وزارة التعليم العالي و البحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مكملة ضمن متطلبات نيل شهادة الماستر

تخصص قانون جنائي و علوم جنائية

بعنوان :

الجرائم الواقعة على بطاقات الائتمان

إعداد الطالب:
مرواني بوزكري

إشراف الدكتور:
نبيلة كردي

أعضاء لجنة المناقشة:

الإسم واللقب	الرتبة العلمية	الصفة في البحث
ربيعة فرحي	أستاذ محاضر قسم *أ*	رئيسا
نبيلة كردي	أستاذ محاضر قسم *أ*	مشرفا ومقررا
خديجة خالدي	أستاذ محاضر قسم *أ*	ممتحنا

السنة الجامعية: 2023/2022

وزارة التعليم العالي و البحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مكملة ضمن متطلبات نيل شهادة الماستر

تخصص قانون جنائي وعلوم جنائية

بعنوان :

الجرائم الواقعة على بطاقات الائتمان

إعداد الطالب:
مرواني بوزكري

إشراف الدكتور:
نبيلة كردي

أعضاء لجنة المناقشة:

الإسم واللقب	الرتبة العلمية	الصفة في البحث
ربيعة فرحي	أستاذ محاضر قسم *أ*	رئيسا
نبيلة كردي	أستاذ محاضر قسم *أ*	مشرفا ومقررا
شريفة خالدي	أستاذ محاضر قسم *أ*	ممتحنا

السنة الجامعية: 2023/2022

بسم الله الرحمن الرحيم

الكلية لا تتحمل أي مسؤولية على ما يرد في هذه المذكرة من آراء

الإهـــــداء

يطيب لي بعد أن يسر لي الله تعالى إتمام هذا العمل أن أهديه إلى

الوالدين الكريمين أطال الله في عمرهما ورزقهما الصحة والعافية

إخوتي وكل الاهل والاصدقاء

أساتذة وطلبة كلية الحقوق والعلوم السياسية بجامعة الشيخ العربي التبسي بتبسة

زملاء الدراسة إلى كل هؤلاء أهدي ثمرة هذا العمل المتواضع.

شكــر وعرفــان

أول الشكرلله الواحد القهار وصاحب الفضل والإكرام اكرمنا بنعمة الإسلام والعقل ويسر لنا سبيل العلم ربي فلك الشكر حتى ترضى ولك الشكر اذا رضيت ولك الشكر بعد الرضا والصلاة والسلام على الحبيب المصطفى صلى الله عليه وسلم تسليما كثيرا .

ثم كامل الشكر والتقدير والإمتنان للأستاذ المشرف الدكتورة نبيلة كردي على تفضلها بالإشراف على إعداد هذه المذكرة المتواضعة ، وعلى ما خصتنا به من وقت وجهد وتوجيهات قيمة .

الشكر الجزيل لكل أساتذة كلية الحقوق والعلوم السياسية والشكر الموصول لكل من ساهم من قريب أو من بعيد في إنجاز هذه المذكرة .

قائمة المختصرات:

ص : صفحة
ط : طبعة
د.ط : دون طبعة
د.س.ن : دون سنة نشر
ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري
ق.ع.ج : قانون العقوبات الجزائري
د.ن.م دون نوع مجلة
د. ق: دون قسم

مقدمـــة

مع ظهور ما يعرف بتكنولوجيا المعلومات نتيجة التطور التكنولوجي الذي شهده العالم في مجالات الحياة المختلفة ، حيث وفرت هذه التكنولوجيا إمكانية تحقق التواصل الإنساني و المعاملات في سهولة ويسر ما أدى للإختصار في الجهد والوقت.

امتدت آثار هذا التقدم التكنولوجي إلى ظهور عدة وسائل حديثة من و سائل الدفع الإلكترونية و لتسهيل المعاملات التجار ية للأفراد ومن بينها بطاقات الائتمان الإلكترونية، هذه الأخيرة التي تعتبر من مظاهر التطور التكنولوجي في الحياة التجارية الإلكترونية، نظرا لما تقدمه من خدمات و تسهيلات مصرفية عديدة لعملائها.

حيث عرفت إنتشار كبيرا وبصورة متسارعة ،لتحل محل النقود الحقيقية و في الشيكات في التداول اليومي بين أفراد المجتمع، لتصبح بذلك عماد العمل المصرفي ، وهو ما جعلها تحتل مكانة هامة وبارزة في الحياة الاقتصادية، سواء على المستوى المحلي أو الدولي .

لكن أمام هذه الايجابيات التي أتت بها بطاقات الإئتمان الإلكترونية، إلا انها لم تسلم من الجريمة فقد وقعت ضحية التصرفات غير المشروعة، فقد وقعت عليها السرقة و التزوير وتم إستخدامها عن طريق التحايل من اجل الإستيلاء على مال الغير، الأمر الذي يشكل تهديدا لحاملها من جهة و للاقتصاد المحلى و الدولى من جهة أخرى .

وما زاد من خطورة الجريمة طريقة عمل هذه البطاقات، بإعتبارها تعتمد في التعامل بها على النظام المعلوماتي ،الأمر الذي سهل على محترفي جرائم الحاسب الآلي الحصول على الأموال بطرق غير شرعية، وكل ذلك في إطار ما يعرف بالجريمة المعلوماتية .

وللموضوع أهمية بالغة علمية وعملية تبرز **أهمية** هذا الموضوع كونه يناقش موضوعا حساسا في الحياة اليومية كونه من الموضوعات المستحدثة التي لم تكن معروفة من قبل، و إنما أرتبط وجودها بظهور تكنولوجيا المعلومات والحاسبات الالية و التي تتصنف من بين الجرائم الخطيرة و ما يجعل منه ذو أهمية ميدانية نظرا لما لها من أثار

سلبية على المستوى الاقتصادي و الإجتماعي بشكل عام والحقوق و المصالح ذات الطابع المالي المتعلقة بالمؤسسات المالية و المصرفية بشكل خاص.

وقد **دفعنا لدراسة** موضوع الجرائم الواقعة على بطاقات الائتمان أسباب ذاتية تمثلت طبعا في كون الموضوع يدخل في الإختصاص الذي أدرسه والحاجة الملحة لمعرفة القوانين التي تضبط حرية إستعمال بطاقاتى الائتمان كونها أصبحت مستعملة وبقوة إضافة إلى معرفة الإجراءات المتبعة في مواجهة الجرائم التي قد تقع على هذه البطاقات وأسباب موضوعية تتمثل في أن الموضوع يمس الصالح العام والخاص لكون مستعملي هذه البطاقات في تزايد مستمر وأصبحت لصيقة بالحياة التجارية لكافة المجتمعات.

وتهدف هذه الدراسة للوصول إلى:

إعطاء تصور واضح وصريح للجرائم التي تقع على بطاقات الائتمان وتنوير مستعمليه على المخاطر و كيفيات التصرف في مواجهة الموضوع وما له من عواقب على سيرورة المعاملات المالية و الحياة التجارية ككل وكذلك تهدف إلى إنجاز بحث أكاديمي قد يساعد المشرع في سد الثغرات القانونية.

-الوقوف على ما إستحدثته ثورة المعلومات و الإتصالات من مفاهيم قانونية ومعرفة مدى مواكبة التشريع النافذ لتطور التكنولوجي الحاصل .

محاولة الربط بين هذا الموضوع و الشروحات القانونية و الفنية المفصلة لفقهاء قانون التجارة الدولية و الإلكترونية .

-محاولة خلع الصورة الذهنية المتخوفة لدى الأفراد بإقدامهم على إستعمال بطاقات الإئتمان الإلكترونية و الذي يتأتى بمعرفة المسؤولية الجزائية المترتبة عن الإستخدام غير المشروع

ومن هذا المنطلق تتبادر في أذهاننا **الإشكالية**الآتية:

- **كيف عالج المشرع الجزائري الجرائم الواقعة على بطاقات الائتمان و آليات مكافحتها؟**

يتفرع من هذه الإشكالية التساؤلات الفرعية التالية:

– في ما تتمثل الجرائم الواقعة على بطاقات الائتمان؟

– و ما هي الإجراءات التي إتبعها المشرع في مواجهة هذه الجرائم ؟

وللإجابة عن الإشكالية في بحثنا هذا اعتمدنا **المنهج** الوصفي الملائم من خلال إعطائنا تصور شامل حول موضوع الجرائم الواقعة على بطاقات الائتمان وذلك بإعطاء تعريفات للمصطلحات الغامضة التي تستدعي الوصف بالإضافة إلى المنهج التحليلي وذلك بتحليل بعض المواد القانونية والنصوص الفقهية.

وقد سبق وأن تطرق لهذا الموضوع عدة باحثين ومن **الدراسات السابقة** نذكر منها:

– واقد يوسف،النظام القانوني لدفع الإلكتروني، مذكرة ماجستير، تخصص قانون تعاون الدولي، جامعة مولود معمري تيزي وزو2011 .

حيث واجهنا **صعوبات** أثناء البحث في الموضوع تتمثل في:

–كون الموضوع يغلب عليه طابعه المدني على طابعه الجنائي .

– يعتبر موضوع غير متناول من جانب المشرع لغياب تشريع خاص بتنظيم بطاقات الإئتمان الإلكترونية.

وفي سبيل عرض هذا البحث في قالب منظم يؤدي الهدف المنوط به اعتمدنا **تقسيم الموضوع** إلى خطة ثنائية تتكون من فصلين:

بالنسبة للفصل الأول والذي جاء تحت عنوان ماهية الجرائم الواقعة على بطاقات الائتمان فقد تم تخصيص المبحث الأول إلى مفهوم بطاقات الائتمان أما المبحث الثاني تناولنا فيه الإستخدام غير المشروع لبطاقات الائتمان.

أما بالنسبة للفصل الثاني والذي جاء تحت عنوان الإطار الإجرائي للجرائم الواقعة على بطاقات الائتمان فقد تم التعرض فيه إلى الإجراءات الردعية في مواجهة الجرائم الواقعة على بطاقات الائتمان كمبحث أول أما المبحث الثاني فخصص للإجراءات الوقائية من هذه الجرئم .

.

الفصل الأول:

ماهية الجرائم الواقعة على بطاقات الائتمان

المبحث الأول: مفهوم بطاقات الائتمان.

المبحث الثاني: الإستخدام غير المشروع لبطاقات الائتمان.

مع التطور التكنولوجي الذي وصل إليه العالم اليوم وإنعكاسه على شتى المجالات كالمجال المصرفي، مطورت وسائل الدفع من تقليدية إلى إلكترونية ، و تعتبر بطاقات الإئتمان الإلكترونية إحدى وسائل الدفع الإلكترونية التي إنتشرت على مستوى العالم انتشارا واسعا، الأمر الذي أدى إلى إقبال الأفراد على التعامل بها، كبديل عن حمل النقود والشيكات، خاصة مع إدخال الحاسب الآلي في العمليات المصرفية، والتي تقوم غالبا على نظام التحويل الآلي للنقود .

وعلى الرغم من المزايا والمنافع التي توفرها هذه الوسيلة لتسهيل المعاملات المالية، فقد تم إستغلالها في العديد من التصرفات غير المشروعة، سواء من قبل حاملها، مصدرها، أومن القابل لها كما كان للغير النصيب في الاعتداء عليها.

لهذا سنخصص هذا الفصل لمعالجة هذا الموضوع وذلك من خلال مبحثين اولهما نتعرف فيه على مفهوم بطاقة الائتمان والمبحث الثاني سنعالج فيه الإستعمال غير المشروع لبطاقة الائتمان سواء بسوء إستعمال البطاقات أو بالإعتداء عليها.

المبحث الأول: مفهوم بطاقات الإئتمان

نتج عن التطور العلمي الذي شهده العالم في جميع المجالات علاقات كبير بين عدة علوم، وفي إطار العلاقة بين الأعمال المصرفيـــة و القانون الخاص والذي يؤطرها هذا الأخير من خلال القانون التجاري، والأعمال المصرفية لها دور حيوي كبير في المجال النشاط المالي، حيث تسدي خدمة كبيرة للأفراد وتساعدهم على المحافظة على أموالهم و منها إصدار بطاقات الائتمان التي تقوم بها المؤسسات المصرفية العالمية الموجودة في أمريكا و بريطانية و غيرها من دول العالم،التي تعتبر وسيلة ائتمان أكبر من الأوراق التجارية.

سنتناول هذا المبحث مفهوم بطاقات الائتمان، ونقسمه إلى مطلبين على التوالي المطلب الأول نتطرق فيه إلى تعريف بطاقة الائتمان ونشأتها وتطورها والمطلب الثاني إلى أنواع بطاقات الائتمان وخصائصها.

المطلب الأول: تعريف بطاقة الإئتمان ونشأتها

لابد من معرفة المقصود ببطاقة الائتمان أولا وإعطاء نبذة تاريخية حول هذه البطاقات وسيكون ذلك من خلال فرعين على التوالي أولهما تحت عنوان المقصود ببطاقات الائمان والثاني نشأة بطاقة الائتمان.

الفرع الأول: تعريف بطاقة الائتمان

تعر ف بطاقات الائتمان بمصطلحات متعددة منها بطاقات الدفع الإلكترونية، النقود الائتمانية، النقود البلاستيكية، بطاقات الوفاء الحديثة، بطاقات الائتمان الممغنطة، بطاقات الضمان، النقود الإلكترونية، الحافظة الإلكترونية، الكروت ذات القيمة المحفوظة والنقود البولمرية، ولكن أكثرها شيوعا هو مصطلح بطاقات الائتمان، و تختلف تعريفات

هذه البطاقات حسب الجانب الذي يتم تعريفها به، ولعل أبرز تلك التعريفات رّكزت على الجانب الشكلي، الوظيفي والقانوني لبطاقات الائتمان على النحو الآتي:

أولا: تعريف بطاقات الائتمان من حيث الشكل : تتفق جميع بطاقات الائتمان في الخواص الشكلية التي تتكون منها، فجميعها مصنوع من مادة كلوريد الفنيل غير المرن، ومدون عليها بيانات مرئية ملقنة ببيانات أخرى غير مرئية وجميعها تستخدم في وسط لإلكتروني.

