيانات التي قاموا بتقديمها وهوما يقلل من تسلل العملاء غير الجادين وبالتالي الحد من تلاعباهم، ويعد إتمام هذه العملية والتأكد من أن هوية الحامل مطابقة للبيانات، يستوجب على البنك تسليم البطاقة إلى حاملها بشكل شخص ومطابقة توقيعه مع الذي مع البطاقة.

- قيام البنوك بإجراء كشوفات دورية قصيرة المدى لحسابات العملاء وإبلاغهم بها، حتى يتم كشف أي اختلاس فور حدوثه[1].

- مراقبة عمليات الوفاء والسحب من العملاء لاكتشاف أي استخدام مشبوه لتلك البطاقة والتأكد من عدم مجاوزة سقف البطاقة أو صلاحيتها[2].

3- بالنسبة للتجار: وكما الحال مع العملاء يتم الاختيار الحسن من قبل البنك التجار والمؤسسات التجارية التي تتمتع بسمعة طيبة، مع الاستقرار القانوني والمهني والمالي[3].

- تزويد البنوك التجار والمؤسسات التجارية بالأجهزة الإلكترونية الحديثة للتعامل بها ومن خلالها يتم الكشف الفوري عن البطاقات المزورة، مع التزامه بتسليم هذه المكينة

[1]- نهى خالد عيسي، ماهية بطاقات الائتمان والآثار القانونية المترتبة عن استخدامها، مجلة المحقق الحلبي للعلوم القانونية والسياسية، العدد الثاني، السنة السابعة، 2015، ص242.

[2]- علي عدنان الفيل، المرجع السابق، ص 79.

[3]- المرجع نفسه، ص 79.

شخصيا، وهذا الاحتمال وقوعها في يد الغير الذي قد يستغلها في أعمال غير شرعية[1].

– مراقبة البنك للعمليات المصرفية للتاجر والتأكد من استيفاء بيانات إشعار البيع كاملة، هذه الأخيرة التي سلمها للبنك وقبض قيمتها وتتمثل في التاريخ الواضح الذي يثبت عملية البيع للعميل ولا تتجاوز أسبوع من تاريخ تقديمه للبنك، كما يجب أن تكون بيانات العميل مطبوعة بشكل واضح بواسطة الماكينة المقدمة له من البنك، وأن يكون المبلغ مكتوبا بشكل واضح في الخانة الخاصة له في الإشعار، وأن تكون المعاملة أجريت بعد أخذ الموافقة عليها من البنك يومها حيث يتم مطابقة رقم الموافقة على المبلغ والتاريخ وإذا ثبت العكس تخصم القيمة من حساب التاجر.

– كذلك يجب أن يتم إجراء المعاملة للعميل في وجوده، وبعد التأكد من هويته واخذ توقيعه على الشعارات البيع بعد مطابقته لتوقيعه على البطاقة حيث وجب أن يكون بشكل واضح، كما يتم رفض أي إشعارات أخرى مخالفة لما سبق بيانه وفي حالة مخالفة التاجر لهذه التعليمات فإن البنك يقوم بإلغاء التعامل معه واسترجاع الأجهزة المقدمة له بالإضافة لاسترجاع المبالغ التي تم صرفها مقابل مخالفته لتلك التعليمات[2].

المطلب الثاني

الإجراءات الوقائية المتخذة من قبل صاحب البطاقة والتاجر والجهاز الأمني

الإجراءات الحد من الجرائم الواقعة على بطاقات الدفع الإلكتروني لا يقتصر على الجهات المصدرة لها والبنوك بصفة عامة، بل يمتد ليشمل الحامل والتاجر وهذا تنفيذا لالتزاماتهم المبرمة في العقد وفي نفس الوقت حفاظا على حقوقهم ومصالحهم لأن الضرر الأكبر يقع عليهما.

[1]– عبد الكريم الردايدة، المرجع السابق، ص 184.

[2]– علي عدنان الفيل، المرجع السابق، ص ص، 80، 81.

ولذلك يجب على صاحب البطاقة المحافظة على بطاقته واتخاذ الاحتياطات اللازمة لذلك، حتى يتفادى وقوع بطاقته في يد الغير ومن ثم التلاعب بها وهذا ما سنتطرق إليه في **(الفرع الأول)** من هذا المطلب، كذلك يجب على التاجر أن يأخذ احتياطاته أثناء التعامل بالبطاقة، واكتشاف الاستعمال غير الشرعي لها وتبليغ الجهات المختصة وهوما سنتناوله في **(الفرع الثاني)**، ومن جهة أخرى تتدخل الشرطة بصفتها الجهاز الأمني بمجموعة من الإجراءات الوقائية لصد هذه الجرائم وهوما سيتم دراسته في **(الفرع الثالث)**.

الفرع الأول: الإجراءات الوقائية المتخذة من قبل صاحب البطاقة

يقوم صاحب البطاقة والمستفيد الأول من خدماتها بمجموعة من التدابير والإجراءات الوقائية للمحافظة على البطاقة وحمايتها من الضياع وكل أشكال الجرائم المنفذة عليها وتتجلى هذه الإجراءات فيما يلي: حماية البطاقة والمحافظة على بياناتها **(أولا)**، حماية البطاقة من خلال المعاملات التجارية **(ثانيا)**.

أولا: حماية البطاقة والمحافظة على بياناتها

ويتم ذلك من خلال عدم إهمال البطاقة والحرص على وضعها في مكان آمن، وأن لا يتركها صاحبها عند أي شخص إلا بعد التأكد من هويته حتى إذا كان موظف البنك نفسه أو ضابط شرطة، كما يجب عدم الإفصاح عن رقم البطاقة أمام الغير أو كتابته على وجه البطاقة أو على أي ورقة مكشوفة وغيرها من الأشكال الأخرى، وأن يتلف الوصل في حال طلبه من الصراف لأنه يحتوي على رقمها وأيضا بالنسبة للفاتورة التي يعطيها التاجر له، كما يجب عليه عند تشكيل الرقم السري للبطاقة أن يختار أرقاما وحرفا يصعب اكتشافها[1].

[1]– عبد الكريم الردايدة، المرجع السابق، ص 188.

وفي حال ضياع البطاقة أو رقمها السري فيجني على صاحبها الإبلاغ الفوري عن ذلك للجية المصدرة لها والتي تقوم بإلغائها بناء على هذا الإبلاغ، إضافة إلى ذلك، يجب على صاحب البطاقة إبلاغ الجهة الصدرة أيضا في حال اكتشاف وجود جهات لم يتعامل معها من خلال وصل كشوفات حساب البطاقة حيث تقوم الجهة المصدرة بالتحقق من هوية هذه الجهات التي استخدمت البطاقة دون علم صاحبها[1].

كما يجب على صاحب البطاقة أن يحرص على عدم شحن رصيد بطاقته بمبالغ كبيرة، ليتجنب خسارة أكبر إذا تم استخدامها من قبل الغير، كذلك عند تعامله عليه أن لا يطلب مساعدة الغير وإذا لاحظ أن هناك من يراقبه أثناء إجراء عملياته المصرفية فعليه أن يقوم بإلغاء تلك العملية والانتقال إلى جهاز آخر في مكان آمن[2].

ثانيا: حماية البطاقة من خلال المعاملات التجارية

وفي هذه الحالة تكون أمام حالتين: الحالة العادية **(1)** ، حالة المعاملات عبر الانترنت **(2)**.

1- الحالة العادية: يحرص صاحب البطاقة أثناء تواجده في المحلات التجارية بأن يتسوق في أماكن آمنة ورفقة أشخاص محل ثقة، كما يجب التأكد من السلعة المراد شراؤها بمعاينتها والتأكد من سعرها الحقيقي ثم كيفية الحصول عليها، إضافة إلى التحقق من هوية ومصداقية التاجر وأيضا مطالبته بكافة الضمانات قبل إجراء المعاملة وأن يتحقق جيدا من وصل الشراء قبل توقيعه كما يجب عليه الاحتفاظ بنسخة منه وبكل الوثائق التي تثبت إجراء المعاملة، كما يجب إبلاغ البنك أو الشرطة في حال لم تسترد بطاقة الدفع من الجهاز أو إذا ما لاحظ صاحبها أشياء غير عادية كأجهزة غريبة متصلة مثلا[3].

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص ص، 122، 123.

[2]- المرجع نفسه، ص 122.

[3]- عبد الكريم الردايدة، المرجع السابق، ص ص189، 193.

2- حالة المعاملات عبر الانترنت: يعتبر التعامل عبر شبكة الانترنت أخطر بكثير من نظيره على الواقع، لذلك وجب على صاحب البطاقة أخن الحيطة والحذر من خلال بعض التدابير قبل إجراءه لأية عملية ومن أهمها:

- الحرص على التعامل مع المواقع المشهورة والموثقة، وتفادي المواقع غير المعروفة والتي تفتق الإجراءات حماية بطاقات الدفع، ولذلك وجب التأكد من وجود اتصال امن من خلال وجود كلمة (https) في بداية عنوان الموقع أوعن طريق التأكد من القفل المغلق أسفل نافذة المتصفح[1].

- أن يلتزم صاحب البطاقة بقراءة صفحة المعلومات على الموقع والمتعلقة بشروط العملية كرسوم التوصيل أو الضرائب والعملات، ومعرفة موقع التاجر والتأكد من جودة سلعته أو كيفية إرجاعها.

- أن يستعمل برامج الحاسوب المشفرة لحماية بريده الإلكتروني كما يجب عليه الحفاظ على كلمة السر الخاصة به ولا يسمح لأحد بمعرفتها، كما لا يسمح للجهاز بحفظها أو تذكرها من خلال تزويده بمفتاح التشفير لمنع اختراقه والوصول للبيانات[2].

- على الحامل إبلاغ الجهة المصدرة للبطاقة في حالة مغادرة العنوان البريدي والانتقال لأخر، وفي حالة وصول رسائل البريد الإلكتروني التي تنسب إلى البنوك أو أي جهة أخرى بعد التحقق منها، وكذلك في حالة ما إذا كان هناك اتفاق مسبق بين صاحب البطاقة والبنك عن موعد وصول البطاقة عبر البريد ولم يحصل ذلك، كما يجب عليه أيضا إبلاغ البنك في حالة التأكد من وصولات كشف الحساب، وتبين له أنه تم التلاعب بها لعدم مطابقتها للموصولات المقدمة من قبل البنك[3].

---

[1]- علي عدنان الفيل، المرجع السابق، ص 84.

[2]- المرجع نفسه، ص 85.

[3]- عبد الكريم الردايدة، المرجع السابق، ص ص 188، 193.

– رفض الرد على المكالمات والرسائل البريدية وبعض المواقع التي تطلب من صاحب البطاقة تفاصيل عن حسابه ورقمه السري ورقم البطاقة، وإن لزم الأمر الاتصال بالشرطة.

الفرع الثاني: الإجراءات الوقائية المتخذة من قبل التاجر

في إطار شروط العقد بين التاجر والجهة المصدرة للبطاقة، يلزم القيام ببعض الإجراءات قبل إجراء المعاملة حتى يضمن سلامتها ومن بينها: أثناء تنفيذ العملية **(أولا)**، التأكد من صحة البطاقة **(ثانيا)**، رفض البطاقات غير الصالحة **(ثالثا)**، رفض التعامل مع حامل البطاقة **(رابعا)**.

أولا: أثناء تنفيذ العملية

– يجب التأكد من هوية صاحب البطاقة من خلال مطابقة توقيعه المدون على الفاتورة بالتوقيع الذي تحمله البطاقة، والتحقق من أن البطاقة ليست ضمن القائمة المحظورة.

