الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور – خنشلة –
كلية الحقوق والعلوم السياسية

قسم: الحقوق
نيابة العمادة للدراسات وشؤون الطلبة

الجرائم الواقعة على بطاقة الدفع الالكتروني

مذكرة مكملة لنيل شهادة الماستر في الحقوق
تخصص: قانون جنائي وعلوم جنائية

إعداد الطالب:
سلامة اسماعيل

إشراف الدكتور:
عبابسة محمد

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الأصلية	الصفة
عمراوي خديجة	أستاذ مساعد _ ب_	جامعة خنشلة	رئيسا
عبابسة محمد	أستاذ محاضر _أ_	جامعة خنشلة	مشرفا ومقررا
قـابوش وهيبة	أستاذ مساعد _أ_	جامعة خنشلة	عضوا ممتحنا

السنة الجامعية: 2018 -2019

بسم الله الرحمن الرحيم

إهداء

إلى من قـال في حقهمـا

﴿وَاخْفِضْ لَهُمَا جَنَاحَ الذُّلِّ مِنَ الرَّحْمَةِ وَقُل رَّبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا﴾

إلى روح والدي الكريمين طيب الله ثراهما

إلى أخي وإخوتي اعترافا بالجميل

إلى زميلي النوي وليد وزديرة أحمد وليد عربون محبة وتقدير

إلى أستاذي ومشرفي "عبابسة محمد" تعظيما مني وتبجيلا

للأكرم منا جميعا لشرفاء هذا الزمن شهدائنا الأجاويد

إليكم جميعا أهدي هذا العمل

سلامة اسماعيل

3DLAT.COM

شكر وعرفان

الشكر أولا للّه سبحان وتعالى على ما أصبغه علينا من نعم وكريم أفضاله وفي ذكره شرف الشاكرين وكما جاء في حديث رسول اللّه صلى اللّه عليه وسلم : من لا يشكر الناس لا يشكر اللّه.

لذا لا يسعني وأنا أقدم هذا العمل إلى أن أتقدم بجزيل الشكر للدكتور عبابسة محمد وفاءا وتقديرا واعترافا مني بالجميل لما قدمه لي من توجيهات طيلة إنجاز هذه المذكرة ولم يبخل عليا من نصائحه وصاحب الفضل في مساعدتي في تجميع المادة العلمية فجزاه اللّه كل خير.

والشكر موصول كذلك لأعضاء لجنة المناقشة الموقرة التي قبلت تحمل عبء مراجعة هذا العمل الشاق وتصويب أخطائه.

كما لا أنسى أن أتقدم بجزيل الشكر لأساتذة وموظفي جامعة عباس لغرور بخنشلة عموما ولكلية الحقوق والعلوم السياسية خصوصا.

وأشكر كل من مد إلي يد العون من قريب أو بعيد

شكرا لكم جميعا

مقدمة

مقدمة:

إن التحولات التكنولوجية الحديثة في مجال الأجهزة والبرمجيات والاتصالات، أدت إلى فرض أشكال جديدة من المعاملات المرتبطة بالاقتصاد والمعلومات ومن أبرز هذه الأشكال دخول البطاقات البلاستيكية أو البطاقات الممغنطة والمحوسبة عالم الخدمات المصرفية نتيجة التطور والتقدم في جميع مجالات الاتصالا والصناعات الالكترونية مما سار على نحو ذلك العالم فأضحت البطاقات الممغنطة ذات توجه عالمي وإنجاز حضاري يحسب في تاريخ الانسانية ودليل على التقدم العلمي فجسدت ما يسمى مجتمع بلا شيكات ولا نقود لذلك لم يعد مفهوم الدفع الالكتروني جديدا في الساحة العالمية نظرا لعصر المعلوماتية الذي ساهم في الانتشار الواسع للشبكة العنكبوتية واستخدامها وعلى رأسها بطاقات الدفع الالكتروني.

كانت بداية ظهور بطاقات الدفع الإلكتروني في الدول الغربية وتحديدا في أمريكا ثم انتشرت في باقي الدول الأوروبية وصولا للدول العربية ومن بينها الجزائر التي تتوفر فيها العديد من بطاقات الدفع الالكتروني التي تستعمل في السحب والوفاء وعلى رأسها البطاقة الذهبية لبريد الجزائر، حيث انتشر استعمالها بين الناس وكثر الحديث عنها خاصة في الفترات الأخيرة إضافة إلى بطاقات الدفع الخاصة للتوفير والاحتياط بنك الفلاحة والتنمية الريفية، الصندوق الوطني للتوفير والاحتياط، كالبنك الخارجي، كما توفر هذه البنوك أيضا بطاقات دفع إلكترونية عالمية كبطاقة "ماستر كارد" و"فيزا كارد".

وبالرغم من المزايا العديدة لهذه البطاقات التي تقدمها للمتعاملين بها إلا أنها لا تخلوا من بعض الآثار السلبية فمن ناحية تدفع خطوات التطور في المجال المصرفي إلى الأمام تسهيلا لحياة الانسان المعاصر وإقصاء لحالة الخوف من حمل النقود في حالة سفر لحاملها من بلد لآخر فهي من ناحية أخرى أصبحت هذه البطاقات محل للعديد من الجرائم في حالة الاستخدام الغير مشروع لها من قبل المجرمين الذين يستغلون هذه الاكتشافات مما انعكس ذلك سلبا على مصداقية هذه البطاقات والجهات المصدرة لها والمستخدمين لها مما يستدعي مواجهة هذه الاعتداءات بتوفير ما يلزم لحمايتها من وسائل قانونية وتقنية على الصعيد الوطني والدولي لضمان استقرار معاملات التجارة الإلكترونية والسير الحسن لها.

أهمية الدراسة:

تتمثل أهمية الموضوع محل الدراسة في إبراز الأهمية الكبرى التي تقوم بها هذه البطاقات ومساهمتها في تطوير الاقتصاد والخروج من وسائل الدفع التقليدية وفرض حماية جزائية موضوعية وإجرائية لضمان استقرار المعاملات التجارية.

إشكالية الموضوع:

من خلال ما تقدم بيانه وعلى ضوء ما سبق ذكره يتجلى لنا أن موضوع الدراسة يتناول أحد الإشكالات القانونية التي يثيرها استخدام بطاقات الدفع الالكتروني في المعاملات المصرفية والمالية وهو ما يتعلق بالجرائم الواقعة على بطاقات الدفع الالكتروني، ومن خلال هذا يمكننا طرح الإشكالية التالية:

إلى أي مدى كفل المشرع الجزائري الجرائم الواقعة على بطاقات الدفع الالكتروني؟

ومن هذه الإشكالية نطرح أسئلة فرعية:

- ماهي بطاقة الدفع الإلكتروني وفيما تكمن أهميتها؟
- ما هي الجرائم التي ترتكب من طرف حامل البطاقة والغير؟
- مامدى فاعلية الحماية الجزائية لهذه البطاقات للتصدي للاعتداءات الواقعة عليها؟

أسباب اختيار موضوع البحث:

يرجع اختيار الموضوع للأسباب التالية:

الأسباب الموضوعية:

- معرفة موقف الجزائر من هذا التطور التكنولوجي ومدى مسايرتها له.
- معرفة مدى ملائمة ومواكبة النصوص التقليدية في الاعتداءات الواقعة على بطاقات الدفع الالكتروني في ظل غياب تشريع خاص لمواجه الجرائم الواقعة على هذه البطاقات.
- معرفة الدور الذي تلعبه هذه البطاقات في الاقتصاد النقدي الحديث.

الأسباب الذاتية:

- الإطلاع على مدى مسايرة بنوكنا العربية لهذا التطور ومعرفة مدى مواكبة النصوص التقليدية للاعتداءات الواقعة على بطاقات الدفع الاكتروني في ظل غياب تشريع خاص.

- البحث بصفة عامة عن سبب تأخر المشرع الجزائري في إدراج بطاقات الدفع الإلكتروني ضمن تشريع خاص.

أهداف الدراسة:

إن الهدف من دراسة هذا الموضوع هو:

- تسليط الضوء على الجرائم الواقعة على بطاقات الدفع الالكتروني والعقوبات المقررة لها
- الالتفات حول موقف المشرع الجزائري من هذه البطاقات والإلمام بكل التدابير الوقائية والأمنية لمواجهة الاعتداءات الواقعة عليها.
- تطوير المنظومة التشريعية وتنبيه المشرع لإنشاء نصوص قانونية خاصة احارب هذه الظاهرة.

منهج البحث:

اعتمدت في إعداد دراستي على المنهج الوصفي المعتمد على آلياته التحليلية والذي يمكننا من استعراض المفاهيم القانونية والإدارية المتعلقة ببطاقات الدفع الالكتروني ووصف الاعتداءات الواقعة عليها. واستخلاص النتائج وتصنيفها وترتيبها وفق الخطة المرسومة.

الدراسات السابقة:

توجد عدة دراسات علمية أكاديمية حول هذا الموضوع بالرغم من أنه جديد ومن بين الدراسات التي اعتمدنا عليها كمرجع مهم نذكر منها ما يلي:

- أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام الغير مشروع لبطاقات الدفع الالكتروني، ط$_1$، دار المسيرة للنشر والتوزيع والطباعة، الأردن، 2010، بحيث توصل من خلال دراسته إلى وصف كافة الجرائم التي تقع على بطاقات الدفع الالكتروني وإقرار الحماية الجنائية لها في كل المستويات، وأضفنا إلى ذلك تعريف بطاقات الدفع الإلكتروني وأهميتها وأهم خصائصها وإساءة استخدامها من طرف صاحبها ومن طرف الغير وتوسعنا في ذلك بغية إثراء هذا الموضوع.
- خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، أطروحة مقدمة لنيل شهادة الماجستير في القانون، خشة حسيبة، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016، والتي توصلت من خلاله الباحثة إلى أن المشرع الجزائري وبإصداره القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، فقد تبنى وبكل أمانة كل القواعد الأساسية الخاصة بالجرائم الالكترونية، وأضفنا إلى ذلك الحماية الجزائية الإجرائية لبطاقات الدفع

الالكتروني على المستوى الوطني والدولي وذلك بهدف ضمان استقرار المعاملات المصرفية والمالية والتجارية.

صعوبات البحث:

خلال مسيرتنا البحثية اعترضتنا عدة عقبات أهمها:

- قلة المراجع المباشرة في هذا الموضوع خاصة الجزائرية منها.
- حداثة الموضوع التي جعلته متشعب التنوال من الباحثين.
- ندرة الأحكام القضائية الخاصة بهذا النوع من الجرائم.
- غياب تشريع خاص ينظم بطاقات الدفع الالكتروني.
- عدم توفر المدة الكافية مما جعلني أسابق الزمن لاعداد مذكرة وافية.

ومع هذه الصعوبات فقد بذلت قصارى جهدي في محاولة إنجاز مذكرة علمية وافية بحق الموضوع من الجانبين العلمي والمنهجي.

خطة البحث:

للإجابة على إشكالية البحث وتحقيق أهداف الدراسة والالمام بأهم جوانب البحث وفقا لما تقتضيه الدراسة العلمية والأكاديمية قمنا بتقسيم بحثنا إلى فصلين تناولنا في الفصل الأول الحماية الجنائية الموضوعية لبطاقات الدفع الالكتروني والذي قسمناه إلى مبحثين تناولنا في المبحث الأول إساءة استعمال بطاقة الدفع الالكتروني من طرف صاحبها، وفي المبحث الثاني تناولنا الاستخدام الغير مشروع لبطاقة الدفع الالكتروني من طرف التاجر والمصدر أما الفصل الثاني خصصناه لدراسة الحماية الجنائية الإجرائية لبطاقات الدفع الالكتروني والذي بدوره قسمناه إلى مبحثين، المبحث الأول منه تناولنا فيه الإجراءات الوقائية والمبحث الثاني الإجراءات الردعية القانونية.

الفصل الأول

الحماية الجنائية الموضوعية لبطاقات الدفع الالكتروني

تمهيد:

يعد ظهور وسائل الدفع الحديثة بشكل عام وبطاقات الدفع الالكتروني بشكل خاص نتيجة حتمية للمسار المنطقي الذي مر به تطور وسائل الدفع من مقايضة إلى نقود فبدائل النقود وصولا إلى هذه البطاقة كوسيلة حديثة للأداء، ولعل ما تمتاز به هذه البطاقات من أزمان وراحة وسهولة بطاقات الدفع الإلكتروني وهذا ما أدى إلى انتشارها الواسع إلى المستوى المحلي والدولي.

وأمام ضعف النظام القانوني لهذه البطاقات وارتباطها الوثيق بالنقود فإن ذلك جعلها هدفا للجناة يسعون إليها بمختلف الطرق اللامشروعة وذلك بالعتداء عليها عن طريق الاستخدام غير الشرعي لها.

ولذلك ستتناول في هذا الفصل تحديد الاعتداءات الواقعة على بطاقات الدفع الإلكتروني والخبرات المترتبة عنها ونقسمه إلى مبحثين في المبحث الأول نتناول الاعتداءات الواقعة من طرف صاحب البطاقة والمبحث الثاني نتناول فيه الاعتداءات المرتكبة من مصدر البطاقة والتجار والغير.

المبحث الأول: إساءة استعمال بطاقة الدفع الإلكتروني من طرف صاحبها.

بطاقات الدفع الالكترونية وسيلة إلكترونية تصدرها الجهة المصدرة لعملائها بهدف القيام نيابة عن موظفي البنك بتأدية العمليات المصرفية من سحب نقود لتحويل الأرصدة وشراء السلع والخدمات وغير ذلك وهذا ما شجع البعض من محترفي النصب والتزوير على الدخول لمحلات بطاقات الدفع لتزويرها واستخدامها في النصب على التجار والبنوك وتجاوز حدود الاستخدام أو تجاوز السقف المسموح به في عملية السحب والوفاء واستخدام البعض لها بعد انتهاء مدة صلاحيتها. (1)

وسنخرج بالدراسة في هذا المبحث إلى ماهية بطاقات الدفع الالكتروني في المطلب الأول ونتناول في المطلب الثاني الاستخدام الغير مشروع للبطاقة أثناء فترة صلاحيتها، وفي المطلب الثالث نتناول استخدام هذه البطاقة خارج فترة صلاحيتها.

المطلب الأول: مفهوم بطاقات الدفع الالكتروني

أحافظ بطاقات الائتمان شأنها في ذلك شأن كل ظاهرة جديدة والتساؤلات التي تتعلق بتعريفها وتحديد مفهومها ومما يزيد من أهمية تعدد التعاريف الخاصة بها وتباينها في ما بينها ضيق واتساعا طبقا للجانب الذي يتم تعريفها من خلاله فهناك الكثير من المصطلحات تطلق على هذه البطاقات أكثرها بطاقات الائتمان على غرار ما يذهب إليه البعض من إطلاق مصطلحات أخرى طبقا لمجال تخصصي على تلك البطاقات منها: الدفع الالكتروني، النقود الممغنطة، بطاقات الضمان، النقود الالكترونية، الحافظة الالكترونية... إلخ.

الفرع الأول: تعريف بطاقات الدفع الالكتروني

وانطلاقا من هذا كله يمكن تقسيم التعريف إلى ثلاث محاور من ناحية الشكل واللغة والمضمون.

أولا: من حيث الشكل:

تتفق جميع البطاقات، بغض النظر عن الوظائف التي تؤديها في الخواص الشكلية التي تتكون منها فجميعها مصنوعة من مادة كولوريد الفينيل PVC غير، مدون عليها بيانات مرئية وملقنة وبيانات أخرى غير مرئية وجميعها تستخدم في وسط إلكتروني. (2)

---

[1]- علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الإئتمان الإلكترونية (دراسة مقارنة) ط1، المؤسسة الحديثة للكتاب، لبنان، 2011، ص 53.

[2]- رياض فتح الله بصلة، جرائم بطاقات الائتمان، ط1، دار الشرق للنشر والتوزيع، القاهرة، جمهورية مصر، 1995، ص 02.

وانطلاقا من هذا كله يتم تعريف بطاقات الائتمان من الناحية الشكلية بأنها بطاقة مستطيلة من البلاستيك تحمل اسم شعار المؤسسة العالمية الراعية لها واسم البنك المصدر لها واسمه ورقم حساب العميل وأحيانا صورته و تاريخ انتهاء صلاحيتها، ومثبت على خلفياتها شريط مغناطيسي يحمل جميع البيانات المشفرة و الخاصة بالبنك المصدر وحامل البطاقة. [1]

ثانيا: التعريف اللغوي:

البطاقة في اللغة تعني الورقة أو الرقعة الصغيرة من الورق وغيره يكتب عليها بيان ما تعلق عليها وقيل أنها عبارة عن رقعة صغيره يثبت فيها مقدار ما تجعل فيه فإن كان عينا فوزنه، أو عدده، وإن كان متاعا فقيمته.

أما كلمة ائتمان فمعناها اللغوي إفتعال من الأمانة يقول تعالى جل شأنه «فَلْيُؤَدِّ الَّذِي اؤْتُمِنَ أَمَانَتَهُ» [2] أي أن يعطي ما عليه لأنه مؤتمن عليه.

ثالثا: من حيث المضمون:

يختلف تعريف بطاقات الائتمان في هذا الإطار باختلاف الجانب الذي يتم تعريفها منه وهكذا يتم تعريفها مصرفيا عبارة عن صك اسمي يصدره البنك لمصلحة عميلة يعطيه الحق في الحصول على ما يلزمه من سلع أو خدمات اتجاه هذه المشروعات، مقابل الوفاء بقيمة السلع والخدمات التي حصل عليها حامل البطاقة استثناء على الشروط المتفق عليها بينهما. [3]

وعرفها جانب آخر في أنها أداة مصرفية بلاستيكية كبديل للنقد والائتمان في نفس الوقت وتعطي لحاملها الحق في الحصول على مصدر هذه البطاقة، وذلك للوفاء بقيمة مشترياته من سلع وخدمات التجار المتعاقد معهم المصدرة بقبول الوفاء بالبطاقات مقابل توقيع الحامل للتاجر على إيصال بقيمة التزاماته على أن يقيد التاجر بتحصيل قيمة البنك مصدر البطاقة ويتعين على حامل البطاقة سداد القيمة لمصدرها في أجل معين متفق عليه ولا تمنح هذه البطاقات إلا بعد التأكد مصدرها من وجود ضمانات كافية. (شخصية أو عينية) تتناسب مع الحد المصرح به للبطاقة.

---

[1]- جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، الطبعة الأولى، دار النهضة العربية، 2003، القاهرة، ص 10.

[2]- سورة البقرة، الآية 238.

[3]- عطية سالم عطية، بطاقات الدفع الإلكتروني وأهميتها في عصرنا، محاضرات البنك الأهلي المصري، محاضرة رقم 12، معهد الدراسات المصرفية، 1997-1998، ص 21.

الفرع الثاني: أنواع بطاقات الدفع الالكتروني

تتخذ عملية تصنيف بطاقات الائتمان صور متعددة فهناك تصنيفات تعطى لها بناء على الجهة المصدرة [1] فهي إما أن تصدر من خلال رعاية منظمات عالمية لها عن طريق تفويض لبعض البنوك التجارية ووضع اسم وشعار المنظمة عليها كبطاقات الفيزا وماستركارد .

وإما أن تصدر تحت رعاية مؤسسة عالمية واحدة و تحت الإشراف المباشر لها أو لأحد فروعها مع عدم منح التراخيص وتفويضات لأي مؤسسة أو بنك آخر كمنظمة الأمريكان اكسبريس، إلى جانب بطاقات خاصة قد تصدرها مؤسسات تجارية معينة بغية استخدامها من طرف عملائه في عمليات الشراء بهدف المحافظة عليهم كالمطاعم الكبيرة والفنادق والشركات التجارية الكبرى ومحطات البنزين...إلخ. [2]

وتتميز البطاقات الصادرة عن هذه المنظمة بمرونة كافية تخضع أولا وأخيرا للأنظمة التي يضعها البنك المصدر ووفقا لما يتناسب مع متطلبات عملائه وأنظمته الداخلية، بحيث تأتي هذه البطاقات على ثلاثة أنواع هي:

أولا: بطاقة الفيزا الفضية: تتصف هذه البطاقة بكونها ذات حدود ائتمانية منخفضة نسبيا الشيء الذي جعلها تمنح لأغلب العملاء عند انطباق الحد الأدنى من المتطلبات الضرورية عليهم، مانحة إياهم كافة الخدمات المتوفرة لدى المنظمة كالسحب النقدي من البنوك وأجهزة الصرف الآلي والشراء من التجار وغيرها من الخدمات الأخرى.

ثانيا: بطاقة الفيزا الذهبية: تمنح هذه البطاقة للعملاء ذوي الكفاءة المالية العالية أي لذوي الحدود الائتمانية الكبيرة والمضمونة، بحيث توفر هذه البطاقة إلى جانب الخدمات التي توفرها سابقا العديد من الخدمات الأخرى كالتأمين على الحياة والحجز في مكاتب السفريات والفنادق والتأمين الصحي الخدمات القانونية.

ثالثا: بطاقة فيزا إلكترونيك: توفر هذه البطاقة للحامل إمكانية السحب الآلي للنقود على المستوى الدولي من خلال أجهزه الصرف الآلي والتي تختلف حيثياتها من دولة إلى أخرى على حدة. [3]

أما بخصوص التصنيفات المعطاة لبطاقات الائتمان بناءا على الحدود الائتمانية (السقف الإئتماني) الممنوحة لحاملها فهي على ثلاثة أنواع كالتالي:

---

[1]- رياض فتح الله بصله، المرجع السابق، ص 29.

[2]- عبد الوهاب إبراهيم سليمان، البطاقات البنكية، دراسة فقهية اقتصادية تحليلية، الطبعة، الثانية، دار القلم للنشر والتوزيع، دمشق سوريا، 1998، ص 37.

[3]- معادي أسعد صوالحة، المرجع السابق، ص 52.

* البطاقات المحليه ذات السقف الائتماني على الحدود والذي لا يتجاوز عدد مبلغ معين، بحيث تمنح هذه البطاقة لطالبيها من فئات الموظفين والأفراد العاديين شريطة وجود حدود معينة من القدرة والملاءمة المالية، الشيء الذي يجعل منها أيسر من البطاقات الموالية نظرا لكون درجة المخاطرة فيها ستكون قليلة أمام استخدامها على المستوى المحلي وبالتالي ستكون بعيده عن أي تلاعب وحتى ولو حصل ذلك فسيكون أمر اكتشافه ممكنا.

رابعا: البطاقة الدولية: تأتي هذه البطاقات في شكل مضاد لسابقاتها (أكثر صعوبة) الشيء الذي يتطلب من حامليها ملاءة وقدرة ماليه تفوق تلك المطلوبة في البطاقات المحلية وتكون موازية إلى حد ما لتلك الضمانات التي تمنح بواسطتها، خاصة وإن مثل هذه البطاقات تسمح لحاملها إمكانية الاستعمال على المستوى الدولي مما يولد معه احتماليه تعرضها للتلاعب والتزوير في حالة فقدها أو سرقتها، الشيء الذي سيصعب بالتالي من إمكانية المراقبة المستمرة لها من طرف السلطات المختصة.

خامسا: البطاقة الذهبية: يشكل هذا النوع من البطاقات قمة الهرم الاجتماعي الممنوح للعميل حاملها ولعل هذا يأتي متماشيا مع الشروط المعقدة التي تفرضها الجهات المصدرة لها في مواجهة العميل طالب الخدمة نظرا لما تمنحه مثل هذه البطاقات من امتيازات مالية وسيولة نقدية تفوق بكثير تلك المبالغ الممنوحة في إطار سابقاتها من جهة، وتزايد حدة المخاطرة نظير استعماله من جهة ثانية. [1]

- **سادسا: بطاقة الخصم أو التسديد على أقساط:** أو ما يسمى crédit card، بحيث يمنح هذا النوع من البطاقات للحامل ميزة تسديد المبلغ الإجمالي الذي قام الحامل بإنفاقه من الائتمان الممنوح له من البنك المصدر على أقساط بحسب ما هو متفق عليه في العقد المبرم بينهما بحيث يحتسب البنك المصدر في هذه الحالة الفوائد من إجمالي المبلغ المقسط وغير المسدد، فهي تقدم إذا لحاملها ائتمانا حقيقيا يستطيع من خلال استخدامها انجاز عمليات الشراء والسحب دون أن يكون له رصيد ودون أن يكون ملزما بدفع كامل المبلغ المستحق في ذمته للبنك. [2]

[1]- عبد الحكيم عثمان، أحكام البطاقات الائتمانية في القانون والآراء الفقهية الاسلامية، الطبعة الأولى، شركة الجلال للطباعة، العامرية، بغداد، 2007، ص 03.

[2]- أحمد شكري السباعي، الوسيط في الأوراق، الجزء الثاني في آليات وأدوات الوفاء والشيك، الطبعة الأولى، دار نشر المعرفة، مطبعة المعارف الجديدة، الرباط، المملكة المغربية، 1998، ص 410.

