ASJP Algerian Scientific Journal Platform

- دراسات اقتصادية -

ISSN 2602-7925

https://www.asjp.cerist.dz/en/PresentationRevue/417

المجلد: 17 العدد: 01(2023)

ص. 821-836

جريمة التلاعب في نظام المعالجة الآلية للمعطيات في قانون العقوبات الجزائري (بطاقة الدفع الالكترونية نموذجا)

The offense of falsification with the automated data processing system in the Algerian penal code (electronic payment card as a model)

نادية دردار

جامعة محمد الشريف مساعدية، سوق أهراس

dardarnadia24@gmail.comصسش

معلومات المقال

تاريخ الإرسال:
2022/11./24

تاريخ القبول:
2023/01/01

الكلمات المفتاحية:
- ✓ نظام المعالجة الآلية للمعطيات
- ✓ بطاقة الدفع الالكتروني
- ✓ الحماية الجزائية

الملخص

إن التسليم بوجود جريمة التلاعب تضر بالمعطيات المعالجة آليا يفترض وجود نظام معلوماتي كمحرك ومشغل له، مهما كانت الوسيلة المستخدمة في ذلك، سواء كان الحاسوب أو أي وسيط معلوماتي آخر.

و تعتبر بطاقة الدفع الإلكتروني من وسائل الدفع الإلكترونية، وهي وسيلة وفاء مستحدثة ذات تقنية تكنولوجية عالية، تتميز بسهولة التعامل بها، وكذا الحماية من مخاطر حمل النقود، ولكن قد تتعرض هذه البطاقة إلى الولوج والتلاعب بالنظام المعلوماتي الذي تعمل عليه، مما دفع بالمشرع الجزائي للتدخل بهدف حمايتها جزائيا.

Article info

Received
24/11/2022

Accepted
01/01/2023

Keywords:
- ✓ *Automated data processing system*
- ✓ *electronic payment card*:
- ✓ *Penal protection*:

Abstract :

Recognizing the existence of the offense of altering automatically processed data presupposes the existence of an information system as engine and operator, regardless of the means used, whether it is a computer or any other information medium.

The electronic payment card is considered one of the means of electronic payment, and it is an innovative high-tech payment method, characterized by its ease of use, as well as protection against the risks associated with the transport of money, but this card can be exposed to access and manipulation of the information system on which it operates, which prompted the criminal legislator to intervene in order to protect it criminally.

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

. مقدمة:

تعتمد نظم التحويلات المالية في الوقت الحالي على استخدام الحاسب الآلي وشبكات المعلومات وهو ما يشكل مخاطر جمة، منها إفشاء وتداول البيانات سواء بقصد أو دونه، وهو ما يسبب أضرار بالغة بالمال والأعمال، حيث أن الاستخدام غير القانوني للتكنولوجيا يؤدي إلى السرقة والاحتيال، وذلك بالتلاعب في البيانات المالية.

وقد استخدمت بطاقات الدفع الإلكتروني كوسيلة للدفع أو أداة للإبراء، ولم تعرف الجزائر بطاقة الدفع الإلكتروني إلا عام 1994 حين تم فتح بنوك خاصة، ولكنها لم تلقى رواجا كبيرا إلا بحلول سنة 2005 ، كما أن المشرع الجزائري لم يسن النصوص القانونية التي تواكب التطور التقني المستمر بالنسبة لإتمام الأعمال التجارية إلكترونيا إلا سنة 2003 ، فحاول إثراء المنظومة التشريعية بخصوص مجال التعامل التجاري الالكتروني وتحديث أنظمة الدفع المتاحة في ظله، وذلك بموجب الأمر رقم11 / 03 المتعلق بالنقد والقرض، وقد ترتب على صدور بطاقة الدفع الإلكتروني أثار إيجابية وأخرى سلبية، ومن أبرز الآثار السلبية هو الاعتداء على هذه البطاقة بالقيام بتصرفات غير مشروعة، وذلك بالولوج والتلاعب بالنظام الذي تعمل عليه، وبالتالي هذه البطاقة تحتاج إلى وسائل حماية فنية وأخرى قانونية، تعزز من وجود بيئة آمنة في عالم التجارة الإلكترونية (بركات، 2022، صفحة 328).

مما سبق نخلص إلى الإشكالية التالية: ماهي طبيعة وحدود فكرة النظام المعلوماتي بوصفه الأساس الذي تقوم عليه الحماية الجزائية للمعطيات الإلكترونية عامة ومنها مجموع الاعتداءات المكونة للتلاعب في بطاقة الدفع الإلكتروني خاصة؟

وللإجابة على هذه الإشكالية اعتمدنا المنهج الوصفي باعتباره الأنسب للموضوع نظرا لما يتيحه من آليات قصد الإحاطة بمختلف جوانب الموضوع، حيث يمكننا من بيان وتحديد موقف النصوص القانونية المختلفة من مسألة النظام المعلوماتي والجرائم التي ترتكب على نظام المعالجة الآلية لهذه المعطيات، والتطرق لبطاقة الدفع الإلكتروني ومحاولة إسقاط هذه الجرائم عليها باعتارها تتضمن نظام معلوماتي قابل لأن يكون محلا لارتكاب هذه الجرائم، الأمر الذي يسمح باستخراج جميع الأحكام، وكذلك معرفة أوجه النقص أو الخلل في التشريع الوطني واقتراح السبل الكفيلة بتلافيها، إلى جانب ذلك اعتمدنا المنهج التحليلي من خلال إخضاع نصوص المواد المتعلقة هذه الدراسة إلى عملية الشرح والتبسيط لمضمونها، والوقوف على المراد منها نصا وروحا، إضافة إلى سرد مجموعة من آراء الفقهاء حول نفس الموضوع.

وتتمثل أهمية الدراسة في الدور الكبير الذي تلعبه بطاقة الدفع الإلكتروني في مسايرة التطورات التكنولوجية والتي بدورها لها تأثير على التطورات المصرفية، وتسليط الضوء على أهم الاعتداءات التي يمكن أن تتعرض لها هذه البطاقة والمواجهة القانونية لها بوضع عقوبات رادعة لمرتكبي هذه الجرائم.

نهدف من خلال هذا البحث إلى تسليط الضوء على النظام المعلوماتي ومدى انطباق وصف نظام معلوماتي على بطاقة الدفع للوصول إلى أهم الجرائم الواقعة على بطاقة الدفع الإلكتروني، وإبراز تدخل قانون العقوبات الجزائري لردع جميع التجاوزات التي تمس بهذه البطاقة سلبا.

2. ماهية النظام المعلوماتي

1.2 مفهـــوم النظام المعلومـــاتي:

1.1.2 تعريفه:

تتعدد المفاهيم التي أعطيت للحاسب الآلي والذي يشمل كل مكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، إضافة إلى الوسائل التي يمكن بواسطتها تحقيق وظيفة أو هدف محدد، وقد عرفه البعض بأنه "مجموعة متداخلة من الأجزاء لديها هدف

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

مشترك من خلال أداء التعليمات المخزنة " أو " هو آلة حسابية إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة " (العريان، 2004، صفحة 56).

كما عرفها البعض بأنه " جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية طبقا للتعليمات المعطاة له بسرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، وبدرجة عالية الدقة، فله القدرة على التعامل ومعالجة كم هائل من البيانات، وكذلك تشغيلها، واسترجاعها عند الحاجة ". (الرومي، 2003، صفحة 13)

هناك تعريف آخر بأنه " نظام يتيح إدخال البيانات ومعالجتها وتخزينها واستخراجها ونقلها وتبادلها، وهو يشمل بالإضافة إلى نظام الحوسبة(الكمبيوتر) بمكوناته المادية والمعنوية ووسائل الاتصال التي تربط بين نظم الكمبيوتر المختلفة وقواعد البيانات فنتج عن دمجها شبكة المعلومات " (عرب، 28- 29 تشرين أول 2002، صفحة 2)

أمام تضارب المفاهيم، وعدم إشتمالها خصائص المعرف على نحو يحول دون إختلاط غيره به ، بحيث يكون شاملا لجميع الخصائص دون تداخل أوصاف أخرى به نأخذ بالتعريف الوارد بالموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، حيث عرفته بأنه " جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات أو إخراج معلومات وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج، أو التخزين والبيانات يتم إدخالها بواسطة مشغل الحاسب، عن طريق وحدات الإدخال، مثل وحدة المعالجة المركزية التي تقوم بإجراءات العمليات الحسابية، وكذلك العمليات المنطقية وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج مثل الطابعات أو وسائط التخزين المختلفة " (محمد سلامة، 2005).

