

الرقمنة وتداعياتها على النظام المصرفي

Digitalization and its repercussions on the banking system

إلياس بوزيدي

المركز الجامعي مغنية (الجزائر)، bouzidi.droit@gmail.com

تاريخ النشر: 2024/01/20

تاريخ القبول: 2024/01/09

تاريخ الاستلام: 2023 /10/11

ملخص:

يهدف البحث إلى إبراز مساهمة التطور التكنولوجي في مجال الاتصالات وتقنيات المعلومات في سرعة انتشار المعلومات وسهولة تداولها عبر خدمات الانترنت، مما أدى إلى ظهور العديد من المخاطر والاعتداءات التي تتم في بيئة الانترنت، الأمر الذي أدى إلى ضرورة وضع تشريعات تحمي أمن المعلومات، ولا سيما في المجال البنكي. ومن النتائج المتوصل إليها، هو امتداد المعلوماتية إلى قواعد القانون التجاري، وأثرت بالخصوص على أحكام المعاملات المصرفية، بسبب ما أوجدته من وسائل الدفع الإلكتروني، وبفعل المفهوم المستحدث للنقد (المال الرقمي)، ومن جهة أخرى فقد أفرزت تقنية المعلومات وسائل حديثة لتقديم الخدمات المصرفية وإدارة العمل البنكي، إضافة لوسائل الدفع الإلكتروني، عمليات التحويل المصرفي الإلكتروني والاعتماد المستندي الإلكتروني.

كلمات مفتاحية: الرقمنة، البنوك، الاعتماد المستندي الإلكتروني، البطاقات البنكية، الانترنت.

Abstract:

The research aims to highlight the contribution of technological development in the field of communication and information technologies to the rapid dissemination of information and the ease of its circulation through Internet services, which has led to the emergence of numerous risks and attacks that take place in the Internet environment, which has led to the need to develop legislation that protects information security, especially in the banking area.

Among the results obtained, there is the extension of information technologies to the rules of commercial law, and this has particularly affected the provisions of banking transactions, due to the means of electronic payment that they have created, and due of the new concept of currency (digital money). On the other hand, information technologies have given rise to modern means of providing and managing banking services, Banking works, in addition to electronic means of payment, electronic bank transfer operations and documentary credit electronic.

Keywords: Digitalization, banks, electronic documentary credit, bank cards, Internet.

مقدمة

أدى التقدم الحضاري والتكنولوجي الحديث إلى اكتشاف وسائل وأدوات متطورة ومتقدمة تتعامل بها البنوك مع الأفراد ويتعامل بها الأفراد في معاملاتهم وأنشطتهم المالية والمصرفية والتجارية محليا ودوليا.

إن الإحاطة التشريعية بتحديات عصر تقنية المعلومات تتطلب إحاطة مسبقة بالعناصر البنائية والفنية المتصلة بالعصر ولو ضمن إطار المعرفة العريضة لسلامة مخرجات التشريع التي تنطوي في الغالب الأعم على معالجة مسائل ذات محتوى تقني.

لقد اتصفت المعلوماتية على قدرة فائقة على تجميع ومعالجة وتبادل المعلومات، والسرعة الهائلة التي وسمت مسيرة تطورها، والاعتماد المتزايد عليها في مختلف أوجه النشاط الإنساني، جعلها تؤثر على مختلف فروع القانون وقواعد النظام القانوني، وقد امتد تأثيرها على قواعد القانون الجنائي فيما يعرف بجرائم الكمبيوتر والانترنت.

كما أنه قد امتد المعلوماتية إلى قواعد القانون التجاري، وأثرت بالخصوص على أحكام المعاملات المصرفية، بسبب ما أوجدته من وسائل الدفع الإلكتروني، وبفعل المفهوم المستحدث للنقد (المال الرقمي)، ومن جهة أخرى فقد أفرزت تقنية المعلومات وسائل حديثة لتقديم الخدمات المصرفية وإدارة العمل البنكي، إضافة لوسائل الدفع الإلكتروني، عمليات التحويل المصرفي الإلكتروني والاعتماد المستندي الإلكتروني.

غالبا ما تقتزن بالاكشافات الجديدة آثار إيجابية وأخرى سلبية، فهي تعمل من ناحية على دفع خطوات التطور في المجالات المختلفة قدما إلى الأمام، وينشأ عنها بعض الآثار السلبية يأتي في مقدمتها العديد من الجرائم التي يرتكبها المجرمون عن طريق استغلال هذه الاكتشافات في تسهيل ارتكابهم لهذه الجرائم أو تقع جرائمهم عليها فتصبح المخترعات الجديدة موضوعا للجريمة أو وسيلة لتسهيل ارتكابها.

من هذا المنطلق نطرح الإشكالية الآتية: إلى أي مدى ساهمت المعلوماتية في تكيفها مع النظام المصرفي؟ وللإجابة على هذا الإشكالية، سنتعرض إلى تجليات المعلوماتية في القطاع البنكي (المبحث الأول)، وإلى صور الاستخدام غير المشروع للنظام الرقمي المصرفي (المبحث الثاني).

المبحث الأول: تجليات المعلوماتية في القطاع البنكي

لقد امتد تأثير الرقمنة على قواعد القانون المصرفي بسبب ما أوجدته من وسائل الدفع المصرفي الإلكتروني، وبفعل المفهوم المستحدث للنقد سواء المال الرقمي والمال الإلكتروني، العملات الرقمية والمشفرة، وكذا العمليات المصرفية المستحدثة المتمثلة في الاعتماد المستندي الإلكتروني والتحويل المصرفي الإلكتروني.

المطلب الأول: وسائل الدفع المصرفي الإلكتروني

تتمثل وسائل الدفع الإلكترونية في بطاقة الدفع الإلكترونية، وكذا الشيكات والنقود الإلكترونية.

