جامعة مولود معمري –تيزي وزو–
كلية الحقوق والعلوم السياسية
قسم القانون

الحماية الجزائية من الاستعمال غير القانوني لوسائل الدفع الالكتروني (بطاقة الائتمان نموذجا)

مذكرة لنيل شهادة الماستر في القانون
تخصص: قانونالأعمال

من إعداد الطالبة:
– حبراش كميلية

تحت إشراف الأستاذة:
د/ مخلوفي مليكة

لجنة المناقشة

د. بن طالب ليندا، أستاذة محاضر(ب)، جامعة مولود معمري، تيزي وزو.....رئيسا
د. مخلوفي مليكة، أستاذة محاضرة (أ)،جامعة مولود معمري، تيزي وزو.....مشرفا ومقررا
د. أيت يوسف صبرينة، أستاذة محاضرة (ب) ، جامعة مولود معمري، تيزي وزو.....ممتحنا

تاريخ المناقشة: 2023/10/08

شكر وتقدير

أسجد لله شاكرة فضله، الذي منحني الإرادة والصّبر حتى جعلني أنجز هذا الجهد العلمي البسيط في مجال القانون، ويقول الرّسول صلى الله عليه وسلّم:

" مَنْ لاَ يَشْكُرُ النَّاسَ لاَ يَشْكُرُ الله".

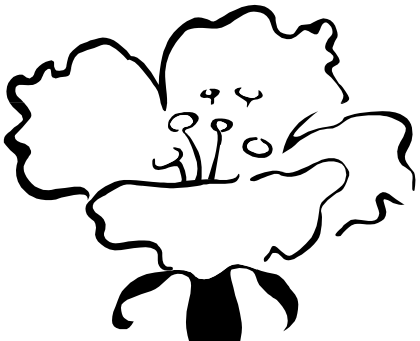
امتثالاً لهذا الحديث النبّوي الشّريف. يسعدني في هذا المقام أن أتقدّم بخالص الشّكر والتّقدير وأصدق آيات العرفان إلى:

الأستاذة " مخلوفي مليكة " التي أشرفت على هذا العمل العلمي المتواضع، والتي وأتاحت لي من وقتها الثّمين وأرشدتني بتوجيهاتها السّامية، فأضاءت لي الطّريق وجنبتني الكثير من الأخطاء في إعداد هذه المذكرة.

فجزاها الله عنّي خير الجزاء وألبسها ثوب الصّحة والعافية، ورزقها صالح الأعمال ونفعت بعلمها مادامت الأرض وبقيت السّموات.

كما أتوجّه بعظيم الشّكر والعرفان لأعضاء لجنة المناقشة المحترمين لتفضّلهم قبول مناقشة وتصويب محتوى هذا العمل العلمي المتواضع، ونسأل الله سبحانه وتعالى أن يبقيهم نبراسًا للعلم ومنارةً للمعرفة.

كميلية.



إهداء

إلى من أوصيتُ بهما وأمرت بطاعتهما وأبغي رضاهما.

إلى من تعلمتُ منهما الصّبر والإيمان والقيم النّبيلة.

إلى والدي أطال الله في عمرهما

...إلى إخوتي الأربعة صفيان، إبراهيم، أسامة وأنيس وكلّ غالٍ...

...إلى كلّ من ساعدني من قريب أو بعيد...إليهم جميعًا أهدي ثمرة علمي هذا عرفانًا وتقديرًا بالجميل.

كميلية

مقدمة

يقتضي التّعامل بنظام الدّفع الإلكتروني الذي يتم تجسيده عبر وسائل الدفع المختلفة بما فيها بطاقات الإئتمان بكل أنواعها ضرورة التقيد بالبنود التي تفرضها جهات إصدارها، ومن هذه الإلتزامات الاستعمال الشّرعي والقانوني لها، وكذا حفظها من الضّياع أو السّرقة، كما أنه يجب المبادرة بالتبليغ عن ضياعها أو عند سرقتها في الوقت المناسب والمحدد، وعليه متى قام الغير الذي بحوزته هذه البطاقة باستخدامها في عمليات السّحب أو الوفاء غير المشروع تقوم المسؤولية الجزائية في مواجهته على أساس التعدي على البطاقة الائتمانية.

تصنّف وسائل الدّفع الالكترونية على أنها ذات طابع شخصي، نظرًا لكونها تصدر باسم الحامل ولاستعماله الشّخصي، وبالتالي فإن استعمال الغير لها يُشكل عملاً غير مشروع سواء كان ذلك عقب فقدها أو ضياعها أو بعد تزويرها.

ويقصد بالغير في هذا الصّدد كل شخص لم تصدر وسيلة الدفع باسمه من الجهة المختصة بإصدارها، فمتى استعمل هذه الوسيلة بغير علم صاحبها كان استعماله هذا غير قانونيا، وذلك بسبب للطّابع الشّخصي الذي تتصّف به هذه البطاقة.

لكن، استخدامها غير المشروع من قبل الغير، ودون علم حاملها الشّرعي يستوجب في حقيقة الأمر التفريق بين عدة حالات فالاستيلاء على وسيلة الدفع ذاتها قد يشكل جريمة سرقة أو استيلاء على بطاقة مفقودة أو نصبًا أو إساءة ائتمان، وذلك كله على حسب الأحوال.

فإذا استولى عليها الغير عنوة أو خِلسة أو بعد تسليم مجرّد اليد العارضة، فإن الواقعة تكون سرقة، أما إذا استولى عليها الغير بالحيلة والخداع بعد استخدام إحدى الوسائل الاحتيالية المحددة قانونا في هذا الشأن، فإن الواقعة تعد جريمة نصب، كما قد تعد جريمة خيانة الأمانة إذا ما استولى عليها الغير نتيجة لتملكها بعد أن قُدّمت إليه بمقتضى سند من

سندات الأمانة، قد يسيء الحامل الشّرعي إستخدام بطاقة الائتمان الإلكترونية كأن يستعملها في غير الحدود المصرح له به رغم صلاحيتها، وهو ما يشكل جريمة السرقة أو يستعملها وهي منتهية الصلاحية مما يشكل جريمة خيانة الأمانة، كما قد يمتنع عن ردّها، وبحكم أن هذه التصرفات الصادرة عنه تعتبر جريمة مما يستلزم تبيان هذه الجرائم و أركانها

تبعًا لهذا الواقع برزت مجموعة من الجهود التي تحاول فرض قواعد تنظيمية على عمل وسائل الدفع الالكتروني، وهذه الجهود ليست واحدة وموحدة في المعايير التي تفرضها، فإذا كانت جميعها ترمي إلى وضع حد أدنى من القيود على شروط العمل بوسائل الدفع هذه بهدف تأمين أكبر قدر ممكن من الحماية للمستهلك، فإن من شأن التطور السّريع لهذه الوسائل، كما هو حاصل بالنسبة للنقود الالكترونية أن يثير الكثير من المسائل التي قد تبدو معها هذه الجهود غير كافية للعمل على حلّها كلّها.

من هنا تظهر أهمية البحث في موضوع حماية وسائل الدفع الالكتروني لاسيما بطاقة الائتمان، وذلك من خلال محاولة التعرض للمجالات التي تستوجب المساءلة الجزائية في مواجهة الغير مع دراسة مدى فعالية العقوبات الجزائية المرصدة للجرائم المتعلقة بها، ومدى توفيق المشرع الجزائري في حماية هذه البطاقة من الاستعمال غير المشروع لها من قبل الغير، لاسيما أن هذه البطاقة قد تكتسب مستقبلا أهمية أكثر واحتمال حلولها كبديل حقيقي للنقود.

وممّا يزيد الموضوع أهمية هو كثرة استعمال بطاقات الائتمان في وقتنا الحاضر بما يتماشى مع نظام الرقمنة سواء في مراكز البريد أو البنوك أو في المحلات التجارية وغيرها، كل هذا يتطلب حمايتها من السرقة والإستعمال دون وجه حقّ.[1]

وعليه يمكن طرح الإشكالية التالية:

فعّالية الحماية القانونية التي كرّسها المشرّع الجزائري لمكافحة جرائم الاستعمال غير القانوني لبطاقة الإئتمان؟

للإجابة على الإشكالية المطروحة تمّ الاعتماد على المنهج التحليلي الوصفي، من خلال تحليل النصوص القانونية ذات صلة بالموضوع بما فيه قانون العقوبات وقانون الإجراءات الجزائية، بالإضافة إلى قانون للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها و المنهج الوصفي من خلال مجموعة من التعاريف المدرجة في هذه الدراسة .

وبغرض الإلمام بالموضوع يجب حصر الجرائم الواقعة على الاستعمال غير القانوني لبطاقة الائتمان **(الفصل الأوّل)** ثم تحديد العقوبات الجزائية المقررة لكل جريمة **(الفصل الثّاني)**.

الفصل الأوّل

الجرائم الواقعة على استعمال غير قانوني لبطاقة الائتمان

استطاعت الانترنت في وقت قصير أن تكون الأداة الأهم في حياة أغلب الأشخاص، حيث أصبحت جزءا لا يتجزأ من تعاملاتنا اليومية، وقد أتاح ظهور هذه الأداة الفرصة لمافيا الجرائم الإلكترونية للتجول من خلالها دون مراقبة ، كما مكّنت السريّة والخصوصية التي تنطوي عليها لغة الكمبيوتر اللّصوص من نقل المعلومات الخطيرة والمحظورة سواء معلومات مخابراتية أو خطط تخريبية أو صور سرية بمجرد الضّغط على زر لوحة المفاتيح دون أدني مجهود أو خوف من العقاب، وما تزال جميع تشريعات الدول عاجزة عن إصدار تشريعٍ كاملٍ وفعالٍ يحظر الجرائم الإلكترونية، خاصة وأن أدلة إثبات الجريمة يصعب التوصل إليها.

ولعلّ من بين أنواع الجرائم الالكترونية نجد عمليات السّطو على بطاقات الائتمان الالكترونية، هذه الأخيرة التي تعد أحدث أنماط السلوك الإجرامي، باعتبارها نقطة تلاقي بين الجريمة المعلوماتية وبطاقات الائتمان الإلكترونية، حيث أصبحت العديد من الدول تعاني من مشكلة الاستخدام غير المشروع لبطاقات الائتمان الإلكترونية، سواء من قبل حاملها(**المبحث الأول**) أو من قبل الغير المشروع (**المبحث الثاني**).

المبحث الأول

استخدام بطاقة الائتمان الالكترونية من قبل صاحبها

تستخدم بطاقة الدّفع الالكتروني استخدامًا مشروعًا عندما يكون الاستخدام الفعلي من المالك الحقيقي لها، وفي حدود ما خُصّص لها وفي حدود سقفها، ويشترط لصحة استخدام البطاقة أن تكون غير مزوّرة، وخلال مدة صلاحيتها وفي حدود وظيفتها، وأيّ استخدام مخالف لشروطها يخرج عن دائرة المشروعية، كأن يتمّ سوء استخدام البطاقة بالنّظر لمدة صلاحيتها **(المطلب الأول)** أو استخدامها عندما تكون ملغاة أو بعد التصريح بضياعها وسرقتها **(المطلب الثاني)**.

المطلب الأول

سوء استخدام بطاقة الائتمان الالكترونية بالنّظر إلى مدّة صلاحيتها

يقصد بصاحب البطاقة الائتمان المالك الأصلي لبطاقة الدفع التي صدرت له، وله الحرية في التصرف فيها كقاعدة وحق، لكن ذلك بقيود، حيث يمكن أن يتعدى حدود استخداماته القانونية لهذه البطاقة وفق ما اتفق عليه في العقد المبرم مع الجهة المصدرة للبطاقة، كأن يستخدمها في خلال فترة صلاحيتها بتجاوزات**(الفرع الأول) أو** يستخدمها عند نهاية صلاحيتها سواء للوفاء أو للسّحب **(الفرع الثاني)**.

الفرع الأول

استخدام بطاقة الائتمان خلال فترة صلاحيتها بتجاوزات

يحدث استخدام بطاقة الائتمان خلال فترة صلاحيتها سواء بالسّحب من الجهاز المخصّص رغم علم صاحبها بأن رصيده غير كافي **(أولا)** أو بالوفاء بقيمة البضائع والخدمات رغم النقص في الرصيد **(ثانيا)**.

أولا: السّحب من جهاز مخصص لذلك رغم النّقص في الرّصيد

يحدث هذا عندما يقوم مالك بطاقة الائتمان[1] الأصلي بالسّحب من الآلية للنقود بمبلغ يزيد عن رصيده بالبنك، أو يتجاوز الحدّ الأقصى المصرّح له، باعتبار أن بطاقة الائتمان[2] دورها هو سحب ما يستحقه صاحبها من المال[1] من خلال الأجهزة الآلية المعدة خصيصا لذلك[2]، وفي حدود ما اتّفق عليه تم التمييز بين الحالات و هي

1- عرفت المادة 543 مكرر 23 من القانون التجاري **بطاقة الائتمان الالكترونية** على أنها **" تعتبر بطاقة الدفع كله بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أمواله"**، كما عرفتها المادة 69 من الأمر رقم 03- 11 المتعلق بالنقد والقرض على أنه **" تعتبر وسائل الدفع كل الأدوات التي تمكن من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل"**.

من خلال هاتين المادتين نجد بأن المشرع الجزائري قد عرف بطاقات ووسائل الدفع بصفة خاصة دون أن يعطي وسيلة بطاقة الائتمان الإلكترونية بتعريف عام، إلا انه يستشف من نص المادة 69 المذكورة أن المشرع في استعماله لعبارة ""**مهما يكون السند أو الأسلوب التقني المستعمل**"" قد اعتمد منهج الحياد أو التعادل التقني فاتحا المجال أمام ما يستجد من وسائل تكنولوجية حديثة منها بطاقة الائتمان الالكترونية و خير ما فعل، إنما تطور التكنولوجي و ثورة المعلومات ظهرت هذه البطاقة الائتمانية و ستظهر في المستقبل بطاقات أخرى.

أعطى المشرع الفرنسي كذلك تعريفا صريحا لبطاقة الائتمان في المادة 02 من القانون رقم 91-1382 : " أداة تصدر من إحدى مؤسسات الائتمان أو إحدى الجهات المنصوص عليها في المادة 02 من القانون 16/83 الصادر في 24 جانفي 1984 و أعاد نشاط رقابة مؤسسات الائتمان و تسمح لصاحبها أو حاملها بالوفاء أو تحويل النقود من حسابه".