2.1.2 مكونات النظام المعلوماتي:

يتكون أي نظام معلوماتي من مكونات مادية ومكونات معنوية أو منطقية، المكونات المادية يقصد بها المكونات الحسية التي يمكن لمسها ورؤيتها مثل الأجهزة المعدنية والبلاستيكية والأسلاك والزجاج وتقسم إلى أقسام ثلاث رئيسية هي: وحدة التشغيل وهي الجزء الرئيسي في الجهاز الحاسب فهي الذاكرة الرئيسية له تتكون من ذاكرة رئيسية ووحدة الحساب والمنطق، ووحدة التحكم (وحدة التشغيل الرئيسية)

كما يتكون من وحدات الإدخال والإخراج والتي تستخدم في إدخال البيانات والمعلومات إلى وحدة التشغيل المركزية أو إخراجها لاستخدامها بواسطة المستخدم، وذلك بتوجيه من وحدة التحكم، ثم أخيرا نجد وحدة التخزين ونجد أهمها وحدة الأقراص المرنة، وحدة الأقراص الصلبة، الشريط المغناطيسي، ووظيفتها تخزين البيانات المعالجة أليا وحفظها لاسترجاعها.

والمكونات المعنوية أو المنطقية تشمل البيانات والبرامج مثل النصوص والخرائط وغيرها من البيانات التي تتحول إلى معلومات وأما البرامج مثل برامج نظم التشغيل ونظم إدارة قواعد البيانات أو البرامج التطبيقية.

3.1.2 البرامـج:

هي فكر الحاسب الذي يوجه الوجهة التي يريدها، مما يقتضي القول أن الحاسب مجرد عامل أو منفذ غبي للأوامر التي يتضمنها برنامجه، ودونه تكون الحاسبات مجرد معدات وآلات صماء لا روح فيها، فالبرنامج يعمل على بث الروح فيها (محمد سلامة، 2005، صفحة 48).

والبرامج تعد من العناصر الأساسية للكيان المنطقي لأي حاسب، الأمر الذي دعى البعض إلى استعمال كل منهما بمعنى مرادف للأخر وعرفها البعض بأنها " الكيان المنطقي يشمل بالإضافة للبرامج، وصفها والوثيقة الاحتياطية " (الشوا، 1998، صفحة 625).

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

ولبرامج الحاسب مفهومان:

- مدلول ضيق: يقتصر على مجموعة التعليمات الموجهة من الإنسان إلى الآلة والتي تسمح لها بتنفيذ مهمة معينة (جدي، 2002،2003، صفحة 40،41).

- مدلول واسع: يشتمل بالإضافة إلى تعريف البرنامج وفقا لمدلوله الضيق، التعليمات والأوامر الموجهة إلى العميل مثل بيانات استعمال البرنامج، وكيفية المعالجة الإلكترونية للمعلومات، أي كافة البيانات الأخرى الملحقة بالبرنامج، والتي تساعد على سهولة فهم تطبيقه، وهي تعتبر بمثابة وصف تفصيلي له متضمنة مراحل تطبيقه، وهذه البيانات عبارة عن تعليمات موجهة من المبرمج الذي يتولى إعداد البرنامج إلى العميل الذي يتعامل مع الآلة، ولهذا عند فرض الحماية الجنائية للحاسب نأخذ بالمفهوم الواسع وذلك للأسباب التالية :

- من شأن الأخذ بالمدلول الواسع أن تمتد الحماية القانونية في حال وجودها في الحاضر والمستقبل إلى كافة التعليمات التي توجه إلى أية آلة أيا كان الاسم الذي يطلق عليها، طالما كانت قادرة على معالجة معلومات وبيانات أو غير ذلك، بغية تحقيق هدف محدد- تشمل الحماية القانونية بالإضافة إلى ما سبق التعليمات التي توجه إلى العميل أيا كان الشكل الذي تتخذه-.

- هذا المدلول يتفق مع التحديد الذي تبنته المنظمة العالمية للفكرية للبرامج بأنه "مجموعة من التعليمات التي تسمح بعد نقلها على دعامة مقروءة من قبل الآلة ببيان أداء أو انجاز وظيفة أو مهمة أو نتيجة معينة عن طريق آلة قادرة على معالجة البيانات " (الشاذلي و عفيفي، 2003، صفحة 26).

البرامج بهذا الوصف لا تعد من قبيل الأموال المادية إلا إذا احتوت في دعامة مادية مهما كان شكلها أو طبيعتها، ورغم هذا فإنها بوصفها مال معنوي منقول تحضى بالحماية القانونية في نصوص مختلفة (عرب، الملكية الفكرية للمصنفات الرقمية P-digital-work) منها قانون حماية حقوق المؤلف في الملكية الفكرية والفنية أو قانون العقوبات بموجب تعديلات 2004 اعترف له بصفة المال، وبالتالي أوجب لها نصوص تحميها من الغش والتلاعب.

4.1.2 الوثيـــــقة المعلوماتية:

هناك عدة تعاريف قدمت للوثيقة الرقمية منها:

* هي وثائق تنشأ وتعالج من خلال نظام حاسوبي وتحتاج لوسيط لقراءتها لاستعمالها منطق الوساطة.

وعرفها محمد أحمد الشامي بأنها أي مادة تحتوي بيانات أو برامج أو كليهما معا ويتم قراءتها والتعامل معها من خلال الحاسوب باستخدام وحدات خارجية متصلة بالحاسوب مباشرة مثل مشغل الأقراص المرنة والصلبة أو استخدام الشبكات مثل الانترنت ويشار إليها عادة بالمصطلح e- ressourse) شاشة(157 .p ,)

وعليه تعد البطاقة المغناطيسية وثيقة أو محرر معلوماتي بوصفها مجموعة بيانات مدونة بشكل كهرومغناطيسي في جسم منفصل عن النظام (البطاقة كدعامة) ، وهي معدة لاستخدام بواسطته، كذلك تعد وثيقة معلوماتية المعلومات المطبوعة بعد معالجتها آليا في جهاز الموزع الآلي، والتي تسلم للعميل في شكل وصل مخالصة بعد عملية السحب، كذلك الأمر نفسه بالنسبة للفواتير المعدة بواسطة القارئ الالكتروني لدى التاجر .

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

الأمر نفسه أيضا بالنسبة للتسجيلات في ذاكرة الموزع الآلي والتي تنقل فيما بعد على دعامات أخرى إلكترونية أو ورقية، وتعد البيانات بعد معالجتها وتخزينها في ذاكرة الحساب الآلي في البنك، والمتعلقة بقوائم اسمية للعملاء وأرقام الحسابات وحجم الأرصدة وحركتها من قبيل الوثائق المبرمجة أيضا.

2.2 طبيعة البيانات الإلكترونية والمعلومات المعالجة آليا

للبيانات مفاهيم عدة سيتلخص منها بأنها عبارة عن كلمات وأرقام ورموز وحقائق أو إحصاءات خام لا يوجد بينها صلات، وهي صالحة لتكوين فكر أو معرفة بمعرفة الإنسان أو الأدوات والأجهزة التي يسخرها الإنسان لذلك وهي ما تسمى بعملية المعالجة الآلية.