الفرع الأول: بطاقات الدفع الالكترونية

لقد أرسى المشرع الجزائري وسائل دفع أكثر حداثة من خلال محاولته عصرنة النشاط البنكي من خلال نصه على استحداث بطاقات الكترونية للوفاء، بموجب القانون 02/05 من خلال الفصل الثالث من الباب الرابع تحت عنوان " في بطاقات السحب والدفع"¹.

وقد عرف المشرع الجزائري بطاقة الدفع في المادة 543 مكرر 23 من القانون التجاري: "تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال.

تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب الأموال". يتبين من خلال المشرع الجزائري أنه عرف نوعين من البطاقات الالكترونية، بطاقة الدفع وبطاقة السحب"، كما أنه اشترط ضرورة صدورهما من البنوك والمؤسسات المالية.

تعد بطاقات الوفاء بطاقة تصدر دوما عن مصرف وتعطي هذه البطاقة للعميل الذي يكون له حساب في ذلك المصرف، لذلك تكون هذه البطاقة أداة وفاء، وبذلك يكون رصيد الحساب المصرفي شبيه بضمان نقدي، ويقوم المصرف بالسحب المباشر من حساب العميل فور ورود فاتورة العملية التي قام بها حامل البطاقة من المورد².

الفرع الثاني: الشيكات والنقود الرقمية.

سنعرض في هذا الصدد إلى أهم بدائل للوسائل الورقية أثرت فيها المعلوماتية، تتمثل في الشيكات الالكترونية، والنقود الالكترونية.

أولا: الشيكات الالكترونية

الشيك الالكتروني في جوهره بديل رقمي للشيك الورقي، فهو التزام قانوني بسداد مبلغ معين في تاريخ محدد لصالح فرد أو جهة معينة. والشيك الالكتروني يحتوي على نفس المعلومات التي يحملها الشيك التقليدي مثل المبلغ والتاريخ والمستفيد والساحب والمسحوب عليه، إلا أنه يكتب بواسطة أداة إلكترونية مثل الحاسوب أو المساعد الرقمي الشخصي PDA أو الهاتف المحمول ويتم تذييله بتوقيع إلكتروني ومن ثم يتمتع بقوة الشيك الورقي في الدول التي تعترف بصحة التوقيع الإلكتروني.

وعلى الرغم من أن الشيك تم توثيقه وقت إبرام الصفقة على الويب إلا أنه لا يحدث سحب للرصيد من حساب العميل قبل مرور عدة أيام، وبالتالي يستفيد العميل من الاحتفاظ بهذا الرصيد في حسابه إلى أن يتم نقل الأموال وفق النظام المتبع في حالة الشيكات التقليدية¹.

¹ الأمر 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري الجزائري، ج ر، عدد 101، المؤرخ في 19 ديسمبر 1975، المعدل والمتمم بالقانون رقم 05-02 المؤرخ في 06 فيفري 2005، ج ر، عدد 11، المؤرخ في 09 فبراير 2005.

² أنس العلي، النظام القانوني لبطاقات الاعتماد، منشورات الحلبي الحقوقية، لبنان، 2005، ص.53.

حيث أن الآلية المتوفرة في الشيك الذكي من خلال الشريط المغنط أو خلية التخزين المثبتة على أطراف الشيك، بحيث يتم إمرار الشيك أو إدخاله في أحد الأجهزة المتوفرة في نقاط البيع، وكذا المستخدمة في قراءة بطاقات الائتمان، حيث يتم إدخال قيمة الشيك في الجهاز والضغط على زر الإدخال وعلى الفور تأتي النتيجة بقبول الشيك من عدمه طبقاً لتوفر رصيد قائم ويغطي قيمة الشيك من عدمه.

ويتم تطبيق نظام الشيك الذكي بقيام العميل بداية بالتقدم للبنك الخاص به، والمشارك بخدمات الشيك الجديد ويطلب الحصول على دفتر شيكات بعد سداد الرسوم التي يحددها البنك. ويقوم هذا الأخير بإصدار الدفتر المطلوب وحسب التعليمات المعتمدة من قبله، وبحيث يحتوي الدفتر على عدد معين من أوراق الشيك الجديد وعلى كل منها شريط مغنط و/أو خلية تخزين على بيانات تعريفية تشتمل على: رقم الشيك، رقم الحساب، وعناصر السيطرة الأمنية اللازمة. وفي الأخير يقوم العميل باستلام دفتر الشيكات الجديد حسب التعليمات المعتمدة لدى البنك².

ثانياً: الانترنت المصرفي

يراد بهذا النظام تعامل الزبون مباشرة مع حسابه من مكان تواجدته وإجراء العديد من العمليات المصرفية الخاصة به عن طريق الانترنت، إذ أتاح انتشار استخدام الانترنت للبنوك التعامل مع العملاء من خلال خدمات المصرف المنزلي، حيث يتم إنشاء مقر لها عبر الانترنت بدلاً من المقر العقاري، ومن ثم يسهل على العميل التعامل مع البنك عبر الانترنت وهو في منزله، ويمكنه محادثة موظف البنك على شاشة الكمبيوتر، ويتم إجراء كافة العمليات المصرفية بسهولة وبدون بذل أدنى جهد أو وقت.

وتتولى أجهزة هذه العمليات التي تتم عن بعد بتسهيل تعامل الأطراف وتوفير الثقة فيما بينهم، وتتولى البنوك بصفة أساسية، عبئ القيام بهذه المهمة، بالإضافة إلى منشآت أخرى يتم إنشاؤها لهذا الغرض³.

