الجمهورية الجزائرية الديمقراطية الشعبية
Peoples democratic republic of Alegria
وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي– برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص : قانون إعلام آلي والأنترنت

الموسومة بـ:

الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير

إعداد الطالبتين:

- **مروى بن بوزيد**
- **نجوى هداج**

نوقشت وأجيزت يوم: 12 جوان 2025

أمام لجنة المناقشة:

عبد الحفيظ بكيس	أستاذ محاضر قسم أ	رئيسا
عيسى بوقرة	أستاذ مساعد قسم ب	مشرفا ومقررا
مريم بلقسام	أستاذ محاضر قسم أ	ممتحنا

السنة الجامعية: 2025/2024

ملحق بالقرار رقم .....1082..... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

موسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

انا الممضي أسفله.

السيد(ة) بن بوزيد هروى الصفة: طالب. أستاذ. باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 100451946 والصادرة بتاريخ 2016-04-09.

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).

عنوانها: الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير.

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في انجاز البحث المذكور أعلاه .

التاريخ: .....

شوهد قبل التصديق

السيد: [illegible]

بطاقة التعريف الوطنية رقم: [illegible]

مستخرجة بتاريخ [illegible]

رئيس المجلس الشعبي البلدي وبتفويض منه

رئيس مكتب الحالة المدنية

حروز زهير

توقيع المعني (ة)

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 2020 ديسمبر 27

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

موسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

انا الممضي أسفله،

السيد(ة): هداج نجوى ..... الصفة: طالب، أستاذ، باحث طالبة .....

الحامل(ة) لبطاقة التعريف الوطنية رقم 112600122 والصادرة بتاريخ 2024-08-30 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: .....

شوهد قصد التصديق
السيد: هداج نجوى
بطاقة التعريف الوطنية رقم: 112600122
سلمت في: 30-08-2024
الحضور في: 2024

توقيع المعني (ة)

عن رئيس المجلس الشعبي البلدي
رئيس مكتب التنظيم العام
بن عمر مصطفى

شكـــر وعرفـــان

الحمد لله حمدا كثيرا حتى يبلغ منتهاه، والصلاة والسلام على أشرف المخلوق أناره الله بنوره واصطفاه.

وانطلاقا من لم يشكر الناس لم يشكر الله نتقدم بكل الشكر والتقدير للأستاذ المشرف **عيسى بوقرة** على استشاراته وتوجيهاته التي لم يبخل علينا بها.

كما لا يفوتنا في هذا المقام أن نتقدم بالشكر إلى أعضاء اللجنة المكلفة بالمناقشة، وكذلك الشكر والتقدير إلى كل أساتذة كلية الحقوق والعلوم السياسية والطاقم الإداري القائم عليها.

كما نتقدم بكل الشكر لكل يد ساهمت معنا من قريب أو بعيد في إنجاز هذا البحث.

إهـــــداء

إلى كل من كلّل العرق جبينه ومن علمني أن النجاح لا يأتي إلا بالصبر والإصرار، إلى النور الذي أنار دربي والسراج الذي لا ينطفئ نوره أبدًا، من بذل الغالي والنفيس واستمديت قوتي واعتزازي بذاتي.

"أبي الغالي".

إلى من جعل الجنة تحت أقدامها وسهلت لي شدائد بدعائها، إلى الإنسانة العظيمة التي لطالما تمنت أن تقر عينها في يوم كهذا.

"أمي الحبيبة".

إلى من شددت عضدي بها فكانت ينبوع أرتوي منه إلى حبيبتي أختي الغالية "منار".

إلى سبب سعادتي وسكر دنيتي إخوتي "سامي، يعقوب، إسحاق".

وإلى زوجي سندي وابنتي قرة عيني "رهف".

لكم من ساندني وكان عونا لي في هذا الطريق إليكم عائلتي صغيرا وكبيرا.

أهديكم هذا الإنجاز وثمرة نجاحي الذي طالما تمنيته.

ها أنا اليوم أكملت أول ثمراته بفضله سبحانه وتعالى.

فالحمد لله على ما وهبني شكرا وحبًا وامتنانًا على البدئ والختام.

وآخر دعوانا أنّ الحمد لله ربّ العالمين.

مـــروى

إهـــــداء

"وآخر دعواهم أن الحمد لله رب العالمين".

أولا الحمد لله الذي بلغني شرف هذا العلم وأعانني على إكماله،

والذي أدين به إلى من قال فيهما: وقضى ربك ألا تعبدوا إلا إياه

وبالوالدين إحسانا".

أهدي هذا العمل المتواضع إلى كل أفراد عائلتي الكريمة التي كانت

خير رفيق في درب العلم.

إلى كل الأشخاص الذين أحمل لهم المحبة والتقدير.

إلى من رافقوني في مسيرتي العلمية.

إلى نفسي التي كافحت واجتهدت وصبرت فأنت تستحقين.

لكم جميعا أهدي هذا العمل فهو ثمرة دعائكم.

نجوى

قائمة المختصرات:

ق.إ.م.إ: قانون الاجراءات المدنية والإدارية

مج: مجلد

د.س.ن: دون سنة نشر

ط: طبعة.

ص: الصفحة.

ص.ص: الصفحة إلى الصفحة.

مقدمة

مقدمة:

أفرزت الثورة الرقمية التي يشهدها العالم اليوم تحولات جذرية في شتى المجالات لا سيما في القطاع المالي، والذي طور في وسائل الدفع والاعتماد على الطريقة الالكترونية منها كبديل عن وسائل الدفع التقليدية، حيث ظهرت بطاقات الدفع الالكتروني الذي بات الاعتماد عليها أمر لا غنى عنه في إنجاز المعاملات المالية، فهي تعتبر وسيلة فعالة لأنها أصبحت محلا للنقود الحقيقة في المعاملات اليومية بين أفراد المجتمع لتصبح أســـاس العمل، وهو ما جعلها تحتل مكانة هامة وبارزة في الحياة الاقتصادية.

إلا أن هذا التقدم التكنولوجي الذي خلفته الثورة الرقمية رافقه ظهور أنماط جديدة من الجرائم الالكترونية، وفي مقدمتها جريمة تزوير بطاقات الدفع الالكتروني التي تهدد الثقة العامة لأنظمة الدفع الحديثة، حيث يعد التزوير في بطاقات الدفع الالكتروني من الجرائم المعقدة التي تجمع بين وسائل التقنية الحديثة والأساليب الاحتيالية، مما يجعل مواجهتها تحديا حقيقيا أمام المنظومة القانونية.

ولا يخفى ما يمثله التزوير من تهديد لحامل البطاقة، وللاقتصاد المحلي والدولي ولا سيما أن هذه البطاقات تعتمد في طرق التعامل بها على النظام، وبذلك أصبحت بطاقات الدفع الالكتروني في وضع متقدم بين وسائل الدفع المختلفة التي تجرى بها المعاملة التجارية في كثير من الدول، ونتيجة للإقبال المتزايد على تلك البطاقات من قبل المتعاملين بها كانت الحاجة ماسة إلى حمايتها من التزوير والتلاعب عن طريق إفراد حماية جنائية خاصة لها يستطاع من خلالها فرض عقوبات على كل شخص يرتكب فعل تزوير يترتب عليه في حق ضرر بالآخرين.

ولذلك أدركت أغلب التشريعات خطورة هذه الظاهرة فسعت إلى توفير حماية جنائية فعالة لها من خلال تجريم الأفعال الماسة بسلامة البطاقات، ومواجهة الاعتداءات الواقعة عليها بتوفير ما يلزم لحمايتها لضمان استقرار المعاملات المالية الالكترونية.

أهمية الدراسة: تتجلى أهمية هذه الدراسة في:

- مواكبة التطور الرقمي الذي يشهده العالم خاصة في مجال الخدمات المالية الالكترونية.

- تبيان مدى خطورة جرائم تزوير بطاقات الدفع الالكتروني لكونها تتم بوسائل تقنية دقيقة يصعب اكتشافها، والمساهمة في توعية مستخدميها.
- كذلك تظهر أهمية الموضوع بأنه موضوع يتسم بالحداثة والمعاصرة، حيث أننا نسلط الضوء على واحدة من أهم جرائم هذا العصر في مجال المعاملات المصرفية الالكترونية التي تتم بطريقة تقنية غير تلك الطريقة التقليدية المعتمدة وهي في تزايد.

أسباب اختيار الموضوع: هناك أسباب ذاتية وأخرى موضوعية:

أسباب ذاتية: تتمثل في:

- الرغبة الذاتية للبحث في مجال المعلوماتي، والاطلاع على المواضيع الحديثة.
- الميول إلى التعرف على نظام الدفع الالكتروني.
- التطلع فيما هو جديد حول مستجدات العصر الحديث.

أسباب موضوعية: تتمثل في:

- إن خطورة هذه الجرائم وسرعة انتشارها كان السبب في اختيارنا لهذا الموضوع خاصة أن هذه الجرائم ترتكب من قبل عصابات متخصصة في هذا المجال.
- أصبح التعامل ببطاقات الدفع الالكتروني أكثر انتشارا في مجال المصرفي، مما يجعلها أكثر عرضة للاستغلال والتزوير.

أهداف الدراسة: تهدف هذه الدراسة إلى:

- بيان مفهوم بطاقات الدفع الالكتروني وذكر أنواعها.
- تحديد مفهوم التزوير الالكتروني.
- بيان دور الأجهزة التشريعية والأمنية في الوقاية من هذه الجرائم ومكافحتها.
- تسليط الضوء على دور التعاون الدولي في مكافحة هذه الجرائم.

الإشكالية:

كما تعد جريمة تزوير بطاقات الدفع الالكتروني والتلاعب بها من الجرائم الحديثة التي لم يكن لها ظهور من قبل، إذ ارتبط وجودها بتطور تكنولوجيا المعلومات الحاسبات، كما أدى انتشارها والتعامل بها في كثير من الدول إلى مساعدة الجناة للاستعلاء

عليها لهدف تحقيق أرباح غير مشروعة، ما له الأثر البالغ في تهديد الأطراف المتعاملين بها، وتعريضهم لأنواع كثيرة من الجرائم، وما تؤديه من أخطار على مصالح المجتمع والاقتصاد.

ومن خلال ما تم التطرق إليه تثار الإشكالية المحورية التالية:

- **هل كفلت القوانين والتشريعات الحماية اللازمة لمستعملي بطاقات الدفع الإلكتروني من جريمة التزوير في ظل التطور السريع للمعاملات المالية بين الأفراد والتزاماتهم؟**

وتنطوي تحت هذه الإشكالية مجموعة من التساؤلات الفرعية والمتمثلة في:

- ما المقصود بالتزوير الالكتروني؟ وما هو الأساس القانوني لحماية بطاقة الدفع الالكتروني منه؟
- ما هي إجراءات المتخذة في مواجهة هذه الجريمة؟

منهج الدراسة:

تتركز دراستنا حول **المنهج الوصفي** معتمدين على نصوص وتشريعات وقوانين مكافحة جرائم تقنية المعلومات، وقانون العقوبات في التشريعات المقارنة وبيان موقفها من تلك الجريمة المستحدثة، كما اعتمدت دراستنا على **المنهج التحليلي** لتحليل آراء الفقهاء وبيان موقفهم من مدى اعتبار البطاقة محررا وأيضا موقفهم من الشريط الممغنط الموجود في ظهر البطاقة، وهل التغيير الذي يناله يعد تزويرا.

صعوبات الدراسة:

مما لا شك أن كل بحث تعتريه بعض الصعوبات والعراقيل ولعل الصعوبات التي واجهتنا في إعداد هذا البحث هي:

- قلة المراجع المتخصصة في الجانب الاجرائي لجريمة التزوير الالكتروني.

- صعوبة الالمام بجميع الجوانب الفنية المتعلقة بأنظمة الدفع الالكتروني وطابعها المتطور والمتغير.
- قصور التشريعات التقليدية مما يجعلها لا تواكب تطور الجرائم الالكترونية، لأن بعض النصوص قد تكون عامة جدا غير كافية لتجريم أفعال التزوير الحديثة في بطاقة الدفع الالكتروني.

هيكل الدراسة:

للإجابة على إشكالية البحث قمنا بتقسيم بحثنا إلى فصلين تناولنا في الفصل الأول الإطار المعرفي لبطاقات الدفع الالكتروني والذي يحتوي على ثلاث مباحث، الأول تطرقنا فيه إلى مختلف المفاهيم المتعلقة ببطاقات الدفع الالكتروني مع استعراض مختلف أنواعهـــا، أما المبحث الثاني يتضمن مفهوم جريمة تزوير الواقع على بطاقة الدفع الالكتروني، وفي المبحث الثالث سلطنا الضوء على الأساس القانوني لحماية بطاقات الدفع الالكتروني من التزوير على المستوى الدولي، والوطني والمقارن.

أما الفصل الثاني خصصناه للإجراءات المتخذة في مواجهة جريمة التزوير الواقعة على بطاقات الدفع الالكتروني، ففي المبحث الأول تطرقنا إلى الإجراءات الوقائية، أما الثاني فتطرقنا إلى إجراءات الردعية، وأخيرا تطرقنا إلى التحديات التي تواجه التعاون الدولي في مواجهة التزوير الالكتروني.

الفصل الأول

الإطار المفاهيمي والأساس القانوني لبطاقات الدفع الإلكتروني وجريمة التزوير

الفصل الأول

الإطار المفاهيمي والأساس القانوني لبطاقات الدفع الإلكتروني وجريمة التزوير

يعتبر الدفع الإلكتروني من الوسائل الحديثة في العصر الرقمي حيث أتاح تطور تكنولوجيا المعلومات والاتصالات إمكانية إجراء المعاملات المالية بشكل أسرع وأكثر أمان وذلك باستعمال بطاقات الدفع الإلكتروني التي تعتبر من وسائل الدفع الحديثة حيث أصبحت بديلا للنقود الورقية والمعدنية. إلا أن استخدامها كأداة وفاء لا يخلو من المخاطر التي تقع عليها فهي أكثر عرضة للاعتداءات أهمها جريمة التزوير، لذلك استوجب حماية بطاقات الدفع من مثل هذه الجرائم الإلكترونية.

ومن خلال ما تم ذكره سوف ندرس في هذا الفصل مختلف المفاهيم المتعلقة ببطاقات الدفع الإلكتروني مع استعراض مختلف أنواعها **(المبحث الأول)**، كما سنتناول مفهوم جريمة التزوير الواقعة على بطاقات الدفع **(المبحث الثاني)**، كما سيتم أيضا تسليط الضوء على الأساس القانونـــي لحمـــاية بطاقات الدفع الإلكتروني من التـــزوير على المستوى الدولي، والوطني والمقارن **(المبحث الثالث)**.

المبحث الأول

بطاقات الدفع الإلكتروني –ضبط مفاهيمي–

لقد ترتب على التطور الذي شهده العالم في الآونة الأخيرة تغيرا في شتى المجالات منها المجال المالي، مما أدى إلى ظهور مصطلح جديد يعرف بالدفع الإلكتروني الذي يعد وسيلة مبتكرة لإتمام المعاملات المالية، حيث يتم الدفع أو التسديد من خلال قنوات اتصال إلكترونية، عبر بطاقات تسمى بالبطاقات الإلكترونية.

وفي هذا المبحث سنحاول تسليط الضوء على مفهوم بطاقة الدفع الإلكتروني في **(المطلب الأول)**، والتطرق إلى أنواع البطاقات في **(المطلب الثاني)**.

المطلب الأول

التعريف ببطاقات الدفع الإلكتروني

سنتطرق في هذا المطلب إلى تبيين مختلف التعاريف التي تخص بطاقات الدفع الإلكتروني منها الشكلي في **(الفرع الأول)**، أما في **(الفرع الثاني)** تناولنا التعريف الموضوعي، وأخيرا التعريف القانوني في **(الفرع الثالث)**.

الفرع الأول: التعريف ببطاقات الدفع من الناحية الشكلية

تعرف بطاقات الدفع من حيث الشكل أنها: "بطاقة بلاستيكية مستطيلة الشكل، مصنوعة من مادة "**كولوريد الفنييل**"، تحمل اسم المؤسسة العالمية الراعية لها واسم البنك المصدر لها واسم ورقم حساب العميل، وتاريخ انتهاء صلاحيتها، مثبت على خلفيتها شريط مغناطيسي يحمل جميع البيانات المشفرة، والخاصة بالبنك المصدر وحامل البطاقة".[1]

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

أبعاد هذه البطاقة هي من 5 إلى 5.5سم للعرض، والطول فيتراوح ما بين 8 و8.5سم. أما بالنسبة لسمكها فيبلغ حوالي من 0.7 إلى 0.8ملم.[1]

وعرفها الدكتور عمر سالم بأنها: "بطاقة صادرة من إحدى المؤسسات إلى عميل لها يقدمها كأداة وفاء للسلع والخدمات، فإذا أراد حامل هذه البطاقة شراء سلعة أو الحصول على خدمة من أحد المجال المعتمد لدى تلك الهيئة يقوم بتقديم البطاقة إليه".[2]

كما تعرف بأنها: "بطاقة بلاستيكية أو ورقية مصنوعة من مادة يصعب العبث بها تصدرها بنك أو شركة استثمار، يذكر فيها اسم العميل الصادرة لصالحه ورقم حسابه حيث يملك الحامل تقديم تلك البطاقة للتاجر لتسديد ثمن مشترياته".[3]

وتعرف كذلك بأنها: "بطاقة بلاستيكية ممغنطة مستطيلة تستخدم في وسط إلكتروني تصدر من قبل هيئة مالية لمصلحة عملائها تحمل اسم المؤسسة. المؤسسة المصدرة لها وشعارها وتوقيع حاملها واسمه وتاريخ نهاية صلاحيتها".[4]

الفرع الثاني: التعريف من الناحية الموضوعية

تتعدد تعاريف بطاقات الدفع الإلكتروني من الناحية الموضوعية، فهناك من عرفها بأنها: "البطاقة التي تصدر عن مؤسسة مالية لمصلحة عمليه يعطيه الحق على ما يلزمه من سلع وخدمات مقابل الوفاء بقيمة السلع التي حصل عليها حامل هذه البطاقة والتزاما بالشروط المتفق عليها".[5]

---

[1]– حنان ريحان مباركي المضحكي، **الحماية الجنائية لبطاقة الائتمان والممغنطة**، دراسة مقارنة، منشورات الحلبي الحقوقية، 2012، ص 41.

[2]– ناظمة محمد نوري الشعري، عبد الفتاح زهير عبدلات، **الصيرفة الإلكترونية**، دار وائل للنشر، الأردن، 2008، ص 47.

[3]– علي جمال الدين عوض، **عمليات البنوك من الوجهة القانونية في قانون التجارة الجديد وتشريعات البلاد العربية**، ط4، دار النهضة العربية، القاهرة، 2008، ص 577.

[4]– عادل يوسف عبد النبي شكري، **الفقه الجبائي**، دار الصفاء، الأردن، 2012، ص 67.

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

وتعرف أيضا بأنها: البطاقة التي تقوم بوظيفتي الوفاء والائتمان يستخدمها صاحبها للوفاء بالتزاماته عوض الدفع الفوري بالنقود، تتيح لحاملها الحصول على السلع والخدمات فور تقديمها، والدفع الآجل لقيمة تلك السلع والخدمات للبنك مصدر البطاقة.[1]

أما مجمع الفقه الإسلامي الدولي بقراره رقم: 7/1/065 الذي صدر في تاريخ هي فعرفها كما يلي: "هي مستند يعطيه مصدره لشخص طبيعي، أو اعتباري بناء على عقد بينها يمكنه من شراء السلع والخدمات مقابل الدفع الآجل لتلك السلع".[2]

وتعتبر كذلك بأنها: عقد تعهد بين البنك المصدر الذي يفتح اعتمادا بمبلغ معين لمصلحة شخص آخر هو حامل البطاقة الذي يستطيع بواسطتها الوفاء وتسديد قيمة مشترياته، لدى المحالات التجارية التي ترتبط مع مصدر البطاقة بعقد يتعهد فيه بقبول الوفاء.[3]

الفرع الثالث: التعريف من الناحية القانونية

تناولت بعض التشريعات تعريف لبطاقة الدفع الإلكتروني وذلك لمواكبة التطور التكنولوجي الحاصل لها، ومن بينها:

أولا: المشرع الجزائري: الذي أورد تعريف لبطاقة الدفع في التعديل الأخير للقانون التجاري في عام 2005 في الفصل الثالث من الباب الرابع من الكتاب 4 من القانون التجاري في المادة 543 مكرر 23[4] من القانون التجاري المعدل والمتمم بموجب قانون رقم 05-02 التي تنص على ما يلي: "بطاقة الدفع هي كل بطاقة صادرة عن الهيئات المالية المؤهلة قانونا التي تسمح لصاحبها بسحب أو تحويل الأموال"، فالمشرع الجزائري اقتصر في تعديله

---

[1]- عصام عبد الفتاح مطر، **التجارة الالكترونية في التشريعات العربية والأجنبية**، دار الجامعة الجديدة، الإسكندرية، 2009، ص 79.

[2]- عذبة سامي حميد الجابر، العلاقات التعاقدية المنبثقة عن استخدام بطاقة الائتمان، **رسالة ماجستير في القانون الخاص**، كلية العلوم القانونية، جامعة الشرق الأوسط للدراسات العليا، الأردن، 2008، ص 26.

[3]- فايز نعيم رضوان، **بطاقات الوفاء**، دار النهضة العربية، القاهرة، 1999، ص 08.

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

الأخير للقانون التجاري المادة 543 من القانون 05-02 على تعريفه للبطاقة فقط، ولم يحدد نصوص قانونية آمرة لها.[1]

كما عرفها أيضا في المادة 69 من قانون النقد والقرض 03-11 كما يلي: "تعتبر وسائل الدفع كل أداة تمكن كل شخص من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل[2].

ثانيا: المشرع الفرنسي

فالمشرع الفرنسي قد عرف بطاقات الدفع 57-01 من المرسوم التشريعي المؤرخ في 1935/10/30، بأنها: "كل بطاقة تصدر من مؤسسة منشأة أو مصلحة تسمح لصاحبها بسحب أو تحويل الأموال".[3]

كما عرفها قانون الشيك الفرنسي رقم 1382/61 لسنة 1991 بموجب المادة 2 من القانون الصادر في 30 ديسمبر 1991 على أنها: أداة تصدر من مؤسسات الائتمان أو إحدى الجهات المنصوص عليها في المادة 8 من القانون رقم 83-46 الخاص بنشاط ورقابة مؤسسات الائتمان التي تسمح لحاملها الوفاء أو التحويل من حسابه.[4]

المطلب الثاني:

أنواع بطاقات الدفع الإلكتروني

تتخذ بطاقات الدفع الإلكتروني أشكال مختلفة استنادا إلى مبدأ المعاملات عبر شبكة الأنترنت والغرض من استعمالها، حيث نقتضي في هذا المطلب إلى عرض مختلف أنواع بطاقات الدفع الإلكتروني، حيث تطرقنا في **(الفرع الأول)** إلى بطاقـــة الائتمان، أمـــا

---

[1]- جهاد رضا الحباشنة، الحماية الجزائرية لبطاقة الوفاء، **رسالة ماجستير**، دار الثقافة، عمان، 2008، ص ص 53، 54.

[2]- المادة 69 من الأمر رقم 03-11 المؤرخ في 27 جمادى الثانية عام 1424هـ الموافق لـ 27-08-2003 المتعلق بالنقد والقرض، الجريدة الرسمية، العدد 52 المعدل والمتمم.

[3]- وسيلة رزيق، بطاقة الائتمان كوسيلة جديدة في النظام المصرفي، **رسالة الماجستير**، فرع قانون أعمال، جامعة الجزائر، كلية الحقوق، 2010، ص 13.

[4]- القانون الفرنسي رقم 91-1382، المتعلق بأن الشيكات وبطاقات الأداء، المؤرخ في 30-12-1991، يعدل ويتمم أحكام المرسوم المؤرخ في 30 أكتوبر 1985.

(الفرع الثاني) بطاقة السحب الآلي، و**(الفرع الثالث)** بطاقة الاعتماد، أما في **(الفرع الرابع)** البطاقة الذكية.

الفرع الأول: بطاقة الائتمان carte de crédit

بما أن بطاقة الائتمان أصبحت جزء أساسيا من الحياة اليومية، لأنها من أبرز الابتكارات المالية في العصر الحديث، لذلك سوف نتعرف في هذا الفرع إلى تعريف بطاقة الائتمان مع ذكر مزاياها وعيوبها.

أولا: تعريف بطاقة الائتمان وأنواعها

لقد تباين التعاريف المتعلقة ببطاقة الائتمان وتنوعت حسب الزاوية التي ينظر منها كل جانب إلى هذه البطاقة.

1-تعريف بطاقة الائتمان:

تعتبر بطاقات الائتمان من أحد أنواع بطاقات الدفع الإلكتروني التي تصدرها البنوك في حدود مبلغ متفق عليه بين البنك والعميل مثل بطاقة فيزا أو الماستر كارت.[1]

كما تعرف بأنها عبارة عن صك اسمي يصدره البنك لمصلحة عميله يعطيه الحق في الحصول على ما يلزمه من سلع أو خدمات اتجاه هذه المشروعات مقابل الوفاء بقيمة السلع والخدمات التي حصل عليها.[2]

وعرفها الدكتور عبد الوهاب أبو سليمان بأنها: "أداة تصدرها هيئة مالية تخول حاملها الحصول على الخدمات، بسحب أثمانها من رصيد أو قرض مدفوع من قبل مصدرها، مع التزام حاملها بالوفاء والتسديد للقرض.[3]

---

[1]- أحمد عبد العليم العجمي، **نظام الدفع الإلكتروني وانعكاساته على سلطات البنك المركزي**، دار الجامعة الجديدة، مصر، 2013، ص 65.

[2]- معادي أسعد صوالحة، **بطاقة الائتمان، النظام القانوني وآليات الحماية الجنائية والأمنية**، المؤسسة الحديثة للكتاب، لبنان، 2012، ص 43.

[3]- عبد الوهاب أبو سليمان، **البطاقات البنكية**، دار القلم، 1993، ص 23، 24.