2- يمكن تصنيف لبطاقات الائتمان من حيث مصدرها إلى **بطاقة الأمريكان اكسبريس**، تصدرها مؤسسات تحمل اسمها من بنوك أمريكان اكسبريس وهي عبارة عن مؤسسة مالية مركزها الولايات المتحدة الأمريكية. و**بطاقة الفيزا:** هذه البطاقة تصدرها مؤسسة لوس انجلوس بولاية كاليفورنيا بالولايات المتحدة الأمريكية وتصدر هذه المؤسسة من البطاقات البلاستيكية الالكترونية ثلاثة أنواع، وكل نوع بحسب المزايا التي تمنحها لصاحبها، كما تصنف بطاقات الائتمان الإلكترونية من حيث مضمونها وعملها إلى بطاقات سحب النقود، وبطاقات الوفاء والاستيفاء الفوري والمؤجل أما بطاقات الاستيفاء المؤجل تسمح للحامل بوفاء ثمن ما حصل عليه من سلع وخدمات، كما تصنف أيضا حسب النظم التكوينية لها إلى بطاقات ممغنطة تحتوي على شريط ممغنط يتم من خلاله إدخال وتخزين وتامين البيانات عليه ويكون ذا شفرة تتميز بها، ويتحقق الدفع بهذه البطاقة من خلال قراءة المعلومات الثابتة على الشريط، أما البطاقة الرقائقية فهي تحتوي على شريحة من السيليكون، تتضمن قيمة النقود في الحساب المصرفي لحاملها وتقوم بعمليات التحويل المصرفي للخصم، وإضافة من حسابات العميل بقيمة معاملته وهي بدورها ثلاثة أنواع بطاقة الذاكرة، البطاقة الذكية، والبطاقة

حالة قيام مصدر البطاقة ببرمجة الأجهزة الآلية المخصّصة لسحب النقد كي لا تتجاوز الحد المضمون في بطاقة أو ما تبقى فيه، ففي هذه الحالة لن يستطيع حامل البطاقة أن يسحب أكثر ما هو مضمون أو ما تبقى له في بطاقته من المال المضمون، وهنا لا يحاسب حامل البطاقة لأنها جريمة مستحيلة، و حالة عدم قيام مصدر البطاقة ببرمجة الأجهزة الآلية، وهنا قد يسحب حامل البطاقة رصيد يفوق ما هو مسموح به مع علمه بذلك أو فوق ما تبقى له من المال المضمون في فترة مدة الصلاحية.

الحادة الذكاء. راجع بخصوص ذلك: محمد نور الدين عبد المجيد، بطاقة الائتمان، النظام القانوني وآليات الحماية الجنائية، المؤسسة الحديثة للكتاب، لبنان، 2017، ص23.

[1]– تتميز بطاقات الائتمان الالكترونية عن غيرها من وسائل الدفع والوفاء الأخرى بالعديد من الخصائص وهي:

–**البطاقة أداة الائتمان:** بحيث أن مجرد الحصول على هذه البطاقة تعطي لحاملها التمتع بفترة ائتمان على مشترياته ويتحصل على خدمات دون القيام بالدفع الفوري للنقود، وهذا ما لا يوجد في أي وسيلة أخرى من وسائل الدفع التقليدية.

– **بطاقة الائتمان تقوم على علاقة ثلاثية الأطراف:** تقوم هذه البطاقة على ثلاثية الأطراف وهي مصدر البطاقة، الحامل، التاجر، والتي تختلف باختلاف الأحكام عن بعضها البعض فكل طرف من هذه الأطراف تترتب له حقوق وعليه التزامات فهذه العلاقات هي علاقة بين البنك مصدر البطاقة ومستخدمها المدين، العلاقة بين المدين والتاجر، العلاقة بين البنك والتاجر، فمثلا بإعتبار أن العلاقة بين مصدر البطاقة و حاملها إتفاق إذن يمكن أن نقول أنه عقد إذعان، أما العلاقة بين مصدر البطاقة(البنك) و التاجر هي علاقة تعاقدية تجارية.

العلاقة بين حامل البطاقة و التاجر يمكن عقد بيع، عقد إيجار، و أيضا هنا حامل البطاقة يحيل التاجر مباشرة إلى الجهة المصدرة للبطاقة ثم تخلق علاقة مديونية جديدة.

أما فيما يخص الطبيعة القانونية لبطاقة الإئتمان فهي طبيعة قانونية خاصة، حيث إختلف الفقه بين وكالة، حوالة حق، نقود ثم نقود إلكترونية، و عليه يمكن القول أن البطاقات بشكل عام نظام مصرفي تجاري جديد، أفرزته الثورة التكنولوجية المعلوماتية، و تم إكتشافها تجاريا لخدمة الإنسان و تأمين معاملاته التجارية لذلك لابد من إيجاد نظام قانوني خاص يحكم تلك المعاملات.

– **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. لتفصيل أكثر أنظر: كيلاني عبد الراضي محمود، النظام القانوني لبطاقات الائتمان، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة عين شمس، 1997، ص 143.

[2]– يتعدد مصدر البطاقات من المؤسسات المالية سواء أكانت بنوكًا أم هيئات أو المؤسسات مالية.

حالة قيام مصدر البطاقة برمجة الأجهزة الآلية مثل الحالة الأولى، لكن قد يصيب الجهاز عطل فيه أو كان هناك قصور في التعليمات المعطاة له فيتمكن حامل البطاقة من تجاوز السقف المسموح به حسب طلب الحامل[1].

وقد اختلفت الآراء حول تجريم هذا العمل، فهناك من اعتبر أن استعمال البطاقة في حالة السّحب يشكل جريمة سرقة مستندين بذلك الى العقد المبرم بين الطرفين والالتزامات المنبثقة عن العقد، و هناك من إعتبرها جريمة إختلاس بإعتبار أن المال يسلم للجاني و هو ما ينطبق على إستعمال البطاقة للسحب مع العلم أنها لا تتوفر على الرصيد الكافي.

لكن هذه الرأي انتقد، بحيث ذهب البعض إلى فكرة السرقة في حق حامل البطاقة وأساس ذلك هو أن هذا الفعل لا ينطوي على سرقة، لأنه من المستحيل في رأيهم أخذ المال دون رضاء المصرف مصدر البطاقة، إضافة إلى أن الأجهزة الإلكترونية لتوزيع الآلي لا تتفق مع القول بالسّرقة لأنها تستجيب لكل طلب مطابق للنظام المحدد سلفا من جانب المصرف، وبرجوع الى قانون العقوبات الجزائري نجد أن المادة 350 منه تنص على أنه كل من اختلس شيئا غير مملوك له يعد سارقا.

من خلال هذه المادة يتضح أن وصف عمل حامل البطاقة بالسرقة ليس صائبا، لأنه أخذ المال يرضى المجني عليه وبعلمه، ولأنه هو من اصدر البطاقة وخوّل لحاملها التصرف بالمال، وكذلك عند أخذه للمال فقد سلم له، وعليه أن انتفاء صفة الاختلاس عن العمل يعدم شرط النشاط الإجرامي للركن المادي، وبالتالي لا يمكن أن تقوم جريمة السرقة.

1-فاجي نهد، بن سليمان ربيحة، جرائم وسائل الدفع الالكتروني، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص قانون الأعمال ، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح ، ورقلة ، 2019-2020، ص 42-43.

ثانيا :الوفاء بقيمة البضائع والخدمات رغم النقص في الرصيد

تمنح بطاقة الائتمان لحاملها ميزة تسديد ثمن مشترياته عن طريق تحويل مبلغها من حسابه لحساب التاجر عن طريق البنك[1]، وفي هذه الحالة يقوم العميل باستخدام بطاقته، حيث يقدمها للتاجر بغية الحصول على خدماته على أن يقوم البنك لاحقا بتسديد قيمتها بناء على ما يوجد في رصيد الحامل شرط أن لا تتعدى هذه القيمة المبلغ الموجود في رصيد البطاقة وبعدها يقوم العميل بتسديد المبلغ للبنك لكنه يتجاوز سقف البطاقة.

واختلفت الآراء في حول ما كان هذا العمل يعتبر جريمة يخضع الجاني للمسائلة الجنائية ومنهم من رفض ذلك ، فمنه من يرى أن الحامل الذي يتحصل على المشتريات بالرغم من عدم وجود رصيد في بطاقته يوفي قيمتها، فانه يخضع للمسائلة الجزائية عن جريمة النصب، وهناك من يرى أنها إخلال بالتزامه تجاه البنك المتعامل معه ويترتب عليه المسؤولية العقدية لتعويض الضّرر[2].

الفرع الثاني

استخدام بطاقة الائتمان المنتهية الصلاحية

بطاقة الائتمان دائمًا مؤقتة، حيث يتوجب على العامل إرجاعها بعد انتهاء هذه المدة، لكن قد يتعمد الحامل إلى الاحتفاظ بها أو استخدامها بعد انتهاء مدتها، فملكية البطاقة تعود إلى الجهة المصدرة لها، هذه الأخيرة تقدم للعميل البطاقة لاستخدامها وفق

[1]– نقلا عن تشكل بطاقة الائتمان فائدة لجميع الأطراف، بحيث يستطيع الحامل 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 –امجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، الطبعة الأولى، دار المسيرة، الأردن، 2010، ص 130.

العقد المتفق عليه بين الطرفين يلزم العميل بإعادتها عند الانتهاء مدة الإعارة، فإن تخلف الحامل عن تنفيذ هذا الالتزام وقام باستخدام البطاقة يكون بذلك قد ارتكب جريمة إساءة الائتمان[1]، وذلك يكون إما باستخدام بطاقة الائتمان المنتهية الصلاحية للوفاء **(أولا)** أو باستخدامها لسحب النقود **(ثانيا)**.

أولا: استخدام بطاقة الائتمان المنتهية الصلاحية للوفاء.

يستخدم مالك البطاقة في الوفاء رغم انتهاء صلاحيتها، إن هو نسي تجديدها أو احتفظ بالبطاقة القديمة رغم تسليمه البطاقة الجديدة، وتعمد شراء السلع أو الخدمات بواسطتها، حتى يحتج فيها بعد على الوفاء للمصدر بأنه لم يقم باستخدامها، كما أن الحامل قد يستخدم البطاقة المنتهية الصلاحية بصورة غير مشروعة متى اتفق مع التاجر على قبولها في الوفاء إضرارا بالمصدر، كأن يقوم التاجر بتزوير تاريخ انتهاء صلاحية البطاقة عن طلب التفويض بالبيع من المصدر[2].

ثانيا: استخدام بطاقة الائتمان المنتهية الصلاحية لسحب النقود

الأصل العام وطبقا لنظام برمجة المستخدم في استخدام الملك الشرعي لبطاقته المنتهية الصلاحية انه تقوم آلة بابتلاع تلك البطاقة أو رفضها، حيث يعد إشعارا من البنك للقيام بتحديد تلك البطاقة إلا أنه في أحيانٍ أخرى يقوم الجهاز بصرف القيمة التي طلبها العميل، ويتم قيد المديونية عليه دون أن يعترض لأنه لم يقصد الغش[3].

1–مجدي محمود شهاب، فتوح الشاذلي، النظرية النقدية المؤسسات، دار الجامعية، بيروت، 1990، ص60.

2 –نضال سليم برهم، أحكام عقود التجارة الالكترونية ، الطبعة الثالثة ، دار الثقافة ، عمان، 2010 ، ص 155.

3–مونية معروف، جرائم بطاقات الائتمان الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي، 2021–2022 ، ص 40.

المطلب الثاني

استخدام بطاقة الائتمان الالكتروني الملغاة أو بعد التصريح بضياعها أو سرقتها(سابقا)

قد يلغي البنك المصدر بطاقة العميل لأي سبب من الأسباب مثل غلق الحساب أو تغيير نظام التعامل أو تغيير نوعية الخدمة التي تؤديها الخدمة، ومع ذلك فقد تظل البطاقة مع العميل وقد يستخدمها بعد إلغائها، حيث يتمادى مالك هذه البطاقة في استخدامها على الرغم من إلغائها إما في سحب النقود وإما في الوفاء بقيمة المشتريات والخدمات التي يحصل عليها **(الفرع الأول)** كما قد يستخدمها بعد الادعاء بضياعها أو سرقتها **(الفرع الثاني)** مما يجعل هذا التصرف يأخذ وصف جرائم مختلفة**(الفرع الثالث)**.

الفرع الأول

استخدام بطاقة الائتمان الملغاة

البطاقة الملغاة هي البطاقة التي يستمر الحامل باستخدامها بالرغم اقرار الجهة المصدرة لها أمر بإيقاف العمل بها نتيجة تعسفه في استعمالها بموجب الوظائف التي تمنحها له، سواء استخدمها لسحب النقود **(أولا)** أو لاستخدامها للوفاء **(ثانيا)**.

أولا: استخدام بطاقة الائتمان الملغاة لسحب النّقود

يتمّ استخدام البطاقة الملغاة في عملية السّحب، حيث يقوم الحامل باستعمال بطاقته الملغاة في سحب النقود من أجهزة الصرّاف الآلي، وفي هذه تم التساؤل هل يتم مساءلته جزائيا عن ذلك أم لا؟

اختلفت الآراء حول هذه المسالة، حيث يرى فريق بأن الفاعل يتم مسائلته جزائيا عن جريمة الاحتيال، في حين ذهب فريق آخر إلى القول بأن الفاعل يسأل عن جريمة

خيانة الأمانة [1]، إذا سحب النقود خطأ وهنا يكون الحامل لا يعلم بانتهاء صلاحيتها عندئذ تتم مساءلته جزائيا عن جريمة خيانة الأمانة ويخضع لأحكامها[2].

لكن، في الوقت الحالي ومع تطور التكنولوجي الحاصل في استحداث برمجة الصراف الآلي فقد أصبح هذا التصرف لا يشكل أي جريمة لأن تلك البرامج كفيلة باكتشاف ما إذا كانت هذه البطاقة صالحة للاستخدام أو أنها منتهية الصلاحية أم تم إلغائها من قبل مصدرها.

ويستنتج من ذلك أن تصرف الحامل المتماثل في استخدام البطاقة الملغاة في السحب لا ينطوي على أية جريمة وفقا للنصوص الجزائية الحالية.

ثانيا: استخدام بطاقة الائتمان المنتهية الصلاحية

تستخدم البطاقة الملغاة في عملية الوفاء أيضا لتسديد ثمن المشتريات، ومن المعلوم أنها تحمل ضمن البيانات الواردة عليها تاريخ انتهاء، لذلك وجب على التاجر أن يتحقق من مدة صلاحيتها ولا يقبلها، وإهماله لهذا الالتزام فانه يتحمل تبعات تصرفه ولا يستطيع مطالبة البنك بتسديد ثمن المشتريات[3].

واختلفت الآراء حول تكييف القانوني لهذه الواقعة بأن كانت جريمة أو لا، فالرأي الأول يرى أن الفاعل مرتكب الجريمة خيانة أمانة، وحجتهم في ذلك أن صاحب البطاقة استمر في استعمال بطاقته وامتنع عن ردها فيعتبر إساءة الأمين استعمال الشيء،إضافة

1–خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الالكتروني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للإعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية جامعة ام البواقي، سنة 2018 ، ص 16.

2 –المرجع نفسه، ص، 17.

3 –عبد الحليم بن مشري، " الحماية القانونية لبطاقات الدفع الإلكتروني"، **مجلة الإجتهاد القضائي**، المجلد 12، العدد 1، 2019، ص58.

لفعل الاختلاس أو التبديد المتمثل في نية الاستمرار في استعمال البطاقة على نحو يجرده من كل قيمته أو جزء منها.

