وزارة التعليم العالي والبحث العلمي

Ministry of high education and scientific research

جامعة محمد البشير الابراهيمي –برج بوعريريج–

University of Mohamed el Bachir el Ibrahimi–bba-

كلية الحقوق والعلوم السياسية

Faculty of law and political science

مذكرة مكملة لنيل شهادة الماستر في الحقوق تخصص: قانون أعمال

التحقيق الجزائي في جرائم تزوير البطاقات المصرفية

إعداد الطالبتين:

بليلي امينة

كمال مارية نسرين

إشراف الدكتور:

بكيس عبد الحفيظ

لجنة المناقشة:

الإسم و اللقب	الرتبة	الصفة
سي حمدي عبد المؤمن	أستاذ محاضر أ	رئيسا
بكيس عبد الحفيظ	دكتور	مشرفا ومقررا
عجيري عبد الوهاب	أستاذ محاضر أ	مناقشا

الموسم الجامعي : 2024/2023

* ملحق بالقرار رقم ... المؤرخ في .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): دلبلي أحينة الصفة: طالب، أستاذ باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم: 109090 والصادرة بتاريخ 19/11/2020

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم علوم قانونية تخصص قانون أعمال

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

عنوانها: التحقيق الجزائي في جرائم تزوير البطاقات الممغنطة

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

التاريخ: 2023.06.18

توقيع المعني(ة)

عن رئيس المجلس الشعبي البلدي
وبتفويض منه
رئيس مصلحة التنظيم والشؤون العامة

ملحق بالقرار رقم ... المؤرخ في .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

1

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): كمال مازيغ لسرين الصفة: طالب، أستاذ باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم: 109823 والصادرة بتاريخ 28/01/22

المسجل(ة) بكلية / معهد: الحقوق والعلوم السياسية قسم: علاقات قانونية أعمال

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

عنوانها: التحقيق الجزائي في جرائم تزوير البطاقات المصرفية

.....

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

التاريخ: 14/06/2023

توقيع المعني(ة)

عن رئيس المجلس الشعبي البلدي
وبتفويض منه
رئيس مصلحة التنظيم والشؤون العامة
نفطي محمد
14 جوان 2023


بسم الله الرحمن الرحيم
Sidi

الشكر والتقدير

اشكرك ربي على نعمك وفضلك الذي مننت به علينا بان وفقتنا الإنجاز هذا العمل.

ولا يسعنا الا ان نتقدم بجزيل الشكر والامتنان والتقدير للدكتور الفاضل بكيس عبد الحفيظ.

الذي أشرف على هذا العمل وتعهده بالتصويب في جميع مراحل إنجازه.

والذي زودنا بالنصائح والارشادات فكان لنا السراج الذي يضيء الطريق.

فجزاه الله كل خير وله منا تحية اجلال وتقدير.

كما لا يفوتنا ان نشكر أعضاء اللجنة المناقشة على ما تجشموه من تعب في سبيل تقييم هذا

العمل فلهم وافر الشكر أيضا والتقدير.

الإهداء

ها انا الان أقف الا قول كلماتي الختامية لكل هذه السنين.

من قال انا لها" نالها" وانا لها وان ابت رغما عنها اتيت بها.

الى من ساندني بكل حب عند ضعفي ...

الى من رسموا لي المستقبل بخطوط من الثقة والحب...

اليكم عائلتي ...

والى معلمي الأول وسندي الثابت في كل خطوات حياتي، مصدر فخري وسعادتي الذي لا أرى الدنيا الا به والدي العزيز حفظه الله.

الى من وضعتني على طريق الحياة وغمرتني بحبها وحنانها، الى من مهدت لي طريق العلم الى من لهج لسانها للدعاء لي امي الغالية حفظها الله.

والى الشموع التي تنير لي الطريق دوما اخواني واخواتي.

والى روح جدي الطاهرة رحمه الله

بليلي أمينة

الإهداء

الحمد لله الذي بنعمته تتم الصالحات في طياتها الكثير من الصعوبات والتعب. ها أنا أقف على عرش التفوق والنجاح بكل فخر وعزة وبهذه المناسبة العظيمة اهدي تخرجي لأهلي فرداً فرداً وإلى كل من ساندني بكلمة وإلى كل من وقف معي، وبالأخص قرة عيني وسر نجاحي أمي الغالية وسندي الدائم الذي لا يميل أبدا أبي كما أنني لن أنسى روحا لم تفارقني يوما أمي الحبيبة التي أنجبتني رحمها الله واسكنها فسيح جنانه

كمال ماريا نسرين

المقدمة

مقدمة

يعد التقدم التكنولوجي المعلوماتي وعولمة السوق من أبرز التطورات العالمية المعاصرة التي حدثت خلال العقد الماضي، وقد أسهمت هذه التطورات في تقديم العديد من المنافع والمزايا. حيث أسهمت العولمة في حدوث العديد من التأثيرات الإيجابية، التي من أهمها سهولة انتقال التكنولوجيا وتدفق الاستثمارات والاستفادة من التجارة الالكترونية.

وانه أصبح واضحا ان تكنولوجيا المعلومات تتمتع بإمكانيات هائلة للنهوض بتنمية النمو الاقتصادي، حيث أدى التقدم الحضاري التكنولوجي الى اختراع العديد من وسائل والأدوات المتطورة وابتكار العديد من الأجهزة الدقيقة، وساهمت هذه الأخيرة بشكل فعال بالتأثير والتغيير على أنظمة الدفع حيث اذ بطاقات الدفع الالكتروني اخذت شيئا فشيئا محل وسائل الدفع التقليدية.

بالرغم من المزايا والمنافع الهائلة الناجمة عن عمليات العولمة والتقدم التكنولوجي في المعلومات والاتصالات، الا انه في ذات الوقت تنجم عنها بعض الظواهر والتأثيرات السلبية خصوصا في مجال جرائم البطاقات المصرفية بالتحديد جريمة التزوير. حيث يعد التلاعب بالبطاقات المصرفية عن طريق التزوير من اهم المعضلات التي تواجه الاقتصاد والمجتمع، لما ينجم عليه من اخطار تؤدي الى زعزعة الثقة في التعاملات المالية والتجارية وهي من

الجرائم غير العادية كونها ذات طبيعة خاصة تتضمن مفهوما جديدا للجريمة وسلوكا اجراميا متميزا ومختلفا عن الجرائم التقليدية الأخرى، وهذا ما يتطلب استحداث آليات وأساليب جديدة وفكر متطور في التعامل مع هذا النوع من الجرائم سواء من قبل الهيئات المصرفية من حيث وضع وتحديث تقنيات التامين او من الأجهزة الأمنية والقضائية من خلال التحقيقات وإجراءات الخبرة.

وكذلك دور المشرع الجزائري في استحداث النصوص القانونية الكفيلة بحماية التعامل ببطاقات الائتمان، ولكونها جريمة ذات خصوصية تستوجب أساليب بحث وتحري مختل تبرز أهمية هذا الموضوع في حداثته، حيث يسلط الضوء على واحدة من جرائم العصر في مجال المعاملات المصرفية الالكترونية الا وهي جريمة تزوير البطاقات المصرفية، وهي جريمة جديدة مما يجعلها تختلف في مكنزماتها عن جريمة التزوير التقليدية، حيث أصبحت البطاقات المصرفية أكثر استعمالا في وقتنا الحالي، وهو ما استغله مجرمو المعلوماتية في ارتكاب هذه الجريمة مما يهدد الثقة بالتعامل بالبطاقات المصرفية.

وتهدف هذه الدراسة الى:

-مطابة النصوص القانونية في تجريم بعض التصرفات غير المشروعة.

-تعرف على القوانين التي سنها المشرع في سبيل حماية البطاقات المصرفية في جريمة التزوير.

-دور المشرع الجزائري في المحافظة على الأموال وحمايتها من التلاعب والتصرفات الغير المشروعة التي تستهدف الاستيلاء عليها.

-التعرف على جريمة التزوير في الجانب المعلوماتي.

-توضيح الطبيعة القانونية لبطاقة الائتمان.

من بين الأسباب الذاتية لاختيارنا لهذا الموضوع الميل للبحث والاستطلاع في هذا الموضوع واكتشاف خباياه وكذا محاولة معالجته من الجوانب القانونية والمساهمة بالجديد.

اما الأسباب الموضوعية من أهمها هي الحداث القانونية للموضوع وانعدام قانون يظمه بالرغم من ان البطاقات المصرفية عرفت انتشارا كبيرا في المجال المصرفي.

من بين الصعوبات التي وجهناها خلال بحثنا الا وهي قلة المراجع التقليدية، مما دفعنا الى الاعتماد على المراجع الالكترونية وكذلك سرية إجراءات التحقيق الجزائية التي خصص لها قطب خاص بقاضي التحقيق.

ومن اهم المراجع التي اعتمدنا عليها:

– دراسة معنونة: "**إجراءات التحقيق في الجريمة الالكترونية** «: وهي مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، بخي فاطمة الزهراء، نوقشت بجامعة المسيلة محمد بوضياف، كلية الحقوق والعلوم السياسية قسم الحقوق، سنة 2014/2013.

– دراسة معنونة: "**جريمة التزوير في بطاقات الائتمان**": وهي أطروحة مقدمة لنيل شهادة الدكتوراه في القانون، عبد العزيز نقطي، نوقشت في جامعة الوادي، مخبر السياسة العامة وتحسين الخدمة العمومية في الجزائر، سنة 2022.

وهذا ما يدفعنا لطرح الاشكال الاتي:

ما مدى فعاليات الإجراءات والتدابير المتخذة في التحقيق الجزائي لحماية البطاقات المصرفية؟

وسنحاول الإجابة على هذا الاشكال وفق منهج وصفي تحليلي بهدف الوصول الى الأهداف المرجوة من هذه المذكرة المفصلة في محاولة الإحاطة بكل الجوانب القانونية لهذا النوع من وسائل الدفع.

لكي نتمكن من تحقيق اهداف هذه الدراسة، والاجابة على إشكالية البحث قمنا بتقسيم بحثنا الى فصلين:

الفصل الأول بعنوان: جريمة التزوير الإلكتروني في البطاقات المصرفية والذي قسمناه الى مبحثين خصصنا **المبحث الأول** الإطار المفاهيمي لجريمة التزوير الالكتروني اما **المبحث الثاني** الإطار المفاهيمي لجريمة التزوير بطاقة الائتمان.

اما الفصل الثاني بعنوان: الحد من جريمة التزوير الالكتروني في البطاقات المصرفية والذي قسمناه بدوره الى مبحثين حيث تناولنا في **المبحث الأول** إجراءات التحقيق في جريمة تزوير البطاقات المصرفية وفقا للجرائم الالكترونية اما **المبحث الثاني** الحماية القانونية للبطاقات المصرفية.

الفصل الأول:

جريمة التزوير الالكتروني في البطاقات المصرفية

تعد بطاقات الائتمان الالكترونية احدى وسائل الدفع الالكترونية التي انتشرت على مستوى العالم انتشارا واسعا حيث أصبحت من الأنشطة المهمة والرئيسية للبنوك والمؤسسات المالية.

الامر الذي أدى الى اقبال الافراد على التعامل بها كبديل عن حمل النقود والشيكات، خاصة مع ادخال الحاسب الالي في العمليات المصرفية، والتي تقوم غالبا عن نظام التحويل الالي للنقود.

وعلى الرغم من المزايا والمنافع التي توفرها هذه الوسيلة لتسهيل المعاملات المالية، فقد قوبلت بعدد من التصرفات الغير شرعية سواء من قبل حاملها، مصدرها او من القابل لها ومن بين هذه التصرفات غير شرعية عملية التزوير.

وهذا ما سنتناوله في فصلنا هذا:

المبحث الأول: الإطار المفاهيمي لجريمة التزوير.

المبحث الثاني: الإطار المفاهيمي لجريمة التزوير الالكتروني.

المبحث الأول:

الإطار المفاهيم لجريمة التزوير الإلكتروني

أدى التقدم الحضاري التكنولوجي الى اختراع العديد من الوسائل والأدوات المتطورة وابتكار العديد من الأجهزة الدقيقة التي تتعامل بها المصارف مع زبائنها او الافراد في معاملاتهم وانشطتهم المالية والمصرفية والتجارية حيث أصبح الصراف الالي سمة عصرنا الحالي وعصب تعاملنا اليومي، فظهرت بطاقة الاتمان الالكتروني او بطاقة الوفاء. نظرا الاعتبار ان بطاقات الائتمان اهم أدوات الدفع المالي المتطورة أصبحت محلا للعديد من جرائم التحايل كالتزوير وتعد هذه جريمة ذات خصوصية تستوجب أساليب رؤية بحث وتحري مختلفة.

المطلب الأول:

تعريف جريمة التزوير الإلكتروني

لم يتطرق المشرع لجزائري وبعض التشريعات الأخرى كالمشرع المصري الى تعريف التزوير قدموا بعض الطرق التي يرتكب بها التزوير وانواعه وعقوباته فقط.

الفرع الأول: التعريف اللغوي لجريمة التزوير

يقصد بالتزوير من الناحية اللغوية التزيين او التحسين، وقد يقصد به تهيئة الكلام وتقديره. وهو فعل الكذب والباطل، ومنه ما يأخذ معنى تغيير الحقيقة بمعنى زور الكلام كذب فيه وزخرفه وموهه. التزوير أصله من زور، يزور، تزويرا فهو مزور وقد ذكر التزوير بمعنى التمويه والانحراف في الكتاب الحكيم في قوله تعالى (تزاور عن كهفهم) وهو بهذا أوسع بكثير من المعنى القانوني.[1]

[1] نقطي عبد العزيز، جريمة التزوير في بطاقة الائتمان ،مخبر السياسة العامة وتحسين الخدمة العمومية في الجزائر، جامعة الوادي ص755.

الفرع الثاني: التعريف التشريعي لجريمة التزوير

التزوير في القانون هو تغيير الحقيقة بقصد الغش بإحدى الطرق المبينة في القانون تغييرا من شانه ان يسبب ضررا للغير، وقد أوردت بعض التشريعات العقابية تعريفا للتزوير يحدده ويبين اركانه، ومن هذه التشريعات قانون العقوبات الفرنسي وهذا في القسم الأول ضمن الكتاب الرابع تحت عنوان الاعتداءات ضد الثقة العامة في المادة 441 المعدلة في المادة 14 ماي 1993 حيث نصت على : ان التزوير يقوم على كل تغيير في الحقيقة بغش من شانه ان يسبب ضررا و الذي يرتكب باي طريقة في محرر، و الذي يكون موضوعه او نتيجته إقامة الدليل علو وجود حق او واقعة ذات نتائج قانونية[1]

كذلك من بين التشريعات العقابية التي نصت على تعريف جريمة التزوير قانون العقوبات اللبناني في المادة 453 كما يلي :(التزوير هو تحريف مفتعل للحقيقة في الواقع والبيانات يراد اثباتها بصك او مخطوط يحتج بهما نجم عنه ضرر مادي او معنوي) وهو ذات التعريف الذي ورد في قانون العقوبات الأردني في المادة 260[2]. وقد عرفت الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية اتفاقية بودابست التزوير المعلوماتي بانه التزوير المرتبط بالحاسب الالي في المادة 07 منها تحت عنوان التزوير المرتبط بالحاسب الالي وهو كل خلق او تعديل غير مصرح به للبيانات المسجلة والتي تكون مؤسسة على صحة البيانات المستخرجة من خلال هذه البيانات، وبالتالي يمكن ان تكون موضوا لخداع المصالح القانونية المحمية[3].

---

[1] مريم تومي، صدراتي وفاء، تزوير بطاقة الائتمان صورة خاصة من جريمة التزوير الالكتروني، جامعة عباس لغرور خنشلة، المجلد الخامس، العدد الثاني، سنة 2013، ص996،997.

[2] نقطي عبد العزيز ، نفس المرجع ، ص 756.

[3] هلالي عبد الله احمد، تزوير بطاقات الائتمان صورة خاصة من جريمة التزوير، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة، ط1، جامعة باتنة، جزائر ص66.

وبالرجوع الى المشرع الجزائري فقد نص على جرائم التزوير في قانون العقوبات الفصل السابع بعنوان التزوير، القسم الخامس التزوير في بعض الوثائق الإدارية والشهادات في المواد 222 الى 229.

انطلاقا من هذه التعريفات للتزوير، نستنتج انه تغيير عمدي للحقيقة من شانه ان يسبب ضررا بالطرق المحددة قانونا في محرر يثبت واقعة لها اثار قانونية بقصد الغش او بنية استعمال المحرر فيما زُور من اجله،

وعليه يمكن القول ان جريمة التزوير الإلكتروني تصنف من الجرائم الالكترونية التي يمكن ان ترتكب اثناء معالجة وتحليل البيانات بشكل مزور او تصب على مخرجات الحاسب الالي او على أي دعامة الكترونية كالأنشطة الممغنطة والأقراص المغناطيسية وغيرها من الدعامات الالكترونية[1].

المطلب الثاني:

اركان جريمة التزوير الالكتروني

تتمثل اركان هذه الجريمة في الركن المادي والركن المعنوي بعنصرية القصد الجنائي العام والقصد الجنائي الخاص.

الفرع الأول: الركن المادي

يتجلى في جريمة تزوير المحررات من خلال تغيير الحقيقة بإحدى الطرق التي نص عليها القانون والتي تسبب ضررا[2].

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزئية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص184.

[2] خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الالكتروني، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق و العلوم السياسية، جامعة العربي بن مهيدي ام البواقي 2018/2017،ص33

محل التزوير: بالرجوع الى المواد من 214 الى 229 من قانون العقوبات فانه يجب ان يقع التزوير على المحررات التي تشكل سندات بما في ذلك المحررات العمومية والرسمية والعرفية، وكذلك المحررات التجارية والمصرفية. او في بعض الوثائق الإدارية وعليه فان بطاقات الدفع تنطوي ضمن المحررات المصرفية، وبذلك تكون محلا للتزوير[1].