– الالتزام بعدم تقسيم المعاملة إلى عدة تمريرات عبر الجهاز والاكتفاء بواحدة فقط، وإذا لم يستطع تمريرها عبره فله أن يرفضها[1].

– اعتماد رمز التفويض على المعاملة من جهاز التاجر أو مركز التفويض لدى المصدر دون غيرهما[2].

– عند تمرير البطاقة وظهور عبارة راجع الجهة المصدرة فعلى التاجر التوقف فورا عن تمريرها، أو الاتصال بالبنك صاحب التفويض للحصول على رمزه وقبول المعاملة[3].

– القيام بإعداد سند المديونية الذي يتمثل في فاتورة وإشعار البيع وما تتضمنه من تاريخ المعاملة وقيمها وبصمة البطاقة، ثم التوقيع عليها من قبل صاحب البطاقة.

---

[1]– عبد الكريم الردايدة، المرجع الساق، ص185.

[2]– أمجد حمدان الجهني، المرجع الساق، ص ص 124، 125.

[3]– وسام فيحل محمود الشواورة، المرجع السابق، ص 107.

– قيام التاجر بالاحتفاظ بالشعرات الخصم أطول مدة ممكنة.

– التزام التاجر بعدم تسوية أي مديونية بين صاحب البطاقة وغيره من التجار.

– يجب على التاجر مراقبة موظفيه أثناء قيامهم بمعاملات بطاقات الدفع حتى يتجنبوا أي تجاوزات[1].

ثانيا: التأكد من صحة البطاقة

يجب أن تكون البطاقة سليمة وسارية المفعول، وأن تحتوي على المبلغ الكافي لقيمة المشتريات، كما يجب أن تكون سليمة من حيث الشريط الخاص بالتوقيع عليها، وأن تكون بياناتها سليمة ومطابقة البيانات صاحبها، كما يجب أيضا التأكد من سلامة رقمها والتوقيع الموجود عليها وذلك بمطابقتها مع ما هو مدون في الوصل[2].

ثالثا: رفض البطاقات غير الصالحة

يحب على التاجر رفض بطاقات الدفع في حالات معينة، كان تكون البطاقة مقدمة من قبل الغير، أو أن تكون قد تم التعديل فيها أو إتلافها، إضافة إلى البطاقات العالمية التي لا تتضمن علامات الضمان كبطاقة فيزا، وماستر كارد، وأمريكان اكسبريس[3].

رابعا: رفض التعامل مع حامل البطاقة

يجب على التاجر رفض التعامل مع حامل البطاقة المشتبه بهم، ومثال ذلك الذين يقومون بعمليات شرائية صغيرة وكثيرة لضمان بقائهم في مستوى آمن، كذلك من يقوم باختيار سلع متنوعة مع إهمالهم للجودة والحجم والسعر، أو شراء أغراض ثمينة

[1]– عبد الكريم الردايدة، المرجع الساق، ص 185.

[2]– علي عدنان الفيل، المرجع السابق، ص 125.

[3]– المرجع نفسه، ص 126.

من خلال تقديمهم لبطاقات حديثة، ولا يملكون أي إثبات لهوياتهم ويظهر عليهم الاضطراب والقلق[1].

ومما سبق فإن التاجر إذا ما اشتبه في أحدهم فيتوجب عليه إبلاغ البنك حتى لا يقع ضحية لجريمة الاحتيال والسرقة أو التزوير، لأنه في حال وقوع أي تجاوزات فإنه هو من يتحمل المسؤولية والقدر الأكبر من الخسائر[2].

الفرع الثالث: الإجراءات الوقائية المتخذة من قبل الأجهزة الأمنية

في ظل غياب تشريع صريح يضبط هذه الجرائم فإن العبء الأكبر يقع على الأجهزة الأمنية، حيث تعرف الشرطة على أنها الجهاز الذي يتكفل بحفظ الأمن وتوفيره للأفراد والمجتمع، ولتحقيق ذلك فهي تقوم بوضع ضوابط لنشاط الأفراد حماية للنظام العام[3].

ومن بين المصالح التي تشملها الحماية الأمنية ما تعلق بالمعاملات المالية ومنها ما يتم ببطاقات الدفع الإلكتروني، حيث تتكفل هذه الأجهزة بمتابعة الجرائم التي تقع على هذه البطاقات عن طريق جهاز الضبطية الإدارية والذي يقوم بتتبع الأشخاص المشتبه بهم لمنع وقوعها مرة أخرى[4]، وفي ما يلي تستعرض جملة من الإجراءات الوقائية التي تتبناها أجهزة الشرطة:

الإجراءات المتعلقة بالبنوك والمؤسسات المالية **(أولا)**، الإجراءات المتعلقة بالأفراد **(ثانيا)**، الإجراءات المتعلقة بتطوير جهاز الشرطة **(ثالثا)**.

---

[1]– أمجد حمدان الجهني، المرجع السابق، ص 125

[2]– المرجع نفسه، ص 126.

[3]– عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان 2013، ص 102.

[4]– معادي أسعد صوالحة، بطاقة الإئتمان النظام القانوني وآليات الحماية الجنائية والأمنية (دراسة مقارنة)، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2011، ص 416.

أولا: الإجراءات المتعلقة بالبنوك والمؤسسات المالية

يتم التنسيق والتعاون مع البنوك والمؤسسات المالية لاطلاعهم بسرعة عن أي حدث مشبوه، أو جريمة أو خطر يهدد الأمن الداخلي للمؤسسة أو يمس بأموال الأفراد المتعاملين معها، كما يتم وضع قوانين وتعليمات لإلزام البنوك والمؤسسات المالية بالتبليغ عن الجرائم التي قد تتم أثناء التعامل بالبطاقات وعدم التستر عليها[1].

محاولة حل ومعالجة المخالفات التي تقع داخل البنك وعدم تركها وغض الطرف عنها، لأن ذلك من شأنه أن يشجع مرتكبيها أكثر ويلحق الضرر بسمعة البنك والصالح العام، وبما أن هذه الجرائم الكترونية فإن عدم معالجتها بسرعة يدفع مرتكبيها لتطوير تقنياتهم ووسائلهم أكثر وهذا ما يؤدي إلى عدم مجاراتهم وإفلاتهم من العقاب[2].

كذلك يعمل جهاز الشرطة على تأمين المؤسسات المتعاملة ببطاقات الدفع الإلكتروني، وإحاطتها بحراس الأمن وأفراد البحث الجنائي لمراقبة المجرمين ومن خلال تركيب أجهزة متطورة لتصوير البطاقات المستعملة حتى يتراجع المجرمون عن ارتكاب مثل هذه الأفعال المجرمة، كما يقوم جهاز الشرطة بإجراءات تفتيش دورية للجهات المصدرة لهذه البطاقات للتأكد من أنها خاضعة للمعايير الفنية والتقنية التي تمنع من تزوير ها، كذلك القيام بإجراءات لوضع خطط مسبقة تتسم بالسرعة والفاعلية تهدف إلى حماية المؤسسات المصرفية وتأميل نقل الأموال[3].

ثانيا: الإجراءات المتعلقة بالأفراد

الإجراءات المتعلقة بالأفراد العاديين **(1)** ، الإجراءات المتعلقة بالأفراد المجرمين **(2)**.

---

[1]– عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، المرجع السابق، ص 130.

[2]– عبد الكريم الردايدة، جرائم بطاقات الائتمان، المرجع السابق، ص130.

[3]– المرجع نفسه، ص ص129، 131.

1- الإجراءات المتعلقة بالأفراد العاديين: وذلك من خلال العمل على تنبيه وتوعية المواطنين ومستخدمي هذه البطاقات بالمخاطر التي تحيط بها، وذلك بعقد الندوات واللقاءات التوعوية والحملات التحسيسية حتى يكونوا على دراية كافية بذلك ومن ثم توخي الحيطة والحذر عند التعامل بها[1].

2- الإجراءات المتعلقة بالأفراد المجرمين: يقوم جهاز الشرطة بمراقبة وتتبع الأشخاص الخطرين ذوو السوابق العدلية في هذه الجرائم، وأيضا ممنيشتبه بهم خلال إحاطتهم بالمراقبة الأمنية المستمرة لضبط نشاطاتهم حتى لا يكرروا جرائمهم السابقة[2].

ثالثا: الإجراءات المتعلقة بتطوير جهاز الشرطة

ولأن جرائم بطاقات الدفع الإلكترونية من الجرائم غير التقليدية، وتتميز بالخصوصية عن بقية الجرائم وكذلك بالنسبة لمرتكبيها الذين يتمتعون بالخبرة العالية في مجال تقنية المعلومات، فمن الصعب التصدي لها ولذلك كان لزاما على الشرطة تطوير أجهزتها التقنية وكذلك أفرادها حتى تكون لهم القدرة على مجاورات هذه الجرائم[3]، ومن بين أهم هذه الإجراءات ما يلي:

- تأهيل العاملين من أفراد الشرطة في مجال المكافحة عن طريق وضع برامج تدريبية تقنية عالية، ذات صلة بإجراءات الوقاية من هذه الجرائم[4].

---

[1]- عبد الكريم الردايدة، جرائم بطاقات الائتمان، المرجع السابق، ص 116.

[2]- المرجع نفسه، ص 131.

[3]- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004، ص ص 163، 164.

[4]- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2015، ص99.

– العمل على إنشاء معمل جنائي متخصص وتدعيمه بالأجهزة والمعدات التقنية المتطورة، لاستغلالها في عمليات فحص البطاقات والمستندات والوثائق المستخدمة في تلك الجرائم للقدرة على مواكبتها[1].

– ضرورة إخضاع أفراد الشرطة لضوابط جدية بهدف انتقائهم من حيث اللياقة البدنية، والكفاءة العلمية والفكرية والثقافية، وذلك لجعلهم مختصين في مواجهة هذه الجرائم من حيث الأشخاص المرتكبين لها وأساليب ارتكابها، وبالتالي القدرة على التحقيق التقني للتعامل مع هذه القضايا[2].

– تدريب أفراد جهاز الشرطة على كيفية استعمال الأجهزة الإلكترونية وأدواتها وآلات الطباعة المخصصة لها، وهوما يؤدي إلى معرفتهم بكيفية استخدامها وهوما من شأنه أن يسهل عليهم اكتشاف ومتابعة الجرائم الواقعة على بطاقات الدفع الإلكتروني[3]، ومن جهة ثانية قدرتهم على التأكد من أن الجهات المتعاملة ببطاقات الدفع حاصلة عليها بموجب تراخيص قانونية أم لا، كما يمكنهم أيضا من وضع قاعدة بيانات إلكترونية تحتوي على أرشيف جميع الجرائم وبيانات مرتكبيها، ومن ثم تزويد البنوك الوطنية بالمعلومات الكاملة المتعلقة بالعملاء وهوما يعزز أمن واستقرار البنوك والمؤسسات المصرفية[4].

[1]– عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، المرجع السابق، ص118.

[2]– المرجع نفسه، ص131.

[3]– محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2014، ص257.

[4]– صراع كريمة، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم التجارية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، الجزائر، 2014، ص 83.

المبحث الثاني

الإجراءات الردعية

لما أدرك المشرع الجزائري خطورة الجرائم الإلكترونية وتناميها بشكل ملحوظ، عمل على تطوير الإجراءات الكلاسيكية الخاصة بالبحث والتحري عن الجرائم بما يتماشى مع هذه الجرائم المتحدة من خلال التعديل القوانين القيمة، كما عمل على وضع مشاريع قوانين جديدة لمواجهة هذه الجرائم، كما تم أيضا المصادقة على الاتفاقيات والمعاهدات الدولية التي تختص بهذا الشأن، والدراسة مختلف هذه الإجراءات لد قسمت هذا المبحث إلى مطلبان، نعرج على الإجراءات المتخذة من قبل المشرع الجزائري بغية تطوير الإجراءات المعتادة في البحث والتحري والمحاكمة بما يتماشى مع الجرائم الإلكترونية، **(المطلب الأول)** في حين خصصنا الدراسة الإجراءات والقوانين المستحدثة وما مدى مساهمة الجزائر في محاربة هذه الجرائم على الصعيد الولي **(المطلب الثاني)**.