لكن هذا رأي انتقد كون جريمة خيانة الأمانة هو أن يستعمل الجاني البطاقة استعمال لا يجوز أن يصدر من غير المالك ويظهر للناس على أنه هو المالك الحقيقي لشيء وهذا لا يتوفر في حامل البطاقة الملغاة أو منتهية الصلاحية، ومنه لا يعد مرتكبا لجريمة الخيانة[1].

أما الرأي الثاني يرى أن هذا الفعل يشكل احتيالاً لأنه يكون مصحوبا بأعمال احتيالية لإقناع التاجر بعدم إلغائها بهدف الحصول من البنك على الوفاء بقيمة مشترياته من التاجر، مما يشكل استيلاء على مال الغير، زيادة على ذلك فقد اعتمد الجاني على صفات كاذبة للحصول على هدفه لأن صفة حامل البطاقة كانت له ثم زالت عنه بإلغائها أو انتهاء صلاحيتها وادعائه بأنه وكيل عن شخص طبيعي أو معنوي وهذه الأساليب، مما تقوم عليها جريمة الاحتيال فبمجرد أن يقدم الجاني البطاقة للتاجر الذي لا يعلم بإلغائها ولم يتم إخطاره بذلك، فإنها تقوم جريمة الاحتيال القائمة على استعمال صفات كاذبة للحصول على أموال الغير.

في الأخير نشير إلى أنه حاليا لا يعد إستخدام البطاقة الملغاة جريمة كما كان في السابق.

ثالثا: حالة امتناع حامل البطاقة عن ردها بعد طلبها من المؤسسة المالية

تعتبر العلاقة ما بين العميل وبين البنك مصدر البطاقة الائتمانية هي علاقة تعاقدية، تبقى بطاقة الائتمان بموجبها ملكا لمصدرها أي البنك الذي يعهد إلى العميل استعمالها عند طلب البنك، ذلك بناء على عقد ساري المفعول ويمثل استخدام العميل

1 –عوض بدير الحداد، تسويق الخدمات المصرفية، البيان للطباعة والنشر، القاهرة، 1999، ص 20.

للبطاقة الائتمانية، بعد أن يتم الإعلان بسحبها وامتناعه عن ردها،ترديد الشيء ثم تسليمه على سبيل عارية الاستعمال.

يمكن القول بأن حامل بطاقة يعد مرتكبا لجريمة خيانة الأمانة إذ ما امتنع عن رد بطاقة الائتمان إلى البنك رغم ثبوت علمه بالإخطار المرسل إليه من طرف البنك بالرد، حيث تسلم هذه البطاقة إلى الحامل بموجب عقد الانضمام الذي يسمح له على سبيل عارية الاستعمال استخدامها وأعادتها بعد انتهاء العقد أو إلغائه، وتظلل بطاقة ملكا للجهة المصدرة وليس للحامل، وبيان ذلك بأن بطاقة الدفع تعد من كل طبيعة مادية وهو ما تقع عليه جريمة خيانة الأمانة [1]، وبالتالي احتفاظ الحامل ببطاقة الدفع بعد انتهاء مدة صلاحيتها أو فسخ العقد بينه وبين المصدر ورفضه ردها تعد جريمة خيانة الأمانة ويتعرض للعقوبات المنصوص عليها في المادة 376 من قانون العقوبات.

الفرع الثاني

استخدام بطاقة الائتمان بعد الإدعاء من صاحبها بضياعها أو سرقتها

يقوم صاحب البطاقة بإبلاغ الجهة المصدرة لها عن فقدانه لهذه البطاقة أو سرقتها في الوقت الذي لا تزال في حوزته وهو يستمر باستعمالها في السحب أو الوفاء، فإذا استعملها في عملية السحب، فإن أجهزة الصراف الآلي الحديثة مبرمجة لرفض البطاقة المفقودة أو المسروقة، وإذا استعملها في الوفاء فإن الحامل وخوفا من اكتشاف أمره يقوم باستخدامها عند التجار الذين يتعاملون بآلة الطباعة اليدوية، التي لا يمكن اكتشاف وضعية البطاقة من خلالها إن كانت ضائعة أو مسروقة، على العكس التجار الذين يستعملون الجهاز الالكتروني pos و هو تطبيق مخصص لأماكن العمل المشتركة التي

1-فتيحة يزيد، رشى جدة لنظام القانوني لوسائل الدفع الالكتروني في الجزائر، مذكرة لنيل شهادة الماستر في العلوم القانونية، تخصص قانون أعمال، كلية الحقوق و العلوم السياسية، جامعة أكلي محند ألحاج، البويرة، 2020-2021 ، ص 49.

تحصل قيمة مبيعاتها و يقوم أيضا باكتشاف حالات الغش بسهولة وهذا يشكل احتيال على التاجر، الغرض منه تحصيل قيمة البضاعة من البنك بدلا منه والاستيلاء على مال البنك دون وجه حق[1].

الفرع الثالث

أركان جرائم بطاقات الائتمان الصّادرة عن صاحب البطاقة

قد يسيء الحامل الشّرعي إستخدام بطاقة الائتمان الإلكترونية كأن يستعملها في غير الحدود المصرح له به رغم صلاحيتها، وهو ما يشكل جريمة السرقة **(أولا)** أو يستعملها وهي منتهية الصلاحية مما يشكل جريمة خيانة الأمانة، كما قد يمتنع عن ردّها، وبحكم أن هذه التصرفات الصادرة عنه تعتبر جريمة فلابد من تبيان أركان هذه الجرائم **(ثانيا)**.

أولا: طبيعة جريمة سوء استخدام بطاقة الائتمان رغم صلاحيتها

تأخذ وصف هذا السلوك بجريمة السرقة التي تظهر أركانها حسب مقتضيات نصّ المادة 350 من قانون العقوبات في ما يلي:

1- الركن المادي: وهو السلوك الإجرامي الذي يتخذه صاحب البطاقة والمتمثل في فعل الاختلاس للبطاقة والاستيلاء عليها واستعمالها رغم الإدعاء بسرقتها أو ضياعها أمام السلطات المختصة.

2-الركن المعنوي: يتمثل في العلم والإرادة.

يقصد به أن يعلم صاحب البطاقة بأن السلوك الذي قام به هو سلوك إجرامي ومعاقب عليه قانونا، ومع ذلك تتجه إرادته إلى القيام به.

---

1 -الشكري عادل يوسف، "الحماية الجنائية لبطاقات الدفع الإلكتروني"، **مجلة مركز دراسات الكوفة**، العراق، العدد11، 2011، ص93.

3- الركن الشّرعي: تظهر في نص المادة 350 من قانون العقوبات الجزائري المعدل والمتمم.

ثانيا: طبيعة جريمة استخدام بطاقة الائتمان المنتهية الصلاحية أو الملغاة

قد يقوم صاحب البطاقة باستعمال بطاقة الائتمان رغم انتهاء مدة صلاحيتها وذلك في الوقت الذي يجب عليه ردها إلى السلطة المختصة، ففي هذه تشكل جريمة خيانة الأمانة، وذلك عملا بنصّ المادة 376 من قانون العقوبات والتي تظهر أركانها في :

1-الركن المادي: يتمثل في عدم قيام صاحب البطاقة بردها إلى السلطة المختصة وهي مركز البريد واستعماله لها دون وجه حق.

2- الركن المعنوي: يظهر في علمه بسلوكه الإجرامي وغير الشرعي واتجاه إرادته إلى ارتكابه وقصده في الاحتفاظ بالبطاقة رغم انتهاء صلاحيتها أو إلغائها ورغم إخطاره بردها.

ج- الركن الشرعي: تجد هذه الجريمة سندها القانوني في نص المادة 376 من قانون العقوبات.

كما قد تعتبر جريمة نصب حسب نص المادة 372 من قانون ذاته التي جاء فيها على**"أنه كل من توصل إلى استلام أو تلاقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك باحتيال لسلب كل ثروات الغير أو بعضها أو الشروع فيه إما باستعمال أسماء وبصفة كاذبة وسلطة خيالية واعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أي واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب الحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 الى 20000 دينار جزائري"**، وعليه فان أركان هذه الجريمة تتمثل في:

1- الركن المادي: تقوم جريمة النصب عندما يقدم الحامل للبطاقة للتاجر وهو يعلم بانتهاء مدة صلاحيتها أو بإلغائها لشراء احتياجاته، يعتبر كاذبا وغشاشا ومجرد تقديمه للبطاقة وإبرازه لها، فهي وسيلة احتيالية لايهام التاجر أن البطاقة مازالت سارية وأن الائتمان الممنوح له مازال ساريا وأن مجرد تسليم التاجر المشتريات للحامل يعتبر ذلك استيلاء على المال مستخدما في ذلك الوسائل الاحتيالية.

ب الركن المعنوي: يتمثل في القصد العام وهو علم الحامل وقت ارتكاب الفعل بأنه يستعمل طرق احتيالية من أجل الاستيلاء على مال منقول مملوك للغير، حيث أنه كان يعلم بأنه ليس له الحق في استخدام البطاقة لانتهاء مدتها أو إلغائها، حيث كان يقصد من ذلك الاستيلاء على مال التاجر دون وجه حق.

المبحث الثاني

استخدام بطاقة الدفع الالكتروني من قبل غير المشروع

بما أن البطاقات الإلكترونية وسيلة جديدة سهلت على الأفراد تعاملاتهم التجارية، الأمر الذي جعل العديد من الأشخاص يستهويهم التلاعب بها بمختلف أشكالها من السرقة و التزوير، وتعد سرقة البطاقة الإلكترونية من أخطر التحايلات التي يقوم بها الغير، و يقصد بالغير من لم تصدر البطاقة باسمه من الجهة المختصة بإصدارها، و هذا الأخير قد يستخدم البطاقة المسروقة أو المفقودة (**المطلب الأول)** كما قد يقوم بتزويرها (**المطلب الثاني)**.

المطلب الأول

الاستخدام غير المشروع لبطاقة مفقودة أو مسروقة

باعتبار أن البطاقة الائتمانية محل الحقوق مالية فقد تقع عليها العديد من الاعتداءات، كسرقة البطاقة عن طريق حاملها بصورة مباشرة قصد استعمالها لسحب النقود **(الفرع الأول)** أو عدم استعملها ورغم ذلك تعد جريمة السرقة لمجرد توافر أركانها **(الفرع الثاني)**.

الفرع الأول

استخدام البطاقة المفقودة أو المسروقة في سحب النقود

وتتمثل هذه الحالة في قيام شخص قام بسرقة هذه البطاقة الإلكترونية من مالكها الشرعي أو قيامه بالعثور عليها في حالة فقدها من مالكها الأصلي، باستعمالها في الحصول على بضائع أو خدمات من التجار سواء كانت السرقة حقيقية أو صورية.

ويقصد بالسرقة الحقيقية امتناع السارق أو من عثر على البطاقة المفقودة عن ردها إلى صاحبها الشرعي أو إلى البنك أو المؤسسة المالية المصدرة لها، بل يقوم باستعمالها

في سحب مبالغ نقدية أو شراء بضائع وخدمات وذلك قبل قيام الحامل الشرعي للبطاقة بإخطار البنك عن سرقتها أو فقدانها في قائمة المعارضات، ومن ثم إعادة برمجة جهاز السحب النقدي حتى لا يقبل البطاقة عند استعمالها في سحب غير مشروع قبل المعارضة فيها.

أما السرقة الصورية فيقصد بها أن تكون البطاقة الإلكترونية بحوزة الحامل الشرعي لها، أي بمعنى أنها لم تسرق أو تفقد، ويقوم بالإجراءات اللازمة في حالة الفقدان أو السرقة بإخطار البنك أو المعارضة فيها، ومع ذلك يستمر في استخدامها في سحب النقود من جهاز السحب النقدي الآلي، الأمر الذي يعكس إساءة في استعمال هذه البطاقة.

وقد اختلف الفقه والقضاء في تحديد التكييف القانوني لجريمة إساءة استعمال البطاقة من قبل الغير ما بين جريمة النصب والاحتيال أو الشروع فيها أو جريمة السرقة.

حيث يذهب جانب من الفقه الفرنسي مؤيدا ببعض الأحكام القضائية، إلى أن هذا السلوك من قبل الجاني ينطوي على جريمة نصب، على اعتبار أن المتهم قد انتحل اسما كاذبا ومن ثم يكون قد استخدم وسيلة احتيالية لإقناع المجني عليه بوجود انتمان.

في حين يذهب جانب آخر من الفقه إلى أن هذا الفعل يشكل جريمة سرقة باستخدام مفتاح مصطنع على اعتبار أن البطاقة الإلكترونية تعد من قبيل المفاتيح المصطنعة، ويسندنها الرأي على أن المادة (2/317) من قانون العقوبات المصري[1] والمادة (397) من قانون العقوبات الفرنسي[2] لم تحدد على وجه الدقة ماهية هذا المفتاح المصطنع

1- المادة 2/317 من القانون رقم 95-03 لسنة 2003، المتضمن قانون العقوبات المصري، المعدل و المتمم لقانون رقم 58-37 لسنة 1937.

2- المادة 397 من القانون رقم 92-683 المتضمن قانون العقوبات الفرنسي.

وبالتالي لا ضير من اللجوء إلى العرف واللغة الدارجة التي تعتبر من قبيل المفتاح كل شيء يستخدم في فتح قفل أو فتح جهاز مغلق[1].

الفرع الثاني

استخدام البطاقة المسروقة أو المفقودة كأداة للوفاء

يتم استعمال هذه البطاقة في حالة للوفاء بواسطتها لدى التجار، حيث لا يقتضي الأمر معرفة الرقم السري للبطاقة، بل تتم المعاملة بتوقيع حامل البطاقة على فاتورة البيع ويساهم في تسهيل استعمال البطاقة على نحو كبير صعوبة تحقق التاجر من شخصية حامل البطاقة، كما أن التحقق من أن البطاقة تم إيقافها لا يتحقق إلا بعد اطلاع على القائمة السوداء التي تحتوي على بيان البطاقات الموقوفة، والتي قد لا تكون البطاقة قد أدرجت بها ومن ناحية أخرى، لأنه لا يمكن اكتشاف تزوير التوقيع المدوّن على البطاقة مع توقيع فاتورة البيع لعدم مضاهاتهم من الناحية العملية و ذلك بسبب التدرب المستمر عليه ومن ناحية عدم خبرة البائع في هذا المجال[2].

المطلب الثاني

تزوير بطاقة الائتمان من قبل الغير

يحدث أن تسرق البطاقة من العميل ويلتقطها الغير، حيث يقوم باستبدال ما بها من بيانات ومعلومات تمهيدًا لاستخدامها في السّحب أو الشّراء، وبذلك يشكل هذا الفعل اعتداء مزدوج على الحامل الذي فقدت منه البطاقة وعلى البنك معا، الأمر الذي يعتبره جمهور الفقهاء جريمة تزوير على أساس أن تزوير هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد أثباتها بالصّك أو مخطوط يحتج به أو يمكن أن ينجم عنه ضرر

1- مونية معروف، جرائم بطاقات الائتمان الالكترونية، مرجع سابق، ص44.

2 - مونية معروف، جرائم بطاقات الائتمان الالكترونية، مرجع سابق، ص 45.