تغيير الحقيقة: حتى تقوم جريمة التزوير يجب أن يحدث تغيير لحقيقة المحرر واستبدال بياناته بأخرى غير حقيقية، وقد يكون هذا التغيير كلي أو جزئي.

طرق التزوير: يلزم أن يكون الأسلوب المتبع في عملية التزوير أسلوبا نص عليه القانون، وقد حددها المشرع الجزائري في قانون العقوبات على سبيل الحصر في المادة 216 من هذا القانون، حيث تكون إما بتقليل أو بتزييف الكتابة أو التوقيع، وإما باصطناع اتفاقات أو نصوص التزامات أو مخالصات بإدراجها في هذه المحررات لاحقا. كذلك بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات التي اعدت هذه المحررات لتلقيها أو إثباتها، وإما بانتحال شخصية الغير، أو الحلول محله.

الضرر: حتى تقوم جريمة التزوير يجب أن يترب عليها ضرر، وهذا الضرر لا يشترط فيه أن يمس الشخص الذي يقصده المزور، بل يكفي أن يقع على أي شخص كان، وقد يكون هذا الضرر ماديا أو معنويا، كذلك يكفي أن يكون الضرر محتمل الوقوع، وبإسقاط ذلك[2]

على بطاقات الدفع الإلكتروني، فإن عنصر الضرر محتمل الوقوع على الجهة المصدرة للبطاقة وحاملها الشرعي.

---

[1] أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، الطبعة الثالثة، الديوان الوطني للأشغال التربويةالجزائر،2001، ص 450.

[2] حسين محمد الشبلي، محمد مهند فايز الدويكات، لتزوير والاحتيال بالبطاقات الائتمانية، الطبعة الأولى، دار مجدلاوي للنشر والتوزيع، عمان،2009، ص59.

الفرع الثاني: الركن المعنوي

جريمة التزوير من الجرائم العمدية التي تستوجب القصد الجنائي العام والخاص معا:

القصد الجنائي العام: ويقصد به العلم والإرادة، وذلك أن تتجه إرادة الجاني إلى تغيير الحقيقة مع علمه ان هذا التغيير فعل مجرم قانونا، يترتب عليه ضرر محتمل، او وقع بالفعل.

القصد الجنائي الخاص: هو اتجاه نية الجاني لاستعمال المحرر فيما زور من أجله، أو دفع مضرة عن الغير او عن نفسه[1].

المبحث الثاني:

الإطار المفاهيمي لجريمة التزوير الالكتروني:

تعد بطاقات الائتمان الإلكترونية إحدى وسائل الدفع الإلكترونية التي انتشرت على مستوى العالم انتشارا واسعا. حيث أصبحت من الأنشطة المهمة والرئيسية للبنوك والمؤسسات المالية .الأمر الذي أدى إلى إقبال الأفراد على التعامل بها، كبديل عن حمل النقود والشيكات، خاصة مع إدخال الحاسب الآلي في العمليات المصرفية، والتي تقوم غالبا على نظام التحويل الآلي للنقود وعلى الرغم من المزايا والمنافع التي توفرها هذه الوسيلة لتسهيل المعاملات المالية، فقد قوبلت بعدد من التصرفات غير المشروعة، سواء من قبل حاملها، مصدرها، أومن القابل لها ومن بين هذه التصرفات الا وهي التزوير.

[1] خشبة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، مذكرة مكملة لنيل شهادة الماجيستير في الحقوق،بن صغير محفوظ، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة ،2016، ص 125-126.

المطلب الأول:

مفهوم بطاقة الائتمان

لقد تباينت التعاريف المتعلقة ببطاقات الائتمان وتنوعت ضيقا واتساعا حسب الزاوية التي ينظر منها الى هذه البطاقة

الفرع الأول: تعريف بطاقة الائتمان

1 التعريف المادي لبطاقة الائتمان:

تعرف بطاقة الائتمان بالنظر الى شكلها وتكوينها المادي بانها بطاقة مستطيلة من البلاستيك تحمل اسم المؤسسة الصادرة لها وشعارها وتوقيع حاملها ورقمها واسم حاملها وتاريخ صلاحيتها.

كما تعرف انها بطاقة معدنية او بلاستيكية ممغنطة عليها اسم حاملها وتاريخ إصدارها وتاريخ نهاية صلاحيتها ورقم سري لا يعرفه الا حاملها[1].كما عرفت انها صك مصنوع من البلاستيك او مادة يصعب تزوير بياناتها يتضمن بيانات خاصة بحامل الصك كاسمه وعنوانه ورقم حسابه[2].

يجمع التعريفات السابقة مجموعة من العناصر المتعمقة بشكل البطاقة الائتمانية وتتمثل في:

ا-المادة المكونة للبطاقة وحجمها: تدخل مادة البلاستيك كمكون أساسي لجسم البطاقة ويتم التحكم بتشكيل هذه المادة عن طريق عملية التسخين الى درجة الانصهار لتشكل على هيئة

[1] مريم تومي، صدراتي وفاء، المرجع السابق، ص 1001.

[2] زين الدين محمد الزماني، التزوير والتزييف عن طريق بطاقات الائتمان، مجلة المحامي، العدد 3، الرياض 1421، ص52.

قطع بلاستيكية مستطيلة الشكل يتراوح عرضها ما بين (5-5,5سم) وطولها (8-8,5سم) وسمكها(0.8سم) ويتم تغليف جسم البطاقة بمواد كيميائية تمهيدا لصياغة وتثبيت البيانات والمعلومات والاشكال عليه[1].

ب-بيانات ومعلومات البطاقة: تتضمن البيانات المدونة على البطاقة شعار الجهة المصدرة للبطاقة وكذا البنك المصدر للبطاقة وكذا الرقم المكون للبطاقة ويتكون من أربع خانات وتاريخ الإصدار والانتهاء او المعلومات المتعلقة بصاحب البطاقة فهي الاسم واللقب ورقم الحساب وصورة الشخص أحيانا[2].

ج-الشريط الممغنط: وهو المكان المخصص لتخزين البيانات الالكترونية حيث لا يمكن قراءتها الا بأجهزة مخصصة لذلك، وتخزن هذه البيانات عل شكل مسارات او أسطر يتضمن كل سطر مجموعة خاصة من البيانات ولا يمكن قراءتها الا من خلال قارئ يرتبط بجهاز الحاسوب مزود ببرنامج خاص مهمته ترجمة هذه البيانات الى بيانات أخرى يفهمها البنك.

د-شريط التوقيع: يقع أسفل الشريط الممغنط وبمسافة امنية محددة توقيع حامل البطاقة المعتمدة لدى البنك وفي معظم البطاقات المصرفية الممغنطة يركب شريط التوقيع بطريقة كيماوية خاصة فحيث إذا وقع عليها خدش او تلاعب بالتوقيع تظهر مباشرة على الشريط وهذا حتى لا يقع من يقبل الوفاء ببطاقة ضحية التزوير[3].

هـ-الرقم السري: يسلم هذا الرقم للعميل بمظروف مغلق عند استلامه للبطاقة ويستخدمه عند الصرف النقدي من ماكينات الصرف.

2 التعريف الموضوعي لطاقات الائتمان: تعرف بطاقة الائتمان بالنظر إلى موضوعها بأنها " بطاقات تصدر بواسطة مؤسسة مالية باسم إحدى الأشخاص وتقوم تلك البطاقة بوظيفتي

---

[1] براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبعة المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، ص255

[2] المرجع نفسه، ص 262.

[3] ماد أحمد الخميل، الحماية الجزائرية لبطاقات الوفاء، دراسة تكميلية مقارنة، دار وائل للنشر، الأردن، ص 22.

الوفاء والائتمان وهذا يعني ان حاملها يملك إمكانية تتابع سداد المبالغ التي استخدمها من الاعتماد الممنوح من صاحب البطاقة.

وعرفها على انها أداة تسمح لحاملها بإيجاد الإجراءات اللازمة والمباشرة لخصم المبلغ الذي يريده لمصلحة شخص اخر من حسابه لدى البنك الذي أصدر هذه البطاقة. فبطاقة الائتمان تقوم على فكرة أساسية وهي الائتمان وهي جوهر البطاقة لافتراضها وجود فاصل زمني بين تقديم مانح الائتمان لوسائل الوفاء لعملية الشراء وبين استرداد كل الوسائل[1].

وهناك من أطلق على هذه البطاقة بطاقة الاعتماد لارتباطها باعتماد يتم فتحه لمصلحة حامل البطاقة، ولكن لما كانت العبرة بفكرة الائتمان وليس بفكرة الاعتماد فان المصطلح اللائق هو مصطلح بطاقة الائتمان[2].

الفرع الثاني: الطبيعة القانونية لبطاقة الائتمان

أولا: الطبيعة القانونية للنظام التعاقدي بين الطرفين

عند استعمال بطاقة الائتمان، الالكترونية تنشا ثلاث علاقات رئيسية تتمثل في العلاقة بين مصدر البطاقة وحاملها، والعلاقة بين التاجر وحامل البطاقة، والعلاقة بين اتاجر وحامل البطاقة. إذ حاول الفقهاء معرفة طبيعتها القانونية من خلال النظام التعاقدي بين الطرفين.

1/ **الطبيعة القانونية بين مصدر البطاقة وحالها:** يحكم العلاقة بين مصدر البطاقة وحاملها يتضمن هذا الاتفاق طلبا من العميل مقرونا بتوقيعه للحصول على البطاقة، وفقا لشروطموضوعة سلفا وغير قابلة للتفاوض بشأنها.

[1] علي عدنان الفيل المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكترونية–دراسة مقارنة، مجلة الحقوق، العدد 3، الكويت، ،2013 ص 465

[2] فداء يحي احمد الحمود، النظام القانوني لبطاقة الائتمان، دار الثقافة للنشر والتوزيع، ط1، الأردن، ،1999، ص13

يعد فحص حالة العميد من قبل البنك لطلب العميل شكل عقد يكون محدد غالبا بمدة معينة –عام من تاريخ إصداره–وعادة ما يتم تحديد العقد بشكل دوري[1].

وفي سبيل تكييف هذا النوع من العقود اعتبر القانون الفرنسي رقم22 الصادر في 10 يناير لسنة 1978 العقد المبرم بين مصدر البطاقة وحاملها من قبل فتح الاعتماد، الذي بمقتضاه يتعهد البنك (مصدر البطاقة) بان يضع تحت تصرف العميل (حامل البطاقة) بطريق مباشر او غير مباشر، أداة من أدوات الائتمان في حدود مبلغ نقدي معين ولمدة محددة نظير عمولة يدفعها الطرف الاخر[2].

ونتيجة لهذا العقد فان البنك المصدر له الحق في سحب البطاقة او الغاء العمل بها في أي وقت متى صدر عن حاملها خطا في استعمالها.

ويبدو هذا واضحا في بنود العقد المبرم بينها، حيث يتم النص على ان البطاقة تظل ملكا لمصدرها، يملك سحبها او الغاء العمل بها في أي وقت يراه، على ان تنفذ جميع المعاملات التي تمت من خلال البطاقة قبل الغاء العمل بها[3].

أما حامل البطاقة فيلتزم بكافة الالتزامات والقواعد العامة للعقود، فمثلا يلتزم باستعمال البطاقة بالطريقة المنصوص عليها في العقد، تنفيذ شروط العقد بما يتفق ومبدأ حسن النية، لا يسيء استخدام البطاقة، كما لا يحق له أن يتجاوز الائتمان المسموح به والمنصوص عليه في العقد والا كان ملزما بمقدار التجاوز[4].

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية تطبيقية) الطبعة الأولى، دار المنشورات الحلبي لبنان ،2005، ص516

[2] كميت طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان المسؤولية الجزائية والمدنية، الطبعة الأولى، دار الثقافة الأردن ،2008، ص 94.

[3] نائلة عادل محمد فريدة قورة، المرجع السابق، ص 516.

[4] كميت طالب البغدادي، المرجع السابق، ص 94

2/**الطبيعة القانونية للعلاقة بين مصدر البطاقة والتاجر:** حاول البعض تكييف تلك العلاقة بعدة أمور فخرجت ثلاثة اتجاهات لتكييف الطبيعة القانونية ونعرضها على النحو التالي:

الاتجاه الأول: لجا الى بعض العقود التقليدية المسماة لتفسير تلك العلاقة، واختلف أنصاره في تحديد الأساس القانوني الذي يلزم المصدر للبطاقة بضمان ثمن السلعة للتاجر في تجاوز صاحب البطاقة الرصيد، او في حالة الضياع او سرقتها منه.

الاتجاه الثاني: بعد فشل المحاولات التقليدية ذهب البعض في تفسير الطبيعة التزام المصدر بالوفاء للتاجر الى ان يكون من خلال اتفاق ضمني، وهذا الراي يذهب الى المصدر لا يضمن الوفاء للتاجر وما هو الا وسيط بين التاجر والحامل فقط وهو ما يفسر التزام المصدر بتحصيل حوق التاجر في مقابل الوكالة بالعمولة.

الاتجاه الثالث: ذهب أنصار هذا الاتجاه ان المصدر ملتزم اتجاه التاجر حتى مع عدم كفاية رصيد الحامل او انعدامه، طالما قام التاجر بما عليه من التزامات وإجراءات عند استخدام البطاقة وذلك عن طريق شرط تامين الاعتماد المشترط بين التاجر والمصدر او عن طريق الكفالة من المصدر للحامل[1].

2/ **الطبيعة القانونية للعلاقة بين التاجر وحامل البطاقة:** إن العلاقة التي تربط بين الشخص حامل بطاقة الائتمان والتاجر المتعاقد معه، أساسها عقد، يمكن أن يكون عقد بيع، أو إيجار أو نقل ... إلخ، ينعقد بين الحامل من جهة والتاجر من جهة أخرى، ومن أهم ما يتميز به هذا العقد أن حامل البطاقة يحيل التاجر بثمن المشتريات منه على الجهة مصدرة البطاقة، لتنشأ من ذلك علاقة مديونية جديدة بين الجهة مصدرة البطاقة والتاجر، حيث تكون الأولى مدينة للتاجر بثمن مشتريات حامل البطاقة.

[1] عبد الحكيم احمد عثمان، احكام البطاقات الائتمانية في القانون والآراء الفقهية الإسلامية، ط1، دار الفكر الجامعي الإسكندرية، 2007، ص262

كما يرى البعض أن العلاقة بين التاجر وحامل البطاقة لا تنتهي بمجرد التوقيع على فاتورة البيع أو تسجيل الشفرة الخاصة بالبطاقة بعد تسليمها إلى البائع. فحامل البطاقة لا تبرأ ذمته في مواجهة التاجر إلا بالسداد الفعلي لقيمة المعاملة من البنك المصدر، ثم حصول البنك عليها من حامل البطاقة.

أما عن الالتزامات المترتبة عن هذه العلاقة فتتمثل في التزام حامل البطاقة تجاه التاجر بالتوقيع على فاتورة الشراء، أو تقديم الخدمة، ويلتزم العميل تجاه التاجر بأن تكون البطاقة صالحة وحقيقية. كما يلتزم التاجر تجاه حامل البطاقة بيع سلع دون زيادة، أو لا يكون بالسلعة عيب، وأن يقوم بالتسليم الفوري للبضائع المشترات بموجب عقد البيع أو تسليمها بالتاريخ المتفق عليه، وغير ذلك من الالتزامات الناشئة عن عقد البيع[1].

ثانيا: الطبيعة القانونية الخاصة لبطاقة الائتمان الإلكترونية:

اختلف الفقهاء حول المعيار الجامع لدمج بطاقات الائتمان الإلكترونية ضمن نظام قانوني معين، بين وكالة (أولا)، حوالة حق (ثانيا)، نقود (ثالثا)، ونقود إلكترونية (رابعا).

1/ **وكالة:** يرى هذا الرأي أن التعامل ببطاقة الائتمان مع الغير سواء أكانوا تجارا أو شركات يعتبر وكالة، يتم بمقتضاها توكيل حامل البطاقة البنك الذي أصدر البطاقة دفع ثمن السلعة أو الخدمة التي حصل عليها ثم يخصمها البنك من حسابه الموجود لديه بوجود وكالة الموكل وهو حامل البطاقة والوكيل هو البنك وهذا هو راي القضاء الإنجليزي في طبيعة الوفاء ببطاقة الائتمان[2].

2/حوالة حق: يميل جانب من الفقه الفرنسي إلى أن السداد بواسطة بطاقات الائتمان يقترب من حوالة الحق، حيث أن حامل البطاقة هو دائن للبنك المصدر بتنازل عن هذا الدين إلى

---

[1] مونية معروف، جرائم بطاقة الائتمان الالكترونية، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون جنائي للاعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي بن مهيدي، ام البواقي 2014-2015، ص25-26.

[2] علي عدنان الفيل، المرجع السابق، ص 470-471

التاجر، غير أن الواقع يختلف. إذ البطاقة ليست سندا مثبتا لدين حاملها، وانما هي دليل على وجود مبلغ نقدي محدد يمكن التعامل في حدوده.

3/ نقود: يرى جانب آخر من الفقه بأن بطاقة الائتمان عبارة عن نقود مضافة إلى النقود المتداولة، غير أنها تتصف بأنها نقود بلاستيكية. حيث انتقد هذا الرأي فيما وصل إليه، وذلك لأن النقود تتمثل في صكوك محددة القيمة متساوية المقدار وهذا ما لا يتفق وطبيعة بطاقة الائتمان الإلكترونية. ومن ذلك يتضح أن بطاقة الائتمان لها استقلالية بنظام القانوني، ولا يمكن أن تكون إحدى صور الأوراق التجارية، ولا يمكن أن تخضع إلى النظام القانوني الذي يحكم الأوراق التجارية[1].