1.2.2 طبيـــعة البيانات:

البيانات هي مجموعة من الحقائق تعبر عن مواقف وأفعال معينة حدثت في الحاضر أو في الماضي أو ستحدث في المستقبل سواء كان التعبير بالكلمات أو الأشكال أو الرموز، والبيانات تشكل المادة الخام التي يتم تشغيلها للحصول على المعلومات، فالبيانات هي معلومات في حالة كمون والمعلومات هي بيانات في حالة تبلور (محمد شتا، 2001، صفحة 62)

غالبا ما يتم الخلط بين المفهومين وعدم الفصل بينهما، فإحداهما عادة ما تستخدم كمرادف للأخرى والبعض يقول بأن البيانات هي معطيات متصلة بجهة ما، والمعلومة هي المعنى المستخلص منها بعد معالجتها، فالبيانات هي المدخلات للحاسب الإلكتروني، وهي ذات طبيعة معنوية غير أنها غير قابلة للاستئثار أو السرية فليس لها قيمة، وبالتالي لا تخضع للحماية القانونية (محمد سلامة، 2005، الصفحات 44-45)، علاوة على أن البيانات قبل معالجتها هي عبارة عن دلالة ذهنية معنوية لا دعامة مادية تحويها، هي إذا لم تعالج أليا بواسطة حاسب آلي وبالتالي لا تعتبر من قبيل الأموال التي تحظى بالحماية .

2.2.2 المعلومات المعالجة آليـــــــا

هي تعبير يستهدف جعل رسالة معينة صادرة من شخص معين قابلة للتوصيل إلى شخص أخر وذلك بفضل علاقة أو إشارة من شأنها أن توصل المعلومة للغير، إذن هذا التعبير وكيفية توصيلة إلى الغير يحقق وظيفة المعلومة، وهي إمكانية نقل أو انتقال المعرفة (الرومي، 2003، صفحة 39) .

وإن تجميع المعلومات المعالجة يشكل قواعد البيانات التي عرفها د/يونس عرب بأنها " تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز، ويكون مخزنا بواسطة الحاسوب ويمكن استرجاعه أيضا " (عرب، الملكية الفكرية للمصنفات الرقمية P-digital-work)

حتى تكون المعلومات محل حماية يجب أن يتوفر فيها عنصر الإبتكار، لأن المعلومات الشائعة سهل الرجوع إليها من قبل الكافة، فلا تكون معلومة مبتكرة، كذلك لابد من أن تتوفر على عنصر السرية والاستئثار، ونقصد بها أن تكون المعلومة سرية بحيث يمثل أي اعتداء عليها فعل يستحق العقاب، ومثال ذلك البطاقة البنكية والمعلومة المسجلة إلكترونيا فيها، وكذلك قاعدة البيانات المرتبطة بها والتي تشمل أسماء العملاء وأرقام البطاقات والأرقام السرية والتوقيع الإلكتروني الشخصي وأرقام الحسابات الجارية وحركة الأرصدة، وطريقة الوصول إليها بواسطة البطاقة والرقم السري تشكل معلومات معالجة آليا وفق نظام معين يحظى بالسرية، لأنها تعتبر الأسرار البنكية والوصول إليها يضر البنك والعميل معا، كذلك لابد أن يكون هنالك استئثار بالمعلومة، والاستئثار يعني حيازة المعلومة من شخص بحيث يصبح هو المتصرف

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

الوحيد فيها (الرومي، 2003، صفحة 43) على المال الذي يريده فهي مال من جهة ومن جهة أخرى فهي أداة للوصول إلى النظام المعلوماتي للبنك والبقاء أو التلاعب فيه (بيومي حجازي، 2002، صفحة 122).

3. الولوج والتلاعب ببيانات بطاقة الدفع

بعد أن تعرفنا على ماهية النظام المعلوماتي وعناصره المادية والمعنوية أصبح من اليسير إضفاء وصف صحيح لبطاقة الدفع، على ضوء ذلك سوف نتطرق إلى مدى انطباق وصف نظام معلوماتي على البطاقات المصرفية، وتكييف فعل التلاعب والتعديل للبيانات.

1.3 مدى انطباق وصف نظام معلوماتي على بطاقة الدفع:

1.1.3 نظام معلوماتي مصغر أو وثيقة معلوماتية:

البطاقة المغناطيسية بوصفها أداة إلكترونية تحوي على ذاكرة عبارة عن شريحة –puce- أو شريط ممغنط مختزن فيه مجموعة بيانات متعلقة بالعميل، البنك، معالجة آليا، ويمكن استرجاعها في أية لحظة بجرد إدخال البطاقة أو وصلها بجهاز إلكتروني أخر – الموزع الآلي، القارئ الإلكتروني، حاسب آلي تعتبر بهذا الوصف نظام معلوماتي مصغر، وذلك على أساس أخذنا بمفهوم الموسع للنظام المعلوماتي، وهي تعد برنامج معلوماتي، والذي سبق أن قلنا عنه بأنه أساس ولب النظام المعلوماتي، حيث يمكن هذا البرنامج المخزن على دعامة البطاقة بأداء وانجاز وظيفة معينة متمثلة في إرسال أمر – رسالة معلومات- إلى الحاسب المركزي بواسطة وسيط الكتروني وهو هنا الموزع الآلي لتحويل مبالغ من حساب البنك إلى حساب العميل وتسليم هذا المبلغ المحول في تلك اللحظة للعميل، فالبطاقة يعطي بواسطتها العميل أمر للبنك عن طريق الآلة بتسليمه مال واقتطاع قيمة ما سحبه أو تم دفعه للتاجر من حساب العميل لدى البنك.

فإذا أخذنا بهذا الوصف أمكن القول بخضوع البطاقة- مستقلة عن الموزع أو الحاسوب – لنصوص التجريم الجديدة المتعلقة بالمساس بنظم المعالجة الآلية للبيانات الواردة في قانون العقوبات.

وإذا ما تم الأخذ بهذا المفهوم لتعريف النظام المعلوماتي أمكن اعتبار البطاقة المغناطيسية بمثابة وثيقة معلوماتية لأنها عبارة عن دعامة معلوماتية تم الحصول عليها بوسائل معلوماتية، أي تكون ناشئة عن جهاز إلكتروني أو كهرومغناطيسي أو طبع ممغنط، وتخزين مجموعة معلومات متعلقة بالعميل، البنك، وطرق تنفيذ المعاملة أعدت منفصلة عن النظام المعلوماتي، ولكن لا تعمل مستقلة عنه فلها دور في تشغيل النظام، وتنفيذ التعليمات، وهي بهذا كما يذهب بعض المختصين بالقول بأنها عبارة عن توقيع أو مفتاح إلكتروني دونه لا يعمل النظام.

2.1.3 البطاقة مفتاح أو تـــوقيع إلكتروني:

بوصفها دعامة إلكترونية ومنفصلة عن النظام المعلوماتي وتسمح بفتحه والدخول إليه وتشغيله اعتبر بعض الفقه البطاقة على أنها مفتاح بينما يعتبرها البعض الأخر توقيع إلكتروني يسمح بتحديد هوية مشغل النظام ومستغله ويستدل به على من قام بإجراءات المعاملة الإلكترونية.

1.2.1.3 البطاقة مفتاح إلكتروني

إن وصف البطاقة بأنها مفتاح الكتروني محل مناقشة وجدل لدى الفقه، بسبب طبيعة البطاقة الخاصة وطريقة أداءها لعملها، فحداثة التكنولوجيا المستخدمة فيها تصطدم مع المفاهيم التقليدية للأشياء في الفقه والقضاء (المناعسة و الزعبي، 2001، صفحة 174،175).

بالرغم من أن نصوص قانون العقوبات جاءت فضفاضة يمكن إعمالها على البطاقات بوصفها أداة إلكترونية للدخول للأنظمة المعلوماتية، خاصة وأن المعلوماتية أوجدت لنا نظم إغلاق وفتح الأماكن إلكترونيا، كأقفال السيارات، البنوك، والمنازل بواسطة شفرة أو كلمة سر على بطاقة إلكترونية.

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

البطاقة المغناطيسية المصرفية أداة تشغيل وإدارة النظام المعلوماتي للدفع الإلكتروني للنقود، ودونها لا يعمل النظام ويؤدي وظيفته بالطرق المشروعة، يمكن إعمال نص تقليد أو تزوير أو اصطناع مفتاح دون الخوف من الاصطدام بمبدأ الشرعية، وذالك بأخذنا بالمفهوم الموسع للنص، ولا نكون هنا بصدد القياس، أو على المشرع التدخل بوضع نصوص خاصة على غرار المشرع الأجنبي حيث أن الجدل والاختلاف حول الطبيعة القانونية للبطاقة بين اعتبارها مفتاح إلكتروني ورفض هذه الفكرة على أساس عدم جواز قياس ذلك على المفتاح بمفهومه التقليدي، وبين اتجاه آخر يميل إلى اعتبار البطاقة من قبيل المحررات لكن محرر معالج أليا، وبين ناقد لهذا الرأي أيضا لأنه يتعارض مع مبدأ الشرعية، وبالتالي عدم اعتبار تزويرها جريمة لأنها ليست محررا بالمفهوم التقليدي.