مادي أو معنوي أو اجتماعي وللتزوير أساليب تستعمل على بطاقات الائتمان مباشرة(**الفرع الأول**) أو على المستندات والإشعارات الخاصة بها (**الفرع الثاني**).

الفرع الأول

أساليب تزوير بطاقة الدفع الالكتروني

لا تقتصر المسؤولية عن استعمال وسائل الدفع الالكتروني بطريقة غير شرعية أو غير مسموح بها على حالات استعمالها بعد سرقتها أو بعد التقاطها عقب ضياعها، بل أن هناك شكلا آخر لهذا الاستعمال فقد يحصل أن يتم تزوير أو تقليد وسائل الدفع الالكتروني أي أن هذه البطاقة ليست سليمة من الناحية القانونية، صنف خبراء الكشف عن التزويرإلى أسلوبين هما أسلوب التزوير الكلي للبطاقة (**أولا**) وأسلوب التزوير الجزئي للبطاقة (**ثانيا**).

أولا: التزوير الكلي للبطاقة الائتمان

يتم التزوير[1] باصطناع بطاقة كاملة ثم تقليد الرسوم الخاصة على جسم البطاقة وتغليفها وعلى الشريط الممغنط وشريط التوقيع كل حسب مكانه، ثم القيام بالطباعة النافرة وتشغيلها بواسطة إشباعها بالمعلومات التي حصل عليها المزورون من البطاقة الصحيحة.

وبعد ذلك يتم استخدامها في عمليات الشراء، وفي حالة ما إذا تحصل المزور على الرقم السّري لبطاقة ما، فانه يقوم باستغلالها بالصنع بطاقة بلاستيكية فارغة من البيانات ويلصق عليها الشريط الممغنط ونسخ بيانات صاحب هذه البطاقة، ومن ثم يقوم

[1]– يقصد بـ "**التزوير**" التغيير في البيانات التي تشمل عليها وسائل الدفع سواء نال هذا التغيير الأرقام الموجودة عليها أو الإمضاءات أو اسم حاملها، أو أي تغيير ينال المعطيات الالكترونية لها، كما يعرف على انه تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر محتمل بنية استعمال المحرر المزور فيما أعد له. لتفصل أكثر راجع: حسين محمد الشبلي، مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية ، دار مجدلاوي للنشر والتوزيع، عمان، 2009، ص 58.

باستخراج نسخ عديدة منها لاستخدامها في الحصول على الأموال من أجهزة الصراف الآلي، كذلك قد يتم تزوير الكلي عن طريق سرقة بطاقات كاملة التجهيز من المؤسسات المصدرة لها عن طريق شركاء بداخل المؤسسات أو المصارف ثم بيعها أو تزويرها، كما قد يتم اخذ البيانات من قوائم حجوزات الفنادق وكالات السّفر ومن الفواتير التي تم رميها[1].

ثانيا: التزوير الجزئي للبطاقة الائتمان

يتم استغلال جسم البطاقة الحقيقي في هذه الحالة وما تحمله من رسوم خاصة وحروف بارزة، وكذلك من كتابات أمنية بغرض تزويرها بواسطة صهر ما عليها من أرقام بارزه لبطاقة صحيحة انتهت فترة صلاحيتها أو إعادة قولبت رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر يتم الحصول عليها بطرق تم ذكرها، كما قد يتم محي ما على الشريط الممغنط من بيانات وإعادة برمجته بمعلومات صحيحة تمت سرقتها أو كشف شريط التوقيع ووضع شريط توقيع آخر[2].

ضمن أهم الظواهر الدالة على التزوير الجزئي الذي يقع على بطاقة الدفع الالكتروني ما يلي:

– انهيار بعض مواضع من شريط التوقيع وإمكانية ظهور سطح البطاقة أسفل مواضيع الانهيار نتيجة للمحو الآلي.

– ظهور بقع قاتمة أو بنية أو مصفرة اللون بأرضية شريط التوقيع نتيجة للمحو الكيميائي.

---

1 – امجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، مرجع سابق، 2010 ، ص157.

2 – صونية مقري، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية قسم الحقوق، 2015 ، ص 131.

– وجود تسلخات أو بقعة سوداء في المواضيع المحيطة بالكتابات أو عدم انتظام الرؤوس البارزة للطباعة.

– تعرض شريط التوقيع للكشط المادي ثم لصق شريط آخر في مكان، مما يجعل تموضع الشريط المصطنع يفتقر إلى الدقة والثبات ويظهر خدوش واتساخ يدل على ذلك، كما قد يظهر أيضا سيلان للمادة اللاصقة في مواضيع حول الشريط المصطنع.

– عدم التطابق بين البيانات المشفرة على الشريط والبيانات المقروءة بصريا.

– وجود تقطعات أو تشوهات أو زيادة في السمك أو الرتوش بالمساحة التي بها صورة العميل بظهر أو بوجه البطاقة.

– احتمالية عدم التوافق في العلاقات الترابطية التي تنظم وتميز إصدار البطاقة الصحيحة.

– يغلب على البطاقة المزيفة تزييفا جزئيا إهمال طلاء الرؤوس البارزة لرموز الطباعة النافرة بها[1].

الفرع الثاني

تزوير الإشعارات والمستندات الخاصة ببطاقة الائتمان

يأخذ تزوير الإشعارات في هذه الحالة عدة صور تلاعب موظف البنك المصدر للبطاقة بإشعارات بطاقة الائتمان **(أولا)** تواطؤ حامل البطاقة مع التاجر**(ثانيا)** تزوير الإشعارات تزوير الإشعارات والفواتير الناتجة عن عمليو البيع **(ثالثا)** تلاعب التاجر في ماكينات البيع الالكترونية **(رابعا)** إصدار بطاقات صحيحة بمستندات المزورة **(خامسا)**.

1 – بوجمعة شهرزاد، عيشاوي أمال، " مظاهر الحماية القانونية لوسائل الدفع الإلكتروني في التشريع الجزائري"، **مجلة البحوث والدراسات القانونية والسياسية**، المجلد 11، العدد 2، 2018، ص 192.

أولا: تلاعب موظف البنك المصدر للبطاقة بإشعارات بطاقة الائتمان

وذلك باتفاق الموظف مع التاجر بتجاوز حد السحب في صرف قيمة إشعارات البيع من بطاقة مزورة آو منتهية الصلاحية أو أن يختلس موظف البنك مبالغ نقدية عندما يقوم حامل البطاقة بسحب أو الإيداع، فيقوم بتزوير المبلغ ويأخذ الفارق لنفسه[1].

ثانيا: تواطؤ حامل البطاقة مع التاجر

ويتم ذلك من خلال قيام حامل البطاقة بإجراء عمليات شراء وهمية بالاتفاق مع التاجر مقابل نسبية من قيمة الفاتورة يحصل عليها التاجر[2].

ثالثا: 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].

رابعا: تلاعب التاجر في ماكينات البيع الالكترونية

وذلك باستغلال 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[4].

خامسا: إصدار بطاقات صحيحة بمستندات المزورة

يقوم المحتالون بالاستعانة بمسندات إثبات شخصية مزورة للحصول على بطاقات بأسماء منتحلة وعناوين وهمية وعادة ما يلجأ محترف هذا النوع من الجرائم إلى استهداف

1- خولة بوقديرة، المرجع السابق، ص 22.

2 -حسين محمد الشبلي مهند فايز الدويكات، المرجع السابق، ص 69.

3- أحمد حمدان الجهني، المرجع السابق، ص 189.

4- عبد الكريم الردايدة، المرجع السابق، ص 65.

أكثر من بنك لإصدار عدة بطاقات لتحقيق أكبر عائد ممكن مستغلين ضعف وخبرة بعض موظفين البنك في كشف تزوير المستندات والوثائق[1].

الفرع الثالث

أركان جرائم استخدام البطاقة الالكترونية من قبل الغير

يتجلى الاستخدام غير المشروع لبطاقة الإلكترونية من قبل الغير إما عن طريق سرقتها من حاملها الشرعي وهو ما يشكل جريمة السرقة قائمة الأركان **(أولا)** أو بتزويرها ومن ثمة تأخذ وصف جريمة التزوير **(ثانيا)** .

أولا: أركان جريمة سرقة البطاقة الالكترونية من حاملها الشرعي

تتمثل أركان جريمة السرقة في:

1- الركن المادي: يتمثل في اختلاس البطاقة بالاطلاع على بطاقة الحامل الشرعي وإخراجها من حيازته بدون رضاه مع اتجاه نيته إلى تملكها أما محل الجريمة هو بطاقة الائتمان وهي تعتبر من المنقولات يمكن أن ترد عليها السرقة فالبطاقة مال منقول مملوك للغير[2].

2- الركن المعنوي:يتمثل في العالم والإرادة، وهو أن يعلم السارق للبطاقة بأن المال المسروق هو ملك للغير ومع ذلك تتجه إرادته إلى القيام بالفعل، وعلى ذلك إذا قام شخص بالاستيلاء على البطاقة وكان الهدف الرئيسي من وراء ذلك تملك البطاقة، فانه يسال في هذه الحالة عن جريمة السرقة المنصوص عليها في المادة 350 من قانون العقوبات الجزائري وذلك بالحبس من سنة إلى خمس سنوات وغرامة مالية من 100,000 إلى 500,000 دينار جزائري.

---

1 – المرجع نفسه، ص 70.

1– باريش أسيا ، مرجع سابق، ص69.

ثانيا : أركان جريمة تزوير الغير للبطاقة الالكترونية

قد تتعرض بطاقات الإلكترونية كغيرها من المحررات أو المستندات إلى التزوير بمختلف إشكاله، والذي يعد من اخطر الاستعمالات غير المشروعة الواقعة على البطاقة وعليه يعتبر هذا التصرف جريمة حسب نص المادة 219 من قانون العقوبات الجزائري التي جاء فيه **" أنه كل من ارتكب تزويرا بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو المصرفية أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500 إلى 20,000 دينار"**

فحسب هذه المادة فإن جريمة التزوير تقوم على ركنين احدهما معنوي والأخر مادي.

1- الركن المادي: يتمثل في العلم بنية الغش وتغيير الحقيقة وكذا نية استعمال المحرر المزور في مزوره من اجله.

2- الركن المعنوي:يتكون من أربعة عناصر: تغيير الحقيقة في المحرر بصورة من الصور التي نص عليها القانون في المادة 216 أن يكون من شأن التغيير إحداث ضرر للغير.

يقصد بتغيير الحقيقة استبدالها بما يغيرها ويخالفها، فلا يمكن تصور وقوع التغيير إلا باستبدال الحقيقة ولكن يعتبر تغيير تزويرا ويشترط فيه أن لا يعدم ذاتية المحرر أو قيمته، كمحو كل الكتابة التي في المحرر أو شطبها بحيث تصبح غير مقروءة وتقوم جريمة التزوير بتغيير الحقيقة سواء كانت تغيير كليا أو جزئيا[1] غير أن هذا التغيير لا يقصد منه التغيير المطلق للحقيقة وإنما تغيير الحقيقة القانونية هذا ويتحقق التغيير في الحقيقة في تزوير البطاقة الائتمانية سواء بتقليد بطاقة صحيحة أو بتغيير بعض بياناتها الجوهرية[2].

1- باريش أسيا، المرجع السابق، ص 71.

1- معروف مونية ، المرجع السابق ، ص70-71.

الفصل الثاني

آليات حماية بطاقة الائتمان من الاستعمال غير القانوني

تشكل الاعتداءات على البطاقات الإئتمانية خطورة بالغة لما تسببه من خسائر في مجال التعاملات المالية، خاصة وأن هذه الجرائم ذات طبيعة تقنية، لكونها ترتبط بأجهزة الكترونية، لذلك نجد أن مرتكبي هذه الجرائم يتصفون بالفطنة والذكاء في هذا المجال وعليه استوجب تبني إستراتيجية فعالة لمكافحة هذا النوع من الجرائم وردعها وردع مرتكبيها.

ولأن جرائم البطاقات الإلكترونية تمتاز بالحداثة، فهي تفتقد الى قوانين خاصة بها تكون كفيلة بالحد من وقوعها مما دفع إلى اتخاذ إجراءات خاصة بذلك سواء على المستوى المحلي من خلال تبني أطراف العلاقة التعاقدية إجراءات كفيلة لحماية حقوقهم ودوام الثقة في تعاملاتهم، أو على مستوى الأجهزة الأمنية المختصة في مكافحة هذه الجرائم، ومن جهة أخرى على الصعيد الدولي، حيث يجب تفعيل آليات كفيلة بمحاربة هذه الجرائم ومتابعة مرتكبيها من خلال هذا الفصل سنتناول الإجراءات الوقائية لمواجهة جرائم الاستعمال غير القانوني لبطاقة الائتمان **(المبحث الأول)** والإجراءات الردعية لمواجهة جرائم الاستعمال غير القانوني لبطاقة الائتمان **(المبحث الثاني)**.

المبحث الأول

الآليات الوقائية للحدّ من استعمال غير القانوني لبطاقة الائتمان

من أجل المحافظة على سلامة وأمن المعاملات البنكية والمصرفية، كان من المفروض وضع إجراءات وقائية من قبل جهات مختلفة سواء الجهات المصدرة للبطاقة أو الجهات المتعاملة بها(**المطلب الأول**) ، إضافة إلى الأجهزة الردعية المختصة في الجرائم الالكترونية(**المطلب الثاني**) .

المطلب الأول

الآليات الوقائية لمواجهة جرائم الاستعمال غير القانوني لبطاقة الائتمان

أمام تزايد عمليات الإستخدام غير المشروعة لبطاقة الائتمان الالكترونية وجب اتباع مجموعة من الإجراءات والأساليب سواء من قبل مصدر البطاقة **(الفرع الأول)** أو من قبل صاحبها وذلك من أجل مواجهة هذه الجرائم والحد من المخاطر التي تنجم عنها(**الفرع الثاني**).

الفرع الأول

الإجراءات الواجب اتخاذها من مصدر بطاقة الائتمان

إن حماية البطاقة من التلاعب والحدّ من الاستخدام غير المشروع لها من واجب الجهة المصدرة لها الذي يقع عليها عبء توفير أكبر قدر ممكن من الحماية للبطاقة التي يصدرها إما بتطور البطاقة تقنيا **(أولا)** من أجل الحد من عمليات تزويرها أو القيام بعدد من الإجراءات الإدارية والمصرفية التي من شأنها المساهمة في مواجهة الاستخدامات غير المشروعة لها(**ثانيا**).

أولا : الإجراءات التقنية

تعد الإجراءات التقنية المتخذة لمواجهة اساءة استخدام بطاقة الائتمان الإلكترونية أولى حلقات هذا التطوير كان باختراع بطاقة دوائر الكترونية من أنها غير قابلة للتأثير عليها أو اختراقها وتحتفظ في ذاكرتها بآخر العمليات المنفذة وتعد من الناحية التقنية غير قابلة للتزوير ومثالها صورة الحمامة في بطاقة فيزا.

ومن بين الإجراءات التقنية التي خصّصت أيضا لمواجهة إساءة استخدام البطاقة نجد الانترنت النموذج التقني الموحد الذي أعلنت عنه شركتي فيزا وماستر كارد والمسمى بـ**"نظام الصفقات الالكترونية الآمنة"**، ومن بعد ذلك انضمام العديد من الشركات الأمريكية له[1].