ثالثاً: النقود الالكترونية

لقد عرف القرار الأوروبي رقم 2000/46 الصادر في 2000/09/18 النقد الإلكتروني بأنه " قيم نقدية مخلوقة من المصدر مخزنة على وسيط إلكتروني وتمثل إيداعاً مالياً، تكون مقبولة كوسيلة دفع من قبل الشركات المالية غير الشركة المصدرة".

¹ نبيل صلاح محمود العربي، الشيك الإلكتروني والنقود الرقمية، دراسة مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 10-12 مايو 2003، ص ص. 66-69.

² موسى عيسى العامري، الشيك الذكي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 10-12 مايو 2003، ص ص. 87-88.

³ نهي خالد عيسى الموسوي، إسراء خضير مظلوم الشمري، النظام القانوني للنقود الإلكترونية، مجلة جامعة بابل، العلوم الإنسانية، المجلد 22، العدد 2، 2014، ص. 274.

وتعرف النقود الالكترونية كذلك على أنها " عملة نقدية إلكترونية تتمثل في الوحدات الرقمية الموثقة والخاصة بالقيمة المحددة من قبل الجهة المصدرة لها، والمخزنة على أداة أو وسيلة إلكترونية ليتم تحويلها من المشتري إلى البائع أو إلى أي جهة أخرى"¹.

بالرغم من كون النقود الالكترونية عبارة عن بيانات لقيم مالية مخزنة إلكترونيًا في الحاسب الآلي ودوائر التخزين، إلا أنها تقوم بنفس وظيفة النقود الاعتيادية عند توفر وسائل تبادلها عبر أدوات معينة كبطاقات الصراف وبطاقات الائتمان والمحافظ والحسابات الالكترونية، حيث يتم تداول قيمها إلكترونيًا عبر شبكات الكمبيوتر والاتصالات (مثل الانترنت) بين مالكيها والمستفيد.

وتعد أنظمة تحويل الأموال الالكترونية أكبر قنوات تبادل النقود على الإطلاق، من أشهر هذه الأنظمة نظام السويتف وشبكة المدفوعات الأوروبية، الذي ينقل من خلاله عشرات المليارات من الدولارات سنويًا بين مختلف دول العالم بدون الحاجة لنقل الأوراق النقدية².

المطلب الثاني: العمليات المصرفية الالكترونية

تتعدد العمليات المصرفية الالكترونية في القطاع البنكي نظرًا للحاجة الملحة لها، وأن أبرزها استعمالًا تتمثل في التحويل البنكي والاعتماد المستندي الإلكتروني.

الفرع الأول: التحويل البنكي

يمر التحويل المصرفي بغيره من العمليات المصرفية بعدة إجراءات، بداية من أمر العميل الموجه للمصرف بتحويل مبلغ من النقود، ثم قيام المصرف بتنفيذ عملية التحويل المصرفي بإجراء القيود المحاسبية اللازمة لها ونقل المبلغ المحول للمستفيد. يعتبر أمر التحويل العمل التحضيري لعملية التحويل المالي، وهو أمر يصدر عن صاحب الحساب موجهًا إلى المصرف للقيام بعملية التحويل المصرفي، ويفترض التحويل المصرفي وجود حساب يخصم فيه، وحساب آخر تضاف إليه القيمة المخصومة، ويفترض وجود الرصيد الكافي بحساب الأمر بالتحويل³.

ولقد أشار المشرع الجزائري إلى أحكام التحويل المصرفي من خلال المادتين 543 مكرر 19، حيث نصت على أنه " يحتوي الأمر بالتحويل على:

- 1 - الأمر الذي يوجهه صاحب الحساب إلى ماسك الحساب لتحويل الأموال أو القيم أو السندات المحددة القيمة.
- 2 - بيان الحساب الذي يتم الخصم منه.
- 3 - بيان الحساب الذي يتم التحويل إليه وصاحبه.
- 4 - تاريخ التنفيذ

¹ المرجع نفسه، ص. 266.

² علي محمد شلهوب، شؤون النقود وأعمال البنوك، شعاع للنشر والعلوم، سوريا، 2007، ص.ص. 96-97.

³ سعيد يحيى، الطبيعة القانونية للتحويل المصرفي، منشأة المعارف، مصر، 1987، ص. 19.

5 - توقيع الأمر بالتحويل".

ونصت المادة 543 مكرر 20 من نفس القانون: "يكون الأمر بالتحويل غير قابل للرجوع فيه ابتداء من تاريخ الإقترع من حساب الأمر بالتحويل.

يعتبر التحويل نهائيا ابتداء من تاريخ دخول المبلغ المحول إلى حساب المستفيد".

وعلى كل لم يعرف المشرع الجزائري التحويل المصرفي بل اكتفى فقط بذكر بياناته وإجراءات تنفيذه من خلال نصوص القانون التجاري، وبالرجوع إلى المادة 66 من قانون النقد والقرض الجزائري¹ التي تنص "تتضمن العمليات المصرفية تلقي الأموال من الجمهور وعمليات القرض وكذا وضع وسائل الدفع تحت تصرف الزبائن وإدارة هذه الوسائل".

وعرفت المادة 69 من نفس القانون وسائل الدفع على أنها: "تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل". وطبقا للمادة 70 من ذات القانون، فالبنوك يحول لها دون سواها بالقيام بالعمليات المحددة في المادة 66 السالفة الذكر، ومن بين هذه العمليات التحويل المصرفي باعتباره وسيلة دفع حديثة.

بخصوص التحويل البنكي الإلكتروني بين بنكين، يقوم بنك العميل الأمر بالتحويل بقيد المبلغ المراد تحويله في الجانب المدين من حساب عميله، ويطلب من بنك المستفيد أن يقيد مثل هذا المبلغ في الجانب الدائن من حساب المستفيد، على أن يضع بنك الأمر اثمانا بهذا المبلغ تحت تصرف بنك المستفيد، لأنه قيد مبلغا في حساب المستفيد ولا يعقل أن يقوم بنك المستفيد بأداء هذا المبلغ من ذمته المالية، ومن ثم تتم عملية التسوية بين البنكين².