المطلب الأول

الإجراءات الكلاسيكية للبحث والتحري في الجرائم المستحدثة

حتى يتم الكشف عن الجرائم وضبط دلال المؤدية إليها وإماطة اللثام عن مرتكبيها، تقوم الشرطة الفضائية بمجموعة من الإجراءات الخاصة بذلك وفقا لما يحدده القانون، وبما أن دراستنا تنصت على جريمة من الجرائم الإلكترونية فإن إجراءات البحث والتحري بها يجب أن تكون على مستوى من الخبرة النقية حيث يكون أفراد الشرطة على علم بهذه الإجراءات من جهة، ومن جهة أخرى تكون لهم خبرة في مجال المعلوماتية، الأجهزة التقنية، ولتباين هذه الأهرامات فقد قسمنا هذا المطلب إلى ثلاثة فروع، خصصنا ،الدراسة مرحلة في تلقي البلاغات وكيفية التعامل معها **(الفروع الأول)** ،

لننتقل بعد ذلك إلى دراسة المعاينة والتفتيش والضبط **(الفرع الثاني)**، في حين تناول في مرحلة المحاكمة **(الفرع الثالث)**.

الفرع الأول: تلقي البلاغات

يختلف التبليغ في الجرائم الإلكترونية عن التبليغ في الجرائم الأخرى، ذلك لأن الجريمة الإلكترونية تتم في فضاء افتراضي، لذا فإن المبلغ عن هذه الجرائم يجب أن يكون على دراية بالتقنية المعلوماتية، وبما أن هذا نادر الحدوث فإنه يتوجب على الشرطة محاولة اكتشاف هذه الجرائم بنفسها عن طريق أجهزتها الأمنية، حيث تقوم بنشر أفرادها حول المؤسسات المصرفية والأسواق والمحلات التجارية ومراقبة العاملين بهذه المؤسسات، والتأكد من مصداقية المعاملات المصرفية، وتتبع المشتبه بهم ورصد أي تحركات غير عادية تتم في داخل أو خارج هذه المؤسسات والمحلات.

وبعد التبليغ عن الجريمة أو الاشتباه بها يقوم أفراد الضبطية القضائية بالتحري وإعداد استراتيجية لبدء العمل واختيار الضباط الذين تتوفر فيهم الخبرة المعلوماتية لتسهيل الكشف المبكر عن الجريمة ومرتكبيها، تلقي البلاغات والشكاوي **(أولا)**، مرحلة البحث والتحري **(ثانيا)**، مرحلة تجهيز الوسائل **(ثالثا)**.

أولا: تلقي البلاغات والشكاوي

(1) المقصود بآلية التبليغ، **(2)** كيفية التبليغ.

1- المقصود بآلية التبليغ:

البلاغ هو إخبار السلطات المختصة عن جريمة حصلت أوقد تحصل، ويلتزم بالإبلاغ عن الجرائم كل فرد في المجتمع سواء كان هو الضحية أو غيره، ويهدف ذلك إلى سرعة تحرك الشرطة القضائية باعتبارها الجهة المختصة في الكشف عن الجرائم والحد من تناميها[1].

[1]- حسين ربيعى، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، رحاب شادية، في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016، ص 215.

أما في الجرائم المعلوماتية يكون الشخص المبلغ عن الجريمة على معرفة بالأجهزة الإلكترونية وتقنياتها، حتى تكون المعلومة المقدمة من طرفه واضحة، ومثال ذلك تلقي بلاغ مفاده ضبط أحد الأفراد بحوزته بطاقة دفع مزورة، أو يستخدم محررات مزورة[1].

وقد نص المشرع الجزائري على هذا الإجراء من خلال المادة 17 فقرة 1 من قانون الإجراءات الجزائية، والتي جاء فيها: " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و13 ويتلقون الشكاوي والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية "[2].

2- كيفية التبليغ:

تضع الجهات الأمنية كالشرطة والدرك تحت تصرف المواطنين مواقع ليتمكنوا من خلالها من التبليغ عن الجرائم، ومثال ذلك الموقع الإلكتروني للدرك الوطني: www.mdn.ppgn.dz،وكذلك الموقع الإلكتروني للأمن الوطني: www.dgsn.dz، لكن هذه المواقع ليست ملزمة للمبلغين حيث لهم الحرية في إتباع هذه الطرق المستحدثة أو الكلية بالطرق العادية[3]، في حين أنهم ملزمون بتحديد أسماء المشتبه بهم، والقيام الطباعة نسخة ثانية للبيانات المتضررة في الأجهزة، كما يجب عليهم الامتناع عن نشر الجريمة للغير، وبالتالي فإن التبليغ دور فعال في مساعدة الأجهزة الأمنية المختصة للتأكد من وقوع الجريمة وتحديد نوعها وتجهيز الوسائل المناسبة للكشف عنها[4].

---

[1]- علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية -دراسة مقارنة-، دون طبعة، المكتب الجامعي الحديث، الموصل، 2012، ص11.

[2]- أنظر المادة 17 من القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، السنة 43، الصادرة بتاريخ 24 ديسمبر سنة 2006.

[3]- حسين ربيعي، المرجع السابق، ص218.

[4]- المرجع نفسه، ص2018.

ثانيا: مرحلة البحث والتحري

انطلاقا من المعلومات المحصل عليها، يقوم رجال الضبطية القضائية بالتحري عن الجريمة من خلال وضع خطة مناسبة لها، وتعيين فريق العمل بهدف احتواء الجريمة والإحاطة بكافة جوانبها وذلك كما يلي: وضع خطة عمل **(1)** ، تشكيل فريق عمل **(2)** ، الخبرة **(3)**.

1- وضع خطة عمل: يقوم المحقق القضائي بتحديد خطة عمل لتحديد الأسلوب الأنسب للتحقيق في الجريمة من خلال معرفة نوع الجريمة وتخصيص الفريق المناسب للبحث والتحري عنها، كذلك يجب الإحاطة بالظروف التي وقعت فيها الجريمة من خلال الضرر الذي خلفته للضحية وللأجهزة الإلكترونية وتحديد مدى اختراقها، كما يتم بيض إنجاز قائمة تحمل أسماء المشتبه بهم وتحديد الأسئلة التي سيتم الاستجواب بشأنها مع مراعاة الأحكام القانونية في ما ذكر، وتقدير ما مدى الحاجة لمساعدة الخبراء في هذا المجال[1].

2- تشكيل فريق عمل: بعد الانتهاء من إعداد الخطة يتوجب على المحقق الرئيسي في الجريمة إعداد فريق عمل، وبالنظر الخصوصية جرائم بطاقات الدفع الإلكتروني التي تتم بسرعة ولا تترك أثارا بعد ارتكابها وصعوبة إيجاد أدلة إثبات لهذه الجرائم التي تعتمد على الذكاء والنضال التقني، ولذلك وجب أن يكون اختيار أفراد فريق العمل بعناية حتى يتمكنوا من الوصول إلى المعلومات المطلوبة ومن ثم توقيف مرتكب الجريمة[2].

ويتكون فريق العمل من مجموعة من الضباط الاتي ذكرهم:

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص 15، 16.

[2]- محمد لموسخ، تنازع الاختصاص في الجرائم الإلكترونية، مجلة الحقيقة، عدد 28، المطبعة العربية، غرداية، الجزائر، 2014، ص 145.

- **المحقق الرئيسي:** هو الذي يشرف على عملية التحقيق ويتولى توزيع المهام على الضباط الآخرين، ويكون خبير في إجراءات التحقيق وفي المجال ألمعلوماتي حتى يتمكن من السيطرة على الوضع واتخاذ القرارات المناسبة[1].

- **خبراء الحاسوب والانترنت:** وهم خبراء يكون عددهم واحد فأكثر حسب ما تطلبه إجراءات التحقيق ليكونوا على اطلاع كافي بالجريمة المعلوماتية وكيفية التحري عنها، خاصة أن الجريمة الإلكترونية تستدعي هؤلاء لدرايتهم بالمجال ألمعلوماتي والتقني.

- **خبراء تدقيق الحسابات:** لهم خبرة ودراية في التعامل مع البرامج المستخدمة في البنوك والمؤسسات المصرفية التي يتم من خلالها تبادل الأموال إلكترونيا، ومهمتهم الكشف عن الأسلوب الإجرامي المتبع في الجريمة وما نتج عنها من أضرار.

- **خبير التصوير**: يختص بالتصوير الفوتوغرافي والفيديو المسرح الجريمة.

- **خبير الرسم التخطيطي:** يتولى القيام بالرسم التخطيطي للجريمة بتقنية دقيقة، حيث توضح تقسيماته أماكن وجود الأشخاص والدلائل.

- **خبير البصمات:** ومهمته رفع البصمات خاصة تلك المرتبطة بالأجهزة المادية للحاسوب المتضرر، والتي تم استخدامها في الجريمة.

- **الخبير الاستشاري:** ويوضح وقائع الجريمة ويزيل الغموض عنها[2].

إضافة إلى ما سبق هناك ضباط آخرون موجودون وفق ما تطلبه ظروف الجريمة، مثل ضباط الحماية والتأمين، وضباط التفتيش وضباط القبض[3].

3- الخبرة: إن اختيار فريق العمل الذي يتولى التحقيق يجب أن تتوفر لديهم الدراية الكافية بالتقنيات الحديثة التي ترتكب الجريمة فيها أو بواسطتها، وذلك من خلال

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص 16، 17.

[2]- حسين ربيعي، المرجع السابق، ص ص221، 223.

[3]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص 18، 19.

تدريبهم في المجال المعلوماتي، وهذا ما يسمح لهم بالتعامل مع الملفات والبرامج والإحاطة بوسائل التلاعب بالأجهزة الإلكترونية ومحتوياتها، بالإضافة إلى ذلك يتم الاستعانة بخبراء مختصين بالحواسيب الإلكترونية وأنظمتها، حيث يتولى هؤلاء المختصون إزالة الغموض عن الجريمة، ومساعدة المحققين في تجميع الأدلة وحفظها وحفظ البيانات وعدم إتلافها خصوصا ما تعلق بالتقنيات الدقيقة التي يصعب على المحققين التعامل معها، ولذلك يساهم اللجوء إلى الخبراء في الكشف عن الجريمة في وقت مبكر وبالطريقة الملائمة[1].

ثالثا: مرحلة تجهيز الوسائل

حتى يصل المحققون إلى النتيجة المرجوة في التحقيق، يجب الاستعانة ببعض الوسائل والبرامج لتتبع العمليات التي تتم داخل أنظمة الحواسيب الآلية، فأما الوسائل فنذكر منها:

- **وضع الرموز:** وتتمثل هذه الوسيلة في تعيين رقم سري معاملة ما، لتتبع معطيات الأنظمة والبرامج المعالجة من خلال هذه المعاملة.

- **تتبع البرنامج:** يتم من خلال استخدام الرقم السري للبرنامج، أومن خلال تشغيل التعليمات الموجودة ضمن البرامج والتي يتمكن من خلالها المحقق من تحيين محتوي هذا البرنامج.

