مداخلة بعنوان: الجرائم المعلوماتية في مجال الدفع الالكتروني

1–د. ليلى بعتاش

استاذ محاضر أ

جامعة الأمير عبد القادر

2–شيبي منال

طالبة دكتوراه جامعة الأمير عبد القادر

ملخص الدراسة:

تهدف هذه الدراسة الى معالجة موضوع ذو أهمية على الصعيدين التشريعي والعملي، ألا وهو الجرائم المعلوماتية في مجال الدفع الالكتروني. حيث تم تسليط الضوء على الجريمة المعلوماتية من خلال الإحاطة بالإطار المفاهيمي لها خصوصا في ظل غياب نصوص تشريعية صريحة، حيث أرتبط وجودها بظهور تكنولوجيا المعلومات والحاسبات الالية والتي تتصنف من بين الجرائم الخطيرة نظرا لما لها من أثار سلبية على المستوى الاقتصادي والاجتماعي بشكل عام والحقوق والمصالح ذات الطابع المالي المتعلقة بالمؤسسات المالية والمصرفية بشكل خاص.

الكلمات المفتاحية: جريمة معلوماتية، الدفع الالكتروني، بطاقة الائتمان

Abstract

This study aims to address a topic of importance on both the legislative and practical levels. "Information crimes in the field of electronic payment" The information crime was shed light on the conceptual framework of it, especially in the absence of explicit legislative texts. Its existence has been linked to the emergence of information technology and computers, which are among the serious crimes. In view of its negative effects on the economic and social level in general, and the rights and interests of a financial nature related to financial and banking institutions in particular.

Key words : information crime, electronic payment, Credit card

مقدمة:

شهد العصر الحديث ثورة تكنولوجية مست جميع مناحي الحياة، ولم تكن المعاملات المالية في منأى عن ذلك بحيث أفرزت هذه التغيرات نوع جديد من التعاملات يعرف بالتعاملات الإلكترونية، أين تتم مختلف عمليات السحب أو الوفاء بطريقة إلكترونية عن طريق الدفع الإلكتروني، وبقدر ما سهلت هذه التطورات إجراء مختلف المعاملات المالية إلا أنها لم تمنع من ظهور اعتداءات عديدة جراء الاستخدام غير الشرعي لهذه البطاقة الإلكترونية.

أصبحت الجزائر اليوم تتوفر على العديد من بطاقات الدفع الإلكترونية، التي تستعمل في الدفع والسحب على رأسها البطاقة الذهبية لبريد الجزائر، بالإضافة إلى الدفع الخاص بالمصارف المحلية، وكمثال على ذلك: القرض الشعبي الجزائري، وبنك الفلاحة والتنمية الريفية، والصندوق الوطني للتوفير والاحتياط، والبنك الخارجي، وبنك البركة، وبطاقات الدفع العالمية كبطاقة "فيز كارد"، وبطاقة "ماستر كارد"، والسماح للبنوك الخارجية ذات السمعة العالمية والتي تعمل بنظام الدفع الإلكتروني بنسبة كبيرة في معاملاتها.

وبالرغم من المزايا العديدة التي تقدمها هذه البطاقة للمتعاملين بها إلا أن ذلك صاحبه الكثير من السلبيات التي أثرت على المعاملات المالية والمصرفية، حيث أصبحت هذه البطاقات محلا للعديد من الجرائم من طرف أشخاص تتوفر لديهم الخبرة في المجال المعلوماتي ما جعلهم يحترفون هذا النوع من الأعمال الإجرامية، وهو ما انعكس سلبا على مصداقية هذه البطاقات والجهات المصدرة لها والأطراف المتعاملين بها، ومن ثم كان لابد من تطوير التشريعات على الصعيد الوطني بما يتلاءم وخصوصية هذا النوع من الجرائم، إضافة إلى تكثيف جهود التعاون على الصعيد الدولي نظرا لطبيعة هذه الجرائم العابرة للحدود.

إشكالية الدراسة:

ماهي الجرائم الواقعة على بطاقات الدفع الالكتروني؟

ولمعالجة هذه الدراسة تم اعتماد المنهج الوصفي وهذا لوصف الاعتداءات الواقعة على بطاقات الدفع الإلكتروني، وعرضها عرضا منهجيا وبأسلوب علمي وقانوني بحت، وعلى المنهج التحليلي لارتباطه الدراسات القانونية.

تساؤلات الدراسة:

- ما تعريف الجريمة المعلوماتية؟
- ماهي الاعتداءات الواقعة على بطاقات الدفع سواء من طرف حاملها أو الغير؟

أهداف الدراسة:

يهدف هذا البحث إلى الإلمام بجميع الجرائم الواقعة على بطاقات الدفع الالكتروني، والوقوف على العقوبات التي أقرها المشرع الجزائري لهذه الجرائم.

أهمية الدراسة:

تبرز أهمية دراسة هذا الموضوع في كونه موضوعا يتسم بالحداثة والمعاصرة، حيث نسلط الضوء على واحدة من أهم جرائم هذا العصر في مجال المعاملات المصرفية الإلكترونية، والتي تتم بطريقة تقنية غير المعهودة، وهي في تزايد مستمر ومذهل.