4/ نقود الكترونية: يرى هذا الرأي أن بطاقة الائتمان الإلكترونية هي نقود الكترونية تشبه العملات الأخرى كالنقود الورقية والمعدنية المعترف بها في تداول قانونا وتعاملا. إلا أن هذا الرأي منتقد كونه يتجاهل الصفة الذاتية للنقود باعتبارها أداة للوفاء، وهي قابلة لإعادة الاستعمال من عدة أشخاص هذا ما لا يتلاءم مع بطاقة الائتمان التي يتم تداولها بطريقة آلية عن طريق استعمالها بأدوات الكترونية حديثة ومن ثم هي غير قابلة للتداول[2].

المطلب الثاني:

اركان جريمة تزوير البطاقات الائتمان واشكالها

الفرع الأول: اركان جريمة تزوير بطاقة الائتمان

تقوم جريمة تزوير بطاقة الائتمان كغيرها من الجرائم بتوافر الركنين المادي والمعنوي.

---

[1] مونية معروف، المرجع السابق، ص 27.

[2] جلال محمد الرغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، ط 1، الأردن، 2010، ص200.

أولا: الركن المادي

يثور هنا التساؤل هل تعتبر بطاقة الائتمان محررا أو صكا يصلح محلا للتزوير أم لا؟ في حقيقةالأمر تم تحدد معظم التشريعات طبيعة المحرر وبالتالي من الممكن أن يكون من الورق أو المعدن أو الخشب وكذلك لم تحدد مادة الكتابة فقد تكون بالكتابة الحرارية أو القلم أو الفحم أو الحاسوب شريطة أن تكون هذه البيانات مقروءة ومدركة وذات دلالة ومعاني محددة، ولذا كلا تصلح الإشارات والرسومات العشوائية ان تكون محلا للتزوير[1].

1 التزوير في المعلومات المقروءة لبطاقة الائتمان: المعلومات الموجودة على البطاقة تعبر عن فكرة تمكن إدراكها بالنظر إليها مباشرة فإن التغيير فيها يكون الركن المادي لجريمة التزوير الانها تتعلق بحامل البطاقة والجهة التي أصدرت فيها وتاريخ الصالحية وهي في مجملها مستندا يتمكن استخدامه فيما اعد له.

وبالتالي إذا ما قام أحد الأشخاص بشطب أو إضافة هذه العبارات الواردة على دعامة من البلاستيك فإن مثل هذا التصرف يعتبر تزويرا من حيث المبدأ، الا أنه وعلى الرغم من ذالك وكما أن التعامل مع البطاقة الائتمانية يكون من خلال جهاز خاص يقرأ البيانات، والبطاقات المختزلة وبعد ذلك يتم قبولها من عدمه .فإذا قام أحد الأشخاص بتعديل الاسم الوارد على هذه البطاقة وقدمها لتاجر فإن ذلك لا يغير من الأمر شيئا حيث أن قبول البطاقة من عدمه يكون بناء على البيانات المخزنة على الشريط الممغنط الأمر الذي ينفي وقوع الضرر، وبما أن الضرر عنصر خاص في جريمة التزوير فإن انتقاء الضرر يرتب انتقاء الجرم ما لم يثبت وقوع مثل هذا الضرر بطريقة أو بأخرى[2].

2التزوير في المعلومات المشفرة في بطاقات الائتمان: المعلومات الموجودة على بطاقات الائتمان لها أهميتها مثل باقي المعلومات الموجودة عليها. ويرى البعض أن التغيير الذي

[1] المرجع نفسه ،ص221.

[2] مريم تومي، صدراتي وفاء، المرجع السابق، ص105.

يمس هذه المعلومات يكون جريمة التزوير، فبطاقة الائتمان تعتبر وثيقة يقع عليها التزوير كونها تحتوي على بيانات واضحة مثل الاسم والتوقيع وتاريخ الصالحية وعلى بيانات أخرى قد تكون أهم لكنها تثبت على الشريط المغناطيسي للبطاقة بصورة غير مرئية. والتغيير الذي يصيب الكيان المعنوي للبطاقة بما تتضمنها الأشرطة الممغنطة من بيانات ومعلومات هو الأكثر إثارة للمشاكل مما لو انصب التغيير على كيان البطاقة المادي[1].

ثانيا: الركن المعنوي

إن جريمة التزوير الإلكتروني من الجرائم القصدية التي يلزم لقيامها توافر القصد الجنائي لدى المزور كما أنها من جية أخرى من جرائم القصد الخاص باعتباره نية يتوخاها الجاني من جراء ارتكابه للركن المادي للتزوير.

يتوافر القصد العام بإدراك الجاني بأنه يغير الحقيقة في المحرر بإحدى الطرق المنصوص عليها قانونا وأن من شأن هذا التغيير حصول ضرر فيشترط أن يثبت علم المتهم على وجه اليقين بأنه يغير الحقيقة، فإذا لم يكن على علم بتغيير الحقيقة فإن مجرد إهماله في تحريرها مهما كانت درجتها لا يتحقق به هذا الشرط ويفترض علم الجاني بأن ما حصل تغيير الحقيقة فيه يعتبر محررا في نظر القانون وأن ما حصل بطريقة من الطرق المنصوص عليها من القانون، فليس للجاني أن يعتذر بجهل القانون.

أما الضرر إن كان عنصرا من عناصر الركن المادي وليس عنصرا في الركن المعنوي فإنه يجب إثبات إدراك الجاني وقت تغيير الحقيقة أن من شأن هذا التغيير أن يترتب عليه ضرر مادي أو أدبي حال أو محصل الوقوع يلحق الأفراد أو الصالح العام. والضرر هنا كنتيجة لفعل التزوير لا يستلزم وقوعه، فتزوير المستندات المعالجة آليا أو

[1] عمر حسن المومني، الموقع الإلكتروني وقانون التجارة الإلكترونية، ط1، دار وائل للنشر والتوزيع، لبنان، 2003، ص50.

محررات الكترونية يعد فاعله عالما بالنتيجة التي ستقع الانه سيؤدي الى الضرر بالغير في ذمته المالية.

أما القصد الخاص المطلوب توفره في التزوير هو اتجاه نية المزور لحظة ارتكاب التزوير تغيير الحقيقة واستعمال المحرر المزور فيما زور لأجله، ذلك الان التزوير لا يشكل خطرا اجتماعيا يستوجب تدخل القانون الجنائي لتجريمه إلا إذا ارتكب بنية استعمال المحرر بعد تزويره[1]. واستعمال المحرر المزور ليس ركنا في جريمة التزوير وانما هو جريمة مستقلة عنه، ألانه قد لا يستخدم المحرر المزور نهائيا لكن نية استعماليا إذا وجدت كمسألة نفسية باطنية محضة يكفي القول بتوفر القصد الخاص، علما ان مسالة القصد بنوعيه هي مسألة موضوعية يرجع تقديرها لقاضي الموضوع[2].

الفرع الثاني: اشكال جريمة تزوير بطاقة الائتمان

قد يتم تزوير بطاقات الائتمان بالتلاعب في محتوياتها بطرق مختلفة سواء تعمق الأمر بالمعلومات المرئية الموجودة عليها أو المعلومات المشفرة الموجودة على الشريط الممغنط حيث لكل نوع من هذه المعلومات أهميته فهو مرتبط بحق أو مركز قانوني ذو طابع مالي. ويكون التزوير كلي او جزئي[3].

أولا: التزوير الكلي لبطاقة الائتمان

يقع التزوير الكلي لبطاقة الائتمان على جميع عناصرها بمعنى آخر يتم تزوير المادة المكونة للبطاقة نفسها وهذا بتقليد بطاقة ائتمان الكترونية أخرى مشابهة لها.

---

[1] سامية بن عديد، الحماية الجنائية لبطاقات الدفع من جرائم التزوير في القانون الجاني الجزائري، مجلة دراساتالعدد57، الاغواط، الجزائر، ص217

[2] حسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، دار هومة للطباعة والنشر والتوزيع، ط9، الجزائر، 2003، ص273.

[3] مريم تومي، صدراتي وفاء، المرجع السابق، ص106

1-طرق التزوير الكلي لبطاقة الائتمان: إن الجاني وهو بصدد تزوير بطاقة الائتمان الإلكترونية كليا يقوم بتقليد البطاقة وذلك بالتلاعب في مكوناتها الأساسية[1]وهي:

المادة المكونة للبطاقة: تتكون البطاقة من ثلاث طبقات بلاستيكية مضغوطة مصنوعة من مادة بولي كلوريد الفنيل اما الطبقة الوسطى فتحتوي على مادة ومادة أكسيد التيتانيوم وهي المادة التي تجعل البلاستيك باللون الأبيض، وهي عبارة عن بطاقة من حيث الحجم الأبعاد إلا أنها لا تحمل أي بيانات وتمكن نقل هذه البيانات إلى البلاستيك الأبيض ونقله للبطاقة واستخدامه بالطريقة التي يرغبون في تطبيقها.

تزوير المعلومات: سواء المعلومات الموجودة على البطاقة الظاهرة أو تلك الموجودة على الشريط الممغنط، وذلك بتقليد الطباعة والنقوش والرسوم على البلاستيك ثم تغليف البطاقة، أما التزوير على الشريط الممغنط فيكون إما بالنسخ أو بالتشفير ليتم بعد ذلك عمل الطباعة عن طريق انتشاءها بمعلومات للحصول عليه بطريقة غير شرعية[2].

كما يمكن الاحتيال على حامل البطاقة عبر شبكة الأنترنت وذلك عن طريق اصطياد البيانات المصرفية عن طريق البريد الإلكتروني حيث يتلقى المستفيد رسالة الكترونية تبدو وكأنها من بنك ومؤسسة حكومية تريد التأكد من بياناته يتم إرسالها إلى موقع أخر يشبه الموقع الأصلي[3].

2-الظواهر الدالة عمى التزييف الكلي لبطاقة الائتمان:

_عدم دقة لصق وعدم ثبات تموضع الشريط الممغنط وشريط التوقيع بظهر البطاقة الأمر الذي يترتب عليه إمكانية نزعها بسهولة بواسطة أظافر الأصبع.

---

[1] براهيمي حنان، المرجع السابق، ص 272.

[2] رياض فتح الله بصلة، جرائم بطاقة الائتمان، ط1، دار الشروق، بيروت، لبنان، ،1995 ص108.

[3] نجاح محمد فوزي، وعي المواطن العربي تجداه جرائم الاحتيال بطاقات الدفع الإلكتروني، الرياض، ط 1، السعودية، ص103. 2007

_اختلاف مواصفات شكل وحجم البيانات المطبوعة.

_إمكانية عدم التطابق بين البيانات المشفرة عمى الشريط الممغنط وبين البيانات المقروءة بصريا والمطبوعة.

ثانيا: التزوير الجزئي لبطاقة الائتمان: يعتمد التزوير الجزئي لبطاقة الائتمان على وجود بطاقة صحيحة ابتداء في يد المزور ليتمكن من التلاعب في مكوناتها المرئية وغير المرئية بالأساليب المناسبة حيث يستثمر المزور في هذه الحالة الجسم الحقيقي للبطاقة وما عليه من نقوش وطباعة وكتابة أمنية[1].

صورالتزوير الجزئي: إن التزوير الجزئي لبطاقة الائتمان يتخذ الصور الثالث الآتية:

سرقة المعلومات الخاصة بالبطاقة: يقوم الجاني في هذه الحالة بالحصول على بطاقة ائتمان صحيحة بطريقة غير مشروعة (منتهية الصلاحية أو ملغاة) حيث يتم العبث في بياناتها أو إحدى البيانات التأمينية بطريقة لا تلاحظ بسهولة، وتتم العملية بالتخلص من البيانات المطبوعة طباعة نافرة عن طريق تسخينها بواسطة التسخين في الماء لدرجة الغليان وضغط الحروف النافرة حتى تختفي ثم وضع أرقام بيانات جديدة مطبوعة طباعة نافرة بواسطة آلة طباعة نافرة ثم يتم تلقينيا بأرقام حسابات تمت سرقة المحل[2].

1-تزوير التوقيع على بطاقات ائتمان مسروقة: في هذا الفرض يقوم الجاني بسرقة بطاقة ائتمان صحيحة ثم كشط ما كان عليها من توقيع ولصق آخر مكانه، والتوقيع عليه، أو المحو الآلي أو الكيميائي للتوقيع الأصلي أو لأجزاء من هذا التوقيع.

---

[1] رياض فتح الله بصمة، المرجع السابق، ص 111.

[2] مريم تومي، صدراتي وفاء، المرجع السابق، ص 108

2-تزوير الشريط الممغنط: يعتمد الجاني في هذه الحالة على تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة وصحيحة مسروقة بواسطة جهاز تشفير.

الظواهر الدالة على التزوير الجزئي لبطاقة الائتمان: من أهم هذه الظواهر:

- انهيار بعض مواضع التوقيع وإمكانية ظهور سطح البطاقة أسفل مواضع الانهيار نتيجة للمحو الالي.
- ظهور بقع قاتمة او بنية او مصفرة اللون نتيجة للمحو الكيميائي.
- إذا كان شريط التوقيع قد تعرض للكشط المادي والثبات وقد يترتب على ذلك خدوشات او سيلان للمادة اللاصقة حول الشريط المصطنع[1].

[1] رياض فتح الله بصمة، المرجع السابق، ص112

خلاصة الفصل

تناولنا في هذا الفصل كل ما يخص الإطار المفاهيمي لجريمة التزوير الالكتروني وبطاقة الائتمان من خلال التطرق لمفهومها عن طريق عرض مختلف التعاريف من تعريف لغوي، تشريعي، مادي وموضوعي ثم الانتقال الى اركان جريمة التزوير الالكتروني حيث تطرقنا الركن المادي والمعنوي.

اما عن الطبيعة القانونية لبطاقة الائتمان فبدانا أولا بالطبيعة القانونية للنظام التعاقدي بين الطرفين حيث نجد فيها علاقات رئيسية بين مصدر البطاقة وحاملها العلاقة بين التاجر وحامل البطاقة والعلاقة بين التاجر وحامل البطاقة.

وأخيرا تم التعرض للطبيعة القانونية الخاصة لبطاقة الائتمان الالكترونية حيث نجد فيها عدة اراء لدمج بطاقة الائتمان ضمن نظام قانوني معين بين وكالة وحوالة حق ونقو ونقود الكترونية.

الفصل الثاني:

إجراءات الحد من جريمة التزوير في البطاقات المصرفية

التقدم التكنولوجي الذي يشهده العصر الحديث يحتم ضرورة وجود قانون حديث يسايره و يتصدى التطورات الإجرامية التي تصاحبه ، محاولا حماية هذه التقنية الحديثة من الانتهاكات الخطيرة التي تهدد سلامة الأفراد ، سواء في أموالهم ، أعراضهم ، حرياتهم الشخصية ، و غيرها من الحقوق التي أصبحت مهددة مع انتشار استخدام الكمبيوتر و الانترنت من مختلف فئات المجتمع ، فرغم ما قدمه التقدم التكنولوجي من تسهيلات في مختلف الميادين إلا انه أصبح أداة لأخطر الجرائم ، و تكمن خطورتها في سهولة ارتكاب الجرائم التقليدية مع صعوبة اكتشافها ، دون اللجوء إلى الوسائل التقليدية في ذلك لان الجرائم باتت ترتكب بتقنيات حديثة كجرائم السرقة ، التهديد ، التشهير ، السب و الشتم.

فبالتالي فهذا النوع من الجرائم يستوجب تحديث القوانين والمعلومات، وكذا خلق جهات أمنية مختصة للتحقيق فيها إلا أن المشرع الجزائري لم يذكر إجراءات التحقيق في جريمة التزوير للبطاقات المصرفية بالتخصيص وبما أنها متطابقة مع آليات التحقيق الخاصة بالجرائم الالكترونية عموما فسنتخذ هذه الأخيرة مثالا لتطبيق الإجراءات على جريمة التزوير الالكتروني ومن خلال هذا الفصل سنتطرق لإجراءات التحقيق في جريمة التزوير وذلك في المبحث الأول مما يستوجب اتصال المحقق بالجريمة الالكترونية مع التطرق إلى الانتقال إلى مسرح الجريمة الالكترونية، أما المبحث الثاني فسنتعرض إلى الحماية القانونية للبطاقات المصرفية[1].

هذا ما سنتناوله في فصلنا هذا:

---

[1] بخي فاطمة الزهراء، إجراءات **التحقيق في الجريمة الالكترونية**، مذكرة مكملة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق، جامعة محمد بوضياف–المسيلة،2014/2013، ص 52.

المبحث الأول: إجراءات التحقيق في جريمة التزوير

المبحث الثاني: الحماية القانونية للبطاقات المصرفية.

المبحث الأول:

إجراءات التحقيق في جريمة التزوير

الجريمة الالكترونية من الجرائم المستحدثة ، تتطلب لارتكابها وسائل ذات تقنية عالية بالإضافة إلى ذكاء و خبرة المجرم في مجال التقنية الحديثة ، و عليه فإجراءات التحقيق فيها تتمتع بنوع من الخصوصية نظرا لطبيعة الجريمة الالكترونية ، حيث توجد في معظم البلدان المتضررة منها أجهزة خاصة بالتحقيق فيها ، يتولى البلاغات و الشكاوى بشأنها عن طريق الانترنت من خلال مواقع الكترونية[1]و من خلال هذا المبحث سنتطرق إلى اتصال المحقق بالجريمة الالكترونية و ذلك من خلال المطلب الأول و سنتعرض إلى الانتقال إلى مسرح الجريمة الالكترونية إبان المطلب الثاني .

المطلب الأول:

اتصال المحقق بالجريمة الالكترونية

القوانين التقليدية التي كانت تنظم إجراءات التحقيق كالتفتيش والمعاينة لا يمكن تطبيقها على الجريمة الالكترونية، كونها جريمة ذات طبيعة خاصة لأنها تتعلق بالبيانات والمعلومات غير الملموسة، مما يصعب تحديد هوية وأمكنة المجرمين وملاحقتهم، وهذا ما يرهق المحققين الذين يصعب عليهم جمع الأدلة من خلال البيئة الالكترونية ذات الطبيعة المعقدة والغامضة.

