الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد لمين دباغين

سطيف-2-

المسؤولية الجزائية عن استخدام وسائل الدفع الإلكتروني في القانون الجزائري

بحث مقدم نيل درجة الدكتوراه في القانون

إعداد الطالبة:

غزالي نزيهة

تحت إشراف الأستاذ الدكتور:

بلمامي عمر

لجنة المناقشة:

الأستاذ الدكتور: بوضياف عبد الرزاق جامعة محمد لمين دباغين-سطيف2- رئيسا

الأستاذ الدكتور: بلمامي عمر جامعة محمد لمين دباغين-سطيف2- مشرفا ومقررا

الدكتـــور : بـن زيوش مبروك جـامعة محمد لمـين دبـاغين- سطيف2- ممتحنا

الدكتـــور : قـارة مـولـود جـامعـة محـمـد بوضيـاف - مسيلـة - ممتحنـا

الدكتـــور : موكا عبد الكريم جامعة محمد الصـديق بن يحي - جيجل - ممتحنا

الدكتـــورة : زايـدي أمـال جـامعة محـمد لميـن دباغيـن - سطيف2 - ممتحنا

تاريخ الايداع :2018/2017

إهداء

إلى والدي أطال الله في عمرهما

إلى إخوتي وأخواتي

إلى كل الأحباب

إلى روح كل من فارقنا من الأحبة :

سهيلة، جدي، الطاهر ، سمير

رحمهم الله

رجـــاء

رجائي من كل من سيسمح له وقته بتصفح

هذه المذكرة أن يدعوا لهم بالرحمة

نزيهة

شكر وتقدير

أتقدم بأسمى عبارات التقدير والاحترام إلى أستاذي الفاضل

الأستاذ الدكتور: بلمامي عمر الذي أعتبره كوالدي أطال الله في عمره

وإلى أساتذتي الأفاضل الأستاذ الدكتور: بوضياف عبد الرزاق، الدكتور: بن زيوش مبروك، الدكتور: قارة مولود، الدكتور: موكة عبد الكريم، الدكتورة: زايدي أمال.

أتقدم إليهم بخالص الشكر على ما سيخصصونه لي من وقتهم

وما سيبدونه من ملاحظات تنير دربي

نزيهة

مقدمة

أحدثت ثورة تكنولوجيا المعلومات تجديدات في القطاع التجاري والمصرفي على وجه الخصوص وأصبح الحديث عن ثورة أصغر وفي نطاق أضيق ألا وهي التكنولوجيا المصرفية التي أخذت نتائجها وافرازاتها تشق الطريق لتحتل مكانة ليست بالهينة في واقع العمل المصرفي، واستحداثها وسائل دفع إلكتروني فاقت في أهميتها الوسائل التقليدية المعروفة وهذا بالنظر إلى ما توفره هذه الوسائل من تكلفة أقل، وسهولة في الدفع والتعامل الكبير بها على المستوى الدولي، وعدم كشفها لهوية الأشخاص المتعاملين بها مقارنة بالوسائل التقليدية للدفع مع ملاحظة الانتشار المحتشم لها داخليا (في الجزائر) مما أتاح للمصارف أن تلعب دورا متزايدا في خلق الائتمان وهذا بالنظر لدور المصارف كعصب محرك للاقتصاد الوطني والعالمي.

لكن أمام هذه الايجابيات لوسائل الدفع الإلكتروني ظهرت أساليب وطرق للتلاعب والتحايل باستعمالها مما يمثل تهديدا للمتعاملين بها من جهة، وتهديدا للاقتصاد الوطني والدولي من جهة أخرى ويسعى المصرفي إلى الحرص على توفير الثقة والأمان للزبائن إلا أن استعمال هذه الوسائل أفرز نوعا جديدا من المشاكل مما أصبح معه الأمان يكتسي شكلا جديدا خاصة أمام خطرها من الناحية المعلوماتية، لذلك تعتبر الجرائم المتعلقة بوسائل الدفع الإلكتروني جرائم معلوماتية من جهة، وجرائم تقليدية من جهة أخرى تمثل الجانب المادي لجرائم الاستعمال غير المشروع لهذه الوسائل، هذه الجرائم عاودت الظهور

بأشكال جديدة واستخدمت في ارتكابها أساليب مستحدثة ومعقدة فهي تتضمن نوع من الخصوصية لأنها تتضمن مجرما جديدا، ومفاهيم جديدة ومسرحا جديدا يشمل العالم بأسره (ولو افتراضيا).