الدراسات السابقة:

الدراسات السابقة التي تناولت هذا الموضوع هي:

– دراسة معنونة ب: " آليات البحث والتحقيق في الجرائم المعلوماتية ": وهي أطروحة مقدمة لنيل شهادة الدكتوراه في القانون ، ربيعي حسين، نوقشت بجامعة باتنة، كلية الحقوق والعلوم السياسية، سنة2016 .

– دراسة معنونة ب: " وسائل الدفع الحديثة في القانون الجزائري ": وهي أطروحة مقدمة لنيل شهادة الماجستير في القانون ، خشة حسيبة، نوقشت بجامعة محمد بوضياف المسيلة، كلية الحقوق والعلوم السياسية، سنة 2016.

ومن أجل الإجابة عن هذه الإشكالية وتساؤلاتها الفرعية قسمنا بحثنا الى مبحثين أساسين، حيث عرفنا في المبحث الأول الجريمة المعلوماتية، وبيننا خصائصها ، أما في المبحث الثاني فقد بيننا الجرائم والتجاوزات التي تقع على بطاقات الدفع الالكتروني وعواقبها

نتيجة التطور في مجال الاتصالات والمعلومات اتسع نطاق استخدام تقنية المعلومات في المجتمع، نظرا لدورها في تيسير كافة أموره، والتي نتج عنها ظهور الجرائم المعلوماتية. وللاهتمام البالغ بالاعتداءات التي تنهب على المجال المعلوماتي، نبين أنواع الجرائم المعلوماتية في مجال الدفع الإلكتروني.

المبحث الأول: تعريف الجريمة المعلوماتية وخصائصها

تباينت التعريفات الفقهية للجريمة المعلوماتية، باعتبارها صنف جديد من الجرائم، حيث تتميز بمجموعة من الخصائص والصفات.

المطلب الأول – تعريف الجريمة المعلوماتية

تعددت التعريفات الفقهية للجريمة المعلوماتية بين موسع ومضيق للمفهوم

الفرع الأول: الاتجاه الذي يضيق من مفهوم الجريمة المعلوماتية

يعرف أنصار هذا الاتجاه الجريمة المعلوماتية، بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لاز ما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخر.[1]

طبقا لهذا التعريف يجب أن تتوفر معرفة تكنولوجيا الحاسبات الآلية بدرجة كبيرة ليس فقط من أجل ارتكاب الجريمة، ولكن أيضا من أجل التمكن من ملاحقتها، أي أن يكون مرتكب الجريمة والقائمون على ملاحقتها على درجة كبيرة من العلم بهذه التكنولوجيا.[2]

كما عرفها الفقيه merwe بأنها ": فعل غير مشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هو الفعل الإجرامي الذي يستخدم في ارتكابه الحاسب الآلي كأداة رئيسية،" فيما عرفه الفقيه " ROSBLATبأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى ٍ المعلومات المخزنة داخل الحاسب الآلي والى تحويل طريقه[3]" .

الفرع الثاني: الاتجاه الذي يوسع من مفهوم الجريمة المعلوماتية:

يرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأن الجريمة المعلوماتية:"كل سلوك إجرامي يتم بمساعدة الكمبيو تر، أو كل جريمة تتم في محيط أجهزة الكمبيوتر ." بينما يرى جانب آخر من الفقه بأنها ": عمل أو امتناع يأتيه الإنسان اضرار بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب أو " هي كل سلوك إجرامي يتم بمساعدة الحاسب الآلي فهي كل جريمة تتم في محيط الحاسبات الآلية[4]".

---

[1] نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، دراسة نظرية تطبيقية، الطبعة الأولى، لبنان، دار المنشورات الحلبي، 2005، ص 28.

[2] نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، المرجع انفسه، ص29.

[3] الفقيه Merwe ، RosBlatمشار له لدى: عبد العال الديربي، محمد صادق اسماعيل، **الجرائم الالكترونية**، الطبعة الأولى، القاهرة، المركز القومي للإصدارات القانونية، 2012 ، ص 4.

[4] محمد حماد مرهج الهيتي، **التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004 .، ص41.

ومن التعريفات السابقة نجد أن الجريمة المعلوماتية تستهدف في جوهرها المعلومات من بيانات ومعلومات وبرامج تطبيقية، وتقوم هذه الجريمة على اعتبارين مهمين أولهما أن تكون المعلوماتية وسيلة للغش والتحايل والاعتداء، والثاني أن تكون المعلوماتية نفسها محلا للاعتداء.[5]

المطلب الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بخصائص تميزها عن الجريمة التقليدية ولعل أهمها ما يلي

الفرع الأول: الجريمة المعلوماتية جريمة عابرة للحدود:

الجريمة المعلوماتية تتسم غالبا بالطابع الدولي، فهي لا تعترف بالحدود الإقليمية للدول باعتبار ساحتها العالم أجمع، وذلك لارتباط هذا العالم بشبكة واحدة. فأغلب الجرائم المرتكبة عبر شبكة الإنترنيت يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى، حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة.[6]

الفرع الثاني: صعوبة إثبات الجريمة المعلوماتية:

ترجع الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الأخيرة لأي أثر خارجي بصورة مرئية. فالجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها. ويضاف إلى ذلك صعوبة الاحتفاظ الفني بالدليل، الحاجة إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، بالإضافة إلى اعتمادها على الخداع والتضليل والذكاء في ارتكابها.[7]

الفرع الثالث: أسلوب ارتكاب الجريمة المعلوماتية:

تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم السرقة والإرهاب، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم هادئة بطبيعتها، لا تتطلب عنفا فكل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب.