وبالتالي يمكن تعريف بطاقات الائتمان من الناحية الشكلية على أنها بطاقات مستطيلة من البلاستيك تحمل اسم وشعار المؤسسة العالمية الراعية لها واسم البنك المصدر لها واسم ورقم حساب العميل، و أحيانا صورته وتاريخ انتهاء صلاحيتها، ومثبت على خلفيتها شريط مغناطيسي يحمل جميع البيانات المشفرة والخاصة بالبنك المصدر و بحامل البطاقة.[1]

ثانيا: تعريف بطاقات الائتمان من حيث الوظيفة: تعرف بطاقات الائتمان طبقا لوظيفتها على أّنها أداة مصرفية للوفاء بالالتزامات مقبولة على نطاق واسع محليا ودوليا لدى الأفراد والتجار والبنوك ، كبديل عن النقود لدفع قيمة السلع والخدمات المقدمة لحامل البطاقة مقابل توقيعه للتاجر على إيصال بقيمة التزامه الناشئ عن شرائه للسلعة أو الحصول على الخدمة، على أن يقوم التاجر بتحصيل قيمته من عند البنك المصدر للبطاقة الذي صرح له بقبول البطاقة كوسيلة للدفع، بحيث يطلق على عملية التسوية بين البنوك الأطراف فيها اسم نظام الدفع الإلكتروني، والذي تقوم بتنفيذه الهيئات الدولية الراعية لتلك البطاقات. و يعتريها جانب آخر من علم الحاسب الآلي على أّنها بطاقات

[1] معادي أسعد صوالحة , بطاقات الائتمان النظام القانوني وآليات الحماية الجنائية والأمنية ـدراسة مقارنةـ دار قباء الحديثة للطباعة والنشر والتوزيع, القاهرة 2007, ص38-40 .

مغطى سطحها بمادة قابلة للمغنطة يمكن تسجيل بيانات عليها، وبالتالي فإن وظيفتها في هذه الحالة هي تخزين البيانات[1].

ثالثا: تعريف بطاقات الائتمان من الناحية القانونية:

تقع بطاقات الائتمان من الناحية القانونية على أّنها عبارة عن عقد يتعهد بمقتضاه مصدر البطاقة بفتح اعتماد بمبلغ معين لمصلحة شخص آخر هو حامل البطاقة الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة بعقد تتعهد فيه بقبولها الوفاء بمشتريات حاملي البطاقات الصادرة عن الطرف الأول على أن تتم التسوية النهائية بعد كل مدة محددة .[2]

كما يدعم مجمع الفقه الإسلامي تعريف بطاقات الائتمان من وجهة نظر قانونية و يعرفها على أّنها مستند يعطيه مصدره (البنك أو غريه) لشخص اعتباري(حامل البطاقة) ، بناء على عقد بينهما يمكن هذا الأخير من شراء السلع والخدمات ممن يعتمد المستند(التاجر) دون دفع الثمن حالا لتضمنه التزام المصدر بالدفع، ويكون الدفع من حساب المصدر ثم يعود على حامل البطاقة في مواعيد دورية، بحيث تفرض بعض البطاقات الائتمانية فوائد على مجموع الرصيد المدفوع بعد م من تاريخ المطالبة وبعضها الآخر لا يفرض تلك الفوائد[3] .

انطلاقا من التعريفات أعلاه، وفي محاولة منا تقديم تعريف شامل لبطاقات الائتمان، يمكننا القول بأنها بطاقات خاصة تصدرها البنوك أو المؤسسات المالية أو حتى الشركات التجارية لشخص معين يعرف بحامل البطاقة، بحيث تتعهد الجهة المصدرة للبطاقة بسداد قيمة مشتريات حامل البطاقة من سلع و خدمات لدى التجار المعتمدين لديها، مقابل التزام حامل تلك البطاقة بالمبالغ المحددة لتعبئتها في الآجال المتفق عليها.

[1] المرجع نفسه, ص43-45.
[2] أيمن عبد الحفيظ, حماية بطاقات الدفع الإلكتروني, دار النهضة العربية للنشر والتوزيع, الأردن 2007,ص10.
[3] معادي أسعد صوالحة,المرجع السابق , ص45-46.

وقد أشار المشرع الجزائري إلى تعريف بطاقات الائتمان المتداولة في الجزائر والمعروفة ببطاقات السحب والدفع، وذلك في المادة 543 مكرر 23 من القانون التجاري، على أنه تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط في سحب الأموال، كما تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال[1].

وتدخل بطاقة الائتمان ضمن بطاقات الإلكترونية المختلفة التي كل منها تتميز بخصائص عن الأخرى فمنها بطاقات للسحب فقد ومنها بطاقات تمكن صاحبها أكثر من خدمة السحب حيث يمكن لبطاقة الائتمان أن تستعمل في حالات دون وجود رصيد بل يكفي وجود البطاقة التي تحمل إسم البنك المصدر حتى يتم إتمام الشراء أو الخدمة وذلك ما سنوضحه أكثر عند تناول أنواع بطاقات الائتمان لاحقا في هذا البحث.

الفرع الثاني: نشأة بطاقات الائتمان و تطورها

تعود نشأة بطاقات الائتمان إلى بداية القرن العشرين في الولايات المتحدة الأمريكية، حيث كانت المتاجر الكبرى والفنادق و وشركات البترول آنذاك هي أول من أصدر هذه البطاقات بهدف ضمان إخلاص عملائهم باستمرار تعاملهم معهم عن طريق منحهم تسهيلات في السداد من خلال تلك البطاقات[2] .

ثم بعد ذلك شهدت بطاقات الائتمان ركودا وكادت أن تتلاشى بسبب الظروف الاقتصادية التي مر بها العالم نتيجة الحربين العالميتين الأولى والثانية، لتعود بعدها بالظهور بقوة في العقد الذي تلا الحرب العالمية الثانية، وهو العقد الذي اخترع فيه أول جهاز حاسب آلي سنة 1946م. ومع انتشار استخدام الحاسب الآلي و الإنترنت في القطاع المصرفي خاصة، توسع استعمال بطاقات الائتمان أيضا، نظرا لكونها أداة دفع

[1] أنظر القانون التجاري الجزائري المادة 543 مكرر23, .
[2] باسم أحمد المبيضين,التجارة الإلكترونية , دار جليس الزمان للنشر والتوزيع, الأردن ,2010, ص126.

الكرتونية تقوم بتسوية المعاملات التجارية والبنكية بين الأفراد والبنوك طبقا لنظام التمويل الآلي للنقود[1] .

و أصبحت هناك شركات مختصة تقدم خدمات البطاقات الائتمانية مثل شركة فيزا وشركة ماستر الأمريكيتين، وذلك من خلال إصدارهما لبطاقات ائتمانية تعرف بالفيزا و االماستر كارد واللتان يتم استخدامهما بهدف تنظيم عملي دفع المالي الإلكتروني في العمليات التجارية كالبيع والشراء، حيث يميكن الحصول على هذه البطاقات الائتمانية عن طريق البنك و ليس من الشركة نفسها، والحصول عليها اختياري بمعنى أن الشخص الذي يريد الحصول على بطاقة الفيزا ا أو الماستر كارد عليه تقديم طلب في البنك الذي يريده، وبعدها تأتيه الموافقة أو الرفض من قبل شركة الفيزا أو شركة الماستر كارد بالحصول عليها، إذ تتعاون شركة الماستر كارد وشركة الفيزا مع البنك الذي يقدم البطاقة لتنظيم عملية سحب المال أو تحويله إلكترونيا[2].

أما في أوروبا فلم تظهر بطاقات الائتمان إلا مع بداية السبعينات من القرن العشرين، ففي فرنسا مثال، ظهرت أولى الموزعات الآلية للنقود سنة 1971م، في حين لم يتم التعامل بأجهزة الدفع الإلكتروني في المحلات والمتاجر الفرنسية إلا في عام 1980م. لكن التأخر الذي سجلته أوروبا في هذا المجال تداركته سريعا فيما بعد و أصدرت بنوكها ومؤسساتها المالية ما يقارب مليار بطاقة ائتمان في 30 سنة منذ بداية التعامل بتلك البطاقات، أي بمعدل 285 مليون بطاقة سنويا[3].

كما تأخر ظهور بطاقات الائتمان في دول العربية إلى غاية بداية التسعينات، ففي مصر مثال، بدأ التعامل ببطاقات الائتمان سنة 1990م، عندما قام بنك مصر بإصدار بطاقة ائتمانية أطلق عليها اسم "فيزا بنك مصر"، ثم إشترك هذا الأخير أيضا في

[1] معادي أسعد صوالحة, المرجع السابق , ص36.
[2] أنظر الموقع: http://mawdoo3.com/ آخر زيارة للموقع: 07/ 2023/06
[3] زهير طافرو الهاشمي بوترفاس, مداخلة بعنوان واقع بطاقات الائتمان في الجزائر, المركز الجامعي بشار, ص 03.

عضوية بطاقة ماستر كارد بإصدار فئة أخرى من بطاقات الائتمان تحت اسم "ماستر كارد بنك مصر."

كما سجل أول ظهور لبطاقة الائتمان في الأردن سنة 1992م، وذلك على إثر حصول الشركة الأردنية لخدمات الدفع على ترخيص من الشركة المصرفية الدولية لإصدار البطاقة المصرفية والماستر كارد[1].

والجدير بالذكر هنا أن الجزائر شهدت ظهور أولى بطاقات الائتمان سنة 1994م، وذلك بمبادرة من بنك الفلاحة والتنمية الريفية على شكل بطاقات سحب مقتصرة على بعض الوكالات الخاصة فقط، ثم بعدها قام ذات البنك سنة 1996م بإصدار بطاقة سحب "زيب–زاب" والتي كانت مخصصة لزبائنه الكبار فقط. كما شهدت سنة 1997م قيام شركة النقد الآلي والعلاقات التلقائية بين البنوك الجزائرية بإصدار بطاقات سحب لما بين البنوك تمكن حامليها من سحب أموالهم منّ أي موزع آلي داخل الجزائر[2] .

ولعل أهم حدث في هذا المجال هو القفزة النوعية التي عرفتها مجموعة من البنوك الجزائرية منذ سنة ،2008 حيث أصبحت تصدر بطاقات ائتمان تحت اسم الفيزا والماستر كارد مثل: بنك التنمية المحلية، البنك الوطني الجزائري، القرض الشعبي الجزائري، البنك الخارجي الجزائري، بنك الخليج بالجزائر، البنك الباريسي بالجزائر BNP (Paribas) ، سوسييتي جنرال الجزائر وترست بنك الجزائر[3] .

بالإضافة إلى إطلاق مؤسسة بريد الجزائر لبطاقةّ الدفع الإلكتروني الذهبية مع نهاية سنة 2016، والتي تسمح بإجراء مختلف معاملات حامليها من سحب ودفع للأموالّ على حساباتهم البريدية عرب الإنترنت وتسديد فواتيرهم الإستهلاكية الخاصة بالكهرباء والغاز والماء.

[1] أنظر الموقع: http://www.aladalacenter.com/index.php/2012-10-31-17-26-38/105-visacard3 تاريخ أخر إطلاع 2023/04/06.

[2] زهير طافر و الهاشمي بوترفاس, المرجع السابق ,ص08-09.

[3] أنظر الموقع:http://iqtissad.blogspot.com/2015/04/societe-generale-algerie-lance-la-carte-visa-classic-et-premier.html تاريخ أخر إطلاع 2023/06/07.

المطلب الثاني: خصائص بطاقات الائتمان و أنواعها

تعتبر بطاقات الائتمان وسيلة دفع إلكترونية بديلة للنقود إلا أن هذه البطاقات هي أنواع تختلف عن بعضها العض وكذلك لبطاقات الائتمان خصائص تتميز بها لهذا سنعالج في هذا المطلب في فرعين على التوالي أول فرع سنتناول خصائص بطاقات الائتمان وفي الفرع الثاني أنواع بطاقات الائتمان.

الفرع الأول: خصائص بطاقات الإئتمان الإلكترونية

لبطاقات الإئتمان الإلكترونية، العديد من الخصائص التي تميزها عن غيرها من وسائل الدفع والوفاء الأخرى ومنها :

أولا – البطاقة أداة إئتمان

إن مجرد الحصول على هذه البطاقة تعطي لحاملها التمتع بفترة ائتمان على مشترياته، والحصول على خدمات دون القيام بالدفع الفوري للنقود، وهذا ما لا تجده في أية وسيلة أخرى من وسائل الدفع التقليدية [1].

حيث تعتبر هذه البطاقة عبارة عن وسيلة تمتع صاحبها بالتبضع دون حمل النقود وفي نفس الوقت تمكنه من بعض الخدمات ما بع البيع بصفته كمتعامل مع البنك المصدر للبطاقة.

ثانيا – بطاقة الائتمان تقوم على علاقة ثلاثية الأطراف

تقوم بطاقة الائتمان على علاقة ثلاثية الأطراف (مصدر البطاقة، الحامل، التاجر) والتي تختلف باختلاف الأحكام عن بعضها البعض.

[1] عبد الكريم الردايدة، المرجع السابق، ص. 46.

فكل طرف من هذه الأطراف تترتب له حقوق وعليه إلتزامات، فهذه العلاقات هي:

أ- العلاقة بين البنك مصدر البطاقة ومستخدمها المدين .

ب – العلاقة بين المدين والتاجر .

جـ – العلاقة بين البنك والتاجر .

لذلك فبطاقة الائتمان الإلكترونية تعتبر ذات طبيعة مختلفة ولا تدخل تحت أي نوع من وسائل الوفاء التقليدية .[1]

وذلك أن في المعاملات التقليدية يكون التعامل حصرا بين المدين والتاجر فقط لكن في بطاقات الائتمان يدخل البنك كطرف ثالث في المعاملة وهو الوسيط أو أداة الربط بين الدائن والمدين.

ثالثا: صفة العالمية

تقوم المنظمات العالمية الراعية لإصدار البطاقات بإضفاء صفة العالمية عليها، في معظم أنحاء العالم، فضلا عن سياسة التوسع والانتشار في جميع دول العالم.[2]

ويكمن ذلك بإتاحة هذه البطاقة لصاحبها مكنة إستعمالها في نطاق أوسع من النطاق الإقليمي الموجود فيه، و يكون عن طريق إستعمال هذه البطاقة في المواقع التي تحمل طابع عالمي الذي وفرته التجارة الإلكترونية، التي سهلت التعاملات خارج الإقليم وإلغائها للحدود الجغرافية وكذلك عند التنقل خارج الإقليم يمكن إستعمال هذه البطاقات في الأماكن التي يكون فيها معترف لهذه البطاقات بالتداول.

رابعا : مصدر البطاقات

[1] كميت طالب البغدادي، الاستخدام غير المشروع لبطاقات الائتمان المسؤولية المدنية و الجزائية,ط1, دار الثقافة , الأردن 2008، ص. 69.
[2] كميت طالب البغدادي، المرجع نفسه، ص 70.