وبين اتجاه ثالثا يعتبرها – أي البطاقة – نظام معلوماتي، ورأي مناقض له يعتبرها توقيع الكتروني – نرى أنه سيتحسن وضع نص تجريمي خاص يضفي وصفا قانونيا مستقلا للبطاقة، ويحميها من مختلف التلاعبات التي يمكن أن تكون عرضة لها على غرار ما فعل المشروع الأمريكي، حيث استحدثت سنة 1984 (الشوا، 1998، صفحة 117) نصا للعقاب على التلاعب في بطاقات الائتمان، ويطبق هذا القانون على " استعمال وإنتاج وحيازة وتسويق وسائل الولوج المزورة أو على أجهزة تصنيع هذه الوسائل ويعاقب القانون بغرامة والحبس أو بإحدى هاتين العقوبتين لكل من اقترف عمدا أو بنية الغش فعل الولوج أو البقاء أو هم أو رتب خطة ما أو صمم حيلة ما بغرض ارتكاب غش أو الإستلاء على مبلغ من النقود أو مال لا يخصه، وولج أو حاول الولوج في الحاسب الآلي بغرض تنفيذ أو محاولة تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة....." و للقانون الأمريكي مفهوم موسع للمال بحيث شمل كل الوسائل المالية والمعلومات التي تحتوي على بيانات معالجة الكترونيا والكيانات المنطقية وبرامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان، وكل قيمة أخرى ذات طابع مادي أو معنوي (علي محمود، 2000).

كما عاقب على إنتاج أو استعمال أو تسويق وسيلة أو أكثر من وسائل الولوج المصطنعة، وكذالك إنتاج أو تسويق الأجهزة التي تستخدم في تصنيع هذه الوسائل، وعرف وسيلة الولوج " بأنها كل بطاقة أو أسطوانة أو شفرة أو رقم حساب أو أي وسيلة ولوج يمكن استخدامها بمفردها أو بالاشتراك مع غيرها من الوسائل الأخرى للحصول على نفوذ أو أموال أو خدمات أو أي شيء آخر له قيمة، أو يمكن استخدامها مباشرة لتحويل النقود". ويقصد " بوسيلة الولوج المزورة أو المغنطة كل وسيلة ولوج مزورة أو صورية أو مقلدة " واستلزم هذا القانون إثبات العلم ونية الغش لدى المتهم على مخترعي الشبكة المعلوماتية على أساس أن مجرد نقل المعلومات غير المسموح بها والمختزنة في حاسب إلى شخص يصعب تقويمها ماليا، وهو ما يتعارض والولوج المعاقب عليه وفقا لهذا القانون الذي يستلزم الحصول على شيء له قيمة (الشوا، 1998، صفحة 120)

2.2.1.3 التوقيع الإلكتروني:

يعرف بعض الفقه التوقيع الإلكتروني بأنه" عبارة عن حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، وهو الوسيلة الضرورية للمعاملات الإلكترونية في إبرامها وتنفيذها، والمحافظة على سرية المعلومات والرسائل (الرومي، النظام القانوني للتوقيع الإلكتروني، 2006، صفحة 13)

وعرفه البعض الآخر بأنه " مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر .عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع من أجله (محمد المطالقة، 2008، صفحة 173).

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

وعرفه البعض الآخر بأنه" مجموعة من الإجراءات والوسائل التي يتيح استخدامها عن طريق الرموز أو الأرقام، وكذا إخراج رسالة إلكترونية تتضمن علامة مميزة من صاحب الرسالة المنقولة إلكترونيا يجري تشفيرها باستخدام مجموعة من المفاتيح واحد معلن والآخر خاص بصاحب الرسالة." (Jean Baptiste, 1998)

كما عرفه المشرع الفرنسي بأنه "توقيع رقمي يرتبط بالمعلومات التي يرغب المرسل في إرسالها إلى الطرف الآخر، واشتمال التوقيع على هذه المعطيات يدل على ارتباط صاحبه واعترافه بما ورد في الوثيقة الإلكترونية المرسلة ويجب أن يتضمن هذا التوقيع الشروط التالية :

أ- أن يكون مرتبطا بشخص آخر مما سيسمح بتعيينه، وأن يتم التوقيع من خلال وسائل تخضع للسيطرة المباشرة من صاحب التوقيع، موضحا ارتباطه بمضمون الوثيقة الالكترونية المرسلة بحيث لا يكون هناك أية قيمة للتغييرات التي قد تحدث بعد ذلك " (أحمد الأناصيري، 2002، صفحة 81).

تتنوع التواقيع الإلكترونية بين تثبيت صورة التوقيع الخطي الصادر بيد الموقع تخزينه إلكترونيا على السند المراد توقيعه، كما قد يشمل إنتاج توقيع الشخص من خلال استعمال رقم سري أو شفرة خاصة بشخص الموقع، كذلك نجد التوقيع الرقمي الذي يتم إنتاجه باستخدام تقنيات علم التشفير، فهو ليس توقيعا تقليديا وإنما هو عبارة عن عمليات متعددة تتضمن تشكيل وإنشاء رسالة إلكترونية واختصارها إلى مجموعة من الأرقام والخانات الرقمية التي تشكل في نهاية المطاف ما يمكن وصفه بالبصمة الإلكترونية والتي تكون مميزة وفريدة، ومن ثم يتم إرسالها إلى المستقبل الذي يمكن له من خلال استعمال برامج حاسوبية على جهازه من التوثق من الرسالة من حيث مضمونها وشخصية مرسلها وسلامة الرسالة من أي تغيير أو تعديل أو تزوير والهدف منه مايلي :

-التحقق من موثوقية الرسالة الإلكترونية. أي تأكيد هوية مرسلها.

-سلامة الرسالة الإلكترونية من أي تزوير أو تعديل.

-سرية الرسالة الإلكترونية حيث لا يمكن أن تقرأ إلا من قبل مستقبلها.

ب- البطاقة الممغنطة البنكية بوصفها بيانات معالجة إلكترونيا أي في شكل حروف وأرقام بلغة الآلة تحوي على بيانات متعلقة بالبطاقة كرقمها التسلسلي وهوية العميل ورقم الحساب وبيانات عن البنك مشفرة وتعتبر بمثابة توقيع، وذلك من خلال إيلاجها في الموزع أو الموزع الإلكتروني والضغط على بعض الأرقام السرية على دعامة ممغنطة بذاكرة حافظة لهذا الرقم يتم تسوية المعاملات التجارية بهذه البطاقة والرقم السري يتم معرفة الشخص المتعامل، والبنك هو الذي يخلق هذه الأرقام الإلكترونية، ويفتح ملف خاص لكل عميل لديه وبالتالي البنك يعتبر ضامنا لسلامة هذا التوقيع الالكتروني في مواجهة غيره من المؤسسات التي يتعامل معها العميل (المومني، 2003، الصفحات 51-137).

لكن يثور الإشكال حول مدى الأمن الذي يوفره هذا التوقيع خاصة وأنه عرضة للسرقة أو الضياع بسبب إهمال العميل وقلة احتياطه أو بسبب السطو والدخول غير المشروع في النظام المعلوماتي للبنك.

لكن هل المفهوم هنا يشمل البطاقة بحد ذاتها أي بياناتها الممغنطة والرقم السري أم أنه ينصرف – أي المصطلح – إلى الرقم السري فقط، واعتبار البطاقة عبارة عن رسالة معلومات ؟ هنا الموضوع بحاجة إلى دراسة مستفيضة ومستقلة من قبل الباحثين والمهتمين بالموضوع.