الفرع الرابع: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص:

تتميز الجريمة المعلوماتية بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها أضرار بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود، شخص متخصص في تقنيات الحاسوب والإنترنيت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خار ج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه[8].

---

[5] إيهاب فوزي السقا، **الحماية الجنائية والأمنية لبطاقات الائتمان**، دار الجامعة الجديد، مصر، دون طبعة، 2007، ص 116

[6] محمد حماد مرهج الهيتي، **التكنولوجيا الحديثة والقانون الجنائي في مكافحة الجريمة المعلوماتية**، المرجع السابق، ص 5.

[7] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، الطبعة الأولى، دار الثقافة: عمان، 2008، 5ص 54.

[8] بيباراميل طوبيا، **بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها**، منشورات حلبي الحقوقية، دون طبعة، 2000، ص 56.

الفرع الخامس: لا تترك أثرا لها بعد ارتكابها:

فهذه الجرائم لا تترك أثرا، إذ ليست هناك أموال ومجوهرات إنما هي أرقام تتغير في السجلات مفقودة، ولذا فإن معظم جرائم الإنترنيت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها علاوة على صعوبة الاحتفاظ الفني بآثارها أن وجدت .

الفرع السادس: خصوصية مجرمي المعلوماتية:

يتمتع المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر الذي يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال التكنولوجي. وهذا ما يتميز به عن المجرم الذي يقترف الجرائم التقليدية[9].

المبحث الثاني: أنواع الجرائم المعلوماتية في مجال الدفع الإلكتروني

إن الدفع الإلكتروني الذي يتم بالوسائل الإلكترونية، كالحواسيب وعبر شبكات الاتصال المفتوحة على كافة المتعاملين والمستخدمين لها، أدى إلى ظهور العديد من الجرائم، كالالتقاط غير المشر وع للبيانات، وانتحال شخصية المتعامل الشرعي بالبيانات.

المطلب الأول: الالتقاط غير المشروع للبيانات.

يعد الالتقاط غير المشروع للبيانات دخول غير مشروع إلى نظام معلوماتي معين كالنظام الخاص بالبنوك أو البائعين بحيث يتمكن المجرم المعلوماتي من التقاط البيانات الشخصية للمتعاملين عبر قنوات الاتصال بعد ذلك، عن طريق التجسس المعلوماتي أو عن طريق الاحتيال فأسلوب التجسس المعلوماتي مثلا يتمثل في قيام قراصنة الإنترنيت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الإنترنيت كالمؤسسات والشركات التجارية ومن ثم استخدام هذه البيانات والمعلومات في ممارسة الأنشطة الجنائية ويمكن أن تكون معلومات سرية تجارية اقتصادية.[10]

فأسلوب التجسس المعلوماتي مثلا يتمثل في قيام قراصنة الإنترنيت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الإنترنيت كالمؤسسات والشركات التجارية ومن ثم استخدام هذه البيانات والمعلومات في ممارسة الأنشطة الجنائية ويمكن أن تكون معلومات سرية تجارية اقتصادية.[11]

---

[9] جعفر حسين جاسم الطائي، **جرائم تكنولوجية المعلوماتية رؤية جديدة للجريمة الحديثة**، الطبعة الأولى، دار البداية للنشر والتوزيع، عمان، 2010 ، ص 58.

[10] محمد أمين أحمد الشوابكة، **جرائم الحاسوب والإنترنيت**، الطبعة الأولى، دار الثقافة للنشر، الأردن، 2004 ص 166.

[11] محمد أمين أحمد الشوابكة، **جرائم الحاسوب والإنترنيت**، المرجع نفسه، ص 167.

المطلب الثاني: انتحال شخصية المتعامل الشرعي بالبيانات :

يسميها البعض جريمة الألفية الجديدة في أمن المعلومات وذلك نظرا لسرعة انتشار وارتكابها، خاصة في الأوساط التجارية .وتتمثل هذه الجريمة في استخدام هوية شخصية أخرى، بطريقة غير شرعية وتهدف إما لغرض الاستفادة من مكانة تلك الهوية أي هوية الضحية أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى.[12]

فهذه الجريمة تتمثل في قيام شخص باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو أمواله أو صلاحياته، عن طريق المعلومات، التي يحصل عليها من الإنترنيت، ويمكن أن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في البنك أو السحب من البطاقات الائتمانية ...وكثيرا ما يقوم المجرم بتغيير العنوان البريدي للضحية إلى عنوانه كي يستقبل بنفسه الفواتير والمتطلبات.[13]

المطلب الثالث: صور الاستخدام غير المشروع لبطاقات الائتمان الإلكترونية

لقد تزايد حجم التعامل ببطاقة الائتمان الإلكترونية، نظرا لما تقدم هـ لحامليها من تسهيلات وخدمات مصرفية جليلة. إلا أنه وفي المقابل قد تم استخدامها بطريقة غير مشروعة، مما أدى إلى نمو في الجرائم التي ترتكب ضد الأموال، بالاعتداء على بطاقة الائتمان الإلكترونية من قبل حاملها أو من قبل الغير.