كما تتأهب حاليا شركات أمريكية أخرى لاستعمال تقنية أمنية جديدة، ومن الشركات العربية التي ساهمت في إطلاق بطاقة آمنة لتسوق عبر الانترنت شركة "**مكتوب دوت كوم**"، حيث أعلنت هذه الأخيرة عن إصدار بطاقة "**كاشيو**" التي تمكن الحامل من شراء السلع والخدمات على شبكة الانترنت بثقة تامة دون أية مخاطر ممكنة، وهي متوفر بثلاثة فئات 10 دولارات أمريكية،20 دولارا أمريكيا، 30 دولارا أمريكيا[2].

كما توجد إجراءات تقنية اتخذت من طرف البنوك لمواجهة مخاطر البطاقات الالكترونية، وذلك بتطبيقها على الحواسيب الآلية وذلك بهدف الكشف المبكر عن أي عملية مشبوهة ولعل أهم هذه الإجراءات هي:

– التحديث الدائم والمتجدد للشفرة البطاقات الالكترونية حتى يصعب على المحتالين التعارف عليها واستحداث تقنيات للتعرف على هوية صاحب البطاقة الأصلي، كإدخال

1 - فتيحة زيد، رشى جدة، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر، مرجع سابق، ص 23.

2 -معروف صونية، جرائم بطاقات الائتمان الالكترونية، مرجع سابق، ص 18.

صورته في البطاقة وتأمينها، بحيث يصعب إزالتها وتزويرها واستخدام بصمات الصوت والعين والأصابع.

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

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

– استخدام كلمات سرية معقدة للدخول إلى الأنظمة الإلكترونية، بحيث تكون مزيج من الأرقام والحروف يصعب على الغير التخمين فيها[1].

ثانيا : الإجراءات الإدارية المصرفية

تتمثل الإجراءات الإدارية في تعيين حد أقصى لاستخدام البطاقة الالكترونية أو سحبها أو المعارضة في قبولها وسنبين هذا فيما يلي:

1– تحديد سقف لعمليات السّحب بالبطاقة

الأصل أن يتم تحديد سقف للبطاقة، بحيث لا يمكن تجاوزه واستثناء قد يسمح بذلك في حالات معينة والهدف من ذلك منع إفراط صاحب البطاقة في استعماله خوفا من عدم إيفائه بمصاريف المشتريات المترتبة عليه بتاريخ تسويتها المتفق عليه مع البنك ولذلك وجب تحديد سقف لاستخدام البطاقة، حيث يكون هذا التحديد سواء عند استعمالها في عملية السحب أو الوفاء على حد سواء[2].

أ– **الحد الأقصى في استخدام البطاقة في الوفاء:** نميز في هذا الصّدد بين حالتين:

1 -علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكترونية، الطبعة الأولى، دار المؤسسة الحديثة للكتاب، لبنان، 2011، ص 82

2– خولة بوقديرة، المرجع السابق، ص 58.

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

عند استخدام البطاقة في الجهاز الالكتروني وخلال تمرير البطاقة في الجهاز يظهر على الشاشة ما إذا كانت تحتوي على رصيد كافي لإتمام عملية الوفاء أم لا، فإذا تجاوز حد الرصيد يرفض الجهاز إتمام هذه العملية إلا بعد حصول التاجر على تفويض من مصدر البطاقة بالموافقة[1].

ب- الحد الأقصى لاستخدام البطاقة في السحب: يتم تحديد السقف الأقصى للبطاقة عند السحب من أجهزة الصراف الآلية حسب المبلغ المسموح به من الرصيد، ففي بطاقات الدفع العادية يكون نصف سقف البطاقة وفي البطاقات التي تستخدم في الوفاء يكون نفس الرصيد المتوفر في الحساب وفي حالة السحب اليومي، فإن الحد الأقصى لسحب يختلف من بنك لآخر حسب التسهيلات التي يمنحها كل بنك لعملائه.

2-سحب البطاقة: قد يتم سحب البطاقة من طرف المصدر أو من طرف التاجر من أجل الحفاظ على حقوق جميع الأطراف ومنع التجاوزات التي قد تتم عن طريق البطاقة، وما يهمنا في هذا الفرع هو سحب البطاقة من طرف المصدر، بحيث للبنك الحق في استرجاع البطاقة من صاحبها بالنص على ذلك في العقد وذلك بأن البطاقة ملك لمصدر البطاقة، حيث يستطيع هذا الأخير الطلب من صاحبها إعادتها إليه أو إلغائها وهذه العملية قانونية إذا كانت ناتجة عن أسباب جوهرية ويخشى بقائها عند صاحبها،أما إذا انعدمت هذه الأسباب فهذا يعتبر تعسف من قبل مصدر البطاقة ووجب التعويض عنها

1 - خولة بوقديرة، الجرائم على بطاقات الدفع الالكتروني، مرجع سابق، ص 60.

ويكون هذا السحب سواء بالطريقة العادية عندما يطلب المصدر إرجاع البطاقة وقد يكون بطريقة فنية في حالة برمجة الصراف الآلي على سحبها[1].

الفرع الثاني

الإجراءات المتّخذة من قبل صاحب البطاقة

لا يقتصر إجراءات الحد من الجرائم الواقعة على البطاقات الإلكترونية على الجهات المصدرة لها فقط، بل يمتد ليشمل الحامل، الذي عليه اتّخاذ الاحتياطات اللازمة لتفادي وقوع بطاقته في يد الغير ومن ثم التّلاعب بحيث يقوم صاحب هذه البطاقة بمجموعة من التدابير والإجراءات الوقائية للمحافظة على البطاقة وحمايتها من كل أشكال الجرائم المنفذة عليها، وتتجلى هذه الإجراءات في حماية البطاقة والمحافظة على بياناتها **(أولا)** وكذا حماية البطاقة من خلال المعاملات التجارية **(ثانيا)**.

أولا : حماية البطاقة والمحافظة على بياناتها

يتم ذلك من خلال عدم إهمال البطاقة والحرص على وضعها في مكان آمن، وألا يتركها عند أيّ شخص إلا بعد التأكد من هويته، حتى إذا كانت موظف البنك نفسه أو ضابط شرطة، كما يجب عليه عدم الإفصاح عن رقم البطاقة أمام الغير أو كتابته على وجه البطاقة أو على أي ورقة مكشوفة وغيرها من الأشكال الأخرى ، وأن يتلف الوصل في حالة طلبه من الصراف لأنه يحتوي على رقمه، كما يجب عليه عند تشكيل رقم السري للبطاقة أن يختار أرقاما وحروفا يصعب اكتشافها[2].

وفي حال ضياع البطاقة ورقمها السرّي يجب على صاحبها الإبلاغ الفوري عن ذلك للجهة المصدرة لها التي تقوم بإلغائها بناء على هذا البلاغ، إضافة إلى ذلك يجب على

1 - امجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، الطبعة الأولى، دار المسيرة، الأردن، 2010، ص 117.

2 -عبد الكريم الردايدة، جرائم بطاقات الائتمان دراسة تطبيقية ميدانية، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013، ص 188.

صاحب البطاقة إبلاغ الجهة المصدرة أيضا في حال اكتشاف وجود جهات لم يتعامل معها من خلال وصل كشوف حساب البطاقة، حيث تقوم الجهة المصدرة بالتحقق من هوية هذه الجهات التي استخدمت البطاقة دون علم صاحبها.

كما يجب على صاحب البطاقة أن يحرص على عدم شحن رصيد بطاقته بمبالغ كبيرة ليتجنب خسارة أكبر إذا تمّ استخدامها من قبل الغير، كذلك عند تعامله عليه أن لا يطلب مساعدة الغير وإذا لاحظ أن هناك من يراقبه أثناء إجراء عمليته المصرفية فعليه أن يقوم بإلغاء تلك العملية والانتقال إلى جهاز آخر في مكان آخر[1].

ثانيا : حماية البطاقة من خلال المعاملات التجارية

ونكون في هذه الحالة أمام حالتين:

1- الحالة العادية: يحرص صاحب البطاقة أثناء تواجده في المحلات التجارية بأن يتسوق في أماكن آمنة ورفقه أشخاص محل ثقة كما يجب التأكد من السلعة المراد شرائها بمعاينتها والتأكد من سعرها الحقيقي، ثم كيفية الحصول عليها، إضافة إلى التحقق من هوية ومصداقية التاجر وأيضا بمطالبته بكافة الضمانات قبل إجراء المعاملة وان يتحقق جيدا من وصل الشّراء قبل توقيعه كما يجب عليه الاحتفاظ بنسخة منه وبكل الوثائق التي تثبت إجراء المعاملة، كما يجب إبلاغ البنك أو الشرطة في حال لم تسترد بطاقة الدفع من الجهاز أو إذا ما لاحظ صاحبها أشياء غير عادية كأجهزة غريبة متصلة مثلا[2].

2-حالة المعاملات عبر الانترنت: يعتبر التعامل عبر شبكة الانترنت اخطر بكثير من نظيره على الواقع لذلك وجب على صاحب البطاقة أخذ الحيطة والحذر من خلال بعض التدابير قبل إجرائه لأيّ عملية ومن أهميتها:

---

1 -امجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني ، مرجع سابق، ص 121 -123.

2- خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الالكتروني، مرجع سابق، ص56 .

– وتفادي المواقع غير المعروفة والتي تفتقد لإجراءات حماية بطاقة الدفع، ولذلك وجب التأكد من وجود اتصال آمن من خلال وجود كلمة **"http "** في بداية عنوان الموقع أو عن طريق التأكد من القفل المغلق أسفل نافذة المتصفح[1].

– أن يستعمل برامج الحاسوب المشفرة لحماية بريده الالكتروني، كما يجب عليه الحفاظ على كلمة السر الخاصة به ولا يسمح لأحد بمعرفتها، كما لا يسمح للجهاز بحفظها أو تذكرها من خلال تزويده بمفتاح التصفح لمنع اختراقه والوصول للبيانات.

–رفض الرد على المكالمات والرسائل البريدية وبعض المواقع التي تطلب من صاحب البطاقة تفاصيل من حسابه ورقم البطاقة وإن لزم الأمر الاتصال بالشرطة[2].

المطلب الثاني

المرتكزات الامنية لمواجهة جرائم الاستعمال غير القانوني لبطاقة الائتمان

في ظل غياب تشريع خاص يضبط جرائم الاستعمال غير القانوني لبطاقة الائتمان

فإن العيب الأكبر يقع على الأجهزة الردعية، حيث تعترف الشرطة على انها الجهاز الذي يتكفل بحفظ الأمن وتوفيره للأفراد والمجتمع ولتحقيق ذلك تقوم بوضع ضوابط لنشاط الأفراد حماية للنظام العام وفيما يلي سنتعرض إلى جملة من الإجراءات الوقائية التي تتبناها أجهزة الشرطة (**الفرع الأول) هذا** إلى جانب الإجراءات الردعية التي يتخذها الحاسب الآلي لحماية البطاقة **(الفرع الثاني)**.

1–أمجد حمدان الجهني، المرجع السابق، ص 124.

2-خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الالكتروني، مرجع سابق، ص 57.

الفرع الأول

الإجراءات الوقائية المتّخذة من قبل الشرطة لحماية البطاقة

تعتبر جرائم بطاقات الدفع الالكترونية من الجرائم الحديثة، لذلك هي تتميز بالخصوصية عن بقية الجرائم التقليدية الأخرى، فمرتكبيها يتمتعون بالخبرة العالمية في مجال تقنية المعلومات، إذ من الصعب التصدي مما كان كان لزاما على الشرطة تطوير أجهزتها التقنية وكذلك إفرادها حتى تكون لهم القدرة على مجارات هذه الجرائم ومن بين أهم هذه الإجراءات نجد:

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

كما عملت على العمل على إنشاء معامل جنائي متخصص وتدعيمه بالأجهزة والمعدات التقنية المتطورة لاستغلالها في عملية فحص البطاقات والمستندات والوثائق المستخدمة في تلك الجرائم للقدرة على مواكبتها[1].

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

وتدريبهم على كيفية استعمال الأجهزة الإلكترونية وأدواتها وآلات الطباعة المخصصة لها وهو ما يؤدي إلى معرفتهم بكيفي استخدامها وهو ما من شأنه أن يسهل عليهم اكتشاف ومتابعة الجرائم الواقعة على بطاقات الدفع الالكتروني، ومن جهة ثانية قدرتهم على التأكد من أن الجهات المتعاملة ببطاقات الدفع حاصلة عليها بموجب تراخيص قانونية أم لا، كما

1 -عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجيه مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان 2013، ص 118.

يمكنهم أيضا من وضع قاعدة بيانات الكترونية تحتوي على أرشيف جميع الجرائم وبيانات مرتكبيها ومن ثم تزويد البنوك الوطنية بالمعلومات الكاملة المتعلقة بالعملاء وهو ما يعزز أمن واستقرار البنوك والمؤسسات المصرفية[1].

الفرع الثاني

الإجراءات الأمنية المتّخذة من قبل الحاسب الآلي لحماية البطاقة

يتم اتخاذ العديد من الإجراءات الأمنية التي يكون الحاسب الآلي أساسها، تنتهج الشرطة في الوقت الحالي الأسلوب العلمي في أدائها لعملها، حيث تم تطوير نظام حفظ المعلومات بجهاز الشرطة وإدخال الحاسب الآلي تطوير برامج تقنية البيانات وإدخال كافة المعلومات ذات الصلة بالجرائم الإقتصادية ومرتكبيها ليصبح لدى الشرطة قاعدة بيانات كاملة باستخدام الأرشيف الالكتروني لحفظ جميع الملفات[2].

إعداد خريطة للموقع الذي سوف يتم مداهمته وتفاصيل المبنى وتحديد مواقع الأجهزة والخزائن والملفات السرية ومواقع بطاقات الائتمان الشخصية.

تحديد عدد وأنواع الأجهزة المحتمل تطورها في ارتكاب الجريمة للتعامل معها والحصول على الاحتياجات الضرورية من أجهزة وبرامج صعبة ولينة للاستعانة بها في الفحص والتشغيل[3].

كما تم تصميم برامج لمكافحة الاعتداءات التي تتم على نظام بطاقات الائتمان، مثل برامج نظم المعرفة عن طريق عزل ووقف البطاقات التي تعاملنها غير طبيعية، حيث توفر هذه البرامج وسائل فعالة لكشف التهديدات التي يستخدمها المحتالون، كالدخول غير

1 -خولة بوقديرة ، الجرائم الواقعة على بطاقات الدفع الالكتروني، مرجع سابق، ص62.

2 -إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقة الائتمان الإلكترونية، دار المؤسسة الحديثة للكتاب، لبنان، 2011 ص 385.

3 - عبد الكريم ردايدة، جرائم بطاقات الائتمان، مرجع سابق، ص130.

الشّرعي لنظام الحاسب الآلي وفتح الحسابات الجديدة بطريقة غير شرعية وإعادة تنشيط الحسابات الساكنة عن طريق تحليل القاعدة السلوكية لتعاملات حامل البطاقة.