سواء كانت البطاقة نظام معلوماتي منفصل أو جزء من نظام معلوماتي باعتبارها مفتاح له أو توقيع يدل على هوية من دخل النظام، فإنها تظل بالتأكيد مجموعة بيانات معالجة آليا ومختزنة على دعامة إلكترونية، وتحوي هذه البيانات معلومات عن حامل البطاقة وكذلك

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

مصدرها، وهذه البيانات تقدر بالمال فهي ترتب لصاحبها حقوق وتخوله إبرام عقود، والبيانات في البطاقة معالجة آليا فتنتج عنها معلومات هي ملك للعميل والبنك كلا فيما يخصه، فهي بالنسبة للعميل تحوي على بيانات تخص حياته الخاصة، ذمته المالية علاوة على بياناته الإسمية، وهي كما نعرف محمية دستوريا في إطار الحياة الخاصة، علاوة على أنها بالنسبة للبنك تشكل وسيلة دخول إلى قاعدة البيانات – databas- تخص أداء البنك وعملاءه والأرصدة وحركتها والحسابات وأرقامها والبطاقات وأرقامها التسلسلية والسرية، أي أنها تمثل نظام مبتكر للدفع الإلكتروني .

إن بطاقة الدفع بهذا الوصف تخضع إلى حماية مزدوجة أولهما عن طريق قانون حماية حقوق الملكية الفكرية والأدبية والفنية .....الخ، علاوة على الحماية التي أفردها لها القانون العقوبات بموجب تعديل 2004.

2.3 التكييف القانوني لفعل التلاعب والتعديل للبيانات:

في دراستنا نستبعد أفعال التعدي على الجزء المادي للنظام المعلوماتي، وذلك لأنه يمثل مال مادي منقول لا خلاف عليه، وبالتالي فإنه يخضع مباشرة للنصوص التقليدية حسب نوع الفعل الذي يقع عليه إلا أنه إذا كان الهدف من المساس بالجزء المادي يهدف إلى الإضرار بالجزء المعنوي أي البرامج والمعطيات فإنه يخضع مباشرة للنصوص الجديدة للغش المعلوماتي.

إن التلاعب ببيانات البطاقة أو النظام المعلوماتي لها يشكل نوعين من الجرائم بموجب قانون العقوبات الجزائري في تعديله لسنة 2004.

نجد جرائم تقع على ذات المعطيات كجرائم الإتلاف والتشويه بأنواعه (تعديل ، إدخال ، محو ، إضافة) للبيانات والمعلومات وبرامج الحاسوب باستخدام مختلف الوسائل، كما نجد جرائم تقع على ما تمثله المعطيات المعالجة آليا من أموال أو أصول كالجرائم التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات وجرائم التزوير واستخدامه (عرب، جرائم الكمبيوتر والأنترنت ، 2002)

1.2.3 تحيين المعلـومات

وهي تعني في لغة الإعلام الآلي عمليات الإدخال والإخراج أو التعديل للبيانات، ويسميها البعض بجريمة إتلاف المعلومات وهو تعريف بالنتيجة للسلوك الإجرامي بينما مصطلح تحيين ينصرف إلى النشاط أو السلوك الإجرامي الظاهر، بإحدى الصور الثلاث الواردة في نص المادة 394 مكرر والتي تنص على ما يلي " يعاقب بالحبس من ستة (06) أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 4000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها "

1.1.2.3 الركن المادي : يشتمل على الصور التالية :

- إدخال بيانات للنظام لم تكن موجودة فيه أصلا، ويقصد به إضافة معلومات جديدة على المعلومات الموجودة داخل النظام، ويتحقق هذا الفعل بمجرد إدخال أي فيروس معلوماتي.
- إزالة بيانات كانت مخزنة في النظام أي حذفها أو محوها، و يقصد به إفناء أو شطب المعلومات الموجودة داخل النظام كليا أو جزئيا. (هلالي، 1999، صفحة 10)

- تعديل البيانات الموجودة في النظام، أي تغيير المعطيات الموجودة داخل النظام واستبدالها بأخرى جزئيا أو كليا، أو التلاعب بالبرنامج بإمداده بمعطيات مغايرة عن تلك التي صمم لأجلها (بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنيت، 2007، صفحة 95)

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

إن الموضوع الذي ينصب عليه فعل الجاني في جريمة الإتلاف المعلومات هي المعلومات و يقصد بالمعلومات البيانات التي تتم معالجتها و ترتيبها و تنظيمها و تحليلها بغرض الاستفادة منها و الحصول على نتائج معينة من خلال استخدامها.

و يشترط كي تتمتع هذه المعلومات بالحماية أن تكون موجودة داخل النظام المعلوماتي أما إذا كانت هذه المعلومات خارج النظام سواء قبل دخولها أو بعد خروجها من هذا النظام ، كان يقع فعل الاعتداء، على المعلومات الموجودة على قرص أو شريط مغنط خارج الخدمة فان الإتلاف المعلوماتي تتحقق في هذا الفرض (مناصرة، 2001 -2004).

ونلاحظ أن استخدام مصطلحات إدخال تعديل محو إزالة كلها تؤدي نفس المعنى، لأن إدخال بيانات جديدة يتطلب بالضرورة محو أو إزالة بعض البيانات وهو ما ينتج تلقائيا تعديلا فهو تزوير للبيانات.

وسيلة إدخال البيانات أو محوها أو تعديلها لا تهم سواء كان ببرنامج معدل أو بوصل البطاقة بالكمبيوتر وقراءة بياناتها وإدخال بيانات أخرى أو محو القديمة أو إضافة بيانات جديدة (حسين محمود، 2002، الصفحات 98-99)

2.1.2.3 **الركن المعنوي**: هذه الجنحة تفترض العمد والغش، حيث يأتي الفاعل سلوكه الإجرامي وهو يعلم أنه يتعدى على سلامة البيانات، ويدرك أنه ليس مختصا لمعالجتها واستخدامها ، ولا يشترط تدليسا خاص ، أي ليس من الضروري القول أن هذه الأفعال التي يأتيها بقصد خاص كإرادة إحداث ضرر خاص (Dr Gattegno, 1999, p. 283).

2.2.3 صنع واستعمال البيانات

تنص المادة 394 مكرر 2 على ما يلي " يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة مالية من 1000.000 دج إلى 5000.000 دج كل من يقوم عمدا وعن طريق الغش بما يلي :

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ."

في الجريمة المعلوماتية يصعب أحيانا كثيرة الفصل بين البيانات ودعامتها الإلكترونية، وذلك أن طريقة عمل البيانات وتوصيلها أو نقلها أو حيازتها هنا لا تنفصل عن حيازة الدعامة المادية، حتى وإن كانت القيمة القانونية والاقتصادية تنحصر في البيانات، لأن البيانات لا يتم نقلها بين الأشخاص إلا بوجود وسائط مادية وهي في هذا البحث عبارة عن بطاقة مغناطيسية.

المادة 394 مكرر 02 تصب حمايتها على البيانات سواء المخزنة في الحاسب أو المرسلة عن طريق منظومة معلوماتية، وبالتالي تمتد الحماية إلى وسائط إرسال البيانات (Dr Gattegno, 1999, p. 283)، وهي مقسمة إلى نوعيين من الأفعال في الركن المادي.

1.2.2.3 **الركن المادي**: نجد فيه جريمتين:

1-الفقرة الأولى من المادة نصت على مجموعة أفعال هي تصميم أو تجميع أو بحث أو توفير أو نشر أو الإتجار.

- تصميم معطيات ونقصد بها تكوين أو خلق أو إنشاء البيانات صحيحة أو مزورة أو برامج معلوماتية جديدة أو معدلة أو مقلدة.
- البحث عن المعطيات والبرامج و ذلك سواء كانت جديدة أو مقلدة حقيقية أو مزورة.

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

- تجميع وتوفير ونشر: نقصد بها جمع عناصر أو مكونات البرامج (الدعامات، البيانات، نظم المعالجة) سواء كانت أصلية أو مقلدة، حقيقية أو مزورة، وتسهيل الحصول عليها.

- الإتجار : بيع وشراء البرامج.

وبالتالي يكفي حصول أحد هذه الأفعال فقط لتكوين الركن المادي، والهدف من هذا التعداد الذي جاء على سبيل الحصر يهدف إلى محاربة أعمال الاتجار غير المشروع (السوق السوداء) وأعمال القرصنة في البيانات والبرامج، وهي حماية جديدة إضافة إلى تلك التي يوفرها قانون حماية حقوق المؤلف خاصة جنحة التقليد.