[1] بخي فاطمة الزهراء، نفس المرجع السابق، تلخيص المذكرة

الفرع الأول: آلية التحقيق في الجريمة الالكترونية

تظل الجريمة مستمرة مالم يتم التبليغ عنها إلى الجهات المختصة بالتحقيق وبمجرد وصول نبا وقوعها إلى تلك الجهات، فإنها تتخذ عدة إجراءات للتأكد من وقوعها وكشف مرتكبيها ومعرفة المحققين وقوع جريمة ما يتم وفق طريقتين[1].

أولا: البلاغات في الجريمة الالكترونية

والبلاغ هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع، أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن، أو عزما على ارتكابها أو وجود شك أو خوفا أنها ارتكبت[2].

أ. **كيفية التبليغ في الجريمة الالكترونية** : قد يكون البلاغ واجب في جميع الجرائم كما في قانون الإجراءات الجنائية المصري و قد يكون اختياري في بعض الجرائم وواجب في جرائم أخرى كما هو منصوص عليه في القانون الجزائري في المادتين :"32 من ق.ع و 91 من ق.إ.ج " و يتم التبليغ بمختلف الوسائل التي توصل المعلومات إلى الجهات المختصة بالتحقيق فقد يكون التبليغ كتابيا ، أو شفويا ومن أي شخص سواء كان متضررا أو غير متضرر و هذا ما يطلق عليه مصطلح البلاغ المادي و قد يقدم بواسطة البريد أو التلفون أو الصحف و هذا ما يصطلح عليه البلاغ المعنوي ، و قد يتم عن طريق الانترنت و هذا ما يسمى بالبلاغ الرقمي[3].

---

[1] نفس المرجع ، ص 54.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، دار الفكر الجامعي الإسكندرية، ط1،2007، ص177

[3] نفس المرجع ، ص 182.

ب. **الجهة المختصة بتلقي البلاغات في الجريمة الالكترونية:** الجهة المختصة بتلقي البلاغات في فرنسا في مثل هذه الجرائم هي البريد الالكتروني للدرك الوطني الفرنسي[1]، باعتبارها الجهة المختصة بالتحقيق والتحري

ثانيا: الشكوى في الجريمة الالكترونية

قد يترتب على الجريمة ضرر خاص قد يصيب احد الأفراد ماديا أو معنويا فينشا له حق في تحريك الدعوى العمومية بتقديم شكوى أمام الجهات المختصة بالتحقيق حيث نص المشرع الجزائري في المادة 72 من ق. إ. ج[2]على " يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بان يتقدم بشكواه أمام قاضي التحقيق المختص " و قد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشان جرائم معينة ، حظر المشرع تحريكها بصددها قبل تقديمه[3]، و لا يوجب القانون للشكوى شكلا معينا و إنما يقتصر فيها المعني بالأمر على ذكر : اسمه ، عنوانه، موجز الوقائع و المواد القانونية التي تعاقب الفعل المرتكب ، و إعطاء كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما[4] .

وقد خصصت العديد من المراكز لمعالجة تلك الشكاوى من بينها:

مركز تلقي الشكاوى عن جرائم الاحتيال عبر الانترنيت " IFCC" الذي تم تأسيسه في فرجينيا الغربية بالولايات المتحدة الأمريكية من طرف مكتب التحقيقات الفدرالي " FBI" والمركز الوطني لجرائم الياقات البيضاء "NW3C" من اجل مكافحة ظاهرة الاحتيال عبر

---

[1] judiciare@gendarmeriedefense.gouv.fr

[2] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، ط2، 2009، ص 28.

[3] نبيلة هبة هروال، المرجع السابق، ص189.

[4] محمد حزيط، المرجع السابق، ص30.

الانترنـت المتصـاعدة والموقـع المخصـص لتلقـي الشـكاوى مـن الضـحايا تحـت عنـوان: http//www.IFCCFBI.gov[1]

ثالثا: الوسائل المساعدة التي يستخدمها المحقق في الجريمة الالكترونية

من اجل إدراك وسائل تثبت وقوع الجريمة ونسبها لمرتكبيها يحتاج المحقق في تنفيذ مهمته إلى وسائل مادية وأخرى معنوية.

أولا/ الوسائل المادية:

أ.عنـاوين الانترنـت: IPو MCA والبريد الالكتروني وبرامج المحادثة، أن عنوان الانترنت Internet Protocol Adresse هو المسؤول عن تراسل حزم البيانات عبر الانترنت وتوجيهها إلى أهدافها، ويوجد عنوان IP بكل جهاز مرتبط بالأنترنت ويتكون من أربعة أجزاء الجز الواحد له ثلاث خانات، يشير الجزء الأول من اليسار إلى المنطقة الجغرافية ويشير الجزء الثاني لمزود الخدمة والثالث لمجموعة الحواسيب المرتبطة، والرابع يحدد الكمبيوتر الذي تم الاتصال منه [2].

في حالة وجود أي مشكلة فان أول ما يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني، وتوجد أكثر من طريقة لمعرفة عنوان IP

الخاص بجهاز الحاسوب منها في حالة العمل على نظام التشغيل Windows

بكتابة winpcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان ip[13]

---

[1] نبيلة هبة هروال، المرجع السابق، ص 193.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص 303.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 303

ب. البروكسي proxy:

البروكسي وسيلة لوصل مواقع الويب و الشبكات المحلية للأنترنت ، فهو برنامج يعالج حركة النقل إلى الأنظمة المضيفة ، نيابة على البرامج المستضافة المشتغلة على الشبكة المحلية مما يعني إمكانية المستخدم الوصول إلى الانترنت عبر الجدار الناري ، لكن لا يمكن للدخلاء رؤية الداخل[1] و يعمل البروكسي كوسيط بين الشبكة و مستخدمها ، حيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة و ضمان الأمن و توفير خدمات الذاكرة الجاهزة cache Memory،حيث يتلقى مزود البروكسي عبر الانترنت طلبا من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن الذاكرة المخفية المحلية فيتحقق البروكسي من وجودها و إذا لم تكن موجودة ، فانه يعمل كمزود زبون و يرسل الطلب إلى العالمية حيث يستخدم احد عناوين IP كما يمكن للذاكرة الخفية الاحتفاظ بالعمليات التي تمت عليها مما يجعل دورها قويا في الإثبات[2].

ج. برامج التتبع : هذه البرامج يمكنها أن تقوم بالتعرف على محاولات الاختراق و من قام بها و مصمم للعمل في الأجهزة المكتتبة و ساكن في خلفية المكتب و عند رصده لأي محاولة قرصنة يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ في عملية المطاردة لاقتفاء اثر المخترق و هذا البرنامج يتكون من شاشة رئيسة تقدم للمستخدم بيانا شاملا لعمليات اختراق ، و تحمل اسم الحدث و تاريخ الحدوث ، عنوانه IP الذي تم من خلاله ، و الشركة المزودة لخدمة الانترنت المستضيفة للمخترق[3]، و فور حدوث أي محاولة للاختراق تظهر

---

[1] بلال بن جامع، المشكلات الأخلاقية والقانونية المثارة حول شبكة الانترنت، ماجستير في علم المكتتبات تخصص إعلام آلي وتقني، جامعة منتوري – قسنطينة، 2006، ص 163

[2] بخي فاطمة الزهراء، نفس المرجع السابق، ص 57

[3] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، ط1 ،2011، ص 207-208

أمـام المسـتخدم شاشـة صـغيرة مصـحوبة بتحـذير صـوتي يظهـر علـى الشاشـة عنوانـه IP الخاص به.

د. نظام كشف الاختراق: يرمز لـه ب ids وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الانترنت مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة تدل على وجود مشكلة قد تهدد امن الحاسوب، ويتم من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في الشبكة، وفي حال اكتشف النظام وجود إحدى هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة[1].

هـ. نظام جرة العسل: هو مصمم خصيصا لكي يعترض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أي بيانات ذات أهمية ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئا بسهولة الاعتداء على النظام، بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز أخر في الشبكة في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، بالتالي تحليلها واتخاذ إجرائي وقائي[2]

و. أدوات الضبط: إن جهات التحقيق وجمع الاستدلالات تحتاج إلى ضبط ماديات الجريمة وإثبات وقوعها والمحافظة على الأدلة حتى يتم نسبتها إلى الجاني، لتقديمها للنيابة العامة لكسب اعترافه ولذا يوجد أدوات تقوم بضبط ماديات الجريمة كغالبية برامج الحماية وأدوات المراجعة وأدوات مراقبة المستخدمين والتقارير التي تنتجها نظم أمن البيانات كما

[1] نفس المرجع، ص 208-209

[2] نفس المرجع، ص 209.

يمكـن اسـتخدام اغلـب الأدوات المسـتخدمة فـي الجريمـة كـأداة ضـبط مثـل أدوات جمـع المعلومات عن الزائرين.[1]

ي. أدوات فحص ومراقبة الشركات: وتشمل ما يلي

1. أداة :ARP وظيفتها تحديد مكان الحاسوب الفيزيائي على الشبكة وهو يحتفظ بجميع أرقام كروت الشبكة mac وله عدة من المداخل المستعملة معه.

2. برنامج :Visual route هو برنامج يلتقط أي عملية فحص عملت ضد الشبكة فيقوم بإعطاء أجوبة معينة تبين العمليات التي حدث فيها المسح و المناطق التي تم فيها الهجوم و بعد معرفة عنوان IP يوضح مسار الهجوم بين مصدره و الجهة التي استهدفها الهجوم[2] .

3.أداة التتبع tracer: ترسم مسارا بين جهازين تظهر فيها كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني، وتوجه من خلالها الوقت والقفزات، وهي تسمح برؤية المسار الذي اتخذه IP من مضيف لآخر وتستخدم هذه الأداة الخيار time to liveالتي تكون ضمن IP لكي تستقبل من كل موجة رسالة، وبذلك يكون هو العدد الحقيقي للإثبات، ويتم بذلك تحديد المسار الذي تسلكه الرزمة بشكل دقيق[3].

4. أداة تفحص حالة الانترنت :Stat net هي أداة لفحص حالة الاتصال الحالي للبروتوكول IP/tcp ولها عدة مهمات من أهمها عرض جميع الاتصالات الحالية ومنافذ التصنت وعرض المنافذ والعناوين بصورة رقمية وعرض كامل جدول ال توجيه[4].

---

[1] نفس المرجع، ص 210

[2] خالد عياد الحلبي، المرجع السابق، ص 211.

[3] نفس المرجع، ص 211

[4] نفس المرجع، ص212

ثانيا/الوسائل الإجرائية:

وتتمثل في:

1 . اقتفاء الأثر: أخطر ما يخشاه المجرم الالكتروني هو تقصي أثره أثناء ارتكابه للجريمة، لهذا فأهمية اقتفاء الأثر في الجريمة الالكترونية أكثر أهمية من أهمية الشهادة في الجرائم التقليدية ويمكن تقصي الأثر بطرق عدة سواء كان ذلك عن طريق البريد الالكتروني تم استقباله، او عن طريق تتبع الأثر للجهاز الذي تم استخدامه للقيام بعملية الاختراق[1].

2 . الاطلاع على نظام المعلوماتي وأسلوب حمايته: على المحقق الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما يجب عليه معرفة نوعية برامج الحماية وأسلوب عملها، من التقارير التي تنتجها نظم امن البيانات وتقارير الجدران النارية.[2]

3 . الاستعانة بالذكاء الاصطناعي: ويتم ذلك من خلال حصر الاحتمالات والحقائق والأسباب والفرضيات، بعدها تتم معرفة النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسوب وفق برامج تعد لذلك، والتي تعطي كافة الاحتمالات، ثم أكثر الاحتمالات وصولا ثم الاحتمال الأقوى مع إعطاء الأسباب[3].

4 . التأكد من وقوع الجريمة: إن توافر المعلومات المنشورة خلال شبكة الانترنيت قد تظهر انتشار الفيروسات، أو وقوع عمليات اختراق أو قرصنة، وعند وصول الجهة المختصة بتلقي البلاغات يجب عليها التأكد من صحة البلاغ، والتحفظ على مكان الجريمة وتأمينه، وتحديد أطراف الجريمة وكل من له صلة بها[4].

---

[1] نفس المرجع، ص 212/213

[2] خالد عيادي الحلبي، المرجع السابق، ص 213/214

[3] نفس المرجع، ص 214/213

[4] نفس المرجع، ص 215

الفرع الثاني: الاستجواب وسماع الشهود في الجريمة الالكترونية

يستدعى الأشخاص للإدلاء بأقوالهم، قد يكونون مشتبه فيهم وهذا ما يطلق عليه الاستجواب، وقد يكون هؤلاء الأشخاص خارجين عن الخصومة إلا أنهم يؤثرون على مسار القضية من خلال سماع شهادتهم[1].

أولا/ الاستجواب في الجريمة الالكترونية:

ينقسم الاستجواب إلى:

1. الاستجواب عند الحضور الأول في الجريمة الالكترونية:

وهو أن يمثل المتهم أمام المحقق لأول مرة وذلك حتى يتحقق من هويته ويحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخير المتهم في أن له الحق في توكيل محامي وإن كان غير قادر ماديا يجوز للمحقق أن يعين له محامي من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغير على عنوانه أن يخطر المحقق.[2]

2. الاستجواب في الموضوع في الجريمة الالكترونية:

ويعني الاستجواب مواجهة المتهم بالتهمة والوقائع المنسوبة إليه ومناقشته فيهما مناقشة تفصيلية ومواجهته بالأدلة القائمة ضده ومطالبته بإبداء رأيه فيها ويكون إجباري كما هو الشأن بالنسبة للجنايات أو اختياري بالنسبة للجنح[3].

---

[1] بخي فاطمة الزهراء، نفس المرجع السابق، ص 63

[2] عبد الرحمان خليفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر ،2012، ص 168.

[3] محمد حزيط، قاضي التحقيق، المرجع السابق، ص 67

3. الاستجواب الإجمالي في الجريمة الالكترونية:

يهدف إلى تلخيص الوقائع وإبراز الأدلة التي سبق جمعها خلال كافة مراحل التحقيق والإشارة إلى الاستعلامات التي وردة في شأن وحياة وسلوك وشخصية والسوابق العدلية للمتهم، ويختم بطرح السؤال التالي: هذا هو استجوابك الأخير فهل لديك ما تدلي به للدفاع عن نفسك؟

ويحتوي الملف الجنائي على الوثائق التالية: –شهادة ميلاد المتهم، –صحيفة السوابق العدلية، –تقرير البحث الاجتماعي، شهادة جيرانه سواء قام به المحقق بنفسه أو عن طريق إنابة قضائية لأحد ضباط الشرطة القضائية[1].

ثانيا/ سماع الشهود في الجريمة الالكترونية:

سماع الشهود هو إجراء من إجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة بحيث يستدعى أشخاص ليست لهم علاقة بالجريمة إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبيها، وتخلف الشاهد عن الحضور للإدلاء بشهادته يعرضه للمسالة الجنائية، وعليه سنتطرق أولا لتعريف الشهادة ثم الشهادة في الجريمة الالكترونية[2].

1. تعريف الشهادة وأنواعها:

تعريف الشهادة: هناك من عرف الشهادة بأنها الأقوال التي يدلي بها الخصوم أمام سلطة التحقيق أو الحكم في شأن جريمة وقعت سواء بثبوت الجريمة وظروف ارتكابها أو إسنادها إلى المتهم أو براءته منها[3]، وعرفها الدكتور عاطف النقيب أنها " تقرير الشخص لحقيقة أمر كان قد رآه أو سمعه «، وعرفها الدكتور احمد فتحي السرور أنها " إثبات واقعة

---

[1] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط3، 2008، ص109/108

[2] بخي فاطمة الزهراء، نفس المرجع السابق، ص 66

[3] نفس المرجع ، ص 66

معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة ".

وتخضع الشهادة إلى عدة قواعد من بينها:

تكليف الشاهد بالحضور بواسطة القوة العمومية، كما يجب ان تسلم النسخة من طلب الاستدعاء إلى الشخص المطلوب حضوره، كذلك يجب ذكر هوية الشاهد قبل سماع شهادته وذكر قرابته أو نسبه للخصوم ومن أهم واجبات الشاهد حلف اليمين، وتجدر الإشارة إلى انه يجوز سماع شهادة القصر وذوي العاهات وذلك وفقا للإجراءات الخاصة بكل حالة[1].

وتؤدى الشهادات بانفراد وأخيرا تدون الشهادات بمحاضر خصصت لذلك دون حشي أو تصحيح أو تخريج، يصادق على المحضر كل من المحقق والكاتب و الشاهد[2].

ب. أنواع الشهادة:

تنقسم الشهادة إلى ثلاث أنواع:

1.الشهادة المباشرة: هي أن يشهد الشاهد بما شاهده أو وقع تحت سمعه[3]

2.الشهادة السماعية: بمعنى من علم بالأمر من الغير شهادة سماعية بحيث لا يشهد الشخص بما رآه أو سمعه مباشرة، بل يشهد بما سمعه رواية عن الغير وهي اقل

شأنا من الشهادة الاصلية[4]

3.الشهادة بالتسمع: وهذه الشهادة تختلف عن الشهادة السماعية حيث تتعلق هذه الأخيرة بأمر معين نقلا عن شخص معين قد شاهد هذا الأمر بنفسه،

---

[1] مبروك نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، ج1، 2003، ص 384/383

[2] نفس المرجع ، ص 385

[3] محمد علي سكيكر، آلية المسؤولية الجنائية، دار الفكر الجامعي، الإسكندرية، ط1، 2008، ص137

[4] العربي شحط عبد القادر، نبيل صقر، الإثبات في المواد الجزائية، دار الهدى، الجزائر، 2006، ص101

أما الشهادة بالتسمع فتتعلق بواقعة معينة ولكنها ليست نقلا عن شخص معين بالذات شاهد الأمر بنفسه كأن يقول الشاهد: سمعت كذا وأن الناس يقولون كذا وكذا عن هذه الواقعة أو الام[1].