الفرع الثاني: الاعتماد المستندي الإلكتروني

يتم تمويل التجارة الخارجية من خلال عمليات تمويل مختلفة، والتي ترتبط مع طبيعة النشاطات المراد تمويلها. فمن أجل تسهيل عمليات تبادل السلع والخدمات مع الخارج، والبحث عن أفضل الطرق التي تسمح بتوسيع التجارة الخارجية، والتخفيف من العراقيل التي تواجهها والتي ترتبط خاصة بالشروط المالية لتنفيذها، يسمح النظام البنكي باللجوء إلى عدة أنواع وطرق للتمويل.

ويعتبر الاعتماد المستندي أفضل وسيلة للتمويل في مجال التجارة الخارجية، وإحدى صور عمليات الاعتمادات المصرفية، بل وأفضل ضمان لكل من البائع والمشتري في مجال المبادلات التجارية الدولية.

ومع التطورات التكنولوجية وظهور عصر المعلوماتية، ظهر الاعتماد المستندي في صورته الجديدة، وعرف بالاعتماد المستندي الإلكتروني، والذي يتم الاعتماد بالأساس في التعامل على المستندات الإلكترونية التي حلت محل المستندات الورقية، وكذا يتم الوفاء عن طريق أنظمة الدفع الإلكترونية.

¹ الأمر 03-11 المؤرخ في 26 غشت 2003، المتعلق بالنقد والقرض، ج ر، العدد 52، المؤرخ في 27 أوت 2003، المعدل والمتمم.

² حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2014-2015، ص.86.

يعرف الاعتماد المستندي على أنه تلك العملية التي يقبل بموجبها بنك المستورد أن يحل محل المستورد في الالتزام بتسديد وارداته لصالح المصدر الأجنبي عن طريق البنك الذي يمثلته مقابل استلام الوثائق أو المستندات التي تدل على أن المصدر قد قام فعلا بإرسال البضاعة المتعاقد عليها¹.

كما عرفه البعض الآخر بأنه تعهد خطي صادر عن بنك المصدر إلى البائع (المستفيد) بناء على طلب ووفقا لتعليمات المشتري (طالب فتح الاعتماد) يتعهد به البنك المصدر بدفع مبلغ محدد أو قبول سحوبات زمنية بقيمة محددة ومقابل استلام المصدر لمستندات محددة².

إن الاعتماد المستندي الإلكتروني على أنه عبارة عن وسيلة دفع وضمنان في مجال التجارة الدولية شأنه في ذلك شأن الاعتماد المستندي التقليدي. وهذا الأخير يعد من ابتكارات الممارسة البنكية، ووسيلة وفاء آمنة تمكن البائع (المستفيد في العملية التجارية) من التغلب على المخاطر المرتبطة بعدم ملاءة المشتري (الآمر بفتح الاعتماد)، أو بسوء نيته، أو ببعد المسافة التي تفصل بينهما.

إن الوثائق والمستندات التي يتعامل بها أطراف العقد في الاعتماد المستندي الإلكتروني، مجردة من أية دعامة ورقية، وغير ملموسة وغير مادية، بل تتخذ الشكل الإلكتروني، أي أنها مستندات الكترونية، غير أن هذه الأخيرة لا تختلف في فحواها عن المستندات الورقية التقليدية المؤيدة للمعاملات التجارية الدولية، والتي تحتوي على توضيحات وبيانات ملائمة للتعامل بين المصدرين والمستوردين، ومن بين تلك البيانات، أسماء أطراف التعامل، واسم السفينة الشاحنة، وتاريخ الشحن، ورقم سند الشحن، واسم البنك، ورقم الاعتماد المستندي. وهي نفس البيانات التي يحتويها أي مستند الكتروني³.

لقد أفضى التقدم التقني إلى ظهور الاعتماد المستندي الإلكتروني، الذي تتم فيه الإجراءات السابقة عن طريق وسائل الاتصال الإلكتروني، فيقوم المستورد بإرسال طلب فتح الاعتماد الكترونيا، ويقوم البنك بالرد عليه بذات الوسيلة، فان قبل أرسل نص الاعتماد الكترونيا إلى المستفيد، وقبل انتهاء مدة صلاحية الاعتماد فان المستفيد يرسل الكترونيا الفواتير اللازمة المتعلقة بالشحن، كما يقوم المستفيد بإرسال رسائل الكترونية للأطراف المشاركة في عملية البيع مثل الشاحن والمؤمن والمفتش لما قبل الشحن، يطلب فيها إرسال مستنداتهم الكترونيا إلى البنك مصدر الاعتماد. ثم يقوم البنك مصدر الاعتماد بإرسال الرسائل الإلكترونية الواردة إليه إلى البنك المراسل⁴.

¹ الطاهر لطرش، تقنيات البنوك، ديوان المطبوعات الجامعية، الطبعة الثانية، الجزائر، 2003، ص. 117

² ماهر شكري، العمليات المصرفية الخارجية، دار الحامد للنشر والتوزيع، عمان، الأردن، 2004، ص. 226

³ ليندة عبد الله، تبييض الأموال عن طريق الاعتماد المستندي الإلكتروني، أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، طرابلس، 24-25 مارس 2017، ص. 4.

⁴ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المنعقد بتاريخ 10-12 ماي 2003، ص. 523.