كما تم تصميم برنامج الشبكة العصبية وهو ما يعني رصد جميع التعاملات التي تتم بواسطة البطاقات والكشف عن أي تعاملات مشكوك في صحتها وفحصها[1].

1 - إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقة الائتمان الالكترونية، مرجع سابق، ص 389.

المبحث الثاني

الآليات الرّدعية للحدّ من استعمال غير القانوني لبطاقة الائتمان

لقد أدرك المشرع الجزائري مدى خطورة الجرائم الإلكترونية وتناميها بشكل ملحوظ لذلك عمل على تطوير الإجراءات الكلاسيكية الخاصة بالبحث والتحري عن الجرائم بما يتماشى مع الجرائم المستحدثة، من خلال تعديل بعض القوانين **(المطلب الأول)** كما تبنى قوانين جديدة لمواجهة هذه الجرائم **(المطلب الثاني)**.

المطلب الأول

الآليات الكلاسيكية للبحث والتحرّي في الجرائم المستحدثة

حتى يتم الكشف عن الجرائم وضبط الأدلة المؤدية إليها وإماطة اللثام عن مرتكبيها تقوم الشرطة القضائية بمجموعة من الإجراءات الخاصة بذلك وفقا لما يحدده القانون وذلك عبر مراحل متتالية أولها مرحلة تلقي البلاغات **(الفرع الأول)** وثم تليها مرحلة إجراءات التحري والتفتيش **(الفرع الثاني)** و أخيرا مرحلة المحاكمة **(الفرع الثالث)**.

الفرع الأول

مرحلة تلقي البلاغات

يختلف التبليغ في الجرائم الإلكترونية عن التبليغ في الجرائم الأخرى ذلك لان الجريمة الإلكترونية تتم في فضاء افتراضي، لذا يجب على المبلغ عن هذه الجرائم أن يكون على دراية بالتقنية المعلوماتية.

أولا: تلقي البلاغات

لابد أن يكون المبلغ عن الجريمة شخص على معرفة بالأجهزة الإلكترونية وتقنياتها حتى تكون المعلومة المقدمة من طرفه واضحة، مثال ذلك تلقي بلاغ مفاده ضبط أحد الإفراد بحوزته بطاقة دفع مزورة أو يستخدم محررات مزورة[1].

نصّ المشرع الجزائري عن هذا الإجراء من خلال الفقرة الأولى من المادة 17 من قانون الإجراءات الجزائية والتي جاء فيها: **"يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و 13 ويتلقون الشكاوي والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية"**[2].

تضع الجهات الأمنية بما فيها الشرطة والدرك الوطني تحت تصرف المواطنين مواقع الكترونية ليتمكنوا من التبليغ عن الجرائم[3].

وكذلك الموقع الالكتروني للأمن الوطني وللمواطنين الحرية في إتباع هذه الطرق المستحدثة أو التبليغ بالطرق العادية، إلا انه ملزمون بتحديد أسماء المشتبه فيهم والقيام بطباعة نسخة ثانية للبيانات المتضررة في الأجهزة[4].

ثانيا: مرحلة البحث والتحري

انطلاقا من المعلومات المحصل عليها يقوم رجال الضبطية القضائية بالتحري عن الجريمة من خلال وضع خطة مناسبة لها، حيث يقوم المحقق القضائي بخطة عمل لتحديد الأسلوب الأنسب للتحقيق من خلال معرفة نوع الجريمة وتخصيص الفريق

---

1 -علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، مرجع سابق، ص 11.

2 - القانون رقم 06 –22، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66–155، المتضمن قانون الإجراءات الجزائية، ج. عدد العدد 84 ، الصادر بتاريخ 24 ديسمبر 2006.

3- ومثال ذلك الموقع الالكتروني للدرك الوطني www.mdn.ppgn

4 -حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل درجة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعةباتنة1، 2016، ص 218.

المناسب للبحث والتحري عنها كما يتم انجاز قائمة تحمل أسماء المشتبه فيهم وتحديد الأسئلة التي سيتم الاستجواب بشأنها وتقديم مدى الحاجة لمساعدة الخبراء في هذا المجال[1].

وبعد الانتهاء من الخطة على المحقق الرئيسي الذي هو قاضي التحقيق في الجريمة إعداد فريق عمل متمكن، حيث لابد أن يكون هذا الفريق متكون من خبراء الحاسوب والانترنت حتى يكونوا على اطلاع كافي بالجريمة المعلوماتية وكيفية التحري عنها كما يجب أن يتضمن الفريق خبراء تدقيق الحسابات الذين لهم خبرة في التعامل مع البرامج المستخدمة في البنوك والمؤسسات التي يتم من خلالها تبادل الأموال الكترونية وخبير في الرسم التخطيطي، والذي يتولى القيام برسم التخطيطي للجريمة بتقنية دقيقة، حيث توضح تقسيماته أماكن وجود الأشخاص والدلائل وخبير استشاري وهو الذي يوضح وقائع الجريمة ويزيل الغموض عنها[2].

ثالثا: مرحلة تجهيز الوسائل

حتى يصل المحققون الى النتيجة المرجوة في التحقيق يجب عليهما الاستعانة ببعض الوسائل والبرامج لتتبع العمليات ومن بين هذه الوسائل:

- تتبع البرامج يتم من خلال استخدام الرقم السري للبرنامج.
- تتبع النظام وهذا الأسلوب يتسم باستخدام الرقم السري أو تشغيل التعليمات يتم داخل نظام التشغيل.
- 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 ويوضح في القرص الصلب أو المرن.

1 -خولة بوقديرة، المرجع السابق، ص64.

2- حسين ربيعي، المرجع السابق، ص 241.

- برنامج xtreeprogold ويتم معالجة الملفات بواسطته والعثور عليها داخل الشبكة أو القرص الصلب.
- برنامج من خلاله تتم عملية نسخ المعطيات عن طريق تشغيله بواسطة القرص المرن، حيث ينقلها من جهاز المتهم الى قرص آخر بالاعتماد على المنفذ المتتالي[1].

الفرع الثاني

مرحلة المعاينة والتفتيش

بعد تلقي البلاغات والاستعداد اللازم لمباشرة التحري يقوم ضباط الشرطة القضائية للانتقال إلى المكان ومعاينته **(أولا)** وتفتيش محتوياته وضبط أي أدلة قد تقودهم لاكتشاف الجريمة **(ثانيا)**.

أولا : المعاينة

تنصّ المادة 61 من قانون الإجراءات الجزائية على انه تتم المعاينة و يكون ذلك سواء من طرق وكيل الجمهورية أو قاضي التحقيق أو من طرف الضبطية القضائية بأمر من وكيل الجمهورية أو قاضي التحقيق، من خلال الانتقال إلى مكان الجريمة ورؤية أثارها والإبقاء على حالتها حتى لا يتم العبث بها مما يتسبب في إتلافها، والمعاينة إجراء وجوبي في الجنايات وجوازي في الجنح وتتم في الأماكن العامة أو الخاصة على حد سواء، غير أنه في حالة الأماكن الخاصة تحتاج لرضا صاحب المكان أو بإذن قضائي وفي نهاية هذه المرحلة يتم وضع الأختام على ما تم معاينته وتعيين حارس عليه.

وفي الجرائم المعلوماتية يجب التفريق بين مسرحين للجريمة فهناك المسرح التقليدي وتتم معاينة الأشياء الملموسة التي تقع خارج أنظمة الأجهزة الإلكترونية ومثال ذلك

1 -حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، دون طبعة، دار الكتب القانونية، مصر 2013 ص690.

الاوراق والمستندات، بينما في مسرح الجريمة التقنية يتم معاينة الأشياء الافتراضية وهي المكونات الموجودة داخل أنظمة الحواسيب والانترنت، ومثال ذلك البرامج والتطبيقات والملفات الالكترونية[1].

ثانيا: التفتيش في المجال المعلوماتي.

يهدف التفتيش إلى ضبط الأدلة والقرائن ولقد وضع المشرع الجزائري ضوابط وشروط شكلية وأخرى موضوعية لصحة هذا الإجراء.

1- الشروط الشكلية: يجب مراعاة الإحكام التالية:

أ- **الحضور:** بالرجوع إلى نص المادة 1/45 من قانون الإجراءات الجزائية نجد أن المشرع الجزائري قد اقر حضور بعض الأشخاص عند إجراء عملية التفتيش لكنه مع خصوصية الجرائم الواقعة على النظم المعلوماتية فقد نفى المشرع عنها هذه الشروط، وذلك بموجب نفس المادة السابقة لذكر في فقرتها الأخيرة بعد التعديل الذي جاء به القانون 06-22 ، حيث نصت على أنه **"لا تطبق هذه الأحكام اذا تعلق الأمر بانظمة المعالجة الآلية للمعطيات"** [2].

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

---

1 -خولة بوقديرة ، المرجع السابق،ص68.

2 -المرجع نفسه، ص69.

3 -القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66-156، سالف الذكر.

ج- محضر التفتيش: يلتزم ضابط التحقيق بتحرير محضر يدون عليه ما توصل له من خلال اجراء التفتيش وهذا المحضر تجب لصحته بعض الشروط، مما تضمنها القواعد العامة وهو نفس الشيء بالنسبة لإجراءات التفتيش، حيث يجب أن يحتوي هذا المحضر على تاريخ تحريره ويجب أن يكتب باللغة الرسمية وان تدون فيه كل الإجراءات المتخذة وفي الأخير يجب أن يوقع عليه من قبل محرره إضافة الى أنه يمكن الاستعانة في تحريره بمن يملك الخبرة في مجال تقنية المعلومات[1].

2- الشروط الموضوعية : وتتمثل فيما يلي:

أ- **السبب:** حتى يتم التفتيش يجب أن يكون سبب مقنع لإجرائه من أجل الوصول الى كشف الجريمة، حيث يجب ان تكون الجريمة قد وقعت بالفعل أو أن تكون ماسة بنظم المعالجة الآلية للمعطيات ولقد ادرج المشرع الجزائري مجموعة جرائم الماسة بنظم المعطيات في قانون العقوبات في الفصل السابع منه تحت مسمى جرائم الاعتداء على نظم المعالجة الآلية ولابد أن تكون الدلائل قوية وقرار ضدهم.

ب- محل التفتيش: يجب أن ينصب التفتيش في هذه الجرائم على نظام المعالجة الآلية للمعطيات بمكوناته المادية والافتراضية والشبكات الانترنت وكل ملحقاتها التقنية الأخرى.

ج-السلطة المختصة في التفتيش: لقد حدد المشرع الجزائري للجهة المختصة بالتفتيش إلى قاضي التحقيق وفي بعض الحالات الاستثنائية يتكفل بإجراء التفتيش موظف الضبطية القضائية بعد إستصدار إذن من وكيل الجمهورية، وهذا إذا كانت الجريمة الإلكترونية متلبس بها من خلال رصد الجاني عبر شبكة الانترنت في حركة مريبة ليتم ترصده عبر هذه الشبكة[2].

---

1 -خولة بوقديرة ، المرجع السابق، ص69.

2 -بلقاسم نجاة، المسؤولية الجزائية عن استعمال البطاقات الإلكترونية، مذكرة ماستر في الحقوق، تخصص قانون خاص، كلية الحقوق، جامعة بلحاج بوشعيب، تمنراست، 2022، ص 50-51.

د-الإذن: كقاعدة عامة يتم إجراء التفتيش من قبل قاضي التحقيق أو وكيل الجمهورية بذلك لكن في حالات يتم تكليف ضابط من الضبطية القضائية وفي هذه الحالة حتى يباشر مهامه يجب حصوله على إذن بالتفتيش بالإنابة عن السلطة المختصة بذلك التي تمنحه له، ويجب ان يتضمن هذا الإذن مكان التفتيش والشخص والأشياء الأخرى كالأجهزة الآلية وبرامج الفيروسات والاختراق ونصت على ذلك المادة 44 من قانون الإجراءات الجزائية بقولها **" يجب أن يعين الإذن بالتفتيش بيان وصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها".**

د-**تفتيش المكونات المادية لنظام المعالجة الآلية:** تتمثل المكونات المادية لنظام المعالج الآلية للمعلومات فيما يلي:

- وحدات الإدخال ومهمتها إدخال البيانات كلوحة التحكم.
- وحدات إخراج ومهمتها 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 سابقا[1].

هـ- 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-09- 04 بموجب المادة 05 منه بقولها **" يجوز للسلطات القضائية المختصة وكذا ضباط ألشرطه القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4- أعلاها الدخول بغرض تفتيش ولو عن بعد:**

أ_ منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

1 -خولة بوقديرة ، المرجع السابق ، ص 71.

ب- منظومة تخزين معلوماتية..."[1].

1- التفتيش عن بعد:

تتكون الشبكة المعلوماتية من مجموعة من الأجهزة الإلكترونية متصلة يبعضها البعض بطريقة سلكية أو لاسلكية وبظهور شبكة الانترنت أصبحت هذه الشبكات تمتد الى كافة أنحاء العالم، ولذلك فإن هذه الشبكات عند تفتيشها تكون بعيدة عن موقع التفتيش وفي الصدد سنميز بين حالتين:

- اتّصال جهاز المتهم بجهاز آخر داخل الدولة وقد نص المشرع الجزائري على ذلك في المادة 05 من القانون 09- 04 /2 والتي جاء فيها: **"إذا تبين ان المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج التقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل"**[2].

يتبين مما سبق بان المشرع الجزائري أجاز التفتيش وسمح بتمديده إلى المنظومات البعيدة والتي تقع خارج الوطن، وذلك لان هذا الأسلوب يعتمده المجرمون من أجل عرقلة البحث والتحري وجعل أمر كشف الأدلة صعبا على المحققين[3].

الفرع الثالث

مرحلة المحاكمة

بعد إتمام إجراءات التّحري والتحقيق اللازمة وضبط دليل المعلومات تقوم النيابة العامة بتقديم نتائج التحقيق إلى المحكمة المختصة لإجراء المحاكمة، ولان الجرائم الإلكترونية تتّسم بالطّابع التّقني، و أنها جريمة عابرة للقارات فإن خطورتها يمتد لكافة

1 -القانون رقم 09 -04، المؤرخ في 05 أوت 2009، المتضمن الوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال، ج ر عدد 47 ، الصادرة بتاريخ 16 أوت 2009.

2- المادة 05 من القانون 09-04، السالف الذكر.

3- خولة بوقديرة، المرجع السابق، ص 73.

الدول، فقد يرتكب الفعل الإجرامي في بلد ما وتتحقق آثاره في بلد آخر وعليه وجب على المشرع الجزائري تحديد المحكمة المختصة بهذه الجرائم وذلك تبعا لمكان وقوعها فقد يؤول الإختصاص الجنائي الدولي **(أولا)** كما قد يكون من الإختصاص الوطني **(ثانيا)**.

أولا: الاختصاص الدولي

يتم تحديد الاختصاص في التشريع الجزائري وفقا للمبادئ التالية:

1- مبدأ إقليمية القانون: ومن خلاله فان كل الجرائم الواقعة على ارض الوطن تخضع للقانون الجزائري دون النظر الى جنسية الضحية أو المجرم.