كما أن هذه الأفعال تعد من قبيل التزوير المعلوماتي، لأن إنشاء أو تصميم وتجميع برامج أو بيانات غير الصحيحة، ومعالجتها آليا وتسهيل الحصول عليها يعد تزويرا معنويا بالمفهوم التقليدي وإن أفرد له المشرع نص خاص.

أما إذا كانت المعطيات المعالجة أو المرسلة صحيحة فإننا نكون بصدد سرقة معلوماتية (بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية الكتاب الثاني، الحماية الجزائية لنظام التجارة الالكترونية، 2004، صفحة 175 ومايليها)، لأن اختلاس البيانات هنا دون رضا صاحبها الشرعي يعد اختلاسا مكونا لجرم السرقة التقليدية، وإن كان محلها معنويا غير محسوس، وهو وصف أو تكييف محل نقاش واسع لدى الفقه، ومحل الجريمة هنا هو البيانات المعالجة أو المخزنة أو المرسلة عن طريق نظام معلوماتي، ولهذا يجب أن تكون معلومات لديها قيمة مالية أو قيمة فنية أو أدبية، وليست عامة أو مشاعة يستطيع أي شخص معرفتها كحالة الطقس أو درجة غليان الماء بمعنى أن البيانات المعالجة بطريقة آلية أصبحت معلومات تتصف بخاصتي السرية والاستئثار، حتى تكون محلا للحماية.

2- الفقرة الثانية: نصت على أفعال الحيازة، إفشاء، نشر، استعمال، وهي تعني:

- الحيازة: وهي الحالة الواقعية التي تخول الشخص القدرة أو السلطة المادية على الشيء فيستطيع استعمال هذا الشيء والتصرف فيه، وإعدامه، بعبارة أخرى أنها وضع مادي يستطيع فيه الشخص السيطرة على الشيء فعليا وهي تامة، وناقصة، أو مؤقتة ويقصد بها وضع اليد على البيانات أو البرامج المعالجة آليا.

- الإفشاء والنشر: ونقصد بها جعل سر صناعة أو إعداد برامج أو بيانات كانت طي الكتمان وممنوع معرفتها من الغير مباحة له وقادرا على الوصول والاستحواذ عليها بيسر، ويمس هذا الفعل عادة من هم بموجب مقتضيات عملهم مقيدون بالسر المهني مطلعون على معلومات أو يستطيعون الوصول إليها بموجب عملهم فيكسرون القاعدة السرية ويفشون بهذه البيانات وهم هنا على سبيل المثال موظفي البنك ، المبرمجون، التاجر المنظم، وكل من له دخل بصناعة وإعداد برامج الدفع الالكتروني.

- الاستعمال : كل من حصل على بيانات أو برامج سواء بطريقة شرعية أو غير مشروعة و استخدامها في ارتكاب جريمة من الجرائم الواردة في القسم 7 مكرر من قانون العقوبات ، محل الجريمة هنا أيضا المعطيات المعالجة آليا أو المخزنة في ذاكرة الحاسب الآلي أو المرسلة بواسطة نظام معلوماتي .

هنا المادة تحمي البيانات بصفة خاصة سواء في مرحلة المعالجة أو التخزين أو الإرسال حيث تمتد الحماية حتى إلى عملية الإرسال، حيث تكون المعلومات في حالة حركة ونقل حيث يسهل الوصول إليها باستخدام مختلف طرق السطو، كتوصيل خط تليفوني مباشر بالنظام أو التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي، إدخال فيروسات تعطل الجهاز وتجعله يمحو أو يخرب البيانات المخزنة (حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، 2002).

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

2.2.2.3 الركن المعنوي: هنا تطلب المشرع الجزائري وجود القصد الجنائي بنوعيه أي العام والخاص والمتمثل في نية الغش، فهذه الجريمة عمدية تتطلب علاوة على القصد العام وجود نية متمثلة في ارتكاب أو تسهيل أو الاستخدام لارتكاب إحدى الجرائم الواردة في القسم حتى وإن كان ارتكاب هذه الجرائم ليس أكيدا بل متحملا، فمجرد صنع أو حيازة أو نشر أو استعمالها (البيانات المعالجة أو البرامج) كاف بحد ذاته للدلالة على نية صانعها أو حائزها في الإضرار بالغير، هذه المادة حددت الهدف أو الغرض من الأفعال السابقة في ارتكاب إحدى الجرائم الواردة في القسم 7 مكرر وهي – الدخول والبقاء غير المشروعين، حذف أو تغيير المعطيات، تخريب عمل النظام، إدخال عمدي لمعطيات أو إزالة أو تعديلها.

4. الولوج والتلاعب بالنظام الذي تعمل عليه بطاقة الدفع

بطاقة الدفع في أضعف أحوالها هي أداة للولوج إلى النظام المعلوماتي للدفع الالكتروني وهي منفصلة عنه تبقى دون فائدة عملية وتظهر خطورتها في إمكانية استخدامها للدخول والتلاعب بالنظام المعلوماتي وفتحه والبقاء فيه وإحداث مختلف الإضرار ببياناته المخزنة، أو تحميل البطاقة ببرنامج فيروسي تؤدي إلى محو منتقى للبيانات أو تعديلها أو محوها وبالتالي تعطيل نظام الدفع الالكتروني أو التشويش عليه ، فيتوقف عن العمل ، وهي كما نعلم بيانات تخص البنك والعميل متعلقة بالأموال و الحسابات والأرصدة في البنك، فالجريمة التي ترتكب هنا الغرض أو الهدف منها هو عادة ارتكاب جريمة أخرى متمثلة في السرقة أو النصب وذلك عن طريق التحويل الالكتروني للأموال وعليه نقسم دراستنا في هذا المطلب كما يلي.

الولوج المشروع بهدف غير مشروع (الفرع الأول) ، الولوج غير المشروع من قبل الغير (الفرع الثاني) .

1.4 الولوج المشروع بهدف غير مشروع

تنص المادة 394 مكرر على ما يلي: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية أو يحاول ذلك تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 دج إلى 150.000دج " وهذه المادة استوحاها المشرع الجزائري من المشرع الفرنسي بنفس العنوان .

واختار أن تكون في فقرات أضاف فقط للمادة المحاولة و عاقب عليها وأخطأ في المصطلح العربي (المنظومة) والأصح "نظام" تعبر عن "«système. فتقع جريمة الدخول أو البقاء بطريق الغش إذا وقع الاعتداء على عنصر يشكل جزء من أنظمة متعددة (مثل هنا الموزع الآلي، البطاقة، الحاسب المركزي)، فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة الاتصال ووقع الاعتداء على جهاز حاسب ألي في نظام منها فالجريمة واقعة ، فما ينطبق على الجزء ينطبق على الكل سواء كانت شبكة مفتوحة (الأنترنت) أو مغلقة (الأنترانت) تبعا لطبيعة الشبكة وطريقة توصيلها باعتبار أن كل وحدة من الشبكة بعناصرها الفيزيائية والمنطقية تشكل منبع Source (مناصرة، 2001 - 2004، صفحة 46).

الركن المادي في الجريمة هو الدخول أو البقاء بالغش في نظام المعالجة الآلية للبيانات ويتمثل في فعل الدخول أو البقاء بغش دون إحداث إتلاف أو تخريب النظام وهي الصورة البسيطة للجريمة في الفقرة الأولى، والصورة المشددة لها تتحقق في توافر نتيجة عن فعل الدخول أو البقاء بالغش إما بمحو أو تغيير في المعطيات الموجودة وإما إتلاف وظيفة تشغيل النظام (Dr Gattegno, 1999, pp. 280-282).

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

وهذا الولوج أو الدخول قد يكون مشروعا من أشخاص لديهم إذن بالدخول إلى النظام والبقاء فيه لكن دخولهم يكون غشا خلال الفترات الخارجة عن الإذن كما سنرى.