الفرع الثالث: خصائص ومزايا بطاقات الدفع الإلكتروني

أولا: خصائص بطاقة الدفع الإلكتروني

من خلال التعريفات السابقة تبين لنا أن البطاقة الدفع الإلكتروني كوسيلة وفاء الالكترونية خصائص تختلف عن خصائص الوفاء بالوسائل التقليدية ونستطيع أن نستخلص هذه الخصائص على النحو الأتي:

1. بطاقات الدفع الإلكتروني تقوم على علاقة ثلاثية الأطراف:

بطاقات الدفع الإلكتروني تقوم على علاقة ثلاثية، وهي علاقة المصدر بالحامل وعلاقة الحامل بالتاجر، وعلاقة المصدر بالتاجر وهي بذلك تختلف عن وسائل الوفاء التقليدية (الأوراق النقدية، والأوراق التجارية) من ناحية أن الوفاء بهذه الوسائل يتم بتدخل الدائن والمدين فقط.

2. بطاقات الدفع الإلكتروني ترتب إلتزامات حقيقية في ذمة أطرافها.

كل طرف من أطراف البطاقة يرتبط بالآخرين بعقود مستقلة يترتب عليها إلتزامات في ذمة أطرافها، ومصدر البطاقة يرتبط بحاملها بعقد يلتزم بمقتضاه إصدار بطاقة مقبولة كوسيلة للوفاء لدى عدد كبير من المحلات التجارية، وكذلك بفتح حساب بمبلغ معين لحامل البطاقة لاستخدامه في الوفاء بكافة مشترياته كذلك يرتبط مصدر البطاقة بالتجار الذين يقبلون البطاقة في الوفاء بعقد يلتزم بمقتضاه تقديم صك مال الوفاء لهم بقيمة المشتريات التي نفذها الحامل في حدود سقف البطاقة. [1]

3. تنظيم العلاقة بين أطراف بطاقات الدفع الإلكتروني:

إن كل طرف من أطراف بطاقات الدفع الإلكتروني يرتبط بالآخر بعقد مستقل فالعقد الأول يربط بين مصدر البطاقة والحامل أما العقد الثاني فيربط بين مصدر البطاقة والتاجر أخيرا العقد الثالث وهو عقد البيع الذي يربط بين حامل بطاقة والتاجر وهذا العقد يكون سببا للعقدين الآخرين وهذا ما يميز بطاقة الدفع الإلكتروني عن غيرها من وسائل الوفاء[2]

عدم خضوع بطاقة الدفع الإلكتروني للتنظيم القانوني الخاص بوسائل الوفاء التقليدية:

من أهم عوامل تطور عمليات البنوك هو عدم خضوع هذه الأخيرة لتنظيم قانوني الذي يترتب عليه جهودكه فبطاقة الدفع الإلكتروني تمتاز عن غيرهم من وسائل الوفاء التقليدية في أن المشروع لم يتدخل فيها بوضع نصوص تشريعية محددة بشأنها لذلك فهي تخضع

[1]- فايز نعيم رضوان، بطاقة الوفاء، دار النهضة العربية، القاهرة، جمهورية مصر العربية، 1999، ص12.
[2]- فايز نعيم رضوان، المرجع نفسه، ص: 13

للقواعد العامة المطبقة على النقود كوسيلة للوفاء وعلى القواعد العامة في النظام المصرفي بالإضافة إلى القواعد العامة الواردة على العقود في القانون المدني وفي غياب هذه النصوص التشريعية يكون المؤسسات المالية التي تهتم بإصدار بطاقات الدفع الإلكتروني فرصة لتطويرها. [1]

ثانيا: مزايا بطاقة الدفع الإلكتروني:

1. بالنسبة للمصدر:

- إنخفاض تكاليف التعامل بالبطاقة مما يؤدي إلى خفظ تكاليف تشغيل الحسابات المصرفية.
- البطاقة وسيلة آمنة للوفاء عن غيرها وتعد حاجزا قويا من السرقة وأكثر أمنا من الشيك.
- البطاقة وسيلة لتقديم الإئتمان للعملاء كصيغة بسيطة ومرنة لتلبية حاجياتهم.
- البطاقة وسيلة لتحقيق الربح أكثر مما تحققه القروض للبنوك.

2. بالنسبة للتاجر:

- استفادة المتاجر من الضمان الكامل للوفاء وذلك بإستفاء أثمان السلع المشترات من قبل الحامل وضمن السقف المسرح به عن طريق المصدر الذي لا يملك إلا أن يدفع أثمانها للتاجر.
- إصلاح خزينة التاجر وهذا ناتج عن سرعة إئتمان حساب التاجر بقيمة المعاملات المنفذة بالبطاقة. [2]
- استفادة التاجر من المساعدات الفنية والتجارية حيث يقوم المصدر للبطاقة. في الغالب بحملة دعائية عن بطاقته، لغايات ترويجها، وتعريف المواطنين بها، وبالتبعية فأنه يعلن عن المحلات التي تقبلها في الوفاء، كذلك تزويد التاجر بالعلامات والشعارات الدالة على إنضمامه للشبكة المصدرة، والآلات اللازمة لسير عملية الوفاء بالطاقة.
- مزايا البطاقة للحامل عدم المخاطرة بحمل مبالغ كبيرة من النقود فالشراء بواسطة البطاقة أعطت حاملها ميزة عدم حمله نقدية كبيرة، وجنبته بالتالي مخاطر فقدهاأو سرقتها.
- عدم الحاجة إلى الشيكات عدم حاجة الحامل لطلب دفاتر شيكات، أو تحريرها عند قيامه بعمليات الشراء. [3]

---

[1]- فايز نعيم رضوان، المرجع السابق، ص: 13

[2]- سامح محمد عبد الحكيم، الحماية الجنائية لبطاقات الإئتمان، جرائم بطاقة الدفع الإلكتروني، دار النهضة العربية، جمهورية مصر العربية، 2003، ص31.

[3]- سامح محمد عبد الحكيم، المرجع السابق، ص22.

- الإستفادة من الإئتمان عند قيام الحامل بالوفاء للتاجر، سواء أكان هذا الوفاء فوريا أم بأجل، فأنه يستفيد من الإئتمان الممنوح له من المصدر دون الحاجة لطلب إئتمان من التاجر.
- الرقابة الدقيقة على نفقاته حيث يستفيد الحامل من خدمة إرسال الكشوف الشهرية المفصلة بصفة دورية بواسطة البريد للحاصلين على البطاقة، ويسمى هذا الكشف بكشف حساب البطاقة.
- البطاقة مستند واحد متعدد الوظائف فالبطاقة يمكن الوفاء بها داخليا وخارجيا، وتمكن الحامل من إجتياز الحدود دون حمل النقود.
- البطاقة مستند واحد يلائم كل الطبقات إدراكا من مصدري بطاقة الدفع الإلكتروني، للتنوع بين فئات المجتمع، ولاختلاف حاجات المواطنين، وتباين مقدرتهم المالية، فقد أصدروا عدة فئات من البطاقات، فمنها المحلية، والدولية، والذهنية ويختلف السقف الأعلى لكل فئة.
- البطاقة سهلة الاستعمال ولا تشغل حيزا وتحظى بالقبول العام. [1]

المطلب الثاني: الاستخدام غير المشروع للبطاقة أثناء فترة صلاحيتها.

نحاول في هذا المطلب شرح الاعتداء بالحصول على بطاقات الدفع بمستندات مزورة في الفرع الأول وإساءة استخدامها أثناء فترة صلاحيتها في الفرع الثاني.

الفرع الأول: الحصول على بطاقة الدفع بمستندات مزورة:

الأصل أن الحصول على بطاقة الائتمان يتم طبعا للقواعد المعمول بها في الجهة المصدرة للبطاقة وحسب المستندات المطلوبة وبشرط أن تكون مستندات صحيحة وليست مخالفة للحقيقة، فلا يجوز أن يتقدم طالب بطاقات الدفع بأسماء منتحلة وعناوين وهمية أو أي ضمانات غير حقيقية وإلا تعرض لعقوبات جزائية فضلا عما يتحمله البنك من خسائر مادية نتيجة استخدام البطاقة في شراء السلع بمبالغ كبيرة. [2]

أولا: التكييف القانوني للفعل الإجرامي:

تكيف الجريمة على أنها جريمة نصب وقد عرفها، المشروع في نص المادة 372 من قانون العقوبات الجزائري كما يلي: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو مسندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء

[1]- المرجع نفسه، ص 33.
[2]- معادي أسعد صوالحة، بطاقات الائتمان النظام القانوني وآليات الحماية الجنائية الأمنية (دراسة مقارنة) الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2011، ص 286.

إلتزامات أو الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها... على الأكثر." [1]

ثانيا: أركان جريمة النصب:

1- الركن المادي:

وفقا لمضمون المادة 372 من قانون العقوبات فالركن المادي يتكون بدوره من هذه العناصر الثلاثة السلوك الإجرامي للنصب وسوء استخدام وسيلة من الوسائل التعليمية التي أوردها المشرع في المادة 372 على سبيل الحصر وعلى أساسها قامت الجهة المصدرة بمنح البطاقة للعميل ونتيجة النصب المعاقب عليها والتي بتحققها تتم الجريمة والتي اؤدي إلى وقوع الضحية في الخدعة وتسليم المال للجاني. [2]

2- الركن المعنوي:

جريمة النصب جريمة عهدية ولهذا يشترط لقيامها توافر القصد الجنائي والقصد في الجريمة يتكون من شقين قصد عام ومؤداه أن يكون الجاني عالما بالاحتيال وله الإرادة في الاتيان وحصول النتيجة والقصد فيتمثل في نية التملك والاعتداء على مال الغير. [3]

3- الركن الشرعي:

ويتمثل في النص القانوني والمجرم لهذا الفعل طبقا للمادة 372 من قانون العقوبات الجزائري والتي جاء فيها الحبس من سنة على الأقل إلى خمس سنوات إلى الأكثر وبغرامة من 500 إلى 20000دينارا جزائري بالإضافة إلى الحرمان من جميع الحقوق الواردة في المادة 14 من قانون العقوبات وهي المنع من الإقامة لمدة سنة على الأقل و5 سنوات على الأكثر.

---

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

[2]- عبد العزيز سعد، جرائم الاعتداء على الأموال العامة والخاصة، الطبعة الرابعة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص 99.

[3]- أسامة حمدان الرقب، جرائم الاحتيال (الأساليب- المظاهر- العلاج)، الطبعة الأولى، دار ياف العلمية للنشر والتوزيع، عمان، 2012، ص 27.

الفرع الثاني: الاستخدام غير المشروع للبطاقة في عملية السحب والوفاء.

الاستخدام غير المشروع لبطاقات الدفع الالكتروني إما أن يتم من قبل الشرعي للبطاقة وهو الحالة الأكثر شيوعا بين أطراف العقد، وإما أن يتم من قبل التاجر أو من قبل المصدر أم الاتفاق بين أكثر حيث سأتناول أولا تجاوز الحامل لسقف البطاقة وبعدها أعرج إلى عمليات غسيل الأموال ثانيا.

أولا: تجاوز الحامل لسقف البطاقة:

يلتزم الحامل، وفق العقد الصرم بينه وبين المصدر، بعدم تجاوز مبلغ السقف المحدد للبطاقة، فإن تجاوزه فإنه يعد بذلك مستخدما للبطاقة استخداما غير مشروع، وتجاوز الرصيد يكون بإحدى الحالتين إما تجاوز الحامل لرصيده في السحب أو عند الوفاء بثمن السلع والخدمات وذلك على النحو الآتي: [1]

1. تجاوز الحامل لرصيده في السحب:

من الوظائف التي تؤديها بطاقات الدفع الإلكتروني السماح لحامليها بسحب الأموال وهذا لسحب يكون بإحدى الصورتين: الصورة الأولى: هي بسحب الأموال من خلال أجهزة الصراف الآلي وذلك باستخدام البطاقة والرقم السري وفي حدود السقف المسموح به يوميا والصورة الثانية هي بسحب الأموال من داخل فروع البنوك المصدرة للبطاقة. [2]

ويحكم نظام سحب النقود بصفة عامة عقد الحامل الذي قد يحيز، أولا يجيز للحامل تجاوز رصيده من خلال السحب، ويحدد الفائدة على المبالغ التي تم تجاوز الرصيد بها ومنهم من يرى بأنها خيانة أمانة وتعسف في استعمال الحق وسرقة واحتيال يعاقب عليها القانون ومنهم من يعتبر ذلك من الفقهاء أنها مجرد إخلال بالالتزامات التعاقدية بين الحامل والبنوك وبالتالي تتم مساءلة الجاني في الشق المدني دون الجزائي. [3]

2. تجاوز الحامل لرصيده في الوفاء:

تحتم الإجراءات المتبعة عن استخدام البطاقة في الوفاء على التاجر أن يحصل على تعويض من مصدر البطاقة على أي عملية بيع ومهما كان مبلغها قبل إتمام عملية البيع وبالتالي يبدوا صعبا من الناحية العملية تجاوز العامل لسقف البطاقة [4] في الوفاء، فإذا قبل التاجر البطاقة من الحامل دون الحصول على تعويض لذلك من المصدر فإنه يتحمل نتيجة

---

[1]- أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقة الدفع الإلكتروني، الطبعة الأولى، دار المسيرة للنشر والتوزيع والطباعة، 2010، ص 129.

[2]- المرجع نفسه، ص 130.

[3]- عبد الكريم الردايدية، جرائم بطاقات الائتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013، ص 59.

[4]- المرجع نفسه، ص ص 59، 60.

هذا القبول إما بالمساءلة الجزائية عن جريمة النصب أو إخلال بالإلتزام يترتب عليه المسؤولية العقدية لتعويض الضرر. [1]

ثانيا: استعمال البطاقة في عملية غسيل الأموال من قبل الحامل:

في هذه الحالة، فإن البطاقة المستخدمة في عملية الوفاء التحويل هي بطاقة صحيحة ومستخدمة من قبل حاملها الشرعي، إلا أن الغاية التي استخدمت من أجلها غير مشروعة والتي لا تعد من الوظائف التي استخدمت البطاقة لأجلها وقد أثار استخدام بطاقات الدفع الإلكتروني كبديل للتعامل بالنقود الورقية العديد من المشكلات وخاصة ما تعلق منها بغسيل الأموال ويكون ذلك بطرقتين: [2]

1- استخدام البطاقة في أجهزة الصراف الآلي:

وغالبا يقوم العميل باصدار طلبات متتالية للبنك المصدر لإصدار بطاقات وفاء للاستخدامات المحلية والدولية له، لموظفيه ومعاونيه وأفراد عائلته ولأي أفراد آخرين يتعاملون معه بضمان ودائع الشركة النقدية والعينية ويتم استخدام هذه البطاقات في مجال التحويلات المالية الإلكترونية عن طريق أجهزة الصراف الآلي في عملية غسيل الأموال بحيث يتم إجراء التحويلات المالية إلكترونيا التي تصل من الخارج وقبل أن تستقر يتم سحبها إلكترونيا أيضا ثم يتم تجميعها ويقوم العميل بتحويلها بمبالغ كبيرة إلى الخارج. [3]

ويقوم العميل بصرف المبالغ عن طريق البطاقة من أجهزة الصراف الآلي بطلب تحويل المال إليه باستخدام رقمه السري من الفرع مصدر البطاقة فيقوم الأخير على هذا الأساس بالتحويل تلقائيا وخصم القيمة من حساب (عملية) عميله والذي قد يكون تهرب بهذه الطريقة من القيود التي تكون مفروضة على التحويلات.

2- غسل الأموال بواسطة الوفاء بالبطاقة:

وتتم هذه العملية على ثلاثة مراحل

المرحلة الأولى: التوظيف (Placement)

حيث يتم إيداع الأموال المشبوهة المتأتية من الجريمة أو عمل غير مشروع في أحد البنوك المحلية أو الخارجية من أجل الحصول على بطاقة الدفع بقيمة الرصيد المودع[4]

---

[1]- محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2006، ص 195.

[2]- المرجع نفسه، ص 196.

[3]- أمجد حمدان الجهني، المرجع السابق، ص- ص، 134- 135.

[4]- المرجع نفسه، ص 136.

المرحلة الثانية: التغطية (Layorting)

وتتم في هذه المرحلة إخفاء أو تمويه علاقة الأموال مع مصادرها غير المشروعة فيتم استخدامها في شراء المعادن واللوحات الفنية الثمينة بطريقة مباشرة أو عن الغير بتسليمه بطاقة الدفع الإلكتروني أو الأنترنت باستخدام أنظمة الحماية والتشفير لضمان سرية المعاملات. [1]

المرحلة الثالثة: الدمج (Intégration)

حيث يتم بيع الأصول المادية نقدا، أو لقاء شيك أو حوالة مالية مسحوبة على بنك آخر من أجل دمج الأموال المغسولة في الاقتصاد. [2]

ثالثا: مدى انطباق النصوص القانونية على جريمة تبييض الأموال:

نص المشرع الجزائري على جريمة تبييض الأموال في المادة 389 مكرر من قانون العقوبات الجزائري والتي نصت على أنه:

1- تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات، على الإفلات من الآثار لفعلته.
2- إخفاء أو تمويه الطبيعة الحقيقية للمتلكات أو مصادرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية.
3- إكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية.
4- المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة إرتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه [3]

[1]- أمجد حمدان الجهني، المرجع السابق، ص 136.
[2]- المرجع نفسه، ص 89.
[3]- أنظر المادة 385 من قانون العقوبات.

1. الركن المادي: وتتمثل في:

فعل النقل والتحويل: نقل الأموال الناتجة عن نشاط مشبوه بنية تحويلها إلى أموال مشروعة.

فعل الإخفاء: وهو التستر على مصدر تلك الأموال

فعل التمويه: دمج تلك الأموال على أموال أخرى مشروعة لتظهر أنها أموال نظيفة.

محل الجريمة: الأموال التي تنتج عن مصدر مشبوه ويتم إستخدامها في أنظنة مشروعة. [1]

العلاقة السببية: الهدف تبيض المال القذر.

التنيجة الجرمية: تنظيف المال بعد القيام بالأفعال السابقة.

2. الركن المعنوي: ويتمثل في القصد العام والخاص كالآتي:

القصد العام ويقصد به عنصر العلم والإرادة أي توظسف الجاني المال القذر في أفعال أخرى لإزالة الشبهة. والقصد الخاص وهو عنصر النية وذلك بإعطاء صيغة شرعية لأموال غير شرعية. [2]

3. **الركن الشرعي:** المشرع الجزائري نص على العقوبة المقررة لها في قانون العقوبات الجزائري من المادة 389 مكرر 1 إلى المادة 389 مكرر 7 [3]

المطلب الثالث: الاستخدام غير المشروع للبطاقة خارج فترة صلاحيتها

بعد تطرقنا في المطلب الأول إلى الاستخدام غير المشروع للبطاقة خلال فترة صلاحيتها فقد يكون استخدام بطاقة الدفع الإلكتروني خارج فترة صلاحيتها وذلك في حالة استخدام البطاقة بعد إلغائها من قبل المصدر أو إذا تم استخدامها بعد إنتهاء مدة صلاحيتها وهذا ما سنتناوله على النحو الآتي:

[1]- فتحي محمد أنورغزت، جرائم العصر الحديث، الطبعة الأولى، دار الفكر والقانون، القاهرة، 2010، ص 278.
[2]- محمد عبد الله الرشدان، جرائم غسيل الأموال، الطبعة الأولى، دار قنديل للنشر والتوزيع، عمان، 2007، ص 278.
[3]- أنظر المواد من 389 مكرر 1- 389 مكرر7 من قانون العقوبات.

الفرع الأول: الاستخدام غير مشروع للبطاقة:

بعد إبرام العقد بين العميل والبنوك فإن التعامل بها يحدد بمدة معينة وغالبا ما تكون هذه المدة سنة واحدة وتمتلك الجهة المصدرة لها الحق في إلغائها أو سحبها من العامل إذا أساء استخدامها فقد يمتنع عن ردها للبنك ويستمر في استخدامها. [1]

أولا: الاستخدام غير المشروع للبطاقة الملغاة:

نشيرإبتداء إلى أنه يحق للمصدر وفي أي وقت إلغاء البطاقة دون إبداء أية أسباب ويستمد المصدر هذا الحق بصفته مالكا لبطاقة الدفع الإلكتروني وسلمها للحامل على سبيل الأمانة إلا أنه أورد صورا لبعض حالات إلغاء البطاقة في عقد الحالمل، وهي واردة على سبيل المثال لا الحصر واحتفظ لنفسه بحق إلغاء البطاقة في أي حالة أخرى يراها مناسبة لمثل هذا الإجراء وفق ما تمليه عليه مصلحته، وما ينتجه من وسائل لحماية البطاقة [2]

وفي الامتناع عن رد البطاقة الملغاة أو منتهية الصلاحية تعد خيانة للأمانة[3]

1- مدى إنطباق النصوص القانونية التقليدية على الجريمة:

قد عالج المشرع الجزائري هذه الجريمة في المادة 376 من قانون العقوبات الجزائري بقولها "كل من أختلس أو بدد بسوء نية أوراق تجارية أو نقودا أو بضاعة أو أوراقا مالية أو مخالفات أو أية محررات أخرى تتضمن أو تثبت إلتزام أو إبرام لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو الاستعمال أو لأداء عمل أجر شرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا لمالكيها أو واضعي اليد عليها أو حائزها يعد مرتكبا لجريمة خيانة الأمانة..." [4]

أ- **الركن المادي لجريمة خيانة الأمانة:** طبقا لنص المادة 376 من قانون العقوبات الجزائري يتمثل الركن المادي في ثلاثة عناصر :

الاختلاس والشديد: ويكون بنقل الشيئ من حيازة مؤقتة إلى حيازة دائمة بنية التملك كحامل البطاقة الذي رفض رجوعها إلى الجهة المصدرة بعد إنتهاء صلاحيتها.

محل الجريمة: وهو المال المنقول أو محررات وبطاقات الدفع تعتبر محررات.

---

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

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

[3]- علي عدنان الفيل، المرجع السابق، ص 42.

[4]- أنظر المادة 376 من قانون العقوبات.

تسليم الشيء: يلزم تسليم الشيء على شكل حيازة مؤقتة كوديعة فبطاقات الدفع الإلكتروني يجب إرجاعها عند إلغائها أو انتهاء صلاحياتها.

ب-**الركن المعنوي:** يشمل قصد عام وخاص:

العام وذلك أن الجاني يعلم أن فعله يعتبر جريمة يعاقب عليه القانون ورغم ذلك تتجه إرادته بإتيانه الخاص ويتمثل في نية الجاني في الحيازة والتملك وحرمان مالكه الأصلي منه. [1]

ج- **الركن الشرعي لجريمة خيانة الأمانة**: طبقا للمادة 376 من ق.ع.ج وبخصوص هذه الجريمة هناك عقوبات أصلية وأخرى كملية:

العقوبات الأصلية: الحبس من ثلاثة أشهر إلى خمس سنوات.

العقوبة التكميلية: بالرجوع إلى نص المادة 9 من قانون العقوبات التي حددت لنا جملة العقوبات التكميلية كالحرمان من الحقوق الوطنية والمدنية ويمكن أن يحكم على الحامل لعقوبات تكميلية إختيارية تتمثل في المنع من التعامل ببطاقة الدفع الإلكتروني لمدة أقصاها خمس سنوات. [2]

2- طرق استخدام البطاقة الملغاة:

يتمثل الاستخدام غير المشروع للبطاقة الملغاة من قبل الحامل، إما في الوفاء بها للتجار أو في سحب الأموال من أجهزة الصراف الآلي وذلك على النحو التالي:

أ- استخدام البطاقة الملغاة في الوفاء:

قد يقوم الحامل الشرعي باستخدام البطاقة الملغاة في الوفاء بثمن السلع والخدمات للتاجر الأمر الذي يؤدي إلى إلزام المصدر بالوفاء بهذه المبالغ للتاجر ما دام هذا الأخير لا يعلم بإلغاء البطاقة، نظرا لأن المصدر لم يزوده بآخر نشرة دورية تحضيرية تتضمن أرقاما لبطاقات التي جرى إلغائه [3] وإذا قام التاجر بالإتصال بمركز التفويض وحصل على الإذن بإجراء العملية ورقم التفويض أو إذا لم يقم الجهاز الإلكتروني (P.O.S) بفرض البطاقة

---

[1]- خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، رسالة مكملة لنيل شهادة الماجستير في الحقوق، محفوظ بن صغير، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016، ص 111.

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

[3]- بن شهرة شول، الحماية الجنائية للتجارة الإلكترونية، أطروحة مقدمة لنيل درجة دكتوراه في القانون، علي أجقو، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2010، ص 22.