ويرى البعض¹ إن ما زاد من أمل المتعاملين التجاريين في حقل التجارة الدولية من أجل الوصول إلى اعتماد مستندي الكتروني يتمثل في صدور آخر تعديل للقواعد والعادات الموحدة المتعلقة بالاعتماد المستندي نشرة رقم 500، وظهور القواعد والعادات الموحدة نشرة رقم 600 لسنة 2007 وملحقها المتعلق بالقواعد والعادات الموحدة الالكترونية، والذي يعد دفعا قانونيا لتطلعات المتعاملين في حقل التجارة الدولية من أجل اعتماد مستندي إلكتروني.

وقد ظهرت هذه القواعد في خضم التطور الهائل لوسائل التكنولوجيا في مختلف الميادين لاسيما عالم التجارة الدولية الذي عرف ازدهارا كبيرا في هذا المجال، في الوقت الذي سجل فيه غياب تام لأطر قانونية لمعلمة العمليات البنكية، لاسيما في مجال الاعتماد المستندي.

إن الهدف التي كانت ترمي إليه غرفة التجارة الدولية من خلال هذه القواعد هو إعداد المتعاملين التجاريين الدوليين لمرحلة انتقالية من عالم الورق إلى عالم المعلوماتية.

هذا ويعتبر هذا الملحق مكتملا للقواعد والعادات الموحدة نشرة رقم 600 لسنة 2007 من أجل استيعاب أفضل لتقديم السجلات الالكترونية سواء بمفردها أو مع وثائق ومستندات ورقية، وأن أحكامها لا تنطبق إلا في الحالة التي ينص فيها صراحة في عقد الاعتماد على ذلك².

المبحث الثاني: صور الاستخدام غير المشروع للنظام الرقمي المصرفي

إن التطور الكبير الذي عرفه مجال تكنولوجيا الإعلام والاتصال، فتح مجالا واسعا لممارسات سلبية تحولت معظمها إلى جرائم تعاقب عليها الأنظمة القانونية، وقد كانت البنوك مسرحا لهذه الجرائم من خلال الحاسوب أو الشبكات الحاسوبية.

المطلب الأول: الجرائم الواقعة على البنك الإلكتروني

اكتسب مفهوم البنك الإلكتروني مكانة بارزة مع ظهور التكنولوجيا المصرفية عبر الإنترنت، وعلى الرغم من أن العديد منها مملوك من قبل البنوك التقليدية يقدم عدد من البنوك الافتراضية فقط حساب توفير عبر الإنترنت، وعادةً ما تقدم هذه البنوك أسعار فائدة أعلى من منافسيها التقليديين، حيث يمكن أن تكون هذه البنوك فعالة جدًا فتزيد نسبة الفائدة كمقابل للتكلفة المنخفضة للتشغيل، وبالرغم من الإيجابيات التي تقدمها في خدمة العملاء إلا أنها لا تسلم من الاعتداءات التي تكون محل تكييف اجرامي من قبل المشرع بهدف حمايتها.

الفرع الأول: تقليد موقع البنك الإلكتروني على شبكة الانترنت

يعد تقليد الموقع الإلكتروني للبنك على شبكة الانترنت من أهم وأخطر الاعتداءات التي يمكن أن تحدث للبنك وأكثر شيوعا.

¹ سعدي عبد الحليم، الأرضية القانونية للاعتماد المستندي، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، العدد 9، ماي 2013، ص ص. 97-98.

² المادة 1 من ملحق الأصول والأعراف الموحدة للاعتمادات المستندية (نشرة رقم 600 لسنة 2007) للتقديم الإلكتروني.

وتتمثل هذه الصورة في محاولة المعتدي تقليد الموقع الإلكتروني للبنك على شبكة الانترنت، في ذات الصميم، وبحمل ذات الشعارات وعدد الصفحات، وأن نشئ به ذات الروابط، وذلك على نحو يظهر معه الموقع المقلد وكأنه الموقع الحقيقي للبنك الإلكتروني.

ويلاحظ أنه لا يشترط أن يظهر الموقع المقلد ماثلاً ومطابقاً للموقع الحقيقي، بل يكفي أن يتسبب الموقع المقلد في إحداث لبس أو خلط لدى العملاء على نحو يدفعهم للتعامل معه على أنه الموقع الحقيقي للبنك، وذلك كما لو قام المعتدي بتقليد العناصر الأساسية المميزة لموقع البنك كعلامته التجارية أو اسمه التجاري¹.

وتقوم المسؤولية الجنائية لمقلد الموقع الإلكتروني للبنك على شبكة الانترنت، على تقليدهم العناصر التي تميز الموقع الإلكتروني، باعتبارها العناصر التي يعتمد عليها العملاء في التعامل مع موقع البنك، فيقومون بتقليد العلامة التجارية والعنوان الإلكتروني وصفحات الويب الخاصة بالبنك الإلكتروني بذات التصميم وعدد الصفحات.

ويعاقب قانون الملكية الفكرية المصري لسنة 2002 في هذا الصدد في الفقرة الأولى من المادة 113 على تزوير العلامة التجارية، حيث ينص على أن " يعاقب بالحبس مدة لا تقل عن شهرين وبغرامة لا تقل عن خمسة آلاف جنيه أو بإحدى هاتين العقوبتين كل من زور علامة تجارية تم تسجيلها طبقاً للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور".

الفرع الثاني: تعطيل نظام عمل البنك على الانترنت

ظهر شكل جديد من أشكال الهجمات التي تستهدف موقع البنك الإلكتروني على شبكة الانترنت، وهو ما يطلق عليه بتعطيل النظام، وتسعى مثل هذه الهجمات إلى منع وحرمان عملاء البنك من الوصول إلى موقعه الإلكتروني على شبكة الانترنت للحصول على الخدمات التي يقدمها.