- **تتبع النظام:** وهذا الأسلوب شبيه بسابقه، حيث أن استخدام الرقم السري أو تشغيل التعليمات يتم داخل نظام التشغيل، وتتم الرقابة على مهامه ومنها تتبع العمليات التي تمت على مستواه.

- **لوحة المفاتيح:** ويتم الاستعانة بها لتزويد البرنامج بمختلف التعليمات التي تمكنهم من تتبع البرامج المشبوهة.

[1]- علي عدنان الفيل، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص21.

- **مقارنة المعلومات:** من خلال هذا الأسلوب تتم مقارنة المعلومات المشبوهة بالمعلومات الصحيحة.

- **التتبع من خلال حساب العميل:** وهذه الوسيلة يتم من خلالها معرفة العمليات التي قام بها الجهاز، فهي تسمح بحفظ وتسجيل معطيات نظام التشغيل وتوضح وضعه، مثل تحديد عدد مرات استخدام بطاقة الدفع على مستوى الجهاز[1].

إضافة إلى الوسائل السابقة الذكر، قد يستعين المحققون بعديد البرامج والتي نوجز أهمها في ما يلي:

- **برنامج إذن التفتيش:** من خلاله يتم إدخال البيانات اللازمة لتحديد الأدلة، وأيضا من خلاله يتم تحديد دليل معين من قائمة الأدلة المتحصل عليها والإحاطة بظروف ضبطه ويوضع في القرص الصلب أو المرن.

- **برنامج (xtree pro gold):** ويتم معالجة الملفات بواسطته والعثور عليها داخل الشبكة أو القرص الصلب.

- **برنامج (lap link):** من خلاله تتم عملية نسخ المعطيات عن طريق تشغيله بواسطة القرص المرن، حيث ينقلها من جهاز المتهم إلى قرص آخر بالاعتماد على المنفذ المتتالي.

- **برنامج (vieudisk):** يسمح هذا البرنامج باختراق القرص المرن مهما كانت درجة تأمينه، والحصول على معطياته.

- **برنامج اتصالات:** يعمل هذا البرنامج على إيصال جهاز المتهم بالجهاز الخاص بالمحقق للحصول على معلوماته[2].

---

[1]- محمود إبراهيم غازى، الحماية الجنائية للخصوصية والتجارة الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية الإسكندرية، 2014، ص ص 704، 705.

[2]- حسام محمد نبيل الشنراقى، جرائم الاعتداء على التوقيع الالكتروني، دون طبعة، دار الكتب القانونية، مصر، 2013، ص690.

الفرع الثاني: المعاينة والتفتيش والضبط

بعد تلقي البلاغات والاستعداد اللازم لمباشرة عملية التحري، يقوم ضباط الشرطة القضائية ببعض الإجراءات للإحاطة بمسرح الجريمة من خلال الانتقال للمكان ومعاينته، وتفتيش محتوياته وضبط أي أدلة من المحتمل أن تقودهم لاكتشاف الجريمة ومرتكبيها وهوما سنوضحه فيما يلي: المعاينة **(أولا)**، التفتيش في المجال المعلوماتي **(ثانيا)**، الضبط **(ثالثا)**.

أولا: المعاينة

تم النص عليها بموجب المادة 61 من قانون الإجراءات الجزائية، ويقصد بالمعاينة الانتقال لمكان الجريمة ورؤية أثارها، والإبقاء عليها على حالتها حتى لا يتم العبث بها مما يتسبب في إتلافها، والمعينة إجراء وجوبي في الجنايات وجوازي في الجنح، وتتم في الأماكن العامة أو الخاصة على حد سواء، غير أنه في الأماكن الخاصة تحتاج لرضا صاحب المكان أو بإذن قضائي وفي نهاية هذه المرحلة يتم وضع الأختام على ما تم معاينته وتعيين حارس عليه[1].

وتلعب المعاينة دور أساسي في توضيح الجرائم من خلال إثباتها وإسنادها لفاعلها الحقيقي، وفي الجرائم المعلوماتية يجب التفريق بين مسرحين للجريمة، فهناك المسرح التقليدي وتتم فيه معاينة الأشياء الملموسة التي تقع خارج أنظمة الأجهزة الإلكترونية ومثال ذلك الأوراق أو المستندات، بينما في مسرح الجريمة التقني يتم معاينة الأشياء الافتراضية وهي المكونات الموجودة داخل أنظمة الحواسيب والانترنت ومثال ذلك البرامج والتطبيقات والملفات الإلكترونية[2].

[1]– محمدي بوزينة أمينة، مداخلة علمية بعنوان: إجراءات مكافحة الجرائم المعلوماتية، ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 57.

[2]– محمود إبراهيم غازي، المرجع السابق، ص ص 718، 721.

ثانيا: التفتيش في المجال المعلوماتي

يقصد بالتفتيش ذلك الإجراء من إجراءات التحقيق، يقوم به أحد رجال الضبطية العدلية المختص في إجراءات التحري ويهدف من خلاله إلى ضبط الأدلة والقرائن، التي تساهم في إثبات وقوع الجريمة وكشف الجاني، ويتم هذا الإجراء مع مراعاة الضوابط القانونية[1].

ومن خلال هذا التعريف تظهر الأهمية البالغة للتفتيش في مجال مكافحة الجريمة، وفيما يلي سوف نستعرض هذه العملية في المجال الرقمي أين يتم التفتيش على نظم المعالجة الآلية للمعطيات التي تضم مكونات غير مادية، شروط تقييد الحريات **(1)** ، تفتيش المكونات المادية لنظام المعالجة الآلية **(2)**. تفتيش المكونات المنوية لنظام المعالجة الآلية **(3)** ، التفتيش عن بعد أن تكون الشبكة المعلوماتية من مجموعة من الأجهزة الإلكترونية **(4)**.

1- شروط تقييد الحريات: قبل التعرض لكيفية التفتيش في البيئة الرقمية، ارتأينا أولا بيان الشروط اللازمة لصحته لأنه إجراء فيه نوع من تقييد الحريات، وقد وضع المشرع الجزائري ضوابط المباشرة هذا الإجراء من خلال شروط شكلية وأخرى موضوعية.

أ- **الشروط الشكلية:** عند إجراء التفتيش يجب مراعاة ما يلي[2]:

- **الحضور**: بالرجوع إلى نص المادة 45 فقرة 1 من قانون الإجراءات الجزائية، نجد أن المشرع الجزائري قد أقر حضور بعض الأشخاص عند إجراء عملية التفتيش، لكنه مع خصوصية الجرائم الواقعة على النظم المعلوماتية فقد لفي المشرع عنها هذه الشروط، وذلك بموجب نفس المادة السابقة الذكر في أقرتها الأخيرة ابعد التعديل الذي

[1]- سلطان محمد شاكر، ضمانات المتهم أثناء مرحلة التحريات الأولية والتحقيق الابتدائي، مذكرة لنيل شهادة الماجستير في القانون، مباركي دليلة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

[2]- محمد إبراهيم غازي، المرجع السابق، ص ص 718، 721.

جاء به القانون 06-22، حيث نصت على أنهلا تطبق هذه الأحكام إذا تعلق الأمر... بأنظمة المعالجة الآلية للمعطيات..." [1]

- **وقت إجراء التفتيش:** بالنسبة لوقت إجراء التفتيش في الجرائم الماسة بالأنظمة الآلية، خرج المشرع الجزائري عن القاعدة التي أقرها بالنسبة للجرائم الأخرى بموجب المادة 47 فقرة 3 من قانون الإجراءات الجزائية والتي نصت على أنه: " وعندما يتعلق الأمر....أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات..... فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني وغير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص" [2].

يتضح من نص المادة أن الجرائم المعلوماتية بصفة عامة يتم التفتيش فيها بشكل مفتوح ليلا ونهارا لأن تأجيل التفتيش في مثل هذه الجرائم قد يؤدي إلى عرقلة تتبعها.

- **محضر التفتيش:** يلتزم ضابط التحقيق بتحرير محضر بدون عليه ما توصل له من خلال إجراء التفتيش، وهذا المحضر تجب لصحته بعض الشروط مما تضمنتها القواعد العامة، وهو نفس الشيء بالنسبة لإجراءات التفتيش في النظم المعلوماتية حيث يجب أن يحتوي هذا المحضر على تاريخ تحريره، ويجب أن يكتب باللغة الرسمية، وأن تدون فيه كل الإجراءات المتخذة وفي الأخير يجب أن يوقع عليه من قبل محرره إضافة إلى أنه يمكن الاستعانة في تحريره بمن يملك الخبرة في مجال تقنية المعلومات[3].

ب- الشروط الموضوعية: وهي القواعد التي يخضع لها التفتيش ضمانا لصحته وتتمثل في ما يلي:

---

[1]- أنظر المادة 45 من قانون الإجراءات الجزائية.

[2]- أنظر المادة 47 من قانون الإجراءات الجزائية.

[3]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص418.

- **السبب:** حتى يتم التفتيش يجب أن يكون سبب مقنع لإجرائه من أجل الوصول إلى كشف الجريمة، حيث يجب أن تكون جريمة قد وقعت بالفعل ماسة ينظم المعالجة الآلية للمعطيات، وقد حدد المشرع الجزائري مجموعة الحر الم الماسة ينظم المعطيات في القانون 04-15 الذي أدرج فصلا كاملا في قانون العقوبات في الفصل السابع منه تحت مسمى جرائم الاعتداء على نظم المعالجة الآلية[1].

كما يجب أن يكون قد تم توجيه تهمة لشخص أو عدة أشخاص معينة بارتكاب جريمة أو المشاركة فيها من خلال قيام دلائل قوية وقرائن ضدهم تدعو للشك فيهم وفي البيئة المعلوماتية، وتشمل هذه الدلالات والقرائن في حاسوب معين تم تحديده، واتضح أنه ملك للمتهم أو ضبط في حوزته على معدات معلوماتية أو الجيزة أو مستندات الكترونية أو دعامات قد استخدمت في ارتكاب الجريمة أو حصلت منها تفيد في مسار التحقيق.

- **محل التفتيش:** يجب أن ينصب التفتيش في هذه الجرائم على نظام المعالجة الآلية للمعطيات بمكوناته المادية والافتراضية وشبكات الانترنت وكل ملحائها التقنية الأخرى[2].

- **السلطة المختصة في التفتيش:** لقد حدد المشرع الجزائري الجهة المختصة بالتفتيش بقاضي التحقيق، وفي بعض الحالات الاستثنائية يتكفل بإجراء التفتيش موظف

[1]- القانون 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات،. الجريدة الرسمية، عدد 71، السنة 41، الصادرة بتاريخ 10 نوفمبر 2004، وقد عززه المشرع الجزائري بالقانون 09-04 المؤرخ في 5 أوت 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، السنة 46، الصادرة بتاريخ 16 غشت سنة 2009.

[2]- رشيد بوكر، المرجع السابق، ص 408.

الضابطة العدلية وهذا إذا كانت الجريمة الإلكترونية متلبس بها من خلال رصد الجاني عبر شبكة الانترنت في حركة مريبة، ليتم ترصده عبر هذه الشبكة[1].

- **الإذن:** كقاعدة عامة يتم إجراء التفتيش من قبل المحقق المختص بذلك، لكن في حالات يتم تكليف ضابط من الضابطة العدلية، وفي هذه الحال حتى يباشر مهامه وجب حصوله على إذن بالتفتيش بالإنابة عن السلطة المختصة بذلك التي تمنحه له، ويجب أن يتضمن هذا الإذن مكان التفتيش والشخص والأشياء الأخرى كالأجهزة الآلية وبرامج الفيروسات والاختراق[2]، وقد نصت على ذلك المادة 44 من قانون الإجراءات الجزائية بقولها: يجب أن يعين الإذن بالتفتيش بيان وصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها..." [3].