الفرع الأول: الاستخدام غير المشروع لبطاقة الائتمان الإلكترونية من قبل حاملها

على الرغم من المزايا التي تقدمها بطاقة الائتمان الإلكترونية، لمالكها إلا أنه لم يكتف بهذا القدر، بل ذهب يبحث عن طرق غير مشروعة، لاستخدامها والاستفادة منها، باستمراره في استعماله لها في غير الحدود المصرح له به رغم صلاحيتها، أو بعد انتهاء مدة صلاحيتها، واستخدامها بعد إلغائها، أو بادعاء فقدها أو سرقتها.

أولا – إساءة استخدام بطاقة الائتمان الإلكترونية بالنظر لمدة صلاحيتها :

قد يسيء الحامل الشرعي لبطاقة الائتمان الإلكترونية متى تعسف في استعماله لها خلال فترة صلاحيتها، أو بعد انتهاء صلاحيتها

– 1 . إساءة استخدام بطاقة الائتمان الإلكترونية خلال فترة صلاحيتها:

رغم أن بطاقة الائتمان صالحة للاستعمال وصحيحة، إلا أنه يتصور أن تستخدم بصورة غير مشروعة، من قبل حاملها أثناء فترة صلاحيتها إذا ما قام بالسحب من جهاز توزيع العملة رغم عدم وجود رصيد كاف، أو الحصول على بضائع أو خدمات تتعدى المبلغ الذي حدده البنك مصدر البطاقة[14].

---

[12] وائل أنور بندق، **موسوعة القانون الإلكتروني والتكنولوجيا الاتصالات**، دار المطبوعات الجامعية، الاسكندرية، دون طبعة، 2007. ص 16.

[13] محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي**، د ط، دار الجامعة الجديدة، 2007، ص 47.

[14] إلهام بن خليفة، **الحماية الجنائية للمحررات الإلكترونية من التزوير**، مذكرة لنيل درجة الدكتوراه فريدة مزياني، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016 ، ص. 32.

– 2إساءة استخدام بطاقة الائتمان الإلكترونية المنتهية الصلاحية:

بطاقة الائتمان دائما مؤقتة، حيث يتوجب على العامل إرجاعها بعد انتهاء هذه المدة. ولكن قد يتعمد الحامل إلى الاحتفاظ بها أو بعد انتهاء مدتها. فملكية البطاقة تعود إلى الجهة المصدرة لها، هذه الأخيرة تقدم للعميل البطاقة لاستخدامها وفق العقد المتفق عليه بين الطرفين، يلزم العميل بإعادتها عند الانتهاء مدة الإعارة، فإن تخلف الحامل عن تنفيذ هذا الالتزام وقام باستخدام البطاقة يكون بذلك قد ارتكب جريمة إساءة الائتمان.[15]

وهنا يجب توضيح حالتين

–أ استخدام بطاقة الائتمان المنتهية الصلاحية في الوفاء :

قد يستخدم الحامل بطاقته في الوفاء رغم انتهاء صلاحيتها إن هو نسي تجديدها، أو احتفظ بالبطاقة القديمة رغم تسليمه البطاقة الجديدة، وتعمد شراء السلع أو الخدمات بواسطتها حتى يحتج فيما بعد على الوفاء للمصدر بأنه لم يقم باستخدامها. كما أن الحامل قد يستخدم البطاقة المنتهية الصلاحية بصورة غير مشروعة، إذ هو اتفق مع التاجر على قبولها في الوفاء إضرارا بالمصدر.

ب – استخدام بطاقة الائتمان المنتهية الصلاحية في سحب النقود :

الأصل العام وطبقا لنظام البرمجة المستخدم في استخدام الحامل الشرعي لبطاقته المنتهية الصلاحية، أنه تقوم آلة بابتلاع تلك البطاقة أو رفضها، حيث يعد إشعارا من البنك للقيام بتجديد تلك البطاقة. إلا أنه وفي أحيان أخرى يقوم الجهاز بصرف القيمة التي طلبها العميل ويتم قيد المديونية عليه دون أن يعترض، لأنه لم يقصد الغش.[16]

ثانيا – إساءة استخدام بطاقة الائتمان الإلكترونية الملغاة:

قد يلغي البنك المصدر بطاقة العميل لأي سبب من الأسباب، مثل غلق الحساب، أو تغيير نظام التعامل، أو تغيير نوعية الخدمة التي تؤديها الخدمة، ومع ذلك فقد تظل البطاقة مع العميل وقد يستخدمها بعد إلغائها[17].

حيث يتمادى الحامل في استخدامها على الرغم من إلغائها، أما في سحب النقود، وأما في الوفاء بقيمة المشتريات والخدمات التي يحصل عليها

– 1 .استخدام بطاقة الائتمان الإلكترونية الملغاة في سحب النقود :

---

[15] نضال سليم برهم، **أحكام عقود التجارة الالكترونية**، الطبعة الثالثة، دار الثقافة، عمان، 2010، ص 155.