ثانيا/ الشهادة الالكترونية:

وتفترض أن تكون في التحقيق النهائي أمام محكمة الموضوع، حيث الحصول على أقوال المتهم بشكل سمعي مرئي، وقد ظهر بعد ظهور فكرة الدوائر الاتصالية الالكترونية المتكاملة من مغلقة ومفتوحة، ولقد كانت بدايات الأخذ بهذا النظام في القضاء الأمريكي عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا برنامج حماية الشهود، فقد قررت المحكمة الفيدرالية العليا الأمريكية قبولها لنظام الشهادة طالما كانت هناك أسباب في القانون تدعو اليه[2].

ويختلف الشاهد في الجريمة الالكترونية عن الشاهد في الجرائم العادية لما

يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية وقد عرف الشاهد الالكتروني بأنه: " الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات ويمكن القول إن الشاهد الالكتروني هو كل من:

أ. **مشغلو الحاسب الآلي:** هو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات

[1] نفس المرجع ، ص 102/101

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 262

واستخراجها كما تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات واستخراجها كما تكون لديه الخبرة الواسعة في الكتابة السريعة عن طريق لوحة المفاتيح[1].

ب. خبراء البرمجة: هم الأشخاص المتخصصون في كتابة أوامر البرامج وينقسمون إلى فئتين: مخططو برامج التطبيقات ومخططو برامج النظم[2].

ج. المحللـون: هـم الأشـخاص الـذين يحللـون الخطـوات، ويقومـون بتجميـع البيانـات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات، كما يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسوب[3].

د. مهندسو الصيانة والاتصالات: هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكات الاتصال المتعلقة به.

هـ. مديرو النظم: هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية[4].

المطلب الثاني:

الانتقال إلى مسرح الجريمة الإلكترونية

عند تلقي المحقق البلاغ أو الشكوى بوقوع جريمة ما، فانه ينتقل مباشرة إلى مكان وقوعها مع إخطار وكيل الجمهورية ، و ذلك بهدف التنقيب عن الأدلة و حمايتها ،إلا انه تجدر الإشارة إلى أن مسرح الجريمة الالكترونية بالإضافة إلى المسرح المادي يوجد مسرح الكتروني متمثل في البيئة الرقمية التي يجد فيها المحقق صعوبة استخلاص الدليل منها

---

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ط1، 2009، ص 612

[2] نفس المرجع ، ص 613

[3] خالد ممدوح إبراهيم، المرجع السابق، ص 264

[4] بخي فاطمة الزهراء، المرجع السابق، ص70

،مما يدفعه إلى الاستعانة بالخبراء الفنيين في هذا المجال، و من بين الإجراءات التي يقوم بها المحقق على مسرح الجريمة التفتيش و ضبط الأدلة الذي سأتطرق لهما في الفرع الأول بالإضافة إلى المعاينة و ندب الخبراء في الفرع الثاني .

الفرع الأول :التفتيش وضبط الأدلة في الجريمة الإلكترونية

التفتيش وضبط الأدلة في الجريمة الالكترونية يحتاجان إلى تقنيات خاصة تختلف عن حالات الجرائم التقليدية وذلك راجع لطبيعة الوسيلة المستخدمة لارتكاب الجريمة، كذألك يرجع الاختلاف إلى إن مسرح الجريمة في الجريمة الالكترونية معلومات وبيانات غير ملموسة مما يصعب هاذين الإجرائيين ويستلزم وسائل خاصة مقارنة بالظروف العادية – الجرائم التقليدية[1].

أولا: التفتيش في الجريمة الإلكترونية:

التفتيش في الجريمة الالكترونية يقع على نظم الحاسوب والانترنيت، وهو إجراء يهدف إلى البحث عن الأدلة المادية والمعنوية التي تثبت ارتكاب الجريمة، ونسبتها إلى مرتكبها ويجدر التطرق إلى تعريف التفتيش عامة ثم التفتيش في الجريمة الالكترونية

1.تعريف التفتيش:

يهدف التفتيش إلى جمع الأدلة من مكان وقوع الجريمة.

أ.**تعريف التفتيش لغة:** من مصدر فتش أي بحث وسال، فتش الرجل عن شيء أي تصفحه[2].

[1] بخي فطيمة الزهراء، نفس المرجع، ص 75.

[2] علي بن عادية، بلحسن البليش، الجيلالي بن الحاج يحيى القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية، الجزائر، تونس، ط1، 1979، ص756.

ب.تعريف التفتيش قانونا: هو البحث المادي في مكان ما بهدف البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق ب شأنها[1].

ج.تعريف التفتيش فقها: تعددت التعريفات الفقهية في هذا الشأن، فعرفه الفقه الفرنسي بأنه بحث بوليسي أو قضائي عن عناصر الدليل عن جريمة ما، ويمكن وفقا لقواعد قانونية خاصة أن ينفذ في المسكن الخاص بأي شخص أو في أي مكان أخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة[2].

وعرف الفقه جانبا من التفتيش بأنه إجراء من إجراءات التحقيق تقوم بها سلطة حددها القانون، يتم البحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة ويتمثل في شخص المتهم أو في المكان الذي يعمل به ويقيم فيه[3].

القواعد العامة لتفتيش نظم الحاسوب والانترنيت: ويمكن تعريف التفتيش بأنه ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي الغرض منه البحث عن أدلة الإثبات المرتكبة، وكل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه في انه مرتكب الجريمة [4] .

الغرض من التفتيش هو البحث عن الأدلة المتعلقة بالجريمة، التي تساعد في كشفها والتفتيش في الجريمة الالكترونية ينقسم إلى تفتيش ماديات الجريمة الملموسة، والتفتيش في نظم الحاسوب الغير ملموسة والتي تخضع لقواعد عامة وهي:

---

[1] محمد حزيط قاضي التحقيق في النظام القضائي الجزائري، المرجع السابق، ص91.

[2] بكري يوسف بكري التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، ط1، 2011، ص58.

[3] بخي فاطمة الزهراء، المرجع السابق، ص 77

[4] بلعيات إبراهيم، اركان الجريمة وطرق اثباتها في قانون العقوبات الجزائري، دار الخلدونية الجزائر، ط1 ،2006، ص210

أ.القواعد الشكلية لتفتيش نظم الحاسوب والانترنيت:

الأصل أن التفتيش لا تقوم به إلا سلطة التحقيق، فيخضع التفتيش في هذه الحالة للخصائص العامة لكافة إجراءات التحقيق.

المتمثلة في وجوب التدوين بمعرفة كاتب والسرية عن الجمهور وحضور الخصوم ووكلائهم إن أمكن ذالك[1].

وهناك شروط للتفتيش تختص بها الجريمة الالكترونية دون غيرها من بينها توافر الخبرة الفنية لدى القائم بالتفتيش من خلال أن يتلقى المحقق في الجريمة الالكترونية تدريبات فنية خاصة، تعرفه كيفية التعامل مع التقنية الحديثة وكيفية ضبط الأدلة والحفاظ عليها في هذا المجال، كذلك يجب أن يتم التفتيش بصورة صحيحة من الناحيتين الموضوعية والشكلية[2].

كذلك من القواعد الشكلية التي تحكم التفتيش عدم التجاوز في التفتيش، وذلك بمنع التفتيش عندما لا توجد تحريات جدية تنبئ عن وجود دلائل قوية عن معلومات تفيد في كشف الحقيقة مع وجوب أن يكون التفتيش في حدود الإذن المكتوب، المؤرخ والموقع من الجهة التي أصدرته وإلا كان التفتيش باطلا[3].

ويجب أن يكون إذن التفتيش محدد المدة التي تحتسب من يوم الإذن إلى الجهة المأذون لها إجراء التفتيش[4]، وأضافت الجمعية الدولية لقانون العقوبات ضرورة وجود خبير معالجة بيانات يساعد في صياغة مسودة إذن التفتيش[5].

_التعرف قدر الإمكان على نظم الكمبيوتر قبل إجراء التفتيش.

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض ،2007، ص19

[2] يوسف بكري، المرجع السابق، ص 105-106.

[3] نفس المرجع ، ص108.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي، الجرائم الالكترونية، المرجع السابق، ص223.

[5] بكري يوسف بكري، نفس المرجع السابق، ص108.

- وضع خطة لتنفيذ التفتيش.
- العناية بمسودة إذن التفتيش–اشتمالها على وصف محل التفتيش–وشرح استراتيجية التفتيش الممكنة[1].

ب.القواعد الموضوعية لتفتيش نظم الحاسوب والانترنيت:

يجب مراعاة القواعد التالية حين قيام المحقق بعملية التفتيش:

1. **وجود سبب للتفتيش:** الإذن بالتفتيش لا يصح إصداره إلا لضبط ماديات الجريمة الواقعة بالفعل واتهام شخص أو عدة أشخاص بارتكابها، والمساهمة فيها مع توافر أمارات قوية على وجود أشياء تفيد فيكشف الحقيقة لدى المشتكى عليه أو غيره[2].

ويمكن حصر الشروط الموضوعية للتفتيش:

- أن يكون التفتيش بصدد جريمة الكترونية واقعة بالفعل سواء كانت جناية أو جنحة.
- لابد من اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة الالكترونية أو المشاركة في ارتكابها.
- لابد من توافر دلالات وأمارات قوية أو قرائن على وجود أجهزة، أدلة معلوماتية تفيد كشف الحقيقة لدى ال متهم[3].

وتفتيش نظم الحاسوب الآلي وفق الأسلوب الأمريكي يلخص فيما يلي:

- اقتحام قوة الشرطة للمكان بصورة سريعة ومن كافة منافذه في وقت واحد.

إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر الموجودة في المكان على الفور كي لا يتمكنوا من تدمير أي دليل وتوضع أجهزة الكمبيوتر الموجودة بالمكان في عهدة فريق يضم اثنين من العملاء. وتوضع أجهزة الكمبيوتر الموجودة بالمكان في عهدة فريق

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص225.

[2] علي حسن محمد الطوالبة، المرجع السابق، ص 62

[3] خالد ممدوح، المرجع السابق، ص 209–210.

يضم اثنين من العملاء أولهما مكتشف تم تدريبه تدريبا متقدما على نظم المعلومات وهو الذي يقوم بعملية الضبط ويتولى نزع مقبس الكهرباء الخاص بسائر الأجهزة كما يقوم بالبحث عن الأقراص المرنة والصلبة والملفات وحاويات الاسطوانات، والثاني مسجل يقوم بتصوير كافة الأجهزة والمعدات بالكيفية التي تم ضبطها عليه كما يقوم بتصوير كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدعي المجرم أن الشركة قد سرقت منزله أثناء التفتيش[1].

2. **تحديد محل التفتيش:** قد يقع التفتيش على شخص وقد يقع على مكان، والمقصود بالشخص قد يكون من مستغلي أو مستخدمي الكمبيوتر ومن خبراء البرامج، وقد يكون من المحللين ومن مهندسي الصيانة والاتصالات أو من مديري النظم المعلوماتية، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب ألي محمولة أو تليفونات متصلة بجهاز المودم أو مستندات[2].

والسلطة المختصة بتفتيش نظم الحاسب الآلي وفقا للقواعد الإجرائية المنصوص عليها في هذا الخصوص، بيد انه لابد من توافر صفة المحقق بمن يقوم بتفتيش مع الإذن بالتفتيش وان يكون أصلا مختصا بالتحقيق في ال جريمة[3]، وإستثناءا فان اغلب النظم الإجرائية تجيز تفتيش الأشخاص بناءا على حالة التلبس دون الحصول على إذن من سلطات التحقيق وفي حالات التلبس فانه يستلزم استصدار أمر بالتفتيش من الجهة المختصة، وفقا لإحكام القانون تحت طائلة البطلان[4].

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزئية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص289-291.

[2] نفس المرجع ، ص 214-215.

[3] عبد الفتاح بيومي حجازي ،نفس المرجع السابق، ص215.

[4] بكري يوسف بكري، المرجع السابق، ص 117-121.

ثانيا: ضبط الأدلة في الجريمة الالكترونية:

ضبط الأدلة مرحلة مهمة من مراحل التحقيق في الجرائم الالكترونية وتعتبر من أصعب الإجراءات التي يقوم بها المحقق، لأنه توجد في الجريمة الالكترونية أدلة رقمية يصعب التعامل معها.

1.مفهوم ضبط الأدلة في الجريمة الالكترونية:

يمكن تعريف الضبط بأنه وضع اليد على شيء يتصل جريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها سواء كان هذا الشيء عقارا أو منقولا، وقد يرد الضبط على الأشخاص وهو ما يصطلح على تسميته بالقبض[1].

والضبط بحسب الأصل لا يرد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات المادية للكمبيوتر، كرفع البصمات مثلا عنها و كذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه غير المشروع أو إتلافه بوسائل تقليدية كالكسر ،الحرق .لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس ، وفي ضبط بيانات الكومبيوتر DATA لعدم وجود أي دليل مرئي في هذه الحالات و لسهولة تدمير الدليل في ثوان معدودة و لعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات.

1. **إجراءات ضبط الأدلة في الجريمة الالكترونية:**

تضبط الأدلة في الجريمة وفق إجراءات خاصة فيما يخص ضبط المكونات المعنوية للجريمة.

أ.ضبط المكونات المادية في الجريمة الالكترونية : وهذا لا يثير أي إشكال فيخضع الضبط في هذه الحالة إلى قواعد الضبط في الجريمة الالكترونية، ذلك إن معظم التشريعات

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص207-208.

أجازت ذلك و مثاله نص المادة 487 من قانون الإجراءات الجنائية الكندي، و المادة 251 من قانون الإجراءات اليوناني ، كذلك ما جاء في قانون إساءة استخدام الحاسوب في انجلترا الصادر سنة1990[1] ، أما المشرع الجزائري فقد تطرق للقواعد الخاصة بالضبط من خلال نص المادة 84 التي يفهم بعد استقرائها انه يجب جرد الوثائق أو الأشياء المضبوطة ووضعها في احراز مختومة يجوز لقاضي التحقيق و ضابط الشرطة القضائية المندوب عنه الاطلاع على الوثائق و المستندات المراد حجزها ووضعها في إحراز مختومة بعد تحرير محضر بذلك[2] .

ولا يجوز فتح هذه الاحراز أو الوثائق إلا بحضور المتهم مصحوبا بمحاميه، ويمكن إصدار نسخ للوثائق التي تبقى مضبوطة، إذا تم تسليم النسخ يقوم الكاتب بالتأشير عليها بمطابقتها للأصل، أما إذا اشتمل الضبط على نقود أو سبائك أو أوراق تجارية أو أوراق ذات قيمة مالية ولم يكن من الضرورة لإظهار الحقيقة الاحتفاظ بها عينا فانه يتم إيداعها بالخزينة[4] و المادة 47 من قانون الإجراءات الجزئية و من بين الأدلة المتحصل عليه[3] :

1.**الورق:** يعتبر الورق من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة ينقسم الورق إلى أربعة أنواع:

- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصوير للعملية التي يتم برمجتها.
- أوراق تالفة تتم طباعتها للتأكد، ومن ثم إلقائها في سلة المهملات.

أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة[4].

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص274.

[2] محمد حزيط، المرجع السابق، ص 98.

[3] نفس االمرجع ، ص 98.

[4] محمد الأمين البشيري التحقيق في الجرائم المستحدثة جامعة نايف العربية للعلوم الأمنية الرياض ط1 2004 ص 117

2.جهاز الكمبيوتر وملحقاته

كذلك تشمل الماسح الضوئي SCANNER: الذي يتم عن طريق إدخال صورة أي مستند أو صورة لخريطة أو لإنسان أو حيوان أو ورقة إلى جهاز الحاسب الآلي ، مشغل الأقراص CD ROOM DRIVER و وظيفته تشغيل الأقراص المدمجة أو قرص الليزر الذي يحوي البيانات و المعلومات التي يريدها المجرم الالكتروني أو يرغب في تزويرها أو اختراقها لغرض إجرامي ، أيا كانت صورة السلوك الإجرامي المقترف.

– **وحدة المعالجة المركزية: Central Processing Unit** وتعتبر بمثابة العقل المفكر والمسيطر على عمل باقي الوحدات المكونة لجهاز الحاسوب وتقوم بمعالجة البيانات حسب التعليمات الواردة في البرنامج.

حيث يتم فيها جميع العمليات الحسابية أو المنطقية وتتكون بدورها من وحدة التحكم والسيطرة Control Unitووحدة الحساب والمنطق Arithemetic Logic Unit

– **وحدة الذاكرة Memory Unit** :هي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز آو تخزين النتائج الآتية من وحدة المعالجة المركزية وتنقسم إلى[1]:

– **وحدة الذاكرة الرئيسية Main Memory** : وهي الوحدة التي تقوم بحفظ البيانات والنتائج بشكل مؤقت[2] وتشمل ذاكرة القراءة فقط ROM والذاكرة العشوائية أو ذاكرة الوصول العشوائي RAM[3].

[1] نهلا عبد القادر المومني، المرجع السابق، ص26.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص398.

[3] نهلا عبد القادر المومني ،المرجع السابق، ص 27.

– **وحدة الذاكرة المساعدة:Auxiliary Memory** وتستخدم لتخزين كمية هائلة من البيانات وبصورة دائمة، حيث لا تفقد محتوياتها بانقطاع التيار الكهربائي، ومن أهم وسائط التخزين المستخدمة: الأقراص المرنة الصلبة، الأشرطة الممغنطة والأقراص المضغوطة[1].

وحدة الإخراج: Output Unitهي الوحدات التي يمكن من خلالها تحويل المعلومات غير المقروءة وغير المرئية إلى معلومات مقروءة، أو مرئية أو هما معا، فهي وسائل استخراج نتائج الاتصال بين الأفراد والحاسب الآلي، وتشمل الشاشات بأنواعها، الطابعات على مختلف أنواعها وكذلك وحدات رسم المنحنيات البيانية والوحدات الطرفية[2].