وبالرجوع إلى نص المادة 47 فقرة 3 المذكورة سابقا يتبين أن المشرع الجزائري اشترط لقيام إجراءات التفتيش في الأماكن الخاصة الإذن من قاضي التحقيق، وأسقط الضمانات الأخرى المعمول بها في الجرائم التقليدية لان الاعتداء على نظم المعلوماتية لها طابع خاص، حيث أنها قد تظهر وتختفي في أقل من دقيقة وقد يكون الدليل التقني هو الدليل الوحيد الذي يقود الإثبات الجريمة[4].

2- تفتيش المكونات المادية لنظام المعالجة الآلية: تتمثل المكونات المادية لنظام المعالجة الآلية للمعلومات في ما يلي:

- **وحدات الإدخال:** مهمتها إدخال البيانات كلوحة التحكم

[1]- رشيد بوكر، المرجع السابق، ص 409.

[2]- المرجع نفسه، ص 410، 411.

[3]- أنظر المادة 44 من قانون الإجراءات الجزائية.

[4]- رشيدة بوكر، المرجع السابق، ص396.

- **وحدات إخراج:** مهمتها إخراج ما توصلت إليه العمليات الإلكترونية إلى شاشة العرض، ويتم إجراء التفتيش والبحث في محتواها بغرض ضبط أي دليل يقودهم لكشف الحقيقة"[1]، وذلك بعد أن تستوفي عملية التفتيش الشروط المذكورة أعلاه.

3- تفتيش المكونات المنوية لنظام المعالجة الآلية: وتشمل المكونات غير المادية للأجهزة الإلكترونية من برامج وتطبيقات، التي يتم التعامل بها داخل هذه الأجهزة وقد أجاز المشرع الجزائري تفتيش هذه المكونات ونص عليها صراحة من خلال القانون 09-04 بموجب المادة الخامسة منه بقولها: يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول بغرض تفتيش ولو عن بعد:

أ-منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظمة تخزين معلوماتية..."[2]

4- التفتيش عن بعد أن تكون الشبكة المعلوماتية من مجموعة من الأجهزة الإلكترونية: متصلة ببعضها البعض بطريقة سلكية أولا سلكية، ومع التطور التكنولوجي وظهور شبكة الانترنت أصبحت هذه الشبكات تمتد إلى كافة أنحاء العالم ولذلك فإن هذه الشبكات عند تفتيشها تكون بعيدة عن موقع التفتيش[3]، وفي هذه الحالة نميز بين حالتين:

أ- **اتصال جهاز المتهم بجهاز آخر داخل الدولة:** وقد نص المشرع الجزائري على ذلك في المادة 05 من القانون 09-04 في فقرتها الثانية والتي جاء فيها:" إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى،

---

[1]- فايز نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، مصر، 2012، ص131.

[2]- أنظر المادة 5 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[3]- رشيدة بوكر، المرجع السابق، ص 401، 402.

يجوز تمديد التفتيش إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك..."[1].

ب- اتصال جهاز المتهم بجهاز آخر خارج الدولة: أجاز المشرع الجزائري تفتيش الأنظمة المتصلة مع نظام المتهم ولوكان مكانها خارج الدولة وذلك في الفقرة الثالثة من نفس المادة السابقة الذكر، حيث جاء فيها: " إذا تبين أن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل "[2].

مما سبق نلاحظ أن المشرع الجزائري قد أجاز التفتيش في المنظومات البعدية بالنظر لكونه أسلوب يعتمده المجرمون الإعاقة التحري وكشف الأدلة.

ثالثا: الضبط

يهدف ضباط الشرطة القضائية من خلال القيام بالإجراءات السابقة إلى المعاينة والتفتيش عن أي شيء يقودهم لمعرفة حقيقة الجريمة ومرتكبها من خلال ضبط الأدلة الموجودة في مسرح الجريمة داخل البيئة المعلوماتية[3].

وقد نص المشرع الجزائري على هذا الإجراء من خلال القانون 09-04 في المادة 06 منه بقولها: " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات

[1]- أنظر المادة 5 فقرة 2 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[2]- أنظر المادة 5 فقرة من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[3]- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09- 04، مذكرة مقدمة النيل الشهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة قاصدي مرباح ورقلة، الجزائر، 2013، ص 94.

اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أجزاء وفقا للقواعد المقررة في قانون الإجراءات الجزائية "[1].

من خلال نص المادة يتضح أنه يتم ضبط كل شيء يفيد في اكتشاف الجريمة، وفيما يلي نبذة عن الأشياء التي يتم ضبطها في البيئة التقنية ،ضبط الأشياء المادية **(1)** ، ضبط البيانات الإلكترونية، **(2)**

1- ضبط الأشياء المادية: يساعد ضبط الأدلة المادية في إثبات جرائم الأجهزة الإلكترونية والتعرف على مرتكبيها ومن بينها[2]:

- **الورق:** يقوم الكثيرون من مستخدمي الحواسيب الآلية بالاعتماد على الورق في طباعة المعلومات لمراجعتها والتأكد منها وقت الحاجة، وبالنظر لأهميتها قد تكون موضوع للجريمة لذا وجب تفتيشها وضبطها سواء كانت أوراق أصلية يتم حفظها للاعتماد عليها أو أوراق ثانوية يتم تحضيرها مؤقتا ثم إهمالها.

- **الحاسب الآلي وملحقاته:** يتم ضبط جهاز الحاسب الآلي المستخدم في الجريمة بعد أن يقوم الخبير بتمييزه عن الأجهزة الأخرى، ومعرفة مواصفاته وتحديد ملحقاته.

- **أقراص الليزر:** تتواجد أقراص الليزر بكثرة في البنوك والمؤسسات المالية، حيث يقوم الخبير بتحليل محتواها لأنها قد تحوي على دليل يمكن من اكتشاف الجريمة ومرتكبها.

- **الشرائط الممغنطة:** تتمثل وظيفة هذه الشرائط في الحفظ الاحتياطي، ويتم حفظها في أماكن آمنة أوفي مراكز التوثيق المحمية كما قد يتم إيداعها في الخزائن الخاصة بالبنوك.

- **المودم:** هو الذي يوفر الانترنت للأجهزة المتصلة يبعضها البعض سواء عن طريق خطوط الهاتف أو لاسلكيا.

---

[1]- أنظر المادة 6 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[2]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص 56، 57.

- **بطاقات الدفع الإلكتروني:** يتم التحفظ على القديمة منها وكذلك ما تم استخدامه في تجهيز هذه البطاقات.

- **بطاقات (pcmcia):** ولها نفس شكل بطاقات الدفع، وتستعمل في الحواسيب الصغيرة.-نوت بوكواللابتوب-.

ويتم التحفظ على هذه المكونات المادية المذكورة كلها أو جزء منها للاستفادة من أي معلومة قد تفيد في مسار الكشف عن الجريمة[1].

2- ضبط البيانات الإلكترونية: فيما يخص البيانات الإلكترونية فهي من الأشياء غير المادية، وقد اختلف بشأنها الفقه وانقسم إلى اتجاهين كما يلي:

أ- الاتجاه المؤيد لقبولها محلا للضبط: يرى هذا الاتجاه بان البيانات الإلكترونية تصلح لأن تكون محلا للضبط، لكون هذه البيانات هي عبارة عن موجات كهرومغناطيسية وذبذبات معلوماتية صالحة للتخزين والحفظ والتسجيل عبر الأقراص والوسائط المادية الأخرى، فهي قابلة للنقل والبث والاستقبال وإعادة الإنتاج وبالتالي فهي من قبيل الأشياء المادية.

ب- الاتجاه الرافض لاعتبارها محلا للضبط: يرى هذا الاتجاه بأنها غير قابلة لأن تكون محلا للضبط، لأنها عبارة عن بيانات افتراضية ليس بها وجود مادي، ويمكن ضبطها في حالة واحدة فقط وهي إذا تم تحويلها إلى أشياء مادية ملموسة بواسطة التصوير الفوتوغرافي لها، أو نسخها على دعامة الكترونية مادية أو أي وسائط مادية أخرى[2].

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص56، 57.

[2]- صالح شنين، الحماية الجنائية للتجارة الإلكترونية-دراسة مقارنة-، رسالة لنيل شهادة الدكتوراه في القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2013، ص ص237، 238.

3- المحافظة على الأدلة المضبوطة: بعد إجراء ضبط الأدلة التقنية يتم تأمينها وتخزينها خوفا من إتلافها أو أي ضرر قد يلحقها، وبما أن هذه الأدلة ضمن البيئة التقنية تستلزم لتأمينها إجراءات خاصة، إلى جانب الإجراءات المتعارف عليها في الجرائم العادية وهي:

- منع الوصول إلى الأدلة المضبوطة من خلال تقيدها أو بالاعتماد على أي طريقة الكترونية أخرى، وقد نص المشرع الجزائري على هذا الإجراء في المادة السابعة من القانون 09-04 السالف الذكر.

- الاحتفاظ بالأقراص كما هي وعدم طيها لضمان عدم إتلافها.

- المحافظة على المعطيات الأصلية المخزنة في الدعائم الإلكترونية وعدم الاكتفاء بالنسخ.

- المحافظة على الأشرطة الممغنطة والأقراص بعيدا عن الحرارة العالية والرطوبة والالتزام بالدرجات المسموح بها[1].

رابعا: استجواب المشتبه بهم

ونقصد بذلك استجواب المتهمين وأخذ إفادة الشهود ومواجهة المتهمين بالأدلة التي تدينهم والعودة بهم عند الاقتضاء للمجال الذي تمت فيه الجريمة وفي ما يلي توضيح لهذه الإجراءات: استجواب المتهمين **(1)** ، الشهادة **(2)** ،

1- استجواب المتهمين: يعتبر الاستجواب من إجراءات التحقيق حيث يتولى قاضي التحقيق مهمة استجواب المتهم وفق ما يقتضه القانون، من خلال ما نص عليه المشرع في المواد 100-105 من قانون الإجراءات الجزائية باحترام كرامة المتهم ومنحه الفرصة للدفاع عن نفسه، وفي الجرائم المعلوماتية وحتى يضمن قاضي التحقيق أفضل النتائج وجب عليه ما يلي[2]:

---

[1]- رشيدة بوكر، المرجع السابق، ص 422.

[2]- حسين ربيعي، المرجع السابق، ص 225.

أ- **قبل الاستجواب:** يجب عليه قبل البدء في الاستجواب الاعتماد على خبير الكتروني حتى يعرف قاضي التحقيق الطريقة المناسبة الاستجواب كل مجرم على حدة حسب موضعه في الجريمة وكيف يوظف المصطلحات المناسبة عند الحوار.

ب- **عند البدء في الاستجواب:** حضور الخبير المعلوماتي أثناء جلسات الاستجواب وتدخله عند الحاجة إليه واستجواب المتهم وفق الإجراءات المقررة قانونا عند الانتهاء من عملية الاستجواب يتم تحرير محضر يتضمن كافة التفاصيل[1].

2- الشهادة: تعتبر إجراء من إجراءات التحقيق، وهي الأقوال الخاصة بالأشخاص غير الخصوم أمام الجهة المكلفة بالتحقيق ولها أهمية كبيرة في إثبات الجريمة، والمحقق هومن يملك صلاحية رفض الشهود من قبولهم متى رأى ذلك، والشاهد في الجرائم المعلوماتية ومن بينها الجرائم الواقعة على بطاقات الدفع الإلكتروني، يكون له خبرة في المجال التقني وكيفية الدخول إلى النظام المعلوماتي، وتقديم ما يلزم من معلومات لفائدة التحقيق القائمين على تشغيل الحواسيب، والمختصون في البرامج والنظم والتطبيقات وكذلك المسؤولون عن أعمال الصيانة، حيث يلتزم الشاهد بتقديم كل ما يحوز عليه من معلومات إلى سلطة التحقيق[2].