على شاشته بأن البطاقة ملغاة وفي حالة استخدامها وهو يعلم أنها ملغاة فتتحول العملية إلى جريمة الخيانة والسرقة والاحتيال وبالتالي قيام المسؤول الجزائية.[1]

ب- استخدام البطاقة الملغاة في سحب الأموال:

لا يتصور في ظل الأنظمة الإلكترونية المطبقة في أعمال البنوك، قبول جهاز الصرف الآلي لعملية سحب الأموال بواسطة بطاقة ملغاة، حيث ترتبط هذه الأجهزة مباشرة بحسابات العملاء في البنك ويتم إدخالها وبرمجتها على سحب البطاقة في حال إدخالها بها، أو على الأقل رفضها ومما سبق أن تصرف الحامل المتمثل في استخدام البطاقة الملغاة في السحب لا ينطوي على أي جريمة[2]

ثانيا: الاستخدام غير المشروع للبطاقة منتهية الصلاحية:

يتم تدوين التاريخ الذي تنتهي فيه صلاحية البطاقة على وجه البطاقة وبأحرف بارزة وعند انتهاء صلاحية البطاقة يتم تجديدها تلقائيا، إلا إذا قام الحامل بإبلاغ المصدر بعدم رغبته في تجديد العقد، وهنا يجب عليه تسليم البطاقة للمصدر.

ورغم أن العقد يجدد تلقائيا، إلا أنه يتوجب على الحامل مراجعة المصدر وتسليمه البطاقة المنتهية الصلاحية واستلام بطاقة مثبت عليها تاريخ إنتاءه صلاحية جديد. [3]

ومن الممكن أن يستخدم الحامل بطاقته في الوفاء رغم انتهاء صلاحيتها إن هو نسي تجديدها أو احتفظ بالبطاقة القديمة رغم تسلمه البطاقة الجديدة، وتعتمد شراء السلع والخدمات بواسطتها حتى يحتج فيما بعد على الوفاء للمصدر بأنه لم يقم باستخدامها. [4]

كماأن الحامل قد يستخدم البطاقة المنتهية الصلاحية بصورة غير مشروعة إن هو أتفق مع التاجر على قبولها في الوفاء إضرارا بالمصدر، وذلك بأن يقوم التاجر بتزوير تاريخ انتهاء صلاحية البطاقة، أو يعلن عمدا تاريخ غير صحيح وبالنسبة لسحب الأموال من أجهزة الصراف الآلي فإنه يتصور أن يكون يتم بنجاح لأن هذا الجهاز لن يقوم بإرجاع البطاقة، أو يقوم برفضها نظرا للبرمجة المتبعة في تشغيله. [5]

---

[1]- بن شهرة شول، المرجع السابق، ص 23.
[2]- علي عدنان الفيل، المرجع السابق، ص ص 42، 43.
[3]- عبد الكريم الردايدة، المرجع السابق، ص 215.
[4]- علي عدنان الفيل، المرج السابق، ص 30.
[5]- المرجع نفسه، ص 42.

الفرع الثني: الاستخدام المقنع للبطاقة:

ويكون في ثلاث حالات سنتناولها كما يلي:

أولا: الإبلاغ غير الصحيح عن فقدان البطاقة أو سرقتها.

في هذه الحالة يقوم الحامل الشرعي للبطاقة بإبلاغ المصدر عن سرقة البطاقة أو فقدانها في حين أنها لا تزال في حوزته ويستمر في استعمالها سواء في سحب النقود أو الوفاء فأما عملية السحب فإن أجهزة الصراف الآلي الحديثة مبرمجة لرفض البطاقة المفقودة أو المسروقة وأما بالنسبة لعملية الوفاء فإن الحامل وخوفا من اكتشافه يقوم باستخدامها عند التجار الذين يتعاملون بآلة الطباعة اليدوية التي لا يمكن إكتشاف وضعية البطاقة من خلالها وهناك تجار يستعملون الجهاز الإلكتروني (POS) الذي يكتشف حالات الغش بسهولة وهذا يشكل احتيالا على التاجر الغرض منه تحصيل قيمة البضاعة من البنوك بدلا منه والاستلاء على مال البنك دون وجه حق. [1]

ثانيا: التواطؤ ما بين الحامل والغير:

ويتم التواطؤ بين الحامل الشرعي، والغير من أجل التحايل على المصدر باستخدام إحدى الطريقتين التاليتين:

أن يقوم الحامل بإعطاء البطاقة للغير من أجل استعمالها في السحب وتزوير توقيعه وبعد ذلك يقوم حامل البطاقة بالاعتراض على عمليات السحب، ويطعن بتزوير توقيعه حتى لا يخصم المبلغ المسحوب من حسابه.

أو أن يقوم الحامل الشرعي للبطاقة بإعطاء الغير بيانات بطاقته في الوفاء أو السحب وإعطاء رقمه السري بهدف تمكينه من تزوير بطاقة على غرارها، واستعمالها في الاستلاء على أموال المصدر والتاجر.[2]

ثالثا: الإدعاء الغير الصحيح بعد استخدام البطاقة:

وتتحقق هذه الحالة عندما يقوم الحامل باستخدام بطاقته في الوفاء أو السحب أثناء السفر وهند عودته لبلاده يدعي أنه لم يسافر، وإن لم يستخدم البطاقة في البد الذي تم استخدام البطاقة فيها، ويثبت ذلك عن طريق جواز سفر آخر يحمله. [3]

---

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

[2]- المرجع نفسه، ص ص، 143، 144.

[3]- وسام فيصل محمود الشواورة، المسؤولية القانونية عن الاستخدام غير المشروع لبطاقات الائتمان، الطبعة الأولى، دار وائل للنشر، عمان، 2013، ص 86.

المبحث الثاني:الاستخدام غير المشروع لبطاقة الدفع الالكتروني من قبل التاجر والمصدر:

ترتبط العلاقة التعاقدية لبطاقة الدفع الإلكترونية بين الجهة المصدرة والتاجر بحيث يترتب عن ذلك إلتزامات أما الغير فهو خارج العلاقة التعاقدية للبطاقة ولا يترتب عليه إلتزامات فقد تقع البطاقة في يده في حالة ضياعها أو يسعى للاستلاء عليها أو تزويرها أو سرقتها وسنخصص مبحثنا هذا لدراسة مختلف الجرائم التي يقوم بها أطراف العلاقة التعاقدية وكذلك الغير على حد سواء.

المطلب الأول: الاستخدام غير المشروع للبطاقة من قبل المصدر والتاجر.

يتم استخدام بطاقة الدفع الإلكتروني بشكل غير مشروع بواسطة التاجر القابل لها والمصدر ولا يقصد بالمصدر هنا الشخص المعني، وإنما الأشخاص القائمين على إدراكه، أو الذين يعملون لديه وسوف أتناول ذلك في ثلاثة فروع، الفرع الأول طرق التلاعب في بطاقة الدفع الإلكتروني التي يمارسها موظفوا المصدر ونتاول في الفرع الثاني طرق التلاعب في بطاقة الدفع الإلكتروني التي تمارس من التاجر وتخصص الفرع الثالث مسؤولية موظفوا البنك والتجار عن الأعمال غير المشروعة. [1]

الفرع الأول: طرق التلاعب في بطاقة الدفع الإلكتروني التي يمارسها موظفوا المصدر:

إن المصدر كشخص معنوي لا يباشر صلاحيته بنفسه، وإنما بواسطة ممثليه وغالبا ما تتخذ أساليب التلاعب التي تقع مع موظفي المصدر أحد الأشكال الآتية:

أولا: تواطؤ موظف المصدر مع حامل البطاقة: وذلك بارتكاب أحد الأفعال الآتية:

- استخراج بطاقة سليمة عليها بيانات مزورة.
- السماح للحامل بتجاوز حد البطاقة في السحب.
- السماح للحامل بالشراء بموجب بطاقة منتهية الصلاحية، أو بعد صدور قرار بسحبها من التعامل.
- التأخر عمدا في إلغاء البطاقة بعد التبليغ الكاذب عن فقد البطاقة أو سرقتها حتى يتمكن الحامل من إتمام أكبر قدر من عمليات الشراء.

[1]- لبنى عمر سقاوي، المسؤولية المصرفية في الاعتماد المالي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006، ص 252.

ثانيا: تواطؤ موظفوا المصدر مع التاجر في ارتكاب بعض الأفعال :

- تجاوز السحب في صرف قيمة سندات البيع.
- اعتماد سندات صدرت استنادا إلى بطاقات وهمية، أو مزورة أو ملغاة أو منتهية الصلاحية.
- السماح للتاجر بإدخال رقم البطاقة على الجهاز الإلكتروني يدويا مما يسمح له بإدخال رقم البطاقة على فواتير دون وجود البطاقة عنده أصلا. [1]

ثالثا: تواطؤ موظف المصدر مع أفراد العصابات:

وذلك بإعطائهم بيانات الدفع الإلكتروني الصحيحة الصادرة والمسلمة لحامليها وذلك لاستخدامها في تقليد أو اصطناع هذه البطاقات. [2]

الفرع الثاني: طرق التلاعب في بطاقة الدفع الإلكتروني التي تمارس من التاجر:

ونقصد بالتاجر الجهة التي تقبل من حاملها كوسيلة دفع مقابل السلع والخدمات المقدمة منها لهؤلاء العملاء، وذلك بشرط توقيعهم للتاجر على إشعارات البيع، ولا يحق لأي جهة قبول هذه البطاقة من العملاء كوسيلة دفع دون وجود تعاقد مع أحد المصدرين في هذا المجال الذي يقوم بتزويد التاجر بالأجهزة اللازمة للتعامل في هذا النشاط، سواء أكانت الأجهزة يدوية أو إلكترونية ومستلزمات التشغيل الخاصة بها (سندات البيع) على أن يقوم التاجر بتحصيل قيمة تلك السندات من المصدر المتعاقد معه.

ويقوم التاجر بدور كبير في إتمام عمليات البيع أو تقديم الخدمة باستخدام بطاقة الدفع الإلكتروني، فهو الذي يقوم باستخدام الآلة، وسندات البيع المسلمة له من المصدر المتعاقد معه، كما أنه يقوم بفحص البطاقة والتأكد من صلاحياتها، والتحقق من شخصية حاملها الحصول على الموافقة لاجراء العملية عن طريق الأدوات المسلمة له لاتمام الشراء، ولذل فإن المجال يكون واسعا أمام التاجر للتزوير، والتلاعب من خلال استخدام اللآلات اليدوية أو الإلكترونية على النحو التالي:[3]

أولا: طرق التلاعب التي يمارسها بعض التجار باستخدام الجهاز اليدوي:

وتتخذ هذه الطرق إحدى الأشكال الآتية:

- قيام بعض التجار بشراء سندات بيع من بعض الأفراد مطبوع عليها أرقام بطاقات عملاء مزورة، وإن كانت البيانات صحيحة لأنها أصطنعت على غرار بيانات بطاقة

[1]- أمجد حمدان الجهني، المرجع السابق، ص 154.
[2]- المرجع نفسه، ص 146.
[3]- المرجع نفسه، ص ص، 146، 147.

موجودة بالفعل، ثم يقومون بطباعة رقم أجهزتهم عليها وذلك لتحصيل ما تم التعامل معه من خلالها على الرغم من عدم قيامهم ببيع أو تأدية أية خدمات لهؤلاء العملاء وهذا الفعل يتمثل في جريمة احتيال واستلاء على أموال الغير بدون وجه حق. [1]

- طباعة أرقام بطاقات العملاء المتعاملين معهم على سندات خالية دون طباعة رقم الآلة وبيعها لتجار آخرين يقومون بأخذ الموافقات وتحصيل قيمتها.
- تقديم سندات مطبوعة عليها أرقام بطاقات عملاء وأرقام موافقات وتاريخ على الرغم من أن تلك البطاقات مبلغ عن سرقتها أو فقدانها بتاريخ سابق على عملية البيع وهذا يعني قيام هؤلاء التجار بشراء البطاقة المفقودة أو المسروقة أو المزورة، واستخدامها في عمليات بيع وهمية وتحصيل قيمتها دون وجه حق. [2]
- تغيير المبالغ الأصلية في سندات البيع بمغافلة حامل البطاقة وخاصة العملاء الأجانب.
- كتابة أرقام موافقات وهمية على السندات بعد الإدعاء بتعطل الآلة الإلكترونية حتى يتمكنو من صرف قيمتها. [3]
- قيام بعض التجار بإتمام عملية البيع بواسطة بطاقات الدفع الإلكتروني على الرغم من إبلاغ مركز البطاقات له بعدم وجود موافقة، ويتحقق ذلك بقيام التاجر بتجزئة قيمة عملية البيع على سندات بيع متعددة، ومبالغ أقل من الحد المطلوب، ثم يقوم التاجر بعد ذلك بتحصيل قيمة هذه السندات من المصدر. [4]

ثانيا: طرق التلاعب التي يمارسها بعض باستحدام الجهاز الإلكتروني (P.O.S)

ومن طرق التلاعب التي يمارسها بعض التجار ما يلي:

- إجراء اتصالات دولية وتحميل القيمة على البطاقات الدفع الإلكتروني الممغنطة الخاصة بالغير فبمناسبة قيام بعض مراكز خدمة رجال الأعمال بتقديم خدمات الاتصالات الدولية، والفاكس يحصلون على أرقام بطاقات بعض العملاء خفية ويحملون عليها قيمة المكالمات التي تتم نقدا من جانب البعض الآخر من العملاء ولم يتم سدادها بعد للجهة المعنية. [5]
- قيام التاجر بوضع جهاز قارئ يتم النسخ بواسطته على جهاز البيع الإلكتروني حيث يقوم بطباعة البيانات على بطاقة أخرى لاستعمالها في علميات بين وهمية دون علم الحامل. [6]

---

[1]- وسام فيصل محمود الشواورة، المرجع السابق، ص 88.
[2]- أحمد حمدان الجهني، المرجع السابق، ص 148.
[3]- أمجد حمدان الجهني، المرجع السابق، ص 149
[4]- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والحاسب الآلي في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2002، ص 383.
[5]- عبد الكريم الردادية، المرجع السابق، ص65.
[6]- وسام فيصل محمد الشواورة، المرجع السابق، ص 89.

- قيام بعض التجار البطاقات المزورة من العملاء، والتلاعب في البرامج الخاصة بالآلة الالكترونية بحيث يتم تعطيل العمل به أثناء عملية قراءة البطاقة حتى لا يتم اكتشاف أنها مزورة، واستخدامها في صرف مبالغ من البنوك. [1]
- قيما بعض التجار باستخدام البطاقات التي ليست لها أرصدة كافية للصرف وذلك عن طريق إجراء عمليات بيع عديدة بمابلغ صغيرة أقل من الحد المطلوب وأخذ الموافقة عليها، وصرفها من البنك، ثم يتضح بعد ذلك عدم وجود أرصدة لأصحاب هذه البطاقات وهذا بهدف الاستلاء على أموال الغير وصرفها دون وجه حق.[2]

الفرع الثالث: مسؤولية موظفوا البنك والتجار عن عدم مشروعية أعمالهم:

إن موظفوا البنك والتجار سيسئلون عن أفعالهم غير الشرعية ضد بطاقات الدفع الإلكتروني وهذا ما سنتناوله في الفرع.

أولا: **مسؤولية موظفي البنك.**

وتتمثل الجرائم التي يقوم بها عند اتفاقه مع حاملها في السماح له بتجاوز سقف رصيدها أو استعمال بطاقة منتهية الصلاحية، أو بعد صدور قرار إلغائها، أو مساعدته على استخراج بطاقة مزورة والتي يسأل عنها النحو التالي:

أ- **جريمة الاشتراك في التزوير واستعمال الضرر:**

وفي هذه الحالة يسأل كشريك في التزوير واستعمال المحررات المزورة لمساعدة العميل في استخراج بطاقة الدفع المزورة، وذلك عندما يقبل المستندات المزورة لاستخراج البطاقة وبالتالي فهو سهل من مهة الجاني مع علمه المسبق بأن تلك السندات مزورة وبالنسبة للعقوبة وحسب نص المادة 221 من قانون العقوبات فإن الشريك في جريمة التزوير استعمال المزور يعاقب بنفس عقوبة الفاعل الأصلي.[3]

ب-**جريمة الرشوة:**

تقوم جريمة الرشوة في حق موظف في حالة اتفاقه مع العميل في حالة انجازه لأفعال غير شرعية ذكرناها سابقا، وذلك مقابل مبلغ مالي يمنحه العميل للموظف لقاء هذه الخدمات. [4]

---

[1]- أحمد حمدان الجهني، المرجع السابق، 152.
[2]- المرجع نفسه، ص 153.
[3]- أنظر المادة 221 من قانون العقوبات
[4]- عبد الكريم الردايدة، المرجع السابق، ص 229.

وجريمة الرشوة كما نص عليها المشرع الجزائري في قانون العقوبات الجزائري وأحالها إلى قانون 06-01 المتعلق بالوقاية من الفساد ومكافحته. [1] وذلك بموجب المادة 25 منه والتي نصت على أنه: "يعاقب بالحبس من سنتين (02) إلى عشرة (10) سنوات وبغرام من 20.000 إلى 1.000.000 دج"

كل من وعد موظفا بمزية غير مستحقة أو عرضها عليه أو منحه إياها بشكل مباشر أو غير مباشر، سواء كان ذلك لصالح الموظف نفسه أو لصالح شخص آخر أو كيان آخر لأداء أو كيا آخر لأداء عمل الامتناع عمل من واجباته.

وفيما يخص أركان جريمة الرشوة فلها صورةتان الأولى في الصورة السلبية من خلال ما ذكر في المادة 25 في فقرتها الثامية، حيث أن الركن المفترض هو صفة الجاني ويجب أن يكون موظف عمومي، وأما الركن المادي فهو القيام يسلوك الطلب أو قبول المزية وهي محل الجريمة، وتكون هذه المزية بصور عديدة فقد تكون مادية كما قد تكون معنوية صريحة أو ضمنية وذلك مقابل قيامه أو امتناعه عن القيام بعمل في وظيفته. [2]

وأما الركن المادي في الصورة الإيجابية يتمثل في قيام شخص ما بوعد الموظف العمومي بمزية غير مستحقة وأن يكون هذا الوعد صادق من أجل إغراء الموظف العمومي وحمله على القيام بما يطلبه منه، بأن يقوم بعمل أو يمتنع عن عمل في إطار وظيفته.

أما بالنسبة للركن المعنوي فتشترك الصورتين في الركن المعنوي والذي يشمل عنصري العلم والإرادة حيث يجب أن يكون موظف البنك على علم بأن هذا السلوك يمثل جريمة رشوة من خلال أنه موظف عمومي ويعلم أن هذه المزية غير مستحقة عند الطلب والقبول. [3]

وأما الركن الشرعي لهذه الجريمة فقد نص عليها المشرع الجزائري بموجب المادة 25 من القانون المتعلق بالوقاية من الفساد ومكافحته وتشمل العقوبات الأصلية لهذه الجريمة الحبس من سنتين إلى 10 سنوات وغرامة مالية من 200.000 إلى 1.000.000 دج. [4]

وعقوبات تكميلية منصوص عليها في المادة 9 من قانون العقوبات الجزائري.

---

[1]- القانون 06-01 المؤرخ في 21 محرم 1427 هـ، الموافق لـ 20 فبراير2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، عدد14،السنة 43، الصادرية بتاريخ 8مارس2006.

[2]- أحسن بوسيقيعة، المرجع السابق، ص 94.

[3]- المرجع نفسه، ص 104.

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

1- مسؤولية موظف البنك في حالة إتفاقه مع التاجر:

وتكون هذه المسؤولية من خلال عذع أفعال يقوم بها الموظف لمساعدة التاجر على أفعاله المجرمة مقابل الحصول على مصلحة معينة من طرف التاجر، ومن بين هذه الأفعال قبوله التعامل بمستندات بيع لبطاقة دفع مزورة أو وهمية أو منتهية الصلاحية وأيضا في حالة السماح بعملية التعامل في مستندات للبيع وصرف قيمتها متجاوزا بذلك السقف المحدد للسحب. [1]

2- مسؤولية موظف البنك في حالة إتفاقه مع أفراد العصابات:

وهذه العصابات تمتهن الإجرام فتقوم بعمليات إجرامية ضد بطاقات الدفع الإلكتروني عن طريق تزويرها وأخذ ما تحتويه من مبالغ مالية، وحتى تتم عملية التزوير تسعى هذه العصابات من أجل الحصول على بيانات وأرقام البطاقات الصحيحة، وحتى تسهل مهمتها تعتمد على موظفي البنك لتزويدهم بالبيانات اللازمة مقابل مبالغ مالية. [2]

ويسأل موظف البنك في هذه الحالة عن جريمتين هما:

أ- جريمة الرشوة: المنصوص عليها في المادة 25 من القانون 01-06 والتي تقوم في حق الموظف.

ب-جريمة إفشاء السر المهني: حيث تقوم هذه الجريمة في حق موظف البنك لأن يسمح للغير بالإطرع على أسرار مهنته، التي وكلت إليه بمناسبة وظيفته المتمثلة في تزويد أفراد العصابات ببيانات البطاقات التي تعود لحامليها حيث يقوم بذلك دون علمهم.

ولقد نص المشرع الجزائري على جريمة إفشاء السر المهني في المرسوم التشريعي رقم 93-10[3] بالحبس من 06 أشهر إلى خمس سنوات وبغرامة مالية قدرها 30.000 دج ويمكن رفع مبلغها إلى أكثر من ذلك حتى إلى أربعة أضعاف مبلغ المغنم المحتمل تحقيقه دون أن تقل هذه الغرامة على مبلغ المغنم نفسه أو يعاقب بإحدى العقوبتين فقط كل شخص تتوافر له بمناسبة مهنته... إلى الجمهور. [4]

وجريمة إفشاء السر المهني لها أركان وهي كالآتي:

---

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

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

[3]- المرسوم التشريعي رقم 93-10 المؤرخ في 2 ذي الحجة عام 1413، الموافق لـ 23 مايو سنة 1993، يتعلق بورصة القيم المنقولة، الجريدة الرسمية الجزائرية الديمقراطية الشعبية، العدد 34، السنة30، الصادرة بتاريخ 30 مايو 1993.

[4]- أنظر المادة 60 من القانون المتعلق بورصة القيم المنقولة.

- **الركن المادي:**

ويتمثل هذا الركن في أن يقوم الموظف بإفشاء السر المهني الذي وصل إليه بمناسبة تأدية وظيفته وفعل الإفشاء هو الكشف عن المعلومات وإيصالها للغير بأي طريقة دون مبرر قانوني بحيث يكون ما تم إفشاؤه سرّا وفق النظام الداخلي للوظيفة. [1]

- **الركن المعنوي:** العلم والإرادة حيث يجب أن يكون الفاعل عالما بأن محل فعلته سرا مهني وأنه حصل عليه بحكم وظيفته. [2]
- **الركن الشرعي:** بالرجوع إلى نص المادة 60 من المرسوم التشريعي 09-10 المتعلق ببورصة القيم المنقولة فإن العقوبات تشمل الحبس من 06 أشهر إلى 05 سنوات وبغرامة مالية قدرها 30.000 دينارا جزائري ويمكن رفعها إلى4 أضعاف المبلغ المغنم المحتمل تحصيله دون أن تقل عن مبلغ المغنم نفسه، أو بإحدى العقوبتين فقط. [3]

ثانيا: المسؤولية الجزائية للتاجر:

يتخذ الاعتداء على نظام بطاقة الائتمان من طرف التاجر عدة سبل منها تلاعب بعض التجار باستخاد الماكنة اليدوية أو الماكنة الإلكترونية وتقوم مسؤوليته الجزائية لعلمه أن البطاقة مسروقة أو مزورة ويسأل عن جريمة خيانة الأمانة عند علمه بأن البطاقة ملغاة أو منتهية الصلاحية وذلك قبل التعامل بها. [4]

1. مسؤولية التاجر عند الاستخدام غير الشرعي للماكينات اليدوية:

فهو يسأل عن جريمة استعمال محرر مزور فقيام التاجر بشراء إشعارات بيع رغم علمه بأنها تحمل أرقام مزورة وقيامه رغم ذلك باستعمال في تحصيل الأموال من بنكه سيخضعه لأحكام النصوص الجزائية المتعلقة بالتزوير واستعمال المزور وفضلا عن استعمال مستند مزور على النحو المسبق فإن جريمة النصب تتوافر في حق التاجرلأنه قدم مساعدة لشخص سارق البطاقة باستعماله لطرق احتيالية في استخدام إشعارات بيع بطاقة مسروقة ويسأل أيضا عن جريمة إخفاء أشياء مسروقة عند قبوله التعامل بأشياء مسروقة أي بطاقة مسروقة

---

[1]- عبد الودود أبو عمر، المسؤولية الجزائية عن إفشاء السر المهني، الطبعة الأولى، دار وائل للنشر والطباعة، عام 1999، ص ص 111، 114.

[2]- المرجع نفسه، ص 115.

[3]- عبد الودود أبو عمر، المرجع السابق، ص 115.

[4]- نضال سليم برهم، أحكام عقود التجارة الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2010، ص157.

رغم علمه بذلك وأيضا يعتبر شريكا في جريمة السرقة عندما يوقع على فاتورة غير صحيحة. [1]

2. مسؤولية التاجر عن الاستخدام غير الشرعي للماكينات الإلكترونية:

ويسأل التاجر عن جريمة الاتلاف والتعطيل للماكنة الإلكترونية سواء كان كليا أو جزئيا بهدف الحصول على أموال البنك.