ومنه جاءت فكرة هذه الرسالة نتيجة التحديات القانونية الواضحة للقوانين التي وضعت لمكافحة جرائم تقليدية مادية في حين لم يتصور المشرع حدوث جرائم أخرى معنوية ونتج عن ذلك مشكل تفسير النصوص القانونية، وحظر القياس في المادة الجنائية لأنه لا قياس لغاية التجريم وحتى لا يفلت الجناة ببعض الصور المستحدثة من الوصف القانوني وبالتالي الافلات من العقاب، ولضمان عدم المساس بمبدأ الشرعية الجنائية حيث لا جريمة ولا عقوبة إلا بنص مما يستلزم علينا مواجهة تشريعية لهذا النوع المستحدث من الجرائم.

ما سنقوم به هو دراسة تحليلية للمسؤولية الجزائية عن استعمال وسائل الدفع الإلكتروني ومدى شمولية النصوص العقابية لمواجهة أكثر صورها الاجرامية استحداثا وخطورة لأن هذا إن دل على شيء فهو يدل على ضعف الضمانات القانونية المتوفرة لمواجهة كل اساءة لاستخدامها واختراق لنظامها الإلكتروني.

شهدت وسائل الدفع الإلكتروني تطورا ملحوظا في الجزائر في السنوات الأخيرة وهذا لعصرنة منظومة الدفع الإلكتروني بصفة خاصة وعصرنة النظام المصرفي عموما، حيث اهتمت المصارف بتطوير وسائل الدفع الإلكتروني التقليدية لاستغلالها في أنظمة الدفع

بين البنوك منها نظام غرفة المقاصة الإلكترونية وأنظمة التحويل الإلكتروني للأموال، وظهرت وسائل جديدة لاستقطاب الزبائن.

مواكبة لهذا الوضع الجديد عدل المشرع الجزائري القانون التجاري واكتفى بإضافة بعض وسائل الدفع لباب السندات التجارية باعتبارها لم تكن مقننة من قبل منها التحويل، البطاقات، والاقتطاع دون أن يرافقه بمواد جزائية واقتصر التعديل على مواد مقتضبة، في حين شهد القطاع المصرفي الجزائري كذلك تطوير لأنظمة الدفع الإلكتروني خاصة ما بين البنوك بإشراف بنك الجزائر حيث تم اصدار النظام رقم 04/05 المتعلق بالتسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل [1]، والنظام رقم 06/05 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى[2]، كما اهتم بنك الجزائر بأمن الدفع الإلكتروني فأصدر النظام رقم 07/05 المتضمن أمن أنظمة الدفع[3]، وتم إحداث الهوية البنكية للزبائن، وتقيس وسائل الدفع الإلكتروني بداية بالشيكات وهذا لضمان عملية التحويل بين البنوك، وبين البنوك وبريد الجزائر ولتفادي مشكل الشيكات بدون رصيد قامت البنوك بتبني الاقتطاع في تعاملها مع الزبائن.

يتصف المسار الجزائري في تطوير الدفع الإلكتروني بالبطيء إلا أن الأخذ بالحسبان للمخاطر المرتبطة بوسائل الدفع الإلكتروني، ومخاطر الصيرفة الإلكترونية ككل ألزم على السلطات الجزائرية هذا النهج حتى لا تقع في فخ آخر يهدد القطاع المصرفي اضافة إلى

[1]- نظام مؤرخ في 15 ديسمبر سنة 2005 الموافق ل13 ذو القعدة عام 1426، ج ر عدد26، 2006.

[2]- نظام مؤرخ في 15 ديسمبر سنة 2005 الموافق ل13 ذو القعدة عام 1426، ج ر عدد26، 2006.

[3]- نظام مؤرخ في 15 ديسمبر سنة 2005 الموافق ل13 ذو القعدة عام 1426، ج ر عدد26، 2006.

الفضائح التي شهدها من قبل، وهذا كذلك مما يحذر منه المختصون في هذا المجال لأن الانبهار بالمزايا التي تقدمها وسائل الدفع الإلكتروني يجب ألا يحجب عن أعيننا المخاطر غير المتوقعة خاصة أمام المعطيات الحالية عن القطاع المصرفي.

القيام بالإصلاحات المصرفية لعصرنة الجانب الإلكتروني يحتاج لتطوير البنية التحتية، بالإضافة إلى ضرورة التحكم في الجانب المتعلق بالأمن الإلكتروني وليس المهم تقليص الوقت لتعميم الدفع الإلكتروني إنما المهم أن نؤسس للبنية التحتية للاقتصاد الرقمي، لأننا سنصبح عرضة لأي هجوم إلكتروني مما يستلزم الاهتمام بالجانب التقني وتأمين العمل بوسائل الدفع الإلكتروني من خلال تقنيات (التوقيع والتشفير والتصديق) الإلكتروني وهذا ما تم بإصدار قانون خاص بالتوقيع والتصديق الإلكترونيين[1].