الفرع الثالث: مرحلة المحاكمة

بعد إتمام إجراءات التحري والتحقيق اللازمة وضبط الدليل المعلوماتي، تقوم النيابة العامة بتقديم نتائج التحقيق إلى المحكمة المختصة لإجراء المحاكمة، وبعد استقراء ومعالجة الأدلة يتقرر توقيع العقاب على الجناة من عدمه، ولأن الجرائم الإلكترونية تتسم بالطابع التقني وهي جريمة عابرة للقارات، فإن خطرها يمتد الكافة الدول فقد يرتكب الفعل الإجرامي في بلد ما وتقوم نتيجته في بلد آخر، وعليه وجب

[1]- حسين ربيعى، المرجع السابق، ص 225.

[2]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص61، 64.

على المشرع الجزائري تحديد المحكمة الجنائية المختصة بهذه الجرائم في مكان وقوعها، الاختصاص الجنائي الدولي **(أولا)**، الاختصاص الجنائي الوطني **(ثانيا)**.

أولا: الاختصاص الجنائي الدولي

في التشريع الجزائري يتم تحديد الاختصاص وفقا للاعتبارات التالية: مبدأ إقليمية القانون **(1)** ، مبدأ شخصية القانون **(2)** ، مبدأ العينية **(3)**.

1- مبدأ إقليمية القانون: ومن خلاله فإن كل الجرائم التي تقع على أرض الوطن يطبق عليها القانون الجزائري بغض النظر جنسية الضحية أو المجرم[1].

2- مبدأ شخصية القانون: وفقا لهذا المبدأ فإن كل جزائري قد يرتكب جريمة من الجرائم الإلكترونية، أو يكون الضحية جزائري فإنه يطبق عليها القانون الجزائري.

3- مبدأ العينية: يختص هذا المبدأ بالجرائم الإلكترونية الماسة بمصلحة الدولة سواء داخل الوطن أو خارجه، وسواء كان مرتكبها من الجزائر أو خارجها وقد نص المشرع الجزائري على ذلك بموجب المادة 588 من قانون الإجراءات الجزائية[2].

ثانيا: الاختصاص الجنائي الوطني

يتم تحديد الاختصاص على المستوى المحلي وفقا للمكان الذي ارتكبت فيه الجريمة، أو المحل السكني الأحد من المشتبه بهم في ارتكابها، أو المكان الذي تم فيه إيقافه فيه[3]، وفيما يخص الجرائم الإلكترونية فان المشرع الجزائري وبالرجوع لقانون الإجراءات الجزائية تجده وزع الاختصاص على النحو التالي: اختصاص النيابة العامة **(1)** ، اختصاص قاضي التحقيق **(2)**. اختصاص محاكم الجنح **(3)**.

1- اختصاص النيابة العامة: بالرجوع للمادة 37 فقرة 2 من قانون الإجراءات الجزائية، نجد أن المشرع الجزائري قد وسع من صلاحيات وكيل الجمهورية ومدد

[1]- صالح شنين، المرجع السابق ص ص 259، 260.

[2]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص ص 267، 268.

[3]- المرجع نفسه، ص 269.

اختصاصه إلى محاكم أخرى، تطيق حسب التنظيم مع مراعاة ضابط الشرطة لالتزاماته وفق المادة 40 مكرر 1 و2 من نفس القانون.

2- اختصاص قاضي التحقيق: كذلك تم تمديد صلاحيات قاضي التحقيق إلى المحاكم الأخرى، وذلك بموجب نص المادة 40 من القانون 04-14[1]، وطبق هذه الأجر امن بحسب التنظيم.

3- اختصاص محاكم الجنح: بالنسبة لاختصام محاكم الجنح في حالة قيام جريمة من جرائم المساس بالمعطيات فإن لمشرع الجزائري قام بتمديد اختصاصها إلى دوائر اختصاص محكم أخرى حسب نص المادة 329- 4 من القانون 04-14 وتطبق أيضا حسب التنظيم، وما يلاحظ على هذا الشديد بالنسبة لكل من النيابة العامة وقاضي التحقيق ومحاكم الجنح له محلي ولا يشمل الجرائم التي ترتكب خارج الدولة[2].

المطلب الثاني

القوانين الخاصة بالجرائم الإلكترونية والإجراءات المستحدثة

حتى يضمن المشرع الجزائري لحماية الجنائية والإجرائية اللازمة للمعاملات الإلكترونية، وبعد دراكه أن الإجراءات الاعتيادية وحدها لا تكفي بالرغم من تطويرها، بل يلزم قوانين وإجراءات جديدة خاصة بها الفلك فقد تدارك الأمر سواء على الصعيد الداخلي أو الخارجي، ولتسليط الضوء على مختلف هذه الإجراءات المتخذة فقد قمنا هذا المطلب إلى فرعين، خصصنا دراسة التطور التشريعي الحاصل فيهذا المجال **(الفرع الأول)** ، الاستعراض الإجراءات المستحدثة **(الفرع الثاني)**.

---

[1]- القانون 04-14 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم56/155 المؤرخ في 8 يونيو1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية الجمهورية الجزائرية، عند71، السنة 41، الصدرة بتاريخ 10 نوفمبر2004.

[2]- صالح شنين، المرجع السابق، ص ص 269، 270، 271.

الفرع الأول: التطور التشريعي

حتى يواكب المشرع الجزائري التطور الدولي الحاصل في مواجهة الجرائم المعلوماتية، اتجه لي استحداث نصوص إجرائية وعقابية للأفعال المكونة لهذه الجرائم والتي سلكت منعرجا خطيرا ومن بينها الجرائم الواقعة على بطاقات الدفع الإلكتروني، على المستوى الوطني **(أولا)**، على المستوى الدولي **(ثانيا)**.

أولا: على المستوى الوطني

(1) التشريعات المستحدثة، **(2)** الجهات المختصة بمكافحة الجرائم المعلوماتية،

1- التشريعات المستحدثة: ومن بين أهم هذه التشريعات نذكر ما يلي:

- القانون 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 والمتضمن قانون العقوبات، والغاية منه مكافحة الجرائم الإلكترونية بتجريم الأفعال المكونة لها، وكان ذلك بإضافة القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، من المادة 394 مكرر إلى غاية المادة مود 7 من هذا القانون[1].

- القانون 09-04 المؤرخ في 5 أوت 2009، والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام أو الاتصال ومكافحتها، ويهدف هذا القانون إلى وضع نصوص إجرائية تتناسب مع الجرائم الإلكترونية[2].

- القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية من خلال المواد التي تنظم الاختصاص النوعي والمحلي والإجراءات الخاصة بالتفتيش[3].

[1]- القانون 04-15، المصدر السابق.

[2]- القانون 09-04، المصدر السابق.

[3]- القانون 06-22، المصدر السابق.

- القانون 16-02 المؤرخ في 19 يونيو 2016، المتمم للأمر 66-156، جاء هذا القانون ليتمم المواد 87 مكرر 11 و87 مكرر 12 إضافة إلى المادة 394 مكرر 8 [1].

- المرسوم الرئاسي 15-261 المؤرخ في 8 أكتوبر 2015 إلى إنشاء الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

2- الجهات المختصة بمكافحة الجرائم المعلوماتية: وهي الهيئات المكلفة بمهام معينة للوقاية ومكافحة الجرائم المعلوماتية وهي كالآتي:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: نص عليها المشرع الجزائري في المادة 13 من القانون 09-04 وكان دخولها حيز النفاذ في سنة 2015 بموجب المرسوم الرئاسي 15-268، وعرفتها المادة 13 بأنها سلطة إدارية مستقلة معنويا وماليا، مقرها بالعاصمة، كما جاءت المادة 14 من القانون 09-04 والمادة 4 من المرسوم الرئاسي سابق الذكر لتحديد مهام اللجنة تحت إشراف السلطة القضائية والمتمثلة أساسا في تنشيط وتنسيق إجراءات الوقاية والمكافحة ومساعدة السلطات القضائية[3].

ب- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

تسعى مديرية الأمن الوطني لمكافحة كافة الجرائم ومن بينها الجرائم الإلكترونية، حيث تتولى نيابة مديرية الشرطة العلمية والتقنية التابعة لها مهمة التصدي للجرائم المعلوماتية، وتتواجد على المستوى الوطني في ثلاث مناطق وهي الجزائر وقسنطينة

[1]- القانون 16-02، المصدر السابق.

[2]- المرسوم الرئاسي 15-261 المؤرخ في 8 أكتوبر 2015، يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 53، السنة 52 الصادرة بتاريخ 8 أكتوبر 2015.

[3]- أنظر المواد 13و14 من القانون 09-04، المصدر السابق.

ووهران، إضافة إلى ثلاث وحدات أخرى طور الانجاز كل من ورقلة وبشار وتمنراست[1].

ج- وحدات الدرك الوطني على غرار مديرية الأمن الوطني: يسعى كذلك جهاز الدرك الوطني لمكافحة الجرائم المستحدثة وذلك بالاعتماد على مصالحه الآتية:

- قيادة الدرك الوطني، الوحدات الإقليمية، الوحدات المشكلة، الوحدات المتخصصة، وحدات الأسنان، هياكل التكوين، المعهد الوطني للأدلة وعلم الإجرام، المصلحة المركزية التحريات الجنائية، المصالح والمراكز العلمية والتقنية، حيث تسعي كل هذه المصالح إلى اكتشاف جميع الجرائم المرتكبة على الأجهزة الإلكترونية وعبر الانترنت[2].

ثانيا: على المستوى الدولي

مكافحة جرائم بطاقات الدفع الإلكتروني لا تقتصر على المستوى المحلي، بل تعداه ليشمل الصعيد العالمي نظرا لكونها جرائم عابرة للحدود مما يجعل مكافحتها أمر صعب بالنسبة لأي دولة بمفردها، لذلك تطلب الأمر تكاثف هود جميع الدول لمحاربة والحد من هذه الجرائم، والجزائر على غرار باقي الدول سعت إلى ذلك من خلال الانضمام والمصادقة على الاتفاقيات والمعاهدات الدولية سواء على الصعيد الأوروبي أو العربي[3]، اتفاقية بودابست **(1)** ، الاتفاقية العربية **(2)**.

1- اتفاقية بودابست: وكانت هذه الاتفاقية نتيجة جهود الاتحاد الأوروبي، حيث تعرف بالاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، وتم إقرارها في 21 نوفمبر 2001، ودخلت حيز التنفيذ بتاريخ 1 جويلية 2004 حيث تضمنت كل ما يتعلق بالجريمة الإلكترونية بما يساهم بشكل دائم ومستمر في تقديم المساعدة لكافة الدول في

[1]- ربيعي حسين، المرجع السابق، ص ص، 176، 177.

[2]- المرجع نفسه، ص ص182، 183.

[3]- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، مذكرة لنيل درجة الدكتوراه فريدة مزياني، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016، ص329.

هذا الشأن، وتهدف هذه الاتفاقية لتعزيز التعاون الدولي والشراكة في إيجاد أساليب مناسبة للكشف عن الجرائم التقنية ومعاقبة مرتكبيها، وقد نصت على صور الجرائم الماسة بالمعطيات من المادة 2 إلى المادة 13 منها، حيث قسمتها إلى خمس طوائف وجاء في طائفتها الثانية الجرائم المرتبطة بالحاسب الآلي كالتزوير والاحتيال المعلوماتي واللتان قد تكون الجرائم المرتكبة على بطاقات الدفع الإلكتروني محلا لهما[1].