وجريمة الاتلاف نص عليها المشرع الجزائري في المادة 394 مكرر من قانون العقوبات وتنطبق على التاجر لأنه عطل الماكنة الإلكترونية، وهو ما يمثل الركن المادي وقصد جنائي يتمثل في الحصول على أموال من البنك دو وجه حق. [2]

كما يسأل التاجر عن جريمة النصب والاحتيال وذلك بإتلافه للماكنة الإلكترونية بهدف تضليل البنك بوجود سبد دين وهو في الحقيقة غير موجود كما يسأل عن جريمة التزوير لأنه قا بتحريض الحقيقة وهو يمثل الركن المادي للجريمة وهذا يضر بمصالح البنك نظرا للاستلاء على أمواله بغير حق وهو الركن المعنوي. [3]

المطلب الثاني: الاستخدام غير المشروع للبطاقة من طرف الغير:

بالرغم كم مل الاحتياطات التقنية والعملية المتخذة أثناء صناعو البطاقات لتفادي تزويرها والتلاعب بحقوق أصحابها، إلا أنها بقيت غير محصنة من الاعتداءات غير المشروعة التي تتأتى من الأطراف (أطراف العملية) كما سبق الإشارة إليه أو من الغير الخارج عن هذه العلاقة، سواء تمثل هذا الاعتداء بالسرقة أو بالتزوير الذي يمس هذه البطاقات بغية استعمالها للاستيلاء على الأموال المحصنة بها وهذا ما سنتناوله في هذا المطلب من جريمتي السرقة واستعمال البطاقة المسروقة أو المفقودة.

الفرع الأول: جريمة التزوير واستعمال المزور:

تقع جريمة التزوير أو جريمة استعمال المزور على بطاقات الدفع الإلكتروني كم طرف الغير في حالة ضياعها أو سرقتها، حيث يقوم هذا الأخير بتجريف حقيقتها وذلك باستبدال البيانات التي تحمله بأخرى مزورة، ما يشكل جريمة ضد حاملها الشرعي والجهة المصدرة

[1]- عبد الكريم الردايدة، المرجع السابق، ص 224.
[2]- أنظر المادة 394 مكرر من القانون 14-01 المتضمن قانون العقوبات.
[3]- عبد الكريم الدرايدة، المرجع السابق، ص 226.

لها، إضافة إلى جريمة التزوير التي تعد جريمة قائمة بذاتها وهذا ما ذهب إليه المشرع الجزائري. [1]

أولا: جريمة تزوير بطاقة الدفع الإلكتروني

1- **تعريفها:** تعرف جريمة التزوير بأنها تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون والتي تلحق الضرر بالضحية. [2]

2- **أركان جريمة التزوير:**

نص عليها المشرع الجزائري في قانون العقوبات المواد: 214 إلى 229 والمحددة أركانها كالآتي: [3]

أ- **الركن المادي:** وتتمثل في تزوير المحررات بكل أنواعها وبطاقة الدفع تنطوي ضمن المحررات المصرفية ولذلك تكون محلا للتزوير وتغيير للحقيقة بكل الطرق التي نص عليها القانون وأسلوب التزوير نص عليه المشرع الجزائري في قانون العقوبات على سبيل الحصر في مادة 216 منه [4] وحتى تقوم جريمة التزوير يجب أن يترتب عليها ضرر وبإسقاط ذلك على بطاقات الدفع الإلكتروني فإن عنصر الضرر محتمل الوقوع على الجهة المصدرة للبطاقة وحاملها الشرعي.

ب-**الركن المعنوي:** جريمة التزوير من الجرائم المعنوية التي تستوجب القصد الجنائي العام والخاص معها كالآتي:

القصد الجنائي العام: ويقصد به العلم والإرادة واتجاه إرادة الجاني إلى تغيير الحقيقة يترتب عليها الضرر محتمل.

القصد الجنائي الخاص: اتجاه نية الجاني لاستعمال المحرر فيما زور من أجله.

النص القانوني المجرم لأفعال التزوير: نص عليها المشرع الجزائري في المادة 219 من قانون العقوبات[5] وحدد لها عقوبات أصلية وهي الحبس من ستة إلى خمس سنوات وبغرامة مالية من 500إلى 20000 دينار جزائري، ويمكن أن يضاعف الحد الأقصى من هذه العقوبات إذا تعلق الأمر بمديري الشركات أو أحد رجال المصارف أو أي من الأشخاص الذين يلجأون إلى الجمهور قصد إصدار أسهم أو حصص سواء لشركة أو مشروع تجاري أو صناعي، وأما العقوبات التكميلية فهي الحرمان من حق

[1]- حسين محمد الشبلي، محمد مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولى، دار مجدلاوي للنشر والتوزيع، عمان 2009، ص 57.
[2]- حسين محمد الشبلي، محمد مهند فايز الدويكات، المرجع السابق، ص 59.
[3]- أنظر قانون العقوبات المواد من 214 إلى 229.
[4]- أنظر قانون العقوبات المادة 216.
[5]- أنظر المادة 219 من قانون العقوبات.

أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة من سنة إلى 5 سنوات على الأكثر. [1]

3- أساليب التزوير:

يقر خبراء الكشف عن التزوير أن هناك طرق وأساليب تزوير بطاقة الدفع الإلكتروني رغن تنوعها إلى طائفتين هما التزوير الكلي والجزئي وهذا ما سنتناوله:

أ- أسلوب التزيور الكلي:

إن خطوات التزوير الكلي لبطاقة الدفع الإلكتروني، تتم بداية باصطناع البطاقة كاملة ثم تقليد الرسوم الخاصة على جسم البطاقة، وتغليفها ولصق الهولجرام، والشريط الممغط أو الشريحة الرقائقية، وشريط التوقيع كل حسب موقعه الأصلي على جسم البطاقة، والقيام بالطباعة النافرة وتشغيلها عن طريق تغذيتها بالمعلومات التي حصل عليها النزورون من البطاقة الصحيحة وبعد ذلك يتم استخدامها في عملية الشراء، وفي حالة ما إذا تحصل المزور على الرقم السري لبطاقة ما فإنه يقوم باستغلالها لاصطناع بطاقة بلاستيكية فارغة من البيانات ويلصق عليها الشريط الممغنط ونسخ بيانات صاحب هذه البطاقة، ومن ثم يقوم باستخراج نسخ عديدة منها لاستخدامها في الحصول على الأموال من أجهزة الصراف الآلي. [2]

ب- أسلوب التزوير الجزئي:

يستفيد المزور في هذه الحالة من جسم البطاقة الحقيقية، وما عليها من رسوم خاصة وحروف بارزة، وكتابات أمنية، ليقوم بتزوير البطاقة عن طريق صهر ما عليها من أرقام بارزة لبطاقة حقيقية انتهت فترة صلاحيتها، أو إعادة قولبة رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر يتم الحصول عليها بالطرق السالفة الذكر أو خلع صورة حامل البطاقة الحقيقي ووضع صورة شخص آخر مكانها. [3]

ج- أدوات التزوير:

وتختلف أدوات التزوير حسب دورها:

- **جهاز المسح:** يستعمل لاستنساخ معلومات الحساب من الشريط الممغنط على البطاقة الصحيحة وهو جهاز صغير يمكن حمله في راحة اليد ويستطيع أن يخزن معلومات

---

[1]- أنظر المادة 14 من قانون العقوبات.

[2]- لامية مجدوب، جريمة التزوير في المحررات الرسمية أو المعلومية في التشريع الجزائري، د ط، دار الجامعة الجديدة، الجزائر، ص 103.

[3]- وسام فيصل محمود الشواورة، المرجع السابق، ص 95.

بما يعادل مائة حساب يتم نسخها من بطاقة أصلية وعندما يحصل الجاني على مبتغاه من الشريط الممغنط، يقوم بتخزينها في الحاسب الآلي الخاص به. [1]

- **منظم سابون:** هو جهاز يدوي يستقبل المعلومات ويخزنها من الجهاز الممغنط الموصول برأسه ليتمكن من قراءة بيانات الشريط المغناطيسي في البطاقة البلاستيكية وعند تمرير البطاقة في الفتحة يقون منظم يابون بتخزين المعلومات على الحاسب الآلي. [2]
- **المشفر**: يستخدم هطا الجهاز لتشفير المعلومات على الشريط المغناطيسي على البطاقة المزورة بالإضافة للبطاقات المسروقة أو المفقودة تمت مصادرته نتيجة لاعتقال مجرمين مشتركين في عملية احتيال على بطاقات الدفع الإلكتروني كما يمكن شراء من المتاجر الإلكترونية، ويحتوي على رأس الكتابة على الشريك الممغنط عند تمرير البطاقة من خلال الفتحة، ويستخدم بالاشتراك مع الحاسب الآلي، وبرامج كمبيوتر مناسبة. [3]
- **جهاز التسجيل المغانطيسي:** يتم وصل هذا الجهاز بكمبيوتر على الشريط الممغنط وتخزين أرقام الحساب التي تم نسخها سابقا على الكمبيوتر بالاعتماد على برامج خاصة، حيث يتم تسجيل المعلومات التي تم الحصول عليها على الأشرطة المغناطيسية لبطاقات مزورة أو مسروقة أو مفقودة حيث أن هذه العملية تجعلها تبدوا البطاقة الحقيقية على الجهاز الإلكتروني عند تمريرها فيه.
- **جهاز الطبع بحروف نافرة:** وهو جهاز يستخدم لطباعة رقم الحساب وأيضا المعلومات بحروف نافرة على الوجه الأمامي للبطاقة. وهو يستخدم أيضا لأغراض شعرية ومن السهل الحصول عليه.
- جهاز طلاء الحروف: وهو جهاز يستخدم لطلاء الأرقام المطبوعة بحروف نافرة على البطاقة المزورة، حيث يتم طلاؤها باللون الفضي أو الذهبي أو الأسود وهذا الجهاز يحتوي على جميع الأرقام التي تم طلاؤها.

[1]- أمجد حمدان الجهني: المرجع السابق، ص ص 163، 164.
[2]- المرجع نفسه، ص ص 164- 165.
[3]- المرجع نفسه، ص ص 165 - 166.

ثانيا: جريمة استعمال بطاقة دفع مزورة من طرف الآخرين:

تصبح جريمة استعمال بطاقة دفع مزورة ضمن جريمة استعمال المحررات المزورة وتعتبر جريمة قائمة بذاتها وقد نص عليها المشرع الجزائري بموجب المادة 221 من قانون العقوبات والتي جاء فيها " في الحالات المشار إليها في هذا القسم يعاقب كل من استعمل المحرر الذي يعلم أنه مزور أو شرع في ذلك بالعقوبات المقررة للتزوير[1]

1 - أركان الجريمة

جريمة استعمال المزور كما في بقية الجرائم تقوم على ركنين، ركن مادي وركن معوي وكذلك الركن الشرعي كالاتي:

أ- **الركن المادي:** الركن المادي لجريمة العمل المحررات المزورة، يتمثل في استعمال ورقة مزورة، حيث أن المشرع الجزائري لم يبين ما المقصود باستعمال ورقة مزورة وتعرف على أنها التمسك والاحتجاج بمحرر مقدم لفرد أو لجهة من الحياته سواء من الشخص المحتج أو من الغير[2] كذلك يجب إتمام الجريمة وانهاؤها حيث تعتبر جريمة استعمال المحرر المزور من الجرائم الآتية حيث تم عند الإحتياج بالمحرر بغض النظر على التيجة

ب- **الركن المعنوي:** يتمثل الركن المعنوي لجريمة استعمال المحرر المزور في أن يكون الجاني عالما عند استعماله للمحرر بأنه مزور، حتى ولو كان هذا الاستعمال لأغراض شرعية، وهنا تجدر الإشارة إلى أن حالة استعمال محرر مزور والفاعل لا يعلم بذلك واكتشف لاحقا بأنه مزور لكنه استمر بالتمسك به فهنا تقوم الجريمة من يوم علمه بالأمر، ويخضع لأحكامها وبدون هذا العلم في حكم الإدانة وإلا كان معينا بالقصور.[3]

ج- **النص القانوني المجرم الاستعمال المحرر المزور :** العقوبة المقررة لجريمة استعمال المحرر المزور في نفسها عقوبة جريمة التزوير المشار إليها سابقا، سواء العقوبات الأصلية منها أو التكميلية. [4]

---

[1]- أنظر المادة 221 من القانون 14-01 المتضمن قانون العقوبات.
[2]- خشنة حسيبة، المرجع السابق، ص129.
[3]- أحمد أبو الروس، قانون جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية، الموسوعة الجنائية الحديثة، المجلد الخامس، المكتب الجامعي الحديث، الاسكندرية، 1997، ص89.
[4]- خشنة حسيبة، المرجع السابق، ص129.

الفرع الثاني.جريمة سرقة بطاقة دفع أو رقمها السري

أولا : جريمة سرقة البطاقة

لقد نص المشرع الجزائري على جريمة السرقة بموجب المادة 350 من قانون العقوبات الجزائري، حيث جاء فيها بأن: " كل من أختلس شيئا غير مملوك له يعد سارق " [1]

مزور والفاعل لا ربما أن بطاقة الدفع الالكتروني تكون ملك لحاملها دون غيره فإن أحكام هذه الجريمة تطبق على الغير الذي قام بسرقتها، وفيما يلي نستعرض مختلف أركان هذه الجريمة:

1 - الركن المادي: يتمثل الركر المادي لجريمة السرقة في فعل الاختلاس الذي يعرف على أنه أخذ مال الغير دون رضا مالكه أو حائره، ومن هذا التعريف يتبين أن فعل الاختلاس يتكون من عناصر أساسية، فالعنصر المادي يتمثل في الاستيلاء على الشيء المملوك للغير ، وأما العصر المعنوي فهر عدم رضا صاحب هذا الشيء على هذا الفعل المجرم، كذلك فيما يتعلق بمحل الجريمة فإن فعل السرقة يقع على شيء مملوك للغير وتقع على المنقولات دون العقارات، وبطاقة الدفع تعتبر مال منقول ملك لحاملها لا يحق لغيره التصرف فيه. [2]

2 - **الركن المعنوي:** تقوم جريمة السرقة على القصد الجنائي العام والخاص، فأما القصد الجنائي العام قهو العلم والإرادة، أي أن الجاني يعلم أن الشيء ملك للغير ، والاستيلاء عليه فعل مجرم قانونا، ومع ذلك تتجه إرادته لإتيانه. وفيما يخص بطاقة الدفع فالجاني يعلم أنها ملك لصاحبها ولا يجور له التصرف فيها وهذا الفعل يعد سرقة ومع ذلك تتجه إرادته لسرقتها. [3]

وأما القصد الجنائي الخاص يقصد به نية التملك، ولكن مع تطور القضاء أصبح لا يؤخذ به كشرط لقيام جريمة السرقة، وإنما تقوم بمجرد الاستيلاء على الشيء واستخدامه وبالتطبيق على بطاقة الدفع الالكتروني فإن جريمة السرقة تقوم بمجرد استيلاء الغير عليها مع علم هذا الأخير بأن هذا الفعل بعد جريمة يعاقب عليها القانون، حتى ولو لم تكن نيته تملكها، والدفع بذلك يعد باطلا. [4]

---

[1]- أنظر المادة 350 من القانون 14-01 المتضمن قنونا العقوبات.
[2]- خشنة حسيبة، المرجع السابق، ص ص، 132، 133.
[3]- أمين طالب البغدادي، الاستخدام الغير مشروع لبطاقة الائتمات المسؤولية الجزائية والمدنية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص206.
[4]- عبد الفتاح بيومي الحجازي، جرائم الكمبيوتر والحاسب الآلي في القانون العربي النمذجي، المرجع السابق، ص587.

3 - النص القانوني المحرم للعل السرقة: بالرجوع إلى نفس المادة 350 من قانون العقوبات وما يليه تجدها تتضمن العقوبات المقررة لجريمة السرقة. [1]

ثانيا : جريمة سرقة الرقم السري لبطاقة الدفع الالكتروني

1- **المقصود بسرقة الرقم السري للبطاقة:** يسأل الغير عن جريمة السرقة عندما يقوم بسرقة الرقم السري لبطاقة الدفع الالكتروني، حيث يستطيع الفاعل الحصول عليه واستخدامه في مختلف العمليات المصرفية، [2] ومن بين أهم عوامل الحصول عليه مايلي:

أ- **إهمال الحامل:** ويحصل هذا الإهمال نتيجة تدوين الرقم السري على وجه البطاقة من قبل حاملها الشرعي، وتركها عرضة لمرأى الغير الذي يتمكن من معرفته بكل سهولة، كذلك قد يقوم حاملها بتكرار الرقم سري في مسمع أو أنظار الغير أثناء قيامه بعملية سحب النقود دون أخذ الحيطة اللازمة. [3]

ب- **تتجسس**: وتم هذه الطريقة إما بمراقبة أجهزة الصراف الآلي ومع كمرات عليه ومن ثم رؤية الأرقام السرية عند إدخالها، أو من خلال وضع جهاز إلكتروني في مكان ما على الصراف الآلي، حيث يقوم بنقل الرقم السري لجهاز آخر لحظة إدخاله من قبل حاملها.

ج- **القرصنة**: ويتم ذلك بالدخول إلى مواقع أجهزة الكمبيوتر التي يتم فيها حفظ بيانات العملاء، وأرقام بطقاتهم وذلك بصورة غير قانونية عبر البنوك المصدرة لها. [4]

2 - سرقة أرقام بطاقات الدفع عبر الأنترنت:

تتم هذه العملية من ذوي الخبرة والمحترفين في مجال شبكات الانترنت، وهي من ضمن أعمال القرصنة الحصول على أرقام بطاقة الدفع، ويتم ذلك بعدة أساليب وتقنيات نذكر من بينها.

أ - إختراق منظومة الاتصالات العالمية: يقصد بخطوط الاتصالات العالمية تلك الخطوط التي تربط بين الحاسب الآلي للمشتري والحاسب الألي للتاجر، وتتم عملية القرصنة بالتنصت على الاتصالات بهدف اختر اقها و التغلب في نظام حمايتها، ومن ثم الو صول إلى أرقام بطاقات الدفع الالكتروني. [5]

---

[1]- أنظر المادة 350، وما بعدها من القانون 14-01 المتضمن قانون العقوبات.
[2]- فيصل محمود الشواورة، المرجع السابق، ص ص، 96، 97.
[3]- المرجع نفسه، ص 100.
[4]- عبد الكريم الردايدة، المرجع السابق، ص 183.
[5]- المرجع نسه، ص 190.

ب - تقنية تفجير الموقع المستهدف: تتمثل هذه النقية في قيام أحد القراصنة وانطلاقا من جهازه الآلي بإرسال رسائل إلكترونية كثيرة تتجاوز مئات الآلاف لجهاز آخر وهو المستهدف، حيث تؤثر هذه الرسال على مساحة التخرين مما يؤدي إلى تفجير هذا الموقع ليتم بعدها تشتيت هذه المعلومات وتناثرها حيث تنتقل إلى جهاز القرصان الذي قام بهذه العملية مما يتيح للجاني التحميل على أرقام بطاقات الدفع الالكتروني، وتستهدف هذه العملية غالبا أجهزة البنوك والمطاعم والفنادق ومختلف مرافق الخدمات. [1]

جـ - أسلوب الخداع: يتجلى هذا الأسلوب في إنشاء مواقع إلكترونية وهمية، شبيهة بالمواقع الأصلية على شبكة الانترت ومثال ذلك موقع المؤسسات التجارية، حيث تظهر هذه المواقع للغير على أنها فعلية، وتتم هذه العملية من خلال قيام القراصنة من الجناة بجمع معلومات كافية متعلقة بموقع أصلي على شبكة الانترنت، وبعد ذلك يتم إنشاء موقع وهي بواسطة تلك البيانات المحصل عليها من الموقع الأصلي حيث يبدو وكأنه نفس الموقع، ليتم بعد ذلك استخدامه من طرف القراصنة في استقبال جميع المعاملات الخاصة بالموقع الأصلي في محل التجارة الالكترونية، ومن بينها المعاملات التي تتم بواسطة بطاقات الدفع الالكتروني لتنتهي هذه العملية بالاستيلاء على بيانات وأرقام هذه البطاقات. [2]

د - اسلوب الإيهام: ويتمثل في قيام القراصنة بانتحال صفة الجهة المصدرة لبطاقات الدفع ومن ثم إرسال رسائل إلكترولية لعملائهم أصحاب البطاقات، والهدف منها تجديد معلوماتهم وبيانات بطاقاتهم عبر الموقع الالكتروني، ليتسنى لهم التعرف على أرقامها وبياناتها. [3]

هـ - أسلوب تخليق رقم بطاقات الدفع: يتم هذا الأسلوب في إيجاد الرقم السري للبطاقة عن طريق القيام بعمليات حسابية ومعادلات، وذلك بتبديل وتوثيق لأرقام حسابية، ومن ثم التعرف على هذا الرقم واستخدامه في العمليات الإجرامية للجناة. [4]

و - أسلوب التجسس: ويشمل هذا الأسلوب في قيام القراصنة بالاعتماد على برامج وظيفتها الإطلاع على بيانات الشركات والمؤسسات التجارية عبر شبكة الإنترنت ومن خلال ذلك يحصلون على أرقام بطاقات الدفع التي استخدمت عبر الشبكة لصالح هذه الشركات. [5]

---

[1]- عماد علي خليل، الحماية الجزائية لبطاقات الوفاء، الطبعة الأولى، دار وائل للطباعة والنشر، عمان، 2000، ص102.

[2]- وسام فيصل محمود الشواورة، المرجع السابق، ص99.

[3]- عبد الكريم الردايدة، المرجع السابق، ص71.

[4]- المرجع نفسه، ص194.

[5]- أمجد حمدان الجهني، المرجع السابق، ص194.

ز - اسلوب تبادل المعلومات: ويقوم هذا الأسلوب على التعاون القائم بين القراصلة المجرمين عبر مختلف الدول، من خلال تبادل الأرقام المتحصل عليها فيما بينهم وذلك لتوسيع نشاطهم الإجرامي باستخدام تلك الأرقام عبر مختلف الدول. [1]

وتجدر الإشارة إلى أن الأساليب السالفة الذكر رغم تعدد صورها، فهي أخطر من الأساليب التقليدية لأنها تتم في عالم افتراضي، وليس لها آثار ملموسة وهذا ما يصعب من مهمة الكشف عن فاعليها، وتلحق أضرارا بليغة بالمؤسسات المالية والتجارية التي تمارس التجارة الالكترونية، كما أنها تخلق العديد من المشاكل بين أطراف التعاملات المالية عبر شبكة الانترنت وتنزع الثقة بينهم. [2]

الفرع الثالث: جريمة استعمال بطاقة دفع مفقودة

هذه الجريمة مفادها أن الغير لم يسرق بطاقة الدفع من صاحبها بل عثر عليها، فقد تكون هذه البطاقة مسروقة أو مفقودة ولم يقم بإرجاعها لصاحبها الشرعي أو الحهة المصدرة لها،[3] وهو ما سيتم التعرض له بالدراسة فيما يأتي:

أولا: استخدام البطاقة المفقودة:

قد يحصل أن يتم العثور على بطاقة دفع ضائعة، وفي هذا يمكن التمييز بين حالتين:

1- استعمال البطاقة من طرف الشخص الذي عثر عليها :

ذلك بأن يقرر هذا الأخير عدم إرجاع البطالة واستخدامها مصلحته الشخصية، وهنا يسأل عن جريمة الاحتيال لأنه استعمل صفات كاذبة عندما ادعى أنه المالك للبطاقة وعن طريق هذا الادعاء يحصل على ما يريد من سلع وخدمات من قبل التجار الذين تم الاحتيال عليهم، إضافة إلى ذلك فقد يتم مساءلته عن جريمة تزوير إذا ما قام بالتوقيع على سندات البيع. [4]

2- عدم استعمال البطاقة من طرف الشخص الذي عثر عليها ومنحها لشخص آخر

قد يقرر من عثر على البطاقة عدم الاحتفاظ بها، وكذلك عدم استعمالها ليسلمها شخص آخر، هذا الأخير الذي قد يكون مالكها أو قد يكون غير ذلك كما يلي:

1- أمجد حمدان الجهني، المرجع السابق، ص195.
2- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، الطبعة الأولة، دار البداية للنشر والتوزيع، عمان، 2010، ص192.
3- عبد الكريم الردايدة، المرجع السابق، ص244.
4- المرجع نفسه، ص ص، 244، 245.