ويعرف تعطيل النظام الإلكتروني بأنه " نوع من الهجمات الإلكترونية المصحوبة بنوايا خبيثة، تهدف إلى إغراق أو تعطيل الموقع الإلكتروني بكثرة الطلبات، على نحو يتسبب في إغلاق الموقع، وحرمان العملاء من الحصول على الخدمة التي يقدمها هذا الموقع².

في هذا الصدد يخلو قانون العقوبات المصري من نص خاص ينظم الإخلال بالنظام كنشاط إجرامي، بل حتى الصور التقليدية للجرائم المعروفة في هذا القانون، غير قادرة على أن تستوعب هذا النشاط.

وتضمنت المادة 323-2 من قانون العقوبات الفرنسي ما يفيد تجريم هذا النشاط، حيث نصت على أن " يعاقب على الإعاقة أو الإخلال بسير نظام معالجة المعلومات، بالحبس مدة لا تزيد على خمس سنوات والغرامة التي لا تزيد على خمس سنوات والغرامة التي لا تزيد على 300 ألف يورو".

الفرع الثالث: الدخول غير المشروع لنظم البنك الإلكتروني على شبكة الانترنت

¹ علاء التميمي، التنظيم القانوني للبنك الإلكتروني على شبكة الانترنت، دار الجامعة الجديدة، مصر، 2011، ص 550-551.

² علاء التميمي، المرجع نفسه، ص 566-567.

يعد اقتحام النظام الإلكتروني للبنك من خلال الدخول غير المشروع إلى النظام الداخلي الخاص بالبنك من أخطر صور الانتهاكات التي يمكن أن يتعرض لها البنك، وتعلل هذه الخطورة بأن الدخول غير المشروع للبنك هو بمثابة حلقة أولى من سلسلة الانتهاكات.

فقد يقوم المعتدي بعد الدخول بالمساس بسرية البيانات الموجودة لدى البنك، وذلك من خلال الاطلاع عليها، وقد يقوم بالمساس بسلامة هذه البيانات الموجودة لدى البنك، وذلك من خلال تعديلها أو محوها، وقد يقوم بزراعة الفيروسات لتدمير الملفات المخزنة، وقد يقوم باستخدام أنظمة البنك الإلكتروني كأداة لارتكاب الجريمة (كما لو قام بإجراء تحويلات غير مشروعة، أو سرقة بطاقات الائتمان، أو نشر مواد غير قانونية على موقع البنك)، بل قد يسعى المعتدي إلى إفقاد القائمين على إدارة البنك السيطرة عليه، وذلك كما لو تمكن بعد الدخول إلى نظام البنك الداخلي من تغيير كلمة المرور، حيث لن يستطيع أحد الدخول على نظام البنك غيره.¹

يتضح أن المشرع الجزائري فرض حماية خاصة على أنظمة المعالجة الآلية للمعطيات أو البيانات في المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري.

وقد تم ذلك بتقرير جريمة الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، ومن ثم فقد جرم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات، فجرم الدخول غير المصرح به إليهما، كما جرم البقاء فيها بغير تصريح، وإذا نجم عن هذا التواجد غير المشروع داخل النظام محو أو تعديل لمعطياته فان العقوبة تتشدد². وعلى اعتبار أن الدخول هو الركن المادي لجريمة فعل الدخول عن طريق الغش لنظام المعلوماتية، والذي يشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي والسيطرة على المعطيات التي يتكون منها والخدمات التي يقدمها³. وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية. والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الإلكتروني، ويقصد بالدخول أيضا الاتصال بجهاز حاسب آلي خاص بشخص الغير بدون موافقته⁴.

¹ المرجع نفسه، ص 580-581.

² تنص المادة 394 مكرر ق.ع.ج على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50 ألف دج إلى 100 ألف دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة بالحبس من ستة أشهر إلى سنتين وبغرامة 50 ألف دج إلى 150 ألف دينار جزائري"، وتقابل المادة 6 من المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج.ر، العدد 57، المؤرخة في 28 سبتمبر 2014.

³ بوخيزة عائشة، الحماية الجزائرية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013، ص.65.

⁴ نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان، الأردن، 2008، ص.158.

ويتخذ الدخول صوراً مختلفة؛ فمنها أن يقوم الفاعل بتشغيل جهاز مغلق وبالتالي الاطلاع على ما به من بيانات. ومنها ما يقوم به الفاعل من استخدام برامج للدخول في النظام بدون إذن صاحبه فيطلع على ما يقوم به صاحب الجهاز أو ينتقل بين أجزاء الجهاز ليطلع على ما يحتويه أقسام هذا الجهاز من معلومات.

وهكذا يقوم التجريم لفعل الدخول بغير إذن إلى نظام المعلومات، سواء كان النظام موصولاً بالشبكة أم لا، وبصرف النظر عن طبيعة النشاط المتبع في الدخول، فقد يكون بالدخول المباشر إلى النظام عن طريق تجاوز جدران الحماية أو عن طريق الالتقاط الهوائي. كما أن الدخول إلى جزء من الأجزاء التي يتكون منها النظام لمعلوماتي هو بمثابة الدخول إلى النظام ككل¹.

كما أنه لم يشترط أن يتم الدخول بوسيلة أو طريقة معينة، أي أنها شاملة بكل طرق الدخول ولم تحدد طريقة بعينها². وجدير بالذكر أن الدخول غير المشروع يبدأ منذ اللحظة التي يصبح فيها الفاعل قادراً على الاطلاع البصري أو السمعي لمحتويات النظام المعلوماتي³.

إن عدم مشروعية الدخول أو ما يعبر عنه بالدخول بطريق الغش يعني الدخول غير المسموح به من قبل من له السلطة في الدخول إلى نظام الحاسب الآلي⁴.

ويكون الدخول إلى النظام المعلوماتي غير مصرحاً به في حالتين⁵:

1- حالة عدم وجود التصريح، بمعنى أن الشخص الذي أقدم على الدخول إلى النظام المعلوماتي، لا يجوز على تصريح يخول له القيام بذلك مطلقاً.