[16] عبد الكريم الردايدة، **الجرائم المستحدثة واستراتيجية مواجهتها**، طبعة الأولى، دار الحامل للنشر والتوزيع، عمان، ص 216.

[17] فتحي محمد أنور عزت، **جرائم العصر الحديث**، الطبعة الأولى، دار الفكر والقانون، القاهرة، 2010. ، ص 175.

إذا حاول الحامل لبطاقة الائتمان سحب نقود من جهاز التوزيع الأتوماتيكي رغم إلغاء البطاقة، فإن الآلة تقوم بابتلاع البطاقة أو عدم تنفيذ أم ر الحامل أي رفض تنفيذ أمر السحب. وهذا ما دفع جانب من الفقه إلى القول بأن سلوك الحامل على هذا النحو لا يشكل جريمة، إلا أن ذلك لا يمنع من توافر جريمة الشروع في السرقة. حيث أن الجاني بدأ في تنفيذ الجريمة والنتيجة الإجرامية لم تتحقق لسبب خارج عن إرادته مع توافر القصد لديه، بشرط عدم وجود رصيد.[18]

– 2استخدام بطاقة الائتمان الإلكترونية الملغاة في الوفاء :

يستعمل الحامل الشرعي البطاقة الائتمانية الممغنطة في الوفاء بثمن سلعة أو خدمة يحصل عليها من الغير، رغم سبق إلغائها من قبل البنك المصدر لها الأمر الذي يؤدي في النهاية إلى التزام البنك في مواجهة البائع أو مؤدي الخدمة بالوفاء لهذه المبالغ، طالما أن البائع أو مؤدي الخدمة لا يعلم أن البطاقة ملغاة، [19]والتكييف فعل استعمال البطاقة الملغاة على هذا في الوفاء ينبغي التفريق بين حالتين :

حالة امتناع الحامل عن رد البطاقة بعد طلبها من البنك :

أن العلاقة ما بين العميل والبنك هي علاقة تعاقدية، حيث تبقى بطاقة الائتمان ملكا لمصدرها، هذا الأخير الذي يعهد إلى العميل استعمالها بناء على العقد المبرم بينها، ويمثل استخدام العميل للبطاقة الائتمانية بعد إعلامه بسحب البطاقة وامتناعه عن ردها وهو ما يشكل اختلاسا تقوم به جريمة خيانة الأمانة.[20]

–حالة استعمال البطاقة الملغاة في الوفاء للتاجر:

أن استخدام الحامل للبطاقة الملغاة في الوفاء بقيمة السلع والخدمات فإذا لم ينصب إلى التاجر أي خطأ في شأن التأكد من صلاحية البطاقة للاستعمال، فإن البنك يلتزم بالوفاء بهذه المبالغ للتاجر، وتشكل هذه الواقعة جريمة احتيال لأن تقديم البطاقة الملغاة مع علم الحامل لذلك يعتبر طريقة احتيالية هدفها الإقناع بوجود ائتمان وهمي والحصول من البنك على المبالغ التي تسدد قيمة المشتريات والخدمات التي سلمها التاجر بالفعل للحامل.

ثالثا – استعمال الحامل للبطاقة بعد ادعاء فقدها أو سرقتها:

قد يدعي الحامل الشرعي للبطاقة بسرقتها أو فقدها، رغبة منه في تحقيق مكاسب مادية غير مشروعة فيقوم بإخطار البنك والسلطات المختصة بذلك، في حين تظل البطاقة في حوزته ويستمر في استخدامها قبل اتخاذ البنك الإجراءات اللازمة لوقف استعمالها أو حتى بعد

[18] فيصل بن عادل أبو خلف، **الحماية الجنائية لبطاقات الائتمان الالكترونية**، رسالة ماجستير، منشورة، جامعة نايف للعلوم الأمنية، 2007، ص 8.

[19] فيصل بن عادل أبو خلف، المرجع نفسه ، ص 80

[20] محمد أمين الشوابكة، **جرائم الحاسوب والأنترنت، جرائم المعلوماتية**، المرجع السابق، ص 197.

ذلك كاستغلاله عدم مراجعة التاجر رقم البطاقة ضمن قائمة البطاقات الملغية نتيجة فقدها أو سرقتها بسبب ادعائه استعجال أو لأن مظهره يوحي بالثقة فيتردد التاجر في القيام بتلك المراجعة.[21]

الفرع الثاني: الاستخدام غير المشروع لبطاقات الائتمان الإلكترونية من قبل الغير

لقد أدى الانتشار الواسع لاستخدام البطاقة الائتمانية إلى استغلالها من طرف الغير والتلاعب فيها من أجل استيلاء على أموال ليست أمواله في الأصل .يتجلى هذا الاستخدام غير المشروع إما بالسرقة أو بالتزوير، أو الاعتداء على نظام بطاقة الائتمان الإلكترونية من خلال شبكة الإنترنيت. وعليه سنحاول تحديد إساءة استعمال بطاقة الائتمان الإلكترونية التي ترتكب من قبل الغير

أولا – الاستخدام غير المشروع ببطاقة مفقودة أو مسروقة

من الاعتداءات التي تقع على البطاقة الائتمانية باعتبارها محل للحقوق مالية سرقة البطاقة عن طريق حاملها بصورة مباشرة، فالسارق سواء استعمل البطاقة أو لم يستعملها، فهو يعد ارتكب لجريمة السرقة لمجرد توافر أركان هذه الجريمة.[22]

أما في الولايات المتحدة الأمريكية فإنها اعتبرت كل من يتعمد القيام بالإدخال الخاطئ للبيانات الائتمانية إلى أجهزة الكمبيوتر المرتبطة بالشبكات الداخلية أو العالمية ومحاولة التلاعب وتركيب الأرقام السرية لكشف حسابات صحيحة هي أفعال مجرمة تحت تشريع احتيال بطاقات الائتمان (3(الفدرالي) CCFA) وبواسطة تشريعات الولايات المتحدة [23].