يحتاج التعامل بوسائل الدفع الإلكتروني إلى تأمين آخر هو التأمين القانوني لأننا سنواجه خطرا جديدا وهو الخطر القانوني ونعني به المسؤولية المترتبة عن استخدامها هذه الأخيرة وإن كنا شرعنا لحماية وسائل الدفع التقليدية، إلا أننا في الجزائر نحتاج إلى تطوير المواجهة التشريعية للجريمة المرتبطة باستعمال وسائل الدفع الإلكتروني التي أصبحت خطر استراتيجي يهدد استخدامها.

الجنوح في مجال وسائل الدفع الإلكتروني ساهم في ارتقاء الجريمة الاقتصادية والمالية فأصبحت عالمية معقدة لاستغلال الشبكات الرقمية في تطوير السلوكات غير القانونية

[1]– القانون رقم 04/15 المؤرخ في 01 فيفري 2015، الموافق ل 11 ربيع الثاني عام 1436، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد06، 2015.

فأصبحنا أمام تبييض إلكتروني للأموال وتزوير واحتيال باستعمال وسائل الدفع الإلكتروني والاستيلاء على المعطيات ذات الطابع الشخصي خصوصا المصرفية فالوقت الحالي ليس لعمليات السطو الكلاسيكية إنما لعمليات السطو الرقمية الأقل خطورة والأكثر ربحا.

في الواقع الاقتصاد الحديث لم يسلم من تكنولوجيا المعلومات التي لها عديد الفوائد إلا أن المجال التشريعي أصبح يتحمل ضرر التأثير خاصة القانون الجنائي العام أو القانون الجنائي الخاص أو القانون الجنائي للأعمال أو بصفة أوسع القانون الاقتصادي والمالي[1]، فوسائل الدفع الإلكتروني سمحت للمجرمين تنفيذ عملياتهم الاجرامية بسرعة فائقة من أي مكان مخترقين الحدود الاقليمية للدوال، وسهلت الجنوح الاقتصادي المالي لاسيما باستغلال الشبكات الرقمية لأنه بالإمكان القيام بعدة تحويلات ضخمة واسترجاع تلك المبالغ في وقت قصير واستعمال معطيات مصرفية وبخطورة أقل.

الجريمة الإلكترونية أصبحت حاضرة يوميا مع الأشخاص لأنها مرتبطة بهواتفهم النقالة، حواسيبهم الشخصية فحضور الجاني ليس ضروريا لأن هذه الجرائم يمكن ارتكابها عن بعد بل عادة يختار المجرمون التواجد بالدوال التي يكون فيها القانون الجنائي الأضعف للتصدي لهذه الأعمال، ومن المحتمل أن تؤثر الجريمة المرتبطة باستعمال وسائل الدفع

[1] -Myriam Quéméner, criminalité économique et financière à l'ère numérique ,pratique de droit, collection dirigée par Nicolas Molfessis, economica.p18 .

الإلكتروني على ثقة الزبائن اتجاه المصرف وأن تمثل خطرا حقيقا خاصة إذا تسبب في قطع المؤسسات المالية والمصارف والتجار المعتمدين لها لتعاملاتهم مع المصرف.

الأرقام تبين أن الجريمة الاقتصادية والمالية تستمر في الزيادة بسرعة أساسا تحت تأثير تكنولوجيا المعلومات الجديدة و تزايد الصيرفة الإلكترونية واستعمال الانترنت والأدوات المتصلة بها أصبح أمرا عاديا وهذا ما يفسر كون المصارف والمؤسسات المالية هي أولى ضحايا مجرمي المعلوماتية الباحثين عن الربح بسهولة[1].

الاستغلال السلبي لتكنولوجيا المعلومات والاتصالات الجديدة سمح بإنشاء أنواع جديدة من الجرائم، وهذا ما يشكل ظهور أوضاع قانونية لجرائم لم تعرف من قبل وهذا ما يؤدي إلى خسارة العديد من الحقوق ومكافحة للجريمة الإلكترونية التي تتطور باستمرار يستلزم علينا تجريم المخالفات المتعلقة بالدفع الإلكتروني حتى يواكب التشريع الثورة التكنولوجية المصرفية لأن غياب العقوبات الجزائية يحفز المجرمين على تطوير قدراتهم وبالنتيجة المساهمة في زيادة هذا النوع من الجرائم، وبالتالي إقرار حماية قانونية جزائية للدفع الإلكتروني شيء ضروري لأنه يسمح من جهة بالمتابعة القضائية للمجرمين ومن جهة أخرى يسمح بمكافحة مخالفاتهم الإجرامية[2].