أما المشرع الجزائري لم يعرف البطاقة ولم يتناول أحكامها بالرغم من انتشارها مؤخرا في الجزائر، فنص المادة 543 مكرر 1/23 من القانون التجاري لم يعطي تعريف محددا بصفة خاصة، بل تعرض إلى تعريف البطاقة بصفة عامة، حيث أنه بين وظيفتها الأساسية "تحويل أو سحب" والتي تكون صادرة عن بنك أو مؤسسة مالية.[1]

أما مجمع الفقه عرفها بأنها: "مستند يعطيه مصدره لشخص طبيعي أو اعتباري على شكل قرض استهلاك، بناءً على عقد بينها يمكنه من شراء السلع والخدمات من محلات تقبل هذا المستند".[2]

2-خصائص البطاقة:

تتميز بطاقة الائتمان بعدة خصائص تجعلها أداة مالية وعملية في الحياة اليومية أهمها:

- البطاقة أداة وفاء وضمان، فتقوم بوظيفة الوفاء بقيمة السلع والخدمات التي يشتريها الحامل بدلا من النقود، وهي في نفس الوقت توفر ضمان للتجار لاستيفاء ثمن مبيعاتهم من المصدر.
- للبطاقة صفة العالمية فيتم قبولها في جميع أنحاء العالم.
- بطاقة ثلاثية الأطراف وهم حامل البطاقة ومصدر البطاقة والتاجر الذي يبرم عقدا مع مصدر البطاقة.
- يتطلب استعمال هذه البطاقة وجود أجهزة آلية إلكترونية من أجل تفعيل الخدمة التي وجدت البطاقة من أجلها مع توفير سهولة في المعاملات المالية.[3]

---

[1]- المادة 543 مكرر 23 من القانون التجاري، **المرجع السابق**.

[2]- قرار رقم 7/1/65 قرارات وتوصيات المجمع الفقهي في دورته السابعة المنعقدة بجدة 1412 هـ.

[3]- بن تركي ليلى، الحماية الجنائية لبطاقات الائتمان الممغنطة، **أطروحة لنيل شهادة الدكتوراه**، تخصص العقوبات والعلوم الجنائية، جامعة الإخوة منتوي، قسنطينة، 2016-2017، ص 13.

3-المزايا والعيوب:

انطلاقا من الخصائص التي ذكرناها يمكن الخلاص إلى أنها فضلا عن كونها تعتبر من أهم التقنيات المبتكرة في المنظومة المصرفية العالمية فهي تتسم بمجموعة من المزايا **(أولا)** التي تميزها عن غيرها من البطاقات التي تشبهها، إضافة إلى اقترانها بمجموعة من العيوب**(ثانيا)**.

أولا: المزايا

ينطوي استعمال بطاقة الائتمان على العديد من المزايا التي تعود على الأشخاص المتعاملين بها، سواءا حاملها أو مصدرها أو التاجر، من أهم هذه المزايا التي تقدمها:[1]

- سهولة حملها واستخدامها.
- تحظى بقبول عام في كل دول العالم تقريبا.
- توفير الأمان والحماية لمال التاجر.
- يمكن الاستفادة منها في حجز تذاكر السفر والفنادق والمطاعم والتسوق الالكتروني.
- توفير الخدمات لعملاء المصاريف في جميع الأوقات، كما تسمح لهم بالتعامل مع العملات المختلف.
- تعزيز الأمان المالي الخاص بصاحب البطاقة لأنه لا يحتاج لحمل مبالغ مالية.
- تمتع صاحب البطاقة أحيانا كثير من العروض.

ثانيا: العيوب:

تعتبر بطاقة الائتمان سلاح ذو حدين فبالرغم من الإيجابيات التي تتمتع بها إلا أنها تشمل بعض العيوب أهمها:

- التزام صاحب البطاقة بتسديد قيمة المشتريات المرتبطة بالبطاقة حتى لو ضاعت أو سرقت.

[1]- بكير علي محمد أبو بكر، **الطبيعة القانونية لبطاقة الائتمان**، المركز القومي للإصدارات القانونية، القاهرة، مصر، ص 33.

- زيادة نسبة الفوائد المترتبة على القروض الخاصة بالبطاقة، وذلك إن لم يتم دفع المبالغ المالية المستحقة بالكامل في الوقت المحدد.
- الوقوع في فخ الديون إذا لم يتم إدارة الانفاق بشكل جيد، مما يؤدي إلى تراكم المبالغ.
- يترتب على هذه البطاقة رسوم إضافية مثل رسوم لسحب النقدي.
- البطاقة أكثر عرضة للاحتيال من طرف المهاجمين غير الأنترنت.[1]

الفرع الثاني: بطاقة السحب الآلي

تعد بطاقة السحب الآلي من أبرز ابتكارات التكنولوجية في مجال الخدمات المصرفية، نظرا لما تقدمه من سرعة وأمان وسهولة في الاستخدام، لذا سوف نسلط الضوء في هذا الفرع إلى التعريف ببطاقة السحب الآلي، مع ذكر كل مميزاتها وعيوبها.

أولا: تعريف بطاقة السحب الآلي

ويطلق عليها بطاقات الصراف الآلي، وهي بطاقة تخول لحاملها إمكانية سحب مبالغ نقدية من حسابه بحد أقصى متفق عليه من خلال أجهزة إلكترونية خاصة، حيث يقوم العميل حامل البطاقة بإدخالها في جهاز السحب الإلكتروني الذي يطلب منه إدخال الرقم السري، وتحديد المبلغ المطلوب سحبه عن طريق لوحة المفاتيح على الجهاز، وبعد عملية السحب يسترد العميل بطاقته آليا، ويسجل المبلغ المسحوب في حسابه مباشرة.[2]

تنقسم بطاقات السحب إلى بطاقات سحب داخلية وهي بطاقات صادرة عن بنك، أو مؤسسة مالية تؤدي وظائفها داخل الدولة الواحدة، وبطاقات سحب دولية وهي التابعة بالمنظمة الدولية الراعية لها، بحيث يستطيع حاملها استخدامها في جميع أنحاء العالم.[3]

---

[1]– هدى برابح، بطاقة الائتمان البنكية والجرائم المتعلقة بها، **أطروحة مقدمة لنيل شهادة الدكتوراه**، تخصص قانون بنكي ومالي، كلية الحقوق العلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2021–2022، ص ص 38، 39.

[2]– نوال بلعباس، بطاقة الائتمان كوسيلة من وسائل الدفع الحديثة، **أطروحة لنيل شهادة دكتوراه علوم في القانون**، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر 1، 2016–2017، ص 63.

[3]– **المرجع نفسه**، ص 64.

وهذه البطاقة ليست بطاقة ائتمانية، لأن وظيفتها الأساسية تتمثل في سحب النقود من حساب الحامل المودع لدى البنك من خلال أجهزة خاصة، أي أن في حالة عدم وجود رصيد للحامل لدى البنك فإن الجهاز لن يصرف للحامل أي مبلغ[1].

وبالتالي بطاقة السحب لا تعتبر أداة وفاء، بل تعتبر أداة سحب فقط.[2]

ثانيا: ميزات هذه البطاقة

تتميز هذه البطاقة بـــ:[3]

- بالنسبة للعميل توفر له سرعة الخدمة في أقل من دقيقة.
- لا تصدر إلا لمن لديه حساب في البنك.
- تصرف دون مقابل.
- يمكن استخدامها للشراء عبر الأنترنت، أو في المحلات التجارية التي تدعم الدفع بواسطة بطاقات السحب الآلي.
- تجنب ازدحام البنك.
- القدرة على التوسع دون الحاجة إلى أيادي عاملة وضمان انعدام الأخطاء، نتيجة الترحيل الأتوماتكي للحركات دون التدخل يدوي وتقليل تداول الاشعارات.

ثالثا: عيوب البطاقة

من عيوب هذه البطاقة:[4]

- البطاقة معرضة للسرقة والاحتيال في حالة استخدامها في أجهزة صراف آلية غير آمنة.

---

[1]– عادل يوسف شكري، " الحماية الجنائية لبطاقات الدفع الإلكتروني (دراسة مقارنة) "، **مجلة الحماية الجنائية**، المجلد الأول، العدد 11، كلية الحقوق، جامعة الكوفة، د.س.ن، ص 19.

[2]– معتز نزيه، محمد الصادق المهدي، **المتعاقد المحترف، مفهومه والتزامه ومسؤوليته**، دار النهضة العربية، القاهرة، مصر، 2009، ص 28.

[3]– أحمد عبد العليم العجمي، **المرجع السابق**، ص ص 68، 69.

[4]– عبد الهادي النجار، التجارة نقود المعرفة وآليات تناولها، **بحث مقدم في المؤتمر السنوي لكلية الحقوق حول الجديد في أعمال المصاريف من الوجهتين القانونية والاقتصادية**، جامعة بيروت، لبنان، 2002، ص 52.

- الرسوم المرتفعة من خلال فرض بعض أجهزة الصراف الآلي رسوما إضافية على السحب.
- في حال فقدان البطاقة أو سرقتها قد يكـــون من الصعب استرجاع الأمـــوال بسرعة، مما قد يعرض المستخدم لمخاطر مالية.
- بعض المشاكل التقنية التي تتعرض إليها الأجهزة تمنع المستخدم من سحب الأموال.
- القيود على السحب النقدي فغالبا ما تكون هناك حدود على المبالغ التي يمكن سحبها يوميا، مما قد يسبب مشاكل إذا كان الشخص يحتاج لمبلغ كبير في يوم واحد.
- سداد حاملي البطاقة للديون المستحقة عليه.

الفرع الثالث: بطاقة الاعتماد charge card

بطاقة الاعتماد هي نوع من البطاقات المصرفية تستخدم كأداة وفاء وائتمان لا تتعدى شهر وبمقتضاها يحصل حاملها على احتياجاته من السلع والخدمات فور تقديمها، تمنح بناءا على عقد خاص بين أحد الأشخاص أو إحدى المؤسسات المالية، وبمقتضى هذا العقد تقوم هذه المؤسسة بفتح اعتماد مالي بمبلغ مالي محدد، فإذا أراد العميل حامل هذه البطاقة شراء سلعة أو الحصول على خدمة معينة من إحدى المجال المعتمد لدى المؤسسة يقوم بتقديم البطاقة إلى ذلك المحل.[1]

ولا يحتاج حاملها إلى الدفع الفوري لقيمة ما يحصل عليه من خدمات من التجار الذين يبيعون بها نقدا، وإنما يكتفي بتقديم بطاقة للتاجر الذي يدون بيـــاناتها في فاتـــورة من عدة نسخ يوقعهـــا حامل البطاقـــة ويرسل التـــاجر نسخة من هذه الفاتورة إلى المصرف، التاجر، أو الجهة المصدرة للبطاقة، وتقوم الجهة المصدرة للبطاقة في ميعاد

[1]– أحمد عبد العليم العجمي، **المرجع السابق**، ص 67.

محددا دوريا في نهاية كل شهر بصفة عامة بإرسال كشف لحامل البطاقة بمشترياته مطالبة إياه بسداد القيمة المستحقة.[1]

أولا: فوائد بطاقة الاعتماد

بطاقة الاعتماد لها عدة فوائد تتمثل في:[2]

- بطاقة الاعتماد تمنح مستخدمها إمكانية شراء السلع مع تأجيل الدفع، مما يوفر مرونة في التعامل.
- إمكانية الشراء عبر الأنترنت بسهولة، مما يسهل الوصول إلى مجموعة واسعة من الخدمات.
- أداة دفع معترف بها دوليا، مما يسهل عملية السفر الدولي.
- يمكن لحامل البطاقة سحب الأموال نقدا من أجهزة الصراف الآلي.

ثانيا: عيوب بطاقة الاعتماد

بالرغم من الفوائد التي تملكها بطاقة الاعتماد إلا أنها تحمل عيوبا يجب الدراية بها وهي:[3]

- الوقوع في الديون بسبب تراكم الفوائد إذا لم يتم دفع المبالغ المستحقة في الوقت المحدد.
- الرسوم الإضافية مثل رسوم التأخير.
- إمكانية التعرض للاحتيال في حال استخدامها بشكل غير قانوني.

الفرع الرابع: البطاقة الذكية smart card

البطاقة الذكية عبارة عن بطاقة بلاستيكية ممغنطة مزودة بشرائح إلكترونية دقيقة ذات ذاكرة وقدرات تفاعلية، تستعمل في الدفع الفوري وتسمح بالتعامل مع الوحدات الطرفية عند

---

[1]– عمر سليمان الأشقر، " بطاقة الائتمان الممغنطة ومخاطر التزوير "، **المجلة العربية للدراسات الأمنية والتدريب**، السنة العاشرة، العدد 19، السعودية،1995، ص 144.

[2]– إيهاب فوزي السقا، **الحماية الجنائية والأمنية لبطاقة الائتمـــان**، دار الجامعـــة الجديدة للنشر، مصـــر، 2007، ص 23.

[3]– عبد العالي النجار، **المرجع السابق**، ص 48، 52.

نقاط البيع أو مع أي حسابات آلية شخصية أخرى، ومزودة بنظام أمان خاص لحمايتها ضد استخدامها من طرف الأشخاص غير المرخص لهم.[1]

كما أنها بطاقة تحتوي على رقائق إلكترونية يتم تخزين عليها جميع البيانات الخاصة لحاملها الاسم، العنوان المصرف، المصدر، أسلوب الصرف، المبلغ المصروف وتاريخه وتاريخ حياة الزبون المصرفية، تمكن هذه البطاقة حاملها من اختيار التعامل بها سواء كان هذا التعامل ائتماني أو حتى عن طريق الدفع الفوري، وتعتبر منظمة للمعلومات إلكترونيا لأنها تحتفظ بكل العمليات وترصد الحسابات الجارية.[2]

تتميز البطاقة الذكية بمجموعة من السمات أهمها:[3]

- أنها بطاقة تحتوي على شريحة يمكن من خلالها حفظ المعلومات الرقمية فيها بالإضافة إلى أنها تتوافق مع أجهزة حاسوبية.
- تتشابه مع بطاقة الائتمان من حيث الشكل والحجم.
- تسهل البطاقة الذكية على العملاء تأمين تخزين المعلومات والنقد للشراء.
- تحتوي على معلومات مهمة كالسجلات الطبية أو معلومات الحساب البنكية للمستخدم.
- البطاقة يجوز استعمالها كبطاقة هوية أو بطاقة صحية أو بطاقة تنقل في وسائل المواصلات العامة.
- في حالة سرقة البطاقة الذكية يكون من الصعب جدا على غير صاحبها معرفة الرقم السري الخاص بالبطاقة.
- لها القدرة في سرعة التعامل وتنفيذ العمليات الأكثر تعقيدا.

---

[1]– طارق طه، **إدارة البنوك في بيئة العولمة والأنترنت**، دار الجامعة الجديـدة للنشر والتوزيع، مصـر، 2007، ص 273.

[2]– محمد عبيد الحسين الطائي، **التسويـق والتجارة الإلكترونيـــة**، المكتبة العصرية للنشر والتوزيع، مصر، 2008، ص 187.

[3]– محمد بن عزة جليلة زويهري، عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر، "عرض تجارب دولية"، **الملتقى الدولي الرابع**، المركز الجامعي خميس مليانة، عين الدفلى، الجزائر، 2011، ص 05.

وتحقق البطاقة الذكية العديد من الفوائد أهمها:[1]

- تستخدم عند إجراء التحويلات المصرفية وعمليات البيع والشراء عبر شبكة الأنترنت.
- توفر السير والسهولة في التعامل.
- بطاقة تؤدي دور بطاقة السحب وبطاقة الائتمان وذلك طبقا لما يريده العميل.
- القدرة العالية على تخزين المعلومات.
- تعدد مجالات استعمالها مثل الخدمات الصحية، سداد الرسوم بطريقة إلكترونية، وفي مجال البنوك.
- التقليل من فرص التلاعب والتحايل في الأعمال.

[1]– أنس العلبي، **النظام القانوني لبطاقات الاعتماد**، منشورات الحلبي الحقوقية، لبنان، 2005، ص 66.

المبحث الثاني

الدلالات المفاهيمية لجريمة التزوير

يعد التزوير من أخطر الجرائم التي تقع على بطاقات الدفع، خاصة أنها أصبحت مهمة في المعاملات المالية، وحسب التطور الحاصل الذي سببته الثورة المعلوماتية ظهر مصطلح جديد هو التزوير الإلكتروني.

لذلك سوف نتعرف في هذا المبحث على مدلول التزوير العادي في **(المطلب الأول)**، وفي **(المطلب الثاني)** نتعرف على معنى التزوير الإلكتروني.

المطلب الأول

مدلول التزوير التقليدي

لتحديد مفهوم التزوير في بطاقات الدفع يجب الرجوع أولا لمعرفة التزوير بمفهومه التقليدي، لذا سوف نقوم بدراسة المفهوم العادي أو التقليدي في **(الفرع الأول)**، أما في **(الفرع الثاني)** سندرس أركان التزوير العادي في بطاقات الدفع.

الفرع الأول: تعريف التزوير التقليدي

يُعد التزوير التقليدي من أخطر الجرائم التي تمس الثقة بالمعاملات اليومية بين الأفراد والمؤسسات، فالغرض منه هو تحريف الحقيقة في المستندات أو الوثائق بهدف تحقيق مكاسب غير مشروعة، وعليه سنتطرق في هذا الفرع إلى تعريف اللغوي والاصطلاحي للتزوير التقليدي مع ذكر أركانه.

أولا: التعريف اللغوي

التزوير من زور يُزور تَزويرًا، وهو محاولة تزيين الكذب وطمس الحقيقة وإلباس الباطل بثوب الحق، فجوهر التزوير هو الكذب الذي يهدف إلى إنشاء حقيقة قائمة.[1]

[1]– إسماعيل بن حماد الجوهري، **تاج اللغة وإصحاح اللغة العربية**، الطبعة الرابعة، دار العلم للملايين، بيروت، لبنان، 1987، ص 674.

كما يقصد به أيضا تغيير الحقيقة أو إحلال أمر غير صحيح، محل الصحيح الواقع عن الأمور، والتزوير في المحررات هو كذب مكتوب وليس كذب بالقول.[1]

ثانيا: التعريف الاصطلاحي للتزوير التقليدي

يعرف التزوير بأنه كل وسيلة يستعملها شخص ليغش بها آخر فجوهر التزوير هو الكذب المكتوب والكذب بصفة عامة.[2]

عرفه الفقيه **غارسون:** بأنه " تغيير الحقيقة بقصد الغش في محرر صالح للإثبات ويرتب عليه أثر قانونيا".[3]

كذلك يعتبر صورة من صور الكذب التي يقوم بها الشخص لتغيير الحقيقة في المحرر وإلحاق الضرر بأطرافه.[4]

وقد عرفها الأستاذ **جون بول دوسي** أيضا: على أنه " كل تزييف أو نفي الحقيقة يكون الغرض منه خداع الآخرين وإلحاق الضرر بهم".[5]

الفرع الثاني: أركان جريمة التزوير التقليدي

تتمثل أركـــان جريمة التزوير التقليديـــة في بطاقات الدفع في الركـن المادي المعنوي، وهذا ما سنتعرف عليه الآن:

أولا: الركن المادي للجريمة

وينقسم إلى أربعة عناصر هي:

1-المحل:

إن محل جريمة التزوير يتمثل في وجود المحرر التي تشكل سندات بما في ذلك المحررات العمومية والرسمية والعرفية، والتجارية أيضا، وبذلك تكون محلا للتزوير.

أ-تغيير الحقيقة:

---

[1]- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، **أطروحة مقدمة لنيل شهادة الدكتوراه**، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2016، ص 53.

[2]- نبيل صقر، **الوسيط في الجرائم المخلة بالثقة العامة**، دار الهدى، الجزائر، 2015، ص 190.

[3]- إيهاب فوزي السقا، **المرجع السابق**، ص 288.

[4]- عبد العزيز سعد، **جرائم التزوير وخيانة الأمانة واستعمال المزور**، دار هومة، الجزائر، 2005، ص 14.

[5]- جمال نجيمي، **جرائم التزوير في قانون العقوبات الجزائري**، دار هومة، الجزائر، 2013، ص 270.

وهو السلوك الإجرامي الذي يقوم عليه التزوير في المحررات، ويعد جوهر التزوير المعاقب عليه جزائيا، حيث أنه لا يشترط أن يكون تغيير الحقيقي كليا بل يكفي أن يكون التغيير جزئيا.[1]

ب-طرق التزوير:

ويتم التزوير بإحدى الطرق التي نص عليها قانون العقوبات الجزائري في نص المادة 216 وهي ما يلي:[2]

- تزييف الكتابة والتوقيع.
- اصطناع اتفاقيات أو التزامات وإدراجها في المحررات.
- إضافة أو تزييف الشروط أو الوقائع التي أعدت في المحررات.
- كذلك انتحال شخصية الغير أو الحلول محلها.

ج-الضرر:

لابد أن يترتب على جريمة التزوير ضررا، وهذا الضرر لا يشترط أن يمس الشخص الذي يقصده المزور بل المهم حدوثه ولو كان قليلا، وقد يكون الضرر ماديا أو معنويا أو اجتماعيا، محققا كان أو محتملا.[3]

ثانيا: الركن المعنوي

جريمة التزوير من الجرائم العمدية التي تستوجب لقيامها وجود القصد الجنائي بشقيه العام والخاص، فالقصد الجنائي العام يقصد علم وإرادة الجاني الذي يقوم بتزوير البطاقة، فهو يعلم بجميع أركان الجريمة، أما القصد الجنائي الخاص هو الذي يظهر في نية استعمال البطاقة المزورة استعمالا غير مشروع.[4]

المطلب الثاني

---

[1]- أحسن بوسقيعة، **الوجيز في القانون الجزائري الخاص**، ط9، الجزء 2، دار هومة، الجزائر، 2008، ص ص 335، 338.

[2]- المادة 216 من الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم.

[3]- أحسن بوسقيعة، **المرجع السابق**، ص 340.

[4]- **المرجع نفسه**، ص 338.

مدلول التزوير المعلوماتي

تعد جريمة التزوير المعلوماتي من أخطر الجرائم في العصر الحالي التي ترتكب بواسطة الحاسب الآلي نتيجة الثورة المعلوماتية.

الفرع الأول: تعريف التزوير المعلوماتي

يحمل التزوير عدة تعريفات في طياته منها التعريف الفقهي والتعريف التشريعي.

أولا: التعريف الفقهي

يقصد بالتزوير الإلكتروني تغيير الحقيقة المقترنة بغش ويتم بإحدى الطرق التي نص عليها القانون ويلحق ضرر بالغير.[1]

حيث عرفه علي عبد القادر القهوجي بأنه: "تغيير الحقيقة التي ترد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة أو عن طريق الطابعة، أو كانت مرسومة عن طريق الراسم ويستوي في المحرر الإلكتروني أن يكون مدونا باللغة العربية أو أية لغة أخرى لها دلالة، وقد تتم في مخرجات ورقية أو محفوظة على دعامة".[2]

كما يعرف أيضا: كل الأفعال العمدية وغير شرعية التي تلحق ضررا بالغير من خلال التلاعب بالمعطيات الإلكترونية الموجودة داخل الجهاز الآلي، سواء كان حذف أو تعديل أو إدخال أو أي شكل من أشكال الاعتداء.[3]

---

[1]– محمد عبد الله أبو بكر سلامة، **جرائم الكمبيوتر والأنترنت**، موسوعة الجرائم المعلوماتية، منشأة المعارف، الإسكندرية، 2006، ص 177.

[2]– حفصي عباس، جرائم التزوير الإلكتروني، **رسالة مقدمة لنيل شهادة الدكتوراه في العلوم الإسلامية**، تخصص شريعة وقانون، جامعة وهران1، 2015/2014، ص 18.

[3]– علي كحلون، " الجريمة المعلوماتية وتوجيهات محكمة التعقيب "، **مجلة الأخبار القانونية**، تونس، المجلد126، العدد127، جانفي 2012، ص 16.

وما يمكن قوله على جريمة التزوير الإلكتروني أنها تعد من بين الجرائم الإلكترونية التي تتم أو ترتكب في بيئة معلوماتية، أو بمعنى آخر هي التي تتم بوسيلة إلكترونية أو معلوماتية في محرر إلكتروني.[1]

ثانيا: التعريف التشريعي

هو تغيير الحقيقة بقصد الغش في المحرر من أجل أن يلحق ضررا ويحدث أثرا قانوني ويكون بإحدى الطرق التي نص عليها القانون، في المادة 216 من قانون العقوبات الجزائري[2].

وإزاء ضيق النصوص التقليدية بشأن مواجهة التزوير الذي يقع في المجـــال الإلكتروني، نجد بعض التشريعات لم تُعطِ تعريف للتزوير الإلكتروني بما فيها قانون العقوبات الجزائري والمصري، بل اكتفت فقط ببيان الطرق التي يرتكب بها التزوير وأنواعه والعقوبات المقررة له.[3]

فالمشرع الجزائري نجده قد نص على جرائم التزوير في المحررات وهذا في المواد 214 إلى 299 من قانون العقوبات دون أن يعطي تعريف للتزوير، بل اكتفى ببيـــان أنواع جرائم التزوير وهي التزوير في المحررات الرسمية العمومية الواردة في المـــواد 214 إلى 217، والتزوير في المحررات التجارية أو المصرفية، وذلك في المـــواد 219 إلى 220، والتزوير في بعض الوثائق الإدارية والشهادات في المواد 222 إلى 229.[4]

---

[1]– عبد الفتاح بيومي حجازي، **جرائم الكمبيوتر والأنترنت في التشريعات العربية**، دار النهضة العربية، مصر، 2009، ص 49.

[2]– بن شهرة شول، الحماية الجنائية للتجارة الإلكترونية، **شهادة الدكتوراه**، كلية الحقوق، تخصص جنائي، 2011/2010، ص 170.

[3]– أمير والي، إسحاق بلعلمي، مكافحة جريمة التزوير الإلكتروني في الجزائر، **مذكرة مقدمة لنيل شهادة الماستر**، تخصص إعلام آلي، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022–2023، ص 12.

[4]– **المرجع نفسه**، ص 13.