1.1.4 ولوج من أذن له: في نظام الدفع الإلكتروني في البنوك أو المؤسسات المالية يسمح بالدخول في النظام الآلي لمعالجة البيانات المتعلقة بالنظام إلى فئتين من الأشخاص هما عملاء البنك الذين يحملون بطاقة دفع أو سحب بنكية مغناطيسية تسمح بإجراء المعاملات المالية والتحويلات الإلكترونية كما توجد فئة ثانية هي موظفي البنك الماسكين أو المسيرين لنظام الدفع الإلكتروني دون غيرهم من موظفي البنك حيث تقضي طبيعة عملهم دخول النظام والإطلاع على بيانات ومراقبة حركة الأرصدة وبالتالي إطلاعهم على كلمة السر أو الشفرة التي تسمح دخولهم النظام .

أ-ولوج حامل البطاقة باستخدام بطاقته :

لا مجال للشك، أن العميل حامل البطاقة المغناطيسية هو مستخدم مصرح له لاستخدام الكمبيوتر فإنه بإعطائه أمرا إلى الآلة بعد إدخال بطاقته التي تفتح و تشغل النظام بتسليمه مبلغ مالي ليس له فيه حق و ذلك بأن يدخل بيانات – رقم المبلغ المسحوب – غير صحيحة تمس بحقوق البنك ، هنا حتى ولو استخدم بطاقته بشكل صحيح فإنه في بعض الأحيان يحمل العميل بطاقته ببرنامج فيروس (الرومي، جرائم الكمبيوتر والأنترنيت ، 2003، صفحة 262 ومايليها) أو يحمل معه جهاز يسمح له بالتقاط إشارات كهرومغناطيسية ويربط بواسطتها اتصال مع الحاسب المركزي (حسن علي محمود، 2002، الصفحات 99-100). وبعد انتهاء عمليته المالية وسحب النقود ويخرج بطاقته ، يظل الجهاز مفتوحا عن طريق الجهاز الإلكتروني الذي ربطه به ويبقى متجولا في النظام المعلوماتي للبنك ، مع أن تصريحه بالدخول ينتهي في كلمة مرة بانتهاء العملية المالية و بالتالي فإنه هنا يرتكب فعل البقاء غير المشروع بطريقة الغش في كل أو جزء من النظام ، فإن كان للبقاء نتيجة هي التلاعب وذلك بالحذف أو التغيير في البيانات تضاعف عقوبته كما قد ينجر عن استخدامه لبرنامج محمل على البطاقة تخريب نظام عمل الجهاز فتضاعف العقوبة أيضا ، نفس الأمر إذا كان دخوله قد تم باستخدام بطاقة مزورة أو مسروقة أو ضائعة أو ملغاة أو منتهية الصلاحية، حيث الدخول هنا غير مشروع والبقاء كذلك .

ب – دخول موظف البنك إلى قاعدة البيانات :

موظف البنك الذي يعمل خلف جهاز الكمبيوتر الخاص بنظام الدفع الإلكتروني والذي أسندت

له مهمة تشغيله وإدارته هو شخص له تصريح للدخول إلى قاعدة بيانات النظام و ذلك بإستخدام شفرة معينة أو كلمة السر فدخول النظام مشروع طالما كان في إطار أداء وظيفته وفي أوقات العمل، أما خارج أوقات العمل أو خارج المهام المسندة إليه فإن دخوله إليه كان مصرح له – وجود الشفرة بحوزه – وبقاء في النظام تدخل تحت طائلة المواد 394 مكرر فان كان دخوله وبقاؤه بهدف التلاعب في البيانات وإجراء تعديلات عليها بالحذف أو الإضافة أو الإزالة ونتج عن ذلك تعديل للنظام أو تعديل لعمله أو استيلاء على البيانات و الاطلاع على اسرار البنك والعملاء ، وقع فعله تحت وصف المادة 394 مكرر، فإن افشي الشفرة أو كلمة السر أو حتى سرب نسخة عن برنامج النظام للغير، بغرض إجراء تحويلات مالية بين الحسابات فإن فعله يقع تحت طائلة المادة 394 مكرر02 .

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

2.1.4 هدف الغش أو التلاعب:

سبق القول أعلاه أن الدخول في النظام والبقاء فيه قد يكون مسموحا به وحصل فاعله على تصريح ، لكن هنا الجاني يستغل هذا التصريح ويتلاعب به ويتعسف في استخدامه غير مراع للثقة التي منحه إياها صاحب النظام أو المسيطر عليه ، لكن نية الجاني هنا انصرفت إلى الغش وهو متمثل في سحب مبلغ تتجاوز الرصيد إذا كانت البطاقة صحيحة. (Abou ela، 1994، صفحة 43)

أو الحصول على مال الغير في حالة الموظف الذي يتلاعب بالبيانات

ويجري تحويلات الكترونية للأموال بين الأرصدة ، فقد يلغي ديون من حسابات أو يجعل حسابات أخرى مدينة فينتج عن عمله إثراء لذمة مالية أو إفقار لها، علاوة على أنه – أي الموظف- إرتكب جريمة خيانة أمانة بسبب علاقة العمل التي تربطه بالبنك أو المؤسسة المالية. (الشوا، 1998، صفحة 138 ومايليها)

2.4 الولوج غير المشروع من قبل الغير:

نقصد غريب عن نظام المعالجة الآلية للبيانات، وغير مرخص له بالدخول إليه أو التواجد فيه أو البقاء فيه أو الاطلاع على المعلومات المخزنة في ذاكرة النظام وهي تشمل في ذلك حامل البطاقة الملغية أو المنتهية الصلاحية، مستخدما البطاقة المزورة أو المغناطيسية، موظف البنك غير المسئول عن الحاسب الآلي لنظام الدفع الإلكتروني أي غير المرخص له بالدخول أو التواجد داخل النظام.

1.2.4 فعل الولوج والإطلاع والبقاء المجرد:

تنص المادة 394 مكرر على أفعال الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا تترتب عن ذلك حذف أو تغيير للمعطيات (نتيجة) أو تخريب نظام شغل أو عمل النظام

يتكون الركن المادي من نشاط إجرامي يتمثل أما فعل الدخول إلى النظام أو جزء منه دون وجود ترخيص وهو ما يستدل عنه بنصه على الغش في الدخول ولم يحدد المشرع وسيلة الدخول ولا الطريقة فيستوي أن يكون بجهاز تنصت أو برنامج التقاط أو تجسس ، أو الشفرة الصحيحة أو الرقم السري الصحيح من طرف من ليس له – بطبيعة الحال - ، وأما البقاء فهو التواجد داخل النظام ضد رغبة من له الحق في السيطرة عليه ، فإذا كان الدخول أو البقاء بطريق الغش والإطلاع على النظام أدى إلى أما محو أو تعديل أو تغيير للمعطيات أو أدى إلى التشويش على العمل العادي للنظام تضاعف العقوبة حيث نكون بصدد معاقبة المساس اللاحق بالأنظمة الغير متعمد أو دور غير قصد إجرامي بسبب الجهل أو سوء التحكم في المسائل المعلوماتية أو الإهمال أو عدم توخي الحذر للدخول بقوة أو عنوة للنظام المعلوماتي أو البقاء بطريق الغش (Véron, 1999, p. 266).

ونعلم أن المعلومات المخزنة في قاعدة البيانات في الحاسب الآلي تحوي على بيانات إسمية للعملاء وبيانات متعلقة بذممهم المالية، وكذلك بيانات عن عمل البنك و طرق أداه و بالتالي فهي بيانات تتوفر لها خصائص سرية والإستئثار فهي بيانات محمية قانونا.