2- الاتفاقية العربية: وهي اتفاقية ذات طابع عربي تم إقرارها في القاهرة بتاريخ 21 ديسمبر 2010، وتم التصديق عليها من أطرف الجزائر من خلال المرسوم الرئاسي 14-252 المؤرخ في 8 سبتمبر 2014[2]، وتضمنت هذه الاتفاقية خمس فصول رجاء مضمونها شبيه لحد كبير مع اتفاقية بودابست، حيث تناولت صور الجرائم الإلكترونية ونصت على جريمة تزوير بطاقات الدفع الإلكتروني في المادة 18 منها، كما تضمنت مختلف الأحكام الإجرائية في مواجهة هذه الجرائم وألزمت هذه الاتفاقية الدول الأعضاء مراعاة أحكام هذه الاتفاقية في التشريعات الداخلية، كما تعمل على تعزيز التعاون القانوني والفضائي بين الدول الأعضاء من خلال تبادل المعلومات ووضع قواعد للاختصاص وحل مشكلة التنازع[3].

الفرع الثاني: الإجراءات المستحدثة

إلى جانب الإجراءات التقليدية التي تطرقنا إليها سابقا فقد استحدث المشرع الجزائري إجراءات أخرى تواكب التقنية الحديثة لجمع الدليل التقني، ومن أهم هذه

[1]- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري المقارن، مذكرة مكملة لنيل شهادة الماجستير، زرقي رمضان، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر، 2012، ص ص101، 102.

[2]- مرسوم رئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية للجمهورية الجزائرية، عدد 75، السنة 51، الصادرة بتاريخ 28 سبتمبر 2014.

[3]- إلهام بن خليفة، المرجع السابق، ص ص 334، 335.

الآليات آلية التسرب وتسجل الأصوات واعتراض المراسلات والتقاط الصور، وستحاول التطرق لهذه الإجراءات كما يلي: عملية التسرب **(أولا)**، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور **(ثانيا)**.

أولا: عملية التسرب

نص عليه المشرع في القانون 06-22، حيث خصص له الفصل الخامس منه وعرفه في المادة 65 مكرر 12من قانون العقوبات بقولها: قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك"، ومن ضمن الجرائم التي أجاز فيها المشرع عملية التسرب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ومن خلال هذا التعريف يتبين أن التسرب هو اندماج ضابط الشرطة مع المجرمين ومشاركتهم نشاطهم وذلك بطريقة سرية إلى غاية تحقيق النتيجة المرجوة[1]، ولعملية التسريب شروط شكلية وأخرى موضوعية نوجزها كما يلي: الشروط الشكلية **(1)** ، الشروط الموضوعية **(2)** ، آثار التسرب **(3)**

1- الشروط الشكلية: يجب أن يكون صادر بإذن عن الجهة القضائية المختصة وأن يكون مكتوبا، كما يجب ذكر هوية الضابط الموكل إليه هذه العملية وتحدد مدته بأربعة أشهر مع جواز إيقافه من قبل القاضي الذي أذن به قبل استكمال مدته، ويجب كذلك الإبقاء عليه سري وحصر العلم به بين القاضي الأذن به والضابط الذي يقوم بالعملية، كذلك يجب أن يقوم العون المكلف به بتحرير تقرير مفصل على أوضاع القضية، كما تقتصر هذه العملية على ضبك وأعوان الشرطة القضائية لا غير، كل هذه الشروط نصت عليها المواد 65 مكررا إلى غاية 65 مكرر 15 من قانون الإجراءات الجزائية[2].

[1]- إلهام بن خليفة، المرجع السابق، ص 305.

[2]- مجراب الداودي، الأساليب الخاصة بالبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة بن يوسف بن خدة، الجزائر، 2016، ص ص 337، 341.

2- الشروط الموضوعية: وتتمثل في أن يكون التسرب مسيبا، بان يتضمن الإذن الخاص به الأسباب التي على أساسها تم القيام به، كذلك يجب تحديد نوع الجريمة محل التسرب حيث يجب أن تكون من الجرائم التي أجاز فيها المشرع هذه العملية، وقد نص عليها المشرع في المادة 65 مكررة من نفس القانون سالف الذكر.

3- آثار التسرب: نص عليها المشرع الجزائري في المواد 65 مكرر 14 و16 والمتمثلة فيما يلي:

- تسخير الوسائل المادية من مواد وأموال أو منتجات أو وثائق المجموعة المجرمين العامل معهم.

- استعمال أو صنع الوسائل ذات الطابع القانوني كالوثائق الرسمية أو المالية تحت تصرف هؤلاء المجرمين.

- سقوط المسؤولية الجزائية عن الأعوان المتسربون أثناء قيامهم بالأفعال السابقة الذكر لكونها أفعال قانونية.

- المحافظة على إبقاء عملية التسرب في سرية تامة لتحقيق نتائجها على أكمل وجه، ويتعرض لعقوبات كلمن خالف ذلك[1].

ثانيا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

(1) التعريف، **(2)** شروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

1- التعريف: لم يرد في القانون تعريف لهذا الإجراء، وقد عرف الفقهاء الاعتراض على أنه مراقبة وترصد المحادثات التي تتم بين الأفراد وحفظه، والعودة إليه كدليل في مرحلة الحث والتحري ضد المتهمين عند الحاجة إليه، كما أن تسجيل الأصوات في

[1]- إلهام بن خليفة، المرجع السابق، ص ص 307، 308.

عملية تتم أثناء التحديث الشفهي للأشخاص وذلك بتسجيل تلك المحادثات، أما التقاط الصور فهي توثيق تواجد الأشخاص فرادى أو جماعات في مكان ما دون علمهم[1].

وقد أجازها المشرع الجزائري في الجرائم الماسة بالمعطيات بموجب المادة 65 فقرة 5 من قانون الإجراءات الجزائية، ويختص للإذن بها وكيل الجمهورية الضباط الشرطة القضائية مع جواز إجرائها بطابع استثنائي بحسب ما نصت عليه المادة 47 من نفس القانون، حيث تتم في أي وقت وفي أي مكان سواء في مرحلة التحري أو التحقيق[2].

2- شروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

تناول المشرع الأحكام الخاصة لصحة هذا الإجراء في المواد 65 مكرر 5 إلى غاية المادة 65 مكرر 10[3]، ونستعرضها فيما يلي:

- يتم القيام بهذا الإجراء فقط بخصوص الجرائم التي ت عليه المادة 47 من نفس القانون، حيث تتم في أي وقت وفي أي مكان سواء في مرحلة التحري أو التحقيق حددها القانون ومن بينها الجرائم الماسة بالمعطيات.

- يتوجب للقيام بهذا الإجراء إذن من طرف وكيل الجمهورية أو قاضي التحقيق وتحت إشرافه في مرحلة التحقيق.

- يجب أن يكون هذا الإذن مكتوبا ويحتوي على كل متطلبات هذا الإجراء، مع إحاطتها بالسرية التامة.

- مدة هذا الإجراء 4 أشهر وإذا لزم الأمر يتم تجديده بنفس طريقة الإجراء الأول[4].

---

[1]- سامية بولافة ومبروك السياسي، "الأساليب المستخدمة في التحريات الجزائية" مجلة الباحث للدراسات الأكاديمية، العدد التاسع، دس، جامعة باتنة1، باتنة، جوان 2016، ص396.

[2]- معتوق عبد اللطيف، المرجع السابق، ص 106.

[3]- أنظر المواد من 65 مكرر 5 إلى غاية المادة 65 مكرر 10 من قانون الإجراءات الجزائية.

[4]- رشيدة بوكر، المرجع السابق، ص ص 442، 444.

يجوز للضابط المكلف بإجراء الاعتراض الاعتماد على من يرى فيه الكفاءة المطلوبة في المجال التقني حسب ما تقتضيه القضية، حيث يكون هذا الأخير عون مؤهل في هيئة عمومية أو خاصة تهتم بالمواصلات السلكية واللاسلكية[1].

– يقوم الضابط المكلف بإجراء الاعتراض بتحرير محضر يتضمن تفاصيل العملية بعد الانتهاء منها، مع ذكر تاريخ بدايتها ونهايتها وساعته.

– يقوم كذلك هذا الضابط بوصف أو نسخ المراسلات والصور والمحادثات المسجلة ضمن مهمته للاعتماد عليها كأدلة نحو كشف الحقيقة وتودع بالملف، وكذلك ترجمة كلماتها الأجنبية بمساعدة مترجم[2].

[1]– رشيدة بوكر، المرجع السابق، ص ص 442، 444.

[2]– إلهام بن خليفة، المرجع السابق، ص313.

الخاتمة

في نهاية الدراسة هذا الموضوع والتي نتناول الجرائم الواقعة على بطاقة الدفع الإلكتروني، نوجز أهم النتائج والتوصيات التي نوضحها كالآتي:

أولا: نتائج الدراسة

1-جرائم بطاقات الدفع الإلكتروني تدخل ضمن الجرائم المعلوماتية، والتي وليدة استخدام تقنية المعلوماتية وهي بتزايد باستخدام هذه التقنيات.

2-المجرم الإلكتروني أخطر من المجرم التقليدي لأنه صعب الكشف ولا تظهر عليه ملامح الاجرام باستخدام ذكائه وخبرته التقنية.

3-صعوبة الكشف عن هذه الجرائم وذلك لنظر لصيغتها الغير مادية، وقابلية البيانات للحذف والاتلاف بسهولة.

4-عدم التبليغ عن هذه الجرائم من قبل المؤسسات المالية حفاظاً على سمعته ودوام تقنية عملتها.

5-لمواجهة هذه الجرائم قام المشرع الجزائري بتعديل بعض القوانين مثال ما هو الحال بالنسبة للقانون 04-15 والذي عدل القانون 66-155 المتضمن قانون العقوبات تمس بالحياة الخاصة للأفراد فقد جعلها تخضع لشروط خاصة للقيام بها.

6-فرض المشرع الجزائري عقوبات على هذه الجرائم الماسة بالمعطيات وجعل لها حد أدنى وحد أقصى، لكنه نص على تجديد العقوبات كلما كانت هذه الجرائم ماسة بأمن الدولة كالدفاع الوطني أو المؤسسات الخاضعة للقانون العام.

7-المشرع الجزائري لم يدقق في ضبط المصطلحات حيث عمم مصطلح الجرائم الماسة بالنظم المعالجة الآلية للمعطيات على كافة الجرائم المعلوماتية دون التفصيل في هذه الجرائم.

8-وسع المشرع بموجب القانون 09-04 الاختصاص الإقليمي للجهات القضائية في متابعة الجرائم الماسة بالمصالح الحساسة في الدولة، حيث عالج هذا القانون مشكلة تنازع الاختصاص بين الدول حول جرائم التقنية نظرا لطبيعتها العابرة للحدود.

ثانيا: التوصيات

1-فأصل بأن سن المشرع الجزائري نصوص صريحة خاصةً ببطاقات الدفع الإلكتروني وعدم الاكتفاء بالنصوص التقليدية، ويجب تطوير هذه القوانين لمواكبة التطورات الحاصلة.

2-ضرورة البحث المستمر والكشف عن هذه الجرائم، قصد اتخاذ إجراءات تتناسب مع مستوياتهم التقنية العالية، تكون كفيلة بردعها.

3-تحديث إجراءات البحث والتحري وتظمينها في قانون خاص، والابتعاد عن دمجها مع الإجراءات التقليدية.