2- حالة تجاوز حدود التصريح، وفي هذه الحالة يقوم الشخص الذي خول له التصريح بالدخول للأنظمة المعلوماتية بتجاوز الحدود التي رسمت له بموجبه، وتتم هذه الحالة عموماً من طرف العاملين في المؤسسة المسؤولة عن النظام التابع لها، فهم يمتلكون عادة تصريح جزئي بالدخول يشمل مناطق محددة من النظام بحسب الوظيفة التي يؤديها كل عامل.

إن جريمة الدخول أو البقاء إلى نظام المعالجة الآلية بطرق غير مشروع، يتطلب القصد فيها علم الجاني بأنه يدخل إلى نظام المعالجة الآلية للمعطيات الخاصة بالغير، وأن تتجه إرادته إلى ارتكاب هذه الجريمة، أي أن اكتمال هذه الجريمة يستدعي توافر الركن المعنوي.

¹ وسيم طعمة، السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، المجلد 39، العدد 68، 2017، ص 166-167.

² بوخبرة عائشة، المرجع نفسه، ص 67.

³ وسيم طعمة، المرجع نفسه، ص 168.

⁴ وسيم طعمة، المرجع السابق، ص 168.

⁵ بوخبرة عائشة، المرجع السابق، ص 69-70.

وعليه لا يتوافر الركن المعنوي إذا وقع الجاني في خطأ، كما لو كان يجهل بوجود خطر الدخول (أو البقاء)، أو كان يعتقد خطأ أنه مسموح له بالدخول¹.

المطلب الثاني: جرائم بطاقات الدفع الالكترونية

بطاقة الدفع الالكترونية أو محفظة النقود الالكترونية هي وسيلة دفع افتراضية تستخدم في سداد المبالغ قليلة القيمة بشكل مباشر أو غير مباشر، ويعني ذلك أن لبطاقة الائتمان وظيفتين وظيفة وفاء سواء كان ذلك الوفاء فوري أو مؤجل لمدة متفق عليها في العقد، ووظيفة سحب النقود من خلال الأجهزة الآلية لتوزيع النقود. وهكذا إذا كان لهذا الاكتشاف التكنولوجي آثار إيجابية، فإنه قد ينجر عنه آثار سلبية، جعلت التشريعات تتسابق من أجل وضع تقنين يجرم الاعتداءات الواقعة على البطاقات البنكية.

الفرع الأول: جريمة تزوير البطاقة البنكية

قد تضيع البطاقة البنكية من حاملها الشرعي أو تتعرض للسرقة من قبل الغير، فيقوم هذا الأخير بتغيير حقيقتها باستبدال البيانات التي كانت تحملها تلك البطاقة ببيانات ومعلومات مزورة، ثم يقوم باستخدامها في عمليات الشراء والسحب، وهذا يشكل اعتداء وجرما مرتكبا ضد كل من البنك المصدر للبطاقة البنكية والحامل الشرعي لها.

ويشكل الفعل المرتكب جريمة تزوير للبطاقة البنكية، وهو الفعل المعاقب عليه بموجب المواد من 214 إلى 229 من قانون العقوبات. ويتمثل الركن المادي لجريمة تزوير المحررات في تغيير الحقيقة في محرر يشكل سنداً بإحدى الطرق التي نص عليها القانون تغييراً من شأنه أن يسبب ضرراً، ومنه يمكن حصر عناصر الركن المادي في²:

- طبقاً لمواد قانون العقوبات يلزم لتحقيق الركن المادي لجريمة التزوير أن يكون تغيير الحقيقة حاصلًا في محرر يشكل سنداً، وبما أن البطاقة البنكية تدخل ضمن مسمى المحررات لأنها تمثل محرراً مصرفياً.

- كما أن الضرر هو عنصر مهم لقيام الركن المادي لجريمة تزوير المحررات، وبالتطبيق على جريمة تزوير البطاقة البنكية فإن وقوع الضرر مفترض، وهو يلحق كلا من البنك المصدر للبطاقة والحامل الشرعي لأنهما طرفي العلاقة التعاقدية المنتجة للبطاقة البنكية، وبالتالي فإن أي اعتداء عليها يعد فعلاً ضاراً مادياً ومعنوياً لكليهما.

وكما أن جريمة التزوير من الجرائم العمدية، إذ تتطلب لقيامها توافر القصد الجنائي، ومن خلال ماسبق وتطبيقاً في مجال تزوير البطاقات البنكية من قبل الغير، فقد يقوم هذا الغير بالتزوير عن طريق عملية النسخ للبيانات الموجودة على الشريط المغنط للبطاقة، أي الحصول على خصائص الهوية الالكترونية من البطاقة الصحيحة ثم يقوم بنقلها إلى بطاقة

¹ وسيم طعمة، المرجع نفسه، ص. 169.

² خشة حسية، وسائل الدفع الحديثة في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2015-2016، ص. 123-125.

أخرى، ويتم نسخ تلك البيانات عن طريق جهاز الكمبيوتر، وكل هذا يحصل رغبة من الجاني في الاستفادة من تلك البطاقة المزورة في القيام بعمليات الشراء والسحب¹.

تقتضي أنه من ارتكب جريمة التزوير في المحررات العرفية التجارية أو المصرفية يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة مالية، ويعاقب على الشروع بنفس العقوبة المقررة للجريمة الكاملة.