يتنوع مصدر البطاقات من المؤسسات المالية سواء أكانت بنوكا أم هيئات أم مؤسسات مالية[1].

فيمكن أن يكون إصدار بطاقات الائتمان من طرف البنوك ونكون هنا بصدد بطاقات الائتمان البنكية التي تحمل إسم البنك المصدر لها ويمكن كذلك لغيرها من المؤسسات المالية إصدار بطاقات الائتمان الخاصة بها ومثال ذلك مؤسة بريد الجزائر بإصدارها للبطاقة الذهبية .

خامسا: تشكل بطاقة الائتمان فائدة لجميع الأطراف

فالحامل يستطيع أن يقوم بشراء حاجياته ودفع ثمنها حسب ظروفه، والتاجر يستوفي ثمن بضاعته. وتحول إلى حسابه بالبنك المصدر للبطاقة دون عناء، كما أن الجهة المصدرة تحقق فائدة تتمثل في الحصول على عمولة من التاجر مقابل التعجيل بثمن المشتريات، وفائدة من العميل مقابل الائتمان الممنوح له .[2]

سادسا: عدم خضوع البطاقة للنظام القانوني الخاص بوسائل الدفع الأخرى

ومن أهم عوامل تطور المعاملات البنكية وحداثتها هو عدم خضوعها لتنظيم قانوني، يجعلها في قالب من الجمود يصعب عليها ملاحقة التطورات السريعة التي تشهدها البيئة التجارية، ومن هنا نستنتج التطور السريع لبطاقات الائتمان وتقديمها للعديد من الخدمات المميزة.[3]

الفرع الثاني: أنواع بطاقات الائتمان

تتنوع بطاقات الائتمان تبعا لعدة زوايا سواء من حيث مصدرها (أولا)، نطاق استخدامها أو وظائفها (ثانيا) أو حسب النظم التكوينية لها (ثالثا) .

[1] عبد الكريم الردايدة، المرجع السابق، ص 47.
[2] محمد توفيق سعودي، بطاقات الائتمان الأسس القانونية للعلاقات الناشئة عن استخدامها الطبعة الأولى، مصر، دار الأمين، 2009ص13.
[3] إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان ، د ط ، دار الجامعة الجديدة الإسكندرية ، 2007 ص20.

أولا – بطاقات الائتمان الإلكترونية من حيث مصدرها:

1. بطاقة الأمريكان أكسبرس: "هذه البطاقة تصدر ها مؤسسات تحمل اسمها من بنوك أمريكان اكسبرس، وهي عبارة عن مؤسسة مالية مركزها الولايات المتحدة الأمريكية وتصدر هذه المؤسسة من البطاقات البلاستيكية الالكترونية نوعين وكل نوع بحسب المزايا التي تمنحها لصاحبها".[1]

2. بطاقة الفيزا: هذه البطاقة تصدر ها مؤسسة لوس أنجلوس بولاية كاليفورنيا بالولايات المتحدة الأمريكية، وتصدر هذه المؤسسة من البطاقات البلاستيكية الالكترونية ثلاث أنواع وكل نوع بحسب المزايا التي تمنحها لصاحبها[2].

ثانيا – بطاقات الائتمان الإلكترونية من حيث مضمونها وعملها :

ولعل أهم تقسيم لهذه البطاقات هو الذي ينظر إليها من حيث كيفية الخصم أو التسديد حيث يتم تقسيمها إلى :

1. بطاقات سحب النقود: جميع بطاقات الائتمان تتمتع بوظيفة سحب النقود، إلا أن بعض أنواعها تقتصر على هذه الوظيفة فحسب، وقد تخول هذه البطاقة حاملها وظيفة سحب النقود داخل القطر الواحد، أو سحب النقود في الخارج، وذلك ضمن الحد الأقصى المحدد المسموح بسحبه يوميا أو أسبوعيا، ويسجل المبلغ المسحوب في الجانب المدين من حساب العميل مباشرة .[3]

---

[1] عبد الحكيم احمد محمد عثمان، أحكام البطاقات الائتمانية والآراء الفقهية الإسلامية، الطبعة الأولى، (مصر،دار الفكر الجامعي 2007، ص 147-149.

[2] بطاقة الأمريكان اكسبرس الخضراء: وتمنح لصغ ار أو متوسطي المدخول.
.بطاقة الأمريكان اكسبرس الذهبية: وتمنح للعملاء الذين يتمتعون .بكفاءة مالية عالية، وتتميز بكون تسهيلاتها الممنوحة للعميل غير محدودة بسقف ائتماني معين.
بطاقة الفيزا الفضية : وهي ذات حدود ائتمانية منخفضة نسبيا وتمنح لأغلب العملاء عند انطباق الحد الأدنى من المتطلبات عليهم، وتوفر هذه البطاقة جميع أنواع الخدمات المتوافرة من قبل منظمة الفيزا، كالسحب النقدي من البنوك أو أجهزة الصرف الآلي، أو الشراء من التجار ...إلخ .
-بطاقة الفيزا الذهبية: وهي ذات حدود ائتمانية عالية وتمنح للعملاء ذو الكفاءة المالية العالية .
–بطاقة فيزا الكترون: وتستخدم في أجهزة الصرف الآلي الدولية أو في أجهزة الطائرة للشريط المغناطيسي.

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية تطبيقية) الطبعة الأولى، (لبنان، دار المنشورات الحلبي، 2005) ص 509.

2. بطاقات الوفاء : تعد البطاقة أولا وقبل كل شيء وسيلة للوفاء موجهة للحصول محل للشيك، بخلاف بطاقة ضمان الشيكات، وتسمح بطاقة الوفاء للحامل بتنفيذ مشترياته من السلع والخدمات، لدى التجار المنضمين لنظام الوفاء بالبطاقات بدون وفاء فوري من جانبه، و إنما يكتفي بتقديم بطاقته فقط والتوقيع على الفاتورة المعدة لذلك أو ترك رقمه السري على مقرأه الخاص به كوسيلة للتحقق من شخصيته كحامل للبطاقة وتنقسم إلى نوعين:

بطاقات الاستيفاء الفوري: لا يستفيد الحامل فيها من مهلة الوفاء .

أما بطاقات الاستيفاء المؤجل تسمح للحامل بوفاء ثمن ما حصل عليه من سلع وخدمات[1].

3. بطاقات الائتمان : تتيح بطاقة الائتمان لصاحبها، استعمال ائتمان في حدود الإتفاق المبرم بينه وبين البنك المصدر، فهي تسمح لحاملها بدلا من تسوية حسابه فورا ، أن يقوم خلال أجل متفق عليه بتسديد ثمن مشترياته على دفعات، وذلك في حدود مبلغ مكشوف معين مسبقا . فهذه البطاقة تفترض أن حاملها مدين، إلا أنه في حاجة إلى الحصول على سلع وخدمات، يقوم البنك بتسويتها مع التاجر ثم يسترد ما دفعه بعد ذلك من حامل البطاقة.[2]

4. بطاقات ضمان الشيكات : تعد هذه البطاقة وسيلة لضمان حصول التاجر أو مقدم الخدمة على المقابل الذي تم تسويته عن طريق البنك، ومؤدي ذلك أن حامل هذه البطاقة يتعين عليه إبرازها مع الشيك، حيث يقوم التاجر بتدوين بياناتها الرئيسية غالبا على ظهر البطاقة، وبموجب ذلك يضمن الحصول على قيمة هذا الشيك من البنك مصدر البطاقة ، وقد أصدر هذا النوع من البطاقات كضمان للشيك وتقوية قبوله في

[1] عبد الحكيم أحمد محمد عثمان، المرجع السابق، ص 165.
[2] نائلة عادل محمد فريد قورة، المرجع السابق، ص -510 511.

التاجر و الفنادق، ولذلك لا تعد بطاقة وفاء ولكن وسيلة ضمان والدليل على ذلك أنها لا تستخدم بعيدا عن الشيك[1].

ثالثا – بطاقات الائتمان الإلكترونية حسب النظم التكوينية لها :

1. البطاقة الممغنطة : تحتوي هذه البطاقة على شريط ممغنط، يتم من خلاله إدخال وتخزين وتأمين البيانات عليه، ويكون ذا شيفرة تتميز بها. ويتحقق الدفع بهذه البطاقة من خلال قراءة المعلومات الثابتة على الشريط .[2]

2. البطاقة الرقائقية : تحتوي هذه البطاقة على شريحة من السيلكون، تتضمن قيد قيمة النقود في الحساب المصرفي لحاملها، وتقوم بعمليات التحويل المصرفي من خصم و إضافة من حسابات العميل بقيمة معاملاته[3] .

وهذه البطاقة ذات أنواع ثلاثة :

أ– **بطاقة الذاكــرة:** وهي التي لا تضمن سوى وسيلة ذاكرة لتخزين البيانات.[4]

ب– البطاقة الذكية: هذه البطاقة ذات تقنية عالية جدا، حيث تتضمن معالجا للبيانات والذاكرة لتخزين المعلومات، وتتميز بمواصفات أمان عالية يصعب استغلالها من قبل الآخرين، حيث لا يوجد لها رقم مطبوع، ولا توقيع ظاهر يمكن استغلاله في عمليات الاحتيال، وقد استبدل ذلك بشريحة إلكترونية صغيرة، تحتوي على كافة البيانات والمعلومات الشخصية.[5]

[1] عبد الكريم الردايدة, جرائم بطاقات الائتمان دراسة تطبيقية ميدانية, ط1 , دار حامد, الأردن, 2013, ص41.
[2] محمود الكيلاني، الموسوعة التجارية والمصرفية (، التشريعات التجارية والالكترونية)، الطبعة الأولى، (الأردن، دار الثقافة، 2009)، ص 465.
[3] محمود الكيلاني المرجع نفسه,ص465.
[4] حسين محمد الشبلي، مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولى (، الأردن، دار مجدلاوي، 2009) ص . 44
[5] عبد الكريم الردايدة, المرجع السابق ص43.

ج – البطاقة حادة الذكاء : وتعتبر هذه البطاقة مفرطا الذكاء، وتتضمن معالجا صغيرا للبيانات وذاكرة وشريطا ممغنطا وشاشة عرض، ومفاتيح إدخال البيانات.[1]

3. البطاقـة البصرية : وهي التي تحتوي على شريط ممغنط، وعلى عناصر تأمين بصرية مثل الصورة المجسمة ثلاثية الأبعاد، لحامل البطاقة، وهذه البطاقة توجد في ألمانيا وغير متداولة خارجها.[2]

[1] حسين محمد الشبلي، مهند فايز الدويكات، المرجع السابق، ص . 23
[2] حسين محمد الشبلي، مهند فايز الدويكات، نفس المرجع، ص. 24.

المبحث الثاني: الإستخدام غير المشروع لبطاقات الائتمان

مما لا شك فيه أن جرائم تكنولوجيا المعلومات باتت تشكل اليوم ظاهرة في المجتمعات الإنسانية، لا سيما مجتمع المعلومات العالمي . حيث أصبح المجتمع أمام مسؤولية جديدة تملي عليه معرفة أنواع وأنماط جرائم تكنولوجيا المعلومات محاولة لتجنبها ومكافحتها .

حيث أصبحت العديد من الدول تعاني من مشكلة الإستخدام غير المشروع لبطاقات الائتمان الإلكترونية، سواء من قبل حاملها أو من الغير.

لهذا خصصنا هذا المبحث لنتناول الإستخدام غير المشروع لهذه البطاقة من خلال مطلبين أولهما تحت عنوان إساءة إستعمال بطاقة الائتمان والثاني بعنوان الإعتداء على بطاقات الائتمان.

المطلب الأول: إساءة إستعمال بطاقات الائتمان

ما يميز بطاقات الائتمان عن الوسائل الدفع التقليدية أن هذه الأخيرة لها طرفين فقط، بينما بطاقة الائتمان لها ثلاث أطراف الحامل والتاجر والبنك، فإساءة استعمال الحامل والتاجر وموظفي البنك لبطاقة الائتمان يتعرضون لمسؤولية جنائية وتطبق عليهم عقوبات من طرف المحكمة.

الفرع الأول إساءة إستعمال بطاقة الائتمان من قبل صاحبها

لبطاقة الائتمان نفع لحاملها سوءا كان مستهلكا عاديا أو مستهلكا إلكترونيا عن طريق الحاسوب ، فيقتني بذلك السلع والخدمات المتوفرة عن طريق بطاقة الائتمان .

فعدم التزام حاملها بقوانين استعمالها الاستعمال الصحيح يتابع جزائيا، ويكون ذلك إما باستخدام بطاقة الائتمان عند انتهاء صلاحيتها وعدم إرجاعها إلى مصدرها أو عند إلغاءها من طرف هذا الأخير ، ومن جهة أخرى قد يقوم حاملها بسحب ما يزيد على رصيده أي أنه يسحب أكثر مما هو مصرح له به.[1]

أولا: الإستخدام غير المشروع لبطاقة الائتمان خلال فترة صلاحيتها

يتعسف حامل بطاقة الائتمان في استعمالها، رغم أنها صالحة للاستعمال، وذلك بتجاوز الرصيد الفعلي الموجود في البنك، حيث يتم السحب من الصراف الآلي أو الحصول على السلع والخدمات من طرف صاحب البطاقة من التاجر بمبلغ يتعدى السقف الذي حدده البنك.

وكذلك يمكن لحامل لبطاقة الائتمان، أن يستعملها استعمالا غير مشروع بتزوير مستنداتها رغم أنها صحيحة.

1. إساءة استعمال البطاقة بتجاوز حد السحب:

قد يتجاوز الحامل السحب مسموح به من طرف المصدر في حالتين:
سحب المبلغ من الصراف الآلي واقتناء السلع والاستفادة من الخدمات بتجاوز المبلغ الذي سقفه البنك أو السحب بما يجاوز الرصيد الفعلي أو الحصول على السلع والخدمات رغم عدم وجود رصيد كاف.

2. حصول حامل بطاقة الائتمان على بطاقة صحيحة بمستندات مزورة

يقصد بالتزوير سواء بطاقات كبطاقة الائتمان أو كتابات أو شهادات وغيرها بأنه "تحريف

[1] شيماء عبد الغني محمد عطا الله،الحماية الجنائية للتعاملات الإلكترونية،دار الجامعة الجديدة، ب ط،الإسكندرية مصر،2007ص150.

مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي ".[1]

ثانيا: الإستخدام غير المشروع لبطاقة الائتمان بعد إنتهاء صلاحيتها وكذلك في حال إلغائها:

بعد انتهاء مدة صلاحية بطاقة الائتمان يلتزم حاملها بإرجاعها إلى مصدرها "البنك"وهذا راجع إلى وجود عقد مكتوب بين حامل البطاقة والمصدر،وكذلك بعد إلغاءها كغلق الحساب، فتحتفظ البنوك المصدرة بحقها في إلغاء البطاقة الممنوحة للعميل في أي وقت ودون الرجوع إلى الحامل،وذلك ضمن شروط العقد المبرم بين البنك المصدر وحامل البطاقة، لذلك فكل مخالفة من الحامل لهذا الشرط العقدي يرتب مسؤولية في ذمته.[2]

1. الإستخدام غير المشروع لبطاقة الائتمان خلال فترة صلاحيتها وبعد إنتهاء صلاحيتها:

يمكن لحامل بطاقة الائتمان استعمالها استعمال غير مشروع ، وهذا بعد إنتهاء تاريخ صلاحيتها، وهنا اختلف فقهاء القانون في تكييفها على أنها جريمة أم لا و إن كانت كذلك تكون أي جرائم جريمة نصب أم خيانة أمانة.

رأت محكمة جنح بفرنسا أنها جريمة نصب وهذا أن العميل استعمل طرق احتيالية للحصول على المال،وذهب بعض الفقهاء أنها جريمة خيانة الأمانة لأن بطاقة الائتمان أمانة عند حاملها وعلى سبيل الوديعة ويجب ردها للمصدر عند انتهاء صلاحيتها.

ويرى أغلبية الفقهاء خاصة الفرنسيين أن الفعل الذي قام به العميل لا يشكل جريمة،وهذا للاعتبارات التالية:

-العمل هو عمل الإدراة هي التي تعرف انتهاء صلاحية البطاقة.

[1] نجيمي جمال، جرائم التزوير في قانون العقوبات الجزائري، دار هومة لنشر و التوزيع ط 2 الجزائر ،2014،ص268.

[2] واقد يوسف،النظام القانوني لدفع الإلكتروني، مذكرة ماجستير، تخصص قانون تعاون الدولي، جامعة مولود معمري تيزي وزو2011 د ص.

- أقرت محكمة النقض الفرنسية أن هذا الفعل لا يدخل في الأفعال المجرمة التي نص عليها قانون العقوبات بل يعد مجرد الإخلال بالتزام تعاقدي.
- إما كونها جريمة نصب فليست كذلك،لأن البطاقة بطاقته والحساب حسابه فكيف مؤاخذته على دخول حسابه، فهو لم يأتي بأية وسيلة تدليس.

وبالتالي ينتفي وصف جريمة عند استعمال البطاقة من قبل العميل رغم انتهاء صلاحيتها إذا قام بالتعامل بطرق الصحيحة، ولكنه فعله سيشكل جريمة بتلاعب بالبيانات والتحايل على البنك.

وفي الأخير تبقى السلطة التقديرية للقضاء، عند انتهاء صلاحية البطاقة واستعمالها من طرف الحامل، وذلك بمراقبة الحامل هل هو حسن النية أو سيئ النية.[1]

2. الإستخدام غير المشروع لبطاقة الائتمان رغم إلغائها:

قد يلغي البنك المصدر بطاقة الحامل لأي سبب من الأسباب كغلق الحساب أو تغيير نوعية الخدمة التي تؤديها البطاقة أو تغيير نظام التعامل، رغم هذا تظل البطاقة مع العميل و ربما يستخدمها بعد إلغاءها،وكذلك يمكن للبنك أن يقوم بإلغاء البطاقة والطلب من حاملها إعادتها في أي وقت يريد دون إعلامه أو دون إبداءه أي أسباب أو عدم إخطاره، وهذا الحق يتوافق مع ما جاء في القانون الجزائري ، حيث تنص المادة 120ق.م.ج بقولها:"يجوز الاتفاق على أن يعتبر العقد مفسوخا بحكم القانون،عند عدم الوفاء بالالتزامات الناشئة عنه بمجرد تحقيق الشروط المتفق عليها، وبدون حاجة إلى حكم قضائي ".[2]

عند استعمال العميل لبطاقة الائتمان بعد إلغاءها من طرف المصدر جريمة أم لا؟

[1] معادي أسعد صوالحة،المرجع السابق،ص283و284.

[2] الأمر رقم 58.75 المؤرخ في 1975/09/26 المتضمن للقانون المدني المعدل والمتمم.

هنا اختلف الفقهاء، فمنهم من يرى أنها جريمة نصب، حيث عند إلغاء البطاقة و قيام الحامل بشراء سلعة أو الاستفادة من خدمة من التاجر فيوهم الحامل التاجر بوجود رصيد في البنك هنا يكون قد نصب العميل على التاجر. وجانب من الفقه رأى أن الجريمة خيانة الأمانة .

الفرع الثاني:إساءة إستعمال بطاقة الائتمان من قبل التاجر وموظفي البنك

الاستخدام غير المشروع لبطاقة الائتمان،لا يكون إلا من الحامل فقط بل قد يكون كذلك التاجر وموظفي البنك لأن عمل بطاقة الائتمان تعتمد على ثلاث أطراف العميل و التاجر

والجهة المصدرة، قد يقوم التاجر بإساءة إستعمال البطاقة و بما أن البنك شخص معنوي، فإن موظفيه هم الذين يقومون بالاستخدامات الغير مشروعة.

أولا: إساءة إستعمال البطاقة من قبل التاجر:

يعتبر التاجر 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 العلاقة تعاقدية لبطاقة الدفع يدوية أو إلكترونية مع مستلزمات التشغيل الخاصة بها.[1]

حيث يقوم التاجر فيما بعد بتحصيل ثمن سندات البيع من المصدر المتعاقد معه 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

[1] أمجد حمدان الجهني، الاستخدامات الغير مشروعة لبطاقة الدفع الإلكتروني من قبل الغير، مركز الدراسات القضائية، المملكة الأردنية الهاشمية، مقال منشور على : .www.coiss.com/replay.php ، أخر زيارة بتاريخ 2023/06/07 على الساعة: 23:28 ص .148

بالاعتماد علي الأجهزة المسلمة له، وبذلك فأن مجال الإستعمال 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].

1. التجاوزات التي تتم بواسطة الأجهزة اليدوية :

شراء بعض التجار من بعض الأفراد لسندات بيع مطبوع عليها أرقام بطاقات صحيحة حتى ولو كانت بياناتها مزورة ، وبذلك تم تقليدها بواسطة بطاقات فعلية، ثم يقوم هؤلاء التجار بطباعة رقم بطاقته عليها وبذلك لتحصيل ما تم التعامل به من خلالها، مع أنهم لم يقوموا ببيع أو تأدية أية خدمات لأصحاب تلك البطاقات، هذا الفعل يمثل جريمة احتيال واستيلاء على أموال الغير وبدون وجه حق .[2]

قيام التاجر بطباعة بيانات بطاقة الدفع الخاصة بالعملاء لديهم علي سندات فارغة وبيعها لتجار أخرين للتعامل بها وتحصيل قيمتها بعد اخذ الموافقة 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.[3]

ادعاء التاجر بتعطل الجهاز الآلي الإلكتروني وبعد ذلك يقوم بكتابة ارقام موافقات وهمية علي السندات ليتمكن بعد ذلك من صرف قيمتها.[4]

2. 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.[1]

[1] أمجد حمدان الجهني، المرجع السابق، ص .148.
[2] وسام فيصل محمود الشواورة، المرجع السابق، ص. 88.
[3] أمجد حمدان الجهني، المرجع السابق، ص .148.
[4] عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والحاسب الآلي في القانون العربي نموذج، المرجع السابق، ص 584.

التلاعب بالماكنة الإلكترونية الخاصة بعمليات البيع ونظام تشغيلها، وبذلك يهدف بإستخدام بطاقات دفع تم التبليغ عن سرقتها أو ضياعها بعد أن تم العبث بنظام التشغيل الخاصة بها.[2]

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، ولم يتم 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.[3]

ثانيا:إساءة موظفي البنك لإستعمال بطاقات الائتمان:

الحدود التي تنظم عمل البنك لا تعطيه صلاحية الانحراف عن مهامه، حيث يعتبر الجهة المصدرة لبطاقة الدفع الإلكتروني وبما أنه شخص معنوي يقوم بأداء المهام عن طريق موظفيه فالاعتداء علي البطاقة يتم بواسطة موظفيها حيث يتم ذلك من خلال تواطؤهم مع صاحب البطاقة أو مع الغير.

1. تواطؤ موظفي البنك مع العميل:

قد يقوم موظفي البنك باستخراج بطاقة دفع الإلكتروني ببيانات مزورة، بحيث يتفق موظف البنك مع العميل وذلك باستخدام بطاقة كل أوارقها ومستنداتها ضرورية، أو يتم استخدامها لعميل ليس له وجود مع علمه بذلك حتي يستفيد هو وذلك العميل بالمبالغ

[1] وسام فيصل محمود الشواورة، المرجع السابق، ص .89.
[2] عبد الكريم الرديدة، المرجع السابق، ص. 65.
[3] أمجد حمدان الجهني، المرجع السابق، ص. 152.

التي تنطوي تحت رصيد البطاقة، وتكيف هذه الواقعة علي أنها جريمة للاستيلاء على أموال البنك دون وجه حق وتزوير للمستندات.[1]

2. 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 فيكون بذلك أمام جريمة التزوير.[2]

3. 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 لدى التجار، أومن خلال أجهزة الصرف الآلي .[3]

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.

المطلب الثاني :الإعتداء على بطاقة الإتمان

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

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

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

لقد أدى الإنتشار الواسع لإستخدام البطاقة الإئتمانية إلى استغلالها من طرف الغير . والتلاعب فيها من أجل إستيلاء على أموال ليست أمواله في الأصل[1] .

يتمثل هذا الإستخدام غير المشروع إما بالسرقة أو بالتزوير ، أو الإعتداء على نظام بطاقة الإئتمان الإلكتر ونية من خلال شبكة الإنترنيت .

وعليه سنحاول تحديد إساءة إستعمال بطاقة الإئتمان الإلكترونية التي ترتكب من قبل الغير كإعتداء على هذه الأخيرة وفقا لثلاث فروع على التوالي.

الفرع الأول :الإعتداء على بطاقة الائتمان بالسرقة

من الإعتداءات التي تقع على البطاقة الإئتمانية باعتبارها محل للحقوق مالية سرقة البطاقة عن طريق حاملها بصورة مباشرة، فالسارق سواء إستعمل البطاقة أو لم يستعملها، فهو يعد ارتكب لجريمة السرقة لمجرد توافر أركان هذه الجريمة [2] .

أما في الولايات المتحدة الأمريكية فإنها إعتبرت كل من يتعمد القيام بالإدخال الخاطئ للبيانات الائتمانية إلى أجهزة الكمبيوتر المرتبطة بالشبكات الداخلية أو العالمية ومحاولة التلاعب وتركيب الأرقام السرية لكشف حسابات صحيحة هي أفعال مجرمة تحت تشريع إحتيال بطاقات الإئتمان الفدرالي (CCFA) وبواسطة تشريعات الولايات المتحدة[3].

ويذكر أ ن الحامل الشرعي لبطاقة إ ئتمان ممغنطة يفقد صفته كحامل شرعي لهذه البطاقة منذ إبلاغ بسرقتها أو فقدها، وبالتالي المعارضة فيها لدى البنك المصدر لها .

[1] يقصد بالغير الشخص الأجنبي عن عقدي استخدام بطاقة الدفع الالكتروني، ولا ينصرف إليه شيء من آثار العقدين، أي لا يصبح دائنا ولا مدينا" أمجد حمدان الجهني، المرجع السابق، ص 155.

[2] -عبد الكريم الردايدة، المرجع السابق، ص 216 .

[33] محمد أمين الشوابكة، جرائم الحاسوب و الانترنت ' الطبعة الاولى ، ،دار الثقافة الاردن ،2004 ، ص 200.

ولذلك فهو يعد من الغير بالنسبة لها في حالة إساءة استعمالها ومن ناحية أخرى فإن التاجر قد يرتكب غشا بقبول البطاقة المسروقة أو المفقودة في الوفاء، وذلك بالتواطؤ مع الجاني، حيث يقوم التاجر بعمل فواتير وهمية لا تقابلها مشتريات حقيقية مستخدما في ذلك الطباعة اليدوية[1] .

أولا: الإستعمال غير المشروع لبطاقة مسروقة أو مفقودة لسحب النقود:

لا يمكن إستعمال بطاقة مسروقة أو مفقودة لسحب النقود من أجهزة السحب الآلي بدون إدخال الرقم السري أو الشفرة الخاصة بها، فبدون إدخال الرقم الصحيح لا يمكن لعملية السحب أن تتم بل أن إدخال رقم غير صحيح ثلاث مرات متتابعة من شأنه سحب البطاقة بواسطة الآلة. وتتعدد الوسائل التي يستطيع بها الجناة بمعرفة الشفرة الخاصة بالبطاقة من أجل القيام بسحب النقود من جهاز الصرف ويكون ذلك إما باللجوء إلى سرقة الشفرة أو استعمال طرق احتيالية.[2]

ثانيا: الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة كأداة وفاء:

يتم إستعمال بطاقة في هذه الحالة للوفاء بواسطتها لدى التجار حيث لا يقتضي الأمر معرفة الرقم السري للبطاقة بل تتم المعاملة بتوقيع حامل البطاقة على فاتورة البيع .

[3]

ويساهم في تسهيل إستعمال البطاقة على نحو كبير صعوبة تحقق التاجر من شخصية حامل البطاقة كما أن التحقق من أن البطاقة قد تم إيقافها لا يتحقق إلا بعد إطلاع على القائمة السوداء التي تحتوي على بيان للبطاقات الموقوفة والتي قد لا تكون

[11] عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الالكترونية (، الكتاب الثاني الحماية الجنائية لنظام التجارة الالكترونية)، الطبعة الأولى، (الاسكندرية، دار الفكر الجامعي، 2002) ص 336.

[2] نائلة عادل محمد فريد قورة، المرجع السابق، ص 540.

[3] ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى(مراكش المطبعة والوراقة الوطنية، 2011,ص 157.

البطاقة قد أدرجت بها ومن ناحية أخرى فإن مضاهاة التوقيع المدون على البطاقة بذلك الذي على فاتورة البيع لا يمكن من الناحية العملية إكتشاف تزويره لتدرب الجاني عليه ومن ناحية عدم خبرة البائع في هذا المجال.[1]

الفرع الثاني: تزوير البطاقة من قبل الغير

في بعض الأحيان تفقد البطاقة أو تسرق من العميل، ويلتقطها الغير حيث يقوم باستبدال ما بها من بيانات ومعلومات تمهيدا لاستخدامها في السحب أو الشراء وبذلك يشكل هذا الفعل إعتداء مزدوج على الحامل الذي فقدت منه البطاقة وعلى البنك معا، الأمر الذي عده جمهور الفقهاء جريمة تزوير[2] .