ب.ضبط المكونات المعنوية: انقسمت التشريعات الإجرائية حول إمكانية ضبط الأشياء المعنوية لاتجاهين الأول يرى عدم إمكانية تصور إجراء الضبط على الكيان المعنوي كونه ينصب على بيانات الحاسوب التي تختلف عن الأشياء المادية المحسوسة القابلة للضبط.

ومن التشريعات التي أخذت بهذا الاتجاه: قانون الإجراءات الجنائية الألماني، حيث حصرت المادة 94 منه محل الضبط على الأشياء المادية المحسوسة أو الملموسة ، نفس النهج، ويقترح إتباع هذا الاتجاه إضافة عبارة المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب إلى النص القانوني الذي ينص على التفتيش والضبط ليشمل التطور التكنولوجي لبيئة المعلومات.

أما الاتجاه الثاني فيرى بأنه لا مانع من ضبط البيانات الالكترونية مستندين إلى أن الغاية من التفتيش هو ضبط الأدلة المادية المفيدة في كشف الحقيقة، وبالتالي يمتد هذا المفهوم ليشمل البيانات الالكترونية بمختلف أشكالها ومن أتباع هذا الاتجاه القانون الكندي

[1] علي جبار الحسناوي، جرائم الحاسوب والانترنت، دار اليازوري، الأردن ،2009، ص24-25.

[2] محمد حماد موهج الهيتي، جرائم الحاسوب، دار المناهج، عمان، ط1، 2006، ص42.

مثاله ما جاء في نص المادة 487 وكذلك الشأن بالنسبة لفرنسا وامريكا[1]، أما المشروع الجزائري فكما سبق القول يأخذ بمبدأ جواز التفتيش والضبط لأنظمة الحاسوب[2].

ويمكن تعريف نظام الحاسوب بأنه تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد يسمى بالنظام المعلوماتي بغرض الوصول إلى نتيجة معينة، أو هو مجموعة من التعليمات المتتابعة بصفة منطقية توجه إلى الكمبيوتر لأداء عمل أو أعمال معينة[3]، ويطلق على أنظمة الحاسوب اسم البرمجيات التي تعد بمثابة العمود الفقري وعصب عمل الحاسب الآلي حيث لا يمكن للفرد أن يقوم بأي عملية ب دونها[4].

ومن بين المكونات المنطقية لجهاز الحاسوب التي يمكن ضبطها هي المعلومات والبيانات وبرمجيات الحاسوب: التي تشمل الوثائق، المستندات والمواد التي يطلق عليها المواد المساندة، وهي مواد مكتوبة في صورة كتيبات أو منشورات تطبع حاليا على الوسائط الالكترونية مثل الأقراص المرنة أو المدمجة.

وتنقسم إلى برمجيات النظم والبرمجيات التطبيقية[5].

الفرع الثاني: المعاينة وندب الخبراء في الجريمة الالكترونية

الانتقال لمكان الجريمة الالكترونية يكون لعدة أغراض منها معاينة مسرح الجريمة وذلك لإثبات صلة الأشخاص، الأماكن والأشياء بالجريمة، إلا أن المعاينة وحدها لا تكفي لإثبات

---

[1] علي حسن محمد طوالبية، المرجع السابق، ص146.

[2] **المادة 47**(القانون رقم 82-03 المؤرخ في 13 فبراير 1982) لايجوز البدء في تفتيش المساكن او معاينتها فيل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساء، الا إذا طلب صاحب المنزل او وجهت نداءات من الداخل او في الأحوال الاستثنائية المقررة قانونا.

المادة 48: يجب مراعا الإجراءات التي استوجبتها المادتان 45 و47 ويترتب على مخالفتها البطلان.

[3] احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2، 2006، ص42.

[4] بلال امين زين الدين، جرائم نظم المعالجة الالية للبيانات، دار الفكر الجامعي، الإسكندرية، ط1 ،2008، ص23.

[5] نهلا عبد القادر، مومني المرجع السابق، ص28-29.

ذلك، الأمر الذي يستدعي الاستعانة بالخبرة الفنية أو التقنية في مجال الانترنيت والعالم الافتراضي[1].

أولا: المعاينة في الجريمة الالكترونية:

قبل التطرق إلى إجراء المعاينة في الجريمة الالكترونية، يجب تحديد تعريف المعاينة لغة واصطلاحا وقانونا.

تعريف المعاينة في الجريمة الالكترونية:

أ. **تعريف المعاينة لغة:** المعاينة هي المشاهدة بالعين، عاين غيره رآه بعينه، وجاء في الأمثال والعيان لا يحتاج إلى بيان، ويضرب لإظهار مزايا المشاهد للتصديق بالشيء دون برهان[2].

ب. **تعريف المعاينة اصطلاحا:** هي أجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها كذلك جميع الأشياء الأخرى التي تفيد في كشف الحقيقة، واتخاذ ما يلزم من إجراءات كضبط بعض الأشياء.

فالهدف من المعاينة هو لغرضين اثنين: الأول جمع الأدلة الناتجة عن الجريمة "الآثار" والثاني إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها ولا غموض وقوع ال جريمة.

وقد أشارت قوانين الإجراءات الجنائية إلى إجراء المعاينة باعتباره إجراء من إجراءات التي تمتلكها السلطات التحقيقية بمختلف فئاتها و طوائفها[3]، و هذا ما ورد في نص المادة

---

[1] بخي فاطمة الزهراء، المرجع السابق، ص 88

[2] علي بن حمادة بلحسن، بليش الجبلاني بن الحاج، ص642.

[3] محمد حماد موهج الهيتي، المرجع السابق، ص255-256-257.

79من قانون الإجراءات الجزائية الجزائرية "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها ...."[1]

ج.تعريف المعاينة قانونا:

المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يرى المحقق أن لها صلة بالجريمة والأصل أن إجراء المعاينة متروك لتقدير المحقق لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة. الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية متلبس بها [2] .

1. **الانتقال والمعاينة في الجريمة الإلكترونية**

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية وذلك لندرة تخلف الآثار المادية عند ارتكاب الجريمة الإلكترونية، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار، فعند تلقي بلاغ عن وقوع إحدى الجرائم الإلكترونية وهذا بعد. التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته.

ومسرح الجريمة الإلكترونية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة

فالجريمة الإلكترونية قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية – السرقة والاحتيال–وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج وتفجير المباني والمنشئات، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة

[1] الامر 66–155 المؤرخ في 18 صفر 1386 الموافق ل 08يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06–22 المؤرخ في 29ذي القعدة عام الموافق ل 20 ديسمبر 2006، المتضمن قانون الإجراءات الجزائية.

[2] عبد الفتاح بيومي الحجازي، المرجع السابق، ص 100

هدفها المداهمة وضبط الأدلة على الطبيعة، وفي الحالة الثانية وبعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن.

وعند إجراء المعاينة بعد وقوع الجريمة في المجال الإلكتروني فيجب مراعاة الإجراءات التالية عند الانتقال إلى مسرح الجريمة[1].

ضرورة وجود معلومات مسبقة عن مكان الجريمة، من حيث الأجهزة المطلوب معاينتها وشبكاتها مع وجود خريطة تبين الموقع المراد معاينته، تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة، سواء من الضبط أو التأمين أو حفظ الأوراق، كما يجب على القائمين بالمعاينة، تأمين الأجهزة والمعدات التي يتم الاستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة، وإخطاره مسبقا حتى يستعد من الناحية الفنية والعملية ويعد خطة مناسبة للمعاينة[2]،

وأكيد قبل كل شيء يجب مراعاة ما جاء في القوانين الجنائية حول المعاينة وذلك تحقيقا لمبدأ الشرعية.

ثانيا: ندب الخبراء في الجريمة الالكترونية

تعتبر الخبرة من أهم الإجراءات التي تتخذ للتنقيب عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها.

1. تعريف الخبرة في الجريمة الإلكترونية

ولمعرفة الخبرة في الجريمة الإلكترونية يجب التطرق أولا لتعريف الخبرة لغة واصطلاحا.

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الاثبات الجنائي بالادلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض،2007، ص17.

[2] عبد الفتاح بيومي حجازي، الجوانب الإجرائية الاعمال التحقيق، دار النهضة العربية، القاهرة، ط1، 2009، ص586.

أ. **تعريف الخبرة لغة:** الخبير لغة هو اسم من أسماء الله تعالى أي العالم بما كان وما سيكون.

ب. **تعريف الخبرة اصطلاحا:** الخبير في اصطلاح المحاكم هو من يعين للتدقيق في مختلف. الأمور المتعلقة بشتى القضايا ويكون لرأيه فيها القول الفاصل[1].

والخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات، فهي في الحقيقة ليست دليلا مستقلا عن القولي أو الدليل المادي، إنما هي تقييم فني لهذا الدليل والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة، الشهادة والتفتيش.[2]

وعليه يمكن تعريف الخبير انه كل شخص له إلمام بأي علم أو فن سواء كان اسمه . مقيدا في جدول الخبراء على مستوى المحاكم أم لا [3].

كما عرف الخبير " بأنه كل شخص له دراية بمسالة من المسائل وقد يستدعي التحقيق فحص مسالة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيرا

كما هو الحال في تقرير الصفة التشريحية في جرائم القتل أو تحليل المادة المطعومة في جريمة تسمم أو فحص لخطوط الكتابة المدعى بتزويرها" ، ولما كان قاضي التحقيق هو المختص بالتحقيق، قد يتعرض في عمله لمسائل فنية يصعب عليه كرجل قانون البت فيها حينئذ يجوز له ندب أهل الخبرة حتى يخرج .التحقيق في صورة موضوعية صادقة[4].

---

[1] علي بن حمادية، بن لحسن البليش ،الحلالي بن الحاج بخي، المرجع السابق ،ص 302.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الانترنت، المرجع السابق، ص 321.

[3] احمد سيولي ابو الروس، التحقيق الجنائي والأدلة الجنائية، ط2، 2008، ص33.

[4] عبد الناصر محمد محمود فرغلي، محمد سيف سعيد المسماري، المرجع السابق، ص 24.

2. الخبير في الجريمة الإلكترونية:

من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة الإلكترونية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه، وان نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخص هؤلاء الخبراء، وكذا يجب على المحقق الجنائي أن يحدد للخبير الإلكتروني دوره في المسالة الانتداب فيها على وجه الدقة، وبالنظر إلى أن الجريمة الإلكترونية لها الخصوصية التي تتعلق بها فإن الخبير الإلكتروني قد يكون من الجناة الذين سبق لهم ارتكاب مثل هذه الجرائم وتم تذويبهم داخل المؤسسات الإلكترونية للاستفادة من . قدراتهم فضلا عن تأهيلهم كمواطنين صالحين[1].

3.أساليب عمل الخبير في الجريمة الإلكترونية:

هناك أسلوبان لعمل الخبير هما:

أ .القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كجريمة

التهديد أو النصب، جرائم النسخ...الخ، ثم يقوم الخبير بعملية تحليل رقمي لها، وذلك لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها وأخيرا التوصل لمعرفة برتوكول الانترنيت "IP" الذي ينسب إلى جهاز .الحاسوب الذي صدرت عنه هذه المواقع.

ب . القيام بتجميع وتحصيل لمجموعة المواقع الذي لا تشكل موضوعها جريمة في ذاته، ولكن الجرائم تقع من جراء تتبع موضوعات هاته المواقع، مثلما ما هو الحال في المواقع التي تساعد الغير على معرفة جرعات المخدرات والمؤثرات العقلية حسب وزن الإنسان، بإيهامه أنه إذا تم تتبع التعليمات الواردة فيها لن يصل إلى الشخص إلى حالة

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص 329-330.

إدمان، كذلك الشأن بالنسبة لكيفية إعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية ...الخ.

4.دور الخبير التقني في حفظ الأدلة الإلكترونية:

إن التحفظ على الأدلة الإلكترونية من العمليات المعقدة، حيث تحتاج أولا إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، وكذلك صحة حركة الكمبيوتر فلو كان هناك فيروس في الجهاز لتم التشكيك في صحة الأدلة المستفادة منه، ويحفظ الدليل في العالم الافتراضي برصد موقع الانترنت أو المعلومات التي تشير إلى الجريمة، والتي تكون في مظاهر مختلفة الأشكال ونأخذ على سبيل المثال جريمة القذف في غرف الدردشة، هنا يتم اللجوء إلى ذلك ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي للتوصل إلى تحديد موضوع القذف وتاريخه، ولقد لجأت العديد من المحاكم إلى ميكنة إدارتها رقميا، . بحيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى حفظ الأدلة الرقمية [1].

ويتعين على الخبير تضمين المسائل التالية في مهمته:

-تركيب الحاسب الآلي، وطرازه ونوعه ونظام تشغيله والأنظمة الفرعية التي يستخدمها.

-بيئة الحاسب أو الشبكة من حيث طبيعتها، تركيزها أو توزيعها، و كذلك نمط ووسائط الاتصالات[2].

-المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.

-الآثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة الإلكترونية.

-كيفية عزل النظام المعلوماتي – عند الحاجة-، دون إتلاف الأدلة أو الأجهزة أو تدميرها.

-إمكانية نقل أدلة الإثبات إلى أوعية أخرى دون تلف.

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 309-310.

[2] بخي فاطمة الزهراء، المرجع السابق، ص 96.

-إمكانية نقل أدلة الإثبات لأوعية مادية كالأوراق على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة[1].

وينصرف رأي الخبير إلى الوقائع اللازم إصدار رأيه الفني بشأنها، كما يجب أن يتوقف رأيه عند المسائل الفنية دون أن يتعدى للمسائل الأخرى كالمسائل القانونية[2].

المبحث الثاني:

الحماية القانونية للبطاقات المصرفية

تسهر الدولة على حماية المصالح القانونية بواسطة مجموعة من التشريعات، تهدف

من ورائها على الحفاظ على الحقوق المشروعة، ولهذا ظهرت الحاجة لتوفير غطاء قانوني للعقاب على الاعتداءات التي تقع على البطاقة الائتمانية، وبما أن جريمة التزوير من الجرائم المضرة بالمصلحة العامة كونها تستهدف الثقة التي أودعها المشرع في المحررات لذلك تحتم المعاقبة على كل الأفعال التي تهدر تلك الحقوق سواء كانت تلك المحررات رسمية أو عرفية

ولتوضيح هذا الموضوع بشكل أكثر، أثرنا أن نقسم هذا المبحث إلى مطلبين بحيث نتناول في المطلب الأول: **الأساس القانوني لتجريم تزوير البطاقات بينما** نخصص المطلب الثاني: لعقوبات **جريمة تزوير البطاقات المصرفية[3].**

---

[1] عبد الفتاح بيومي، المرجع السابق، ص 330-331.

[2] بخي فاطمة الزهراء، المرجع السابق، ص97.

[3] عبد العزيز نقطي، **(جريمة التزوير في بطاقات الائتمان)**، مجلة العلوم القانونية والسياسية، المجلد 13، العدد 01، ص 752-771، ابريل 2022.

المطلب الأول:

الأساس القانوني لتجريم جريمة التزوير للبطاقات المصرفية

يتحدد الإطار القانوني لجريمة تزوير البطاقة الائتمانية وفق مجموعة من النصوص الواردة في الاتفاقيات الدولية والتشريعات الداخلية، لتضفي حماية من الاعتداءات الواقعة عليها والمتمثلة بالأفعال المحققة لتغيير الحقيقة وللحديث بشكل أكثر قسمنا هذا المطلب إلى فرعين، الفرع الأول: الأساس القانوني على المستوى الدولي ويتضمن الفرع الثاني الأساس القانوني على المستوى الوطني.

الفرع الأول: الأساس القانوني على المستوى الدولي

حرصت دول العالم على تجريم التزوير وأفردت لها تشريعات في الاتفاقيات والتوصيات الناتجة عن المؤتمرات الدولية، لكون العالم يشهد ثورة كبيرة في مجال التجارة الالكترونية تمثلت بانتقال رؤوس الأموال والبضائع، مما أدى إلى ظهور عصابات دولية تمارس أعمال التزوير على نطاق واسع، ولذلك وضعها البعض تحت المسمى الجرائم المنظمة التي يقصد بها مجموعة من المنظمات أو الجمعيات الإجرامية، واستخدم لفظ " الجريمة المنظمة " لأول مرة في نشرات البوليس الدولي للجريمة المنظمة، ومن بين هذه الاتفاقيات[1].

أولا: الاتفاقيات الدولية المنعقدة برعاية منظمة الشرطة الدولية

تطلع منظمة الشرطة الدولية (الانتربول) بدور هام وفعال في متابعة الظواهر الإجرامية بصورة عامة والإجرام ألمعلوماتي على وجه الخصوص، من خلال الأقسام والشعب التي تتكون منها المنظمة كشعبة الإجرام الاقتصادي والمالي وشعبة التقصي الآلي وتحليل المعلومات وغيرها من الأقسام الخاصة المهتمة بمتابعة الظواهر الإجرامية على المستوى

---

[1] هدى حامد قشقوش، **جرائم الحاسب الالكتروني في التشريع المقارن**، دار النهضة العربية للنشر والتوزيع، القاهرة،2000، ص 6

الدولي وهي كذلك تقوم بالتعاون المتبادل في مجال المعلومات ومكافحة ومنع انتشار الجرائم من خلال الخطط التي تضعها والمتابعة المستمرة للإجرام الدولي[1].

وبخصوص دورها في متابعة الجرائم الواقعة على البطاقة الائتمانية فقد نظمت السكرتارية العامة أولى مؤتمراتها الدولية بخصوص الاحتيال والغش في البطاقة الائتمانية في عام 1994 وتمخض عن هذا المؤتمر وصيتين وهما:

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

2- إنشاء مجموعات عمل بوليسية من خبراء متابعة جرائم الغش والاحتيال على المستوى الدولي التابعين لبوليس هونك كونك والشرطة الكندية والخدمة السرية الأمريكية وخدمة الاستخبارات القومية الجنائية النيوزلندية ومندوبين من منظمات الائتمان لمكافحة هذا النوع من الإجرام ووضع الأسس الخاصة لتبادل المعلومات والحد منه[2].