ويذكر أن الحامل الشرعي لبطاقة ائتمان ممغنطة يفقد صفته كحامل شرعي لهذه البطاقة منذ إبلاغ بسرقتها أو فقدها، وبالتالي المعارضة فيها لدى البنك المصدر لها. ولذلك فهو يعد من الغير بالنسبة لها في حالة إساءة استعمالها ومن ناحية أخرى فإن التاجر قد يرتكب غشا بقبول البطاقة المسروقة أو المفقودة في الوفاء، وذلك بالتواطؤ مع الجاني، حيث يقوم التاجر بعمل فواتير وهمية لا تقابلها مشتريات حقيقية مستخدما في ذلك الطباعة اليدوية[24].

1–الإستعمال غير المشروع لبطاقة مسروقة أو مفقودة لسحب النقود:

لا يمكن استعمال بطاقة مسروقة أو مفقودة لسحب النقود من أجهزة السحب الآلي بدون إدخال الرقم السري أو الشفرة الخاصة بها، فبدون إدخال الرقم الصحيح لا يمكن لعملية السحب أن تتم بل أن إدخال رقم غير صحيح ثلاث مرات متتابعة من شأنه سحب

[21] مجدي محمود شهاب، فتوح الشاذلي، **التعاقد الإلكتروني عبر الأنترانت**، المرجع نفسه، ص 39.

[22] عبد الكريم الردايدة، **الجرائم المستحدثة واستراتيجية مواجهتها**، المرجع السابق، ص 216 .

[23] محمد أمين الشوابكة، **جرائم الحاسوب والأنترنت، جرائم المعلوماتية**، المرجع السابق، ص 20

[24] عبد الفتاح بيومي حجازي، **النظام القانوني للتجارة الالكترونية**، الطبعة الأولى، دار الفكر الجامعي: الاسكندرية، 2002، ص 336.

البطاقة بواسطة الآلة. وتتعدد الوسائل التي يستطيع بها الجناة بمعرفة الشفرة الخاصة بالبطاقة من أجل القيام بسحب النقود من جهاز الصرف ويكون ذلك إما باللجوء إلى سرقة الشفرة أو استعمال طرق احتيالية.[25]

– 2الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة كأداة وفاء:

يتم استعمال بطاقة في هذه الحالة للوفاء بواسطتها لدى التجار حيث لا يقتضي الأمر معرفة الرقم السري للبطاقة بل تتم المعاملة بتوقيع حامل البطاقة على فاتورة البيع.[26]

ويساهم في تسهيل استعمال البطاقة على نحو كبير صعوبة تحقق التاجر من شخصية حامل البطاقة كما أن التحقق من أن البطاقة قد تم إيقافها لا يتحقق إلا بعد إطلاع على القائمة السوداء التي تحتوي على بيان للبطاقات الموقوفة والتي قد لا تكون البطاقة قد أدرجت بها ومن ناحية أخرى فإن مضاهاة التوقيع المدون على البطاقة بذلك الذي على فاتورة البيع لا يمكن من الناحية العملية اكتشاف تزويره لتدرب الجاني عليه ومن ناحية عدم خبرة البائع في هذا المجال.[27]

ثانيا – تزوير البطاقة من قبل الغير :

في بعض الأحيان تفقد البطاقة أو تسرق من العميل، ويلتقطها الغير حيث يقوم باستبدال ما بها من بيانات ومعلومات تمهيدا لاستخدامها في السحب أو الشراء وبذلك يشكل هذا الفعل اعتداء مزدوج على الحامل الذي فقدت منه البطاقة وعلى البنك معا، الأمر الذي عده جمهور الفقهاء جريمة تزوير.[28]

على أساس أن التزوير هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي .إلا أن لهذا التزوير أساليب تستعمل على بطاقة الائتمان مباشرة أو على المستندات والاستعارات الخاصة بها[29]

– 1أساليب تزوير بطاقات الائتمان الإلكترونية– :

أ التزوير الكلي لبطاقات الائتمان:

---

[25] محمود ابراهيم غازي، **الحماية الجنائية للخصوصية والتجارة الإلكترونية**، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2010، ص 540.

[26] ضياء علي أحمد نعمان، **الغش المعلوماتي الظاهرة والتطبيقات**، الطبعة الأولى، المطبعة والوراقة الوطنية: مراكش، 2011، ص 157

[27] نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية** ، المرجع السابق، ص 540.

[28] عبد الكريم الردايدة، **الجرائم المستحدثة واستراتيجية مواجهتها**، المرجع السابق، ص216.

[29] نضال سليم برهم، المرجع السابق، ص 158.