أما المشـــرع المصري وبالرجـــوع إلى نص المـــادة 23 من قانـــون التوقيع الإلكتروني، فنجده يشير إلى أن التزوير يتم عن طريق الاصطناع أو التعديل أو أي طريق آخر، كما أنه لم يبين طبيعة الوثيقة المعلوماتية محل الحماية، حيث لم يتطرق لتلك القيمة القانونية التي تتمتع بها تلك المعلومات التي تتضمنها.[1]

لكن هناك بعض التشريعات العقابية التي أوردت تعريفا للتزوير المعلوماتي منها قانون العقوبات الفرنسي من خلال القسم الأول ضمن الكتاب الرابع تحت عنوان الاعتداءات ضد الثقافة العامة، وهذا في المادة 441 المعدلة في 14 ماي 1993 حيث نصت أن "التزوير يقوم على كل تغيير في الحقيقة بغش من شأنه أن يسبب ضررا، والذي يرتكب بأي طريقة كانت في محرر مكتوب".[2]

وقد عرفت اتفاقية الأوروبية لمكافحة الجريمة المعلوماتية اتفاقية بودابست في المادة 7 منها التزوير الإلكتروني بأنه التزوير المرتبط بالحاسب الآلي الذي يكون عن طريق حذف أو تعديل للمعلومات أو البيانات المسجلة به.[3]

ثالثا: طرق وأساليب تزوير بطاقة الدفع الإلكتروني

تتعرض بطاقات الدفع كغيرها من المحررات والمستندات إلى التزوير بمختلف أشكاله وطرقه، والذي يكون عن طريق التلاعب بالبيانات والمعلومات الذي تشمل هذه البطاقة.

1- التزوير الكلي للبطاقة:

إن التزوير الكلي في بطاقة الدفع يمس المادة المكونة لبطاقة الدفع، حيث يتم اصطناع بطاقة كاملة ثم يتم تقليد الرسوم الخاصة على هيكل البطاقة، وتغليفها وتلصيق الشريط الممغنط وشريط التوقيع ثم القيام بالطباعة النافرة وتشغيلها عن طريق إشباعها بالمعلومات التي حصل عليها المزور من البطاقة الصحيحة، بعد ذلك يتم القيام بنسخ نُسخ عديدة من البطاقة المزورة ليتم تسويقها بهدف استخدامها استخدام غير مشروع.[4]

---

[1]- المادة 23 من قانون التوقيع الالكتروني المصري، رقم 15، 2004، المؤرخ في 6 أفريل 2004.

[2]- مسعود خثير، **الحماية الجنائية لبرنامج الكمبيوتر**، دار الهدى، عين مليلة، الجزائر، ص ص 135، 136.

[3]- المادة 7 من الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية.

[4]- رياض فتح الله بصلة، **جرائم بطاقة الائتمان**، دار الشروق، بيروت، لبنان، 1995، ص 108.

2- التزوير الجزئي للبطاقة:

في هذه الحالة من التزوير يتم استغلال جسم أو هيكل البطاقة الحقيقي وما عليها من رسوم خاصة وحروف بارزة، وكتابات أمنية، ليقوم بتزوير البطاقة عن طريق صهر ما عليها من أرقام بارزة لبطاقة صحيحة انتهت صلاحيتها، أو إعادة قولبة رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر يتم الحصول عليه بالطريقة السابقة، أو تقليد الشريط الممغنط عن طريق حذف ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة مسروقة أو كشف التوقيع، ووضع شريط بتوقيع جديد[1].

الفرع الثاني: أركان جريمة تزوير البطاقة الإلكترونية

تقوم جريمة التزوير الإلكتروني كغيرها من الجرائم على أركان وهي:

أولا: أركان الجريمة

1-الركن المادي:

يعتبر من أهم العناصر المكونة لجريمة التزوير، فشأنه هو تغيير الحقيقة في المحرر بطريقة نص عليها القانون بشرط أن يلحق الضرر بالغير يقوم هذا الركن على عدة أسس وهي:

أ-تغيير الحقيقة:

سبقت الإشارة إلى أن الركن المادي في جريمة التزوير الإلكتروني هو تغيير الحقيقة في محرر بالطرق المنصوص عليها قانونا، أي استبدالها بما يغايرها تغييرا من شأنه أن يسبب ضررا، حيث أنه لا يشترط أن يكون تغيير الحقيقة كليا بل يكفي التغيير أن يكون جزئيا فيها، على نحو يغير مضمونه دون الإهدار من قيمته، وبالتالي ينصب تغيير الحقيقة كعنصر من عناصر الركن المادي على المعلومات والبيانات مهما كانت طبيعتها وذلك باستخدام جهاز الحاسب الآلي.[2]

---

[1]- رياض فتح الله بصلة، **المرجع السابق**، ص 111.

[2]- أحسن بوسقيعة، **المرجع السابق**، ص 335.

ب- المحل:

إن محل جريمة التزوير في بطاقة الدفع هو وجود المحرر الذي يعد من أحدث طرق الإثبات التي ظهرت مع الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات.

فالمحرر يعتبر البنية الأساسية لجريمة التزويـــر فإن لم يكن محرر لا يتحقــق التزوير، فقد عرف قانون الأونسترال النموذجي للتجارة الإلكترونية المحرر الإلكتروني في المادة 2 من الفقرة 01: "يراد برسالة البيانات المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية، أو بوسائل متشابهة".[1]

وقد سايرت العديد من التشريعات التعريف الوارد في قانون الأونسترال النموذجي منها التشريع الجزائري والمصري.

فالمشرع الجزائري عرف المحرر لكن بطريقة غير مباشرة من خلال تعريفه للإثبات بالكتابة، حيث أقر في المادة 323 مكرر 1 من القانون المدني بأنه: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرساله، فالمشرع اعتبر الكتابة تحمل على أي وسيلة سواء ورقية كانت أو إلكترونية ترسل بأي وسيلة سواء ورقية كانت أم إلكترونية ترسل بطريقة تقليدية أو إلكترونية".[2]

كذلك المشرع المصري الذي عرف المحرر في المادة 01 من القانون الخاص من التوقيع الإلكتروني: "كل رسالة بيانات أو معلومات تخزن أو ترسل كليا أو جزئيا بوسيلة إلكترونية".[3]

---

[1]- المادة 02 من القانون النموذجي الأونسترال للتجارة الإلكترونية الدولية 1996.

[2]- المادة 323 مكرر 1 من القانون 10/05 المؤرخ في 18 جمادى الأولى عام 1426هـ الموافق لـ 6 يونيو سنة 2005 المعدل والمتمم للقانون المدني، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية المؤرخة في 19 جمادى الأولى 1426هـ الموافق لـ 26 يونيو 2005، ص 17.

[3]- تقابلها المادة 1316 من القانون المدني الفرنسي، المعدلة بموجب قانون إثبات تكنولوجيا المعلومات المتعلق بالتوقيع الالكتروني، المؤرخ في 13 مارس 2000.

ج/ الضرر:

حتى تقوم جريمة التزوير يجب أن يترتب عليها ضررا لأنه إذا انعدم الضرر انعدم وجود وقوع جريمة التزوير، فقد يكون هذا الضرر ماديا أو معنويا أو اجتماعيا، فهو يعرف بأنه الاخلال بالمصلحة التي يحميها القانون.[1]

ثانيا: الركن المعنوي

جريمة تزوير بطاقة الدفع الإلكتروني من الجرائم العمدية التي تستوجب القصد الجنائي بشقيه العام والخاص.

فالقصد العام، الجاني يعلم بجميع أركان الجريمة خاصة تغيير حقيقة البطاقة وأن يعلم بأن ينتج على هذا السلوك ضررا، فهو يقوم على عنصر العلم والإرادة، أما القصد الخاص، يتمثل في نية الجاني بتزوير البطاقة الإلكترونية.[2]

ثالثا: الركن الشرعي

ويقصد بالركن الشرعي في جريمة تزوير بطاقات الدفع توفر نص التجريم الواجب تطبيقه على الفعل بمعنى أن يخضع التزوير بمبدأ الشرعية، أو يخضع لنص قانوني يجرمه.

من بين بعض التشريعات التي جرمت التزوير نجد:

1-التشريع المصري:

الذي جرم فعل التزوير في المحررات الإلكترونية في قانون التوقيع الإلكتروني، إذ جاء في المادة 23 الفقرة ب وج أنه: "يعاقب كل يزور محررا إلكترونيا عن طريق التعديل أو الحذف أو إضافة أو بأي طريقة".[3]

كما جرم المشرع المصري في قانون الأحوال المدنية تزوير الوثائق الرسمية ذات الطبيعة المعلوماتية كجهاز الحاسب الآلي الموجود بمراكز الأحوال المدنية من خلال المادة

---

[1]- فوزية عبد الستار، **شرح قانون العقوبات، القسم الخاص وفقا لأحدث التعديلات**، ط3، دار النهضة العربية، مصر، 2012، ص 291.

[2]- أحسن بوسقيعة، **المرجع السابق**، ص ص 341، 342.

[3]- المادة 23 من قانون التوقيع الإلكتروني المصري، **المرجع السابق**.

72 التي تنص على: "تطبيق أحكام هذا القانون وقانون العقوبات تعتبر المعلومات المسجلة بالحاسب الآلي وملحقاتها بمراكز الأحوال المدنية ومحطات الإصدار الخاصة بها".[1]

2-التشريع الإماراتي:

والذي حظي اهتمام في هذا الجانب من خلال القانون الاتحادي لمكافحة جرائم تقنية المعلومات، فقد جرم بعض الأفعال التي تتصل بالأنظمة المعلوماتية من بينها فعل التزوير في مستند من مستندات الحكومة الاتحادية المعترف بها قانونا وهي السجن المؤقت.[2]

3-التشريع الجزائري:

ما يؤكد اهتمامه هو رسم ووضع خطط قانونية لتنفيذ سياسة وقائية وردعية ضد الجرائم الإلكترونية، من بين هذه الخطط القانونية 09-04 المؤرخ في 05-08-2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، والذي يعتبر قانونا نموذجيا خاص بمكافحة الجريمة المعلوماتية.[3]

رابعا: تمييز التزوير الإلكتروني والتزوير التقليدي

يشكل التزوير الالكتروني تطورًا حديثا يختلف عن التزوير التقليدي، مما يستدعي التمييز بينهما لضمان فعالية المواجهة القانونية لكل نوع.

1-أوجه الاختلاف:

هناك اختلاف بين الجريمتين التزوير التقليدي والعادي يتمثل فيما يلي:

أ-من حيث البيئة التي يتم فيها التزوير:

فالتزوير التقليدي يتم ارتكاب الجريمة فيه على دعامة ورقية، وبوسائل تقليدية، عكس التزوير الإلكتروني الذي يتم ارتكاب الجريمة فيه في وسط آلي أو بيئة معلوماتية.[4]

---

[1]- محمد أمين الرومي، **جرائم الكمبيوتر والأنترنت**، دار المطبوعات الجامعية، مصر، ص 88.

[2]- القانون 06/02 المؤرخ في 30 يناير 2006 المتعلق بمكافحة جرائم تقنية المعلومات الجديدة الرسمية، عدد 442، الصادرة في 31 يناير 2006، ص 55.

[3]- القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية المؤرخة في 25 شعبان 1430هـ الموافق لـ 16 أوت 2009، ص 09.

[4]- أحمد خليفة الملط، **الجرائم المعلوماتية**، ط2، دراسة مقـارنة، دار الفكـر الجـامعي، 2006، ص 93.

ب- من حيث اكتشاف الجريمة:

فجريمة التزوير التقليدي سهلة الاكتشاف بسبب التغيير الذي يترك أثرا في المحرر، على عكس التزوير الالكتروني الذي يصعب اكتشافه، لأن التغيير فيه لا يترك أي أثر مادي، ومثال ذلك هو التوقيع الإلكتروني الذي يسهل ارتكابه ويصعب اكتشاف هوية صاحبه لأنه يتألف من شفرة يمكن تغييرها بسهولة[1]

فجريمة التزوير الإلكتروني يتم اكتشافها بعد مدة من الزمن لأنها جريمة فنية غير ملموسة، لا تظهر أثارها ذلك لأنها تتم من خلال الوصول إلى المعلومات عن طريق النظام المعلوماتي وتغير مضمونها.[2]

ج- جريمة التزوير عابرة للحدود:

بما أن جريمة التزوير تقليدي تتم على دعامة ورقية، فغالبا ما تكون معاملتها داخل دولة واحدة، على عكس جريمة التزوير الإلكتروني التي تتم بواسطة الأنترنت التي أرجعت العالم قرية صغيرة، فهي سهلت التعامل بين الأشخاص فنجد طرف في دولة والطرف الآخر في دولة أخرى، ذلك لأن التعامل يتم بشكل إلكتروني.[3]

د- شخصية المجرم:

شخصية المجرم في جريمة التزوير الإلكتروني هي شخصية تتمتع بقدرة ومهارة ذو كفاءة وخبرة عالية في المجال الإلكتروني حتى يتم تزوير البطاقة، أي أنه شخص فائق الذكاء في النظام التكنولوجي لأن جريمة التزوير الإلكتروني في بطاقة الدفع تعتمد على المعارف التكنولوجية التي فرضها التقدم العلمي، عكس شخصية المجرم في جريمة التزوير التقليدي التي لا تحتاج مثل هذه الثقافة والقدرة على التزوير.[4]

---

[1]- أشرف توفيق شمس الدين، حجية المحررات الإلكترونية في الاثبات، **ورقة عمل مقدمة في ندوة المعاملات القانونية.**

[2]- سعود بن محمد السراني، فعالية الأساليب المستخدمة لإثبات جريمة التزوير الالكتروني، **أطروحة دكتوراه**، جامعة نايف العربية، الرياض، السعودية، 2009، ص 66.

[3]- الطاهر برهوم، جرائم التزوير الالكتروني، **مذكرة مقدمة لنيل شهادة ماستر**، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة، الجزائر، 2018-2019، ص 17.

[4]- عبد العزيز سعد، **المرجع السابق**، ص 14.

2-أوجه التشابه:

بالرغم من الاختلاف الموجودة بين الجريمتين، إلا أن هناك تشابه بينهما والمتمثل في السلوك المجرم وهو تغيير الحقيقة الموجودة في المحرر.

كذلك يشتركان في القصد ففيه الجاني في كلتا الجريمتين هو إلحاق الضرر بالغير.

أيضا المعلومات التي يتضمنها المحرر في كلتا الجريمتين هي بيانات تصلح لتكون دليلا للإثبات.

المبحث الثالث:

الأساس القانوني لحماية بطاقة الدفع الإلكتروني من التزوير

بما أن استعمال بطاقات الدفع الإلكتروني أصبح منتشرا كثيرا في وقتنا الحالي، فهي أصبحت أكثر عرضة للاعتداءات والجرائم الماسة بها، مثل جريمة التزوير، الأمر الذي دفع المعنيين في هذا المجال إلى الحد من هذه الاعتداءات، واستوجب وضع أساس قانوني لحماية بطاقات الدفع الإلكتروني سواء على المستوى الدولي أو الوطني والمقارن.

لذا سنتناول في هذا المبحث الأساس القانوني لحماية بطاقات الدفع الإلكترونية من التزوير على المستوى الدولي **(المطلب الأول)** وعلى المستوى الوطني والمقارن **(المطلب الثاني)**.

المطلب الأول:

على المستوى الدولي

هناك العديد من الأطر القانونية التي تهدف إلى حماية بطاقات الدفع الإلكترونية من التزوير، من أبرز هذه الأسس ما يلي:

الفرع الأول: المنظمة الدولية للشرطة الدولية الأنتربول

تأسست هذه المنظمة الدولية في 07 سبتمبر 1923 من طرف الدكتور "جاهانوسويرا" مدير شرطة فينا في المؤتمر الدولي الثاني، مقرها ليون بفرنسا من أجل تسهيل التعاون بين أجهزة الشرطة في مختلف البلدان لمكافحة الجريمة عبر الحدود، والتي تشمل المجالات التالية: الأمن العام، الإرهاب، الإجرام المنظم لجرائم المخدرات، الإجرام المالي المتعلق بالتكنولوجيا الحديثة.[1]

[1]– نجاح محمد فوزي، **وعي المواطن العربي اتجاه جرائم الاحتيال**، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 152.

تعد المنظمة الدولية للشرطة الدولية المعروفة بالأنتربول أكبر منظمة دولية في العالم ناشطة في مجال مكافحة الجريمة، نظرا لما تقدمه من إمكانيات للقبض على مرتكبي الجرائم بمختلف أنواعها أينما وجدوا وتسليمهم إلى الهيئات المختصة، حيث يعتبر الإجرام المالي من الجرائم التي يجري التركيز عليها من طرف هذه المنظمة.[1]

كما يقتصر دورها في مواجهة جرائم تزوير بطاقات الدفع الإلكتروني من خلال تنظيم السكريتارية العامة الخاصة بمؤتمراتها الدولية، بخصوص الاحتيال والغش اللذان يهددان نظام بطاقات الدفع الإلكتروني في أكتوبر 1994 والذي نتج عنه توصيتين هما:

1- على الدول الأعضاء مراجعة تشريعاتها وقوانينهـا الخاصة ببطاقات الدفع الإلكتـروني، بما يضمن تجريم كل فعل يتضمن تصنيع أو امتلاك معلومات غير قانونية تم الحصول عليها بطريقة غير مشروعة.

2- إنشاء مجموعات عمل بوليسية من خبراء الاحتيال الدولية التابعين لبوليس هونغ كونغ، والشرطة الكندية، والخدمة السرية الأمريكية، وخدمة الاستخبارات القومية الجنائية نيوزيلاندا، ومندوبي من منظمات بطاقات الدفع الإلكتروني لمكافحة هذا النوع من الجرائم من خلال وضع أسس خاصة يتبادل المعلومات للحد منها.[2]

وفي نفس العام 1999 قام الأنتربول أيضا بتوقيع اتفاقيات مع المنظمات التي تهدف لحماية البطاقات، وهي أمريكان إكسبرس، ماستر كارد الدولية والفيزا الدولية، وذلك بهدف التعاون لمواجهة جرائم بطاقات الدفع الإلكتروني.

الفرع الثاني: اتفاقية بودابست

اتفاقية بودابست هي أول المعاهدات الدولية التي تكافح جرائم الأنترنت، والحد منها خاصة بعد أن وصلت إلى حد خطير أصبح يهدد حياة الأشخاص والممتلكات[3]. تم توقيعها

---

[1]- نوال حاج مخناش، " التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني "، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01، أفريل 2009، ص ص 1118، 1135.

[2]- محمد علي سليمان، عباس طالب زروقي، " الأساس القانوني لحماية بطاقة الائتمان من التزوير "، **مقال منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية**، العدد 02، 2015، ص ص 127، 128.

[3]- منير محمد الجنيهي، ممدوح الجنيهي، **جرائم الأنترنت والحاسب الآلي، ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، 2004، ص ص 96، 100.

في 23-11-2001، حيث وقعت عليها 26 دولة من أعضاء المجلس الأوروبي، بالإضافة إلى الدول التالية: كندا، اليابان، جنوب إفريقيا، الولايات المتحدة الأمريكية بهدف تعزيز التعاون بين الدول في مكافحة الجرائم.

تضمنت الاتفاقية عدة مواد تناولت أوجه الإجرام المعلوماتي إذ عرفت المادة 07 منها التزوير الإلكتروني بأنه: إدخال أو تعطيل أو محو أو شطب، سواء ارتكب بقصد أو بدون وجه حق المساس بالمعطيات الإلكتروني، والحصول على المعلومات الصحيحة، واستعمالها بطريقة غير مشروعة.[1]

أما المادة 08 من هذه الاتفاقية فقد نصت على: يجب كل طرف أن يتخذ الإجراءات التشريعية، أو أي إجراءات أخرى التي يرى أنها ضرورية لتجريم أي فعل يتسبب في إحداث ضرر مالي للغير عن طريق ما يلي:[2]

- الاتلاف أو التلاعب ببيانات الحاسب الآلي.
- الغش الإلكتروني من أجل الحصول على منفعة لمرتكب هذا الفعل فاتفاقية بودابست تعتبر بمثابة أساس قانوني يكفل حماية البطاقة الإلكترونية، وأجهزة السحب الآلي من التحايل.[3]

الفرع الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي خطوة لمكافحة الجرائم الإلكترونية في الدول العربية، تم توقيعها في 2010 من طرف الدول العربية، تم اعتمادها في 2012 بهدف حماية المجتمع العربي من الجرائم التقنية والحد من خطرها للحفاظ على الأمن العربي من الناحية المعلوماتية، ووضع إطار قانوني موحد بين الدول العربية لمكافحة الجرائم وتعزيز التعاون بينهم في هذا المجال، كما تسعى أيضا إلى حماية الأمن سيبيراني من خلال وضع أسس قانونية تهدف إلى القضاء على الحوادث الإلكترونية.

---

[1]- المادة 07 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001/11/23 مجلس أوروبا مجموعة معاهدات الأوروبية 1985.

[2]- المادة 08 من اتفاقية بودابست، **المرجع نفسه.**

[3]- محمد علي سليمان، عباس طالب زروقي، **المرجع السابق**، ص ص 128، 129.

ومن خلال تحليل نصوص الاتفاقية العربية نجد أنها قد جرمت الاعتداءات الواقعة على البيانات والمعلومات بصفة عامة وجريمة التزوير بصفة خاصة، حيث نصت المادة 10 على أن التزوير المعلوماتي هو: استعمال وسائل تقنية من أجل تغيير الحقيقة في المعلومات، تغييرا من شأنه إحداث ضرر بغرض استعمالها كمعلومات صحيحة.[1]

كما نصت المادة 18 منها على الاستخدام الغير المشروع لوسائل التزوير المعلوماتي في مجال بطاقات الدفع الإلكتروني وجاءت كما يلي:[2]

- كل من زور أو اصطنع أو وضع أي أجهزة تساعد على تزوير أي أداة من أدوات الدفع الإلكتروني.
- كل من استولى على أداة من أدوات الدفع الإلكتروني.
- كل من استخدم الشبكة الآلية بدون حق من أجل الحصول على بيانات أدوات الدفع.

وبالتالي نستنتج أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي خطوة هامة لمكافحة الجرائم الإلكترونية في الدول العربية.

المطلب الثاني:

الأساس القانوني لحماية بطاقة الدفع الإلكتروني من التزوير على المستوى الوطني والمقارن

حماية بطاقات الدفع الإلكتروني تعد من أهم القضايـــا المهمة على المستـــوى الوطني، لذلك يتطلب الأمر وضع أسس قانونية لحماية بطاقات الدفع الإلكتروني من طرف بعض التشريعات الوطنية والمقارنة منها التشريع الجزائري، الفرنسي والمصري.

[1]– مرسوم سلطاني، رقم 2015/5، الصادر في 17 من جمادى الأولى لسنة 1436 هـ الموافق لـ 8 مارس سنة 2015، ج.ر، عدد 193، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ص 05.

[2]– المادة 18 من اتفاقية بودابست، **المرجع السابق**.

الفرع الأول: التشريع الجزائري

تناول التشريع الجزائري حماية بطاقات الدفع الإلكتروني من التزوير في بعض النصوص القانونية منها:[1]

- تضمن القانون 09-04 المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي نص في المادة الأولى منه على أن الهدف الذي وضع من أجله هو وضع قواعد خاصة للحماية من هذه الجرائم المنتشرة في العصر التكنولوجي الحالي.
- كما أنشأ هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والذي يتمثل دورها في تنشيط عمليات الوقاية من الجرائم.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات.
- كما نجد أيضا القانون الخاص بحماية الملكية الفكرية في الجزائر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة في الفصل الخاص بالخدمات المحمية في المادة الرابعة الفقرة الأولى التي أشارت إلى برامج الحواسيب ضمن نطاق الملكية الفكرية الذي يعاقب على التعدي عليها من طرف الغير دون رخصة مالكها الأصلي.

كذلك نجد قانون التوقيع والتصديق الإلكتروني رقم 15-04 من القوانين التي أقرت حماية التوقيع الإلكتروني، لأنه يعد من أحد مكونات بطاقة الدفع الإلكتروني، حيث عرفت المادة 02 من هذا القانون التوقيع الإلكتروني بيانات إلكترونية متصلة بيانات أخرى تستعمل كأداة للتوثيق.[2]

---

[1]- المادة 1/4 من الأمر رقم 05/03 المؤرخ في 19-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، رقم 44، المؤرخة في 23-07-2003.

[2]- المادة 02 من قانون التوقيع الالكتروني، رقم 15-04، المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني.

كما نصت المادة 394 مكرر المضافة بموجب القانون رقم 06-03 المؤرخ في 20 ديسمبر 2006 على: "مصادرة الأجهزة المستعملة والبرامج والوسائل مع إلحاق ذلك بغلق المواقع، وكذا أماكن الاستغلال شرط أن تكون الجريمة قد ارتكبت بعلم مالك تلك المحلات".[1]

الفرع الثاني: التشريع الفرنسي

تناولت فرنسا موضوع جريمة تزوير بطاقات الدفع الإلكتروني في عدة قوانين هي:

- القانون رقم 88/19 المتعلق بالغش المعلوماتي الذي تناول مادتان تتناولان استعمال مستندات إلكترونية مزورة جاء فيهما ما يلي:[2]
- المادة 5/462 التي نصت على "يعاقب بالحبس من عام إلى خمسة أعوام، والغرامة من عشرين ألف فرنك حتى مليون فرنك كل من قام بتزوير المستندات المعالجة آليا التي من شأنها تحدث ضرر للغير.
- والمادة 6/426 التي تنص على تطبيق العقوبات الواردة في المادة 5/146 على كل من استعمل المستندات المزورة المعالجة آليا كان عالما بتطبيقها.
- جرم المشرع الفرنسي في المادة 11 من القانون رقم 1382/91 الصادر في 30 ديسمبر 1991 بعض صور الاستعمال غير المشروع لبطاقات الدفع الإلكتروني، وهي تقليد أو تزوير بطاقة من بطاقات السحب أو محاولة استعمال البطاقة المقلدة أو المزورة.[3]
- وبعد صدور قانون العقوبات الفرنسي الجديد في 1992/12/16 قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا

---

[1]- تنص المادة 394 مكرر 6 على أنه: "مع الاحتفاظ بحقوق الغير يحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة".