الفرع الثاني: استعمال بطاقة ائتمان مزورة

لقد أجمع الفقه والقضاء على مساءلته جنائيا وفقا لنصوص قانون العقوبات وإن اختلفوا فيما بينهم حول نوع الجريمة التي يسأل عنها: فهناك من يرى مساءلته عن جريمة السرقة باستعمال مفتاح مصطنع، وهناك من يرى مساءلته على جريمة استعمال محرر مزور، وبهذا فقد وجد رأيين في هذا الصدد²:

هناك من اعتبر استعمال بطاقة ائتمان مزورة دون أن يكون هو الذي زورها جريمة سرقة باستعمال مفتاح مصطنع، حيث يتم مساءلة مرتكب الواقعة عن جريمة سرقة مشددة لاستعماله مفتاح مصطنع، إذ أن المال خرج من حيازة المجنى عليه بغير رضائه، وأن البطاقة المزورة تعد من قبيل المفتاح المصطنع المنصوص عليه في قانون العقوبات، على أساس أن المفتاح المصطنع هو كل أداة تقوم بذات الوظيفة التي يقوم بها المفتاح بغض النظر عن شكلها أو حجمها أو المادة المصنوع منها، خاصة وأن البطاقة في حقيقتها مجرد أداة للوصول إلى سحب النقود، فالجهاز يعتبر خزانة نقود والرقم السري لبطاقة الائتمان هو المفتاح الذي الذي يفتح به الجاني خزانة النقود.

غير أنه تم انتقاد هذا التكييف من خلال أن تسليم النقود تم إراديا من قبل الجهاز الآلي لتوزيع النقود بمجرد إدخال البطاقة في الآلة وكتابة الرقم السري لها، فضلا على أن بطاقة الائتمان لا تعد مفتاحا مصطنعا لأن المفتاح المصطنع هو الذي يستخدم للدخول في المكان الذي يرتكب فيه جريمة سرقة، وهو مالا يتوافر في بطاقة الائتمان.

إلا أن غالبية التشريعات اعتبر هذه الواقعة جريمة استعمال محرر مزور وفقا لنصوص قانون العقوبات وذلك لتوافر أركان هذه الجريمة، إذ أن موضوع الجريمة يرد على كل محرر مزور وهو هنا بطاقة الائتمان المزورة كما يشترط في النشاط المادي لجريمة استعمال محرر مزور أن يحتج بالمحرر المزور على أنه صحيح وهو ما حدث في هذه الواقعة، حيث استعمالها حائزها في سحب النقود أو الوفاء لدى أحد التجار، وبشرط كذلك أن ينخدع التاجر أو الآلة (الموظف المختص) بها وهو

¹ المرجع نفسه، ص. 127.

² محمود أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، بحث مؤتمري الأعمال المصرفية الالكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص. 1143-1145.

ما حدث بالفعل حيث تمكن من السحب أو الوفاء، فضلا عن توافر القصد الجنائي لدى مستعملها فهو يعلم بأنها مزورة وتنصرف إرادته إلى استعمالها فيما زورت من أجله.

خاتمة:

إن مساهمة التطور التكنولوجي في مجال الاتصالات وتقنيات المعلومات في سرعة انتشار المعلومات وسهولة تداولها عبر خدمات الانترنت، قد أدى إلى ظهور العديد من المخاطر والاعتداءات التي تتم في بيئة الانترنت، الأمر الذي أدى إلى ضرورة وضع تشريعات تحمي أمن المعلومات، ولا سيما في المجال البنكي.

ومن النتائج المتوصل إليها، هو امتداد المعلوماتية إلى قواعد القانون التجاري، وأثرت بالخصوص على أحكام المعاملات المصرفية، بسبب ما أوجدته من وسائل الدفع الإلكتروني، وبفعل المفهوم المستحدث للنقد (المال الرقمي)، ومن جهة أخرى فقد أفرزت تقنية المعلومات وسائل حديثة لتقديم الخدمات المصرفية وإدارة العمل البنكي، إضافة لوسائل الدفع الإلكتروني، عمليات التحويل المصرفي الإلكتروني والاعتماد المستندي الإلكتروني.

لقد ازداد اعتماد المصارف على التقنية في بيئة عمل تنافسية بشكل متسارع، وبالتالي يجب عليها إدارة أمن تقنية المعلومات والمخاطر الأخرى المتعلقة بها، بل أكثر من ذلك، أصدرت لجنة بازل للرقابة المصرفية في عام 2003 " مبادئ إدارة المخاطر المصرفية الإلكترونية".

ولغرض فاعلية المعلوماتية في المجال المصرفي الذي ينعكس إيجابا على أدائها واجتذاب العملاء، نوصي بالتصدي للمخاطر المصرفية الإلكترونية كالبرمجيات الخبيثة والذهاب إلى قدسية أمن المعلومات.

كما نوصي بضرورة التدخل بوضع نصوص خاصة صريحة لمعالجة الاعتداءات الماسة ببطاقات الدفع الإلكتروني.

قائمة المراجع:

1. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المنعقد بتاريخ 10-12 ماي 2003.
2. بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013.
3. حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2014-2015.
4. خشة حسبية، وسائل الدفع الحديثة في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2015-2016.

5. سعدي عبد الحليم، الأرضية القانونية للاعتماد المستندي، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، العدد 9، ماي 2013.
6. الطاهر لطرش، تقنيات البنوك، ديوان المطبوعات الجامعية، الطبعة الثانية، الجزائر، 2003.
7. علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، دار الجامعة الجديدة، مصر، 2011.
8. ليندة عبد الله، تبييض الأموال عن طريق الاعتماد المستندي الالكتروني، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، طرابلس، 24-25 مارس 2017.
9. ماهر شكري، العمليات المصرفية الخارجية، دار الحامد للنشر والتوزيع، عمان، الأردن، 2004.
10. محمود أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، بحوث مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.
11. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان، الأردن، 2008.
12. وسيم طعمة، السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، المجلد 39، العدد 68، 2017.