2- مبدأ شخصية القانون: ومعناه إن كل جزائري قد يرتكب جريمة من الجرائم الالكترونية أو يكون ضحية جزائري فانه يطبق عليه القانون الجزائري[1].

3- مبدأ العينية: يختص هذا المبدأ بالجرائم الالكترونية ألماسه بمصلحة الدولة سواء داخل الوطن أو خارجه وسواء كان مرتكبها من الجزائر أو خارجها وقد نص المشرع الجزائري على هذا المبدأ في المادة 581 من قانون الإجراءات الجزائية[2].

ثانيا الاختصاص الوطني

يتم تحديد الاختصاص على المستوى المحلي وفقا للمكان الذي ارتكبت فيه الجريمة أو المحل السكني لأحد من المشتبه بهم في ارتكابها، وفيما يخص الجرائم الالكترونية فان المشرع الجزائري وبالرجوع لقانون الإجراءات الجزائية نجده حدد الاختصاص على النحو التالي:

1- **اختصاص النيابة العامة:** بالرجوع إلى الفقرة الثانية من المادة 37 من قانون الإجراءات الجزائية نجذ المشرع الجزائري قد وسع من صلاحيات وكيل الجمهورية ومدد

1 - بلقاسم نجاة ، المرجع السابق، ص55.

2 -خولة بوقديرة ، المرجع السابق، ص76.

اختصاصه إلى محاكم أخرى تطبق حسب التنظيم مع مراعاة ضبط الشرطة لالتزاماته وفق المادة 40 مكرر الفقرتين الأولى والثانية منه.

2- اختصاص قاضي التحقيق: تم تمديد صلاحيات قاضي تحقيق إلى المحاكم الأخرى وذلك بموجب نص المادة 40 من قانون رقم 04-14 وتطبق هذه الإجراءات بحسب التنظيم.

3- اختصاص محاكم الجنح: حسب نص المادة 329 فقرة 4 من القانون 04-14 في حالة قيام جريمة من جرائم المساس بالمعطيات يمتد اختصاص محاكم الجنح إلى دوائر اختصاص محاكم أخرى، وما يلاحظ على هذا التمديد بالنسبة لكل من النيابة العامة وقاضي تحقيق ومحاكم الجنح انه محلي ولا يشمل الجرائم التي ترتكب خارج الدولة.

المطلب الثاني

القوانين الخاصّة بالجرائم الالكترونية والإجراءات المستحدثة

حتى يضمن المشرع الجزائري الحماية الجنائية والإجرائية اللازمة للمعاملات الالكترونية و عند إدراكه أن الإجراءات الإعتيادية وحدها لا تكفي بالرغم من تطويرها ، بل يلزم قوانين و إجراءات جديدة خاصة بها لذا تدارك الامر سواء على الصّعيد الداخلي أو الخارجي، و هذا ما سنبينه من خلال دراسة التطور التشريعي الحاصل في هذا المجال **(الفرع الأول) و إستعراض الإجراءات المستحدثة (الفرع الثاني).**

الفرع الأول

التطوّر التشريعي في مواجهة الجرائم المعلوماتية

لمواكبة التطور الحاصل في مواجهة الجرائم المعلوماتية استحدثت نصوص إجرائية وعقابيه للأفعال المتصلة بها وذلك سواء المستوى الوطني **(أولا)** أو الدولي **(ثانيا).**

أولا : على المستوى الوطني

ضمن أهم التشريعات الوطنية المستحدثة نجد ما يلي:

1-التشريعات المستحدثة: ومن بين أهم هذه التشريعات:

القانون رقم 04- 15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون العقوبات، وكانت الغاية منه مكافحه الجرائم الالكترونية بتجريم الأفعال المكونة لها، و ذلك باضا فه القسم السابع تحت عنوان المساس بانظمه المعالج الآلية للمعطيات من المادة 394 مكرر إلى غاية 394 مكرر سبعة من هذا القانون[1]، بعدها تم إستحداث القانون رقم 09- 04، المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها ويهدف هذا القانون إلى وضع نصوص اجرائيه تتناسب مع الجرائم الالكترونية[2]، ثم المرسوم الرئاسي رقم 15-61، المؤرخ في 08 أكتوبر 2015 الذي يهدف إلى إنشاء الهيئة الوطنية المكلفة بالوقاية والجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3] و أخيرا القانون رقم 06-22، المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للقانون الإجراءات الجزائية من خلال المواد التي تنظم الاختصاص النوعي والمحلي والإجراءات الخاصة بالتفتيش[4].

2-الجهات المختصة بمكافحه الجرائم المعلوماتية: وهي الهيئات المكلفة بمهام معينه للوقاية ومكافحه الجرائم المعلوماتية وهي كالتالي:

أ-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: نص عليها المشرع الجزائري في المادة 13 من القانون 09-04 ودخلت حيز التنفيذ سنة 2015

---

1 -القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، ج ر عدد 71، الصادر بتاريخ 10 نوفمبر 2004.

2 - القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتضمن الوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ج ر عدد 47 ، الصادر بتاريخ 16 أوت 2009.

3 - المرسوم الرئاسي رقم 15- 61، المؤرخ في 8 أكتوبر 2015، يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 53، الصادرة بتاريخ 8 أكتوبر 2015.

4 -القانون رقم 06- 22، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66- 156 المتضمن قانون الإجراءات الجزائية، ج ر عدد 84 ، الصادرة بتاريخ 24 ديسمبر 2006.

بموجب المرسوم الرئاسي رقم 15- 68، وعرفتها المادة 13 بأنها: **"سلطة إدارية مستقلة معنويا وماليا مقرها بالعاصمة» وتتمثل مهام اللجنة تحت إشراف السلطة القضائية والمتمثلة أساسا في تنشيط وتنسيق إجراءات الوقاية والمكافحة ومساعدة السلطات القضائية".**

ب- المصلحة المركزية لمكافحه الجريمة المعلوماتية التابعة لمديريه الأمن الوطني: حيث تسعى مديرية الأمن الوطني لمكافحة الجرائم ومن بينها الجرائم المعلوماتية، حيث تتولى نيابة مديرية الشرطة العلمية والتقنية التابعة لها مهمة التصدي للجرائم المعلوماتية وتتواجد على المستوى الوطني في ثلاث نقاط وهي الجزائر وقسنطينة ووهران إضافة إلى ثلاث وحدات أخرى في كل من ورقلة وبشار وتمنراست[1].

ج- وحدات الدرك الوطني: على غرار مديرية الأمن الوطني يسعى كذلك جهاز الدرك الوطني لمكافحة الجرائم المستحدثة وذلك بالاعتماد على المصالح والمتماثلة في قيادة الدرك الوطني الوحدات الإقليمية الوحدات المشكلة الوحدات المتخصصة وحدات الإسناد هياكل التكوين المعهد الوطني للادله وعلم الإجرام المصلحة المركزية لتحريات الجنائية المصالح والمراكز العلمية والتقنية حيث تسعى كل هذه المصالح إلى اكتشاف جميع الجرائم المرتكبة على الأجهزة الالكترونية وعبر الانترنت[2].

ثانيا : على المستوى الدولي

لا تقتصر مكافحة جرائم بطاقات الدفع الالكتروني على المستوى المحلي فقط، بل تتعدى إلى الصعيد العالمي مما تطلب تكاثف جهود جميع الدول لمحاربة هذه الجرائم والجزائر وعلى غرار باقي الدول ساعات إلى الانضمام والمصادقة على الاتفاقيات والمعاهدات الدولية على الصعيد الدولي أو العربي.

1 - حسين ربيعي، المرجع السابق، ص 176 .

2 - حسين ربيعي المرجع السابق، ص182.

1- اتفاقية بودابست: كانت هذه الاتفاقية نتيجة جهود الاتحاد الأوروبي، حيث تعرف بالاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، تمّ إقرارها في 21 نوفمبر 2001 ودخلت حيز التنفيذ بتاريخ 1 جويلية 2004، حيث تضمّنت كل ما يتعلق بالجريمة الالكترونية 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[1].

2-الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات: تم إقرارها في القاهرة، بتاريخ 21 ديسمبر 2010، وتم تصديق عليها من طرف الجزائر من خلال المرسوم الرئاسي رقم 14-52، المؤرخ في 8 سبتمبر 2014، وتضمنت هذه الاتفاقية 5 فصول وجاء في مضمونها صور الجرائم الالكترونية ونصّت على جريمة تزوير بطاقات الدفع الالكتروني في المادة 18 منها، كما تضمنت مختلف الإحكام الإجرائية في مواجهه هذه الجرائم، كما تعمل على تعزيز التعاون القانوني والقضاء بين الدول الأعضاء من خلال تبادل المعلومات ووضع قواعد للاختصاص وحل مشكله التنازع[2].

الفرع الثاني

الإجراءات المستحدثة لمواجهة الجرائم المعلوماتية

إلى جانب الإجراءات التقليدية استحدث المشرع الجزائري آليات أخرى تواكب التقنية الحديثة لجمع الدليل التقني ومن أهم هذه الآليات آلية التسرب **(أولا)** وتسجيل الأصوات واعتراض المراسلات والتقاط الصور **(ثانيا)**.

1- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري المقارن، مذكرة ماجيستر، قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة العقيد الحاج لخضر، 2012، ص101-102.

2- مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 ، جريدة رسمية عدد 75، الصادرة بتاريخ 28 سبتمبر 2014.

أولا: عملية التسرّب

نصّ على هذه الآلية القانون رقم 06- 22 المتضمن تعديل قانون أللإجراءات الجزائية، حيث خصص له الفصل الخامس منه وعرفه في المادة 65 مكرر 12 بأنه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبه الأشخاص المشتبه في ارتكابهم جناية أو جنحه باتهامهم انه فاعل معهم أو شريك" ومن ضمن الجرائم التي أجاز فيها المشرع عمليه التسرب الجرائم الماسّة انظمه المعالجة الآلية للمعطيات ومن خلال هذا التعريف يتبين إن التسرب هو اندماج ضابط الشرطة مع المجرمين ومشاركتهم نشاطهم وذلك بطريقه سرية إلى غاية التوصل إلى نتيجة المرجوة وللقيام بعملية التسرب شروط شكلية وأخرى موضوعية وهي كالتالي:

1- الشروط الشكلية: يجب أن يكون التسرب بإذن صادر عن الجهة القضائية المختصة، وان يكون مكتوبا كما يجب ذكر هوية الضابط الموكل إليه هذه العملية، وتحدد مدته بأربعة أشهر مع جواز إيقافه من قبل القاضي الذي إذن به قبل استكمال مدته، كذلك يجب أن يقوم العون المكلف به بتحرير تقرير مفصل على أوضاع القضية كما تقتصر هذه العملية على الضباط وأعوان الشرطة القضائية لا غير وهذا طبقا لنص المواد 65 مكرر 11 إلى غاية 65 مكرر 15 من قانون الإجراءات الجزائية[1].

2- الشروط الموضوعية: يجب أن يكون التسرب مسببا وذلك بان يتضمن الأسباب التي على أساسها تم القيام به كما يتم تحديد نوع الجريمة محل التسرب حيث يجب إن تكون من الجرائم التي أجاز فيها المشرع هذه العملية، وقد نص عليها المشرع في المادة 65 مكرر خمسة من قانون الإجراءات الجزائية، كما نص المشرع الجزائري على أثار التسرب في المواد 65 مكرر 14 و 16 من قانون الإجراءات الجزائية والمتمثلة فيما يلي:

1 -مجراب الداودي، الأساليب الخاصة بالبحث والتحالف الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة بن يوسف بن خدة، الجزائر، 2016، ص 337 .

–تسخير الوسائل المادية من مواد وأموال آو منتجات أو وثائق لمجموعة المجرمين العامل معهم.

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

–سقوط المسؤولية الجزائية عن الأعوان المتسربين إثناء قيامهم بالأفعال السابقة الذكر لكونها أفعال قانونية.

–المحافظة على إبقاء عمليه التسرب في سريه تامة لتحقيق نتائجها على أكمل وجه ويتعرض لعقوبات كل من خالف ذلك[1].

ثانيا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

عرف الفقه الاعتراض على انه مراقبة وترصد المحادثات التي تتم بين الإفراد والعودة كدليل في مرحلة البحث والتحري ضد المتهمين عند الحاجة إليه كما ان تسجيل الأصوات هي عملية تتم إثناء التحدث الشفهي للأشخاص، وذلك بتسجيل تلك المحادثات أما التقاط الصور فهي توثيق تواجد الأشخاص فرادى أو جماعات في مكان ما دون علمهم.

ولقد أجاز المشرع الجزائري في الجرائم الماسة بالمعطيات بموجب المادة 65 مكرر فقرة 5 من قانون الإجراءات الجزائية، ويختص للإذن بها وكيل الجمهورية لضباط الشرطة القضائية مع جواز إجرائها بطابع استثنائي بحسب ما نصّت عليه المادة 47 من القانون ذاته، حيث تتم في أي وقت وفي أي مكان سواء في مرحله التحرير او التحقيق[2].

ولهذه الآلية شروطا ذكرها المشرع الجزائري في المواد 65 مكرر 5 إلى غاية المادة 65 مكرر 10 وهي كالتالي:

1 -الهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، مذكرة لنيل درجة الدكتوراه، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016، ص 305.

2 -خولة بوقديرة ، الجرائم على بطاقات الدفع الالكتروني، مرجع سابق، ص81.

1-يتم القيام بهذا الإجراء فقط بخصوص الجرائم التي حددها القانون ومن بينها الجرائم الماسة بالمعطيات.

2-يتوجب القيام بهذا الإجراء إذن من طرف وكيل الجمهورية أو قاضي التحقيق وتحت إشرافه في مرحله التحقيق.

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

4-تتراوح مدة هذا الإجراء أربعه أشهر، وإذا لزم الأمر يتم تجديده بنفس طريقة الإجراء الأول.

5-يجوز لضابط المكلف بإجراء الاعتراض الاعتماد على من يرى فيه الكفاءة المطلوبة في المجال التقني حسب ما تقتضيه القضية حيث يكون هذا الأخير عون مؤهل في هيئه عموميه أو خاصة تهتم بالمواصلات السلكية واللاسلكية.

6- يقوم ضابط المكلف بإجراء الاعتراض بتحرير محضر يتضمن تفاصيل العملية بعد الانتهاء منها على ذكر تاريخ بدايتها ونهايتها وساعتها.

7- يقوم كذلك الضابط بوصف أو نسخ المراسلات والصور والمحادثات المسجلة ضمن مهمته للاعتماد عليها كأدلة نحو كشف الحقيقة وتودع بالملف وكذلك ترجمه كلماتها الأجنبية بمساعدة مترجم[1].

1 -الهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، مرجع سابق، ص 313.

خاتمة

نستخلص من هذه الدراسة أن نظام بطاقات الائتمان هو نظام حديثا للوفاء يثير العديد من المشاكل القانونية المترتبة عن سوء استعمالها.

ودراسة موضوع الحماية الجزائية للاستعمال غير القانوني لبطاقة الائتمان ومعالجته من الناحية القانونية أضفى نوعا من الخصوصية على هذا النظام المستحدث في التعاملات المالية بشكل عام على المتعاملين فيه بشكل خاص.