[2]- إيهاب فوزي، مرجع سابق، ص ص 326، 327.

[3]- صليحة مرباح، النظام القانوني لبطاقة الائتمان، **رسالة ماجستير**، فرع قانون الخاص، جامعة الجزائر، 2005-2006، ص ص 121، 122.

واستعمالها، والاكتفاء بإضافته إلى جريمة التزوير العادية، وذلك بتعديل المادة 1/441 من الكتاب الرابع من قانون العقوبات.[1]

- وقد تواصلت جهود المشرع الفرنسي في هذا المجال بشكل مكثف بعد تصديق فرنسى في 23 نوفمبر 2001 على الاتفاقية الأوروبية الخاصة بالجرائم الإلكترونية عام 2001، فقامت بتعديل تشريعاتها النهائية مع هذه الاتفاقية لتتجاوب مع أحكامها، كذلك قامت باستخدام مجموعة أخرى من نصوص قانونية أخرى خاصة لمواجهة الجريمة الإلكترونية أهمها القانون رقم 1062/03 المتعلق بالأمر اليومي المؤرخ في 2001/11/15[2] والقانون رقم 204/04 المتضمن مواكبة العدالة لتطورات الإجرام.[3]

كما نظم قانون العقوبات الفرنسي كل من التزوير التقليدي والإلكتروني من خلال وضع نص عام يمكن من خلاله المعاقبة، وهذا ما جاء في المادة 1/1441 كما يلي: كل تغيير في الحقيقة من شأنها أن تحدث ضررا بأي وسيلة كانت، سواء في محرر أو أي سند والذي من الممكن أن يكون له في إنشـــاء دليل على حق أو فعـــل تكون له نتائــج قانونية، وبالتالي ينطبق هذا النص على بطاقات الدفع الإلكتروني كون البطاقة عبارة عن مستند مُعد أو قادر على إقامة دليل على حق.[4]

كما استحدث المشرع الفرنسي إجراءات تحري للكشف عن الجرائم الإلكترونية كاعتراض المراسلات والتسرب والتحفظ والكشف عن المعطيات المشفرة.

الفرع الثالث: التشريع المصري

عالج المشرع المصري مسألة التزوير بموجب أحكام العقوبات من خلال المواد من 211 إلى 227 الواردة في الباب السادس من الكتاب الثاني[5]، حيث نصت المادتين 211

---

[1]– عبد الفتاح بيومي حجازي، **الدليل الجنائي في جرائم الكمبيوتر والأنترنت**، دار الكتب القانونية، مصـــر، 2008، ص 143.

[2] –loi N2001,1062,15nov-2001 relative a la sécurité quotidienne. JORF 16 Nov-2001, P 18. 215.

[3] –loiN:2004-239,18mars2003 pour la sécurité intérieure, JORF 19 mars 2004, P 4567.

[4]– محمد علي سليمان، عباس طالب زروقي، **المرجع السابق**، ص 131.

[5]– القانون رقم 58 لسنة 1937 المتضمن قانون العقوبات المصري المعدل بتاريخ 02 أفريل 2018.

إلى 213 عن طرق التزوير سواء في المحررات الرسمية والعرفية، كما عاقب المشرع المصري على المساس والاعتداء على سلامة البيانات والمعلومات الموجودة في النظام المعلوماتي، وذلك بموجب المادة 17 من القانون رقم 175 لسنة 2018 بشأن جرائم تقنية المعلومات التي نصت على أنه: يعاقب بالحبس مدة 8 تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه و8 تتجاوز خمسمائة ألف حنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو ألغى كليا أو جزئيا، بدون وجه حق البيانات المخزنة على نظـــام معلوماتي، مهما كانت نوع الوسيلة المستعملة في ارتكاب الجريمة.[1]

كما نظم قانون التوقيع الإلكتروني رقم 15 لسنة 2004 التعامل في المحررات الإلكترونية، حيث تم من خلاله تجريم التزوير الواقع على التوقيع الإلكتروني، وكذلك تزوير شهادة اعتماد التوقيع، فالمشرع قد ساوى بين حجية المحرر العادي والإلكتروني في نطاق المعاملات التجارية المدنية والإدارية متى استوفت الشروط القانونية والضوابط الفنيـة والتقنية، وبالتالي نستنتج أن الكتابة الإلكترونية تتساوى مع الكتابة العادية من حيث الحجيـة، وعلى هذا الأساس فقد جرمت كل الأفعال الماسة بصحة التوقيع بصورة عامة والتزوير الواقع عليه بصورة خاصة، فقد نصت المادة 23 على أنه: "مع عدم الاخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات، أو أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:[2]

- أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.
- أتلف أو عيب توقيعا أو محررا إلكترونيا، أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو بأي طريقة أخرى.
- كل من استعمل توقيعا مزورا مع علمه بذلك.

---

[1]– المادة 17 من القانون المصري رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، المؤرخ في 14 أغسطس 2018، منشور في ج.ر، عدد 32 مكرر، مؤرخة في 14 أغسطس 2018.

[2]– هدى حامد قشقوش، **الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت**، دار النهضة العربية، مصر، د.س، ص 49.

خلاصة الفصل:

في الختام هذا الفصل وما تم توضيحه، يتبين لنا أن بطاقات الدفع الإلكتروني واحدة من أهم التطورات في مجال المعاملات الحديثة لأنها قدمت العـــديد من المـــزايا لمستخدميها، ومع زيادة انتشارها أصبحت مهددة للكثير من الجرائم أهمها جريمة التزوير التي أصبحت كموضوع مهم في العصر الرقمي لأنها جريمة تهدف إلى تحقيق مكاسب مالية غير مشروعة، وخسائر تقع على عاتق الأفراد والشركات، وهذا ما دفع الدول المتطورة إلى مكافحة مثل هذه الجرائم لنجاح استعمال هذه البطاقات كوضع أسس وأطر تهدف إلى حمايتها من المخاطر.

الفصل الثاني

الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير بين التحديات والحلول

الفصل الثاني

الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير بين التحديات والحلول

جريمة تزوير بطاقات الدفع الالكترونية تعد من أخطر الجرائم المالية المعاصرة، ذلك لما تنطوي عليه من تهديد يقع على أمن التعاملات الرقمية، مما يستدعي ذلك اتخاذ إجراءات فعالة للحد منها ومواجهتها، حيث تقتضي الدراسة في هذا الفصل حول ذكر مختلف الإجراءات المتخذة لمواجهة هذه الجريمة منها الإجراءات الوقائية **(المبحث الأول)** والإجراءات الردعية للوقاية من جريمة التزوير الواقعة على الدفـــع الالكترونـــي في **(المبحث الثاني)**، وفي **(المبحث الثالث)** تطرقنا إلى التحديات التي تواجه التعاون الدولي في مواجهة التزوير الالكتروني.

المبحث الأول:

الإجراءات الوقائية المتخذة لمواجهة جريمة التزوير الواقعة على بطاقات الدفع الالكتروني

أمام تزايد الاعتداءات التي تتعرض إليها بطاقات الدفع الالكتروني، وجب اتباع مجموعة من الإجراءات الوقائية للحد منها والمحافظة على أمن وسلامة التعاملات المالية لأنها تسبب خطورة بالغة لما تسببه من خسائر في المجال المالي، وهذا ما دفع الهيئات الدولية والبنوك بالنهوض لحماية البطاقات، لذلك سوف نتطرق في هذا المبحث إلى تبيان دور كل من الهيئات الدولية والبنوك **(المطلب الأول)**، وإضافة إلى ذكر دور كل من صاحب البطاقة، والتاجر، والجهاز الأمن في اتخاذ الإجراءات اللازمة للقضاء على جريمة التزوير **(المطلب الثاني)**.

المطلب الأول

دور الهيئات الدولية والبنوك في حماية البطاقات من جريمة التزوير

أدى الانتشار الواسع لبطاقات الدفع الالكتروني إلى تسهيل المعاملات المالية، ومع تزايد في استخدامات ظهرت تحديات أمنية خطيرة تتعلق بعمليات التزوير مما شكل تهديد حقيقيا لسلامة الأنظمة المالية، مما استدعى تدخلا فاعلا من قبل الهيئات الدولية لضمان حماية بيانات المستخدمين وعمليات تهم المالية.

لذلك سوف نتطرق في هذا المطلب إلى تبيان دور كل من الهيئـــات الدولية في **(الفرع الأول)**، ودور البنوك **(الفرع الثاني)**.

الفرع الأول: دور الهيئات الدولية

اتخذت الهيئات الدولية عدة إجراءات بغية الاستعمال الأمثل لبطاقات الدفع الالكتروني وحمايتها لكونها هي من يضع هذه البطاقات ويضفي عليها صفة القبول دوليا، مما يسمح

بتداولها والتعامل بها عن طريق الأنترنت وفي حال وقوع أي مشاكل أو تجاوزات فقد تتدخل هذه الهيئات لحلها.[1]

أولا: الإجراءات التقنية لتطوير البطاقة

لم يتم إنشاء بطاقة مكونة من دوائر إلكترونية تجعلها غير قابلة للاختراق، وهذا بفضل المادة المصنوعة بها (PVC)، كما تحتوي أيضا هذه البطاقة على ذاكرة لها القدرة على حفظ العمليات الأخيرة التي تم إجراءها، وكذلك دمج البطاقة الذكية وهي بطاقة بلاستيكية حجمها كحجم بطاقات الدفع الأخرى، حيث تتميز هذه البطاقة بدوائر متكاملة تسمح لها بتخزين ومعالجة البيانات.[2]

كذلك تم استخدام نظام الصفقات الأمنة الذي أعلنت عنه الشركتين العالمتين ماستركارد وفيزا كارد سنة 1996، حيث قامت شركة ماستر كارد العالمية بطرح بطاقة "ماستركارد باي إباس" عام 2002، التي تعتبر برنامج دفع دون اتصال حيث يتم بواسطة تقنية متطورة فيقوم العامل بتمريرها قرب جهاز إلكتروني مهيأ لهذا الغرض، وبعد إرسال هذه البطاقة معلومات الدفع لاسلكيا وبعد معالجة العملية يستلم الحامل إشارة بتأكيد الدفع.[3]

إضافة إلى ذلك فقد قامت الشركات العربية بإصدار بطاقات مماثلة، حيث أعلنت شركة "دوت عوم" عن إصدار البطاقة الالكترونية بمسماة ماستر كارد، والتي توفر لحاملها خدمات البيع والشراء عبر الأنترنت بثقة وبصورة أمنة دون أي مخاطر.[4]

---

[1]– عبد الكريم الردايدة، **جرائم بطاقة الائتمان**، دار حامد للنشر والتوزيع، عمان، 2013، ص 179.

[2]– علي عدنان الفيل، **المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الالكتروني (دراسة مقارنة)**، المؤسسة الحديثة للكتاب، لبنان، 2011، ص ص 76، 77.

[3]– **المرجع نفسه**، ص 77.

[4]– أمجد حمدان الجهني، **المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني**، دار المسيرة، عمان، 2010، ص 115.

ثانيا: تصميم البرنامج

قامت الهيئات الدولية بإنشاء العديد من البرامج لمكافحة جريمة تزوير بطاقات الدفع الإلكتروني والحد من الاعتداءات التي تتعرض عليها بسبب تطور أساليبها التقنية، من أبرز هذه البرامج:

1- برنامج التقييم:

هو أحد البرامج التي وضعتها الهيئات الدولية هدفه هو فحص حسابات حاملي بطاقات الدفع بالاعتماد على تعليمات خبراء مكافحة الاحتيال المزودة بها ثم عزل الحسابات التي يثبت بأنها تتم بطرق احتيالية.[1]

2- برنامج الاختيار:

والذي يظهر من خلال الحسابات التي تستخـــدم هذه البطاقـــات بصفـــة غير شرعية، ومن ثم عدم إتمام التعامل بها.

3- برنامج نظم المعلومات الارشادية:

والذي تعمل على مراقبة أساليب الغش والاحتيال التي قامت المؤسسة البنكية في بريطانيا بتطويرها.[2]

4- برنامج الشبكة العصبية:

الذي يتم من خلاله رصد جميع التعاملات المتخذة بواسطة بطاقات الدفع، والكشف عن المشكوك في صحتها وإعادة فحصها.

5- برنامج نظم المعرفة:

يعمل هذا البرنامج على إيقاف البطاقات التي يكشف أن تعاملاتها غير شرعية، وذلك من خلال وسائلها الفعالة للكشف عن التهديدات من طرف المجرمين.

---

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

[2]- أمجد حمدان الجهني، **المرجع السابق**، ص 115.

الفرع الثاني: الإجراءات الوقائية المتخذة من قبل البنوك للحد من جريمة التزوير

تتخذ البنوك مجموعة من الأساليب الوقائية للحد من جريمة التزوير وذلك بتوفير الحماية التامة للحسابات التي تخص عملائهم لتحقيق الأمان ومنع التلاعبات التي تقع عليها، من خلال جملة من الإجراءات الرقابية(**أولا**)، والإجراءات الإدارية(**ثانيا**)، وأخرى تقنية(**ثالثا**).

أولا: الإجراءات الرقابية

تخضع البنوك في أداء مهامها إلى قواعد تنظيمية داخلية يتولى تنظيمها البنك المركزي من حيث إجراءات الإشراف والرقابة والتوجيه، وهذا بهدف الحفاظ على أموال العملاء وتتجلى هذه الرقابة في التوجيهية (**1**)، والداخلية (**2**)، والخارجية (**3**)، والزجرية (**4**):

1-الرقابة التوجيهية:

تعد من أهم الأدوات التي تستخدمها المؤسسات المصرفية للحد من جرائم التزوير وذلك من خلال التي تواجهها عن طريق دراستها ثم تقديم الاقتراحات المناسبة لها، وتحديد قواعد تسيير العمل المصرفي، كما أن للبنك المركزي سلطة توجيه التعليمات والمطالبة الالتزام بالتقيد بمحتواها، وتوجه هذه التعليمات إلى كافة البنوك والمؤسسات المالية في الدولة وإلزامها باحترامها وتنفيذها.[1]

2-الرقابة الداخلية:

هي الإجراءات التي تنتهجها الإدارة بغرض تقييد هذه البنوك والمؤسسات بالسياسة الموضوعة من طرفها، والتأكد من الأداء الدقيق لعمل البيانات المالية ومنع الغش، ويقوم بذلك أشخاص توظفهم الإدارة بعد التأكد من كفاءاتهم المهنية، تطبق هذه الرقابة من خلال جزء من صلاحيات النظام الداخلي لأداء الرقابة على الحسابات والتي تختص بحماية الصور والسجلات لضمان دقة البيانات.[2]

---

[1]- حسين محمد الشلبي، محمد مهند فايز الدويكات، **التزوير والاحتيال بالبطاقات الائتمانية**، دار مجلاوي للنشر والتوزيع، عمان، 2009، ص ص 100، 102.

[2]- **المرجع نفسه**، ص 103.

3-الرقابة الخارجية:

وهي الرقابة التي تمارس من جهات مستقلة عن البنك بفحص ومراجعة البيانات الختامية للبنوك، وأيضا مراقبة سلامة النظام الداخلي ومراجعة الرقابة الداخلية وإبلاغ إدارة البنك والسلطات المصرفية عن أي ملاحظة من شأنها مخالفة القوانين المعمول بها.[1]

4-الرقابة الزجرية:

وهي الرقابة التي تعتمد على ردع من خلال العقوبات الصارمة، المطبقة على من يخالف الأنظمة، يقوم بهذا 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 عملية فحص الأوضاع الإدارية والمالية والتأكد من أن رأس المال مناسب للسيولة والتأكد أيضا من فعالية الوسائل المتبعة في الرقابة الداخلية ووسائل الإدارة.[2]

ثانيا: الإجراءات الإدارية

تعد الإجراءات الإدارية جزءا أساسيا من منظومة الحماية في البنوك تتخذ داخل البنك لضمان سلامة العمليات المصرفية لمنع التزوير في بطاقات الدفع الالكترونية، تتمثل هذه الإجراءات في تعيين حد أقصى لاستخدام البطاقة الالكترونية **(1)** أو سحبها **(2)** أو المعارضة في قبولها **(3)** وهذا ما سنبينه فيما يلي:

1-تحديد سقف لعمليات السحب بالبطاقة:

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

---

[1]- عبد الكريم الردايدة، **المرجع السابق**، ص 101.

[2]- حسين محمد الشلبي، محمد مهند فايز الدويكات، **المرجع السابق**، ص ص 102، 103.

[3]- بيار إميل طوبيا، **بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها**، منشورات الحلبي الحقوقية، بيروت، 2000، ص 40.

أ-الحد الأقصى لاستخدام البطاقة في السحب:

يتم تحديد السقف الأقصى للبطاقة عند السحب من أجهزة الصراف الآلي حسب مبلغ المسموح به من الرصيد، ففي بطاقات الدفع العادية يكون نصف سقف البطاقة، وفي البطاقات التي تستخدم في الوفاء يكون نفس الرصيد المتوفر في الحساب، وفي حالة السحب اليومي فإن الحد الأقصى للسحب يختلف من بنك لآخر حسب التسهيلات التي يمنحها كل بنك لعملائه.[1]

ب-الحد الأقصى لاستخدام البطاقة في الوفاء:

وفي هذه الصدد تمييز 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 الحالة المخصصة له على الفاتورة لأنه لا يعلم برصيد البطاقة.
- عند استخدام البطاقة في الجهاز الالكتروني ومن خلال تمرير البطاقة في الجهاز يظهر على الشاشة ما إذا كانت تحتوي على رصيد كافي لإتمام عملية الوفاء أم لا، فإذا تجاوز حد الرصيد يرفض الجهاز وإتمام هذه العملية إلا بعد حصول التاجر على تفويض من مصدر البطاقة.[2]

2-سحب البطاقة:

قد يتم سحب البطاقة الإلكترونية من طرف المصدر أو من طرف التاجر حفاظا على جميع حقوق الأطراف.

أ-سحب البطاقة عن طريق المصدر:

للبنك الحق في استرجاع البطاقة من صاحبها بالنص على ذلك في العقد وذلك بأن البطاقة ملك لمصدر البطاقة، حيث يستطيع هذا الأخير الطلب من صاحبها إعادتها أو إلغائها، وهذه العملية تعتبر عملية قانونية إذا كانت عن أسباب جوهرية، إما إذا انعدمت

---

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

[2]- خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الإلكترونية، **مذكرة مكملة لنيل شهادة الماستر في الحقوق**، تخصص قانون جنائي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2014-2015، ص 50.

هذه الأسباب فهذا يعتبر تعسف من قبل مصدر البطاقة ووجب التعويض عنها، وقد يكون هذا السحب سواء بالطريقة العادية عندما يطلب المصدر إرجاع البطاقة، وقد يكون بطريقة فنية في حالة برمجة الصراف الآلي على سحبها.[1]

ب-سحب البطاقة عن طريق التاجر:

ينشأ اتفاق بين مصدر البطاقة بصفته مالكا مع التاجر بصفته وكيلا على القيام بسحب البطاقة وإرجاعها للمصدر مقابل مكافأة على كل بطاقة مسحوبة، وذلك لتشجيعهم على مكافحة جريمة التزوير ويقوم التاجر بسحب لبطاقة في حالات عدة، كأن تكون البطاقة ضمن قائمة البطاقات التي ورد رقمها في الكشف الدوري التحذيري الذي تم توزيعه على التجار، أو أن يكون يعرف التاجر صاحب البطاقة ولكن تم استخدامها من قبل الغير والشك في كيفية وصور إليه .[2]

3-المعارضة في قبول البطاقة:

تعد إجراء وقائي يعمل على عدم قبول البطاقة في عمليات الوفاء، وهذا في حالة سرقتها أو فقدانها أو أي سبب آخر، غير عادي بهدف حمايتها من الأفعال غير مشروعية.

وعملية المعارضة قد تصدر من قبل صاحبها عندما يكون فقدها أو سرقت منه، كذلك قد تصدر من طرف الجهة المصدرة عندما يتم إلغاؤها.

ويمكن تعريفها على أنها نظام يعمل على توزيع رقم البطاقة عن طريق نشرات تحذير بصفة دورية، وتقديمها للتجار الذين يتعاملون بها في عمليات الوفاء والطلب منهم عدم قبولها في معاملاتهم سواء المتعاملين بالجهاز اليدوي أو الجهاز الالكتروني.[3]

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، وبتالي يتم قبولها إذا كانت مخالفة لهذه الأرقام وفي الحالة تطابقها

---

[1]- وسام فيصل محمود الشواوة، **المسؤولية القانونية عن الاستخدام غير المشروع لبطاقات الائتمان**، دار وائل للنشر، عمان، 2013، ص 116.

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

[3]- **المرجع نفسه**، ص 119.

مع أحد الأرقام يتم رفضها، 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.[1]

ب-نشر المعارضة لدى التجار المزودة بالجهاز الالكترونية:

يتم تزويد هؤلاء التجار بشكل إلكتروني لدى التاجر، موصول بجهاز المصدر بأرقام البطاقات المرفوضة، حيث بمجرد تمرير البطاقة عليه يتحدد تلقائيا ما إذا كانت مقبولة أو مرفوضة.[2]

ثالثا: الإجراءات التقنية

اتخذت البنوك العديد من الإجراءات التقنية للحد من جريمة التزوير التي تتعرض إليها البطاقات الالكترونية من أبرزها:

- 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.
- استخدام كلمات سرية معقدة للدخول إلى الأنظمة الالكترونية بحيث تكون مزيج من الأرقام والحروف يصعب إيجادها.[3]
- التحديث الدائم والمتجدد لشيفرة البطاقات الالكترونية حتى يصعب على المحتالين التعرف عليها.

المطلب الثاني:

الإجراءات المتخذة من قبل صاحب البطاقة والتاجر والجهاز الأمني

للحد من جريمة التزوير الواقعة على بطاقات الدفع الالكترونية لابد من أن يتخذ كل من صاحب البطاقة احتياطات اللازمة تمنع التلاعب بها ووقوعها في يد الغير وهذا ما

---

[1]- خولة بوقديرة، **المرجع السابق**، ص 51.

[2]- علي عدنان الفيل، **المرجع السابق**، ص 82.

[3]- **المرجع نفسه**، ص 82.

سنبينه في **(الفرع الأول)**، كذلك يجب على التاجر أن يأخذ حذره أثناء التعامل بالبطاقة وهو ما سنتناوله في **(الفرع الثاني)**، ومن جهة أخرى يجب على الجهاز الأمني أن يتدخل هو الأخير مجموعة من التدابير الوقائية لمحاربة جريمة التزوير وهذا ما يتم دراسته في **(الفرع الثالث)**.

الفرع الأول: الإجراءات الوقائية المتخذة من قبل صاحب البطاقة

من أجل الحفاظ على البطاقة الالكترونية يقوم صاحب البطاقة بمجموعة من الإجراءات تتمثل في حماية البطاقة والبطاقة والمحافظة على بياناتها **(أولا)**، حماية البطاقة من خلال المعاملات التجارية **(ثانيا)**:

أولا: حماية البطاقة والمحافظة على بياناتها

فعلى صاحب البطاقة التخلي بعدم إهمالها والحرص على وضعها في مكان آمن، وألا يتركها عند أي شخص إلا بعد التأكد من هويته، كما يجب عليه بعدم الإفصاح عن رقم البطاقة أمام الغير أو كتابته على وجه البطاقة أو على أي ورقة مكشوفة، وأن يتلف الوصل في حالة طلبه من الصراف لأنه يحتوي الصراف لأنه يحتوي على رقمه، كذلك يجب على صاحب عند تشكيله للرقم السري أن يختار أرقاما وحروفا يصعب اكتشافها.[1]

وفي حالة ضياعها يجب على صاحبها الإبلاغ الفوري للجهة المصدرة لها، والذي تقوم بإلغائها بناءا على هذا البلاغ، إضافة إلى ذلك يجب على صاحب البطاقة الإبلاغ في حالة إيجاد جهات لم يتعامل معها من خلال وصل كشوفات الحساب، حيث تقوم الجهة المصدرة بالتحقق من هوية هذه الجهات التي استخدمت البطاقة.[2]

كذلك يجب عليه الحرص على عدم شحن رصيد بطاقته مبالغ كبيرة ليتجنب لخسارة في حالة استخدامها من الغير، وإذا لاحظ هنا لأمن يراقبه أثناء إجراء عملياته المصرفية فهي أن يقوم بإلغاء هذه العملية والانتقال لجهاز آخر تجنب للوقوع في أي تلاعب بها.[3]

---

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

[2]– علي عدنان الفيل، **المرجع السابق**، ص 84.

[3]– أمجد حمدان الجهني، **المرجع السابق**، ص ص 122، 123.

ثانيا: حماية البطاقة من خلال المعاملات التجارية

حماية بطاقات الدفع الالكتروني من التزوير في المعاملات التجارية، تعد من الأمور الحيوية لضمان أمن البيانات وحماية المستهلكين والتجار.

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

1-الحالة العادية:

لحماية بطاقات الدفع الالكتروني في المعاملات التجارية في الحالة العادية يمكن اتخاذ عدة إجراءات أهمها:

- يحرص صاحب البطاقة أن يتسوق في أماكن آمنة، كما يجب عليه التأكد من السلعة المراد سراؤها بمعاينتها والتأكد من سعرها الحقيقي ثم كيفية الحصـــول عليها، إضافة إلى التحقق من هوية ومصداقية التاجر وأيضا مطالبته بكافة الضمانات قبل إجراء المعاملة وأن يتحقق من وصل الشراء قبل توقيعه، كما يجب عليه الاحتفاظ بكافة الوثائق التي تثبت إجراء المعاملة، كذلك يجب الإبلاغ في البنك أو الشرطة، في حالة إذا لم تسترد البطاقة من الجهاز، أو إذا لاحظ صاحبها أشياء غير عادية كأجهزة غير عادية كأجهزة غريبة متصلة مثلا.[1]

2-حالة المعاملات عبر الأنترنت:

يعتبر التعامل عبر الأنترنت أحار بكثير من نظيره على الواقع لذلك وجب على صاحب البطاقة أخذ جملة من التدابير قبل إجراءه لأية عملية أهمها:

- الحرص على التعامل مع المواقع المشهور والموثقة، وتفادي المواقع غيـر المعروفة، لذلك وجب التأكد من وجود اتصال أمن من خلال وجود كلمة https في بداية عنوان الموقع أو عن طريق التأكد من القفل المغلق أسفل نافذة المتصفح.[2]
- أن يستعمل برامج الحاسوب المشفرة لحماية يريده الالكتروني كما يجب عليه الحفاظ على كلمة السر الخاصة به بالإضافة إلى رفضه الرد على المكالمات والرسائل

[1]- خولة بوقديرة، **المرجع السابق**، ص 56.