على أساس أن التزوير هو عبارة عن : " تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو إجتماعي ".[3]

إلا أن لهذا التزوير أساليب تستعمل على بطاقة الائتمان مباشرة أو على المستندات والإستعارات الخاصة بها .

أولا: أساليب تزوير بطاقات الإئتمان الإلكترونية :

أ. التزوير الكلي لبطاقات الائتمان: إن خطوات التزوير الكلي لبطاقة الدفع الإلكتروني، تتم بداية باصطناع البطاقة كاملة ثم تقليد الرسوم الخاصة على جسم البطاقة وتغليفها، ولصق الهولجرام، والشريط الممغنط أو الشريحة الرقائقية وشريط التوقيع، كل

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 540.
[2] عبد الكريم الردايدة، المرجع السابق، ص216.
[3] نضال سليم برهم، المرجع السابق، ص 158.

حسب موقعه الأصلي على جسم البطاقة، والقيام بالطباعة النافرة وتشغيلها عن طريق تغذيتها بالمعلومات التي حصل عليها المزورون من البطاقة الصحيحة .[1]

ومن الظواهر الدالة على التزوير الكلي للبطاقة :

. إختلاف مواصفات شكل وحجم البيانات المطبوعة طباعة بارزة بالبطاقة المصطنعة.

. عدم دقة لصق الشريط الممغنط وشريط التوقيع بظهر البطاقة حيث يمكن نزعها بسهولة .

. خلو البطاقة المصطنعة من التأمينات غير المرئية والسرية المميزة لنظيرتها الصحيحة.

. خلو البطاقة من الخواص المميزة للطباعة المجهرية نتيجة للنقص في الإمكانيات في آلات التصوير التجارية التي يستخدمها المزورون [2] .

ب – التزوير الجزئي لبطاقات الائتمان: يقوم المزور في هذه الحالة بالعديد من الأساليب لتزوير البطاقة جزئيا إما عن طريق صهر ما عليها من أرقام بارزة لبطاقة حقيقية إنتهت صلاحيتها، أو إعادة قولبة رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر، تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات مسروقة، كشط شريط التوقيع ووضع شريط آخر يتضمن توقيعه، أو أن يقوم بخلع صورة حامل البطاقة الحقيقي وتثبيت صورة شخص آخر[3] .

ومن الظواهر الدالة على التزوير الجزئي للبطاقة :

- ظهور بقع قاتمة أو بنية أو مصفرة اللون بأرضية شريط التوقيع نتيجة للمحو الكيماوي.

[1] أمجد حمدان الجهني، المرجع السابق، ص 157.
[2] حسين محمد الشبلي، مهند فايز الدويكات، المرجع السابق، ص 66.
[3] أمجد حمدان الجهني، المرجع السابق، ص 162.

- وجود تسلخات أو بقع مسودة في المواضع المحيطة بالكتابات النافرة أو عدم إنتظام الرؤوس البارزة للطباعة البارزة.

- الإختلاف في مواصفات التشكيل الطباعي لأرقام وحروف الطباعة البارزة .

- عدم التصاق حواف الصورة المجسمية ثلاثية الأبعاد .

-عدم التطابق بين البيانات المشفرة على الشريط الممغنط والبيانات المقروءة بصريا[1] .

ثانيا: تزوير الإشعارات والمستندات الخاصة ببطاقات الائتمان:

أ - تزوير الإشعارات: ويتمثل ذلك في عدة صور :

1-تلاعب موظف البنك المصدر للبطاقة بإشعارات بطاقة الائتمان :

كأن يتفق الموظف مع التاجر بتجاوز حد السحب في صرف قيمة إشعارات البيع من بطاقة مزورة أو منتهية الصلاحية، أو أن يختلس موظف البنك مبالغ نقدية عندما يقوم حامل البطاقة بسحب أو الإيداع فيقوم بتزوير المبلغ ويأخذ الفارق لنفسه .

2-تزوير الإشعارات والفواتير الناتجة عن عملية البيع: تحصل في الغالب مع كبار السن بمغافلة التاجر له فيحصل على بصمته على إشعار خالي من البيانات ثم يقوم بتعبئته بالمبلغ الذي يريد أو يقوم بتزوير مبالغ الإشعارات.

3-تلاعب التاجر في ماكينات البيع الإلكترونية: كأن يستغل التاجر الماكينة اليدوية في الحصول على أكثر من إشعار دون علم صاحب البطاقة بحيث يقلد توقيع حامل البطاقة على تلك الإشعارات ليتم تحصيل قيمتها بعد ذلك من البنك.

[1] حسين محمد الشبلي، مهند فايز الدويكات، المرجع السابق، ص 66.

ب- إصدار بطاقات صحيحة بمستندات مزورة : يقوم المحتالون بالإستعانة بمستندات إثبات شخصية مزورة للحصول على بطاقات بأسماء منتحلة وعناوين وهمية. وعادة ما يلجأ محترفو هذا النوع من الجرائم إلى استهداف أكثر من بنك لإصدار عدة بطاقات لتحقيق أكبر عائد ممكن مستغلين ضعف وخبرة بعض موظفي البنك في كشف تزوير المستندات والوثائق[1] .

الفرع الثاني :الإعتداء على نظام بطاقة الائتمان من خلال شبكة الإنترنيت

تقوم عملية الدفع الإلكتروني من خلال شبكة الإنترنت،بعد أن يدخل العميل عن طريق تلك الشبكة التي تعرض منتجاتها، فيرغب في الشراء ويقوم بملئ نموذج مطبوع على أعلى صفحة الويب تلك، ويدون به بيانات البطاقة وكمورد السلعة التي يرغب في شرائها والعنوان الذي ترسل إليه، ويسمى هذا النوع من الشراء التجارة الإلكترونية [2] .

إلا أنه في بعض الأحيان يحدث تلاعب من مستخدمي هذه الشبكة، أي قراصنة الإنترنيت[3].

وبعد حصولهم على البيانات الخاصة بالبطاقات بأساليب إحتيالية، لدراستهم ومعرفتهم الفنية بأنظمة الاتصالات والمعلومات، يقومون باستخدام أرقام هذه البطاقات الإئتمانية للحصول على السلع والخدمات، ويستخدمون في ذلك عدة أساليب نذكر منها:

-أسلوب الخداع: عن طريق إنشاء مواقع وهمية على شبكة الإنترنيت، بحيث يظهر الموقع الاصطناعي وكأنه الموقع الأصلي لإحدى الشركات الكبرى، وتبدأ العملية بقيام

[1] حسين محمد الشبلي، مهند فايز الدويكات، المرجع السابق، ص 70,
[2] إيهاب فوزي السقا، المرجع السابق، ص 202.
[3] عبد الكريم الردايدة، المرجع السابق، ص.

الموقع الوهمي باستقبال تعاملات الموقع الأصلي، وبعد حصوله على الأموال يتم إغلاقه .[1]

-أسلوب التجسس : حيث يقوم قراصنة الإنترنيت باستخدام البرامج التي تتيح لهم الإطلاع على البيانات والمعلومات الخاصة بالشركات التجارية الكبرى للحصول على أرقام بطاقات الائتمان ويعاد استخدامها بطريقة غير مشروعة[2] .

-أسلوب تفجير الموقع المستهدف : بتزويد الحاسب بمعلومات فوق طاقته التخزينية، الأمر الذي يؤدي إلى تبعثر البيانات والمخزنة تنتقل إلى الجهاز الخاص بالفاعل، وترتكب هذه الطريقة د الإجرامية على مواقع المؤسسات المالية والفنادق والشركات[3] .

-أسلوب الإيهام : هو أن يقوم القراصنة من أجل الحصول على بيانات ومعلومات للأشخاص مع أرقام بطاقاتهم الائتمانية، بإرسال رسائل إلى زبائن أحد المواقع الالكترونية، بحجة أن الموقع بحالة تحديث يرغبون بالحصول على كل المعلومات من أجل التحديث، وبعد ذلك يقوم المجرمون باستخدام تلك الأرقام في الشراء عبر شبكة الإنترنيت[4].

من خلال ما سبق فإنه يمكن تكييف الطرق السابقة للاستيلاء على أرقام البطاقات الائتمانية ضمن الأفعال الماسة بنظام المعالجة الآلية للمعطيات، حيث نجد أن المشرع الجزائري قد جرم هذه الأفعال بموجب القسم 7مكرر من قانون العقوبات الجزائري في المواد من 394 مكرر إلى 394 مكرر 7 حيث جاء في نص المادة 394 مكرر 2 بأنه " يعاقب بالحبس من شهرين إلى ثالث سنوات وبغرامة من 1.000.000دج إلى 5.000.000 دج.[5]

[1] ضياء علي أحمد نعمان، لا مرجع السابق، ص 245.
[2] عبد الكريم الردايدة، المرجع السابق، ص . 70.
[3] ضياء علي أحمد نعمان، لا مرجع السابق، ص 245.
[4] عبد الكريم الردايدة، المرجع السابق، ص 70.
[5] العروسي حاقة , المرجع السابق , ص265.

الفصل الثاني:

الإطار الإجرائي لجرائم الواقعة على بطاقات الائتمان

المبحث الأول: الإجراءات الردعية في مواجهة الجرائم الواقعة على بطاقات الائتمان

المبحث الثاني: الإجراءات الوقائية في مواجهة الجرائم الواقعة على بطاقات الائتمان

تتسم الجرائم الواقعة على بطاقات الائتمان بالخطورة على الحياة التجارية و عرقلتها لسيرورة المعاملات التجارية التي مسها التطور الحاصل في شتى المجالات والتي مكنت المجرمين من إستعمال هذه التكنولوجيا في المجال الإجرامي ما أكسب هذه الجرائم صفة الحداثة.

فهي تفتقد إلى قوانين خاصة بها تكون كفيلة بالحد من وقوعها، وذلك ما دفع إلى اتخاذ إجراءات خاصة على المستوى المحلي من خلال تبني إجراءات لحماية أطراف العلاقة التعاقدية والمحافظة على الثقة في تعاملاتهم، وكذلك على مستوى الأجهزة الأمنية المختصة في مكافحة هذه الجرائم، ومن جهة آخرة وعلى الصعيد الدولي تم تفعيل آليات كفيلة بمحاربة هذه الجرائم ومتابعة مرتكبيها .

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

المبحث الأول: الإجراءات الردعية في مواجهة الجرائم الواقعة على بطاقات الائتمان

لخطورة الجرائم الواقعة على بطاقات الائتمان وتناميها بشكل ملحوظ، عمل المشرع على تطوير الإجراءات الكلاسيكية الخاصة بالبحث والتحري عن الجرائم بما يتماشى مع هذه الجرائم المستحدثة من خلال تعديل القوانين القديمة، كما عمل على وضع مشاريع قوانين جديدة لمواجهة هذه الجرائم، كما تم أيضا المصادقة على الاتفاقيات والمعاهدات الدولية التي تختص بهذا الشأن.

ولدراسة مختلف هذه الإجراءات سنعالج في هذا المبحث المقسم إلى مطلبان، نعرج على الإجراءات المتخذة من قبل المشرع الجزائري بغية تطوير الإجراءات المعتادة في البحث والتحري والمحاكمة بما يتماشى مع الجرائم الإلكترونية من خلال المطلب الأول، في حين خصصنا المطلب الثاني لدراسة الإجراءات والقوانين المستحدثة وما مدى مساهمة الجزائر في محاربة هذه الجرائم على الصعيد الدولي.

المطلب الأول: الإجراءات الكلاسيكية للبحث والتحري في الجرائم المستحدثة

تقوم الشرطة الفضائية بالبحث والتحري حتى يتم الكشف عن الجرائم وضبط الدلائل المؤدية إليها و ومتابعة مرتكبيها 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 الحداثة و الخبرة التقنية حيث يكون أفراد الشرطة على علم بهذه الإجراءات من جهة، ومن جهة أخرى تكون لهم خبرة في مجال المعلوماتية و الأجهزة التقنية، فقد قسمنا هذا المطلب إلى ثلاثة فروع، خصصنا

لمرحلة تلقي البلاغات وكيفية التعامل معها ضمن الفرع الأول ثم دراسة المعاينة والتفتيش والضبط في الفرع الثاني، في الفرع الثالث نتناول ذلك في مرحلة المحاكمة.

الفرع الأول: تلقي البلاغات من قبل السلطات المخولة قانونا

لخصوصية الجرائم الإلكترونية يختلف التبليغ في هذه الجرائم 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[1] .

وبعد التبليغ عن الجريمة أو الاشتباه بها يقوم أفراد الضبطية القضائية بالتحري وا إستراتيجية لبدء العمل واختيار الضباط الذين تتوفر فيهم الخبرة المعلوماتية ٍ عداد لتسهيل الكشف المبكر عن الجريمة ومرتكبيها.

أولا: تلقي البلاغات والشكاوي :

لتعرف على المقصود بآلية التبليغ، و كيفية إستعمال هذه الآلية .

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

[1] حسين ربيعى، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1 ،،2016 ص .213.

إلى سرعة تحرك الشرطة القضائية باعتبارها الجهة المختصة في الكشف عن الجرائم و التصدي لها.[1]

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.[2]

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 و إجراء التحقيقات الابتدائية.[3]

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 :، الوطني للأمن www.mdn.ppgn.dz، وكذلك الموقع الإلكتروني: www.dgsn.dz لكن هذه المواقع ليست ملزمة للمبلغين حيث لهم الحرية في إتباع هذه الطرق المستحدثة أو الكلية بالطرق العادية ، 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] حسين ربيعي , المرجع السابق, ص215.
[2] علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية -دراسة مقارنة-، دون طبعة، المكتب الجامعي الحديث، الموصل، ،2012 ص.11.
[3] نظر المادة 17 من القانون 22-06 المؤرخ في 20 ديسمبر ،2006 المعدل والمتمم للأمر 155-66 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد ،84 السنة ،43 الصادرة بتاريخ 24ديسمبر سنة .2006.
[4] حسين ربيعي, المرجع السابق,ص218.

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 ، تشكيل فريق عمل ، الخبرة .