إن خطوات التزوير الكلي لبطاقة الدفع الإلكتروني، تتم بداية باصطناع البطاقة كاملة ثم تقليد الرسوم الخاصة على جسم البطاقة وتغليفها، ولصق الهولجرام، والشريط الممغنط أو الشريحة الرقائقية وشريط التوقيع، كل حسب موقعه الأصلي على جسم البطاقة، والقيام بالطباعة النافرة وتشغيلها عن طريق تغذيتها بالمعلومات التي حصل عليها المزورون من البطاقة الصحيحة .ومن الظواهر الدالة على التزوير الكلي للبطاقة

- اختلاف مواصفات شكل وحجم البيانات المطبوعة طباعة بارزة بالبطاقة المصطنعة .
- عدم دقة لصق الشريط الممغنط وشريط التوقيع بظهر البطاقة حيث يمكن نزعها بسهولة
- خلو البطاقة المصطنعة من التأمينات غير المرئية والسرية المميزة لنظيرتها الصحيحة،
- خلو البطاقة من الخواص المميزة للطباعة المجهرية نتيجة للنقص في الإمكانيات في آلات التصوير التجارية التي يستخدمها المزورون.[30]

ب – التزوير الجزئي لبطاقات الائتمان:

يقوم المزور في هذه الحالة بالعديد من الأساليب لتزوير البطاقة جزئيا إما عن طريق صهر ما عليها من أرقام بارزة لبطاقة حقيقية انتهت صلاحيتها، أو إعادة قولبة رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر، تقليد الشريط الممغنط عن إعادة تشفيره بمعلوم طريق محو ما عليه من بيانات مسروقة، كشط شريط التوقيع ووضع شريط آخر يتضمن توقيعه، أو أن يقوم بخلع صورة حامل البطاقة الحقيقي وتثبيت صورة شخص آخر.[31]

ومن الظواهر الدالة على التزوير الجزئي للبطاقة:

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

–وجود تسلخات أو بقع مسودة في المواضع المحيطة بالكتابات النافرة أو عدم انتظام الرؤوس

البارزة للطباعة البارزة.

– الاختلاف في مواصفات التشكيل الطباعي لأرقام وحروف الطباعة البارزة.

– عدم التصاق حواف الصورة الجسمية ثلاثية الأبعاد.

[30] حسين محمد الشبلي، مهند فايز الدويكات، **التزوير والاحتيال بالبطاقات الائتمانية**، المرجع السابق، ص 66.

[31] أمجد حمدان الجهني، المرجع السابق، ص 162.

– عدم التطابق بين البيانات المشفرة على الشريط الممغنط والبيانات المقروءة بصريا.[32]

2 – تزوير الإشعارات والمستندات الخاصة ببطاقات الائتمان:

– أ **تزوير الإشعارات:** ويتمثل ذلك في عدة صور :

– تلاعب موظف البنك المصدر للبطاقة بإشعارات بطاقة الائتمان:

كأن يتفق الموظف مع التاجر بتجاوز حد السحب في صرف قيمة إشعارات البيع من بطاقة

مزورة أو منتهية الصلاحية، أو أن يختلس موظف البنك مبالغ نقدية عندما يقوم حامل البطاقة

بسحب أو الإيداع فيقوم بتزوير المبلغ ويأخذ الفارق لنفسه.

– تواطؤ حامل البطاقة مع التاجر: ويتم ذلك من خلال قيام حامل البطاقة بإجراء عمليات شراء وهمية بالإنفاق مع التاجر مقابل نسبة من قيمة الفاتورة يحصل عليها التاجر.

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

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

ب– إصدار بطاقات صحيحة بمستندات مزورة:

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

ثالثا – الاعتداء على نظام بطاقة الائتمان من خلال شبكة الإنترنيت:

تقوم عملية الدفع الإلكتروني من خلال شبكة الإنترنت، بعد أن يدخل العميل عن طريق تلك الشبكة التي تعرض منتجاتها، فيرغب في الشراء ويقوم بملء نموذج مطبوع على أعلى صفحة الويب تلك، ويدون به بيانات البطاقة وكمورد السلعة التي يرغب في شرائها والعنوان الذي ترسل إليه، ويسمى هذا النوع من الشراء التجارة الإلكترونية. إلا أنه في بعض الأحيان يحدث تلاعب من مستخدمي هذه الشبكة، أي قراصنة الإنترنيت .

[32] فايز نبيل عمر، **الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية**، د ط، دار الجامعة الجديدة الإسكندرية، 2012 .ص 66.

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

–**أسلوب الخداع:** عن طريق إنشاء مواقع وهمية على شبكة الإنترنيت، بحيث يظهر الموقع الاصطناعي وكأنه الموقع الأصلي لإحدى الشركات الكبرى، وتبدأ العملية بقيام الموقع الوهمي باستقبال تعاملات الموقع الأصلي، وبعد حصوله على الأموال يتم إغلاقه[33] .

– **أسلوب التجسس:** حيث يقوم قراصنة الإنترنيت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالشركات التجارية الكبرى للحصول على أرقام بطاقات الائتمان ويعاد استخدامها بطريقة غير مشروعة[34] .