- **تسليم البطاقة لشخص يدعي أنه مالكها:**

يعتقد الشخص الذي عثر على البطاقة أنه قد سلمها لمالكها الحقيقي، لكن في الحقيقة هو ادعاء كاذب من قبل الشخص المسلمة إليه بغرض الاستيلاء عليها، وفي هذه الحالة لا يخضع مسلم البطاقة لأي سائلة جزائية لأنه فعل ذلك بحسن نية. [1]

- **تسليم البطاقة لغير مالكها مع العلم بذلك:**

يكون مسلم البطاقة في هذه الحالة سيء النية، ويعتبر شريك لغير الذي استلمها وقام باستخدامها، أما في ما يتعلق بسؤولية الغير الذي تم تسليمه البطاقة قصد استخدامها فإنه يسأل عن جريمة سرقة لأنه وضع يده على شيء ملك للغير. [2]

كما يسأل عن جريمة احتيال في مواجهة من عثر على البطاقة وسلمه إياها على أساس أنه صاحبها، وأيضا في مواجهة التاجر عندما يقدم له الخدمات والسلع على أساس أنه الحامل الشرعي ويسأل كذلك عن جريمة التزوير إذا قام باستخدام توقيعه الشخصي على سندات البيع عند التاجر . [3]

ثانيا : استخدام البطاقة المسروقة:

يقصد بهذا الاستخدام أن يقوم الشخص الذي سرق بطاقة دفع بتسليمها للغير قصد استعمالها، وفي هذا الصدد نميز بين حالتين:

1- استلام البطاقة المسروقة مع علمه برقمها السري:

إذا قام من استخدم بطاقة الدفع مع علمه برقمها السري، سواء في عمليات السحب أو الوفاء فإنه يسأل عن عدة جرائم، فيسأل عن جريمة إخلاء الأشياء المسر وقة لأنه يعلم أن البطاقة مسروقة ومع ذلك احتفظ بها، [4]وقد نص المشرع الجزائري على هذه الجريمة في المدة 387 من قانون العقوبات.[5]

كذلك يسأل عن جريمة احتيال عند تعامله مع التاجر في الوفاء أو في سحب النقود لأنه استعمل صفات كاذبة، والتي على أساسها تحصل على النقود والخدمات، كما أنه يسأل

1- علي عدنان الفيل، المرجع السابق، ص 59.
2- المرجع نفسه، ص 59.
3- عبد الكريم الردايدة، المرجع السابق، ص 245.
4- علي عدنان الفيل، المرجع السابق، ص ص، 59، 60.
5- أنظر المادة 387 من قانون العقوبات الجزائري.

ايضا عن جريمة التزوير عندما يستعمل البطاقة في الوفاء نتيجة توقيعه باسم صاحب البطاقة حتى يدفع البنك ثمن مستحقاته. [1]

2- استلام البطاقة المسروقة دون معرفة رقمها السري:

في هذه الحالة فإن الفاعل يسأل عن جريمة إخفاء أشياء مسروقة، أما بالنسبة للاستخدام وبما أنه لا يعرف رقمها السري فإنه لا يستطيع استخدامها في عمليات السحب والدفع وفي حالة ما إذا حاول ذلك فيه يسأل عن الشروع في جريمة احتيال، ولن تتحقق النتيجة بسبب خارجي وهو عدم معرفته للرقم السري، وكذلك فإن أجهزة الصراف الآلي مبرمجة على سحب البطاقة عند الإدخال المتكرر لثلاث مرات لرقم سري خاطئ،[2] وقد يحدث وأن يصادف وينجح في إدخال رقم سري صحيح ففي هذه الحالة تتم مساءلته عن جريمة احتيال. [3]

أما بالنسبة لمسؤولية سارق البطاقة الذي قدمها للغير فإنه إذا سلم البطاقة للغير على اعتبار أنه حاملها الشرعي، فهذا لا يسأل عن أية جريمة لأنه يعتبر إعارة للبطاقة وأما إذا سلمه إياها مع علمه بأنه ليس مالكها فهنا يسأل عن جريمة السرقة، كما يسأل أيضا بصفته شريك في جريمة احتيال أو تزوير التي قام بها من سلمها له. [4]

1- علي عدنان الفيل، المرجع السابق، ص 60.
2- أمجد حمدان الجهني، المرجع السابق، ص181.
3- علي عدنان الفيل، المرجع السابق، ص 61.
4- المرجع نفسه، ص 61.

خلاصة الفصل

من خلال ما تقدم بيانه وتوضيحه يتجلى لنا أن بطاقة الدفع الالكتروني لها أنواع عديدة وتختلف تسمياتها باختلاف وظائفها والجهات المصدرة لها، كما أن لها جملة من الخصائص والمزايا تميزها عن ومختلف البطاقات الأخرى وقد يسوء استخدامها من طرف حاملها أو من طرف الغير وذلك إما عبر مختلف الأجهوة الالكترونية أو عبر الانترنيت وهذا ما يتطلب قيان المسؤولية الجزائية عن هذه الأفعال المجرمة وتسليط العقوبات المناسبة لها لردع المجرمين وضمان حقوق الضحايا بما يكفل تحقيق العدالة.

الفصل الثاني

الحماية الجنائية الإجرائية لبطاقات الالكتروني

تمهيد:

إن سلسلة الاعتداءات الواقعة على بطاقة الدفع الالكتروني تشكل خطورة وحدقة لما تسببه من خسائر في مجال التعملات المالية، خاصة أن هذه الجرائم ذات طبيعة تقنية متطورةلكونها ترتبط بأجهزة إلكترونية ويتصف مرتكبوها بالفطنة والذكاء في هذا المجال وعليه فيجب وضع استراتيجيات محكمة لمكافحة هذا النوع من الجرائم للحد منها ومعاقبة وزج مرتكبيها.

لأن جرائم بطاقة الدفع الإلكتروني تمتاز بالحداثة، فهي تفتقر إلى قوانين خاصة بها تكون كفيلة لها عند وقوعها، ذلك مما دفع إلى إتخاذ اجراءات خاصة بذلك سواء على المستوى المحلي من خلال تبني أطراف العلاقة التعاقدية إجراءات لحماية حقوقهم ودوام الثقة في تعاملاتهم وكذلك على مستوى الأجهزة الأمنية المختصة في مكافحة هذه الجرائم، ومن جهة أخرى وعلى الصعيد الدولي إذ يستوجب تفعيل آليات كفيلة بمحاربة هذه الجرائم ومتابعة مرتكبيها.

سنتناول من خلال هذا الفصل مختلف الإجراءات المتبعة في مجال الجرائم الواقعة على بطاقة الدفع الإلكتروني، نختص المبحث الأول لدراسة الإجراءات الوقائية والمبحث الثاني لدراسة الإجراءات الردعية.

المبحث الأول: الإجراءات الوقائية لمواجهة الجرائم الواقعة على بطاقات الدفع الالكتروني

قصد المحافظة على سلامة وأمن المعاملات المصرفية ببطاقات الدفع الإلكتروني كان من اللازم وضع إجراءات وقائية من قبل جهات مختلفة في المجتمع سواء الجهات المصدرة للبطاقة أو المتعاملة بها إضافة إلى الأجهزة الأمنية المختصة، وذلك لمنع أي جرائم قد تقع على البطاقة من خلال الإحاطة بمسبباتها ودوافعها التي تؤدي لارتكابها ومحاولة معالجتها حتى لا تتكرر مجددا ولتسليط الضوء على ذلك فقد قسمنا هذا المبحث إلي مطلبين، لنتناول في المطلب الأول الإجراءات الوقائية على صعيد الهيئات الدولية وكذلك البنوك، بينما خصصنا المطلب الثاني للإجراءات الوقائية على مستوى صاحب البطاقة والتاجر والجهاز الأمني.

المطلب الأول: دور الهيئات الدولية والبنوك في حماية بطاقة الدفع الالكتروني

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

الفرع الأول: الإجراءات الوقائية المتخذة من طرف الهيئات الدولية

تتمتع الهيئات الدولية المنشئة لبطاقات الدفع الإلكتروني ومثال ذلك بطاقات فيزا كارد وماستر كارد، بالدور الكبير في حماية هذه البطاقات لكونها هي من يصنع هذه البطاقات ويضفي عليها صفة القبول دوليا، مما يسمح بتداولها والتعامل بها حتى عن طريق الإنترنت وفي حال وقوع أي تجاوزات أو مشاكل فهذه الهيئات هي من يتدخل لحلها، ولذلك فقد اتخذت العديد من الإجراءات بغية الإستعمال الأمثل لهذه البطاقة ومن أهمها:

1- الإجراءات التقنية لتطوير البطاقة

لقد تم إنشاء بطاقة مكونة من دوائر إلكترونية تجعلها غير قابلة للاختراق، وهذا بفضل المادة المصنوعة بها (pvc)، وكذلك عن طريق إدخال الهوليجرام وهو عبارة عن أشعة الليزر والتي من خلالها تنعكس الصورة المراد تصويرها على مكان معين، كما تحتوي أيضا هذه البطاقة على ذاكرة لها القدرة على حفظ العمليات الأخيرة التي تم إجراؤها، كذلك دمج الطاقة الذكية وهي بطقة بلاستيكية حجمها كحجم بطاقات الدفع الأخرى، حيث تتميز هذه البطاقة بدوار متكاملة تسمح لها بتخرين ومعالجة البيانات. [1]

[1]- علي عدنان الفيل، المرجع السابق، ص ص، 76، 77.

كذلك فقد تم استخدام الأنترنت النموذجي التقني الموحد والمسمى بنظام الصفقات الإلكترونية الأمنة، والذي أعلنت عنه الشركتين العالميتين ماستر كارد وفيزا كارد سنة 1996، وانظم إليه لاحقا مجموعة من الشركات الأمريكية، ومن جهة أخرى فقد قامت شركة ماستر كارد العالمية بطرح بطاقة ماستر كارد باي بلس ويلك عام 2002 وهي عبارة عن برنامج للدفع دون اتصال حيث يتم بواسطة تقنية متطورة ويمتاز برقلقة كمبيتر مخفية ولاقط، حيث يقوم الحامل بتمريرها قرب جهاز إلكتروني مهيأ لهذا العرض وبعد تلك ترسل هذه البطاقة معلومات الدفع لاسلكيا ويذ معالجة العملية يستلم الحامل إشارة بتأكيد الدفع. [1]

إضافة إلى ذلك فقد قامت الشركات العربية بإصدار بطاقات مماثلة، حيث أعلنت شركة "دوت كوم" عن إصدار البطاقة الالكترونية المسمات " كاش يو"، والتي توفر لحاملها خدمات البيع والشراء عبر الإنترنت بثقة تامة وبصورة آمنة دون أي مخاطر. [2]

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

2- تصميم البرامج:

قامت الهيئات المصدرة للبطاقة الالكترونية بانشاء برامج للحد من وقوع الاعتداءات على البطاقة ومن بينها على سبيل المثال مايلي :

- برنامج الشبكة العصبية: ومن خلاله يتم رصد جميع التعاملات المنفذة بواسطة بطاقات الدفع، والكشف عن المشكوك في صحتها وإعادة فحصها.
- برامج نظم المعرفة: يعمل هذا البرنامج على عزل وإيقاف البطاقات التي يكتشف أن تعاملاتها غير شرعية، وذلك من خلال وسائلها الفعالة للكشف عن التهديدات من طرف المجرمين.
- برامج نظم المعلومات الإرشادية: والتي تعمل على مراقبة أساليب الغش والاحتيال التي قامت المؤسسة البنكية في بريطانيا بتطويرها.
- برنامج الاختيار: يعمل على تطبيق المعايير الأولية على حساب حاملي بطاقات الدفع، حيث تظهر من خلاله الحسابات التي تستخدم هذه البطاقات بصفة غير شرعية ومن ثم عدم إتمام التعامل بالبطاقة.

[1]- علي عدنان الفيل، المرجع السابق، ص 77.
[2]- أمجد حمدان الجهني، المرجع السابق، ص 115.

- برنامج التقييم: يعمل على فحص صابت حاملي بطاقات بقع العملاء بالاعتماد على تعليمات حراء مكافحة الاحتيال المزودة بها ثم عرل الحسابات التي بثت أنها تتبع طرق احتيالية[1]

الفرع الثاني: الإجراءات الوقائية المتخذة من من البنوك

تقوم البنوك والمؤسسات المصرفية بتوفير الحماية التامة للحسابات التي تخص عملائهم لتحقيق الأمان ومنع التلاعبات التي تقع عليها من جهة، ولتعزيز الثقة بينها وبين عملها من جهة أخرى، وذلك عن طريق إجراءات إدارية خاصة وكذلك إجراءات تقنية وأخرى رقابية[2]

أولا: الإجراءات الرقابية

تخضع البنوك والمؤسسات المصرفية في آداء مهامها إلى قواعد تنظيمية داخلية يتولى تنظيمها البنك المركزي من حيث إجراءات الاشراف والرقابة والتوجيه، وهذا بهدف الاستقرار الداخلي للبنوك وللحفاظ على أموال العملاء، وتتجلى هذه الرقابة فيما يلي:

1- **الرقابة التوجيهية:** وتتمثل هذه الرقابة في اصدار التوصيات والتوجيهات البنوك المشرف عليها ولك اللاهتمام بالمشاكل التي تواجهها هذه الأجهزة ومساكنها على تجاورها ع الريق دراستها ثم تقني الاقتراحات المناسبة لها، وأيضا تحديد قواعد سير العمل المصرفي بما يتماشى مع التناسب بين الموجودات أو المطلوبات كما أن للبنك المركزي سلطة توجيه التعليمات والمطالبة بالتقيد بمحتراها، وتوجه هذه التعليمات إلى كافة البنوك والمؤسسات المالية في الدولة وإلزامها بالتقيد باحترامها وتفيدها[3]

2- **الرقابة الداخلية:** وتتم هذه الرقابة من خلال تحديد جزء من صلاحيات النظام الداخلي لاداء الرقابة على الحسابات التي تحتمس بحماية الأصول والسجلات لضمان دقة البيانات المحاسبية، كذلك تحديد جزء من النظام الداخلي للرقابة الإدارية وهي الإجراءات التي تنتهجها الإدارة بغرض تقييد هذه البنوك والمؤسسات بالسياسة الموضوعة من طرفها، والتأكد من الأداء الدقيق لعمل البيانات المالية ومنع الغش والخطأ، ويقوم بذلك أشخاص توظفهم الإدارة بعد التأكد من كفاءاتهم المهنية. [4]

3- **الرقابة الخارجية:** وتتمثل هذه الرقابة في قيام أشخاص أو مؤسسات مستقلة بفحص ومراجعة البيانات الحكامية للبنوك ومعرفة مدى صحتها ومصداقيتها بالاعتماد على القوات المهنية المتبعة في ذلك، وأيضا مراقبة سلامة النظام الداخلي ومراجعة

[1]- عبد الكريم الردايدة، المرجع السابق، ص 180.
[2]- أحمد سفر، أنظمة الدفع الالكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008، ص 28.
[3]- حسين محمد الشلبي ومهند فايز الدويكات، المرجع السابق، ص ص 100، 102.
[4]- المرجع نفسه، ص 103.

الرقابة الداخلية، ثم إبلاغ إدارة البنك والسلطات المصرفية عن أي ملاحظة من شأنها مخالفة القوانين المعمول بها. [1]

4- **الرقابة الزجرية:** يمارس البنك المركزي رقابة زجرية عن طريق وضع قوات وتعليمات، والمطالبة بالالتزام التام بها ويتعرض كل من يخالفها إلى عقوبات مدنية أو جزائية، حيث يقوم بهذه الرقابة هيئات ولجان محددة لذلك تختص بالتأكد من التزام البنوك بما أقرته من أحكام، وتقوم هذه اللجان والهيئات الرقابية بهذه الوظيفة بصفة مباشرة أو من خلال موظفيها بقيامهم بدورات تفتيش مفاجئة للبنوك، وكذلك إجراء عمليات فحص للأوضاع الإدارية والمالية والتأكد من أن رأس المال مناسب للسيولة والتأكد أيضا من فعالية الوسائل المتبعة في الرقابة الداخلية ووسائل الإدارة، وما مدى قدرتها على المحافظة على سلامة البنك. [2]

ثانيا: الإجراءات الإدارية:

وتكون هذه الإجراءات عن طريق تعيين حد أقصى لإستخدام البطاقة أو سحبها أو المعارضة في قبولها وسنتناول فيما يلي كل عصر على حدة:

1- تحديد سقف لعمليات السحب البطاقة:

الأصل أن يتم تحديد سقف للبطاقة لا يمكن تجاوزه، واستثناءا قد يسمح بذلك في حالات معينة والهدف من ذلك منع إفراط صاحب البطالة في استعمال بطاقته خوفا من عدم إيفاءه بمصاريف المشتريات المترتبة عليه بتاريخ تسويتها المتفق عليه مع البنك، كذلك خويا من وقوعها في يد الغير ولذلك وجب تحديد سقف لاستخدام البطاقة حيث يكون هذا التحديد سواء عند استخدامها في عمليات السحب أو الوفاء على حد سواء. [3]

أ - الحد الأقصى لاستخدام البطاقة في الوفاء

في هذه الحالة نميز بين استخدامين

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

- عند استخدام البطاقة في الجهاز الالكتروني يظهر خلال تمرير البطاقة في الجهاز على الشاشة ما إذا كانت تحتوي رصيد كافي لاتمام عملية الوفاء لم لا، فإذا تجاوز حد

---

[1]- حسين محمد الشلبي ومهند فايز الدويكات، المرجع السابق، ص 102، 103.
[2]- المرجع نفسه، ص 102.
[3]- بيار إميل طوبيا، بطاقة الاعتماد والعلاقات التعاقدية المبثقة عنها، د ط، منشورات الحلبي الحقوقية، بيروت، 2000، ص 40.

الرصيد برفض الجهاز إتمام هذه العملية إلا بعد حصول التاجر من المصدر على تقريض بالموافقة[1]

ب - الحد الأقصى لاستخدام البطاقة في السحب

تم تحديد السقف الأقصى للبطاقة على السحب من أجهزة الصراف الآلي حسب المبلغ المسموح به من ترصيد، ففي بطاقات الدفع العادية يكون نصف سقف البطاقة وفي البطاقات التي تستخدم في الوفاء يكون نفس الرصيد المتوافر في الحساب، وفي حالة السحب اليومي فإن الحد الأقصى للسحب يختلف من بنك لأخر حب التسهيلات التي يمنحها كل بلك لعلائه.

2- سحب البطاقة

قد يتم سحب البطاقة من طرف المصدر أو من طرف التاجر من أجل الحفاظ على حقوق جميع الأطراف ومع التحاوزات التي قد تتم عن طريق البطاقة.

أ - سحب البطاقة عن طريق المصدر:

للبنك الحق في استرجاع البطاقة من صاحبها بالنص على ذلك في العقد بأن البطاقة ملك المصدر، حيث يستطيع هذا الأخير الطلب من صاحبها بإعادتها إليه أو إلغاءها وهذه العملية قانونية إذا كانت ناتية عن أسباب جوهرية ويخشى بقاؤها عند صاحبها، أما إذا انعدمت هذه الأسباب فهذا يعتبر تعسف من قبل المصدر ووجب التعويض، ويكون هذا السحب سواء بالطريقة العادية عندما يطلب المصدر إرجاع البطالة، وقد يكون بطريقة فنية في حالة برمجة الصراف الآلي على سحبها

ب - سحب البطاقة عن طريق التاجر:

ينشأ اتفاق بين المصدر بصفته مالك للبطاقة مع التاجر بصفته وكيل على القيام بسحب البطاقة وإرجاعها للصدر مقابل مكافاة على كل بطاقة مسحوبة، وذلك لتشجيعهم على مكافحة الجرائم الناتجة عنها، ويقوم التاجر بسحب البطاقة في حالات عدة كأن تكون البطاقة ضمن قائمة الطاقات التي ورد رقمها في الكشف الدوري التحذيري الذي تم توزيعه على التجار، وكان يعرف التاجر صاحب البطاقة ولكن تم استخدامها من قبل الغير فشك في كيفية وصولها إليه. [2]

[1]- أمجد حمدان الجهني، المرجع السابق، ص 116.
[2]- المرجع نفسه، ص ص 118، 119.

3- المعارضة في قبول البطاقة:

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

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

أ- نشر المعارضة لدى التجار المزودين بالجهاز اليدوي:

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

ب - نشر المعارضة لدى التجار المزودين بالجهاز الالكتروني pos:

يتم تزويد هؤلاء التجار بشكل الكتروني من خلال تزويد الجهاز الالكتروني لدى التاجر والموصول بجهاز المصدر بأرقام البطاقات المرفوضة، حيث بمجرد تمرير المنطقة عليه يتحدد تلقائيا ما إذا كانت مقبولة أو مرفوضة في الوفاء. [3]

جـ - نشر المعارضة من خلال جهاز الصراف الآلي:

ويكون ذلك ببرمجة جهاز الصراف الآلي الموصول بكمبيوتر البنك على رفض البطاقة خلال عمليات السحب وفي حالة ما إذا كانت الطاقة مسروقة أو مفقودة فالجهاز يقوم بسحبها رغم إعادتها. [4]

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص 119.
[2]- المرجع نفسه، ص 119.
[3]- المرجع نفسه، ص 120.
[4]- المرجع نفسه، 121.

ثانيا: الإجراءات التقنية

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

- التحديث الدائم والمتجدد لشفرة بطاقات الدفع حتى يصعب على المحتالين التعرف عليها واستحداث تقنيات التعرف على هوية البطاقة الأصلي كإدخال 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 الاشعارات لأصحابها لتخبرهم فور إجراء أي عملية.

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

- استخدام كلمات سرية معقدة للتحول إلى الأنظمة الالكترونية بحيث تكون مزيج من الأرقام والحروب يصعب تخمينها من الغير. [1]

ثالثا: إجراءات أخرى

حتى تضمن البنوك الحماية التامة لتعاملاتها سواء مع عملائها أو مع التجار، وضمان إيفاء أموالها في الوقت المناسبا، وسلع التلاعات تقوم بآداء مهامها على أكمل وجه من خلال إجراءات رقابية وتأهلية خاصة إما بالموظفين أو العمال أو التجار.

1- بالنسبة للموظفين:

وتتمثل الإجراءات الرقابية الخاصة بالموظفين في

- قيام المصرف بمنع الموظفين من استخدام أي أجهزة من دون تلك المحددة من طرف المصرف من خلال المراقبة المستمرة لها، وهذه الأجهزة والنقاط تعمل على ربط الشبكة والأنظمة الداخلية للمصرف مع الفضاء الخارجي. [2]

- قيام البنك بمراقبة جميع الأجهزة وحمايتها وحمايتها في أماكن آمنة لا يسمح لأحد بدخولها من غير الموظفي المخولين بالدخول، كما لا يسمح لغير الموظفين المعنيين من الاطلاع على معلومات الشبكة الداخلية حتى لا يقوموا بالعبث بالشبكة، لأن الكثير من الجرائم تتم من طرفهم أو بمساعدتهم نظرا لمعرفتهم بالنظام الداخلي أكثر من المجرمين خارج

[1]- علي عدنان الفيل، المرجع السابق، ص 82.
[2]- أمجد حمدان الحهني، المرجع السباق، ص 184.

المصرف وأيضا بهدف عند تسريب المعلومات وكذلك منع الموظفين من إنشاء السرية الخاصة بالحامل.

أما إجراءات التأهيل تمثل في:

- إنشاء برامج تدريبية للموظفين في المصارف بهدف تعليمهم كيفية فحص بطاقات الدفع الالكتروني ليتم اكتشاف التلاعب فيها بشكل دوري وتحديد السلوك المشوه المتبع في ذلك.

- القيام بتدريب موظفي المصرف على طرح أسئلة معينة أثناء مكالماتهم الهاتفية للرد على طلبات التجار بالحصول على مرافقات أو متابعة المعاملات الفورية، والمعاملات ذات المبالغ الكبيرة التي تتم على بطاقة أجنبية [1]

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

2- بالنسبة للعملاء:

إن الاختيار الحسن للعملاء المتقدمين للبنوك بنية الحصول على بطاقات الدفع الالكترونية، حيث يتم اخضاعها لمعايير خاصة بغرض دراسة مركزهم القانوني والمهني والمالي، والتأكد من صحة البيانات التي قامو بتقديمها وهو ما يقلل من تسلل العملاء غير الجادين وبالتالي الحد من تلاعباتهم ، وبعد إتمام هذه العملية والتأكد من أن هوية الحامل مطابقة للبيانات، يستوجب على البنك تسليم البطاقة إلى حاملها بشكل شخصي ومطابقة توقيعه مع الذي مع البطاقة.

- قيام البنوك بإجراء كشوفات دورية قصيرة المدى لحسابات العملاء وإبلاغهم بها حتى يتم كشف أي اختلاس فور حدوثه. [2]

- مراقبة عمليات الوفاء والسحب من العملاء لاكتشاف أي استخدام مشبوه لتلك البطاقة والتأكد من عدم مجاوزة سقف البطاقة أو صلاحيتها. [3]

[1]- عبد الكريم الردايدة، المرجع السابق، ض 183.
[2]- نهى خالد عيسى، ماهية بطاقات الائتمان والآثار القانونية المترتبة عن استخدامها، مجلة المحقق الحلبي للعلوم القانونية والسياسة، العدد الثاني، السنة السابعة، 2015، ص 242.
[3]- علي عدنان الفيل، المرجع السابق، ص 79.

3- بالنسبة للتجار:

وكما الحال مع العملاء يتم الاختيار الحسن من قبل البنك للتجار والمؤسسات التجارية التي تتمتع بسمعة طيبة، مع الاستقرار القانوني والمهني والمالية [1]

- تزويد البنوك للتجار والمؤسسات التجارية بالأجهزة الالكترونية الحديثة التعامل بها ومن خلالها يتم الكشف الفوري عن البطاقات المزورة، مع التزامه بتسليم هذه المكينة شخصيا، وهذا لاحتمال وقوعها في يد الغير الذي قد يستغلها في أعمال غير شرعية [2]

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

- كذلك يجب أن يتم إجراء المعاملة للعميل في وجوده، وبعد التأكد من هويته وخذ توقيعه على إشعارات البيع بعد مطابقته لتوقيعه على البطاقة حيث وجب أن يكون بشكل واضح كما يتم رفض أي اشعارات أخرى.