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 الأتي ذكرهم:

[1] علي عدنان الفيل, المرجع السابق, ص16.
[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.[2]

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.[3]

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.[4]

خبير البصمات: ومهمته رفع البصمات خاصة تلك المرتبطة بالأجهزة المادية للحاسوب المتضرر، والتي تم استخدامها في الجريمة.[5]

الخبير الاستشاري: ويوضح وقائع الجريمة ويزيل الغموض عنها.[6]

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

[1] علي عدنان الفيل, المرجع السابق ,ص17.
[2] المرجع نفسه ص17.
[3] حسين ربيعي, المرجع السابق, ص221.
[4] المرجع نفسه 221.
[5] المرجع نفسه ص221.
[6] علي عدنان الفيل, المرجع السابق, ص19.

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 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.[2]

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, المرجع السابق, ص19.
[2] المرجع نفسه 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 gold pro xtree : ويتم معالجة الملفات بواسطته والعثور عليها داخل الشبكة أو القرص الصلب.

برنامج link lap : 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 704، 705.

[2] حسام محمد نبيل الشنراقى، جرائم الاعتداء على التوقيع الالكتروني، دون طبعة، دار الكتب القانونية، مصر، ، 2013ص.690.

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]

ثانيا: التفتيش في المجال المعلوماتي

[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 718 .

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 المعنوية 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.[2]

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

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 جاء به

[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] محمود إبراهيم غازي، المرجع السابق، ص 721.

القانون ،22-06 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:

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

[1] أنظر المادة 45 من قانون الإجراءات الجزائية الجزائري.
[2] أنظر المادة 47 من قانون الإجراءات الجزائية الجزائري.
[3] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص.418.

للمعطيات، وقد حدد المشرع الجزائري مجموعة الحر الم الماسة ينظم المعطيات في القانون 15-04 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 الضابطة العدلية وهذا إذا كانت الجريمة الإلكترونية متلبس بها من خلال رصد الجاني عبر شبكة الانترنت في حركة مريبة، ليتم ترصده عبر هذه الشبكة.[3]

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 ،[4] وقد نصت على ذلك المادة 44 من قانون الإجراءات الجزائية بقولها: يجب

[1] أنظرالقانون 04-09 المؤرخ في 5 أوت 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، عدد ،47 السنة ، 46الصادرة بتاريخ 16 غشت سنة .2009.
[2] رشيد بوكر, المرجع السابق, ص408.
[3] رشيد بوكر، المرجع السابق، ص 409.
[4] المرجع نفسه, ص411.

أن يعين الإذن بالتفتيش بيان وصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها...".[1]

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.[2]

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

وحدات الإدخال: مهمتها إدخال البيانات كلوحة التحكم.

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 ، وذلك بعد أن تستوفي عملية التفتيش الشروط المذكورة أعلاه.[3]

3- "**تفتيش المكونات المعنوية 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 -04 09بموجب 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 :

[1] أنظر المادة44 من قانون الإجراءات الجزائية الجزائري.
[2] رشيد بوكر, المرجع السابق, ص396.
[3] فايز نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، مصر، 2012، ص.131

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

ب- منظمة تخزين معلوماتية..."[1].

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،[2] 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 04-09 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، يجوز تمديد التفتيش إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك..."[3].

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 "[4].

[1] أنظر المادة 5 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
[2] رشيدة بوكر، المرجع السابق، ص 401، 402.
[3] أنظر المادة 5 فقرة 2 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
[4] أنظر المادة 5 فقرة من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

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.[1]

وقد نص المشرع الجزائري على هذا الإجراء من خلال القانون 04-09 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 اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أجزاء وفقا للقواعد المقررة في قانون الإجراءات الجزائية" .[2]

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:

الورق: يقوم الكثيرون من مستخدمي الحواسيب الآلية بالاعتماد على الورق في طباعة المعلومات لمراجعتها والتأكد منها وقت الحاجة، وبالنظر لأهميتها قد تكون

[1] 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، ، 2013ص .94

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

موضوع للجريمة لذا وجب تفتيشها وضبطها سواء كانت أوراق أصلية يتم حفظها للاعتماد عليها أو أوراق ثانوية يتم تحضيرها مؤقتا ثم إهمالها.[1]

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.[2]

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.

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

بطاقاتpcmcia : ولها نفس شكل بطاقات الدفع، وتستعمل في الحواسيب الصغيرة {نوتبوك و اللابتوب}.

ويتم التحفظ على هذه المكونات المادية المذكورة كلها أو جزء منها للاستفادة من أي معلومة قد تفيد في مسار الكشف عن الجريمة.[3]

[1] علي عدنان الفيل, المرجع السابق ,ص56.
[2] المرجع نفسه, ص57.
[3] علي عدنان الفيل, المرجع السابق, ص57.

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 وا بالتالي ٍ عادة الإنتاج و 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.[1]

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 04-09 السالف الذكر.
- الاحتفاظ بالأقراص كما هي وعدم طيها لضمان عدم إتلافها .

[1] 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 ص،237 .238

- 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 105–100 من قانون الإجراءات الجزائية باحترام كرامة المتهم ومنحه الفرصة للدفاع عن نفسه، وفي الجرائم المعلوماتية وحتى يضمن قاضي التحقيق أفضل النتائج وجب عليه مايلي:

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[2].

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.[3]

[1] رشيدة بوكر، المرجع السابق، ص .422
[2] حسين ربيعى، المرجع السابق، ص .225
[3] المرجع نفسه, ص225.

2-**الشهادة:** تعتبر إجراء من إجراءات التحقيق، وهي الأقوال الخاصة بالأشخاص غير الخصوم أمام الجهة المكلفة بالتحقيق ولها أهمية كبيرة في إثبات الجريمة، والمحقق هو من 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.[1]

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 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] علي عدنان الفيل المرجع السابق, ص61.

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 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 اختصاصه إلى محاكم أخرى، تطيق حسب التنظيم مع مراعاة ضابط الشرطة لالتزاماته وفق المادة 40 مكرر1 و2 من نفس القانون.

[1] صالح شنين، المرجع السابق ص ص ،259 .
[2] علي عدنان الفيل., المرجع السابق 267.
[3]علي عدنان الفيل, المرجع السابق, ص269.

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

المطلب الثاني: القوانين الخاصة بالجرائم الإلكترونية والإجراءات المستحدثة

حتى يضمن المشرع الجزائري لحماية الجنائية والإجرائية اللازمة للمعاملات الإلكترونية، وبعد إدراكه 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 في هذا المجال(الفرع الأول) ، الاستعراض الإجراءات المستحدثة (الفرع الثاني).

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

[1] صالح شنين، المرجع السابق، ص 270.

والتي سلكت منعرجا خطيرا ومن بينها الجرائم الواقعة على بطاقات الدفع الإلكتروني، على المستوى الوطني (أولا)، على المستوى الدولي (ثانيا).

أولا: على المستوى الوطني

سنعالج على المستوى الوطني من خلال التشريعات المستحدثة(1)، الجهات المختصة بمكافحة الجرائم المعلوماتية(2).

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

- القانون 15-04 المؤرخ في 10 نوفمبر ،2004 المعدل والمتمم للأمر 156-66 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 04-09 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 22.06 المؤرخ في 20 ديسمبر ،2006 المعدل والمتمم لقانون الإجراءات الجزائية من خلال المواد التي تنظم الاختصاص النوعي والمحلي والإجراءات الخاصة بالتفتيش.[3]
- القانون 02-16 المؤرخ في 19 يونيو،2016 المتمم للأمر،156-66 جاء هذا القانون ليتمم المواد 87 مكرر11 و87 مكرر 12 إضافة إلى المادة 394 مكرر8.[4]

[1] أنظر قانون العقوبات الجزائري.
[2] انظر القانون 09-04 , المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها.
[3] أنظر قانون الإجراءات الجزائية الجزائري.
[4] المصدر نفسه.المعدل والمتمم.

- المرسوم الرئاسي 261–15 المؤرخ في 8 أكتوبر 2015 إلى إنشاء الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

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 04–09 وكان دخولها حيز النفاذ في سنة 2015 بموجب المرسوم الرئاسي ،268–15 وعرفتها المادة 13 بأنها سلطة إدارية مستقلة معنويا وماليا، مقرها بالعاصمة، كما جاءت المادة 14 من القانون –09 04والمادة 4 من المرسوم الرئاسي سابق الذكر لتحديد مهام اللجنة تحت إشراف السلطة القضائية والمتمثلة أساسا في تنشيط وتنسيق إجراءات الوقاية والمكافحة ومساعدة السلطات القضائية.[2]

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 ووهران، إضافة إلى ثلاث وحدات أخرى طور الانجاز كل من ورقلة وبشار وتمنراست[3].

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

[1] المرسوم الرئاسي 261-15 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 ، 53السنة 52 الصادرة بتاريخ 8 أكتوبر 2015.
[2] أنظر المواد 13و14 من القانون ،04-09 المصدر السابق.
[3] ربيعي حسين، المرجع السابق، ص ص، ،176 .177.

التحريات الجنائية، المصالح والمراكز العلمية والتقنية، حيث تسعي كل هذه المصالح إلى اكتشاف جميع الجرائم المرتكبة على الأجهزة الإلكترونية وعبر الانترنت.[1]

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. [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 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.[3]

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

[1] المرجع نفسه، ص ص،182 .183.

[2] لهام 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 ص.329.

[3] 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، ، 2012ص101.

14–252 المؤرخ في 8 سبتمبر 2014 ،[1] 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 والقضائي بين الدول الأعضاء من خلال تبادل المعلومات ووضع قواعد للاختصاص وحل مشكلة التنازع.[2]

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 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 ،22–06 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

[1] مرسوم رئاسي رقم 252-14 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 ، 75السنة ،51 الصادرة بتاريخ 28 سبتمبر.
[2] إلهام بن خليفة، المرجع السابق، ص 334.

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]

2-**الشروط الموضوعية:** وتتمثل في أن يكون التسرب مسببا، 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]

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 .

[1] المرجع نفسه, ص305.
[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.
[3] إلهام بن خليفة، المرجع السابق، ص ص 307، .

- 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 بالإجراء:** 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 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.[2]

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.[3]

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 ،[4] ونستعرضها فيما يلي:

[1] إلهام بن خليفة، المرجع السابق، ص ص 308.
[2] سامية بولافة ومبروك السياسي، "الأساليب المستخدمة في التحريات الجزائية" مجلة الباحث للدراسات الأكاديمية، العدد التاسع، دس، جامعة باتنة1، باتنة، جوان 2016، ص.
[3] معتوق عبد اللطيف، المرجع السابق، ص .106
[4] أنظر المواد من 65 مكرر 5 إلى غاية المادة 65 مكرر 10 من قانون الإجراءات الجزائية.

- 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
- 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.

المبحث الثاني : الإجراءات الوقائية في مواجهة الجرائم الواقعة على بطاقات الائتمان

أمام تزايد عمليات الاستخدام غير المشروعة لبطاقة الإئتمان الإلكترونية ومن اجل المحافظة على سلامة وأمن المعاملات المصرفية ببطاقات الائتمان، وجب إتباع مجموعة من الإجراءات الإجراءات 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 .

لدراسة هذه الإجراءات ولتسليط الضوء عليها فقد قسمنا هذا المبحث إلى مطلبين، نتناول فيه الإجراءات الوقائية من قبل المصدر والتعاون الدولي في مواجهة هذه الجرائم في المطلب الأول، بينما خصصنا للإجراءات الوقائية على مستوى صاحب البطاقة والتاجر والجهاز الأمني من خلال المطلب الثاني.

المطلب الأول: الإجراءات الوقائية المتبعة من المصدر والتعاون الدولي في مواجهة الجرائم الواقعة على بطاقات الائتمان

بالتداول المتزايد و الإستعمال المتنامي لبطاقات الائتمان و نظرا للتزايد الكبير في المقابل 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 من قبل المصدر للبطاقة من خلال الفرع الأول ، في حين خصصنا الفرع الثاني للتعاون الدولي للوقاية من الواقعة على بطاقات الائتمان.

الفرع الأول: الإجراءات المتخذة من قبل مصدر البطاقة

إن حماية البطاقة من التلاعب والحد من الاستخدام غير المشروع لها، من واجب الجهة المصدرة لها الذي يقع عليها عبء توفير أكبر قد ممكن من الحماية للبطاقة التي يصدرها،[1] إما بتطور البطاقة تقنيا (أولا)، ، من أجل الحد من عمليات تزويرها، أو القيام بعدد من الإجراءات الإدارية و المصرفية (ثانيا)، التي من شأنها المساهمة في مواجهة الاستخدامات غير المشروعة لها .

أولا – الإجراءات التقنية:

نحاول إيجاز أهم الإجراءات التقنية المتخذة لمواجهة إساءة إستخدام بطاقات الائتمان الالكترونية.

أول حلقات هذا التطوير كان بإختراع بطاقة ذات دوائر إلكترونية، من مزاياها أنها غير قابلة للتأثير عليها أو إختراقها، وتحتفظ في ذاكراتها بآخر العمليات المنفذة، وتعد من الناحية التقنية غير قابلة للتزوير ومثالها صورة الحمامة في بطاقة فيزا[2] .

ومن بين الإجراءات التقنية التي خصصت أيضا لمواجهة إساءة استخدام البطاقة، نجد الإنترنيت، النموذج التقني الموحد الذي أعلنت عنه شركتي فيزا وماستر كارد، والمسمى نظام الصفقات الالكترونية الآمنة، ومن بعد ذلك إنضمام العديد من الشركات الأمريكية له[3] .

كما أعلنت ماستر كارد العالمية في عام (2002) عن طرح بطاقة (ماستر كادر باي باس ،) وهو برنامج للدفع للبطاقة دون إتصال .

فهي تعد بطاقة دفع مطورة تمتاز برقاقة كمبيوتر مضمنة ومخ ة في و أنتينا (لاقط) وكل ما على حامل البطاقة فعله هو تمرير البطاقة أمام أو قرب جهاز إلكتروني مهيأ

[1] أمجد حمدان الجهني، المرجع السابق، ص ص ، 112، 121
[2] علي عدنان ففيل , المرجع السابق, ص76..
[3] أمجد حمدان الجهني، المرجع السابق، ص 113.

خصيصا لدى التاجر، وبعدها تقوم البطاقة بإرسال معلومات الدفع لاسلكيا، وتبادل المعلومات مع الجهاز الإلكتروني، ثم معالجتها من خلال شبكة ماستر كارد، وبعد لحظات يستلم إشارة بتأكيد الدفع بينما يكون هو في طريقه إ لى منزله أو عمله[1] .