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

البريدية وبعض المواقع التي تطلب من صاحب البطاقة رقم البطاقة وتفاصيل من حسابه.

الفرع الثاني: الإجراءات المتخذة من طرف التاجر

يُلزم التاجر بالقيام ببعض الإجراءات قبل التعامل بالبطاقة الالكترونية حتى يضمن سلامتها ومن بينها إجراءات تكون أثناء تنفيذ العملية **(أولا)**، والتأكد من صحة البطاقة **(ثانيا)**، ورفض البطاقات غير صالحة **(ثالثا)**.

أولا: إجراءات أثناء تنفيذ العملية

- عند تمرير البطاقة وظهور عبارة راجع الجهة المصدرة فعلى التاجر التوقف فورا عن تمريريها، والاتصال بالبنك صاحب التفويض للحصول على رمزه وقبول المعاملة.[1]
- التزام التاجر بعدم تسوية أي مديونية بين صاحب البطاقة وغيره من التجار.
- يجب التأكد من هوية صاحب البطاقة من خلال بطاقة توقيعه المدون على الفاتورة بالتوقيع الذي تحمله البطاقة.
- اعتماد رمز التفويض على المعاملة من جهاز التاجر أو مركز التفويض لدى المصدر دون غيرها.[2]
- القيام بإعداد سند المديونية الذي يتمثل في فاتورة وإشعار البيع وما يتضمنه من تاريخ المعاملة وقيمها، والتوقيع عليه من قبل صاحب البطاقة.

ثانيا: التأكد من صحة البطاقة

- يجب أن تكون البطاقة سارية المفعول، وأن تختوي على المبلغ الكافي لقيمة المشتريات، كما يجب أن تكون سليمة من حيث الشـريط الخـاص بالتوقيـع

[1]– وسام فيصل محمود الشواوة، **المرجع السابق**، ص 107.

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

عليها، كما يجب التأكد أيضا من سلامة رقمها والتوقيع الموجود عليها وذلك بمطابقتها مع ما هو مدون في الوصل.[1]

ثالثا: رفض البطاقات غير صالحة

يجب على التاجر رفض التعامل مع حامل البطاقة في حالات معينة، كأن تكون البطاقة مقدمة من قبل الغير، أو أن تكون قد تم التعديل فيها، إضافة إلى البطاقات العالمية التي لا تتضمن علامات ضمان كبطاقة فيزا، وماستر كارد.[2]

الفرع الثالث: الإجراءات الوقائية المتخذة من قبل الأجهزة الأمنية

بما أن جريمة تزوير بطاقات الدفع الالكتروني من أخطر الجرائم الالكترونية، ذلك لما تحمله من تهديد مباشر للأمن، فأصبح من الضروري أن تضطلع الأجهزة الأمنية بدور فاعل وناشط في الوقاية من هذه الجرائم، ولتحقق ذلك فهي تقوم بوضع ضوابط لنشاط الأفراد وحماية النظام العام وسنعرض فيما يلي الإجراءات الوقائية التي ثبتها أجهزة الشرطة وهي الإجراءات المتعلقة بالأفراد والإجراءات المتعلقة بتطوير جهاز الشرطة.

أولا: الإجراءات المتعلقة بالأفراد

وتشمل الإجراءات المتعلقة بالأفراد العاديين **(1)** والأفراد المجرمين **(2)**. الإجراءات الوقائية التي تأخذها الأجهزة الأمنية المتعلقة بالأفراد العاديين تظهر في توعية المواطنين ومستخدمي البطاقات بمختلف المخاطر التي تتعرض إليها، وذلك من خلال لقاءات توعوية وحملات تحسيسية حتى يكونوا على دراية كافية بذلك ومن ثم توفي الحذر عند التعامل بها.[3]

2-الإجراءات المتعلقة بالأفراد المجرمين:

ويظهر دور الشرطة الأمنية في مراقبة وتتبع الأشخاص الخطرين ذو السـوابق العدلية، في هذه الجرائم عن طريق المراقبة الأمنية المستمرة لضبط نشاطاتهم حتى لا يكرروا جرائهم السابقة.

---

[1]- علي عدنان الفيل، **المرجع السابق**، ص 125.

[2]- **المرجع نفسه**، ص 126.

[3]- عبد الكريم الردايدة، **جرائم بطاقة الائتمان، المرجع السابق**، ص 116.

ثانيا: الإجراءات المتعلقة بتطوير جهاز الشرطة

بما أن جريمة تزوير بطاقات الدفع الالكتروني من الجرائم المستحدثة، تتميز بالخصوصية عن بقية الجرائم وكذلك بالنسبة لمستخدميها الذين يتمتعون بالخبرة العالية في مجال تقنية المعلومات فمن الصعب التصدي لها، ولذلك كان لزاما على الشرطة تطوير أجهزتها التقنية، وكذلك أفرادها حتى تكون لهم القدرة على تجاوز هذه الجريمة[1]، ومن أهم هذه الإجراءات نجد ما يلي:

- تأهيل العاملين من أفرادا الشرطة في مجال المكافحة عن طريق ومع برامج تقنية عالية ذات صلة بإجراءات الوقاية من التزوير.[2]
- ضرورة إخضاع أفراد الشرطة لضوابط جدية لجعلهم مختصين في مواجهة هذه الجرائم من حيث الأشخاص المرتكبين لها، وأساليب ارتكابها، وبالتالي القدرة على التحقيق التقني للتعامل مع هذه القضايا.
- تدريب أفراد جهاز الشرطة على كيفية استعمال الأجهزة الالكترونية وأدواتها وآلات الطباعة المخصصة لها ليسهل عليهم اكتشاف ومتابعة جريمة التزوير الواقعة على بطاقات الدفع الالكتروني.[3]
- كما يمكنهم وضع قاعدة بيانات إلكترونية تحتوي على أرشيف جميع الجرائم وبيانات مرتكبيها، ومن ثم تزويد البنوك الوطنية بالمعلومات الكاملة المتعلقة بالعملاء وهو ما يعزز أمن واستقرار البنوك والمؤسسات المصرفية.[4]

---

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

[2]– لينا محمد الأسدي، **مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية**، دار حامد للنشر والتوزيع، عمان، 2015، ص 99.

[3]– محمد فتحي عيد، **الاجرام المعاصر**، دار الحامد للنشر والتوزيع، عمان، 2014، ص 257.

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

المبحث الثاني:

الإجراءات الردعية المتخذة للوقاية من جريمة التزوير الواقعة على بطاقات الدفع الالكتروني

تعد بطاقات الدفع الالكتروني من الوسائل الحيوية التي سهلت عمليات الشـراء والدفع، إلا أنها أصبحت هدفا للعديد من الجرائم الالكترونية أبرزها جريمة التزوير الذي تمس الثقة بالنظام المالي الرقمي، أمام هذا الخطر أصبح من الضروري اتخاذ إجراءات ردعية فعالة للوقاية من هذه الجريمة، وهذا ما سنتعرف عليه في هذا المبحث الإجراءات الكلاسيكية للبحث والتحري عن جريمة التزوير في **(المطلب الأول)**، والإجراءات المستحدثة للوقاية من جريمة التزوير الواقعة على بطاقات الدفع الالكتروني في **(المطلب الثاني)**.

المطلب الأول:

الإجراءات الكلاسيكية للبحث والتحري عن الجريمة

رغم الطبيعة الرقمية لجريمة التزوير الالكتروني، إلا أن الجهات الأمنية لا تزال تعتمد في بداية التحقيق على الإجراءات الكلاسيكية للبحث والتحري عن جريمة التزوير والتي تمثل الأساس في كشف أدلة وملابسات هذه الجريمة، ولتبيان هذه الإجراءات قسمنا هذا المطلب إلى ثلاث فروع **(الفرع الأول)** يتضمن مرحلة البحث والتحري عن الجريمة، أما **(الفرع الثاني)** يتضمن مرحلة التحقيق، لننتقل أخيرا إلى مرحلة المحاكمة في **(الفرع الثالث)**.

الفرع الأول: مرحلة البحث والتحري عن الجريمة

تمثل جريمة تزوير بطاقات الدفع الالكتروني تحديا كبيرا للأنظمة الأمنية في البنوك ومقدمي خدمات الدفع الالكتروني، حيث يصعب أحيانا اكتشـاف التزوير حتى بعـد حدوثه، ولذلك فإن مرحلة البحث والتحري تلعب دورا مهما في الكشف عن المجرمين من خلال جمع الأدلة وتحليلها باستخدام تقنيات متطورة في التدقيقات الرقمية، حيث يكون أفراد الشرطة لهم خبرة في مجال المعلوماتية، لذلك خصصنا الدراسة في هذا الفرع في كيفية تلقي البلاغات والشكاوي **(أولا)**، والبحث والتحري عن الجريمة **(ثانيا)**، إضافة إلى مرحلة تجهيز الوسائل **(ثالثا)**.

أولا: تلقي البلاغات والشكاوي

بما أن جريمة تزوير بطاقات الدفع الالكتروني تتم في وسط إلكتروني، فلا بد أن يكون الشخص المبلغ عن الجريمة على دراية بالأجهزة الالكترونية وتقنياتها حتى تكون المعلومة المقدمة من طرفه واضحة، ومثال ذلك تلقى بلاغ مفاده ضبط أحد الأفراد بحوزته بطاقة دفع مزورة أو يستخدم محررات مزورة.[1]

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

فالتبليغ يعد الخطوة الأولى للكشف عن ملابسات الجريمة حيث تضع الجهات الأمنية كالشرطة تحت تصرف المواطنين مواقع ليتمكنوا من خلالها التبليغ، ومثال ذلك الموقع الالكتروني للدرك الوطني www.ndn.ppgn.dz، وكذلك الموقع الالكتروني للأمن الوطني www.dgsn.dz وللمواطنين الحرية في اتباع هذه الطرق المستحدثة أو التبليغ بالطرق العادية، في حين أنهم ملزمون بتحديد أسماء المشتبه فيهم، والقيام طباعة نسخة ثانية للبيانات المتضررة في الأجهزة.[3]

ثانيا: البحث والتحري

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

---

[1]– علي عدنان الفيل، **إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية–دراسة مقارنة**، المكتب الجامعي الحديث، الموصل، 2012، ص 11.

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

[3]– حسن ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، **أطروحة مقدمة لنيل شهادة الدكتوراه**، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016، ص 218.

الفريق المناسب للبحث والتحري عنها، كما يتم أيضا إنجاز قائمة تحمل أسماء المشتبه فيهم، وتحديد الأسئلة التي سيتم الاستجواب بشأنها.[1]

وبعد إتمام الخطة على المحقق الرئيسي في الجريمة أن يشكل فريق عمل متمكن حتى يستطيعوا الوصول إلى المعلومات المطلوبة ومن ثم توقيف مرتكب الجريمة، يتضمن الفريق مجموعة من الضباط وهم: المحقق الرئيسي، خبراء في الرسم التخطيطي، خبير استشاري.[2]

ثالثا: مرحلة تجهيز الوسائل

ليتم الوصول إلى الهدف الموجود في التحقيق، يجب على المحققين الاستعانة ببعض الوسائل والبرامج لتتبع العمليات من بينها:

- وضع الرموز: تتمثل في تعيين رقم سري معاملة ما، لتتبع معطيات الأنظمة المعالجة من خلال هذه المعاملة.[3]
- تتبع البرامج، يتم من خلال استخدام الرقم السري البرنامج، أو من خلال تشغيل التعليمات الموجودة ضمن البرامج التي يتمكن المحقق من خلالها تشغيل التعليمات الموجودة ضمن البرامج الذي يتمكن المحقق من خلالها تحيين محتوى هذا البرنامج.
- برنامج الاتصالات الذي يعمل على إيصال جهاز المتهم بالجهاز الخاص بالمحقق للحصول على معلوماته.[4]
- برنامج إذن التفتيش الذي يتم من خلاله إدخال البيانات اللازمة لتحديد الأدلة.

---

[1]– خولة بوقديرة، **المرجع السابق**، ص 64.

[2]– حسن ربيعي، **المرجع السابق**، ص ص 221، 223.

[3]– محمود إبراهيم غازي، **الحماية الجنائية الخصوصية والتجارة الالكترونية**، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص ص 704، 705.

[4]– حسام محمد نبيل الشنراقي، **جرائم الاعتداء على التوقيع الالكتروني**، دار الكتب القانونية، مصر، 2013، ص 690.

الفرع الثاني: مرحلة التحقيق

بعد التحري عن الجريمة يقوم ضباط الشرطة القضائية ببعض الإجراءات للإحاطة بمسرح الجريمة من خلال الانتقال للمكان ومعاينة وتفتيش محتوياته، وضبط أي أدلة متعلقة بالجريمة وهذا ما سنوضحه فيما يأتي: المعاينة **(أولا)**، التفتيش **(ثانيا)**، والضبط **(ثالثا)**.

أولا: المعاينة

ويقصد بالمعاينة الانتقال لمكان الجريمة ورؤية آثارها، والإبقاء على حالتها حتى لا يتم إتلافها، تتم في الأماكن العامة أو الخاصة على حد سواء، غير أن في الأماكن الخاصة تحتاج إلى رضا صاحب المكان أو بإذن قضائي، وفي نهاية هذه المرحلة يتم وضع الأختام على ما تم معاينته وتعيين مراقب عليه.[1]

وفي جرائم بطاقات الدفع الالكتروني والجرائم الالكترونية تتم معاينة الأشياء الافتراضية وهي المكونات الموجود داخل أنظمة الحواسيب، ومثال ذلك البرامج والتعليقات والملفات الالكترونية[2]. ومن الإجراءات التي يتم مراعاتها عن إجراء المعاينة ما يلي:

- القيام بتصوير جهاز الحاسب الآلي وما قد يتصل به من أجهزة أخرى.
- القيام بحذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية.
- ربط الأقراص الكمبيوترية التي قد تحمل أدلة مع جهاز يمنع الكتابة عليها مما يتيح للمحققين قراءة بياناتها من دون تغييرها.[3]

ثانيا: التفتيش

التفتيش هو إجراء من إجراءات التحقيق يهدف إلى العثور على الأدلة التي ترتبط مع مراعاة الشروط والضوابط القانونية.

1-الشروط الشكلية والموضوعية:

أ-الشروط الشكلية: ويجب مراعاة الأحكام الآتية:

---

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

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

[3]- فاطمة بوعناد، مكافحة الجريمة الالكترونية في التشريع الجزائري، **مجلة الندوة للدراسات القانونية**، عدد 01، الجزائر، 2013، ص 68.

-**الحضور**: فنجد أن المشروع الجزائري قد أقر حضور بعض الأشخاص عند إجراء عملية التفتيش، لكن مع خصوصية الجرائم الواقعة على النظام الآلي فقد نص المشرع هذه الشروط وذلك بموجب المادة 45 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".[1]

-**وقت إجراء التفتيش**: فموجب المادة 47 الفقرة 3 من قانون الإجراءات الجزائية التي تنص على أنه: "وعندما يتعلق الأمر... أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".[2]

-**محضر التفتيش**: يلزم ضابط التدقيق بتحرير محضر يدون عليه ما توصل إليه خلال عملية تفتيش حيث يجب أن يحتوي على تاريخ تحريره ويجب أن يكتب باللغة الرسمية، وأن تدون فيه كل الإجراءات المتخذة، وفي الأخير يجب أن يوقع عليه من قبل محرره، إضافة إلى أنه يمكن الاستعانة في تحريره بمن يملك الخبرة في مجال تقنية المعلومات.[3]

ب-الشروط الموضوعية: وتتمثل فيما يلي:

-**السبب**: أي أن يكون سبب مقنع يدل على جريمة التزوير، حيث يجب أن تكون الجريمة قد مست بنظم المعالجة الألية للمعطيات، وقد أدرج المشرع الجزائري مجموعة 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.[4]

---

[1]- المادة 45 من القانون 06-22، **المرجع السابق**.

[2]- المادة 47 من القانون 06-22، **المرجع نفسه**.

[3]- رشيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن**، منشورات الحلبي الحقوقية، لبنان، 2012، ص 418.

[4]- القانون 05-15، المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو 1996، المتضمن قانون العقوبات، الجريدة الرسمية، عدد 71، العدد 41، الصادرة بتاريخ 10 نوفمبر 2004.

-**محل التفتيش:** في جريمة التزوير الإلكتروني، يكون التفتيش غالبا ينصب على نظام المعالجة الآلية للمعطيات.

-**السلطة المختصة في التفتيش:** فقد حدد المشرع الجزائري الجهة المختصة بالتفتيش بقاضي التحقيق، وفي بعض الحالات الاستثنائية يتكفل بإجراء التفتيش موظف الضابطة لعدلية وهذا إن كانت الجريمة الالكترونية متلبس بها.[1]

-**الحصول على إذن:** فالأصل يتم التفتيش من قبل المختص بذلك، لكن في بعض الحالات يتم تكليف ضباط من الضابطة العدلية وحتى يباشر مهامه لابد من الحصول على إذن بالتفتيش بالإنابة عن السلطة المختصة ويجب أن يتضمن هذا الإذن مكان التفتيش والشخص والأشياء الأخرى كالأجهزة الآلية.[2]

2-تفتيش المكونات المادية والمعنوية لنظام المعالجة الآلية:

بما أن الجريمة تتم بواسطة جهاز الحاسب فهو الأخير يجب أن يتعرض للتفتيش.

أ-تفتيش المكونات المادية لنظام المعالجة الآلية: تتمثل المكونات المادية لنظام المعالجة الآلية فيما يلي:

- **وحدات الإدخال:** مهمتها هي إدخال البيانات كلوحة التحكم.
- **وحدات الإخراج:** ومهمتها هي إخراج ما توصلت إليه العمليات الالكترونية إلى شاشة العرض، ويتم إجراء التفتيش والبحث بغرض أي دليل يقودهم إلى كشف الحقيقة.[3]

ب-تفتيش المكونات المعنوية لنظام المعالجة الآلية:

ويشمل المكونات غير مادية للأجهزة الالكترونية كالبرامج ونظام التشغيل وقواعد البيانات.

---

[1]- رشيد بوبكر، **المرجع السابق**، ص 409.

[2]- **المرجع نفسه**، ص ص 410، 411.

[3]- فايز نبيل عمر، **الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2012، ص 131.

ثالثا: الضبط

وهو الاجراء الذي تقوم به السلطات المختصة لحجز الأشياء أو الأدلة المتعلقة بالجريمة للمحافظة عليها وعرضها عند الحاجة كدليل إثبات، ومن بين الأشياء المضبوطة في البيئة الرقمية هي:

1-ضبط الأشياء المادية: مثل الورق، الحاسب الآلي وملحقاته، بطاقات الدفع الالكتــروني، المودم، حيث يتم التحفظ بهذه المكونات للاستفادة من أي معلومة قد تفيد في مسار الكشف عن الجريمة.[1]

2-ضبط البيانات الإلكترونية: فاختلفت الآراء وانقسمت إلى اتجاهين فيما يخص ضبط هذه البيانات، فهناك من يرى بأن البيانات الإلكترونية تصلح لأن تكون محلا للضبط لكونها عبارة عن ذبذبات معلوماتية صالحة للتخزين، فهي قابلة للنقل والبث وبالتالي هي من الأشياء المادية.

في حين يرى الاتجاه الآخر بأنها غير قابلة للضبط لأنها عبارة عن بيانات افتراضية ويمكن ضبطها في حالة واحدة فقط، وهي إذا تم تحويلها إلى أشياء مادية ملموسة بواسطة التصوير الفوتوغرافي لها أو نسخها على دعامة إلكترونية مادية.[2]

3-المحافظة على الأدلة المضبوطة: بعد إجراء ضبط الأدلة يتم تخزينها خوفا من إتلافها أو أن يلحقها أي ضرر، من خلال إجراءات تتمثل في:

- المحافظة على المعطيات الأصلية المخزنة على الدعامة الالكترونية.
- منع الوصول إلى الأدلة المضبوطة من خلال تقيدها، أو الاعتماد على أي طريقة إلكترونية أخرى.
- الاحتفاظ بالأقراص كما هي وعدم طيها لضمان عدم إتلافها.
- المحافظة على الأشرطة الممغنطة والأقراص بعيدا عن الحرارة والرطوبة والالتزام بالدرجات المسموح بها.[3]

---

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

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

[3]- خولة بوقديرة، المرجع السابق، ص 74.

4-استجواب المشتبه بهم:

ويقصد به استجواب المتهمين وأخذ إفادة الشهود ومواجهة المتهمين بالأدلة التي تدينهم.

أ-استجواب المتهمين:

استجواب المتهمين في جريمة التزوير الواقعة على بطاقات الدفع الالكتروني يعد من الإجراءات الجوهرية في التحقيق لأنه يهدف إلى كشف الحقيقة، لذلك وجب على قاضي التحقيق حتى يضمن أفضل النتائج ما يلي:

فقبل الاستجواب يجب عليه الاعتماد على خبير إلكتروني حتى يعرف قاضي التدقيق الطريقة المناسبة استجواب كل مجرم على حدة حسب موضعه في الجريمة، أمام عند البدء في الاستجواب حضور الخبير المعلوماتي أثناء جلسات الاستجواب تدخله عند الحاجة إليه واستجواب المتهم وفق الإجراءات المقررة قانونا، وعند الانتهاء من عملية الاستجواب يتم تحرير محضر يتضمن كافة التفاصيل.[1]

ب-الشهادة:

لها أهمية كبيرة في إثبات الجريمة، وهي الأقوال الخاصة بالأشخاص غير الخصوم أمام الجهة المكلفة بالتدقيق والمحقق هو من يملك صلاحية رفض الشهود من قبولهم من رأى ذلك والشاهد في الجرائم المعلوماتية تكون له خبرة في المجال التقني وكيفية الدخول إلى النظام المعلوماتي، وتقديم ما يلزم من معلومات لفائدة سلطة التحقيق.[2]

الفرع الثالث: مرحلة المحاكمة

بعد إتمام إجراءات التحري والتحقيق اللازمة وضبط الدليل المعلوماتي تقوم النيابة بتقديم نتائج التدقيق إلى المحكمة المختصة لإجراء المحاكمة وبما أن جريمة التزوير

[1]- حسن ربيعي، **المرجع السابق**، ص 225.

[2]- علي عدنان الفيل، **إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق**، ص ص 61، 64.

الالكتروني تتسم بالطابع التقني وجريمة عابرة للحدود، فإن خطرها يمتد لكافة الدول فقد يرتكب الفعل الاجرامي في بلد ما وتقوم نتيجته في بلد آخر لذلك وجب على المشرع الجزائري تحديد المحكمة الجنائية المختصة بهذه الجرائم في مكان وقوعها، الاختصاص الجنائي الدولي **(أولا)**، الاختصاص من الجنائي الوطني **(ثانيا)**.

أولا: الاختصاص الجنائي الدولي

يتم تحديد الاختصاص في التشريع الجزائري وفقا للميادين التالية:

1-مبدأ إقليمية القانون:

فكل الجرائم الواقعة على التراب الوطني تخضع للقانون الجزائري دون النظر لجنسية الضحية أو المجرم.[1]

2-مبدأ شخصية القانون:

فكل جزائري يرتكب جريمة من الجرائم الالكترونية أو يكون الضحية جزائري فإنه يطبق عليه القانون الجزائري.

3-مبدأ العينية:

يختص هذا المبدأ بالجرائم الالكترونية الماسة بمصلحة الدولة سواء داخل الوطن أو خارجه، وسواء كان مرتكبها من الجزائر أو خارجها.

ثانيا: الاختصاص من الجنائي الوطني

يتم تحديد الاختصاص على المستوى المحلي فيما يخص الجريمة الالكترونية، نجد المشرع الجزائري وزع الاختصاص على النحو التالي:

1-اختصاص قاضي التحقيق:

يتم تمديد صلاحيات قاضي التحقيق إلى المحاكم الأخرى وذلك بموجب نص المادة 40 من القانون 04-14.[2]

---

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

[2]- المادة 40 من القانون 04-14، المؤرخ في 10 نوفمبر 2001 المعدل والمتمم للأمر رقم 56-155، المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية الجزائرية، عدد 71، العدد 41، الصادرة بتاريخ 10 نوفمبر 2004.

2-اختصاص محاكم الجنح:

بالنسبة لاختصاص محاكم الجنح في جريمة التزوير الواقعة على بطاقات الدفع، قام المشرع الجزائري بتمديد اختصاصها إلى دوائر اختصاص المحاكم الأخرى وذلك حسب نص المادة 329 من القانون 04-14.[1]

المطلب الثاني:

الإجراءات المستحدثة لمكافحة جريمة التزوير الواقعة على بطاقات الدفع الالكتروني

نظرا لخطورة جريمة التزوير التي تستهدف بطاقات الدفع الالكتروني التي باتت تشكل تهديدا حقيقيا للأمن المعلوماتي، كان لابد من استحداث إجراءات جديدة تواكب التقنية الحديثة لجمع الدليل التقني من أهمها: التسرب في **(الفرع الأول)** واعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور **(الفرع الثاني)**.

الفرع الأول: التسرب

يعد التسرب من الإجراءات المستحدثة والأساليب الاستخبارية التي تعتمد عليها الأجهزة الأمنية تعرض كشف المعلومات الخاصة بالجريمة، فيمكن تجسيد عملية التسرب في الجرائم الالكترونية كاشتراط ضباط أو عون الشرطة في محادثات غـرف الدردشـة مثلا، فيتخذ المتسرب أسماء مستعارة ويحاول كيفية اقتحام الموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم وتصح عملية التسرب إذا توافرت الشروط التالية:

- صدور إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
- أن يكون الإذن مكتوبا ومسببا.
- تحديد مدة التسرب التي لا يمكن أن تتجاوز 4 أشهر.[2]

---

[1]- المادة 329 من القانون 04-14، **المرجع السابق**.