المطلب الثاني: الإجراءات المتخذة من قبل حامل البطاقة والتاجر ومختلف الأجهزة:

تعتبر مهمة حماية البطاقة من التلاعب، والحد من الاستخدام غير المشرع لها من واجبات المصدر الذي يقع عليه عبء توفير أكبر قدر من الحماية للبطاقة التي يصدرها، كذلك الحال بالنسبة للحامل والتاجر عليهم مسؤوليات يجب عليهم القيام بها وهي إجراءات وقائية فعلى الحامل المحافظة على البطاقة وعلى التاحر معرفة المميزات الخاصة لكل بطاقة من الطاقات القابل لها، وذلك حتى يسهل عليه معرفة البطاقة المزورة من البطاقة الصحيحة.

الفرع الأول : الإجراءات المتخذة من قبل حامل البطاقة:

تتمثل الإجراءات التي يقوم بها الحامل، وهي عدد من الوسائل الوقائية التي تهدف إلى المحافظة إما على الطاقة من الضياع أو السرقة، أو المحافظة على الرقم السري حتى لا تستخدم استخداما غير مشروع من قبل الغير وهذه الإجراءات هي:

[1]- علي عدنان الفيل، المرجع السابق، ص 79.
[2]- عبد الكريم الردايدة، المرجع السابق، ص 184.

1- أن يقوم الحامل بوضع الطاقة في مكان أمين، وأن لا يتركها في مكان تسهل فيه سرقتها أو ضياعها.

2- أن لا يقوم الحامل بإعطاء البطالة إلى أي شخص حتى لو كان أحد أصوله، أو فروعه أو زوجه.

3 - أن لا يقوم الحامل بكتابة الرقم السري على جسم الطاقة، أو على ورقة منفصلة مع البطاقة، بل يجب عليه أن يحفظ الرقم السري غيبا، ويتلف الوثيقة التي يكون بها الرقم السري أو يحرقها.

4 - يجب على الحامل ألا يقوم بترديد رقمه السري أمام أي شخص، كذلك أن يحرص على أن لا يشاهده أحد وهو يقوم بإدخال الرقم السري في جهار الصراف الآلي.

5 - علم طلب الوصل المطبوع من جهاز الصراف الآلي، وإن طلبه يقوم بإتلافه ولا يتركه لأنه يحتوي على رقم حساب الحامل.

6 - عدم رمي نسخة الفاتورة التي يعطيها التاجر اللحامل، لأنها تحوي على رقم البطاقة.

7- عدم استخدام البطاقة لدى المحلات التجارية الصغيرة أو المشكوك فيها.

8- عند شك الحامل أن رقم البطاقة قد عرف، يقوم بإبلاغ المصدر فورا وطلب منه إلغاء البطاقة.

9- حرص الحامل ألا يكون رصيده مبالغ كبيرة حتى تكون الخسارة صغيرة، ويطلب من المصدر أن لا ايسمح للتاحر بتجاوز الرصيد، إلا إن قام هو بالاتصال بالمصدر وقام بالطلب منه بعد أن يعطيه رمز التعريف الخاص به.

10- التأكد من البيانات والمستندات الخاصة بالمعاملات غير المباشرة.

11- عدم الاستجابة لرسائل البريد الإلكتروني (الخادعة) التي ترد منسوبة لبعض البنوك أو الجهات الأخرى، وذلك للتحقق من مصدرها.

12- إخطار البنك فور التأكد من عدم سلامة معاملة تضمنها كشف الحساب الوارد من البنك.

13- عدم خدش البطلة باستخدام آلات حادة.

14- عدم إعطاء رقم البطاقة للأخرين عن طريق الهاتف، إلا في حالة التعامل مع شركة موثوق فيها [1]

"أما بالنسبة لعملية الشراء من خلال الانترنت، فأهم إجراء لابد من اتخاذه، هو التأكد من وجود اتصال آمن، والمتمثل بوجود كلمة، https : // بدلا من http : // في بداية عنوان الموقع، والتأكد من وجود القفل المغلق في أسفل نافذة المتصفح، وأن يكون الموقع الذي يتعامل معه على درجة عالية من الثقة، ولكن لا ينصح بشكل عام بالتسوق عبر الانترنت بسبب المخاطر التي سوف يتعرض لها العميل وحتى لو كان ذلك بالنسبة الضئيلة" [2]

الفرع الثاني: الإجراءات المتخذة من قبل التاجر.

"فالمستهدف الأول من عملية الاستخدام الغير مشروع للبطاقة الدفع الالكتروني هو التاجر باعتبار أنه هو الذي سيتحمل الخسائر المادية وربما الدعاوي القانونية، لذا فإنه عليه أن يقوم بالإجراءات التالية للوقاية من الاستخدام غير المشروع للطاقة وهي" [3]

أولا: أثناء تنفيذ عملية الوفاء بواسطة البطاقة:

وذلك بالقيام بالإجراءات التالية:

الطلب من شخص مقدم البطاقة هويته الشخصية، فإن لم يكن الحامل الشرعي لها، وجب عليه هنا أن يرفض الوفاء بها.

1- تثبت التاجر من وجود توقيع على البطاقة وقت الشراء، فإن لم يكن هناك توقيع في للتاجر هنا أن بطلب من الحامل التوقيع عليها بعد التثبت من هويته.

2- عدم تجزئة العملية الشرائية الواحدة إلى أكثر من تمريرة واحدة للبطاقة على الجهاز.

3- في حال عدم التمكن من تمرير البطاقة على الجهاز، فهنا على التاجر أن يقوم بختم البطاقة بواسطة الجهاز اليدوي أو رفض البطاقة.

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

[1]- عبد الكريم الردايدة، المرجع السابق، ص ص ، 187- 188.
[2]- وسام فيصل محمود الشواورة، المرجع السابق، ص ص، 106- 107.
[3]- أمجد حمدان الجهني، المرجع السابق، ص 124.

5- وفى حالة إظهار عبارة "اتصل بـ أميكس" أو "راجع جهة الإصدار" عند تمرير البطاقة به، فلا داعي للمحاولة مرة أخرى، بل على التاجر الاتصال بمركز التفويض للحصول على رمز التفويض والموافقة على العملية [1]

6- وأن يكون لدى التاجر القدرة على التمييز بين البطاقات المزورة والصحيحة، أي لديه العلم بخصائص بطاقة الوفاء وممزاته، فعند استلامه البطاقة من الحامل، عليه التأكد من أن البطاقة سليمة وسارية المفعول، وأن لا تكون غريبة الشكل أو خالية من أحد علامات الضمان كوجود الحمامة، عدم وجود أي كشط على الشريط الممغنط، وأن البيانات المدونة على البطاقة مطابقة لصاحبها، وأن يكون التوقيع المدون على فاتورة الشراء هو نفسه التوقيع المدون على البطاقة [2]

ثانيا: وجوب تأكد التاجر من الأمور الآتية:

1 - أن البطاقة سليمة تماماً وسارية المفعول.

2 - سلامة الشريط المخصص للتوقيع على البطاقة.

3 - أن البيانات المسجلة على البطالة مطابقة لبيانات حاملها (الاسم. العمر. الجنس).

4- مطابقة رقم البطاقة والتوقيع المدون عليها مع الإيصال الموقع.

5 – "من أن البطاقة المقدمة في التعامل من صاحبها نفسه.

6 - من أن المبلغ المسموح به لحامل البطاقة يغطي قيمة مشترياته" [3]

ثالثا: ألا يقبل التاجر البطاقات التالية:

1 - أي بطاقة تالفة، أو معدل عليها، أو ذات شكل غير متعارف عليه.

2 - أي بطاقة فيزا، أو ماستر كارد، أو داينرز كلوب، أو أمريكان اكسبريس، لا تحتوي على علامات الضمان. [4]

رابعا: وجوب أخذ الحيطة والحذر من حاملي البطاقة الذين يتصرفون كالآتي:

- يخرجون بطاقة الدفع الالكتروني من الجيب بدلا من المحفظة.

- يقومون عشوائيا بانتقاء سلع دون الاهتمام إلى سعرها أو جودتها أو حجمها.

---

[1]- أمجد حمدان الجهني، المرجع السابق، ص ص، 124 – 125.
[2]- وسام فيصل محمود الشواورة، المرجع السابق، ص 107.
[3]- عبد الكريم الردايدة، المرجع السابق، ص ص، 185- 186.
[4]- المرجع السابق، ص 125.

- يقومون بعمليات شرائية صغيرة ومتعددة تبقيهم ضمن الحد الآمن.

- يقومون بشراء أغراض ثمينة بواسطة بطاقات وقاء صادرة حديثا. [1]

- يبرزون جواز سفر لا يوجد عليه ختم لدخول البلاد لا يستطيعون تقديم أي إثبات هوية عند الطلب.

- يظهر عليهم السلوك العصبي، أو التعرق المفرط أو الاستعجال. [2]

لذا يتوجب على التاجر إذا اشتبه في أحدهم فيتوجب عليه إبلاغ البنك حتى لا يقع ضحية لجريمة الاحتيال والسرقة أو التزوير لأنه هو من يتحمل المسؤولية القدر الأكبر من الخسائر.

الفرع الثالث: الإجراءات الوقائية المتخذة من طرف بعض الأجهزة:

إن غياب تشريع خاص يضبط هذه الجرائم فإن عبء المسؤولية يقع على الأجهزة الأمنية ومن بين المصالح التي تشملها الحماية الأمنية ما تعلق بالمعاملات المالية ومنها ما يتم ببطاقة الدفع الإلكتروني، حيث تتكفل هذه الأجهزة بمتابعة الجرائم التي تقع على هذه البطاقة بجملة من الإجراءات الوقائية تتمثل فيما يلي: [3]

أولا: الإجراءات المتعلقة بالبنوك والمؤسسات المالية:

تعمل أجهزة الشرطة على التنسيق والتعاون مع البنوك والمؤسسات المالية وذلك بغية إخطارهم عن أي جريمة أو خطر يهدد الأمن الداخلي للمؤسسة أو يمس بأموال الأفراد. كما يتم وضع تعليمات بإلزام البنوك والمؤسسات المالية بالتبليغ عن الجرائم التي قد تحدث أثناء التعامل بالبطاقات وعدم التستر عليها لمنع المجرمين من الافلات من العقاب، كما يتم أيضا تأمين المئسسات المتعاملة ببطاقات الدفع الالكتروني وإحاطتها بحراص الأمن وأفراد البحث الجنائي لمراقبة المجرمين ووضع أجهزة متطورة لتصوير البطاقات المستعملة حتى يتراجع المجرمون عن ارتكاب مثل هذه الأفعال الإجرامية. [4]

---

[1]- أحمد حمدان الجهني، المرجع سابق، ص 125.
[2]- المرجع نفيسه، ص
[3]- عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، ط، دار الحامد للنشر والتوزيع، عمان، 2013، ص128
[4]- عبد الكريم الردايدة، المرجع نفسه، ص 129.

ثانيا: الإجراءات المتعلقة بالأفراد:

وذلك بتوعية المواطنين ومستخدمي هذه البطاقات بالمخاطر التي تحيط بها عن طريق الحملات التحسيسية وعقد الندوات واللقاءات التوعوية، وذلك لتوخي الحيطة والحذر ومراقبة الأشخاص الخطرين ذوو السوابق العدلية في هذه الجرائم وإحاطتهم بالمراقبة الأمنية المستمرة. [1]

ثالثا: الإجراءات المتعلقة بتطوير الأجهزة التقنية للمؤسسات الشرطية:

من الصعب التصدي لجرائم بطاقات الدفع الالكترونية لأنها من الجرائم التقنية غير التقليدية فهي تتميز بالخصوصية عن بقية الجرائم ومرتكبوها يتميزون بالخبرة في مجال تقنية المعلومات لذا كان لزاما على الشرطة تطوير أجهزتها التقنية عن طريق ما يلي: [2]

- العمل على إنشاء معمل جنائي متخصص وتدعيمه بالأجهزة والمعدات التقنية المتطورة لاستغلالها في عمليات فحص البطاقات والمستندات والوثائق المستخدمة في تلك الجرائم.[3]

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

تدريب أفراد جهاز الشرطة على كيفية استعمال الأجهزة الالكترونية وأدواتها ولآلات الطباعة المخصصة لها من شأنه أن يسهل عليهم اكتشاف ومتابعة الجرائم الواقعة على بطاقات الدفع الالكتروني.

المبحث الثاني: الإجراءات الردعية لمواجهة الجرائم الواقعة على بطاقات الدفع الإلكتروني:

إن خطورة الجرائم الالكترونية وتفاقمها بشكل ملحوظ، تستدعي العمل على تطوير الإجراءات الكلاسيكية الخاصة بالبحث والتحري عن الجرائم التي تتماشى مع هذه الجرائم المستحدثة من خلال تعديل القوانين القديمة وبالنظر إلى أن مخاطرها ليست ذات طبيعة وطنية فقط، بل تتعدى الفواصل الجغرافية بين الدول فإن الأمر يستدعي تدخلا شرعيا بالنص الصريح سواء على المستوى الداخلي أو الدولي ولذلك قمنا بتقسيم دراستنا في هذا البحث إلى مطلبين (المطلب الأول) إجراءات المكافحة على المستوى الوطني و(المطلب الثاني) إجراءات المكافحة على المستوى الدولي.

---

[1]- عبد الكريم الردايدة، المرجع السابق، ص 130.

[2]- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004، ص ص 163 – 164.

[3]- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2015، ص 99.

[4]- محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2014، ص 257.

المطلب الأول: الإجراءات الكلاسيكية أو المعتادة في الجرائم المستحدثة:

تملك العديد من الدول أجهزة متخصصة في مجال مكافحة جرائم بطاقات الدفع الالكتروني وتبذل جهودا فائقة في مجال الجرائم الالكترونية نظرا لخطورتها وتسعى لمحاولة الحد من مخاطر هذه الجرائم في حين أن هناك دولا أخرى تفتقر لمثل هذا التخصص ففي الجزائر تقوم الشرطة القضائية بمجموعة من الإجراءات الخاصة بذلك وفقا لما يحدده القانون وبما أن دراستنا تنصب على جريمة من جرائم الالكترونية فإن إجراءات البحث والتحري فيها يجب أن تكون على مستوى عال من الخبرة والدقة التقنية حيث يكون أفراد الشرطة على علم بهذه الإجراءات من جهة ومن جهة أخرى ولتبيان هذه الإجراءات سنقسم مطلبنا إلى ثلاثة فروع، نخصص الفرع الأول منه لدراسة مرحلة تلقي البلاغات وكيفية التعامل معها (التحقيق) في حين نتناول في الفرع الثالث مراحلة المحاكمة. [1]

الفرع الأول: مرحلة البحث والتحري

يختلف التبليغ في الجرائم الالكترونية عن التبليغ في الجرائم الأخرى، ذلك لأن الجريمة الإلكترونية تتم في فضاء إفتراضي، 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 به بهذه المؤسسات والتأكد من مصداقية المعاملات المصرفية، وتتبع المشتبه بهم ورصد أي تحركات غير عادية تتم في داخل أو خارج هذه المؤسسة والمحلات.

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

أولا: تلقي البلاغات والشكاوي

1- المقصود بآلية التبليغ:

البلاغ هو إخبار السلطات المختصة عن جريمة حصلت أو قد تحصل، ويلتزم بالإبلاغ عن الجرائم كل فرد في المجتمع سواء كان هو الضحية أو غيره، ويهدف ذلك إلى سرعة

[1]- صراع كريمة، واقع وأفاق التجارة الالكترونية في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم التجارية، كربالي بغداد، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، 2014، ص 83.

تحرك الشرطة القضائية باعتبارها الجهة المختصة في الكشف عن الجرائم والحد من تناميها. [1]

أما في الجرائم المعلماتية يكون الشخص المبلغ عن الجريمة على معرفة بالأجهزة الالكترونية 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 وإجراء التحقيقات الابتدائية". [3]

2 - كيفية التبليغ:

تضع الجهات الأمنية كالشرطة والدرك تحت تصرف المواطنين مواقع ليتمكنوا من خلالها من التبليغ عن الجرائم، ومثل ذلك الموقع الالكتروني للدرك الوطني: www.mdn.ppgn.dz وكذلك الموقع الالكتروني الأمن www.dgsn.dz، لكن هذه المواقع ليست ملزمة للمبلغين حيث لهم الحرية في اتباع هذه الطرق المستحدثة أو التبليغ بالطرق العادية، [4] في حين أنهم ملزمون بتحديد أسماء المشتبه بهم، والقيام بطباعة نسخة ثانية للبيانات المتضررة في الأجهزة، كما يجب عليهم الامتناع عن نشر الجريمة للغير وبالتالي فإن للتليغ دور فعال في مساعدة الأجهزة الأمنية المختصة للتأكد من وقوع الجريمة وتحديد نوعها وتجهير الوسائل المناسبة للكشف عنها. [5]

ثانيا: مرحلة البحث والتحري

إنطلاقا من المعلومات المحصل عليها، يقوم رجال الضبطية القضائية بالتحري عن الجريمة من خلال وضع خطة مناسبة لها، وتعيين فريق العمل بهدف أحتواء الجريمة والإحاطة بكافة جوانبها وذلك كما يلي:

---

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

[2]- علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية – دراسة مقارية- ، دط، المكتب الجامعي الحديث، الموصل، 2012، ص 11.

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

[4]- حسن ربيعي، المرجع السابق، ص 218.

[5]- المرجع نفسه، ص 218.

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 أيضا 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 لخصوصية جرائم بطاقات الدفع الإلكتروني التي تتم بسرعة ولا تترك آثارا بعد ارتكابها وصعوبة إيجاد أدلة إثبات لهذه الجرائم التي تعتمد على الذكاء والتضليل 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:

- **المحقق الرئيسي:** هو الذي يشرف على عملية التحقيق ويتولى توزيع المهام على الضباط الأخرين، ويكون خبير في إجراءات التحقيق وفي المجال المعلوماتي حتى يتمكن من السيطرة على الوضع واتخاذ القرارات المناسبة. [3]

- **خبراء الحاسوب والانترنت:** وهم خبراء يكون عددهم واحد فأكثر حسب ما تتطلبه إجراءات التحقيق ليكونوا على اطلاع كافي بالجريمة المعلوماتية وكيفية التحري عنها خاصة أن الجريمة الالكترونية تستدعي هولاء لدرايتهم بالمجال المعلوماتي والتقني.

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

---

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

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

[3]- علي عدنان الفيل، المرجع السابق، ص ص 16، 17.

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

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

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

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

إضافة إلى ما سبق هناك ضباط أخرون موجودون وفق ما تتطلبه ظروف الجريمة مثل ضباط الحماية وضباط التفتيش وضباط القبض. [1]

3- الخبرة:

فلا بد من الدراية الكافية بالتقنيات الحديثة في المجال المعلوماتي ليسمح لفريق الفريق العمل الذي يتولى التحقيق بالتعامل مع الملفات والبرامج والإحاطة بواسطة التلاعب بالأجهزة الالكترونية ومحتواتها، لذلك يساهم اللجوء إلى الخبراء في الكشف عن الجريمة وقت مبكر وبطريقة مناسبة. [2]

ثالثا: مرحلة تجهيز الوسائل:

فلتحقيق الهدف المنشود في التحقيق يجب استخدام بعض الوسائل والبرامج لتتبع العمليات التي تتم داخل أنظمة الحواسيب الآلية ومن أهم الوسائل ما يلي:

- **وضع الرموز:** تتمثل هذه الوسيلة في تعيين الرقم السري معاملة ما، لتتبع معطيات الأنظمة والبرامج المعالجة من خلال هذه المعاملة. [3]
- **تتبع البرامج:** يتم من خلال استخدام الرقم السري للبرامج، أو من خلال تشغيل التعليمات الموجودة ضمن البرامج والتي يتمكن من خلالها المحقق من تحسين محتوى هذا البرنامج بالمعلومات الصحيحة.

---

[1]- حسين ربيعي، المرجع السابق، ص ص، 221، 223.

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

[3]- محمود ابراهيم غازي، الحماية الجنائية الخصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2014، ص ص 704، 705.

وقد سيتعين المحققون أيضا بمجموعة من البرامج أيضا:

- **برنامج إذن التفتيش:** من خلاله يتم إدخال البيانات اللازمة لتحديد الأدلة.
- **برنامج (vieu disk):** يسمح هذا البرنامج باختراق القرص المرن مهما كانت درجة تأمينه، والحصول على معطياته.
- **برنامج اتصالات:** يعمل هذا البرنامج على ايصال جهاز المتهم بالجهاز الخاص بالمحقق للحصول على معلوماته. [1]

الفرع الثاني: مرحلة التحقيق:

في هذه المرحلة يقوم ضباط الشرطة القضائية ببعض الإجراءات للإحاطة بمسرح الجريمة من خلال الانتقال للمكان ومعاينته وتفتيشه وضبط الأشياء المتعلقة بالجريمة وهذا ما سنوضحه بذكر أهم مراحل التحقيق ومجرياته:

أولا: المعاينة

تعتبر المعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأى في ذلك ضرورة تتعلق بالتحقيق والأصل أن يحضر المعاينة أطراف الدعوى وقد يجريها المحقق في غيابهم والمعاينة إجراء وجوبي في الجنايات وجوازي في الجنح وتتم في الأماكن العامة والخاصة على حد سواء وفي الأماكن الخاصة تحتاج إلى رضا صاحب المسكن أو بإذن قضائي وفي نهاية هذه المرحلة يتم وضع الأختام على ماتم معاينته وتعيين مراقب عليه. [2]

وفي جرائم بطاقات الدفع الالكترونية والجرائم المعلوماتية إما أن يكون مسرح الجريمة تقليدي وتتم فيه معاينة الأشياء الملموسة التي تقع خارج أنظمة الأجهزة الالكترونية ومثال ذلك الأوراق أو المستندات أما في مسرح الجريمة التقني يتم معاينة الأشياء الافتراضية وهي المكونات الموجودة داخل أنظمة الحواسيب والأنترنيت ومثال ذلك البرامج والتطبيقات. [3]

[1]- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، د ط، دار الكتب القانونية، مصر، 2013، ص690.

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

[3]- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2014،ص ص، 718، 721.

ثانيا: التفتيش

بالإضافة إلى المعاينة في الجرائم المعلوماتية، يقوم رجال الضبطية القضائية المختص بالتفتيش الذي يعتبر إجراء من إجراءات التحقيق يهدف إلى ضبط الأدلة والقرائن مع مراعاة شروط وضوابطه القانونية. [1]

1- الشروط الشكلية:

- **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 ولكنه مع خصوصية الجرائم الواقعة على النظام المعلوماتية فقد نفى المشرع عنها هذه الشروط، وذلك بموجب نفس المادة السابقة الذكر في فقرتها الأخيرة بعد التعديل الذي جاء به القانون 06-22، حيث نصت على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بأنظمة المعالجة الآلية للمعطيات..." [2]..
- **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". [3]

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 علاقلة تتبعها.

- **محضر التفتيش:** يلتزم ضابط التحقيق بتحرير محضر يدون عليه ما توصل 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 تحريرع بمن يملك الخبرة في مجال تقنية المعلومات.

---

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

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

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

2- 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 بنظم المعالجة

الآلية للمعطيات، وقد حدد المشرع الجزائريمجموعة الجرائم الماسة بنظم المعطيات في القانون 04-15 الذي أدرج فصلا كاملا في قانون العقوبات في الفصل السابع منه تحت مسمى جرائم الاعتداء على نظم المعالجة الآلية. [1]

كما يجب أن يكون قد تم توجيه تهمة لشخص أو عدة أشخاص معينة بارتكاب جريمة أو المشاركة فيها من خلال قيام دلائل قوية وقرائن ضدهم تدعو للشك فيهم وفي البيئة المعلوماتية، وتشمل هذه الدلالات والقرائن في حاسوب معين تم تحديده، واتضح أنه ملك للمتهم أو ضبط في حوزته على معدات معلوماتية أو أجهزة أو مستندات إلكترونية 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 الأنترنيت وكل ملحقاتها 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 الالكترونية متلبس بها من خلال رصد الجاني عبر شبكة الأنترنيت في حركة مريبة، ليتم ترصده عبر هذه الشبكة. [3]

- **الإذن:** كقاعدة عامة يتم إجراء التفتيش من قبل المختص بذلك، لكن في حالات يتم تكليف ضابط من الضابطة العدلية، وفي هذه الحال حتى يباشر مهامه وجب حصوله على إذن بالتفتيش بالإنابةعن السلطة المختصة بذلك التي تمنحه له، ويجب أن يتضمن هذا الإذن مكان التفتيش والشخص والأشياء الأخرى كالأجهزة الآلية وبرامج الفيروسات

---

[1]- القانون 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية، عدد 71، السنة 41، الصادرة بتاريخ 10 نوفمبر 2004، وقد عززه المشرع الجزائري بالقانون 09-04 المؤرخ في 5 أوت 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، عدد47، السنة 46، الصادرة بتاريخ 16 غشت سنة 2009.