كما تتأهب حاليا شركات أمريكية أخرى لاستعمال تقنيات أمنية جديدة ،[2] ومن الشركات العربية التي ساهمت في إطلاق بطاقة آمنة للتسوق عبر الأنترنيت شركة " مكتوب دوت كوم"، حيث أعلنت هذه الأخيرة عن إصدار بطاقة "كاش يو" التي تمكن الحامل من شراء السلع و الخدمات على شبكة الأنترنيت بثقة تامة دون أية مخاطر ممكنة، وهي متوافرة بثلاث فئات : عشرة دولارات أمريكية،عشرين دولارا أمريكيا ثلاثين دولارا أمريكيا.[3]

ثانيا – الإجراءات الإدارية المصرفية :

للبنوك دور هام في منع إساءة إستخدام بطاقات الإئتمان الإلكترونية، إذ يجب عليها الحد من الثغرات التي تسهل من عملية إرتكاب الجرائم . وذلك بمراعاتها بعض الإجراءات عند إصدارها بطاقات الإئتمان الإلكترونية، أهم الإجراءات الواجب مراعاتها من طرف البنوك مصدرة البطاقة :

- الاستعلام الجيد والدراسة المتأنية للعملاء طالبي الحصول على البطاقات والتأكد من صحة وسلامة المستندات المقدمة .
- الدقة في إختيار الموظفين العاملين فيها، مراقبتهم بصورة دورية وتدريبهم بصورة جيدة لكيفية التعامل مع هذه البطاقات وملحقاتها .

[1] علي عدنان الفيل، المرجع السابق، ص -77. 78.
[2] شركة ابلايد ديجيتال سوليو شيتر IDS عرفت بتطوير رقائق، تزرع تحت الجلد لتحديد الهوية الشخصية لتتعرف على موقع حامليها، لتأمين طريقة موثوقة لزبائنها لتفادي الغش، بتوظيف الرقائق في تعاملات الدفع ببطاقة الدفع الإلكتروني وأسمتها (رقيقة فيريتشيب)، وقدمت الرقيقة كطريقة متفوقة على بطاقة الدفع الإلكتروني الحالية، والبطاقة الذكية اللتين باتتا . أمجد حمدان الجهني، المرجع السابق، ص 114.
[3] علي عدنان الفيل، المرجع السابق، ص79.

- التنسيق على إنشاء وحدات إدارة المخاطر للبنوك المركزية الخاصة ببطاقات الإئتمان . بالإضافة إلى دراستها للعمل على مواجهتها، والحد من تكرار الجرائم المتعلقة بها .
- مراقبة التجار المتعاقدين مع البنوك من خلال فواتير البيع والشراء لذات البنوك لمنع أي تلاعب .[1]
- إصدار نوع من البطاقات تتناسب مع نوعية العملاء واحتمالات المخاطرة العالية، مع أخذ الموافقة عند الصرف، بالإضافة إلى تزويد البطاقة بشفرات معينة تتم تحديثها دائما.
- حسن إختيار التجار والمؤسسات التجارية التي تتمتع بسمعة طيبة ، استقرار مهني ومالي وقانوني , مع تزويدهم بأحدث الأجهزة الإلكترونية للتعامل لضمان الكشف الفوري عن البطاقات المزورة.
- تضييق نطاق ضوابط تنظيم تداول إيصالات الدفع، لمنع تسريب المعلومات[2] .
- القيام بسحب البطاقة إذا تم الإبلاغ عن سرقتها أو فقدها، إذا أن البنك يقوم ببرمجة جهاز الصراف الآلي على عدم قبول البطاقة وسحبها وعدم إعادتها، في حالة إذا تم إدخال للرقم السري ثلاث مرات، فالبنك يفترض في هذه الحالة أن الشخص الذي قام بإدخال الرقم السري ليس هو الحامل الشرعي للبطاقة .[3]

الفرع الثاني: التعاون الدولي للوقاية من جرائم بطاقات الائتمان

يعرف بعض الفقه التعاون الدولي بأنه ": تبادل العون والمساعدة وتضافر الجهود المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة مشتركة سواء كانت هذه الخدمة أو

[1] حسين محمد الشبلي، مهند فايز الدويكات، المرجع السابق، ص -106 107.
[2] علي عدنان الفيل، المرجع السابق، ص -79. 80.
[3] أمجد حمدان الجهني، المرجع السابق، ص ص، -115 118.

النفع على مستوى عالمي أو على مستوى إقليمي أو على المستوى الوطني للدول التي يتم الاتفاق فيما بينها ".[1]

فالتعاون الدولي يسعى لمكافحة الجريمة بشكل عام ولا يقتصر على مجال معين، ومن بينها جرائم بطاقات الائتمان التي تعد من الجرائم الاقتصادية التي لها مخاطر كبيرة على الاقتصاد القومي والعالمي، ولما تمثله من تهديد لأنظمة الدفع وتحويل الأموال إلكترونيا، سواء كانت المنظمة الدولية للشرطة الجنائية(أولا) أو مجلس وزراء الداخلية العرب (ثانيا)، أو المنظمة الدولية لضباط الجرائم المالية (ثالثا)، و هو يتكون من عدة منظمات قد تكون دولية أو إقليمية تهدف بصفة عامة إلى مكافحة الجريمة .

أولا – المنظمة الدولية للشرطة الجنائية (الأنتربول) :

لقد نظمت السكرتارية العامة الخاصة بالمنظمة أول مؤتمراتها الدولية بخصوص الاحتيال والغش الذين يهددان نظام بطاقات الائتمان في أكتوبر 1994 وقد قامت بتبني توصيتين :

1 -على الدول الأعضاء مراجعة تشريعاتها وقوانينها الخاصة ببطاقات الائتمان الإلكترونية، بما يضمن تجريم تضيع أو امتلاك البطاقات المزورة أو امتلاك معلومات غير قانونية، أو الحصول عليها بطريقة غير مشروعة، واستخدامها في إدخالها نظام بطاقات الائتمان[2].

2 - إنشاء مجموعات عمل بوليسية من خبراء العمل في مواجهة الإحتيالات الدولية، التابعين لبوليس هو نج كونج والشرطة الكندية و الخدمة السرية الامريكية وخدمة الاستخبارات القومية الجنائية لنيوزيلاندا و مندوبين من منظمات بطاقات الائتمان،

[1] ضياء علي أحمد نعمان، المرجع السابق، ص 229.
[2] عبد الكريم الردايدة، المرجع السابق، ص 168.

لمكافحة هذه النوعية من الجرائم، والتقوا جميعا في شهر فبراير 1995وتم وضع الأسس الخاصة بتبادل المعلومات بهدف الحد من هذه الجرائم .[1]

وقد قام الأنتربول بتوقيع خمس اتفاقيات مع المنظمات الراعية للبطاقات وهي فيزا وماستر كارد، وأمريكان أكسبرس، وديسكفري، وأيروبال أنتر ناسيونال من أجل التعاون في مجال جرائم بطاقات الائتمان عام 1999.[2]

ثانيا – دور مجلس وزراء الداخلية العرب مواجهة جرائم بطاقات الائتمان :

كان لهذه المنظمة بصمات واضحة في مواجهة مثل هذه الجرائم حيث تم تناول هذا الموضوع من قبل اللجنة المتخصصة في اجتماعها الثاني عشر . حيث أوصت بوضع تشريعات خاصة لمواجهة جرائم بطاقات الائتمان، تأهيل أجهزة العدالة الجنائية بتقنيات البطاقات وتوعية المواطنين والمتعاملين بها . ومن ثم دعوة الأجهزة الأمنية إلى إجراء التنسيق فيما بينها للوقوف على مستجدات الجرائم، و دعوة الدول الأعضاء إلى تعزيز التعاون فيما بينها لمواجهة الجرائم وكشف العصابات الدولية التي تديرها.[3]

وقد اعتمد المجلس في دورته الحادية والعشرون التي انعقدت عام 2004 قانون الإمارات الخاص بمكافحة جرائم تقنية المعلومات، كقانون استرشادي للدول الأعضاء، لمواجهة الجرائم المتزايدة، الناتجة عن تقنية المعلومات ومنها استخدام بطاقات الائتمان بوساطة الحاسب الآلي.

ثالثا – دور المنظمة الدولية لضباط الجرائم الماليةLAFCL :تعتبر منظمة الدولية لضباط الجرائم المالية منظمة دولية غير ربحية تسعى لتوفير الخدمات، و توفير البيئة التي يمكن من خلالها جمع المعلومات حول الاحتيال المالي وطرق التحقيق والحماية المالية، وقد تم إنشاء هذه المنظمة عام 1986 عن طريق التعاون بين 68 محققا دوليا

[1] إيهاب فوزي السقا، المرجع السابق، ص 508.
[2] ضياء علي أحمد نعمان، المرجع السابق، ص 231.
[3] عبد الكريم الردايدة، المرجع السابق، ص 168.

متخصصا بجرائم الأموال، و تم من خلال ذلك إنشاء منظمة دولية لضباط جرائم بطاقات الائتمان.[1]

ومنذ عام 1998 وهذه المنظمة تمنح عضويتها العادية لضباط الشرطة ومحقق مؤسسات إصدار البطاقات، وخبراء مكافحة الاحتيال بشيء صورة، من خلال شروط خاصة.

كما تتيح عضوية هذه المنظمة لأعضائها الحصول المعلومات السرية الخاصة بالجرائم المالية، الدولية والمجرمين الدوليين ، بالإضافة إلى إرسال إنذارات لأعضائها بالأماكن المعرضة لهذه الجرائم ، فهي تتيح للعضو الدخول على شبكات الحاسب الآلي التي تخص الجرائم المالية [2].

المطلب الثاني: الإجراءات المتخذة من قبل الحامل و التاجر والأجهزة الأمنية

بهدف تجنب وقوع جريمة من الجرائم الواقعة على بطاقات الائتمان لابد من إتباع مجموعة من الإجراءات الوقائية سواء من قبل الحامل لها أو من قبل التاجر أو من قبل أجهزة الأمن وذلك لحيلولة دون وقوع هذه الجرائم ولذلك سنخصص هذا المطلب لدارسة هذه الإجراءات الوقائية وذلك من خلال ثلاث فروع, أول فرع بعنوان الإجراءات المتخذة من قبل الحامل للبطاقة, وثاني فرع الإجراءات المتخذة من قبل التاجر فيما نخصص الفرع الأخير للإجراءات التي تتخذها أجهزة الأمن.

الفرع الأول: الإجراءات المتخذة من قبل الحامل

[1] إيهاب فوزي السقا، المرجع السابق، ص 508.
[2] ضياء علي أحمد نعمان، المرجع السابق، ص 231.

تعتبر بطاقات الإئتمان الإلكترونية عملة اليوم، ولحمايتها من الإستخدام غير المشروع وجب على حامل البطاقة تأمين البطاقة والبيانات المدونة عليه (أولا)، و القيام بمجموعة من الإجراءات اللازمة لحمايتها من النصب (ثانيا).

أولا – تأمين بطاقة الإئتمان والبيانات المدونة عليها:

- عند إختيار الرقم السري وجب محاولة الإبتعاد عن إختيار حروف وأرقام ذات صلة، حتى لا يصبح من السهل كشفها ومعرفتها كتاريخ الميلاد أو رقم الهاتف . كما يتجتنب الحامل كتابة الشفرة السرية على البطاقة، وعدم لإا فصاح عنها لأي شخص آخر.
- عدم إعطاء رقم البطاقة عن طريق الهاتف، إلا في حالة التعامل مع شركة موثوق فيها.
- تجنب الإستجابة لرسائل البريد الالكتروني الخادعة قبل التحقق من مصدرها .[1]
- حفظ الرقم السري غيبا ويتلف الوثيقة التي يكون بها الرقم السري، ويقوم بالحرص على أن لا يشاهده أحد وهو يقوم بإدخال ِ الرقم السري في جهاز الصراف الآلي، لا يطلب الوصل المطبوع من جهاز الصراف الآلي، و ن ا طلبه فإن عليه أن يقوم بأخذه ولا يتركه،لأنه يحتوى على رقم حساب الحامل.[2]

ثانيا – الاجراءات التي يقوم بها حامل بطاقة الإئتمان الإ لكترونية لحمايتها من النصب :

[1] عبد الكريم الردايدة، المرجع السابق، ص 188.
[2] علي عدنان الفيل، المرجع السابق، ص 83.

هناك مجموعة من الاجراءات يتبعها حامل البطاقة من أجل حمايتها من عملية النصب،بأن يتعامل بحذر مع المكالمات الهاتفية أو رسالة تطلب منه محرفة معلومات عن حسابه المالي .

- عدم إعلام أي أحد برقمPIN ، واذا أحس بأن شخصا يعرف رقمه فيجب عليه إبلاغ الجهة المختصة لتعطي له رقما آخر .
  - الإ حتراس من الرسائل أو MAILE ، الذي يعطي عن طريقWET NET مع العلم أن الشبكة لا تسأل عن أي تفاصل عن حساب أحد لذلك ويجب عدم الرد عليها .[1]
- التأكد من موثوقية الموقع، فلا يعطي رقم البطاقة إلا مع المواقع المشهورة ، كما لا يقوم بإرسال المعلومات الشخصية عبر الشبكة، مثل العنوان الشخصي ، رقم الهاتف، رقم البطاقة، إ لا إذا كانت هذه المعلومات مرسلة باستخدام وسائل مشفرة.
- إستخدام برامج كمبيوتر مشفرة مثل برنامج (good pretty) ، (PGP) لضمان خصوصية البريد الالكتروني (MAIL-E) ، وبعد إتمام العملية يطبع الصفحة التي تحتوي على مختصر للعملية التي قام بها، حتي يتمكن من معرفة ماله وما عليه.[2]
- استخدام طرق PIN and CHIP وهي أحدث طريقة تستخدم في البنوك ضد النصب بالبطاقات، فعند ما ما يتم دفع شيء بواسطة البطاقة ،سيطلب من حامل البطاقة إدخال الرقم المكون من أربعة أرقام بدلا من التوقيع على إيصال الاستلام.[3]

[1] عبد الكريم الردايدة، المرجع السابق، ص ص، 193-191.
[2] علي عدنان الفيل، المرجع السابق، ص -84.
[3] عبد الكريم الردايدة، المرجع السابق، ص 192.

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.
- قيام التاجر بالاحتفاظ بالشعرات الخصم أطول مدة ممكنة .

[1] عبد الكريم الردايدة، المرجع الساق، ص.185.
[2] أمجد حمدان الجهني، المرجع الساق، ص ص ،124 .125.
[3] وسام فيحل محمود الشواورة، المرجع السابق، ص .107

- 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 من

[1] عبد الكريم الردايدة، المرجع الساق، ص .185
[2] علي عدنان الفيل، المرجع السابق، ص .125
[3] المرجع نفسه، ص .126

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).