2.2.4 فعل الولوج مع قصد الغش:

علاوة على إمكانية تطبيق نص المادة 394 مكرر فإنه يمكن أن يقع هذا الفعل تحت نص المادة 394 مكرر 1 حيث أن الدخيل على النظام الآلي لمعالجة البيانات لا يكتفي بمجرد الدخول أو البقاء المسالم في النظام وإنما تتجه نيته إلى العبث بالنظام والبيانات المخزنة فيه و تأخذ هذه النية مظهرها المادي المتمثل في نشاط إجرامي يكون إما: إدخال أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها النظام وهو ما يعرف بتحيين المعلومات – سبق دراسته أعلاه- فالفعل هنا ينصب على البيانات ذاتها وليس العناصر المادية اللازمة لعمل

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

النظام بأية وسيلة كان هذا الدخول سواء بطريقة مباشرة أو غير مباشرة وسواء كانت هذه البيانات أو النظام محمي أو غير محمي .(CROZE, 1988, pp. 5-7)

5.خاتمة:

لقد زاد التعامل ببطاقات الدفع الإلكتروني باعتبارها تؤدي دور فعال خاصة في المجال المصرفي، وهذا الأمر أدى بدوره إلى كثرة وتنوع الجرائم المصاحبة لاستخدامها، هذه الجرائم التي تعد من جرائم المعلوماتية تهدد حامل البطاقة وجميع المتعاملين بها، ويتم ذلك عبر الأجهزة الإلكترونية وباستخدام الانترنيت، ومن ثم بات من الضروري حماية استعمال وسائل الدفع الإلكتروني والتي تعتبر من أهم أسباب قيام التجارة الإلكترونية، إلا أنه نتيجة للطبيعة غير المادية لهذه الجرائم المستحدثة نجد عدم وجود نص قانوني يحمي من جرائم الاحتيال المعلوماتي .

- جرائم بطاقات الدفع الإلكتروني تدخل ضمن الجرائم المعلوماتية، وهي وليدة استخدام تقنية المعلومات حيث تتزايد بتزايد استخدام هذه التقنيات.

- صعوبة الكشف عن هذه الجرائم نظرا لطبيعتها غير المادية، وقابلية البيانات للحذف والإتلاف بسهولة

- يثير الركن الشرعي في جرائم المعلوماتية إشكالية استخدام مصطلحات مختلفة ذات دلالات متباينة، وإن كانت بعض التشريعات قد عمدت إلى تحديدها، فإن غالبية المشرعين يوكلون تلك المهمة للفقه والقضاء، وقد اتجه المشرع الجزائري الإتجاه الثاني.

- لقد جمع المشرع الجزائري فعلي الدخول والبقاء غير المشروعين داخل أنظمة المعلوماتية في نص تجريمي واحد إلا أنه دل عليهما بمصطلحين مختلفين ولم يشر إلى فعل الإعتراض، مما يفتح الباب واسعا أمام اعتبار اعتراض الأنظمة مجرما بتجريم الدخول باعتباره أحد أشكاله أو اعتبره فعلا مباحا إلى حين تجريمه بنص خاص.

وفي ظل الإعتداءات المصاحبة لاستخدام بطاقة الدفع الالكتروني، وكمحاولة للمساهمة في إنجاح نظام التعامل بها نقديم الاقتراحات التالية:

- على المشرع الجزائري التدخل بوضع نص خاص واضح لتجريم مختلف أنواع الغش التي ترتكب بواسطة البطاقة أو عليها وذلك بتحديد ماهيتها هل هي محرر معلوماتي أو مفتاح إلكتروني أو توقيع الكتروني، أم نظام معلوماتي فتخضع لمقتضات القسم 7 مكرر من قانون العقوبات.

- يجب تكثيف الجهود على مستوى التعاون الدولي لمواجهة هذه الجريمة العابرة للحدود.

- ضرورة تجريم اعتراض أنظمة المعلوماتية غير المصرح به بنصوص خاصة ومنفصلة عن تلك المتعلقة بجريمة الدخول إلى هذه الأنظمة.

- تحديث إجراءات البحث والتحري وتضمينها في قانون خاص ، والابتعاد عن دمجها مع الإجراءات التقليدية.

- 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.

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

قائمة المراجع

مؤلفات

-أحمد الأناصيري ,ف .م .(2002) .*عقد الإشتراك في قواعد المعلومات عبر شبكة الأنترنت –دراسة تطبيقية لعقود التجارة الالكترونية الدولية* .الإسكندرية.دار الجامعة الجديدة للنشر.

-الرومي ,م .أ .(2006) .*النظام القانوني للتوقيع الإلكترونيا.الأسكندرية* .دار الفكر الجامعي.

-الشوا ,م .س .(1998) .*ثورة المعلومات وانعكاساتها على قانون العقوبات .القاهرة* .دار النهضة العربية.

-المناعسة ,أ & .,الزعبي ,ج .م .(2001) .*جرائم الحاسب و الأنترنت دراسة تحليلية مقارنة* .الأردن :دار وائل للنشر والتوزيع.

-المومني ,ع .ح .(2003) .*التوقيع الإلكتروني وقانون التجارة الالكترونية . الأردن* .دار وائل للنشر والتوزيع.

-بيومي حجازي ,ع .ا .(2004) .*النظام القانوني لحماية التجارة الإلكترونية الكتاب الثاني، الحماية الجزائية لنظام التجارة الالكترونية* .الاسكندرية :دار الفكر الجامعي.

-بيومي حجازي ,ع .ا :(2002) .*النظام القانوني لحماية التجارة الإلكترونية –الكتاب الأول :نظام التجارة الإلكترونية وحمايتها مدنيا* .الاسكندرية :دار الفكر الجامعي.

-حسن علي محمود ,ع .ا .(2002) .*سرقة المعلومات المخزنة في الحاسب الألي .القاهرة* .دار النهضة العربية.

-ذ *الزعبي ، صايل ف الهواوشة :جرائم الحاسب و الأنترنت دراسة تحليلية مقارنة* ، .الأردن :دار وائل للنشر والتوزيع.

- عبد الفتاح بيومي حجازي. (2007). *الإثبات الجنائي في جرائم الكمبيوتر والأنترنيت*. مصر: دار الكتب القانونية.

-عبد الله حسين محمود. (2002). *سرقة المعلومات المخزنة في الحاسب الآلي*. الإمارات العربية المتحدة: دار النهضة العربية.

-عماد محمد سلامة. (2005). *الحماية القانونية لبرامج الحاسب الآلي و مشكلة قرصنة البرامج. عمان، دار وائل ، 2005.*

-فتوح الشاذلي، و عفيفي كامل عفيفي. (2003). *جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون- دراسة مقارنة-عمان. الأردن. منشورات الحلبي الحقوقية.*

-محمد المطالقة ,م .ف .(2008) .*الوجيز في عقود التجارة الالكترونية* .الأردن :دار الثقافة.

-محمد أمين الرومي. (2003). *جرائم الكمبيوتر والأنترنيت* . الإسكندرية، مصر: دار المطبوعات الجامعية.

-محمد شتا ,م .(2001) .*فكرة الحماية الجنائية لبرامج الحاسب الألي* .المطبعة الجامعية.

-محمد علي العريان. (2004). *الجرائم المعلوماتية* . الاسكندرية، مصر: دار الجامعة الجديدة للنشر .

-هلالي ,ع .ا (1 .(1999) .حجية المخرجات الكمبيوترية، في المواد الجنائية دراسة مقارنة .القاهرة :النسر الذهبي للطباعة.

- CROZE, H. (1988). « L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatiqu, I,. JCP G..
- Dr Gattegno, p. (1999). *droit pénal spéciale*. Dalloz.
- Jean Baptiste, M. (1998), *crée et exploiter un commerce électronique*. paris.
- Véron, M. (1999). *droit pénal spéciale*. Dalloz.

المقالات

-بركات ,ك .(2022) .تجريم الإستخدام غير المشروع لبطاقة الدفع الالكتروني من قبل أطرافها في القانون الجزائري .*مجلة طبنة للدراسات العلمية الأكاديمية* ,المجلد 1،العدد 5 ,الصفحات 327-350

Abou ela, A. M. (1994). le droit pénal face a l'utilisation abusive ou frauduleuse des cartes bancaires magnétiques. . *مجلة العلوم القانونية والاقتصادية العدد 2 ,السنة 36.*

المداخلات

-يونس عرب. (2002). جرائم الكمبيوتر والأنترنت . *مؤتمر الأمن العربي*: المركز العربي للدراسات و البحوث الجنائية .أبو ظبي

-يونس عرب. (28- 29 تشرين أول 2002). التشريعات و القوانين المتعلقة بالأنترنيت في الدول العربية. *مؤتمر ومعرض التكنولوجيا المصرفية العربية و الدولية*. اتحاد المصارف العربية.عمان، الأردن

مواقع الأنترنيت

-شاشة ,ف .(s.d.) .*الوثيقة الرقمية، إعادة تعريف في ظل البيئة الإلكترونية على الموقع* www.pixelplanet.de/pdfprinter-info.htm

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)