[2]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 408.

[3]- المرجع نفسه، ص 409.

والاختراق[1]، وقد نصت على ذلك المادة 44 من قانون الإجراءات الجزائية بقولها: "يجب أن يعين الإذن بالتفتيش بيان وصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها..."[2]

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 الدليل التقني هو الدليل الوحيد الذي يقود لاثبات الجريمة. [3]

3- 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[4]، وذلك بعد أن تستوفي عملية التفتيش الشروط المذكورة أعلاه.

4- تفتيش المكونات المعنوية لنظام المعالجة الآلية:

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

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

ب- منظومة تخزين معلوماتية..."[5].

5- التفتيش عن بعد:

تتكون الشبكة المعلوماتية من مجموعة من الأجهزة الالكترونية متصلة ببعضها البعض بطريقة سلكية أو لا سلكية، ومع التطور التكنولوجي وظهور شبكة الأنترنيت أصبحت

---

[1]- رشيدة بوكر، المرجع السابق، ص ص، 410- 411.
[2]- أنظر المادة 44 من قانون الإجراءات الجزائية.
[3]- رشيدة بوكر، المرجع السابق، ص 396.
[4]- فايز نبيل عمر، الحماية الجنائية للمحل الالكتروني في الجرائم المعلوماتية، د ط، دار الجامعة الجديدة، الاسكندرية، 2012، ص 131.
[5]- أنظر المادة 5 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

هذه الشبكات تمتد إلى كافة أنحاء العالم ولذلك فإن هذه الشبكات عند تفتيشها تكون بعيدة عن موقع التفتيش[1]، وفي هذه الحالة نميز بين حالتين:

أ- **اتصال جهاز المتهم بجهاز داخل الدولة:** وقد نص المشرع على ذلك في المادة الخامسة من القانون 09-04 في فقرتها الثانية والتي جاء فيها: "إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك..." [2].

ب- اتصال جهاز المتهم بجهاز آخر خارج الدولة: أجاز المشرع الجزائري تفتيش الأنظمة المتصلة مع تظام المتهم ولو كان 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 السلطاب الأجنبية المختصةطبقا للاتفاقيات الدولية ذات الصلة ووفقا لمعاملة بالمثل" [3].

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

يهدف التفتيش إلى ضبط الاشياء المتعلقة بالجريمة ويفيد كذلك في التحقيق الجاري شأنها سواء كانت تلك الأشياء أوراق استعملت في ارتكاب الجريمة أو نتجت عنها أو مما يفيد في كشف الجريمة وهذا ما جاء به نص المادة 6 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومن خلالها تتم عليه الضبط كما يلي:

1- ضبط الأشياء المادية:

يساعد ضبط الأدلة المادية في اثبات جرائم الأجهزة الالكترونية والتعرف على مرتكبيها ومن بينها:

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

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

- **الحاسب الآلي وملحقاته:** ويتم ضبط جهاز الحاسب الآلي المستخدم في الجريمة بعد أن يقوم الخبير بتمييزه عن الأجهزة الأرى، ومعرفة مواصفاته وتحديد ملحقاته.
- **أقراص الليزر:** تتواجد أقراص الليزر بكثرة في البنوك والمؤسسات المالية، حيث يقوم الخبير بتحليل محتواها لأنها قد تحتوي على دليل يمكن من اطتشاف الجريمة ومرتكبها.
- **الشرائط الممغنطة:** وتتمثل وظيفة هذه الشرائط في الحفظ الاحتياطي، ويتم حفظها في أماكن آمنة في مراكز التوثيق المحمية كما قد يتم ايداعها في الخزائن الخاصة بالبنوك.
- **المودم:** هو الذي يوفر الأنترنيت للأجهزة المتصلة ببعضها البعض سواء عن طريق خطوط الهاتف أو لا سلكيا.
- **بطاقات الدفع الإلكتروني:** يتم التحفظ على القديمة منها وكذلك ما تم استخدامه في تجهيز هذه البطاقة.
- **بطاقات (Pcmcia):** ولها نفس شكل بطاقات الدفع، وتستعمل في الحواسيب الصغيرة – نوت بوك- واللابتوب.
- ويتم التحفظ على هذه المكونات المادية المذكورة كلها أو جزء منها للاستفادة من أي معلومة قد تفيد في مسار الكشف عن الجريمة[1].

2- ضبط البيانات الالكترونية:

فيما يخص البيانات الالكترونية فهي من الأشياء غير المادية، وقد اختلفت بشأنها الفقه وانقسم إلى اتجاهين كما يلي:

أ- الاتجاه المؤيد لقبولها محلا للضبط: يرى هذا الاتجاه بأن البانات هي عبارة عن موجبات كهرومغناطيسية وذبذبات معلوماتية صالحة للتخزين والحفظ والتسجيلعبر الأقراص والوسائل المادية الأخرى، فهي قابلة للنقل والبث والاستقبال وإعادة الانتاج وبالتالي فهي من قبيل الأشياء المادية.

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

---

[1]- علي عدنان الفيل، المرجع السابق، ص ص 56- 57

[2]- صالح شنين، الحماية الجنائية للتجارة الالكترونية – دراسة مقارنة- ، رسالة لنيل شهادة الدكتوراه في القانون الخاص محمد رايس، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2013، ص ص، 237- 238.

3- المحافظة على الأدلة المضبوطة:

بعد إجراء ضبط الأدلة التقنية يتم تأمينها وتخزينها 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 7 من القانون09- 04 السالف الذكر. [1]
- الاحتفاظ بالأقراص كما هي وعدم طيها لضمان عدم اتلافها.
- المحافظة على المعطيات الأطلية المخزنة في الدعائم الإلكترونية وعدم الاكتفاء بالنسخ .
- المحافظة على الأشرطة الممغنطة والأقراص بعيدا عن الحرارة العالية والرطوبة والالتزام بالدرجات المسموح بها. [2]

الفرع الثالث: مرحلة المحاكمة

إن القضاء وفي أي دولة يلعب دورا مهما للتصدي في جميع الاعتداء التي يمكن أن يتعرض لها أفراد المجتمع أو المصالح التي حماها القانون فبعد إتمام إجراءات التحري والتحقيق اللازمة وضبط الدليل المعلوماتي، تقوم النيابة بتقديم نتائج التحقيق إلى المحكمة المختصة لإجراء المحاكمة، وبعد استقرار الأدلة توقيع العقاب على الجناة من عدمه، ولأن الجرائم الالكترونية تتسم بالطابع التقني وهي جريمة عابرة للقارات، فإن خطرها يمتد لكافة 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.[3] خاصة إذا كانت الجريمة تمس بالنقود والأوراق المصرفية الوطنية وإن كان مرتكبها أجنبيا.

أولا: الاختصاص الجنائي الدولي

في التشريع الجزائري يتم تحديد الاختصاص وفقا للاعتبارات التالية:

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]- أنظر المادة 7 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.
[2]- رشيدة بوكر، المرجع السابق، ص 422.
[3]- صالح شنين، المرجع السابق، ص ص، 259 - 260.

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

3- مبدأ العينة: يختص هذا المبدأ بالجرائم الالكترونية 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. [1]

ثانيا: الاختصاص الجنائي الوطني

يتم تحديد الاختصاص على المستوى المحلي وفقا للمكان الذي ارتكبت فيه الجريمة أو المحل السكني لأحد من المشتبه بهم في ارتكابها، أو المكان الذي تم إيقافه[2]، وفيما يخص الجرائم الالكترونية فإن المشرع الجزائري وبالرجوع لقانون الإجراءات الجزائية نجده وزع الاختصاص على النحو التالي:

1- اختصاص النيابة العامة: بالرجوع للمادة 37 فقرة 2 من قانون الاجراءات الجزائية نجد أن المشرع الجزائري قد وسع من صلاحيات وكيل الجمهورية ومدد اختصاصه إلى محاكم أخرى، تطبق حسب التنظيم مع مراعاة ضابط الشرطة لالتزاماته وفق المادة 40 مكرر1و2 من نفس القانون.

2- إختصاص قاضي التحقيق:

كذلك تم تمديد صلاحيات قاضي التحقيق إلى المحاكم الأخرى، وذلك بموجب نص المادة 40 من القانون 04-14[3]، وتطبيق هذه الإجراءات بحسب التنظيم.

3- إختصاص محاكم الجنح:

بالنسبة لاختصاص محاكم الجنح في حالة قيام جريمة من جرائم المساس بالمعطيات فإن المشرع الجزائري قام بتمديد اختصاصها إلى دوائر اختصاص محاكم أخرى حسب نص المادة 4-329 من القانون 04-14 وتطبق أيضا حسب التنظيم، وما يلاحظ على هذا التمديد بالنسبة لكل من النيابة العامة وقاضي التحقيق ومحاكمة الحنح أنه محلي ولا يشمل الجرائم التي ترتكب خارج الدولة. [4]

---

[1]- صالح شنين، المرجع السابق، ص ص، 267- 268.

[2]- المرجع السابق، ص 269.

[3]- القانون 04- 14 المؤرخ في 10 نوفمبر 2001، المعدل والمتمم للأمر رقم 155/56 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية الجزائرية، عدد 71، السنة 41، الصادرة بتاريخ 10 نوفمبر 2004.

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

المطلب الثاني: الإجراءات الخاصة أو المستحدثة

حتى يضمن المشرع الجزائري الحماية الجنائية والإجراءات اللازمة للمعاملات الالكترونية، وبعد إدراكه أن الإجراءات الاعتيادية وحدها لا تكفي بالرغم من تطورها بل يلزم قوانين وإجراءات جديدة خاصة بها لذلك فقد تدارك الأمر سواء على الصعيد الداخلي أو الخارجي، ولتبسيط الضوء على مختلف هذه الإجراءات المتخذة فقد قسمنا هذا المطلب إلى فرعين، خصصنا الفرع الأول منه لدراسة التطور التشريعي الحاصل في هذا المجال، بينما خصصنا الفرع الثاني منه لاستعراض الاجراءات المستحدثة.

الفرع الأول: التطور التشريعي

لمواكبة التطور الدولي الحاصل في مواجهة الجرائم المعلوماتية، اتجه المشرع الجزائري إلى استحداث نصوص إجرائية وعقابية للأفعال المكونة لهذه الجرائم والتي سلكت منعرجا خطيرا ومن بينها الجرائم الواقعة على بطاقات الدفع الالكتروني.

أولا: على المستوى الوطني

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

- القانون 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 والمتضمن قانون العقوبات، والغاية منه مكافحة الجرائم الالكترونية بتجريم الأفعال المكونة لها، وكان ذلك بإضافة القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، من مادة 394 مكرر إلى غاية المادة 394 مكرر7 من هذا القانون. [1]
- القانون 09-04 المؤرخ في 5 أوت 2009، والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويهدف هذا القانون إلى وضع نصوص إجرائية تتناسب مع الجرائم الالكترونية. [2]

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

---

[1]- القانون 04-15، المصدر السابق.
[2]- القانون 09-04، المصدر السابق.
[3]- القانون 06-22 ، المصدر السابق.

- القانون 16-02 المؤرخ في 19 يونيو 2016، المتمم للأمر 66-156، جاء هذا القانون ليتمم القانون 87 مكرر77 و87 مكرر 12 إضافة إلى المادة 394 مكرر8. [1]
- المرسوم الرئاسي 15-261 المؤرخ في 8أكتوبر 2015إلى إنشاء الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [2]

2- الجهات المختصة بمكافحة الجرائم المعلوماتية:

وهي الهيئات المكلفة بمهام معينة للوقاية ومكافحة الجرائم المعلوماتية وهي كالآتي:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

نص عليها المشرع الجزائري في المادة 13 من القانون 09-04 وكان دخولها حيز النفاذ في سنة 2015 بموجب المرسوم الرئاسي 15-268، وعرفتها المادة 13 بأنها سلطة إدارية مستقلة معنويا وماليا، مقدرها بالعاصمة، كما جاءت المادة 14 من القانون 09-04 والمادة 4 من المرسوم الرئاسي سابق الذكر لتحديد مهام اللجنة تحت إشراف السلطة القضائية أساسافي تنشيط وتنسيق إجراءات الوقاية والمكافحة ومساعدة السلطات القضائية.[3]

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

تسعىمديرية الأمن الوطني لمكافحة الجرائم ومن بين الجرائم الالكترونية، حيث تتولى نيابة مديرية الشرطة العلمية والتقنية التابعة لها مهمة التصدي للجرائم المعلومتية، وتتواجد على المستوى الوطني في ثلاث مناطق وهي قسنطينة ووهران، إظافة إلى ثلاث وحدات أخرى طور الانجاز في كل من ورقلة وبشار وتمنراست. [4]

جـ- 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 الاسناد، هياكل التكوين، المعهد الوطني للأدلة وعلم الإجرام، المصلحة

---

[1]- القانون 16-02، المصدر السابق.

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

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

[4]- ربيعي حسين: آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتورة رحاب شادية، قسم الحقوق والعلوم السياسية، جامعة باتنة1، 2016، ص ص، 176- 177.

المركزية للتحريات الجنائية، المصالح والمراكز العلمية والتقنية، حيث تسعى كل هذه المصالح إلى اكتشاف جميع الجرائم المرتكبة على الأجهزة الالكترونية وعبر الأنترنيت. [1]

الفرع الثاني: الإجراءات المستحدثة:

مكن المشرع هذه الهيئات بموجب القانون 06-22 من اختصاصات جديدة لم يتمتعوا بها من قبل صدور هذا القانون والمتمثلة في سلطة مراقبة الأشخاص ووجهة الأموال والأشياء واعتراض المراسلات وتسجيل الأصوات والصور والقيام بعمليات التسرب[2]، وذلك نظرا لعجز وسائل التحري والتحقيق التقليدية والكلاسيكية عن مواجهة الجرائم الحديثة وخاصة الجرائم المعلوماتية، وقد استحدث المشرع الجزائري مجموعة من الإجراءات، سنتطرق إليها على النحو الآتي:

أولا: إعراض المراسلات وتسجيل الأصوات والتقاط الصور

1- التعريف: لم يرد في القانون تعريف لهذا الإجراء، وقد عرف الفقهاء الاعتراض على أنه مراقبة وترصد المحادثات التي تتم بين الأفراد وحفظه، والعودة إليه كدليل في مرحلة الحث والتحري ضد المتهمين عند الحاجة إليه، كما أن تسجيل الأصوات هي عملية تتم أثناء التحدث الشفهي للأشخاص وذلك بتسجيل تلك المحادثات، أما التقاط الصور فهي توثيق تواجد الأشخاص فرادى أو جماعات في مكان ما دون علمهم. [3]

وقد أجازها المشرع الجزائري في الجرائم الماسة بالمعطيات بموجب المادة 65 فقرة 5 من قانون الإجراءات الجزائية، ويختص للإذن بها وكيل الجمهورية لضباط 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. [4]

---

[1]- ربيعي حسين: المرجع السابق، ص 182- 183.

[2]- صالح شنين: المرجع السابق، ص 297.

[3]- سامية بولافة ومبروك الساسي، الأساليب المستخدمة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، العدد التاسع، د س، جامعة باتنة 1، باتنة، جوان 2016، ص 396.

[4]- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري المقارن، مذكرة لنيل شهادة الماجستير زرقي رمضان، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر، 2012، 2012، ص106.

2- شروط اعتراض المراسلات وتسجيل الأصوات والتقاط الضور:

تناول المشرع الأحكام الخاصة لصحة هذا الإجراء في المواد 65 مكرر5 إلى غاية المادة 65 مكرر10[1]، ونستعرضها فيما يلي:

- يتم القيام بهذا الإجراء فقط بخصوص الجرائم التي 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 نجديده بنفس طريقة الإجراء الأول. [2]
- 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 بتهتم بالمواصلات السلكية واللاسلكية.
- يقوم الضابط المكلف بإجراء الاعتراض بتحرير محضر يتضمن تفاصيل العملية بعد الانتهاء منها، مع ذكر تاريخ بدايتها ونهايتها وساعتها.
- 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. [3]

ثانيا: عملية التسرب

نص عليه المشرع في القانون 06-22، حيث خصص له الفصل الخامس منه وعرفه في المادة 65 مكرر12 من قانون العقوبات بقولها: "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيه في ارتكابهم جناية أو جنحة بإيهامهم أنه الفاعل معهم أو شريك"، ومن ضمن الجرائم التي أجاز فيها المشرع عملية التسرب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ومن خلال هذا التعريف يتبين أن التسرب هو اندماج ضابط الشرطة مع المجرمين ومشاركتهم نشاطهم وذلك بطريقة سرية إلى غاية تحقيق النتيجة المرجوة.

ولعملية التسرب شروط شكلية وأخرى موضوعية نوجزها كما يلي:

---

[1]- أنظر المواد من 65 مكرر5 إلى غاية المادة 65 مكرر10 من قانون الإجراءات الجزائية.
[2]- رشيد بوكر، المرجع السابق، ص ص 442- 444.
[3]- إلهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، مذكرة لنيل درجة الدكتوراه فريدة مزياني قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2016، ص 313.

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 الابقاء عليه سري وحصر العلم له بين القاضي الآذن به والضابط الذي يقوم بالعملية، كذلك يجب أن يقوم العون المكلف به بتحرير تقرير مفصل على أوضاع القضية، كما تقتصر هذه العملية على ضباط وأعوان الشرطة القضائية لا غير، كل هذه الشروط نصت عليها المواد 65 مكرر11 إلى غاية 65 مكرر15 من قانون الإجراءات الجزائية. [1]

2- الشروط الموضوعية:

وتتمثل في أن يكون التسرب مسببا، بأن 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 في المادة 65 مكرر 5 [2] من نفس قانون سالف الذكر.

3- آثار التسرب:

نص عليها المشرع الجزائري في المواد 65 مكرر 14 و16 والمتمثلة فيما يلي:

- تسخير الوسائل المادية من مواد وأموال أو منتوجات أو وثائق لمجموعة المجرمين العامل معهم.
- استعمال أو صنع الوسائل ذات الطابع القانوني كالوثائق الرسمية أو المالية [3] تحت تصرف هؤلاء المجرمين.
- سقوط المسؤولية الجزائية عن الأعوان المتسربون أثناء قيامهم بالأفعال السابقة الذكر لكونها أفعال قانونية.

الفرع الثالث: إجراءات المكافحة على المستوى الدولي

من المتعارف عليه أن التعاون الدولي هو تبادل العون والمساعدة وتظافر الجهود المشتركة بين دولتين أو أكثر وذلك من أجل تحقيق خدمة مشتركة بين الدول سواء كان ذلك يحقق النفع على المستوى العالمي أو الإقليمي أو على المستوى الوطني للدول في حالة الاتفاق فيما بينهما لذلك كان من الواجب على الدول التعاون فيما بينها للحد من الجرائم

---

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

[2]- أنظر المادة 65 مكرر 5 قانون الإجراءات الجزائية.

[3]- أنظر المادة 65 مكرر 14- 16 قانون الإجراءات الجزائية

التي تقع على بطاقات الدفع الالكتروني لمكافحتها ولما كانت الجرائم المعلوماتية تتنوع بحسب تنوع الطرق والأساليب التي ارتكبت بها وجدت كذلك عدة أساليب ووسائل للتعاون الدولي في مكافحة الجرائم المعلوماتية بصفة عامة وجرائم بطاقات الدفع الالمتروني بصفة خاصة.

أولا: منظمات ومؤتمرات التعاون الدولي

تزايدت وبشكل عام منظمات مكافحة الجريمة سواء على المستوى الدولي أو الإقليمي فلم يقتصر دورها على مكافحة الجريمة بعينها بل امتدت إلى أي جريمة أخرى سواء كان ذلك جرائم بطاقات الدفع الالكتروني أو غيرها من الجرائم لذلك سنتطرق إلى هذه المنظمات وبيان أهدافها ودورها في مكافحة جرائم بطاقات الدفع الالكتروني بصفة خاصة والجرائم بصفة عامة. [1]

1- المنظمة الدولية للشرطة الجنائية (الأنتربول)

تم إعداد برنامج من أجل تصنيف جرائم بطاقات الدفع الالكتروني على مستوى العالم سنة 1999م من خلال موقع المنظمة على الشبكة الدولية وعد السماح بالدخول لقاعدة البيانات المشار إليها سوى لمسؤولي أجهزة المكافحة في الدول الأعضاء والمسؤولون عن إنتاج وتوزيع تلك البطاقات من خلال كلمة السر ونظرا لارتباط هذا النشاط بجرائم تكنولوجيا المعلومات فقد قامت المنظمة بتشكيل مجموعات عمل إقليمية أوروبية أمريكية آسياوية إفريقية تعمل على تنسيق الجهود الدولية في مواجهة هذه الجرائم[2] ومن أهداف المنظمة ما يلي:

أ- جمع المعلومات المتعلقة بالجرائم والمجرمين من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء ويتم ذلك عبر شبكة اتصالات حديثة.

ب- ضبط الهاربين والمطلوبين مهما كانت جنسياتهم وذلك بالتعاون مع الدول الأعضاء من خلال إصدار النشرات الدولية لمختلف أنواعها.

جـ - تنمية وإنشاء المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم بطاقات الدفع الالكتروني.

د- مكافحة الإجرام العابر للحدود من خلال دعم مجهود الشرطة وتقديم الخدمات في مجال الأدلة الجنائية كبصمات الأصابع والحمض النووي DNA.

[1]- عادل عبد العال ابراهيم خراشي، دور الضبطية الإدارية والقضائية في مكافحة جرائم بطاقات الائتمان الالكترونية والتعاون الدولي والأمني حيالها، د ط، دار الجامع الجديدة، مصر، 2015، ص 162.
[2]- عبد الكريم الردايدة، مرجع سابق، ص 172.

هـ - تنمية وتأمين التعاون المتبادل على أوسع نطاق بين كل سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان. [1]

كما نظمت السكريتارية العامة الخاصة بالمنظمة مؤتمرها الدولي في أكتوبر 1993م بخصوص الاحتيال والغش والنصب الذين يهددون نظام بطاقات الدفع الالكتروني حيث قام بتبني هذا المؤتمر توصيتين هامتين هما:

الأولى: مراجعة التشريعات والقوانين الخاصة ببطاقات الائتمان من طرف الدول الأعضاء بما يضمن تجريم تصنيع أو امتلاك البطاقات المزورة أو امتلاك معلومات غير قانونية واستخدامها في إدخالها في نظام بطاقات الائتمان.

الثانية: إنشاء مجموعات عمل بوليسية من خبراء الحتيالات الدولية التابعين لبوليس هون كونغ والشرطة المندية وغيرها لمكافحة هذه النوعية من الجرائم ووضع الأسس الخاصة بتبادل ونقل المعلومات للحد من هذه الجرائم. [2]

2- مشروع جولد فيش: تبنى الأنتربول الدولي مشروع جولد فيش وذلك من أجل تكثيف الجهود الدولية لمواجهة هذه الظاهرة منذ شهر يونيو 2005 بالمشاركة مع فرق عمل من عدة دول ووصل عددها حتى الآن أربع وعشرون دولة مع العلم بأنه لم ينظم لهذا المشروع حتى الآن أي من الدول العربية، وذلك بهدف تنسيق على المستوى الدولي في إجراء التحديات لمواجهة هذا النشاط وتتبع أثر الأموال المسروقة ومتحصلات هذا النشاط في الدول المختلفة. [3]

3- شبكة الاتصال الأنتربول (1- 7/24)

تفعيلا لما ورد في الفصل الثالث من معاهدة بوداباست بشأن جرائم الحاسبات المعلوماتية والاتصالات وبهدف إتاحة الفرصة الأخيرة لأجهزة المكافحة من دول العالم فقد بينت المنظمة الدولية هذا النوع من الجرائم حتى تتبادل تلك الدول المعلومات الفنية فيما بينها وتستفيد في سبيل ذلك إجراءات المواجهة. [4]

4- منظمة الاتحاد الأوروبي:

وهو جمعية دولية تضم سبعة وهشرين دولة من الدول الأوروبية تأسست بناءا على اتفاقية معروفة باسم معاهدة "ماسترخت" الموقعة سنة 1992م، وبعد التوقيع على المعاهدة بدأ التعاون الأمني الأوروبي يظهر بصورة شاملة، وقد اتخذ الاتحاد

---

[1]- عادل عبد العال ابراهيم خراشي، المرجع السابق، ص ص 127- 128.
[2]- المرجع نفسه، ص ص 128- 129.
[3]- عبد الكريم الردايدة، المرجع السابق، ص 173.
[4]- المرجع نفسه، ص ص 172- 173.

الأوروبي مجموعة من الإجراءات في مجال مكافحة الجريمة المنظمة، أمهما: إنشاء وحدة المخابرات الأوروبية داخل الهيكل التنظيمي للاتحاد الأوروبي، وقرها لاهاي وكانت مهامها الأولية تبادل المعلومات بين وكالات تشريع القانون في مجال المخدرات وغسل الأموال، وتبادل المعلومات في مجال الأنشطة الإجرامية المنظمة التي تمتد آثارها إلى دولتين فأكثر، ويدخل الاتجار غير المشروع في المواد المشعة، والاتجار في نطاق هذه الوحدة.