4-تدريب أفراد الجهات الأمنية المختصة في مكافحة هذه الجرائم بالشكل الدائم ما يتماشى ومستجدات التقنيات هذه الجرائم وتوفير أحدث الوسائل والتجهيزات التقنية لضمان تحقيق أفضل النتائج.

5-عقد المؤتمرات والندوات العلمية بصفة دورية للوقوف على أحداث مستجدات هذه الجرائم.

6-تعزيز التعاون الدولي ودعوى إلى الانضمام الجزائر للاتفاقيات والمعاهدات الأخرى التي تسعى لمكافحة هذه النوع من الجرائم.

مما سبق فقد حولنا في هذه الدراسة تناول موضوعاً حديثاً وهو الجرائم الواقعة على بطاقات الدفع الإلكتروني، والذي يعد من الموضوعات التي فرضت نفسها بقوة خلال الفترة الحالية، لكونه يمثل إفرازاً طبيعيا تولد عن التطور التكنولوجي والتقني الذي يشهد قطاع المعاملات المصرفية والمالية.

حيث سعى المشرع الجزائري إلى تعزيز الترسانة القانونية في مواجهة هذه الجرائم سواء بتعديل بعض القوانين السارية أو باستحداث قوانين أخرى تتماشى وتطور الرهيب لهذه الجرائم، ورغم المجهودات التي تقوم بها الجرائم سواء على الصعيد المحلي أو الدولي إلى أنها تحتاج إلى المزيد من الجهود سواء من الجانب التشريعي أو التقني للحد من الظاهرة.

قائمة المصادر والمراجع

أولا: الكتب

1- ابراهيم العيسوي، التجارة الإلكترونية، الطبعة الأولى، المكتبة الأكاديمية، مصر، 2003.

2- ابراهيم بختي، التجارة الإلكترونية، المفاهيم والاستراتيجيات التطبيقية في المؤسسات، ديوان المطبوعات الجامعية، الجزائر، 2005.

3- أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، الطبعة الثالثة، الديوان الوطني للأشغال التربوية، الجزائر،2001.

4- أحمد أبو الروس، قانون جرائم التزوير والتزييف والاختلاس المال العام من الوجهة القانونية والفنية، الموسوعة الجنائية الحديثة، المجلد الخامس، المكتب الجامعي الحديث، الاسكندرية، 1997.

5- أحمد سفر، أنظمة الدفع الإلكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008.

6- ايهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديد، مصر، دون طبعة، 2007.

7- بيارا ميل طوبيا، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، منشورات حلبي الحقوقية، دون طبعة، 2000.

8- جعفر حسين جاسم الطائي، جرائم تكنولوجية المعلوماتية رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البداية للنشر والتوزيع، عمان، 2010.

9- شريفي محمد نعام، محفظة النقود الإلكترونية، الرؤية المستقبلية، دار الجامعة الجديدة للنشر، مصر، دون طبعة، 2007.

10- عبد الرحمان ابن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، الحاسب الآلي وشبكة المعلومات الأنترانت، الطبعة الأولى، دار أبوراق للطباعة والنشر والتوزيع، 2004.

11- عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، طبعة الأولى، دار الحامل للنشر والتوزيع، عمان، 2013.

12- علي عدنان الفيل، إجراءات، التحقيق وجمع الأدلة والتحقيق في الجرائم المعلوماتية، دراسة مقارنة، دون طبعة، المكتبة الجامعية الحديثة، الموصل، 2012.

13- فتحي محمد أنور عزت، جرائم العصر الحديث، الطبعة الأولى، دار الفكر والقانون، القاهرة، 2010.

14- محمد أمين الرومي، التعاقد الإلكتروني عبر الأنترانت، الطبعة الأولى، دار المطبوعات الجامعية، الاسكندرية، 2004.

15- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، جرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2015.

16- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004.

17- محمد خليفة، الحماية الجنائية للمعطيات الحاسب الآلي، دار الجامعة الجديدة، دون طبعة، 2007.

18- محمد عبد الله الرشدان، جرائم غسل الأموال، الطبعة الأولى، دار قنديل للنشر والتوزيع، عمان، 2007.

19- محمد عبد الودود أبو عمو، المسؤولية الجزائية عن إفشاء السر المهني، الطبعة الأولى، دار وائل للنشر والطباعة، عمان، 1999.

20- محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2014.

21- محمود ابراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2014.

22- مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ماهيتها مكافحتها، دراسة مقارنة، دار الكتب القانونية، دون طبعة، 2005.

23- منير الجهيني، البنوك الإلكترونية، دار الفكر الجامعي، مصر، دون طبعة، 2006.

24- نادر شعبان ابراهيم السواج، النقود البلاستكية وأثر المعاملات الإلكترونية على المراجع الداخلية في البنوك التجارية، الدار الجامعية، دون طبعة، 2006.

25- نضال اسماعيل برهم، أحكام عقود التجارية والإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، دون طبعة، 2005.

26- نضال سليم براهيم، أحكام عقود التجارية الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2010.

27- وائل أنور بندق، موسوعة القانون الإلكتروني والتكنولوجيا الاتصالات، دار المطبوعات الجامعية، الاسكندرية، دون طبعة، 2007.

28- ناظم محمد نوري الشعري وعبد الفتاح زهير عبدالات، الصيرفة الإلكترونية، دار وائل للنشر، الأردن، 2008.

29- فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الأنترنت، دار الجامعة الجديدة للنشر، دون طبعة، 2002.

30- معادي أسعد صوالحة، بطاقة الإئتمان النظام القانوني وآليات الحماية الجنائية والأمنية (دراسة مقارنة)، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2011.

ثانيا: الأطروحات الرسائل والمذكرات

أ- الأطروحات والرسائل

1- حسن ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتي، أطروحة مقدمة لنيل شهادة الدكتوراه، رحاب شادية، قسم الحقوق، كلية الحقوق والعلوم السياسة، جامعة باتنة 1، 2016.

2- مجراب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة بن يوسف بن خدة، الجزائر، 2016.

ب- المذكرات

1- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، مذكرة لنيل درجة الدكتوراه فريدة مزياني، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016.

2- خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري ، مذكرة مكملة لنيل شهادة الماجستير في الحقوق، بن صغير محفوظ قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016.

ثالثا: المقالات

1- أيمن قديح، الدفع الإلكتروني من يحميه، مقال منشور في:

http:/analysées.net ,2006.

2- أمجاد حمدان الجهيني، الاستخدامات الغير مشروعة لبطاقة الدفع الإلكتروني من قبل الغير، مركز الدراسات القضائية، المملكة الأردنية الهاشمية، مقال منشور على موقع : www.coiss.com/replay.php.

3- محمد محرم محمد علي، جريمة النصب والتجارة الإلكترونية، مقال منشور على الموقع : www.f,law.net/law/index.php,2007

رابعا: النصوص القانونية

1- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتمم.

2- الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق لـ 26 سبتمبر سنة 1975 المتضمن القانون المدني المعدل والمتمم بالقانون رقم 07-05 المؤرخ في 13 مايو سنة 2007.

3- المرسوم التنفيذي رقم 2000-307 المؤرخ في 16 رجب عام 1421 الموافق لـ14 أكتوبر سنة 2000 يعدل المرسوم التنفيذي رقم 98 -257 المؤرخ في 3 جمادى الأول عام 1419 الموافق لـ 25 أوت سنة 1998 الذي يضبط شروط وكيفيات إقامة خدمات أنترانت واستغلالها.

4-القانون 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات،. الجريدة الرسمية، عدد 71، السنة 41، الصادرة بتاريخ 10 نوفمبر 2004، وقد عززه المشرع الجزائري بالقانون 09-04 المؤرخ في 5 أوت 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، السنة 46، الصادرة بتاريخ 16 غشت سنة 2009.

5- قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ5 أوت.

6- قانون رقم 90-10 المؤرخ في 14 أفريل 1990 المتعلق بالنقد والقرض الجريدة الرسمية العدد16 المؤرخ في 18 أفريل 1990 الملغى.

7- مرسوم تنفيذي رقم 05-448 المؤرخ في 12 شوال عام 1426 الموافق لـ 14 نوفمبر 2005 يحدد الحد المطبق على العمليات الدفع التي يجب أن تتم بوسائل الدفع وعن طريق القنوات البنكية والمالية، الجريدة الرسمية العدد 75، 20 نوفمبر 2005.

الفهرس

الشكر:.....

الإهداء:.....

مقدمة..... **01**

الفصل الأول: مفهوم الدفع الإلكتروني والاعتداءات الواقعة عليها

المبحث الأول: المقصود بالدفع الإلكتروني.....08

المطلب الأول: مفهوم الدفع الإلكتروني.....08

الفرع الأول: تعريف الدفع الإلكتروني.....09

الفرع الثاني: خصائص ا لدفع الإلكتروني.....12

المطلب الثاني: إساءة استخدام البطاقة من قبل صاحبها.....13

الفرع الأول: الحصول على بطاقة الدفع بطريقة غير شرعية.....13

الفرع الثاني: الاستخدام الغير شرعي للبطاقة في عملية السحب والوفاء.....15

المطلب الثالث: الاستخدام الغير الشرعي للبطاقة خارج فترة صلاحياتها.....19

الفرع الأول: الاستخدام الغير شرعي للبطاقة.....19

الفرع الثاني: الاستخدام المقنع للبطاقة.....27

المبحث الثاني: إساءة استخدام البطاقة من قبل المصدر والتاجر والغير.....29

المطلب الأول: الاستخدام الغير الشرعي للبطاقة من قبل المصدر والتاجر.....29

الفرع الأول: استخدام غير الشرعي من قبل المصدر..... 29

الفرع الثاني: الاستخدام الغير شرعي من قبل التاجر.....31

الفرع الثالث: المسؤولية موظفي البنك والتاجر عن الأعمال الغير شرعية.....33

المطلب الثاني: الاستخدام الغير الشرعي للبطاقة من قبل الغير.....40

الفرع الأول: جريمة التزوير واستعمال المزور.....40

الفرع الثاني: جريمة سرقة بطاقة الدفع أو رقمها السري.....46

الفرع الثالث: جريمة استعمال بطاقة الدفع المفقودة.....49

الفصل الثاني: الإجراءات المتخذة في مواجهة الاعتداءات الواقعة على بطاقة الدفع الإلكتروني

المبحث الأول: الإجراءات الوقائية.....54

المطلب الأول: دور الهيئات الدولية والبنوك في حماية بطاقة الدفع الإلكتروني.....54

الفرع الأول: الإجراءات الوقائية المتخذة من قبل الهيئات الدولية.....54

الفرع الثاني: الإجراءات الوقائية المتخذة من قبل البنوك.....54

المطلب الثاني: الإجراءات الوقائية المتخذة من قبل صاحب البطاقة والتاجر والجهاز الأمني.....65

الفرع الأول: الإجراءات الوقائية من قبل صاحب البطاقة.....65

الفرع الثاني: الإجرائية الوقائية المتخذة من قبل التاجر.....69

الفرع الثالث: الإجراءات الوقائية المتخذة من قبل الأجهزة الأمنية.....71

المبحث الثاني: الإجراءات الردعية.....74

المطلب الأول: الإجراءات الكلاسيكية البحث والتحري في الجرائم المستحدثة.....74

الفرع الأول: تلقي البلاغات.....75

الفرع الثاني: المعاينة والتفتيش والضبط.....81

الفرع الثالث: مرحلة المحاكمة.....91

المطلب الثاني: القوانين الخاصة بالجرائم الإلكترونية والإجراءات المستحدثة.....93

الفرع الأول: التطور التشريعي.....93

الفرع الثاني: الإجراءات المستحدثة.....97

الخاتمة:.....102

قائمة المراجع:.....105

الفهرس:.....111