[2]- فاطمة الزهرة بوعناد، **المرجع السابق**، ص 70

الفرع الثاني: اعتراض المراسلات وتسجيل الأحداث بالتقاط الصور

عرف الاعتراض على أنه مراقبة وترصد المحادثات التي تتم بين الأفراد والعودة كدليل في مرحلة البحث والتحري ضد المتهمين عند الحاجة إليه، كما أن تسجيل الأصوات هي عملية تتم أثناء التحدث الشخصي للأشخاص وذلك بتسجيل تلك المحادثات، أما إلتقاط الصور فهي توثيق تواجد الأشخاص فرادى أو جماعات في مكان ما دون علمهم.

ولقد أجاز المشرع الجزائري في الجرائم الماسة بالمعطيات بموجب المادة 65 مكرر فقرة 05 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 سواءا في مرحلة التحري أو التحقيق.[1]

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

1- يتم القيام بهذا الاجراء فقط بخصوص الجرائم التي حددها القانون ومن بينها الجرائم الماسة بالمعطيات.
2- يتوجب القيام بهذا الاجراء بإذن من طرف وكيل الجمهورية أو قاضي التحقيق.
3- يجب أن يكون هذا الإذن مكتوبا ويحتوي على كل متطلبات هذا الاجراء مع إحاطتها بالسرية التامة.
4- تتراوح مدة هذا الاجراء 4 أشهر وإذا لزم الأمر يتم تجديده بنفس طريقة الاجراء.[2]
5- يجوز للضابط المكلف بإجراء الاعتراض.
6- يقوم الضابط المكلف بإجراء الاعتراض بتحرير محضر يتضمن تفاصيل العملية بعد الانتهاء منها على ذكر تاريخ بدايتها ونهايتها وساعتها.
7- يقوم كذلك الضابط بوصف نسخ المراسلات والصور والمحادثات المسجلة ضمن مهنته للاعتماد عليها كأدلة نحو كشف الحقيقة.[3]

---

[1]- خولة بوقديرة، **المرجع السابق**، ص 82.

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

[3]- إلهام بن خليفة، **المرجع السابق**، ص 313.

المبحث الثالث:

التحديات التي تواجه الحد من التزوير الالكتروني على المستوى الوطني والدولي

يواجه التعاون الدولي في مكافحة جريمة التزوير الالكتروني تحديات كبيرة نتيجة الطبيعة المعقدة لهذه الجرائم وصعوبة تتبع مرتكبيها وجمع الأدلة الرقمية، هذه التحديات تنعكس سلبا على فعالية سلطات التحقيق والعدالة، ومن هذا المنطلق سنحاول من خلال هذا المبحث بيان الصعوبات التي تواجه التعاون الدولي في مواجهة جريمة التزوير الالكتروني في **(المطلب الأول)** في حين نخصص **(المطلب الثاني)** لبيان الحلول القانونية للقضاء على هذه الصعوبات التي تواجه التعاون الدولي.

المطلب الأول:

الصعوبات التي تواجه الدول (التعاون الدولي)

سنتطرق في هذا المطلب إلى تبيان أهم الصعوبات التي تحول دون تحقيق الهدف المنشود من التعاون الدولي والتي يكون سببها الطبيعة الخاصة للجريمة الالكترونية والتي سندرسها في **(الفرع الأول)**، أو الصعوبات بسبب ضعف قوانين مكافحة الجرائم الالكترونية ونوضحها في **(الفرع الثاني)** إضافة إلى الصعوبات الناتجة عن عدم فعالية التعاون الدولي والتي سندرسها في **(الفرع الثالث)**.

الفرع الأول: الصعوبات الناتجة عن الطبيعة الخاصة لجريمة التزوير الالكتروني

تعد جريمة التزوير الالكتروني من الجرائم المعقدة بسبب طبيعتها المستحدثة وتقنياتها المتطورة، ما يفرض تحديات عديدة أمام سلطات التحقيق في ظل بيئة افتراضية عابرة للحدود، انعكاسات الطابع العابر للحدود لجريمة التزوير الالكتروني على التحقيق **(أولا)**، صعوبة إثبات جريمة التزوير الالكتروني **(ثانيا)**.

أولا: انعكاسات الطابع العابر للحدود لجريمة التزوير الالكتروني على التحقيق

من أهم خصائص الجريمة الالكترونية أنها جريمة دولية وعابرة للحدود إذ لا تعرف إقليم أو مكان، مما يصعب مكافحتها ويتطلب تنسيقا دوليا فعالا لحد من انتشارها، كما تتسم بسرعة التنفيذ وصعوبة اكتشافها ولا يشترط وقوع الجاني والنتيجة الجرمية في نفس المكان ممّا يعقد مهنة التحقيق والمساعدة القانونية.[1]

وتثير الجرائم الالكترونية خلافا بين الفقه حول إشكالية تنازع الاختصاص بين الدول نظرا لطبيعتها الدولية وتجردها من الطابع المادي مما يؤدي إلى صعوبة تحديد المحكمة المختصة، وقد ينتج عن ذلك تداخل في الولايات القضائية ويستلزم اعتمادا أكثر من معيار قانوني لحسم النزاع القضائي[2].

فقد يحدث أن ترتكب جريمة من الجرائم الالكترونية من طرف أجنبي على إقليم دولة معينة فيؤول الاختصاص في هذه الحالة إلى الدولة التي ارتكبت الجريمة على إقليمها استنادا إلى مبدأ الإقليمية وإلى الدولة التي تحمل جنسيتها استنادا إلى مبدأ الشخصية، وقد تشكل هذه الجريمة تهديدا لأمن دولة أخرى أو تمس لمصالحها الأساسية، فتدخل في اختصاصها استنادا إلى مبدأ العينية وهو ما يترتب عليه تنازع الاختصاص بين الدول كل واحد حسب المعيار الذي يربطها بالجريمة.[3]

وقد ذهب جانب من الفقه إلى أن الاختصاص في الجرائم الالكترونية يعقد إلى محاكم الدولة التي تم فيها تحميل البيانات كون جميع البيانات والأدلة ستكون سهلة لكونها المصدر.[4]

---

[1]– حنان ريحان مبارك المضحكي، **الجرائم المعلوماتية–دراسة مقارنة–**، منشورات الحلبي الحقوقية، لبنان، 2014، ص 373.

[2]– جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، **أطروحة مكملة لنيل شهادة الدكتوراه في العلوم**، تخصص قانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص 186.

[3]– عبد محمد بحر، معوقات التحقيق في جرائم الأنترنت، **مذكرة مكملة لنيل شهادة الماجستير في العلوم الشرطية**، جامعة نايف للعلوم الأمنية، دبي، 1999، ص 26.

[4]– حنان ريحان مبارك المضحكي، **المرجع السابق**، ص 373.

ولقد وجهت العديد من الانتقادات لأصحاب هذا الجانب لعل أهمها أن بعض الأفعال قد لا تعد مخالفة للقانون في دولة التحميل، مما يصعب معاقبة مرتكبيها ولهذا السبب يرى بعض الفقهاء ضرورة منح اختصاص دولي لمحاكمة هذه الأفعال خصوصا إذا تسببت في أضرار لدول أخرى، خاصة إذا لم تكن دولة التحميل مسؤولية عن الفعل.[1]

لكن هذا الرأي مردود أيضا حيث لم يضع في الحسبان مصلحة المتهم بأن تطبق عليه قوانين غير قوانين الدولة التي يحمل جنسيتها مما يزيد من تكلفة المحاكمات الجرائم وزيادة مدة وأجل المحاكمة.[2]

كل هذه المبررات استدعت نشأة اتجاه ثالث يرى بانعقاد والاختصاص القضائي لمكان المعتدي كونه المكان الذي تحققت فيه الجريمة ومرتبطا بشخص المعتدي عليه، وهو يتجنب السلبيات والانتقادات التي وجهت للاتجاهين السابقين.[3]

وأمام عدم نجاعة الحلول الفقهية المقترحة لتجاوز مشكلة تنازع الاختصاص لجأت الدول إلى تنظيم مسألة الاختصاص بنصوص واضحة في اتفاقيات دولية ثنائية ومتعددة الأطراف، فقد نصت المادة 15 من اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة على أنه "يتعين على كل دولة طرف أن تعتمد ما يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجريمة التي ترتكب في إقليم تلك الدولة أو ضد أحد مواطني تلك الدولة أو حينما ترتكب الجريمة من طرف أحد مواطني تلك الدولة أو من طرق شخص عديم الجنسية اتخذ مكان إقامته المعتاد في إقليمها...".

وأضافت هذه المادة على أنه إذا تم إبلاغ دولة ما عن سلوك إجرامي يستوفي معايير معينة، أو علمت به تلقاء نفسها فعلى سلطتها القضائية المختصة التنسيق مع الدول الأخرى المعينة لاتخاذ الإجراءات المناسبة لمتابعة الجريمة.

---

[1]– محمد عوض محمد، مشكلات السياسة الجنائية المعاصرة من جرائم نظر المعلومات، **بحث مقدم إلى مؤتمر القانون الكمبيوتر والأنترنت**، الفقرة 1– 3 ماي 2000، كلية الشريعية والقانون، الامارات العربية المتحدة، ص 21.

[2]– حنان ريحان مبارك المضحكي، **المرجع السابق**، ص 374.

[3]– جمال براهيمي، **المرجع السابق**، ص 188.

في حين نصت المادة 22 من اتفاقية مجلس أوروبا لمكافحة الجريمة الالكترونية على ضرورة إلتزام كل دولة بوضع تشريعات تحدد اختصاصات القضائي، خصوصا عندما ترتكب الجريمة على إقليمها أو من أحد مواطنيها، حتى وإن وقعت خارج حدودها إذا كانت معاقبا عليها بموجب القانون الجنائي.

وجئت هذه الاتفاقيات الأطراف المتعاقدة على التشاور فيما بينها عند وجود تنازع في الاختصاص القضائي بشأن جريمة مشمولة بالاتفاقية بهدف تحديد الجهة الأنسب لمتابعة القضية.[1]

ثانيا: صعوبة إثبات جريمة التزوير الالكتروني

تعد جريمة التزوير الإلكتروني صعبة الاثبات بسبب طبيعتها غير المادية ووقوعها في بيئة رقمية افتراضية تمحي آثارها بسهولة، ما يجعل تعقب مرتكبها تحديا كبيرا خاصة لكونها لا تحتاج إلى عنف أو قوة وترتكب غالبا بوسائل ذكية يصعب كشفها.[2]

وتزداد صعوبة كشف جريمة التزوير الإلكتروني وإثباتها بسبب تعقيد الوسائل التقنية المستخدمة فيها، إذ غالبا ما تنفذ باستخدام أدوات عالية التقنية تفتقر إلى آثار مـادية واضحة، مما يصعب تحديد الفاعل وربط الجريمة بشخص معين.[3]

كما تعد سهولة إخفاء الأدلة وسرعة محوها من أبرز التحديات في إثبات جريمة التزوير الالكتروني، حيث يستخدم الجناة تقنيات متقدمة تمكنهم من طمس آثار الجريمة والتلاعب بالمعلومات عبر إدخال بيانات مزيفة أو تعديل أنظمة الحاسب، مما يصعب اكتشاف الجريمة وتتبع مرتكبها.[4]

وقد بلجأ المتهم إلى تشفير البيانات المخزنة داخل الحواسيب، مما يصعب على المحققين الوصول إلى الأدلة، ويستخدم في ذلك رموز معقدة وإشارات غير قابلة للفهم إلا من خلال مفاتيح خاصة، وتعتمد هذه العمليات على خوارزميات رياضية معقدة، أمام

---

[1]– الفقرة 5 من المادة 22 من اتفاقية مجلس أوروبا بالمكافحة الجريمة الالكترونية.

[2]– حسين بن سعيد الغافري للتحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت.

[3]– جمال براهيمي، **المرجع السابق**، ص 197.

[4]– حسين بن سعد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، دراسة مقارنة، **أطروحة دكتوراه**، كلية الحقوق، جامعة عين شمس، مصر، 2007، ص 09.

المحقق خياران إما امتلاك المفاتيح أو استخدام علم تحليل الشفرات لاستخراج النص المشفر.[1]

وما يزيد من الصعوبات التي تواجه الجهات المختصة في إثبات جريمة التزوير الالكتروني، وأبرز نقص مهارات رجال الضبط والقضاء في التعامل مع التكنولوجيا الحديثة، وضعف الالمام بطرق ارتكاب الجرائم الالكترونية، بالإضافة إلى التعقيد الفني والدقة التي تتطلبها الأدلة الرقمية، ويؤدي هذا النقص إلى إتلاف الأدلة أو محوها بسبب أخطاء ناتجة عن سوء التعامل مع الوسائط الالكترونية مثل الأقراص الصلبة مما يعرقل عملية التحقيق والاثبات.[2]

أدى العجز في مواجهة الجرائم الالكترونية إلى توجه بعض الدول لاستقطاب الكفاءات المتخصصة في تكنولوجيا الاعلام والاتصال، وتنظيم دورات تدريبية للأجهزة الأمنية والقضائية لتعزيز قدراتهم، ومع ذلك تظل هذه الأجهزة غير قادرة على مواكبة التطورات المتسارعة في هذا المجال، بسبب حداثة ظاهرة الاجرام الالكتروني وصعوبة اكتساب الخبرة الأزمة للتعامل معها.[3]

الفرع الثاني: الصعوبات الناتجة عن ضعف قوانين مكافحة الجرائم الالكترونية

تواجه القواعد الجنائية التقليدية تحديات كبيرة في مجازات التطور العلمي والتكنولوجـــي، ما ينعكس سلبا على فعالية ملاحقة الجرائم الالكترونية ومكافحتها، ويعزي ذلك إلى طبيعتها الثابتة والاجرائية، مما أدى إلى قصور في النصوص القانونية وعدم كفايتها لمواجهة الجرائم المستحدثة بالإضافة إلى صعوبات في التعاون الدولي والمعاينة التقنية للبيئة الالكترونية.

ونفصل ذلك فيما يلي:

---

[1]– إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت، **بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت**، كلية الشريعة والقانون، الامارات العربية المتحدة، 2000، ص 11.

[2]– محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، **بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت**، الطبعة الثالثة، كلية الشريعة والقانون، الإمارات العربية المتحدة، الفقرة من 1إلى 3، ماي 2004، ص 1070.

[3]– جمال براهيمي، **المرجع السابق**، ص 211.

أولا: عدم كفاية النصوص العقابية التقليدية

على الرغم من تطور تكنولوجيا وظهور جرائم مستحدثة، لا تزال مكافحتها تعالج ضمن النصوص العقابية التقليدية، مما يسبب صعوبات في ملاحقتها وجمع الأدلة، وقد يؤدي ذلك إلى الطعن في مشروعية الإجراءات المتخذة بشأنها.[1]

كما أن تطور القوانين بنفس السرعة والوتيرة التي تتطور بها وسائل الاعلام التكنولوجيا ومهارات الذهن البشري جعل القوانين التقليدية تقف عاجزة عن مواجهة العديد من الجرائم التي أصبحت مرتبطة بالأجهزة الالكترونية فهناك أفعال جديدة، وتوجد أفعال جديدة تتعلق باستخدام الحاسوب لا تعتبر جرائم وفق القوانين التقليدية، رغم تهديدها للمصالح العامة وخطورتها على المجتمع ويصعب تطبيق هذه القوانين عليها لأنها صممت لحماية الأشياء المادية مما يجعل من الصعب معاقبة الاعتداءات على البيانات والمعلومات.[2]

بسبب قصور القوانين التقليدية في مواجهة الجرائم الالكترونية، سعت بعض الدول إلى تفسير النصوص الجنائية التقليدية بشكل مرن تشمل هذه الجرائم وتفادي إفلات الجناة من العقاب.[3]

ثانيا: الصعوبات المتعلقة بالتفتيش والضبط في البيئة الالكترونية

تعاني إجراءات التفتيش والضبط في البيئة الالكترونية من صعوبات كبيرة بسبب عدم توافق القوانين التقليدية مع طبيعة الجرائم الالكترونية، حيث تعتمد هذه الإجراءات على وجود دليل مادي، وهو ما يتعارض مع الطبيعة غير المادية لمكونات الحاسوب.

وقد أثار خلاف حول مدى جواز التفتيش الوسط الافتراضي، وظهر في ذلك ثلاثة اتجاهات فذهب الاتجاه فذهب الاتجاه الأول إلى جواز تفتيش وضبط المكونات المعنوية للحاسوب بمختلف أشكالها وجواز تفتيش وضبط أي شيء يتعلق بالجريمة ويساعد في الكشف عن حقيقة وقوعها ليشمل كل مكونات المادية والعفوية للحاسوب معا.[4]

---

[1]– جمال براهيمي، **المرجع السابق**، ص 220.

[2]– يوسف بكري، **التفتيش من المعلومات في وسائل التقنية الحديثة**، دار الفكر الجامعي، مصر، 2011، ص 23.

[3]– جمال براهيمي، **المرجع السابق**، ص 222.

[4]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت–دراسة مقارنة، **أطروحة مقدمة لنيل شهادة دكتوراه**، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2014، ص 225.

بالمقابل ذهب اتجاه فقهي آخر وهو الغالب إلى عدم إمكانية إخضاع المكونات المعنوية للحاسوب من برامج وبيانات لعملية التفتيش والضبط لأن الغرض الأساسي من التفتيش هو ضبط الأدلة المادية، ولما كانت هذه المكونات الالكترونية المنطقية تفتقر إلى مظهر مادي ملموس إلا إذا تم تعديل غاية التفتيش تلك يجعلها تشمل ضبط الأدلة المادية وغير مادية على حد سواء.[1]

وعكس ما ذهب إليه الاتجاهين الفقهيين الأول والثاني، هناك من يرى أنه لا يجب الخلط عند تحليل مدلول الشيء بالنسبة لمكونات الحاسب بين الحق الذهني للشخص على البرامج والبيانات، وبين طبيعة هذه البرامج، إنما ينبغي الرجوع إلى ذلك إلى تحديد مدلول كلمة "المادة" في العلوم الطبيعية.

فلما كانت المادة تعرف على أنها "كل ما يشغل حيزا ماديا في فراغ معين" وكان الحيز مما يجوز قياسه والتحكم فيه فإن البرامج والكيانات المنطقية باعتبارها تشغل حيزا ماديا في ذاكرة الحاسب الآلي وهو يمكن قياس حيزها بوحدات قياس خاصة، وتأخذ شكل بنبضات إلكترونية تتوفر على خصائص المادة وبالتالي فهي من قبيل الأشياء المادية.[2]

واجهت التشريعات التقليدية صعوبات في التعامل مع الجرائم الالكترونية بسبب غموض المفاهيم وعدم وضوح خضوع مكونات الحاسوب للتفتيش والضبط مما دفع بعض الدول لتعديل قوانينها ورغم اعتماد الاتفاقيات الدولية مثل الاتفاقية الأوروبية حول مكافحة الجرائم الالكترونية ببوداست وهذا في مادتها 19 على شمول التفتيش للبرامج والبيانات الالكترونية لا يزال الجدل قائما بسبب تمسك بعض الدول بالإجراءات التقليدية مما يعرقل التحقيق الملاحقة الفعالة للجناة.

الفرع الثالث: الصعوبات الناتجة عن عدم فعالية التعاون الدولي

تواجه مكافحة الجرائم الالكترونية صعوبات كبيرة بسبب ضعف التعاون الدولي، إذ تعجز الدول عن مواجهة هذه الجرائم العابرة للحدود، يتطلب التصدي لها تنسيقا دوليا فعالا

---

[1]– علي محمود علي محمود، الأدلة المحصلة من الوسائل الالكترونية في إطار نظريات الجنائي، **بحث مقدم إلى المؤتمر العلمي حول الجوانب القانونية للمعلومات الالكترونية**، الإمارات العربية المتحدة، 2003، ص 13.

[2]– جمال براهيمي، **المرجع السابق**، ص ص 225، 226.

في التحقيق والملاحقة القانونية، تعرقل هذا التعاون، ناهيك على اختلاف النظم القانونية وغياب نماذج موحدة للنشاط الاجرامي إضافة إلى ضعف قنوات الاتصال والمساعدة القضائية الدولية وفيما يلي تفصيل ذلك:

أولا: عدم وجود نموذج موحد للنشاط الاجرامي

إذا نظرنا إلى الأنظمة القانونية في الكثير من الدول لمواجهة الجرائم الالكترونية يتضح لنا من خلالها صعوبة في توحيد نماذج تجريم الأفعال الالكترونية حيث قد يعد سلوك ما جريمة في دولة ومباحا في أخرى، ويعود هذا التفاوت إلى اختلاف البيئات الثقافية والدينية والاجتماعية مما يؤدي إلى اختلاف في السياسات التشريعية بين المجتمعات.[1]

ولعل السبب أيضا في هذا التباين يعود إلى قصور التشريع ذاته وعدم مسايرته لسرعة التقدم التكنولوجي، ومن ثم الجريمة الالكترونية فلن أن نتصور أنه لم يصدر قانون في دولة عربية خاصة بالجوانب الموضوعية والاجرامية الجريمة الالكترونية بل لا زال الوصول ما إن كان من الأفضل تعديل التشريعات العقابية كي تستوعب نماذج الجريمة الالكترونية أو إدراج هذه الأخيرة في قوانين فرعية متخصصة كقانون حماية الملكية الفكرية.[2]

كما أن عدم وجود تعريف موحد للجريمة الالكترونية أدى إلى إحداث ثغرات في منظومة القانون الدولي في مجال مكافحة هذه الجرائم وإبقاء أفعال إجرامية دون تجريم أو عقاب، مما يسهل إفلات الجناة من المسؤولية الجزائية كون نص التجريم هو بمثابة الركن الشرعي لقيام الجريمة وانتقاؤه يؤدي حتما إلى انتقاء المسؤولية الجزائية.[3]

ثانيا: اختلاف النظم القانونية الاجرامية

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحدي والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى كما هو الحال بالنسبة للمراقبة الالكترونية وتسليم المراقب فقد اعتبرت طريقة ما من طرق جمع الاستدلالات أو أنها قانونية في دولة معينـــة قد يكون غيــر مشروعـة في دولـة

---

[1]– غانم مرضي الشمري، **الجرائم المعلوماتية**، الدار العلمية للنشر والتوزيع، الأردن، 2016، ص 124.

[2]– عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت في التشريعات العربية**، دار النهضة العربية، مصر، 2009، ص 103.

[3]– جمال براهيمي، **المرجع السابق**، ص 235.

أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة ملفات الدولة الأخرى على استخدام ما تعتبره هي أنه فعالة بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام إلى دليل إثبات عليه في اختصاص قضائي وبشكل غير مشروع.[1]

ولعل أحسن مثال على ذلك التباين التشريعي القائم بين القوانين اللاتينية والأنجلوساكسونية حول مدى حجية الدليل الرقمي في الاثبات الجنائي، ومنها القانون الفرنسي والجزائري والسوري واللبناني فإن القاضي الجزائري يتمتع بحرية مطلقة في تقدير الأدلة المطروحة أمامه والأخذ منها حسب قناعته، في حين أن النظر الأنجلوساكسونية مثل بريطانيا والو.م.أ لا تعترف للدليل الرقمي بحجة للإثبات الجنائي إلاّ إذا أخذ أحد الأشكال التي حددها المشرع.

ثالثا: عدم وجود قنوات اتصال

إن تبادل المعلومات في مجال الجرائم الالكترونية والحصول على البيانات والمعلومات من أهم أهداف التعاون، فعدم وجود قنوات اتصال بين الجهات المختصة يعيق تبادل المعلومات والأدلة في قضايا الجرائم الالكترونية، هذا النقص يحد من فعالية التحقيق ويقلل من القدرة على التصدي للجريمة بشكل فعال.

رابعا: التحديات الخاصة بالمساعدات القضائية

لما كانت جريمة التزوير الالكتروني جريمة عبرة للحدود فإن مكافحتها والعقاب عليها يعد أمرًا احتماليًا في ظل الوضع الراهن للأنظمة القانونية، حيث من الصعب ملاحقة القضايا بسبب عدم القدرة على التوفيق بين المدة التي تتطلبها المتابعة القضائية والسرعة التي تتسم بها الجرائم الالكترونية.[2]

كما أن محاكمة المجرم المتواجد على أراضي دولة أجنبية يحتاج إلى إجراءات طويلة ومكثفة الأمر بالنسبة لتنفيذ الأحكام الصادرة في الخارج لأن تطبيقها سوف يصطدم بالعديد

---

[1]– يوسف حسن يوسف، الجرائم الدولية للأنترنت، **المركز القومي الإصدارات القانونية**، مصر، 2011، ص ص 186، 187.

[2]– أيمن رمضان محمد أحمد، **الحماية الجنائية للتوقيع الالكتروني–دراسة مقارنة**، دار النهضة العربية، القاهرة، 2011، ص 260.

من العقبات، ومن أهم هذه التحديات الإشكالات التي تطرحها الإنابة القضائية وكذا إشكالية تسليم المجرمين حيث تعتبر الإنابة القضائية أهم صور المساعدات القضائية.

أ-إشكالية الإنابة القضائية:

تعتبر من أهم صور المساعدات القضائية في مجال الجنائي والتي تتم بالطرق الدبلوماسية كون إجراءاتها تتسم بالبطئ والتعقيد وهو ما يتعارض مع طبيعة الجرائم الالكترونية، وبالتالي يستحيل معها القيام بإجراءات فعالة تؤدي إلى كشف الجريمة ونسبتها إلى مرتكبيها كون الجريمة تستلزم ردود سريعة خشية التلاعب بالبيانات التي قد تشكل دليلا ضد المتهم ويرجع البطئ إلى عدة أسباب أهمها نقص الموظفين أو الفوارق في الإجراءات.[1]

ومن هنا نجد الحاجة الملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة، للقضاء على مشكل البطئ في تسليم طلبات الإنابة وهذا ما أوصى به مؤتمر الأمم المتحدة الحادي عشر لمنح الجريمة والعدالة الجناية المنعقد في بانكوك 2005/04/25 حيث أكد على تعزيز فعالية السلطات المركزية، وإقامة قنوات تباشر للاتصال فيما بينها بغية تنفيذ الطلبات في الوقت المناسب.[2]

أما بالنسبة للرد على طلبات المساعدة فإنه من الضرورة الاستجابة الفورية والسريعة على هذه الطلبات، لذلك نصت غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على الضرورة للاستجابة الفورية والسريعة على طلبات التماس المساعدة وهذا ما أكدته الفقرة 3 من المادة 25 من الاتفاقية الأوروبية للإجرام المعلوماتي.