– أسلوب تفجير الموقع المستهدف: بتزويد الحاسب بمعلومات فوق طاقته التخزينية، الأمر الذي يؤدي إلى تبعثر البيانات والمخزنة تنتقل إلى الجهاز الخاص بالفاعل، وترتكب هذه الطريقة الإجرامية على مواقع المؤسسات المالية والفنادق والشركات[35] .

– **أسلوب الإيهام:** هو أن يقوم القراصنة من أجل الحصول على بيانات ومعلومات للأشخاص مع أرقام بطاقاتهم الائتمانية، بإرسال رسائل إلى زبائن أحد المواقع الالكترونية، بحجة أن الموقع بحالة تحديث يرغبون بالحصول على كل المعلومات من أجل التحديث، وبعد ذلك يقوم المجرمون باستخدام تلك الأرقام في الشراء عبر شبكة الإنترنيت[36] .

---

[33] علي عدنان الفيل، **إجراءات التحقيق وجمع الأدلة والتحقيق في الجرائم المعلوماتية**، دراسة مقارنة، دون طبعة، المكتبة الجامعية الحديثة، الموصل، 2010، ص 245.

[34] –عبد الكريم الردايدة، **الجرائم المستحدثة واستراتيجية مواجهتها** ، المرجع السابق، ص . 70

[35] علي عدنان الفيل، **إجراءات التحقيق وجمع الأدلة والتحقيق في الجرائم المعلوماتية**، مرجع السابق، ص 245.

[36] عبد الكريم الردايدة، **الجرائم المستحدثة واستراتيجية مواجهتها**، المرجع السابق، ص 70.

خاتمة:

مما سبق فقد حولنا في هذه الدراسة تناول موضوعا حديثا يتمثل في الجرائم المعلوماتية في مجال الدفع الالكتروني، والذي يعد من الموضوعات التي فرضت نفسها بقوةً طبيعيا تولد عن التطور التكنولوجي والتقني خلال الفترة الحالية، لكونه يمثل إفرازا الذي يشهد قطاع المعاملات المصرفية والمالية.

حيث أن جرائم بطاقات الدفع الإلكتروني تدخل ضمن الجرائم المعلوماتية، وهي وليدة استخدام تقنية المعلومات حيث تتزايد بتزايد استخدام هذه التقنيات. فالمجرم الإلكتروني أخطر من المجرم التقليدي، لأنه صعب الاكتشاف ولا تبدو عليه ملامح الإجرام ويستغل ذكائه وخبرته التقنية لارتكاب هذه الجرائم. وتظهر صعوبة الكشف عن هذه الجرائم نظرا لطبيعتها غير المادية، وقابلية البيانات للحذف والإتلاف بسهولة لأنه يصل إليها من أي مكان بالعالم. عدم التبليغ عن هذه الجرائم من قبل المؤسسات المالية حفاظا على سمعتها ودوام ثقة عملائها.

الجزائر وعلى غرار بقية الدول حاولت جاهدة التنسيق والتعاون مع نظيراتها من الدول في سبيل مكافحة هذه الجرائم والحد منها وذلك بالانضمام والمصادقة على مختلف الاتفاقيات المتعلقة بهذه الجرائم. وسع المشرع بموجب القانون 09-04 الاختصاص الإقليمي للجهات القضائية في متابعة الجرائم الماسة بالمصالح الحساسة في الدولة، حيث عالج هذا القانون مشكلة تنازع الاختصاص بين الدول حول الجرائم التقنية نظرا لطبيعتها العابرة للحدود.

التوصيات:

- دعوة المشرع الجزائري الى تبين نظام بطاقات الائتمان الإلكترونية، مسايرة التطور التكنولوجي، تطوير البنوك الوطنية، بتقنيات التسيير وادارة الاعمال الحديثة من أجل مواكبة لمختلف أنظمة ِ والبطاقات الإلكترونية الموجودة على المستوى العالمي.
- تدريب أفراد الجهات الأمنية المختصة في مكافحة هذه الجرائم بشكل دائم مع ما يتماشى ومستجدات تقنيات هذه الجرائم، وتوفير أحدث الوسائل والتجهيزات التقنية لضمان تحقيق أفضل النتائج.

- تعزيز التعاون الدولي ودعوى إلى الانضمام الجزائر للاتفاقيات والمعاهدات الأخرى التي تسعى لمكافحة هذه النوع من الجرائم.

قائمة المراجع:

أ- الكتب:

- أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، الطبعة الثالثة، الديوان الوطني للأشغال التربوية، الجزائر، 2001.
- أحمد سفر، أنظمة الدفع الالكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008.
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى منشورات الحلبي الحقوقية، لبنان، 2012.
- – عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2013.
- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت – الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2006.
- – إلهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، مذكرة لنيل درجة الدكتوراه فريدة مزياني، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016.

ب- المقالات:

- سامية بولافة ومبروك الساسي، " الأساليب المستخدمة في التحريات الجزائية "، مجلة الباحث للدراسات الأكاديمية، العدد التاسع، جامعة باتنة ، 1 الجزائر، 01 جوان 2016.
- عبد الجبار الحنيص، "الاستخدام غير المشروع لبطاقات الائتمان الممغنطة في وجهة نظر القانون الجزائي"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، االمجلد26 ،العدد الأول، 2010.