والتشريع الجزائري لم يواجه بعد المشاكل القانونية المترتبة عن استعمال بطاقة الائتمان، وإن كانت نصوص القانون المدني ضمن القواعد العامة بها ما يحفظ من الحقوق تعتبر إطار قانوني مؤقت لتنظيم التعامل بالبطاقة البنكية إلا أنه بخصوص المسؤولية الجنائية نجد أن نصوص قانون العقوبات توفر بعض الحماية، إلا أنها لا تكفي لتعرضها مع مبدأ الشرعية في قانون العقوبات، وعليه يمكن استخلاص بعض النتائج المتوصل إليها وهي أن بطاقة الائتمان هي وسيلة وفاء فرضتها البيئة التجارية وطورتها التكنولوجيا الحديثة كأداة إلكترونية لإدارة النقود النقدية.

كما أنها بطاقة بلاستيكية تصدر من مؤسسة مالية بناء على عقد مبرم بينها وبين عميلها لتمكينه من الشراء بها أو الحصول على خدمات أو النقد من طرف ثالث متعاقد معها، والذي يقوم بتسوية قيمة استخدام البطاقة مع مصدرها على أن يقوم حامل البطاقة بتسديدها لهذا المصدر فيما يعد مع فوائدها بموجب عقد معه.

ولهذا، يواجه مستعمليها العديد من الثغرات في التعامل بها، خاصة بالنظام اليدوي، حيث يسمح بالتلاعب بفواتير إشعارات البيع، بإضافة مبالغ نقدية مخالفة للحقيقة، كما يسمح بقبول البطاقات الائتمانية غير الصحيحة والمزورة، ممّا يؤدي إلى خسائر مالية جسيمة.

كما نستنتج أيضا أن نصوص قانون العقوبات الجزائري لا تكفل حماية جنائية كاملة لبطاقة الائتمان، فإساءة استعمالها من جانب حاملها الشرعي أثناء فترة صلاحيتها سواء في سحب النقود من أجهزة التوزيع الأوتوماتيكي أو في وفاء بثمن السلع والخدمات على الرغم من أن رصيده لا يسمح بذلك لا يقع تحت طائلة أي صنف جزائي رغم ما ينطوي عليه الفعل من إخلال بالثقة الواجب توافرها في بطاقة الائتمان.

وعلى إثر هذه النتائج يمكن اقتراح بعض التوصيات التي تخدم الموضوع وهي: –

ضرورة إجراء دورات تحسيسية وتوعية بالمخاطر المترتبة عن جرائم البطاقات الالكترونية لفائدة جميع شرائح المجتمع، قصد تجنب وقوعهم كضحايا ومساهمتهم في الإبلاغ عنها.

– تدريب أفراد الجهات الأمنية المختصة في مكافحة هذه الجرائم بشكل دائم مع ما يتماشى ومستجدات تقنيات هذه الجرائم، أيضا توفير احدث الوسائل والتجهيزات التقنية لضمان تحقيق أفضل النتائج.

– ضرورة البحث المستمر والكشف عن مثل هذه الجرائم قصد اتخاذ إجراءات تتناسب مع مستوياتها التقنية العالية تكون كفيلة بردعها والحد منها.

– تحديث إجراءات البحث والتحري وتضمينها بقانون خاص والابتعاد عن دمجها مع الإجراءات التقليدية، وضرورة إفراد قانون خاص بتنظيم التعامل بالبطاقات الالكترونية يعالج مخاطرها ويجرم إساءة استخدامها إعمالا لمبدأ شرعية الجرائم والعقوبات، بحيث تجاري التطور التقني والعلمي وتتلاءم مع المتغيرات والمستجدات والوقائع المادية باستمرار.

– التنسيق الأمني على المستوى الدولي مع الأجهزة المختصة في هذا المجال لضمان استقرار المعاملات التجارية.

– العمل على تأهيل القائمين على أجهزة تنفيذ القانون لتطوير معلوماتهم في مجال تقنية المعلومات، وذلك من خلال تدريبهم وتأهيل القائمين بالضبط والخبراء والسلطات التحقيق

والقضاة وخاصة تدريب القضاة على التعامل والتفاهم لهذا النوع من القضايا التي تحتاج إلى خبرات فنية عالمية لملائمة قبول هذا النوع من الأدلة في الإثبات وتقديرها حتى يتمكن من الفصل في القضايا المتعلقة بالجرائم الالكترونية.

– ضرورة اهتمام الجهات المصدرة لبطاقات الالكترونية بالشركات التجارية العربية والأجنبية، والتي تتعامل بالبطاقة الالكترونية وذلك للوقوف على كل طرق وأساليب الاحتيال والخداع والتزوير في الاستخدام غير المشروع للبطاقة الالكترونية.

قائمة المراجع و المصادر

أولا : الكتب

1- امجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، الطبعة الأولى، دار المسيرة، الأردن، 2010.

2- محمد نور الدين عبد المجيد، بطاقة الائتمان، النظام القانوني وآليات الحماية الجنائية، المؤسسة الحديثة للكتاب، لبنان، 2017.

3- عوض بدير الحداد، تسويق الخدمات المصرفية، البيان للطباعة والنشر، القاهرة، 1999.

4- إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقة الائتمان الإلكترونية، الطبعة الأولى، دار المؤسسة الحديثة للكتاب، لبنان، 2011 .

5- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، دون طبعة، دار الكتب القانونية، مصر 2013.

6- حسين محمد الشبلي، مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية ، دار مجدلاوي للنشر والتوزيع، عمان، 2009.

7- عبد الكريم الردايدة، جرائم بطاقات الائتمان دراسة تطبيقية ميدانية، الطبعة الاولى، دار حامد للنشر والتوزيع، عمان، 2013.

8- الجرائم المستحدثة واستراتيجيه مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان 2013.

9- علي عدنان الفيل، المسؤولية الجزائية عن أساءه استخدام بطاقة الائتمان الإلكترونية، الطبعة الأولى، دار المؤسسة الحديثة للكتاب، لبنان، 2011.

10- مجدي محمود شهاب، فتوح الشاذلي، النظرية النقدية المؤسسات، دار الجامعية، بيروت، 1990

11- نضال سليم برهم، أحكام عقود التجارة الالكترونية، الطبعة الثالثة، دار الثقافة، عمان، 2010 .

ثانيا : الرسائل والمذكرات الجامعية.

أ-رسائل الدكتوراه.

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

2- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل درجة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016.

3-مجراب الداودي، الأساليب الخاصة بالبحث والتحالف الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة بن يوسف بن خدة، الجزائر، 2016.

4- كيلاني عبد الراضي محمود، النظام القانوني لبطاقات الائتمان، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة عين شمس، 1997.

ب- مذكرات الماجستير

- صونية مقري، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، مذكرة مقدمة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية قسم الحقوق، 2015.

- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري المقارن، مذكرة ماجيستر، قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة العقيد الحاج لخضر، 2012.

ج-مذكرات الماستر

1-بلقاسم نجاة، المسؤولية الجزائية عن استعمال البطاقات الإلكترونية، مذكرة ماستر في الحقوق، تخصص قانون خاص، كلية الحقوق، جامعة بلحاج بوشعيب، تمنراست، 2022.

2-خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الالكتروني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية جامعة ام البواقي، سنة 2018.

3-فاجي نهد، بن سليمان ربيحة، جرائم وسائل الدفع الالكتروني، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص قانون الأعمال ، جامعة قاصدي مرباح ، ورقلة ، 2019-2020.

4-فتيحة يزيد، رشى جدة لنظام القانوني لوسائل الدفع الالكتروني في الجزائر، مذكرة لنيل شهادة الماستر في العلوم القانونية، تخصص قانون أعمال، كلية الحقوق و العلوم السياسية، جامعة آكلي محند أولحاج، البويرة 2020-2021.

5-مونية معروف، جرائم بطاقات الائتمان الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي، 2021-2022.

ثالثا: المقالات:

1-الشكري عادل يوسف، "الحماية الجنائية لبطاقات الدفع الإلكتروني"، **مجلة مركز دراسات الكوفة**، العدد11، 2011 ص ص 85-108.

2-بوجمعة شهرزاد، عيشاوي أمال، " مظاهر الحماية القانونية لوسائل الدفع الإلكتروني في التشريع الجزائري"، **مجلة البحوث والدراسات القانونية والسياسية**، المجلد 11، العدد 2، 2018 ص ص 188-208.

3-عبد الحليم بن مشري، " الحماية القانونية لبطاقات الدفع الإلكتروني"، **مجلة الإجتهاد القضائي**، المجلد 12، العدد 1، 2019 ص ص 55-74.

رابعا: النصوص القانونية

1- النصوص التشلريعية:

1-القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، ج ر عدد 71، الصادر بتاريخ 10 نوفمبر 2004، المعدل والمتمم.

2-القانون رقم 06 -22، المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، ج ر عدد العدد 84 ، الصادر بتاريخ 24 ديسمبر 2006، المعدل والمتمم.

3- القانون رقم 09 -04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47 ، الصادر بتاريخ 16 أوت 2009.

1-النصوص التنظيمية:

-المرسوم الرئاسي رقم 15- 161، المؤرخ في 8 أكتوبر 2015، يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 53، الصادر بتاريخ 8 أكتوبر 2015.

- مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 ، جريدة رسمية عدد 75، الصادرة بتاريخ 28 سبتمبر 2014.

الفهرس	
مقدمة:	1
الفصل الأول **الجرائم الواقعة على استعمال غير قانوني لبطاقة الائتمان**	4
المبحث الاول: استخدام بطاقة الائتمان الإلكترونية من قبل صاحبها بتجاوزات	6
المطلب الاول:سوء استخدام بطاقة الائتمان الإلكترونية بالنظر إلى مدة صلاحيتها	6
الفرع الاول: استخدام بطاقة الائتمان خلال فترة صلاحيتها	6
أولا: السحب من جهاز مخصص لذلك رغم النقص في الرصيد	7
ثانيا: الوفاء بقيمة البضائع والخدمات رغم النقص في الرصيد	9
الفرع الثاني: استخدام بطاقة الائتمان المنتهية الصلاحية	10
أولا: استخدام بطاقة الائتمان المنتهية الصلاحية للوفاء	11
ثانيا: استخدام بطاقة الائتمان المنتهية الصلاحية لسحب النقود	11
المطلب الثاني: استخدام بطاقة الائتمان الإلكترونية الملغاة أو بعد التصريح بضياعها أو سرقتها	11
الفرع الأول: استخدام بطاقة الائتمان الملغاة	12
أولا: استخدام بطاقة الائتمان الملغاة لسحب النّقود	12
ثانيا:استخدام بطاقة الائتمان الملغاة للوفاء	13
ثالثا: حالة امتناع حامل البطاقة عن ردها بعد طلبها من المؤسسة المالية	14
الفرع الثاني: استخدام بطاقة الائتمان بعد الادعاء من صاحبها بضياعها أو سرقتها	15
المبحث الثاني:استخدام بطاقة الدفع الالكتروني من قبل غير المشروع	15
المطلب الاول: الاستخدام غير المشروع للبطاقة مفقودة أو مسروقة	16
الفرع الأول: استخدام البطاقة المفقودة أوالمسروقة في سحب النقود	16
الفرع الثاني:استخدام البطاقة المسروقة أو المفقودة كأداة للوفاء	17

المطلب الثاني: تزوير بطاقة الائتمان من قبل الغير	18
الفرع الأول: أساليب تزوير بطاقة الدفع الالكتروني	18
أولا: التزوير الكلي لبطاقة الائتمان	19
ثانيا: التزوير الجزئي لبطاقة الائتمان	19
الفرع الثاني: تزوير الاشعارات والمستندات الخاصة ببطاقة الائتمان	21
أولا: تلاعب موظف البنك المصدر للبطاقة بإشعارات بطاقة الائتمان	21
ثانيا: تواطؤ حامل البطاقة مع التاجر	21
ثالثا: تزوير الإشعارات والفواتير الناتجة عن عملية البيع	21
رابعا: تلاعب التاجر في ماكينات البيع الالكترونية	22
خامسا: إصدار بطاقات صحيحة بمستندات المزورة	22
الفصل الثاني **آليات حماية بطاقة الائتمان من الاستعمال الغير القانوني**	23
المبحث الأول: الاجراءات الوقائية والردعية للحد من استعمال الغير القانوني لبطاقة الائتمان	25
المطلب الاول: الاجراءات الوقائية لمواجهة جرائم الاستعمال الغير قانوني لبطاقة الائتمان	25
الفرع الأول: الاجراءات الواجب اتخاذها من مصدر البطاقة	25
أولا : الاجراءات التقنية	25
ثانيا: الاجراءات الادارية المصرفية	27
الفرع الثاني: الاجراءات المتخذة من قبل صاحب البطاقة	29
المطلب الثاني: الاجراءات الردعية لمواجهة جرائم الاستعمال الغير قانوني لبطاقة الائتمان	31
الفرع الاول: الاجراءات الردعية المتخذة من قبل الشرطة لحماية البطاقة	32
الفرع الثاني: الاجراءات الامنية المتخذة من قبل الحاسب الآلي لحماية البطاقة	33

المبحث الثاني: الاجراءات الردعية للحد من استعمال غير القانوني لبطاقة الائتمان	34
المطلب الأول: الاجراءات الكلاسيكية للبحث والتحري في الجرائم المستحدثة	34
الفرع الاول: تلقي البلاغات	35
أولا: تلقي البلاغات والشكاوى	35
ثانيا: مرحلة البحث والتحري	36
ثالثا: مرحلة تجهيز الوسائل	36
الفرع الثاني: المعاينة والتفتيش	37
أولا:المعاينة	38
ثانيا: التفتيش	38
الفرع الثالث: مرحلة المحاكمة	42
أولا: الاختصاص الدولي	42
ثانيا: الاختصاص الوطني	43
المطلب الثاني: القوانين الخاصة بالجرائم الإلكترونية والاجراءات المستحدثة	43
الفرع الأول: التطور التشريعي	44
أولا: على المستوى الوطني	44
ثانيا: على المستوى الدولي	46
الفرع الثاني: الاجراءات المستحدثة	47
أولا: عملية التسرب	47
ثانيا: اعتراض المراسلات وتسجيل الاصوات والتقاط الصور	49
خاتمة	51
قائمة المراجع	54
فهرس	64

ملخص

هذه الدراسة مكرسة للإستخدام الإحتيالي لبطاقات الإئتمان الإلكترونية ، و نظرا لتكاثر هذا الإستخدام الضار و تنوعه تبذل الجزائر كباقي الدول كل الجهود للحد من الجرائم المرتكبة بمناسبة إستعمال هذه البطاقات، و في هذا المسعى أدخل المشرع تشريعا قمعيا كافيا لمعاقبة مرتكبي هذه الجرائم ، و من خلال هذه الجهود تساهم الجزائر أيضا في الكفاح الدولي ضد هذا الشكل الجديد من الجريمة.

الكلمات المفتاحية: الجريمة ، بطاقة الإئتمان ، أليات المكافحة.