ب-إشكالية تسليم المجرمين:

تتمثل إشكالية تسليم المجرمين في مشكلة ما يسمى بالتجريم المزدوج والذي يعتبر من أهم الشروط الخاصة بنظام تسليم المجرمين والمنصوص عليه في معظم التشريعات

---

[1]- حسين الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت-دراسة مقارنة، **أطروحة دكتوراه**، كلية الحقوق، جامعة عين الشمس، مصر، ص 194.

[2]- يوسف حسن يوسف، **المرجع السابق**، ص 194.

الوطنيــة، وعلى الرغم من أهميته إلا أنه يعتبر من أهم العقبات التي تواجه التعاون الدولي في مجال تسليم المجرمين.[1]

وهذا إذا كان قانون الدولة المطلوب منها التسليم لا يجرم الفعل الذي ارتكبه المطلوب تسليمه، إضافة إلى مشكلة التزاحم في طلبات التسليم وهذا يصل فيها إلى الدول المطلوب منها التسليم سواءا كان الطلب متعلقا بذات الجريمة أو بجرائم أخرى.[2]

وتزداد هذه الإشكاليات أكثر في الجرائم الإلكترونية لا سيما وأن معظم الدول لا تجرم هذه الجرائم بالإضافة إلا أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تطبق على الجرائم الالكترونية أو لا؟ الأمر الذي يعيق تطبيق الاتفاقيات الدولية في حال تسليم المجرمين.

المطلب الثاني:

الحلول القانونية لمواجهة التحديات الخاصة لمكافحة جريمة التزوير الالكتروني

رأينا فيما سبق أن مكافحة جريمة التزوير الالكتروني وملاحقة مرتكبيها تتخللها العديد من العقبات والصعوبات لا سيما منها بالجانب الإجرامي وهذا ما انعكس سلبا على مردود سلطات لتحقيق والقضاء في ملاحقة مرتكبي الجريمة، وما جعل الدول عاجزة عن أداء واجبها الدستوري والقانوني لحماية الأفراد، وهذا ما سنوضحه في **(الفرع الأول)**، كما أن الطابع الدولي العابر للحدود كجريمة التزوير الالكتروني، كما رأينا يشكل أكثر العقبات التي تواجه مكافحة هذه الجريمة، مما جعل الدول تسعى إلى وضع جملة من الحلول القانونية القضائية، وهذا ما سنفصله في **(الفرع الثاني)**.

---

[1]– محمود إبراهيم غازي، **المرجع السابق**، ص 61.

[2]– إلهام بن خليفة، **المرجع السابق**، ص 375.

الفرع الأول: الحلول القانونية لتدارك تحديات مكافحة جريمة التزوير الالكتروني على مستوى التشريعات الوطنية

من المعلوم أن الاستثمار في مجال الحاسبات والمعلوماتية له شأن عظيم، لذلك يلزم وضع استراتيجيات وبرامج على المستوى الوطني بدرجة أولى وعلى المستوى العالمي، والإشكال الذي يطرح في هذا المجال كيف كانت مواقف الدول وما هي الاستراتيجيات المتبعة؟

بصدد هذا التساؤل انقسم الفقه الجنائي في هذا المجال، فهناك من يرى أن المواجهة الفعالة للتحريات الاجرامية لمواجهة جريمة التزوير الالكتروني في حين يرى البعض الآخر أنه لا ينبغي التعويل كثيرا على القواعد التفكيرية إذ يجب مراجعة تلك النصوص بصفة دورية وتقدير قواعد قانونية جديدة وفيما يلي تفصيل ذلك: تطبيق النصوص الجنائية التقليدية على الجرائم الالكترونية **(أولا)**، ضرورة إرساء قواعد قانونية لمواجهة جريمة التزوير الإلكتروني **(ثانيا)**:

أولا: تطبيق النصوص الجنائية التقليدية على الجرائم الالكترونية

يعد تطبيق النصوص الجنائية التقليدية على الجرائم الالكترونية من الحلول الممكنة لمواجهتها في ظل غياب التشريعات خاصة، وتكون المكافحة في هذا المجال بالاعتماد على التفسير الموسع للنصوص العقابية التقليدية وتطبيقها على الجرائم الالكترونية، ويعطي للقاضي الجزائي حرية تفسير هذه النصوص تفسيرا يسمح بوضع هذه الجرائم تحت طاولة التجريم والمتابعة الجزائية.[1]

فعندما تعرض قضية جزائية على القاضي، فإن أول شيء يقوم به هو تكثيف الواقعة لمعرفة مدى تطابقها مع النص القانوني وذلك باستخلاص عناصر هذه الواقعة من النص، وقد يصادفه صعوبة أو غموض فيلجأ إلى تفسير النص الجنائي.[2]

---

[1]– هدى حامد قشقوش، **السياسة الجنائية لمواجهة الجريمة المعلوماتية**، دار النهضة العربية، مصر، 2012، ص 72.

[2]– يوسف حسن يوسف، **المرجع السابق**، ص 126.

وفي هذا الصدد لجأ القضاء الجنائي في العديد من الدول إلى تفسير النصوص الجنائية وهذا ما اعتمده القضاء الفرنسي من خلال المادة 145 من قانون العقوبات في مجال تزوير المحررات التقليدية قبل تعديدها بالمادة 462 من قانون الغش المعلوماتي وكذلك ما قام به القضاء الياباني حيث لجأ ملاحقة التزوير المعلوماتي إلى تبني المفهوم الموسع لجريمة التزوير.[1]

ولا يقتصر العمل على تمديد النصوص الجنائية التقليدية إلى الجرائم الالكترونية فحسب بل لابد أن تمتد إلى النصوص الاجرائية خاصة ما تعلق بإجراءات التحقيق وأدلة الاثبات، وهو ما أوصلت به اللجنة الأوروبية، من خلال توصياتها رقم (89) و(95) الصادرة في عام 1990.[2]

ثانيا: ضرورة إرساء قواعد قانونية لمواجهة جريمة التزوير الإلكتروني

تباينت التشريعات في التعامل مع تزوير المحررات الالكترونية، فبعضها عدل نصوص التزوير التقليدية لاستيعاب صور التزوير الحديثة، بينما فضلت أخرى سن قوانين بالإجرام الالكتروني، وقد أفردت تشريعات تعالج التزوير الالكتروني بشكل مستقل عن التزوير التقليدي، وتأسيس على ذلك فقد استدركت أغلب الدول بمختلف أنظمتها القانونية العجز في ملائمة القوانين النافذة للاعتداءات الحاصلة على النظم المعلوماتية وسنأخذ على سبيل الاستدلال ما جاء به المشرع الفرنسي والجزائري.

أ-التشريع الفرنسي:

يعد المشرع الفرنسي من أوائل المشرعين اللذين يتيقنوا بأن التصدي للجريمة الالكترونية لن يكون إلا من خلال نصوص عقابية وإجرائية خاصة، وقد كانت أولى محاولاته قانون العقوبات ليشمل المجال المعلوماتي الصادر عام 1978 ليصدر من بعده المرسوم

[1]- جمال براهيمي، **المرجع السابق**، ص 246.

[2] -conseil de l'Europe، la criminalité informatique recommandation NR89 ru la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels, Strasbourg, 1990, p19.

المؤرخ في 1981/12/23 الذي حدد فيه بعض المخالفات المرتبطة بالمعلوماتية وفي سنة 1988 صدر القانون 19-88 المعدل لقانون العقوبات بشأن الغش المعلوماتي.[1]

وجاء في المادة 462[2] فقرة 5 و462 فقرة 6 أحكام تتضمن تجريم المستندات المعالجة آليا وكذا استعمال تلك المحررات، إلا أنه بعد صدور قانون العقوبات الفرنسي الجديد في 1992/12/16 قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص تزوير المستندات المعالجة آليا، وذلك بتعديل المادة 1/441 من الكتاب الرابع من قانون العقوبات.

وقد تواصلت جود المشرع الفرنسي في هذا المجال بشكل مكثف بعد تصديقها في 23 نوفمبر 2001 على الاتفاقية الأوروبية الخاصة بالجرائم الالكترونية، فقامت بتعديل تشريعاتها النهائية، ومن جهة أخرى استحدث نصوص أخرى خاصة لمواجهة الجريمة الالكترونية أهمها القانون رقم (1062/23) المتعلق بالأمن اليومي المؤرخ في 2001/11/15[3] والقانون رقم (239/03) المتضمن التوجيه والتخطيط للأمن الداخلي المؤرخ في 2003/03/18[4] وكذا القانون 204/04 المتضمن لمواكبة العدالة لتطورات الاجرام.[5]

وكذا القانون رقم (575/04) المتعلقة بالثقة في الاقتصاد الرقمي المؤرخ في 22/2004[6] والقانون رقم (699/04) المتعلق بالاتصالات الالكترونية وخدمات الاتصال لعام 2004.[7]

---

[1] -Chopin Frédérique، **les politiques publiques de lutte contre la cybercriminalité**، aliéna، paris، France، p 102.

[2] - المادة 462 من قانون العقوبات الفرنسي، المتضمن أحكام تجريم المستندات المعالجة آليا، المؤرخ في 1981/12/23، والصادر في 1988 المعدل والمتمم.

[3] -sécurité quotidienne، JORF 16 nov-2001, P18-215.

[4] -loi N-2003-239.18mars2003 pour la sécurité intérieure، JORF 19 mars 2003 , p 4761.

[5] -loi N-2004, 9 mars 2004, pourtant adaptant de la justice aux évolution de la criminalité, JORF 19 mars, 2004, P 4567.

[6] -loi N-2004-575-21 juin 2004 pour la confidence a de l'économie numérique، JORF 22 juin 2004, P 11508.

[7] -loi N-2004-669 du 9 juillet 2004 relative aux communications, JORF du 10 juillet 2004, P 12483.

كما أدخل المشرع الفرنسي تعديلات على إجراء المتابعة الجزائية والتحقيق والاثباتات التقليدية كإجراءات التحري والتفتيش والمعاينة، كما استحدث إجراءات تحري للكشف عن الجرائم الالكترونية كاعتراض المراسلات والتسرب وغيرها.[1]

ب-المشرع الجزائري:

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في إطار ما يسمى بأزمة القانون الجنائي في مواجهة واقعة المعلوماتية، وهنا كانت الضرورة لتخطي هذه الأزمة.

وبالنسبة للتشريع الجزائري فقد تدارك الأمر مؤخرا ولو نسبيا، وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية المتضمن تعديل قانون العقوبات، حيث أدرج في الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 156/66 القسم سابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد 394 مكرر 394 مكرر.[2]

وتجدر الإشارة إلى أن المشرع الجزائري في هذا التعديل قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتجات الاعلام الآلي والمتمثلة في لتزوير المعلوماتي، كما أدرك المشرع الجزائري أن المواجهة الفعالة للإجرام الالكتروني لا تكون بإرساء قواعد قانونية ذات طبيعة ردعية فقد بل لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية تحفظية وذلك من خلال القانون رقم (06-22) المعدل لقانون إ.ج يتعلق بالتحقيق في الجرائم الالكترونية (كاعتراض المراسلات، تسجيل الأصوات...).[3]

وأضاف أيضا المشرع الجزائري القانون رقم (09-04) الذي تضمن جملة من النصوص القانونية لمواجهة الجرائم الناشئة عن الاستخدام غير المشروع لوسائل الاعلام

---

[1] -Chopin Frédérique، op، cit, p 110.

[2]- الأمر 156/06 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم بموجب الأمر 21-08 المؤرخ في 8 يونيو 2021، الجريدة الرسمية للجمهورية الجزائرية، العدد 45، الصادرة بتاريخ 09 يونيو 2021.

[3]- القانون 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 115/66، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، الصادر بتاريخ 24 ديسمبر 2006.

والاتصال الالكتروني وشبكة الأنترنت والذي تضمن مجموعة من التدابير المستحدثة وغير المألوفة في القوانين السابقة تتنوع بين تدابير وقائية وأخرى إجرائية.[1]

ونخلص في الأخير إلى أن التشريع الجزائري أحدث قصورًا في مواكبة تطورات الجريمة الالكترونية، رغم صدور القانون 15/04 الذي جرم بعض الأفعال المتعلقة بالاعتداء على الأنظمة المعلوماتية، إلا أنه لم يتطرق إلى جرائم أخرى كالتزوير الإلكتروني، مما يستدعي إصدار قانون أكثر شمولا لمكافحة هذا النوع من الجرائم، بالاعتماد على التكنولوجيا الحديثة، والتعاون الدولي وتفعيل وسائل المراقبة والتفتيش للوصول إلى الجناة.

وعليه فالمشرع الجزائري أطلق على الجرائم المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وأورد تعريف لها في المادة 02 فقرة أ على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل بارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".[2]

ومن خلال المادة المذكورة أعلاه نجد أن الجرائم المعلوماتية المنصوص عليها هي جريمة الدخول أو البقاء بغش في النظام وجريمة الاعتداء العمدي على سلامة المعطيات، وجريمة التعامل في المعلومات الغير مشروعة، وكذلك أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، وهذا ما ينطبق على جريمة التزوير الالكتروني طبقا لمبدأ الشرعية بطابعه المرن والمستحدث.

كما أن نصوص التزوير في قانون العقوبات لم تتضمن إشارة بإمكانية تطبيق هذه النصوص على التزوير الالكتروني في ظل الاعتراف بالقيمة الثبوتية للمحرر الالكتروني بموجب تعديل القانون المدني، وهنا يستلزم على المشرع أن يعدل في نصوص التزوير

---

[1]– القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد 47، المؤرخة في 25 شعبان 1420هـ الموافق لـ 16 أوت 2009.

[2]– القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجمهورية الجزائرية، المؤرخة في 25 شعبان 1430 الموافق لـ 16 أوت 2009، ص 09.

ويستوعب حتى العقاب على تزوير المحرر أو المستند الالكتروني خاصة أن هذه الجرائم تتميز بالطابع الدولي والتقني بالقدر الذي تستطيع أجهزة العدالة من خلاله تطبيق الإجراءات المنصوص عليها في هذا القانون من جهة وتفعيل آليات التعاون الدولي لمواجهة مثل هذه الجرائم من جهة أخرى[1]، رغبة من المشرع الجزائري في وضع حد لظاهرة التزوير الالكتروني، عمد المشرع إلى وضع ترسانة من القوانين للتصدي إلى هذه الظاهرة، ولا يتم ذلك إلا من خلال جملة من الإجراءات:

- المكلفون بمعاينة جرائم التزوير الالكتروني ذو الاختصاص العام:

حاول المشرع الجزائري تدارك الفراغ القانوني الذي عرفه مجال الاجرام الالكتروني، فقام بتعديل قانون العقوبات بموجب قانون 04-15 جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات وحدد كل فعل منها وما يقابلها من جزاء.[2]

✓ المديرية العامة للأمن الوطني ودورها في مكافحة جريمة التزوير الالكتروني:

حيث قامت منذ 2003 بتكوين إطارات متخصصة ومتابعة مستمرة للتطورات الدولية، إضافة إلى دعم مصالح الشرطة العلمية وتأسيس خلايا مختصة على المستوى الوطني، كما اهتمت بالجانب التوعوي من خلال فتح موقع إلكتروني للتبليغ، وتنظيم حملات تحسيسية وندوات توعوية.[3]

✓ الدرك الوطني ودوره في مكافحة جريمة التزوير الالكتروني:

حيث بدأ منذ سنة 2004 بتكوين مستخدمين متخصصين، وإنشاء مركز وطني لمكافحة الجرائم المرتبطة بتكنولوجيا الاعلام والاتصال، كما استفاد من تكوينات في دول

---

[1]- أمير والي، إسحاق بلعمي، **مكافحة جريمة التزوير الالكتروني في الجزائر**، مذكرة مقدمة لنيل شهادة ماستر أكاديمي في الحقوق، تخصص قانون إعلام آلي، 2022-2023، برج بوعريريج، ص ص 32، 33.

[2]- جمال براهيمي، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، المجلة النقدية للقانون والعلوم السياسية، عدد 02، جامعة مولود معمري، تيزي وزو، ص ص 124، 125.

[3]- عبد الرحمان حملاوي، **دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية**، جامعة بسكرة، الجزائر، 2015، ص ص 03، 09.

متقدمة، وساهم في ندوات وطنية ودولية على المستوى المركزي، يعمل من خلال هيئات مثل المعهد الوطني للأدلة الجنائية ومركز مكافحة جرائم الإعلام الآلي، أما على المستوى المحلي فيضم فرق بحث وتحقيق متخصصة وخلايا علمية وتقنية لمواجهة هذا النوع من الجرائم.[1]

-العقوبات التي نص عليها المشرع الجزائري على تزوير بطاقات الدفع الالكتروني:

أقّر المشرع الجزائري على عقوبات صارمة لمكافحة جريمة التزوير الواقعة على بطاقات الدفع الالكتروني، وذلك بهدف حماية المعاملات المالية وتعزيز الثقة في الوسائط الرقمية أهمها:

- ✓ إنجاز المشرع الجزائري من خلال الفقرة 03 من المادة 219[2] من قانون العقوبات مضاعفة الحد الأقصى للعقوبة الأصلية والمتمثل في الحبس لمدة 05 سنوات لتصبح 10 سنوات ورفع قيمة الغرامة المالية من 20 ألف دينار لتصبح 40 ألف دينار إذا كان الشخص القائم بعملية من رجال المصارف أو مدير الشركة.
- ✓ العزل أو الاقصاء من جميع الوظائف والمنصب العمومي التي لها علاقة بالجريمة.
- ✓ الحرمان من حق الترشح والانتخاب.
- ✓ المنع من الإقامة.
- ✓ عدم الأهلية لأن يكون مساعدا محلفًا أو خبير أو شاهدًا أمام القضاء إلا على سبيل الاستدلال.
- ✓ الحرمان من الخدمة في المؤسسات التعليم بصفة أستاذ أو مدرس أو مراقب.
- ✓ عدم الأهلية بأن يكون وصيًا.

---

[1]– مريم أحمد مسعودي، **آليات مكافحة جرائم التكنولوجيا الاعلام والاتصال على ضوء القانون 09-04**، مذكرة مقدمة لنيل شهادة الماجستير، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2012-2013، ص 47.

[2]– المادة 219 من الأمر 66-156 المؤرخ في 2006/06/08، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 49.

الفرع الثاني: الحلول القانونية لتدارك تحديات مكافحة جريمة التزوير على مستوى التشريعات الدولية

تصطبغ الجرائم الالكترونية بصفة دولية وعابرة للحدود، مما يستوجب تظافر الجهود الدولية لمكافحتها، خاصة مع خروجها عن الإطار الفردي وقيام جهات غير منظمة بارتكابها دون انتماء ديني أو عرقي أو إقليمي، وأكدت على أهمية تعزيز التعاون القانوني والدولي لمواجهة هذه الجرائم، مع الإشارة إلى التحديات المرتبطة بالجوانب التشريعية والعملية، خاصة في حالات التزوير الالكتروني، وضرورة وضع حلول قضائية فعالة ضمن الأطر الوطنية والدولية، تعزيز المساعدة القضائية **(أولا)**، التدريب كآلية لمواجهة تحديات التعاون الدولي في مكافحة جريمة التزوير الإلكتروني **(ثانيا)**.

أولا: تعزيز المساعدة القضائية

فيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ في الرد نجد الحاجة ملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة من خلالها طلبات الإنابة لتعيين سلطة مركزية مثلا.[1]

وهذا بالفعل ما أوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة، والعدالة الجنائية المنعقدة في بانكوك 2005، حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعينة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية تنفيذ الطلبات وهذا ما نجده في البند الثاني من المادة 27 من الاتفاقية الأوروبية بشأن الاجرام المعلوماتي، وكذا المادة 35 من ذات الاتفاقية الأوروبية التي أوجبت على الدول ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يوميًا طوال أيام الأسبوع، وذلك من خلال المساعدة المباشرة للتحقيقات أو استقبال الأدلة في الشكل الالكتروني من الجرائم، كما أوجبت أيضا على الدول ضرورة أن نتمكن نقطة الاتصال السريع بنقطة الاتصال السريع بنقطة اتصال الطرف الآخر.[2]

---

[1]– يوسف حسن يوسف، **المرجع السابق**، ص 194.

[2]– غانم مرضي الشمري، **المرجع السابق**، ص 130.

ولقد لقيت المساعدة القضائية صدى كبير في العديد من الاتفاقيات سواء على الصعيد الدولي أو الإقليمي كمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنـــائية، وكذا المادة 48 فقرة 18 من البند 5 من اتفاقية الأمم المتحدة لمكافحة الفساد والتعاون الدولي والمادة الرابعة فقرة 1 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، وكذا ما جاء من الفقرات الثالثة والرابعة والخامسة من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية يضاف لها على المستوى الإقليمي ما أوصت به المادة الأولى من اتفاقية الرياض العربية وما ورد في المادتين الأولى والثانية من القانون الاسترشادي لاتفاقية التعاون القضائي والقانوني.[1]

أما بالنسبة للرد على طلبات إلتماس المساعدة فإنه من الضرورة الاستجابة الفورية والسريعة على هذه الطلبات لذلك نصت غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة السريعة والفورية.[2]

وبخصوص نقل الإجراءات كإحدى صور المساعدة القضائية فقد ازدادت إليها مع إشاعة الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال الحديثة، لكن ليس على الطريقة التقليدية والبطيئة القائمة على نقل الوثائق الخطية وإنما وفق وسائل فورية وسريعة وذات مصداقية بالقدر الذي يتطلبه التعامل مع مثل هذه الجرائم.[3]

---

[1]– جمال براهيمي، **المرجع السابق**، ص ص 317، 318.

[2]– وهذا ما أكدته الفقرة 3 من المادة 25 من الاتفاقيات الأوروبية للإجرام المعلوماتي، حيث نصت على أنه "يمكن لكل طرف في الحالات الطارئة أن يوجد طلب للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة، مثل الفاكس أو البريد الالكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها، ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر، وتقوم الدولة بالموافقة على هذا الطلب والرد على هذا الطلب والرد على هذا الطلب عن طريق إحدى وسائل الاتصال السريعة".

[3]– المادة 25 من الاتفاقية الأوروبية بشأن الإجرام المعلوماتي.

ولأجل هذا استحدث جلس الاتحاد الأوروبي آلية جديدة تسمى بقضاة الاتصال وهي تقنية تسمح لكل دولة عضو بتعين هيئة قضاة وطنية يكون اختصاصها الإشراف عن عملية المساعدة القضائية الدولية والتنسيق المباشر والفوري.[1]

كما ذهبت فرنسا إلى أبعد من ذلك إذ قامت بتعيين قضاة اتصال تعمل مع دول ليست أعضاء في الاتحاد، تساهم في تطوير وتسيير المساعدات القضائية بين دول الأعضاء من خلال اختصار الوقت والإجراءات وهذا من خلال التواصل المباشر.[2]

وفيما يتعلق بتبادل الإنابة القضائية كصورة من صور المساعدة القضائية هدفها تسهيل الإجراءات بين الدول، لذلك أصبحت المعاهدات والاتفاقيات الدولية تشترط على الدول إرسال الطلبات مباشرة وذلك من أجل اختصار الوقت وتسريع الإجراءات بدلا من الطرق الدبلوماسية التي تأخذ وقاتا طويلا.[3]

وفيما يتعلق بالتحديات تواجه نظام تسليم المجرمين كشكل من أشكال التعاون القضائي الدولي لمكافحة الجريمة، حيث سارعت معظم الدول في عقد اتفاقيات دولية وإقليمية لتبادل تسليم المجرمين، حيث كانت سباقة لذلك الدول الأوروبية فكانت أول اتفاقية عام 1957 في مجال تسليم المجرمين حيث نظمت كل ما يتعلق به من أحكام وشروط وإجراءات وقد تم تثبيتها لعام 2001.[4]

---

[1]– تم الاعتماد على هذه الآلية بشكل تجريبي، بموجب المادة الأولى من ورقة العمل المشترك المصادق عليها من طرف المجلس الأوروبي في 1996/04/22 طبقا للمادة 3 من اتفاقية الاتحاد الأوروبي، أنظر الجريدة الرسمية للاتحاد الأوروبي، عدد 105، الصادر في 1996/04/27.

[2] –Vuellta Simon، les nouveaux acteurs de la coopération pénale européenne LPAN :1-2005,P4.

[3]– نصت على ذلك المادة 27 فقرة 2 من الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 بقولها:

أ–يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسؤولة عن إرسال أو الرد على طلبات المساعدة المتبادلة أو إرسالها إلى السلطات المختصة.

ب–يجب على الهيئات المركزية أن تتصل ببعضها البعض بشكل مباشر".

[4]– تنص المادة 24 على أنه: "تطبق هذه المادة على تسليم فيما يبين الأطراف بالنسبة للجرائم المنصوص عليه في المواد من (2–11) من هذه الاتفاقية، تعبّر الجرائم الجنائية الواردة في الفقرة1 من هذه المادة مدرجة يجب فيها التسليم في أي اتفاقية بشأن تسليم المجرمين قائمة بين الأطراف ويتعهد الأطراف بإدراج هذه الجرائم على أنها تتم التسليم في أي اتفاقية بشأن تسليم المجرمين يتم إبرامها مما فيه".