وبناء على هذه التوصيات عقدت خمس اتفاقيات بين المنظمات المصدرة للبطاقات الائتمانية وأجهزة المنظمة لتوثيق التعاون ولمكافحة الجرائم الواقعة على البطاقة الائتمانية.

ثانيا: اتفاقية بودابست

سميت الاتفاقية كذلك باتفاقية مكافحة الإجرام السيبيري أو الإجرام الافتراضي أو الكوني و تم توقيعها في عام 2001 ، تضمنت المذكرة الإيضاحية للاتفاقية .ظهور الثورة الالكترونية في عالم المعلومات ضاعف من ارتكاب الجرائم الاقتصادية و منها الغش و

---

[1] معادي اسعد صوالحة **بطاقات الائتمان، النظام القانوني و آليات الحماية الجنائية و الأمنية**– دراسة مقارنة – ، المؤسسة الحديثة للكتاب ، لبنان ، 2010 ، ص 489

[2] محمد عبيد الكعبي **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت**،دار النهضة العربية للنسر والتوزيع،القاهرة،2009، ص 276 .

الاحتيال و التزوير في بطاقات الائتمان فالأصول المالية التي يتم تداولها بواسطة الحاسب الآلي أصبحت هدفا للتداول ، و تتضمن هذه الاتفاقية عدة مواد تناولت أوجه الاجرام ألمعلوماتي، فقد عرفت المادة 7 التزوير بأنه " إدخال أو إفساد أو تعطيل أو محو أو شطب عن قصد و بدون وجه حق " و التزوير وفقا لهذا المفهوم يعني أن الصور التي يتحقق بها التزوير[1]

ألمعلوماتي هي الإدخال أو التعطيل أو الإفساد أو المحو أو الشطب إذا ارتكبت عن قصد وبدون وجه حق في المعطيات الالكترونية، والحصول على معطيات غير صحيحة.

بهدف استعمالها بطريق غير مشروع كما لو كانت تلك الوسائط صحيحة وأصلية، أم المادة 8 نصت على انه: " يجب على كل طرف أن يتخذ الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية للتجريم تبعا للقانون الوطني وتجريم أي فعل يتسبب في إحداث ضرر مالي للغير عمدا وبدون وجه حق عن طريق ما يلي:

الإدخال أو الإتلاف أو المرور ضمن نشاطات الحاسب الآلي.

كل شكل من أشكال الاعتداء على الحاسب الآلي بنية الغش أو أي نية إجرامية مشابهة للغش من اجل الحصول بدون حق على منفعة اقتصادية لمرتكب الفعل "[2].

و يتضح من النص أعلاه أن التزوير الواقع على البطاقة الائتمانية وفقا لما جاءت به الاتفاقية قد نص عليه في المادة 7 التي نظمت الأفعال التي يقع بها التزوير ، إلا أن ما تجدر به الإشارة إليه هنا هو عدم تطرق هذه المادة للتزوير الواقع بطريق التغيير و اكتفى النص بالإدخال أو المحو ، أما المادة 8 فقد أوجبت على الدول اتخاذ الإجراءات التشريعية اللازمة لتجريم هذه الأفعال لضمان مساءلة المزورين وفقا للقوانين الداخلية ، و هي انتقاله

---

[1] عبد العزيز نقطي، **نفس** المرجع السابق، ص 10.

[2] هلال عبد اللاه احمد، **اتفاقية بودابست لمكافحة جرائم المعلوماتية**، دار النهضة العربية للنشر والتوزيع، القاهرة، 2011، ص94

نوعية تؤكد الاتجاه الدولي لوضع نصوص قانونية تعالج الجريمة المعلوماتية و على ذلك فهي تشكل أساس قانوني كفيل لحماية البطاقة و لأجهزة الصراف الآلي من التلاعب[1].

ثالثا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

شرعت الاتفاقية المعقودة برعاية جامعة الدول العربية لمكافحة الجرائم المعلوماتية ولذلك فنطاق سريانها يكون إقليميا وذلك للحد من خطر هذه الجرائم والآثار السلبية للحفاظ على الأمن العربي من الناحية المعلوماتية و من خلال تحليل نصوص الاتفاقية العربية نجد أنها قد جرمت الاعتداءات الواقعة على البيانات و المعلومات و من وجهة نظر عامة، و جرمت التزوير ألمعلوماتي بشكل خاص، فنصت المادة 10 على أن التزوير ألمعلوماتي هو:" استخدام وسائل تقنية المعلومات من اجل تغيير الحقيقة في البيانات، تغييرا من شأنه إحداث ضرر، و بنية استخدامها كبيانات صحيحة " .

ويمكن القول بان الاتفاقية العربية قد سابرة التطور التشريعي على المستوى الدولي ووضعت أساس قانوني تمثل بتجريم الاستخدام غير مشروع لوسائل تقنية المعلومات من اجل تغيير الحقيقة بشكل عام لتكون أساس مهم لتوضيح مفهوم التزوير ألمعلوماتي، بينما خصصت المادة 18 الاستخدام غير مشروع لوسائل التزوير ألمعلوماتي في مجال بطاقات الدفع الالكتروني من خلال ما يلي:

*كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على التزوير أو تقليد أي أداة من أدوات الدفع الالكتروني بأي وسيلة كانت.

*كل من استولى على بيانات أو أي أداة من أدوات استعمالها أو قدمها للغير أو سهل للغير للحصول عليها.

[1] هدى حامد قشقوش، نفس المرجع السابق، ص 8.

*كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات تخص بطاقات الدفع.

*كل من قبل بأداة من أدوات الدفع المزورة مع علمه بذلك [1].

الفرع الثاني: الأساس القانوني على المستوى الوطني

تأثر المشرع الوطني كغيره من التشريعات المقارنة بالاتفاقيات الدولية التي نصت على ملاحقة ومعاقبة المتورطين في جرائم تزوير بطاقات الائتمان، فجاء صدور القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وتبنى المشرع الجزائري المفهوم الواسع للجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 02 منه بقولها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية " نلاحظ من خلال هذا التعريف أن المشرع أدرج جميع جرائم المعلوماتي[2].

سواء التي نص عليها قانون العقوبات أو الجرائم التي يمكن أن تقع مستقبلا وذلك بقوله: " أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ".

و في إطار الوقاية من جرائم المعلوماتية و التي تدخل جريمة التزوير تحت أحكامها ، فان المشرع أورد في المادة 14 من القانون 09-04 المهام التي تقوم بها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و المتمثل في

[1] عبد العزيز نقطي، نفس المرجع السابق، ص 11

[2] نفس المرجع، ص 12.

تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بخصوص الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال ، تبادل المعلومات مع نظيرتها في الخارج قصد التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تحديد مكان تواجدهم .

و على صعيد قانون العقوبات نجد أن المشرع استحدث جرائم جديدة تمثلت في الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات و هذا بنص المواد 394 مكرر، و على صعيد قانون التوقيع و التصديق الالكترونيين نجد بان المشرع نص على تزوير التوقيع الالكتروني و ضرورة حمايته من التزوير عن طريق توفير التقنيات اللازمة للحماية وقت الاعتماد[1] .

نشير هنا إلى أن المشرع الفرنسي كذلك جرم التزوير ألمعلوماتي في عدة مواقع، ذكر منها القانون الصادر في 1988/1/5 المتعلق بالغش ألمعلوماتي وتجريم استعمال الوثائق المعلوماتية المزورة بشكل عام، وعاقب على تزوير بطاقة الوفاء بشكل خاص ويلاحظ البعض أن القانون استعمل تعبيرا جديدا في ذلك الوقت وهو– المستندات المعالجة آليا –

إلا أن القانون لم يحدد مضمون تلك العبارة فجاء النص واسعا و الذي أعطى دلالة لإمكانية وقوع التزوير على أي دعامة أو سند معلوماتي تم الحصول عليه بواسطة وسائل معلوماتية و كذلك لم يحدد النطاق الذي ينطبق عليه النص و إنما ترك ذلك دون تحديد[2] .

كذلك قانون امن الشيكات (91/1382) فقد أورد المشرع مادة مستقلة عاقب فيها على ظاهرة تزوير البطاقة المصرفية بشكل خاص ، إما قانون العقوبات الفرنسي الجديد و الساري

---

[1] هدى حامد قشقوش، نفس المرجع السابق، ص 115.

[2] محمد نورالدين سيد عبد المجيد ، **المسؤولية الجنائية عن تزوير بطاقات الائتمان** ، دار النهضة العربية للنشر و التوزيع ، ط1 ، القاهرة ، 2012 ، ص 106

المفعول منذ 01 مارس 1994 فقد نظم التزوير بشكل جديد و هذا بقصد استيعاب التزوير العادي و الالكتروني و ذلك من خلال وضع نص عام يمكن من خلاله المعاقبة على كل من دخل تحت مضمونه من مفاهيم [1].

المطلب الثاني:

عقوبات تزوير البطاقات المصرفية

ينحصر النشاط الإجرامي المعلوماتي في أفعال الإدخال و المحو و التعديل و لا يشترط إجماعها معا حتى يتوافر النشاط الإجرامي فيها إذ يتوفر الركن المادي للجريمة بمجرد القيام بفعل واحد على حدا ، لكن القاسم المشترك في هذه الأفعال جميعها هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل و للحفاظ على امن و خصوصيات بطاقات الائتمان سنتطرق الى عقوبة تزوير بطاقة الائتمان عند التشريع الفرنسي في الفرع الأول ثم عقوبة تزوير بطاقة الائتمان في التشريع الجزائري في الفرع الثاني .

الفرع الأول: عقوبة تزوير البطاقات المصرفية في التشريع الفرنسي

تضمن التشريع الفرنسي مجموعة من النصوص التي تتعلق ببطاقة الائتمان في القانون رقم 88-19 الصادر في 05 جانفي 1988 والخاص بالغش المعلوماتي، والذي كفل لها حماية جنائية جزائية في نطاق المستندات المعالجة آليا، حيث يعاقب على تزويرها وذلك من خلال نص المادتين 5/462 و6/462 من قانون العقوبات.

حيث نصت المادة 5/462 على انه:" يعاقب من عام إلى خمسة أعوام والغرامة من عشرين ألف فرنك، وحتى مليوني فرنك كل من قام بتزوير المستندات المعالجة أليا، أيا كان شكلها طالما من شأن ذلك إحداث ضرر للغير " كما نصت المادة 6/462 على تطبيق

[1] عبد العزيز نقطي، نفس المرجع السابق، ص12

العقوبتين السابقتين أو إحداهما على كل من استعمل المستندات المزورة المعالجة اليا، والمنصوص عليها في المادة السابقة إذا كان عالما بطبيعتها[1].

و بتزايد تداول البطاقات بين أفراد المجتمع الفرنسي و بالتالي تزايد حجم الخسائر الناجمة عن إساءة استعمالها، و بالنظر إلى الاعتبارات القانونية القائمة بالدرجة الأولى على مبدأي الشرعية الجزائية و حظر القياس لغايات التجريم، فقد اصدر المشرع الفرنسي قانون خاص يكفل حماية واضحة و صريحة و مباشرة لمعظم صور الاعتداء على البطاقات الالكترونية، و هو القانون رقم 91-1382 الصادر بتاريخ 30 ديسمبر 1991 و أطلق عليه قانون امن الشيكات و بطاقات الوفاء[2] .

وتنص المادة 1/67 من هذا القانون على انه:" يعاقب بالعقوبات المنصوص عليها في المادة 67 وهي الحبس من سنة إلى سبع سنوات والغرامة تتراوح ما بين 3600 إلى 500.000 فرنك أو بإحدى هاتين العقوبتين فقط، كل من قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب «، كما تنص المادة 163-1/4 على انه:" يعاقب بالعقوبات المنصوص عليها في المادة 163-3 وهي الحبس سبع سنوات وبغرامة تقدر 750.000 اورو كل شخص يقوم بتقليد أو تزوير بطاقة وفاء أو سحب "[3].

نشير هنا بان العقوبة المقررة من قبل المشرع الفرنسي على جرائم تزوير البطاقات وفقا للمادة 67-1 و هي:" السجن لمدة لا تقل عن سنة و لا تزيد عن سبع سنوات بالإضافة إلى الغرامة المالية " هي عقوبة اشد من تلك المقررة من خلال المادة 462-5 من القانون رقم 88-19 و التي تقضي بالسجن من سنة إلى خمس سنوات[4] .

---

[1] Loi N°88-19 du 5 Janvier 1988 relative à la fraude informatique

[2] بلعالم فريدة، **المسؤولية القانونية عن الاستخدام غير المشروع لبطاقة الائتمان** ، dépôt Dspace ، 2015، ص 167 ، في 2023/05/22 على 14:45 .

[3] بلعالم فريدة، المرجع السابق، ص 167

[4] عبد العزيز نقطي المرجع السابق، ص 17

بالإضافة إلى العقوبات المشار إليها سابقا في قانون النقد الفرنسي ، أكد أيضا على مصادرة و تخريب الأجهزة المستخدمة في تزوير و تزييف البطاقات بنفس الطريقة المطبقة على تزوير و تزييف الشيكات ، و هذا بنص المادة 163 الفقرة الخامسة كعقوبة تكميلية ، إلا إن اعتبار المشرع الفرنسي مصادرة و إعدام الأدوات و الآلات و الأجهزة و الوسائل التي استعملت في تزوير و تزييف بطاقات الائتمان كعقوبة تكميلية ، إلا أن هناك استثناء حيث جعل المشرع الفرنسي هذه العقوبة تكميلية إذا كان مالك هذه الوسائل و المعدات المستعملة حسن النية ، و هذا ما أكدته الفقرة الثانية من المادة 67 من القانون الخاص بالأمان في الشيكات و البطاقات الصادر في 30 ديسمبر 1991 بنصها : " ماعدا إذا تم استعمالها بدون علم مالكها " ، و هذا ما يعني عدم مصادرة و إتلاف الأشياء المستعملة في الجريمة و نستنتج من ذلك أن هذه العقوبة التكميلية هي عقوبة وجوبيه مع الاحتفاظ بحق الغير حسن النية و هو نفس النهج الذي سار عليه المشرع الجزائري[1] .

الفرع الثاني: عقوبة تزوير البطاقات المصرفية في التشريع الجزائري

جاءت عقوبة التزوير متنوعة بحسب الطريقة المتبعة في التزوير والجهة التي تقوم به، بحيث كانت مشددة إذا صدرت من قاض أو موظف أو قائم بوظيفة عمومية، وهو ما أكدت عليه المادتان 214 و215 من قانون العقوبات الجزائري، ونصت على أن العقوبة تكون بالسجن المؤبد إذا ثبت التزوير بالطرق التي حددتها نفس المادة.

أما إذا وقع التزوير في محررات رسمية أو عمومية من طرف أي شخص، عدا الأشخاص المذكورين في المادة 214، من قانون العقوبات، تكون العقوبة بالسجن من 10 سنوات إلى 20 سنة وبغرامة مالية تتراوح من 1.000.000 دج إلى 2.000.000 دج.

[1] محمد نور الدين سيد عبد المجيد، نفس المرجع السابق، ص 381

ونصت المادة 219 من قانون العقوبات الجزائري على عقاب الشخص الذي يرتكب تزويرا بإحدى الطرق المحددة في المادة 216 من نفس القانون، بالحبس من سنة إلى خمس.

سنوات وبغرامة مالية من 500 إلى 20.000 دج كعقوبة أصلية، إضافة إلى العقوبة التكميلية والمتمثلة بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 من نفس القانون، وكذلك المنع من الإقامة من سنة إلى خمس سنوات على الأكثر.

وشددت المادة 219 من قانون العقوبات سالفة الذكر العقوبة ورفعتها إلى الضعف في حالة ما إذا ارتكبت الجريمة من طرف أحد رجال المصارف أو مدير شركة، أو أي شخص من الأشخاص الذين يلجئون إلى الجمهور بقصد إصدار أسهم، أو سندات، أو اذونات، أو حصص، أو أية سندات كانت سواء لشركة، أو مشروع تجاري أو صناعي.

وجاءت عقوبة التزوير في المحررات العرفية في المادة 220 من قانون العقوبات الجزائري السالف الذكر، بحيث حددتها بالحبس من سنة إلى خمس سنوات وبغرامة مالية من 500 إلى 2.000 دج كعقوبة أصلية بالإضافة إلى عقوبة تكميلية، والمتمثلة في الحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 من نفس القانون والمنع من الإقامة من سنة إلى خمس سنوات على الأكثر.

و نلاحظ من خلال المواد القانونية السابقة أنها استهدفت التزوير الذي يتعرض له المحرر من الناحية المادية ، أما فيما يخص التزوير المعنوي أو التزوير المعلوماتي ، فقد جاءت العقوبات عليه في المواد من 394 مكرر إلى 394 مكرر 7 ، حيث نصت المادة 394 مكرر من قانون العقوبات الجزائري على المعاقبة بالحبس من ثلاثة أشهر إلى سنة و بغرامة مالية من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ، و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، و إذا ترتب على الأفعال المذكورة

أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج.

ونشير هنا إلى أن الشروع في جريمة التزوير يأخذ حكم جريمة التزوير التامة من حيث التكييف والعقوبة المقررة لها وهذا استنادا للمادتين 216 و219 من قانون العقوبات، كما عاقبت المادة 394 مكرر 1 من نفس القانون بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية من 500.000 دج إلى 2.000.000 دج كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات، أو زال أو عدل بطريق الغش المعطيات التي يتضمنها[1].