أولا: الإجراءات المتعلقة بالبنوك والمؤسسات المالية

[1] أمجد حمدان الجهني، المرجع السابق، ص 125.
[2] المرجع نفسه، ص 126.
[3] الكريم الردايدة، المرجع السابق ص 102.
[4] معادي أسعد صوالحة، المرجع السابق ص 416.

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-**الإجراءات المتعلقة بالأفراد العاديين:** وذلك من خلال العمل على تنبيه وتوعية المواطنين ومستخدمي هذه البطاقات بالمخاطر التي تحيط بها، وذلك بعقد الندوات

[1] عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، المرجع السابق، ص .130.
[2] عبد الكريم الردايدة، جرائم بطاقات الائتمان، المرجع السابق، ص.130.
[3] المرجع نفسه، ص ص،129 .131.

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 ممن يشتبه 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]
- 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.[5]
- ضرورة إخضاع أفراد الشرطة لضوابط جدية بهدف انتقائهم من حيث اللياقة البدنية، والكفاءة العلمية والفكرية والثقافية، وذلك لجعلهم مختصين

[1] عبد الكريم الردايدة، جرائم بطاقات الائتمان، المرجع السابق، ص .116.
[2] عبد الكريم الردايدة، جرائم بطاقات الائتمان، المرجع السابق، ص .131.
[3] حمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ،2004 ص ص 163، 164.
[4] ينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، ،2015 ص.99.
[5] عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، المرجع السابق، ص.1.

في مواجهة هذه الجرائم من حيث الأشخاص المرتكبين لها وأساليب ارتكابها، وبالتالي القدرة على التحقيق التقني للتعامل مع هذه القضايا.[1]

- 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 .[2]

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 وهو ما يعزز أمن واستقرار البنوك والمؤسسات المصرفية [3].

[1] عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، المرجع السابق، ص.131.
[2] محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، ،2014 ص257.
[3] 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.

الخاتمــة

الخاتمة

في الختام بعد دراستنا لموضوع الجرائم الواقعة على بطاقات الائتمان نجد أنه مع التطور الحاصل في جميع الميادين، تمثل بطاقات الائتمان مرحلة جديدة ومعاصرة في الممارسة المصرفية والمالية، حيث تتميز بطابع خاص عن باقي وسائل الدفع الاخرى بكونها قائمة على علاقة ثلاثية الأطراف متمثلة في المصدر للبطاقة والتاجر والحامل لهذه البطاقة.

رغم صدور القانون 05/18 المتعلق بالتجارة الإلكترونية إلا أنه لم يحمل في طياته المأمول بخصوص الموضوع محل الدراسة، وظلت حماية بطاقة الائتمان رهينة التكييفات القانونية الكلاسيكية خصوصا ما تعلق بالجانب الجزائي الذي هو محل دراستنا.

ونخلص في الأخير بعد دراستنا لهذا الموضوع لجملة من النتائج تتمثل في:

- لايزال الغموض يشوب جوانب بطاقات الائتمان والحماية المتعلقة بها المتأرجحة بين المدني والجزائي غير كافية .
- عدم إنطباق نصوص قانون العقوبات على تصرف الحامل سيء النية ، الذي إستخدم البطاقة أثناء فترة صلاحيتها بتجاوز حد السحب، على الرغم من كون رصيده لا يسمح بذلك، حيث لا يقع تحت طائلة أي نص جنائي وهذا ما ينجر عنه الإخلا بالثقة الواجب توافرها في نظام بطاقات الائتمان.

وبناءا على ذلك نقترح مجموعة توصيات:

- إلزامية مواكبة المشرع للجرائم المستحدثة وتبنيه آليات وقائية تكفل تجنب وقوع مثل هذه الجرائم بالتنسيق مع الأجهزة التقنية المحيطة بتقنيات المعلومات الحديثة و الخبراء مع الشرطة و القضاء و السلطة التشريعية.

- دعوة المشرع للتشريع في مجال بطاقات الائتمان وما يقع عليها من جرائم وذلك إعمالا لمبدأ الشرعية.

قائمة المصادر والمراجع

أولا: المصادر:

القرآن الكريم.

النصوص الرسمية:

1. القانون رقم 04/09 المؤرخ في 5 أوت 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.، ج.ر.عدد 47 الصادرة في 16 أوت لسنة 2009.
2. أمر رقم 66.156 مؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، بالجريدة الرسمية عدد49، بتاريخ 11جوان 1966، المعدل والمتمم.
3. الأمر رقم 66/ 155 الموافق لـ 8يونيو سنة، 1966 المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر صادرة في 1966.المعدل والمتمم.
4. المرسوم الرئاسي رقم 15/261 المؤرخ في 08/10/2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد .53 2015.
5. مرسوم رئاسي رقم 252-14 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 ، 75السنة ،51 الصادرة بتاريخ 28 سبتمبر 2014.

ثانيا: المراجع

الكتب :

1. أيمن عبد الحفيظ, حماية بطاقات الدفع الإلكتروني, دار النهضة العربية للنشر والتوزيع, الأردن 2007.

2. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان ، د ط ، دار الجامعة الجديدة الإسكندرية ، 2007.
3. باسم أحمد المبيضين,التجارة الإلكترونية , دار جليس الزمان للنشر والتوزيع, الأردن ,2010.
4. حسام محمد نبيل الشنراقى، جرائم الاعتداء على التوقيع الالكتروني، دون طبعة، دار الكتب القانونية، مصر ، ،2013.
5. حسين محمد الشبلي، مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولى (، الأردن، دار مجدلاوي، 2009).
6. حمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ،2004.
7. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.
8. شيماء عبد الغني محمد عطا الله،الحماية الجنائية للتعاملات الإلكترونية،دار الجامعة الجديدة، ب ط،الإسكندرية مصر ،2007.
9. ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى مراكش المطبعة والوراقة الوطنية، 2011.
10. عبد الحكيم احمد محمد عثمان، أحكام البطاقات الائتمانية والآراء الفقهية الإسلامية، الطبعة الأولى، مصر ،دار الفكر الجامعي 2007.
11. عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الالكترونية (، الكتاب الثاني الحماية الجنائية لنظام التجارة الالكترونية)، الطبعة الأولى، (الاسكندرية، دار الفكر الجامعي، 2002).
12. عبد الكريم الردايدة, جرائم بطاقات الائتمان دراسة تطبيقية ميدانية, ط1 , دار حامد, الأردن, 2013.

13. علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية –دراسة مقارنة،– دون طبعة، المكتب الجامعي الحديث، الموصل، ،2012.

14. فايز نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، مصر، ،2012.

15. كميت طالب البغدادي، الاستخدام غير المشروع لبطاقات الائتمان المسؤولية المدنية و الجزائية,ط1, دار الثقافة , الأردن 2008.

16. لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، ،2015.

17. معادي أسعد صوالحة , بطاقات الائتمان النظام القانوني وآليات الحماية الجنائية والأمنية دراسة مقارنة. دار قباء الحديثة للطباعة والنشر والتوزيع, القاهرة 2007.

18. محمد توفيق سعودي، بطاقات الائتمان الأسس القانونية للعلاقات الناشئة عن استخدامها الطبعة الأولى، مصر، دار الأمين، 2009

19. محمد أمين الشوابكة، جرائم الحاسوب و الانترنت ' الطبعة الاولى ، ،دار الثقافة الاردن ،2004 .

20. محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، ،2014.محمود إبراهيم غازى، الحماية الجنائية للخصوصية والتجارة الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية الإسكندرية، ،2014.

21. محمود الكيلاني، الموسوعة التجارية والمصرفية (، التشريعات التجارية والالكترونية)، الطبعة الأولى، (الأردن، دار الثقافة، 2009).

22. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية تطبيقية) الطبعة الأولى، (لبنان، دار المنشورات الحلبي، 2005).
23. نجيمي جمال، جرائم التزوير في قانون العقوبات الجزائري، دار هومة لنشر و التوزيع ط 2 الجزائر ،2014.

I. المذكرات :

دكتوراه:

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. حسين ربيعى، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1 ،2016.
3. 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.
4. مجراب الداودي، الأساليب الخاصة بالبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة بن يوسف بن خدة، الجزائر، ،2016.

ماجستير:

1. 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.
2. 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.
3. 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.
4. 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.
5. واقد يوسف،النظام القانوني لدفع الإلكتروني، مذكرة ماجستير، تخصص قانون تعاون الدولي، جامعة مولود معمري تيزي وزو2011 .

II. **المقالات :**

1. أمجد حمدان الجهني، الاستخدامات الغير مشروعة لبطاقة الدفع الإلكتروني من قبل الغير، مركز الدراسات القضائية، المملكة الأردنية الهاشمية، مقال منشور على : .www.coiss.com/replay.php ، أخر زيارة بتاريخ 2023/06/07 على الساعة: 23:28.
2. سامية بولافة ومبروك السياسي، "الأساليب المستخدمة في التحريات الجزائية" مجلة الباحث للدراسات الأكاديمية، العدد التاسع، دس، جامعة باتنة،1 باتنة، جوان ،2016.

3. محمد لموسخ، تنازع الاختصاص في الجرائم الإلكترونية، مجلة الحقيقة، عدد 28، المطبعة العربية، غرداية، الجزائر، 2014.

الملتقيات و المداخلات :

1. زهير طافرو الهاشمي بوترفاس, مداخلة بعنوان واقع بطاقات الائتمان في الجزائر, المركز الجامعي بشار.
2. محمدي بوزينة أمينة، مداخلة علمية بعنوان: إجراءات مكافحة الجرائم المعلوماتية، ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.

المواقع الالكترونية:

1. أنظر الموقع: http://mawdoo3.com/ آخر زيارة للموقع: 07/ 06/ 2023
2. أنظر الموقع: http://www.aladalacenter.com/index.php/2012-10-31-17-26-38/105-visacard3 تاريخ أخر إطلاع 2023/04/06.

الفهـــرس

العنـــــــاوين	الصفحة
شكر وعرفان	/
إهداء	/
مقدمة	3-1
الفصل الأول: ماهية جرائم التحريض عبر وسائل التواصل الإجتماعي	
تمهيد الفصل	5
المبحث الأول مفهوم جرائم التحريض.	6
المطلب الأول: تعريف التحريض و أنواعه	6
الفرع الأول: تعريف التحريض وتمييزه عن جريمة نشر الأخبار الكاذبة	6
الفرع الثاني : أنواع التحريض على فعل الجريمة	12
المطلب الثاني عناصر التحريض وشروطه	15
الفرع الأول عناصر جريمة التحريض	15
الفرع الثاني شروط التحريض	19
المبحث الثاني : أركان وصور جريمة التحريض عبر وسائل التواصل الإجتماعي	23
المطلب الأول أركان جريمة التحريض عبر وسائل التواصل الإجتماعي	24
الفرع الأول: الركن المادي لجريمة التحريض عبر وسائل التواصل الإجتماعي	25
الفرع الثاني الركن المعنوي لجريمة التحريض عبر وسائل التواصل الإجتماعي	27
المطلب الثاني صور جريمة التحريض عبر وسائل التواصل الإجتماعي	28
الفرع الأول التحريض على العنف والتطرف	30
الفرع الثاني التحريض عم الفساد الأخلاقي	31
الفرع الثالث: التحريض على إستعمال المخدرات	33
الفرع الرابع: التحريض على السب والقذف	35
الفصل الثاني: الإطار الإجرائي لجرائم التحريض عبر وسائل التواصل الإجتماعي ومنظورها	

الدولي.	
تمهيد وتقسيم	44
المبحث الأول: المسؤلية الجزائية وآليات المكافحة لجرائم التحريض عبر وسائل التواصل الإجتماعي	47
المطلب الأول: إجراءات المتابعة ووسائل الإثبات في جريمة التحريض عبر وسائل التواصل الإجتماعي	48
الفرع الأول : الوسائل التقنية للمتابعة الجزائية عن الجرائم الالكترونية	50
الفرع الثاني: التقنيات الحديثة للإثبات الجنائي في جرائم المعلوماتية	53
المطلب الثاني: المسؤلية الجزائية عن جريمة التحريض عبر وسائل التواصل الإجتماعي	55
الفرع الأول: بالنسبة للشخص الطبيعي.	56
الفرع الثاني: عقوبات الشخص المعنوي.	58
المبحث الثاني : جريمة التحريض عبر وسائل التواصل الإجتماعي من المنظور الدولي	60
المطلب الأول: الإطار القانوني لمنع جريمة التحريض من منظور مبدأ مسؤولية الحماية	61
المطلب الثاني: نهج تفعيل مبدأ مسؤولية الحماية لمنع جريمة التحريض الالكتروني.	62
الفرع الاول: دور منظمة الأمم المتحدة في تجسيد مبدأ مسؤولية الحماية	65
الفرع الثاني: الإلتزام بالوقاية على المستوى الوطني	66
الخاتمة	69
قائمة المصادر والمراجع	74

الفهرس

ملخص:

تتضمن هذه المذكرة موضوع الحماية القانونية لبطاقة الإئتمان الإلكترونية من الجرائم . الواقعة عليها، حيث استعرضنا بداية إلى الجرائم الواقعة على البطاقة الإئتمانية والتي قد تصدر من مالكها سواء في فترة صلاحيتها، أو بعد إنتهاء صلاحيتها أو البطاقة الملغاة، وتلك الجرائم الصادرة من الغير سواءا عن طريق استعمال البطاقة المسروقة أو الضائعة بكافة صور الجرائم مع دراسة التكييف القانوني لهذه الجرائم في التشريع الجزائري مقارنا مع التشريع الفرنسي، كما تطرقنا إلى الحماية القانونية المقررة لبطاقة الإئتمان الإلكترونية على مستوى القوانين والإتفاقيات والهيئات الدولية، ثم تطرقنا إلى الحماية المقررة في التشريع الجزائري سواءا من خلال القوانين العامة وتلك الحماية المقررة لبطاقة الائتمان في القوانين الجزائرية الخاصة ، واستعرضنا النتائج والتوصيات التي توصلنا إليها.

Abstract:

This memorandum includes the subject of the legal protection of the electronic credit card from the crimes committed on it, as we reviewed first the crimes committed on the credit card that may be issued by its owner, whether during its validity period, or after its expiration or the canceled card, and those crimes issued by third parties, whether through The use of the stolen or lost card in all forms of crimes with a study of the legal adaptation of these crimes in the Algerian legislation compared with the French legislation. General and those established for credit card protection in private Algerian laws, and we reviewed the findings and recommendations that we reached and we reviewed the findings and recommendations that we reached