ثانيا: التدريب كآلية لمواجهة تحديات التعاون الدولي في مكافحة جريمة التزوير الإلكتروني

إن التقدم الحاصل في تكنولوجيا الحاسب الآلي يفرض على جهات انقاد القانون أن تسير في خطوات متناسقة مع التطور الحاصل، والإلمام بها حتى يتمكن التصدي لتلك الأفعال الإجرامية، ومن ناحية أخرى فإن أعمال القانون في مواجهة الجزائر الالكترونية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم العقابية التقليدية لما تتسم به هذه الجرائم من سرعة وسهولة في التنفيذ والقدرة على محو آثارها.[1]

وبالتالي فإن ظهور الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق جميع أجهزة العدالة الجنائية، لذلك يجب أن تكون على درجة كبيرة من الكفاءة على كشف غموض تلك الجرائم وهذا لا يتحقق إلا بالتدريب ومن هذا المنطلق وجوب تأهيل القائمين على هذه الأجهزة كما أن الدولة لا يمكن بمفردها النجاح في مواجهة هذا النوع من الإجرام وهنا كانت الحاجة إلى ضرورة وجود تعاون دولي في مجال التدريب وهذا ما سنوضحه فيما يلي:

أ-أهمية التدريب في مجال مكافحة جريمة التزوير الالكتروني:

يعد التدريب[2] جزء من عملية التنمية الإدارية ويهتم بالكفاءة والفعالية في إنجاز العمل، وهذا ما حرصت عليه الكثير من المنظمات العامة والخاصة، إضافة إلى تحمل المزيد من المسؤوليات من خلال زيادة قدراتهم على مواجهة المهام المعقدة.[3]

---

[1]- السيد عبد الحميد أحمد، **جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية**، مكتب الوفاء القانونية، مصر، 2018، ص 136.

[2]- يعرف التدريب بأنه: "نشاط مستمر ومخطط يهدف إلى سد الفجوة بين الأداء الحالي والأداء المتوقع لشاغل الوظيفة، ومن ثم إحداث التغيرات في سلوك وقدرات الفرد أو الجماعة المسؤولة عن أداء هذه الوظيفة"، أنظر، صالح محمد النويجم، تقوم كفاءة العملية التدريبية في معاهد التدريب الأمنية، بمدينة الرياض من وجهة نظر العاملين فيها، **رسالة ماجستير في العلوم الإدارية**، جامعة العلوم الأمنية، الرياض، 2003، ص 9.

[3]- يوسف حسن يوسف، **المرجع السابق**، ص 176.

يعد التدريب المتخصص في تكنولوجيا المعلومات ضرورة لمكافحة التزوير الالكتروني، مع التركيز على الجوانب الفنية والعملية واكتساب الخبرات من مدربيـن مؤهلين، لضمان كفاءة رجال القانون في التعامل مع هذه الجرائم.[1]

ويجب أن يشمل المنهج التدريبي على بيان المخاطر ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب وكذلك ذكر الصفات التي يتميز بها المجرم المعلوماتي والدافع وراء ارتكاب لجريمة الالكترونية.[2]

وفيما يتعلق بمنهج التحقيق فإنه لابد أن يشتمل على إجراءات التحقيق والتخطيط وجمع المعلومات وتحليلها وكذا طريقة الاستجواب.[3]

بالإضافة إلى ذلك لابد أن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على أدلة فيما يخص الملاحقة الدولية والتعاون.[4]

ويتطلب أن يقوم بالتدريب جهة مختصة ولها الخبرة الكافية في اختيار المتدربين والصفات المميزة ولابد لعملية التدريب أن تكون مستمرة لأن هذه الجرائم في تطور مستمر وسريع، ويجب على الجهات الأمنية مسؤولية عن التحقيق.[5]

ب-مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجنائية:

يتجلى التعاون الدولي في مجال تدريب رجال العدالة الجنائية من خلال تنظيم برامج ودورات تدريبية مشتركة، وتبادل الخبرات والمعلومات حول أساليب التحقيق والتقنيات الحديثة، إضافة إلى تقديم الدعم الفني واللوجستي وإيفاد خبراء دوليين لتأهيل الكوادر

---

[1]- غانم مرضي الشمري، **المرجع السابق**، ص ص 116، 117.

[2]- السيد عبد الحميد أحمد، **المرجع السابق**، ص 140.

[3]- هشام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية-دراسة مقارنة**، مكتبة الآلات الحديثة، مصر، 1994، ص 497.

[4]- السيد عبد الحميد أحمد، **المرجع السابق**، ص 140.

[5]- غانم مرضي الشمري، **المرجع السابق**، ص 118.

المحلية، فضلا عن عقد اتفاقيات تعاون ثنائية ومتعددة الأطراف لتعزيز كفاءة أجهزة إنفاذ القانون في مكافحة الجريمة.[1]

ففي مصر نجد النيابة العامة تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقد داخل مصر أو خارجها، بالإضافة إلى إرسال أعضاء النيابة العامة من مختلف الدرجات.[2]

والهدف من عقد هذه اللقاءات والندوات لتبادل الخبرات وتعزيز التعاون الدولي في مجال مكافحة الجرائم الالكترونية من خلال التدريب وتطوير القدرات الفنية للجهات المختصة، كما نبرز دور الولايات المتحدة في تقديم الدعم الفني والتقني للدول الأخرى، بما في ذلك تدريب الشرطة والقضاة وأجهزة العدالة الجنائية، بهدف تحسين فعلية التصدي للجرائم الحديثة وتعزيز تطبيق القانون عبر التعاون الدولي.[3]

---

[1]– يقصد بتدريب رجال العدالة تلك العملية التي يخطط لها وتصمم لها البرامج ويبذل لها الجهد والمال وتغيير سلوك العاملين في أجهزة العدالة سواء كانوا من القضاة أو رجال التحقيق أو النيابة العامة أو رجال الضبط القضائي، وهذا بهدف رفع مستوى كفاءاتهم ومهاراتهم للمزيد أنظر، السيد عبد الحميد أحمد، **المرجع السابق**، ص 144.

[2]– غانم مرضي الشمري، **المرجع السابق**، ص 119.

[3]– **المرجع نفسه**، ص 120.

خلاصة الفصل:

بما أن جريمة تزوير بطاقات الدفع الالكتروني من أخطر الجرائم الالكترونية، نظرا لما تسببه من أضرار جسيمة للأفراد والمؤسسات، وإخلال الثقة بالنظام المالي، فحماية البطاقات أصبحت ضرورة ملحة للتصدي لمثل هذه الجرائم، وذلك من خلال وضع مجموعة من الإجراءات الوقائية والتي تتخذ قبل وقوع الجريمة، وإجراءات ردعية تتم بعد وقوع الجريمة بداية بمباشرة الدعوى وصولا إلى المحاكمة والقبض على الجاني، ونظرا لخصوصية هذه الجريمة والصعوبات التي لحقت الدول من أجل القضاء على التزوير الالكتروني اقترحت التشريعات بعض الحلول القانونية للحد والتقليل من الجرائم الالكترونية خاصة التزوير.

خاتمة

خـــاتمة:

وفي الختام نستنتج بأن بطاقات الدفع الالكتروني أداة أساسية في المعاملات المالية الحديثة، غير أن سهولة استخدامها وانتشارها أخيرا جعلها عرضة لمخاطر متعددة أبرزها جريمة التزوير الالكتروني التي تعد من الجرائم المعقدة التي تدمج بين الأساليب الاحتيالية التقليدية وتقنيات الرقمية الحديثة، مما استوجب حماية جنائية لبطاقة الدفع الالكتروني من هذه الجريمة من خلال النصوص القانونية تجرم فعل التزوير، واستخدام بطاقات بطرق غير مشروعة وذلك لضمان الأمن المالي في العصر الرقمي، لذلك يجب على التشريعات والسلطات المختصة الاستمرار في تطوير هذه الحماية بما يواكب التغيرات المتسارعة في هذا المجال، خاصة في ظل تطور الأساليب التقنية المستخدمة في التزوير.

وفي نهاية هذه الدراسة توصلنا إلى مجموعة من النتائج والتوصيات سنوضحها كالآتي:

أولا: النتائج

توصلنا إلى مجموعة من النتائج تتمثل في:

- أن جرائم تزوير بطاقة الدفع الالكتروني يدخل ضمن الجرائم المعلوماتية التي هي وليدة استخدام تقنيات معلوماتية.
- المجرم الالكتروني أخطر من المجرم التقليدي لأنه يصعب الكشف عليه.
- صعوبة الكشف عن جريمة التزوير نظرا لطبيعتها الغير مادية وقابلية البيانات للحذف.
- الحاجة الماسة لتحديث الأدلة الجنائية الرقمية وتدريب الكوادر المختصة في التحقيقات الالكترونية.
- تعد البطاقة الالكترونية وسيلة مستحدثة للوفاء دون أن يتم الدفع نقدا.

ثانيا: التوصيات

من خلال دراستنا للموضوع توصلنا لبعض التوصيات تتمثل فيما يلي:

- ضرورة سن تشريعات جنائية متخصصة لمكافحة جريمة التزوير الالكتروني تشمل نصوص واضحة حول تزوير بطاقات الدفع.
- إجراء دورات تحسيسية وتوعوية للمخاطر الالكترونية المترتبة عن جرائم البطاقات الالكترونية لتجنب الوقوع فيها.
- تعزيز التعاون الدولي لتتبع وملاحقة مرتكبي جرائم التزوير.
- التنسيق الأمني على المستوى الدولي مع الأجهزة المتخصصة في هذا المجال لضمان استقرار المعاملات المالية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر

أ-القوانين:

1- القانون 04-14 المؤرخ في 10 نوفمبر 2001 المعدل والمتمم لأمر رقم 56-155، المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائرية، ج.ر، عدد 71، 41، الصادر بتاريخ 10 نوفمبر 2004.

2- القانون 05-15 المؤرخ في 16 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1986 الموافق لـ 8 يونيو 1996، المتضمن قانون العقوبات، ج.ر، عدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

3- القانون 05-02 المؤرخ في 6 فبراير 2005 يعدل ويتمم الأمر رقم 75-59 في 26 سبتمبر 1975 والمتضمن القانون التجاري، ج.ر، العدد 11، 2005.

4- القانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم 66-155، المتضمن قانون الإجراءات الجزائرية، ج.ر، للجمهورية الجزائرية، العدد 84، الصادر بتاريخ 24 ديسمبر 2006.

5- القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، الجمهورية الجزائرية الديمقراطية الشعبية، المؤرخة في 25 شعبان 1430 الموافق لـ 16 أوت 2009.

6- القانون 05-10 المؤرخ في 18 جمادى الأولى عام 1426 الموافق لـ 6 يونيو 2005 المعدل والمتمم للقانون المدني، ج.ر، الجمهورية الجزائرية الديمقراطية الشعبية، المؤرخة في 30 يناير 2006، المتعلق بمكافحة جرائم تقنية المعلومات، ج.ر، العدد 442، الصادر في 31 يناير 2006.

-القوانين الأجنبية:

1- القانون الفرنسي رقم 91-1382 المتعلق بأمن الشيكات وبطاقات الأداء المؤرخ في 30-12-1991 يعدل ويتمم أحكام المرسوم المؤرخ في 30 أكتوبر 1985.
2- قانون العقوبات الفرنسي، المتضمن أحكام تجريم المستندات المعالجة آليا، المؤرخ في 23-12-1981 الصادر في 1988.
3- قانون التوقيع المصري رقم 15-2004، المؤرخ في 6 أفريل 2004.
4- القانون رقم 58 لسنة 1937، المتضمن قانون العقوبات المصري المعدل بتاريخ 2 أفريل 2018.
5- القانون المصري رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنيات المعلومات، المؤرخ في 14 أغسطس 2018، ج.ر، العدد 32 مكرر في 14 أغسطس 2018.
6- loi N2001,1062,15nov-2001 relative a la sécurité quotidienne. JORF 16 Nov-2001.
7- loiN:2004-239,18mars2003 pour la sécurité intérieure, JORF 19 mars 2004.
8- loi N-2003-239.18mars2003 pour la sécurité intérieure, JORF 19 mars 2003.
9- loi N-2004, 9 mars 2004, pourtant adaptant de la justice aux évolution de la criminalité, JORF 19 mars, 2004.
10- loi N-2004-575-21 juin 2004 pour la crnfience a de l'économie numérique, JORF 22 juin 2004.
11- loi N-2004-669 du 9 juillet 2004 relative aux communications, JORF du 10 juillet 2004.

-القوانين الدولية:

1- قانون الأنسترال النموذجي للتجارة الإلكترونية الدولية 1996.

ب-الأوامر:

1- الأمر 06-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم بموجب الأمر 08/21، المؤرخ في 8 يونيو 2021، ج.ر، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 45، الصادر بتاريخ 9 يونيو 2021.

2- الأمر 03-05 المؤرخ في 2003/07/19، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر، رقم 44، المؤرخة في 2003/07/23.

3- الأمر 03-11 المؤرخ في 27 جمادى الثانية عام 1424 الموافق لـ 2003/08/27، المتعلق بالنقد والقرض، ج.ر، العدد 52، المعدل والمتمم.

ج-المراسيم:

1- المرسوم سلطاني، رقم 05-2015 الصادر في 17 جمادى الأولى 1436هـ، الموافق لـ 8 مارس 2015، ج.ر، عدد 193، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات.

د-الاتفاقيات:

1- الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية.

2- اتفاقية بودابست المتعلقة بالجريمة الالكترونية.

3- اتفاقية مجلس أوروبا المتعلق بمكافحة الجريمة الالكترونية.

هـ- القرارات:

1- القرار رقم 65-01-07 قرارات وتوصيات المجمع الفقهي في دورته السابعة المنعقدة بجدة 1412هـ.

ثانيا: المراجع

1-الكتب:

1- أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، ط9، الجزء 2، دار هومة، الجزائر، 2008.

2- أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دراسة مقارنة، دار الفكر الجامعي، 2006.

3- أحمد عبد العليم العجمي، نظام الدفع الإلكتروني وانعكاساته على سلطات البنك المركزي، دار الجامعة الجديدة، مصر، 2013.

4- إسماعيل بن حماد الجوهري، تاج اللغة وإصحاح اللغة العربية، الطبعة الرابعة، دار العلم للملايين، بيروت، لبنان.

5- أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الالكتروني، دار المسيرة، عمان، 2010.

6- أنس العلبي، النظام القانوني لبطاقات الاعتماد، منشورات الحلبي الحقوقية، لبنان، 2005.

7- أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الالكتروني-دراسة مقارنة، دار النهضة العربية، القاهرة، 2011.

8- إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقة الائتمان، دار الجامعة الجديدة للنشر، مصر، 2007.

9- إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقة الائتمان، دار الجامعة الجديدة للنشر، مصر، 2007.

10- بكير علي محمد أبو بكر، الطبيعة القانونية لبطاقة الائتمان، المركز القومي للإصدارات القانونية، القاهرة، مصر.

11- بيار إميل طوبيا، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، د ط، منشورات الحلبي الحقوقية، بيروت، 2000.

12- جمال نجيمي، جرائم التزوير في قانون العقوبات الجزائري، دار هومة، الجزائر، 2013.

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

14- حسين محمد الشلبي، محمد مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولى، دار مجلاوي للنشر والتوزيع، عمان، 2009.

15- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية-دراسة مقارنة-، منشورات الحلبي الحقوقية، لبنان، 2014.

16- حنان ريحان مباركي المضحكي، الحماية الجنائية لبطاقة الائتمان والممغنطة، دراسة مقارنة، منشورات الحلبي الحقوقية، 2012.

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

18- رياض فتح الله بصلة، جرائم بطاقة الائتمان، دار الشروق، بيروت، لبنان، 1995.

19- السيد عبد الحميد أحمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، الطبعة الأولى، مكتب الوفاء القانونية، مصر، 2018.

20- صلاح الدين حسن السيسي، اقتصاد الفساد، دار الكتاب الحديث، القاهرة، 2012.

21- طارق طه، إدارة البنوك في بيئة العولمة والأنترنت، دون طبعة، دار الجامعة الجديدة للنشر والتوزيع، مصر، 2007

22- عادل يوسف عبد النبي شكري، الفقه الجبائي، ط1، دار الصفاء، الأردن، 2012.

23- عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، دار هومة، الجزائر، 2005.

24- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والأنترنت في التشريعات العربية، الطبعة الأولى، دار النهضة العربية، مصر، 2009.

25- عبد الكريم الردايدة، جرائم بطاقة الائتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013.

26- عبد الوهاب أبو سليمان، البطاقات البنكية، دار القلم، 1993.

27- عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، 2009.

28- علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية في قانون التجارة الجديد وتشريعات البلاد العربية، ط4، دار النهضة العربية، القاهرة، 2008.

29- علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية-دراسة مقارنــة، د ط، المكتب الجامعي الحديث، الموصل، 2012.

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

31- غانم مرضي الشمري، الجرائم المعلوماتية، الدار العلمية للنشر والتوزيع، الأردن، 2016.

32- فايز نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

33- فايز نعيم رضوان، بطاقات الوفاء، دار النهضة العربية، القاهرة، 1999.

34- فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص وفقا لأحدث التعديلات، ط3، دار النهضة العربية، مصر، 2012.

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

36- محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، مصر.

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

38- محمد عبيد الحسين الطائي، التسويق والتجارة الإلكترونية، المكتبة العصرية للنشر والتوزيع، مصر، 2008.

39- محمد فتحي عيد، الاجرام المعاصر، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2014.

40- محمود إبراهيم غازي، الحماية الجنائية الخصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014.

41- مسعود خثير، الحماية الجنائية لبرنامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر.

42- معادي أسعد صوالحة، بطاقة الائتمان، النظام القانوني وآليات الحماية الجنائية والأمنية، المؤسسة الحديثة للكتاب، لبنان، 2012.

43- معتز نزيه، محمد الصادق المهدي، المتعاقد المحترف، مفهومه والتزامه ومسؤوليته، دار النهضة العربية، القاهرة، مصر، 2009.

44- منير محمد الجنيهي، ممدوح الجنيهي، جرائم الأنترنت والحاسب الآلي، ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004.

45- ناظمة محمد نوري الشعري، عبد الفتاح زهير عبدلات، الصيرفة الإلكترونية، دار وائل للنشر، الأردن، 2008.

46- نبيل صقر، الوسيط في الجرائم المخلة بالثقة العامة، دار الهدى، الجزائر، 2015.

47- نجاح محمد فوزي، وعي المواطن العربي اتجاه جرائم الاحتيال، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

48- هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية، مصر، د.س.

49- هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، مصر، 2012.

50- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية-دراسة مقارنة، دون طبعة، مكتبة الآلات الحديثة، مصر، 1994.

51- وسام فيصل محمود الشو عبد الكريم الردايدة، اوة، المسؤولية القانونية عن الاستخدام غير المشروع لبطاقات الائتمان، الطبعة الأولى، دار وائل للنشر، عمان، 2013.

52- يوسف بكري، التفتيش من المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، 2011.

53- يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي الإصدارات القانونية، مصر، 2011.

2-المقالات:

1- إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، الامارات العربية المتحدة، 2000.

2- أشرف توفيق شمس الدين، حجية المحررات الإلكترونية في الاثبات، ورقة عمل مقدمة في ندوة المعاملات القانونية.

3- جمال براهيمي، مكافحة الجريمة الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، عدد 02، جامعة مولود معمري، تيزي وزو.
4- عادل يوسف شكري، " الحماية الجنـــائية لبطاقـــات الدفع الإلكتـــروني (دراسة مقارنة)"، مجلة الحماية الجنائية، المجلد الأول، العدد 11، كلية الحقوق، جامعة الكوفة، د.س.ن.
5- عبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة بسكرة، الجزائر، 2015.
6- عبد العالي النجار، التجارة نقود المعرفية وآليات تناولها، بحث مقدم في المؤتمر السنوي لكلية الحقوق حول الجديد في أعمال المصاريف من الوجهتين القانونية والاقتصادية، جامعة بيروت، لبنان، 2002.
7- علي كحلون، " الجريمة المعلوماتية وتوجيهات محكمة التعقيب "، مجلة الأخبار القانونية، تونس، المجلد126، العدد127، جانفي 2012.
8- علي محمود علي محمود، الأدلة المحصلة من الوسائل الالكترونية في إطار نظريات الجنائي، بحث مقدم إلى المؤتمر العلمي حول الجوانب القانونية للمعلومات الالكترونية، الإمارات العربية المتحدة، 2003.
9- عمر سليمان الأشقر، " بطاقة الائتمان الممغنطة ومخاطر التزوير "، المجلة العربية للدراسات الأمنية والتدريب، السنة العاشرة، العدد 19، السعودية،1995.
10- فاطمة بوعناد، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، عدد 01، الجزائر، 2013.
11- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، الطبعة الثالثة، كلية الشريعة والقانون، الإمارات العربية المتحدة، الفقرة من 1إلى 3، ماي 2004.
12- محمد علي سليمان، عباس طالب زروقي، " الأساس القانوني لحماية بطاقة الائتمان من التزوير "، مقال منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد 02، 2015.

13- محمد عوض محمد، مشكلات السياسة الجنائية المعاصرة من جرائم نظر المعلومات، بحث مقدم إلى مؤتمر القانون الكمبيوتر والأنترنت، الفقرة 1- 3 ماي 2000، كلية الشريعة والقانون، الامارات العربية المتحدة.

14- نوال حاج مخناش، " التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني "، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أفريل 2009.

3-الملتقيات:

1- محمد بن عزة جليلة زويهري، عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر، "عرض تجارب دولية"، الملتقى الدولي الرابع، المركز الجامعي خميس مليانة، عين الدفلى، الجزائر، 2011.

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

4-محاضرات:

1- عطية سالم عطية، بطاقات الدفع الإلكتروني وأهميتها في عصرنا، محاضرات البنك الأهلي المصري، محاضرة رقم 12، معهد الدراسات المصرفية، 1998/1997.

5-الموسوعات:

1- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والأنترنت، موسوعة الجرائم المعلوماتية، منشأة المعارف، الإسكندرية، 2006.

4-الرسائل الجامعية:

أ-أطروحات دكتوراه:

1- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2016.

2- بن تركي ليلى، الحماية الجنائية لبطاقات الائتمان الممغنطة، أطروحة لنيل شهادة الدكتوراه، تخصص العقوبات والعلوم الجنائية، جامعة الإخوة منتوي، قسنطينة، 2016-2017.

3- بن شهرة شول، الحماية الجنائية للتجارة الإلكترونية، شهادة الدكتوراه، كلية الحقوق، تخصص جنائي، 2011/2010.

4- جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة مكملة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2018.

5- حسن ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016.

6- حسين الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت-دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين الشمس، مصر.

7- حسين بن سعد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2007.

8- حفصي عباس، جرائم التزوير الإلكتروني، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم الإسلامية، تخصص شريعة وقانون، جامعة وهران1، 2015/2014.

9- صالح شنين، الحماية الجنائية للتجارة الإلكترونية-دراسة مقارنة، رسالة لنيل الدكتوراه في القانون الخاص، محمد رايس، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2013.

10- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت-دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2014.

11- نوال بلعباس، بطاقة الائتمان كوسيلة من وسائل الدفع الحديثة، أطروحة لنيل شهادة دكتوراه علوم في القانون، تخصص قانون خاص، كلية الحقوق، جامعة الجزائر1، 2016-2017.

12- هدى برابح، بطاقة الائتمان البنكية والجرائم المتعلقة بها، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون بنكي ومالي، كلية الحقوق العلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2021-2022.

ب-رسائل الماجستير:

1- جهاد رضا الحباشنة، الحماية الجزائرية لبطاقة الوفاء، رسالة ماجستير، دار الثقافة، عمان، 2008.

2- عبد محمد بحر، معوقات التحقيق في جرائم الأنترنت، مذكرة مكملة لنيل شهادة الماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، دبي، 1999.

3- عذبة سامي حميد الجابر، العلاقات التعاقدية المنبثقة عن استخدام بطاقة الائتمان، رسالة ماجستير في القانون الخاص، كلية العلوم القانونية، جامعة الشرق الأوسط للدراسات العليا، الأردن، 2008.

4- كريمة صراع، واقع وآفاق التجارة الالكترونية في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم التجارية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، الجزائر، 2014.

5- مريم أحمد مسعودي، آليات مكافحة جرائم التكنولوجيا الاعلام والاتصال على ضوء القانون 09-04، مذكرة مقدمة لنيل شهادة الماجستير، تخصص قانون

جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2012-2013.

6- وسيلة رزيق، بطاقة الائتمان كوسيلة جديدة في النظام المصرفي، رسالة الماجستير، فرع قانون أعمال، جامعة الجزائر، كلية الحقوق، 2010.

ج-مذكرات الماستر:

1- أمير والي، إسحاق بلعلمي، مكافحة جريمة التزوير الإلكتروني في الجزائر، مذكرة مقدمة لنيل شهادة الماستر، تخصص إعلام آلي، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022-2023.

2- خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الإلكترونية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2014-2015.

5-المراجع باللغة الأجنبية:

1- Chopin Frédérique, les politiques publiques de lutte contre la cybercriminalité, ajipénal, paris, France.

2- Vuellta simon, les nouveaux acteurs de la coopération pénale européenne LPAN :1-2005.

فهـرس المحتويـات

فهـــرس المحتويـــات

الملخص:

في ظل التطور السريع للتكنولوجيا المالية أصبحت بطاقات الدفع الالكتروني من أبرز الوسائل المستخدمة في المعاملات المصرفية، لكن هذا التطور رافقه ظهور أساليب إجرامية مستحدثة أبرزها تزوير بطاقات الدفع الالكتروني التي باتت تشكل خطرا تهديدا مباشر في المنظمة المالية، مما استدعى تدخلا تشريعيا وأمنيا لتوفير حماية جنائية لها تفرضها طبيعة العصر الرقمي، لأن التزوير الالكتروني يشكل جريمة خطيرة وحديثة، تستدعي تشريعات خاصة وآليات متطورة لضمان أمن المعاملات المالية.

الكلمات المفتاحية: بطاقات الدفع الإلكترونية، جريمة التزوير.

Abstract:

In light of the rapid development of financial technology, electronic payment cards have become one of the most prominent means used in banking transaction. However, this development has been accompanied by the emergence of new criminal methods, the most notable of which is the counterfeiting of electronic payment cards, which has become a direct threat to the financial organization. This necessitated legislative and security intervention to provide criminal protection for these cards imposed by the nature of the digital age, as electronic counterfeiting constitutes a serious and modern crime that requires special legislation and advanced mechanisms to ensure the security of financial transaction.

Keywords: the crime of forgery, electronic payment cards.