لم يكتف المشرع بالعقوبة على التزوير عند هذا الحد بل ذهب إلى ابعد من ذلك، عندما أكد على معاقبة كل من يقوم بنشر وتوزيع المعطيات المتحصل عليها من الأنظمة المعالجة آليا وحددت المادة 394 مكرر 2 العقوبة بالحبس من شهرين إلى ثلاث سنوات وبغرامة مالية من 1.000.000 دج إلى 5.000.000 دج وشدد المشرع عقوبة التزوير المعلوماتي إذا كانت تستهدف الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام مع الاحتفاظ بتطبيق العقوبة الأشد في حالة تعدد الجرائم، وهو ما أكدت عليه المادة 394 مكرر 3 من قانون العقوبات.اضافة إلى ما أوردناه سابقا فإن المشرع لم يستثني الشخص المعنوي من العقوبة في حالة ارتكابه لجريمة التزوير المعلوماتي، وحدد العقوبة بخمس أضعاف الحد الأقصى للعقوبة المقررة للشخص الطبيعي، كما أكد المشرع على مصادرة جميع الأدوات، والوسائل التي استخدمت في الجريمة مع إغلاق المواقع التي تكون محلا للجريمة، بالإضافة إلى إغلاق المحل، أو المكان الذي استغل لارتكاب الجريمة شريطة علم مالكه بذلك، غير انه لا يتم مباشرة هذه الإجراءات بالنسبة للغير حسن النية[2] .

---

[1] عبد العزيز نقطي، نفس المرجع السابق، ص 15

[2] عبد العزيز نقطي، نفس المرجع السابق، ص 16.

خلاصة الفصل

تشكل الاعتداءات على البطاقات المصرفية خطورة بالغة لما تسببه من خسائر في مجال التعاملات المالية ، خاصة و أن هذه الجرائم ذات طبيعة تقنية لكونها ترتبط بأجهزة الكترونية و لذلك نجد أن مرتكبي هذه الجرائم يتصفون بالفطنة و الذكاء في هذا المجال ، و عليها وجب تبني استراتيجية لمكافحة هذا النوع من الجرائم للحد منها و ردع مرتكبيها ، حيث تطرقنا لذلك من خلال المبحث الأول تحت عنوان إجراءات التحقيق في جريمة تزوير البطاقات المصرفية وفقا للجرائم الالكترونية و يحتوي على أهم العناصر الإجرائية و التي تتمثل في : اتصال المحقق بالجريمة الالكترونية ثم الانتقال إلى مسرح الجريمة الالكترونية و للحد من هذه الجريمة وجب على المشرع وضع حماية قانونية للبطاقات المصرفية و هذا ما تناولناه في المبحث الثاني ، و يتمثل ذلك في الأساس القانوني لتجريم تزوير البطاقات المصرفية و العقوبات المقررة لمرتكبي هذا النوع من الجرائم المعلوماتية .

الخاتمة

تتجلى مجهودات المشرع الجزائري في حماية البطاقات المصرفية من خلال وضع نظام سياسي للحد من الجرائم التي تتعرض لها ، و كذلك آليات وقائية و ردعية مختلفة حسب خطورة الفعل المجرّم و من بين هذه الاعتداءات التي تتعرض لها البطاقات المصرفية جريمة التزوير ، التي لا تشكل في وقتنا الحاضر مشكلة مقارنة بما يحدث مع المجتمع الغربي ، إلا أن هذا لا يدعو للاطمئنان و خاصة أن الجزائر تسعى لانتهاج سياسة الانفتاح الاقتصادي و الذي بدوره يساعد على انتقال هذه الجريمة عبر الأسواق المفتوحة على بعضها البعض ، لذا وجب على المشرع الجزائري ندارك الأمر بسرعة و مواكبة التشريعات الأجنبية في هذا الشأن .

حيث نلاحظ أن الإجراءات والتدابير الوقائية لحماية البطاقات المصرفية من أهم الحلول والتي تسعى بدورها لمحاربة هذا النوع من الجرائم.

النتائج:

ومن خلال دراستنا توصلنا إلى النتائج التالية:

1 –إثبات التزوير من الأمور المستعصية على الجهات القضائية وجهات التحقيق خاصة إذا تعلق الأمر بالجاني المعلوماتي للبطاقة بحيث تتطلب مهارات وخبرات عالية في مجال المعلوماتية والانترنت.

2 – جريمة التزوير والتلاعب بالبطاقات المصرفية من الجرائم التي لم تكن موجودة سابقا، وأن ظهورها مرتبط بتكنولوجيا المعلوماتية والحاسب الآلي.

3 – توعية وتحسيس حاملي البطاقات المصرفية إلى ضرورة إتباع الأسلوب الوقائي في استعمال الحذر للبطاقات المصرفية.

4 – حامل البطاقة المصرفية يجب أن يكون كامل الأهلية بالنظر للالتزامات ومسؤولية البطاقة، أما ناقص الأهلية وعديمها فيجوز فتح اعتماد مصرفي باسمهم على أن يكون التعامل بها لممثلهم القانوني.

5–يتلخص دور ضباط الشرطة القضائية في مكافحة الجزائم الالكترونية في اجراء عمليات البحث والتحري لجمع الأدلة.

6–يتمثل دور الخبراء في اثبات الجرائم المعلوماتية وكشف انماطها.

7–اتفاقية بودابست أداة دولية رئيسية التي تسمح بالتعاون الدولي الفعال والمناسب بشأن الأدلة الالكترونية.

إقتراحات:

1 – العمل على إصدار قانون جنائي رقمي من طرف المشرع الجزائي الجزائري بشقيه الموضوعي والإجرائي.

2 – التركيز على الجانب الإجرائي وأساليب التحري والتحقيق الخاصة لتتلاءم مع طبيعة جريمة التزوير، تفاديا للقصور التشريعي والثغرات القانونية التي قد يستفيد منها المجرم المعلوماتي للإفلات من المتابعة والعقاب.

3 – العمل على إنشاء أجهزة ووحدات أمنية متخصصة في التحقيق في هذه الجرائم، يكون لديها الخبرة والإلمام الكافي بالجوانب التقنية والفنية عن طريق تكثيف البرامج والدورات التدريبية وعدم اقتصارها على المستوى الوطني فقط وإتاحة المشاركة في الدورات المنعقدة في الدول الأجنبية.

4 –إنشاء منظمة شرطة عربية تهتم بالتنسيق بين الدوال في مجال مكافحة الجرائم الالكترونية، كمنظمة الانتربول والاوروبول وغيرها.

قائمة المراجع

- **الاتفاقيات الدولية:**

1. اتفاقية بودابست 28 ابريل 1977.
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

- **القوانين:**

1. القانون 04/09 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.
2. الامر رقم 66-155 المؤرخ والمتمم في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية، المعدل والمتمم. المواد 72/48/47.
3. الامر رقم 156/66 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو سنة. 1999، الذي يتضمن قانون العقوبات المعدل والمتمم. المواد215/214.
4. القانون الفرنسي رقم 19.88 بتاريخ 5 يناير 1988 المتعلق بجرائم الغش المعلوماتي.

- **الكتب :**

- **الكتب العامة:**

1.بلعليات ابراهيم،اركان الجريمة و طرق اثباتها في قانون العقوبات الجزائري،دار الخلدونية،الجزائر،ط1،2006.

2.عبد الرحمان خليفي،محاضرات في قانون اجراءات جزائية،دار الهدى،الجزائر2012.

3.العربي شحط عبد القادر نبيل صقر،الاثبات في المواد الجزائية،دارالهدى،الجزائر ،2006.

4.علي بن هادية،بلحسن البليش،الجيلالي بن الحاج يحيى،القاموس الجديد للطلاب،الشكة الوطنية،الشركة التونسية،الجزائر ،تونس،ط$_1$،1979.

5.محمد خريط،قاضي التحقيق في النظام القضائي الجزائري،دار هومة،الجزائر ،ط$_2$،2009.

6.محمد خريط،مذكرات في قانون الاجراءات الجزائية الجزائري،دار هومة،الجزائر ،ط$_3$،2008.

7.محمد علي سكيكر،الية المسؤولية الجنائية،دار الفكر الجامعي،الاسكندرية،ط$_1$،2008.

8.مروك نصر الدين،محاضرات في الاثبات الجنائي،دار هومة،الجزائر ،ج$_1$،2003.

- **الكتب الخاصة:**

1.خالد عياه الحلبي،اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيت،دار الثقافة،الاردن،ط$_1$،2011.

2.خالد ممدوح ابراهيم،فن التحقيق الجنائي في الجرائم الالكترونية،دار الفكر الجامعي،الاسكندرية،ط$_1$،2009.

3.عبد الفتاح بيومي حجازي،مكافحة جرائم الانترنيت،دار الفكر الجامعي،الاسكندرية،ط$_1$،2006.

4.عبد الناصر محمد محمود فرغلي،محمد سيف سعيد المسماري،الاثبات الجنائي بالادلة الرقمية من الناحيتين القانونية و الفنية،جامعة نايف العربية للعلوم الامنية،الرياض،2007.

5.محمد الامين البشيري،التحقيق في الجرائم المستحدثة،جامعة نايف العربية للعلوم الامنية،الرياض،ط1،2004.

6.نبيلة هبة هروال،الجوانب الاجرائية لجرائم الانترنيت،دار الفكر الجامعي،الاسكندرية،ط1،2007.

7.نهلا عبد القادر المومني،الجرائم المعلوماتية،دار الثقافة،الاردن،ط1،2008.

1.احسن بوسقيعة،قانون العقوبات في ضوء الممارسة القضائية،ط2،الديوان الوطني للاشغال التربوية،الجزائر.

2.جلال محمد العربي،اسامة احمد المناعسة،جرائم تقنية نظم المعلومات الالكترونية،دراسة مقارنة،دار الثقافة للنشر و التوزيع،ط1،الاردن،2010.

3.حسين محمد الشبلي،مهند فايز الديوكات،تزوير و احتيالبالبطاقات الائتمانية،ط1،دار مجدلاوي،للنشر و التوزيع،عمان2009.

4.رياض فتح الله بصلة،جرائم بطاقة الائتمان،ط1،دار الشروق،بيروت،لبنان،1995.

5.عبد الحكيم احمد عثمان،احكام البطاقات الائتمانية في القانون و الاراء الفقهية الاسلامية،ط1،دار الفكر الجامعي،الاسكندرية،2007.

6.عمر حسن المومني،الموقع الالكتروني و قانون التجارة الالكترونية،ط1،دار وائل للنشر و التوزيع،لبنان2003.

7.فداء يمي احمد الحمود،النظام القانوني لبطاقة الائتمان،دار الثقافة للنشر و التوزيع،ط1،الاردن،1999.

8.ماد احمد الجميل،الحماية الجزائرية لبطاقات الوفاء،دراسة تكميلية مقارنة،دار وائل للنشر،الاردن.

9.نائلة عادل محمد فريد قورة،جرائم الحاسب الالي الاقتصادي،دراسة نظرية تطبيقية،ط1،دار المنشورات الحلبي،لبنان،2005.

10. هلالي عبد الله احمد،تزوير بطاقة الائتمان صورة خاصة من جريمة التزوير،اتفاقية بوداست لمكافحة جرائم المعلوماتية دار النهضة،ط1،جامعة باتنة،الجزائر.

- **المذكرات والاطروحات**

1.اطروحة الدكتوراه،براهمي حنان،جريمة تزوير الوثيقة الرسمية الادارية ذات الطبعة المعلوماتية،اطروحة مقدمة لنيل شهادة دكتوراه،كلية الحقوق و العلوم السياسية،جامعة بسكرة،الجزائر.

2.بلال بن جامع،المشكلات الاخلاقية و القانونية المثارة حول شبكة الانترنيت ماجستير في علم المكتبات تخصص اعلام علمي،جامعة مختوري،قسنطينة،2006.

3.خشبة حسيبة،وسائل الدفع الحديثة في القانون الجزائري،مذكرة مكملة لنيل شهادة الماجستير في الحقوق،ين صغير محفوظ،قسم الحقوق،كلية الحقوق و العلوم الساسية،جامعة محمد بوضياف،المسيلة،2016.

4.خولة بوقديرة،الجرائم الواقعة على بطاقات الدفع الالكتروني،مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للاعمال،كلية الحقوق و العلوم السياسية،جامعة العربي بن مهيدي،ام البواقي،2018،207.

5.صوفية معروف،جرائم بطاقة الائتمان الالكترونية،مذكرة تكميلية لنيل شهادة الماستر،تخصص قانوني جنائي للاعمال،كلية الحقوق و العلوم السياسية،قسم الحقوق،جامعة العربي بن مهيدي،ام البواقي،2014،2019.

- **المقالات:**

1.زيـن الـدين محمـد الزمـاني،التزوير و التزييـف،عن طريـق بطاقـات الائتمان،مجلـة المحامي،العدد3،الرياض،1421

2. سامية عديد،الحماية الجنائية لبطاقات الدفع من جرائم التزوير في القانون الجنائي الجزائري،مجلة دراسات،العدد57،الاغواط،الجزائر

3. علـي عـدنان الفيل،المسـؤولية الجزائيـة عـن سـوء اسـاءة اسـتخدام بطاقـة الائتمـان الالكترونية،دراسة مقارنة،مجلة الحقوق،العدد3،الكويت2013.

4. .مريم تومي،صـدراتي وفـاء،تزوير بطاقـة الائتمان،صـورة خاصـة مـن جريمـة التـزوي الالكتروني،جامعة عباس لغرور،خنشلة،المجلد الخامس،العدد الثاني،سنة2013.

5. .نقضـي عبـد العزيز،جريمـة التزويـر فـي بطاقـة الائتمـان،مخبر السياسـة العامـة و تحسين الخدمة العمومية في الجزائر،جامعة الوادي

- **المواقع الالكترونية:**

1. Judiciere@gendarmeridefende.gouv.fr، 05/12/2023 22H30MIN.،

ملاحق

وثيقة 1

CIB / 755

Algérie Poste بـــريد الجزائـر

DEMANDE DE RÉEXPEDITION D'UNE CARTE MONÉTIQUE EDAHABIA

طلب إعادة إرسال بطاقة نقديّة "الذّهبيّة"

Bureau de poste de dépôt de la demande — **مكتب بريد إيداع الطلب**

(Bureau choisi par le demandeur pour la récupération de la carte monétique) (المكتب المختار من قبل صاحب الطلب لسحب البطاقة النقدية)

Nom du bureau de poste : .... : إسم مكتب البريد

Code Postal : ⎣ _ _ _ _ _ ⎦ : الرمز البريدي

Nom et Prénom du titulaire de la carte «EDAHABIA» : اسم ولقب صاحب البطاقة النقدية "الذهبية" :

N° CCP ⎣ _ _ _ _ _ _ _ _ _ _ ⎦ **Clé** ⎣ _ _ ⎦ رقم الحساب الجاري البريدي

N° téléphone mobile du titulaire de la carte : ⎣ _ _ ⎦ ⎣ _ _ _ _ _ _ _ _ ⎦ : رقم الهاتف النقال الخاص بالشخص الحائز على البطاقة

(Pour les clients n'ayant pas fourni leurs numéros de téléphone lors de la commande de la carte) (بالنسبة للزبائن الذين لم يقوموا بتسجيل أرقام هواتفهم لدى إيداعهم لطلب الحصول على البطاقة)

Bureau de poste détenteur de la carte « EDAHABIA » مكتب البريد الحائز على البطاقة "الذهبية"

(Information disponible sur le reçu de la commande via internet) (معلومة متوفرة على وصل طلب البطاقة عبر الأنترنت)

المعلومات الخاصة بوثيقة إثبات الهوية الخاصة بصاحب الطلب **Description de la pièce d'identité du demandeur**	التاريخ وتوقيع صاحب الطلب **Date et Signature du demandeur**
N° (PC) ou (CNI) : .... : رقم (ر.س) أو (ب ت و) Délivré(e) par : .... : الصادرة من طرف Le : .... : بتاريخ Valable au : .... : صالحة إلى غاية	

Apposer ici les Timbres poste représentant le montant du tarif de réexpédition توضع الطوابع البريدية التي تمثل قيمة تعريفة إعادة الإرسال

T.A.D

Date de dépôt

- -

RÉCÉPISSÉ DE LA DEMANDE DE RÉEXPÉDITION DE LA CARTE MONÉTIQUE « EDAHABIA »
(à détacher et à remettre au client)

وصل عن طلب إعادة إرسال البطاقة النقدية "الذهبية"
(يسلم للزبون)

Nom et Prénom du demandeur titulaire de la carte «EDAHABIA» اسم ولقب صاحب طلب البطاقة النقدية "الذهبية"

N° CCP ⎣ _ _ _ _ _ _ _ _ _ _ ⎦ **Clé** ⎣ _ _ ⎦ رقم الحساب الجاري البريدي

Bureau de poste de remise : .... : مكتب بريد التسليم

T.A.D

Date de dépôt

La carte ne peut être remise qu'au titulaire ou à un mandataire dûment mandaté. لا يتم تسليم البطاقة إلا لصاحبها، أو لموكل عنه يحمل وكالة رسمية

وثيقة 2

الفهرس

الملخص

الجرائم الالكترونية التي تمس البطاقات المصرفية متعددة من بينها جريمة التزوير الالكتروني و التي اصبحت منتشرة في عصرنا هذا ، و هذا ما الزم بعض التشريعات التدخل مباشرة كالتشريع الفرنسي و التشريع الجزائري .

حيث تتميز اجراءات التحقيق في هذه الجريمة بالسرية و الخصوصية على غرار الاجراءات الخاصة بالجرائم التقليدية .

الكلمات المفتاحية : البطاقات المصرفية ، بطاقات الائتمان ، اجراءات التحقيق الجزائية ، الجرائم الالكترونية ، جريمة التزوير الالكتروني .

Abstract

Electronic crimes that concern bank cards are multiple. Nowadays, the crime of electronic fraud has become widespread. Hence, some legislative systems such as French legislation and Algerian legislation intervene to reduce it.

The investigation procedures for this crime are characterized by confidentiality and privacy, as in the procedures for conventional crimes.

Key words: Bank cards, credit cards, criminal investigation procedures, electronic crimes, electronic fraud crime.