وفي ضوء تأكيد الاتحاد الأوروبي على أهمية التعاون الدولي في مكافحة الجريمة حيث أبرمت الدول الأعضاء في الاتحاد عددا من الاتفاقيات، وكما تم إبرام معاهداة الاتحاد الأوروبي حول المساعدة المتبادلة في المساءل الجنائية بغرض تسهيل الحصول على الدليل من البلدان الأخرى وتطور التحقيقات عبد الحدود.

وبخصوص جرائم بطاقات الدفع الالكتروني فقد أولى الاتحاد الأوروبي المعاملات المالية عناية بالغة، ويعود هذا الاهتمام إلى المجموعة الاقتصادية الأوروبية، التي سعت إلى ضرورة حماية الدفع الالكتروني، ويظهر ذلك من خلال التوصية رقم 598/87 التي وضعتها اللجنة الأوروبية حول القانون الأوروبي للسيرة الحسنة الخاصة بالدفع الالكتروني، وتدعوا هذه التوصية كافة المتعاملين للمثول لهذا القانون من أجل ترقية الحماية والضمان للمستهلكين، والحماية المتواصلة بيم مقدمي الخدمات ومصدر هذا النوع من وسائل الدفع.

كما حرص على التزام المستهلك أو حماية البطاقة على ضرورة الأخذ بالعناية اللازمة عند استعمال بطاقة الدفع. [1]

4- التحالف العالمي لمكافحة جرائم الاحتيال عبر شبكة الانترنيت.

تعرض الآلاف من الضحايا للاحتيال عبر شبكة الأنترنيت باستخدام بطاقات الائتمان لمخاطر كبيرة ولمواجهة هذا الخطر، تكاتف الكثير من مسؤولي المواقع الالكترونية، حيث تم تشكيل تحالف عالمي يضم ما يزيد على 1600 من الشركات التجارية والمؤسسات المالية، وكذلك المنظمات المسؤولة عن بطاقات الدفع الالكتروني، ومجموعة كبيرة من البنوك وشركات تكنولوجيا المعلومات، وذلك بهدف استقطاب المعلومات الفنية حول المواقع والمصادر المتورطة في عمليات احتيال، إلى قاعدة بيانات تدعى شبكة تقارير الاحتيال، مما يتيح لجميع الأطراف المعنية إمكانية الاطلاع على أسماء تلك المواقع، لإدراجها في مختلف البرمجيات وخدمات التصفح، لحماية المستخدمين من أية عملية احتيال عبر الانترنيت.

[1]- عبد الكريم الردايدة، المرجع السابق، ص من130 إلى 132.

ثانيا: المؤتمرات الدولية

للمؤتمرات الدولية دور كبير في إتاحة الفرصةلتبادل الخبرات وتنسيق الجهود بين أجهزة المكافحة، حيث أوكل لقسم مكافحة جرائم التكنولوجيا عالية التقنية بمنظمة الأنتربول مهمة الإعداد لعقد مؤتمرات دورية مرة كل عامين في المجال، حيث كان آخرها المؤتمر الدولي الخامس للإجرام السيبري الذي عقد في القاهرة سنة 2015م، كما كان لقسم الأخطار بمنظمتي الفيزا الماستر كارد العالمية إعداد وعقد مؤتمرات دورية سنوية، حيث يشارك فيها المختصون من أجهزة المكافحة في العديد من دول العالم، وكذلك مسؤولي الإخطار بمراكز البطاقاتبالمؤسسات المالية والمصرفية، بهدف الحد من تأثير هذا النوع من الجرائم على الأنشطة المالية والمصرفية. [1]

ثالثا: اتفاقيات التعاون الدولي

نظمت السكرتارية العامة أولى مؤتمراتها الدولية بخصوص الاحتيال والغش في البطاقة الائتمانية في عام 1994 وتمخض عن هذا المؤتمر المؤتمر توصيتين هما:

1- يجب على الدول الأعضاء مراجعة تشريعاتها وقوانينها الخاصة ببطاقات الائتمان بما يتضمن كل فعل يتضمن تصنيع وامتلاك أي معلومات غير قانونية تم الحصول عليها بطريقة غير مشروعة أو تم استخدامها في نظام بطاقات الائتمان.

2- إنشاء مجموعات عمل بوليسية من خبراء متابعة جرائم الغش والاحتيال على المستوى الدولي التابعين لبوليس (هونك كونغ والشرطة الكندية والخدمة السرية الأمريكية وخدمة الاستخبارات القومية الجنائية ومندوبين من منظمات الائتمان).

[1]- عبد الكريم الردايدة، المرجع السابق، ص ص 173- 174.

خلاصة الفصل

نلخص من خلال ما تقدم بيانه وتوضيحه في هذا الفصل بأن هناك مجموعة من الإجراءات المتخذة في مواجهة الاعتداءات الواقعة على بطاقات الدفع الالكتروني سواءا كانت إجراءات وقائية تتخذ قبل وقوع الجريمة، بحيث تهدف إلى الإطاحة بدوافع ارتكاب هذه الجرائم ومعالجتها، أو كانت إجراءات ردعية قانونية تتم بعد وقوع الجريمة بداية بمباشرة الدعوى وصولا إلى المحاكمة وردع الجاني، ونظرا لخصوصية هذه الجرائم وصعوبة الكشف عنها والتصدي لها فقد استحدث المشرع الجزائري بعض القوانين التي تتماشى مع التطور السريع الذي تشهده الجرائم الالكترونية، فالجزائر وفي الآونة الأخيرة ساهمت في تعزيز الجهود الدولية الرامية للحد من هذه الجرائم.

خاتمة

خاتمة

من خلال ما تقدم بيانه وتوضيحه وتأسيسا على ما سبق يتجلى لنا أن موضوع الجرائم الواقعة على بطاقات الدفع الالكتروني يتميز بخصوصيته كآلية مستحدثة في التعاملات المالية بوجه عام ويدخل ضمن الجرائم المعلوماتية ويصنف ضمن نطاق الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مما يعني عدم إمكانية تطبيق أحكام الجرائم التقليدية عليه كونها جرائم إلكترونية يقوم بها مجرم إلكتروني صعب الاكتشاف ولا تبدو عله ملامح الإجرام فهو يستغل ذكاءه وخبرته لارتكاب مثل هذه الجرائم مما دفع بأغلب التشريعات إلى محاولة وضع تشريع خاص ببطاقات الدفع الالكتروني ولمواجهة هذه الجرائم فالجزائر من بين هذه الدول التي تتعامل اليوم وبكثرة بهذه البطاقات، حيث قام المشرع الجزائري بتعديل بعض القوانين مثل ما هو الحال بالنسبة للقانون 04-15 والذي عدل القانون 66-156 المتضمن قانون العقوبات في القسم السابع منه تحت عنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ليصدر بعدها القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال. وبموجب هذه القوانين تم تبني إجراءات جديدة تواكب التطور التقني الحاصل ومع ذلك لا يزال المشرع الجزائري بعيدا عن مستوى التشريعا العالمية في هذا المجال ولقد تبينت لنا مجموعة من النتائج التي توصلنا إليها ونتبعها ببعض الاقتراحات والتوصيات كمحاولة لاستدراك ما وقع فيه المشرع.

النتائج:

1. أن بطاقات الدفع الالكتروني أداة للوفاء ظهرت كوسيلة بديلة للنقود وتتخذ شكلا معينا يميزها عن غيرها من البطاقات قد تكون محلية أو دولية.
2. إن عدم إقبال كثير من الأفراد عن استخدام هذه الوسيلة مرده الخوف من فكرة أنها ليست محمية بالقدر الكافي.
3. تعد مشكلة حماية بطاقات الدفع الالكتروني من أخطر المشكلات التي يواجهها النظام الاقتصادي الداخلي والدولي.
4. أن الجرائم التي ترد على بطاقات الدفع الالكتروني المتنوعة فهي إما سرقة أو تزوير أو خيانة للأمانة.
5. المشرع الجزائري أبدى إهتمامه ببطاقات الدفع الالكتروني من خلال استحداث قوانين جديدة ومثال ذلك القانون 09-04 غير أنه أغفل تنظيمها المفصل ولم يتطرق إلى حمايتها الجزائية بشكل خاص.
6. وسّع المشرع الجزائري بموجب القانون 09-04 الاختصاص الإقليمي للجهات القضائية في متابعة الجرائم الماسة بالمصالح الحساسة للدولة كإجراء ردعي عن طريق الوسائل القانونية المستحدثة نظرا لطبيعتها العابرة للحدود.

7. فرض المشرع الجزائري عقوبات على هذه الجرائم الماسة بالمعطيات وجعل لها حد أدنى وحد أقصى لكنه نص على تشديد العقوبة كلما كانت هذه الجرائم الماسة بأمن الدولة كالدفاع الوطني أو المؤسسات الخاضعة للقانون العام.
8. الجزائر وعلى غرار بقية الدول حاولة جاهدة التنسيق والتعاون في إطار تظافر الجهود بين الدول لمكافحة هذه الجرائم والحد منها وذلك بالمصادقة على مختلف الاتفاقيات والمشاركة في بعض المؤتمرات.

الاقتراحات والتوصيات

بناءا على ما تم التوصل إليه من نتائج توصي هذه الدراسة بما يلي:

1. نأمل بأن يدمج المشرع الجزائري نصوص جرائم نظام جرائم المعلومات في قانون العقوبات الوطني وسن نصوص صريحة خاصة ببطاقات الدفع الالكتروني لا الاعتماد على القواعد العامة في التجريم.
2. نأمل بأن يقوم المشرع بالتحديث الدائم لهذه القوانين حتى تواكب كل التطورات الخاصة بهذه الجرائم.
3. تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وذلك بتوفير أحدث الوسائل والتجهيزات التقنية وفريق من الخبراء والمؤهلين لضمان تحقيق نتائج مرجوة.
4. إجراء حملات تحسيسية توعوية تتضمن المخاطر المترتبة عن جرائم بطاقات الدفع الالكتروني لفائدة شرائح المجتمع والتأكيد على ضرورة إنشاء دائرة خاصة في البنك تهتم بالرقابة على البطاقة البنكية.
5. تعزيز التعاون الدولي في إطار تظافر الجهود ودعوة الجزائر للانضمام إلى الاتفاقيات والمعاهدات أخرى التي تسعى جليا لمكافحة مثل هذه الجرائم

قائمة
المصادر والمراجع

I. القرآن الكريم

II. القوانين والمراسيم:

أولا: القوانين

1. القانون 04-14 المؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18صفر عام 1386هـ الموافق 08يونيو 1966. والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71، السنة 41، الصادرة بتاريخ 10 نوفمبر سنة 2004.
2. القانون 06-01 المؤرخ في 21 محرم 1427 هـ، الموافق لـ 20 فبراير2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، عدد14،السنة 43، الصادرية بتاريخ 8مارس2006.
3. القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، السنة 43، الصادرة بتاريخ 24ديسمبر سنة 2006.
4. بالقانون 09-04 المؤرخ في 5 أوت 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، عدد47، السنة 46، الصادرة بتاريخ 16 غشت سنة 2009.

ثانيا: المراسيم

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

2. المرسوم التشريعي رقم 93-10 المؤرخ في 2 ذي الحجة عام 1413، الموافق لـ 23 مايو سنة 1993، يتعلق بورصة القيم المنقولة، الجريدة الرسمية الجزائرية الديمقراطية الشعبية، العدد 34، السنة30، الصادرة بتاريخ 30 مايو 1993.

III. الكتب

1- الكتب العامة

1. - أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، الطبعة الثالثة، الديوان الوطني للأشغال التربوية، الجزائر، 2001.
2. أحمد أبو الروس، قانون جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية، الموسوعة الجنائية الحديثة، المجلد الخامس، المكتب الجامعي الحديث، الاسكندرية، 1997.

3. أسامة حمدان الرقي، جرائم الاحتيال (الأساليب- المظاهر- العلاج)، الطبعة الأولى، دار ياف العلمية للنشر والتوزيع، عمان، 2012.
4. أحمد شكري السباعي، الوسيط في الأوراق، الجزء الثاني في آليات وأدوات الوفاء والشيك، الطبعة الأولى، دار نشر المعرفة، مطبعة المعارف الجديدة، الرباط، المملكة المغربية، 1998.
5. بيار إميل طوبيا، بطاقة الاعتماد والعلاقات التعاقدية المبثقة عنها، د ط، منشورات الحلبي الحقوقية، بيروت، 2000.

6. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، الطبعة الأولة، دار البداية للنشر والتوزيع، عمان، 2010.
7. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، الطبعة الأولى، دار النهضة العربية، 2003، القاهرة.

8. حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، د ط، دار الكتب القانونية، مصر، 2013.
9. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.
10. عبد العزيز سعد، جرائم الاعتداء على الأموال العامة والخاصة، الطبعة الرابعة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007.

11. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الطبعة الأولى، دار الفكر العربي، الاسكندرية، 2002.
12. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والحاسب الآلي في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2002.
13. عبد الحكيم عثمان، أحكام البطاقات الائتمانية في القانون والآراء الفقهية الاسلامية، الطبعة الأولى، شركة الجلال للطباعة، العامرية، بغداد، 2007.
14. عبد الكريم الردايدية، جرائم بطاقات الائتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013.
15. عبد الوهاب إبراهيم سليمان، البطاقات البنكية، دراسة فقهية اقتصادية تحليلية، الطبعة، الثانية، دار القلم للنشر والتوزيع، دمشق سوريا، 1998.

16. علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الإئتمان الإلكترونية (دراسة مقارنة)، الطبعة الأول، المؤسسة الحديثة للكتاب، لبنان، 2011.
17. فايز نعيم رضوان، بطاقة الوفاء، دار النهضة العربية، القاهرة، جمهورية مصر العربية، 1999.

18. فتحي محمد أنورغزت، جرائم العصر الحديث، الطبعة الأولى، دار الفكر والقانون، القاهرة، 2010.
19. لامية مجدوب، جريمة التزوير في المحررات الرسمية أو المعلومية في التشريع الجزائري، د ط، دار الجامعة الجديدة، الجزائر.
20. لبنى عمر سقاوي، المسؤولية المصرفية في الاعتماد المالي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006.
21. - لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2015.
22. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2006.
23. محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004.
24. محمد عبد الله الرشدان، جرائم غسيل الأموال، الطبعة الأولى، دار قنديل للنشر والتوزيع، عمان، 2007.
25. محمد فتحي عيد، الإجرام المعاصر، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2014.
26. محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2014.
27. محمد توفيق سعودي، بطاقات الائتمان والأسس القانونية الناشئة في استخدامها، الطبعة الأولى، دار النهضة للطباعة والنشر، القاهرة، مصر، 2001.
28. نضال سليم برهم، أحكام عقود التجارة الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2010.

2- الكتب المتخصصة:

1. أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقة الدفع الإلكتروني، الطبعة الأولى، دار المسيرة للنشر والتوزيع والطباعة، 2010.
2. أمين طالب البغدادي، الاستخدام الغير مشروع لبطاقة الائتمات المسؤولية الجزائية والمدنية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.
3. حسين محمد الشبلي، محمد مهند الدويكات فايز، التزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولى، دار مجدلاوي للنشر والتوزيع، عمان 2009.
4. عبد الكريم الردايدية، جرائم بطاقات الائتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013.
5. علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الإئتمان الإلكترونية (دراسة مقارنة)، الطبعة الأول، المؤسسة الحديثة للكتاب، لبنان، 2011.

6. - عماد علي خليل، الحماية الجزائية لبطاقات الوفاء، الطبعة الأولى، دار وائل للطباعة والنشر، عمان، 2000.
7. سامح محمد عبد الحكيم، الحماية الجنائية لبطاقات الإئتمان، جرائم بطاقة الدفع الإلكتروني، دار النهضة العربية، جمهورية مصر العربية، 2003.
8. وسام فيصل محمود الشواورة، المسؤولية القانونية عن الاستخدام غير المشروع لبطاقات الائتمان، الطبعة الأولى، دار وائل للنشر، عمان، 2013.

IV. الرسائل والمذكرات الجامعية:

أولا: أطرواحات دكتوراه:

1. بن شهرة شول، الحماية الجنائية للتجارة الإلكترونية، مذكرة مقدمة لنيل درجة دكتوراه في القانون، علي أجقو، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2010، ص 22.
2. صالح شنين، الحماية الجنائية للتجارة الالكترونية – دراسة مقارنة- ، رسالة لنيل شهادة الدكتوراه في القانون الخاص محمد رايس، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2013.
1. إلهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، مذكرة لنيل درجة الدكتوراه فريدة مزياني قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2016.
2. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، رحاب شادية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2016.
3. مجراب الداودي، الأسباب الخاصة بالبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه كلية الحقوق، جامعة يوسف بن خدة، الجزائر، 2016.

ثانيا: رسائل الماجستير

1. خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، مذكرة مكملة لنيل شهادة الماجستير في الجقوق، بن صغير محفوظ، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016.
2. سلطان محمد شاكر، ضمانات المتهم أثناء مرحلة التحريات الأولية والتحقيق الابتدائي، مذكرة لنيل شهادة الماجستير في القانون، مباركي دليلة، قسم الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

3. صراع كريمة، واقع وأفاق التجارة الالكترونية في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم التجارية، كربالي بغداد، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، 2014.
4. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري المقارن، مذكرة لنيل شهادة الماجستير زرقي رمضان، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، 2012.

V. المقالات

أ- المقالات العامة:

1. محمد لموسخ، تنازع الاختصاص في الجرائم الالكترونية، مجلة الحقيقة، العدد 28، المطبعة العربية، غرداية، 2014.
2. نهى خالد عيسى، ماهية بطاقات الائتمان والآثار القانونية المترتبة عن استخدامها، مجلة المحقق الحلبي للعلوم القانونية والسياسة، العدد الثاني، السنة السابعة، 2015.
3. سامية بولافة ومبروك الساسي، الأساليب المستخدمة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، العدد التاسع، جامعة باتنة 1، باتنة، جوان 2016.

ب- المقالات المتخصصة:

1. عبد الجبار الحنيص، الاستخدام غير المشروع لبطاقة الائتمان الممغنطة في وجهة نظر القانون الجزائي، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010.

VI. الملتقيات العلمية:

1. محمدي بوزينة أمينة، مداخلة علمية بعنوان: إجراءات مكافحة الجرائم المعلوماتية، ملتقى آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.

VII. المواقع الالكترونية:

1. بطاقات الدفع والسحب الالي في الجزائر مقال
http : « forum.univbiskra.net/ index منشور علي شبكة الانترنت علي الموقع www.djelfa:inf/vb/showthrea.php=145341 تاريخ الزيارة 2019.04.18 علي الساعة 09.30.

فهرس الموضوعات

فهرس الموضوعات

الرقم	العنوان	الصفحة
01	**إهداء**	
02	**شكر وعرفان**	
03	**المقدمة**	أ- د
04	**الفصل الأول: الحماية الجنائية الموضوعية ليطاقات الدفع الالكتروني**	
05	**المبحث الأول: إساءة استعمال بطاقة الدفع الإلكتروني من طرف صاحبها.**	07
06	**المطلب الأول:** ماهية بطاقات الدفع الالكتروني	07
07	الفرع الأول: تعريف بطاقات الدفع الالكتروني	07
08	الفرع الثاني: أنواع بطاقات الدفع الالكتروني	09
09	الفرع الثالث: خصائص ومزايا بطاقات الدفع الإلكتروني	11
10	**المطلب الثاني:** الاستخدام غير الشرعي للبطاقة أثناء فترة صلاحيتها.	13
11	الفرع الأول: الحصول على بطاقة الدفع بمستندات مزورة	15
12	الفرع الثاني: الاستخدام غير الشرعي للبطاقة في عملية السحب والوفاء.	15
13	**المطلب الثالث:** الاستخدام غير الشرعي للبطاقة خارج فترة صلاحيتها	18
14	الفرع الأول: الاستخدام غير مشروع للبطاقة	19
15	الفرع الثاني: الاستخدام المقنع للبطاقة	22
16	**المبحث الثاني:الاستخدام غير المشروع لبطاقة الدفع الالكتروني من قبل التاجر والمصدر**	23
17	**المطلب الأول:** الاستخدام غيرالمشروع للبطاقة من قبل المصدر والتاجر.	23
18	الفرع الأول: طرق التلاعب في بطاقة الدفع الإلكتروني التي يمارسها موظفوا المصدر	23
19	الفرع الثاني: طرق التلاعب في بطاقة الدفع الإلكتروني التي تمارس من التاجر	24
20	الفرع الثالث: مسؤولية موظفوا البنك والتجار عن عدم مشروعية أعمالهم	26
21	**المطلب الثاني:** الاستخدام غير المشروع للبطاقة من طرف الغير	30
22	الفرع الأول: جريمة التزوير واستعمال المزور	30
23	الفرع الثاني.جريمة سرقة بطاقة دفع أو رقمها السري	35
24	الفرع الثالث: جريمة استعمال بطاقة دفع مفقودة	38
25	**خلاصة الفصل**	41

26	**الفصل الثاني: الحماية الجنائية الإجرائية لبطاقات الدفع الالكتروني**	
27	**المبحث الأول : الإجراءات الوقائية لمواجهة الاعتداء الواقعة على بطاقات الدفع الالكتروني.**	43
28	**المطلب الأول:** دور الهيئات الدولية والبنوك في حماية بطاقة الدفع الالكتروني	43
29	الفرع الأول: الإجراءات الوقائية المتخذة من طرف الهيئات الدولية	43
30	الفرع الثاني: الإجراءات الوقائية المتخذة من من البنوك	46
31	**المطلب الثاني:** الإجراءات المتخذة من قبل حامل البطاقة والتاجر ومختلف الأجهزة	52
32	الفرع الأول : الإجراءات المتخذة من قبل حامل البطاقة	52
33	الفرع الثاني: الإجراءات المتخذة من قبل التاجر	54
34	الفرع الثالث: الإجراءات الوقائية المتخذة من طرف بعض الأجهزة	56
35	**المبحث الثاني: الإجراءات الردعية لمواجهة الاعتداء الواقعة على بطاقات الدفع الالكتروني.**	57
36	**المطلب الأول:** الإجراءات الكلاسيكية أو المعتادة في الجرائم المستحدثة	58
37	الفرع الأول : مرحلة البحث والتحري	58
38	الفرع الثاني: مرحلة التحقيق	68
39	الفرع الثالث: مرحلة المحاكمة	68
40	**المطلب الثاني:** الإجراءات الخاصة أو المستحدثة	70
41	الفرع الأول: التطور التشريعي	70
42	الفرع الثاني: الإجراءات المستحدثة	72
43	الفرع الثالث: إجراءات المكافحة على المستوى الدولي	74
44	**خلاصة الفصل**	79
45	**خاتمة**	81
46	**قائمة المصادر والمراجع**	84
47	**فهرس الموضوعات**	90
48	**ملخص الدراسة**	/

ملخص الدراسة

I. ملخص الدراسة باللغة العربية

إن وسيلة الدفع هي الوسيلة المتفق عليها في جميع المعاملات التجارية، ولقد تنوعت واختلفت باختلاف الجهات المصدرت لها التي ساهمت في تسهيل المعاملات المالية والمصرفية وهي كأداة سحب للنقود وأداة وفاء والائتمان ظهرت نتيجة التطور التكنولوجي خاصة بظهور شبكة الانترنيت، بحيث أصبحت المؤسسات المصريفية تعتمد على هذه الأخيرة إلا أن هذا التطور أدى إلى ظهور استخدامات غير شرعية لهذه البطاقة من خلال عمليات التزوير والسرقة والنصب والاحتيال سواء كانت هذه الأخيرة من طرف حاملها أو الجهات المصدرة لها أو الغير، مما يستوجب ذلك حماية جزائية إجرائية لها لدفع الأخطار الواقعة على هذه البطاقات وذلك على المستويين الوطني والدولي والجزائر وعلى غرار الدول الأخرى وفي إطار تظافر الجهود تسعى إلى حماية الأموال من كل الانتهاكات في ظل غياب تشريع خاص لهذه البطاقات، وذلك بإصدار المشرع الجزائري القانون 04-09 المتضمن الوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال

II. Résumé en français

Les moyens de paiement sont les moyens convenus dans toutes les transactions commerciales: ils varient et diffèrent selon les émetteurs, ce qui contribue à faciliter les transactions financières et bancaires, ils constituent un outil de retrait d'argent et un outil de paiement, ce qui résulte du développement technologique, notamment de l'émergence de l'Internet. Toutefois, cette évolution a conduit à l'émergence d'utilisations illégales de cette carte par le biais de la fraude, du vol, de la fraude et de la fraude, qu'elles soient de celle-ci par le titulaire ou par les émetteurs ou des tiers, ce qui impose la protection de la sanction procédurale au paiement des risques. L'incident sur ces cartes aux niveaux national et international, l'Algérie, à l'instar d'autres pays et dans le cadre des efforts concertés cherchent à protéger les fonds de toutes les violations en l'absence d'une législation spéciale pour ces cartes, l'émission législateur algérien 04-09 loi contenant la prévention des infractions liées aux technologies de l'information et de la communication