---

[1]-Myriam Quéméner , criminalité économique et financière à l'ère numérique ,pratique de droit, collection dirigée par Nicolas Molfessis, economica, p31.

[2]-Hatem Adnan Bezzo, le paiement électronique en matière d'opérations bancaires et de commerce en ligne, thèse en vue de l'obtention du doctorat, université de Toulouse, 2012, p200.

المشرع الجزائري لم يتدخل لإقرار هذه المسؤولية بنص جزائي واضح مما يدفعنا إلى محاولة استخلاص هذه المسؤولية من خلال النصوص العقابية الموجودة ومحاولة وضع أسس جديدة للمسؤولية الجزائية عند استخدام هذه الوسائل الحديثة واللامادية، وفي الوقت الراهن ليس أمامنا حل سوى اللجوء إلى القواعد التقليدية لتجريم هذه السلوكيات مع ما يصاحب ذلك من مشكلات معقدة لأن هذه القواعد وضعت لتطبق وفقا لمعايير معينة لمنقول مادي وليس بوسعها معالجة المعلومة موضوع الجريمة وإعمال النصوص التقليدية يثير مشكلة التكييف القانوني للفعل ومحدوديته فالمشرع الجزائري لم يشر في تعديله لهذا النوع من الجرائم، إضافة إلى صعوبة تحديد الأطراف المسؤولة جزائيا عن الجريمة التي تتم باستخدام هذه الوسائل والمتدخلين من مستخدمها ومصدرها والتاجر والغير حيث يصعب الوصول إلى الفاعل الحقيقي.

الوضع في الجزائر مازال في بداية تكوينه عكس الوضع في الخارج أين يتزايد استخدام هذه الوسائل على حساب وسائل الدفع التقليدية، مما يدفع مصدريها إلى تطوير نظام الدفع وتطوير أنظمة الأمان المصاحبة لها كما أن المسؤولية المدنية وحدها لا تكفي للردع لذا لابد من إقرار المسؤولية الجزائية.

شهدت الجزائر سنة 2018 قفزة تشريعية على مستوى التشريعات المتعلقة بالجانب الإلكتروني منها اصدار قانون خاص بالبريد والاتصالات الإلكترونية[1] وقانون خاص

[1]- القانون رقم 18-04 المتعلق بالبريد والاتصالات الإلكترونية، المؤرخ في 10 ماي 2018 الموافق لـ24 شعبان 1439، ج ر عدد27، 2018.

بالتجارة الإلكترونية[1] وقانون يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2] وهي اصلاحات لطالما انتظرناها في هذا المجال ولازلنا ننتظر اصلاحات أخرى ترتبط بمواجهة الجرائم المتعلقة باستعمال وسائل الدفع الإلكتروني حتى لا نصطدم بمبادئ القانون الجنائي، خاصة وأن المصارف اليوم أصبحت تواجه خطرا مستجدا مرتبط بالسرعة والموثوقية لأنه بالرغم من المزايا التي توفرها وسائل الدفع الإلكتروني للزبائن والمصارف على حد السواء إلا أنها فاقمت من المخاطر المصرفية التقليدية وأصبح يهدد القطاع المصرفي خطر آخر ألا وهو الخطر المعلوماتي اضافة لباقي الأخطار التي يعرفها هذا القطاع وخاصة الخطر القانوني الذي تفاقم باستعمال وسائل الدفع الإلكتروني لأن الجرائم التقليدية أصبحت معلومة للمصارف وبقيت تتعامل معها بنوع من الحيطة والحذر لمنع حدوثها والتقليل منها كما أن المصارف أضحت مؤهلة للتعامل مع هذا النوع من الجرائم بإصدارها للتعليمات والتوجيهات وتدريب العاملين المختصين -رغم أنه ينبغي أن يكون دورها هو الحد من هذه المشاكل- خاصة وأن التشريعات في الجزائر لم تتصدى لهذه التطورات بعد حيث تساهم وسائل الدفع الإلكتروني في تفاقم مشكل التهرب الضريبي وتسهيل عمليات تبييض الأموال لما توفره من سرية لأنه يستحيل على المصارف معرفة إذا كان من يقوم بالعملية هو الشخص

[1]- القانون رقم 18-05 المتعلق بالتجارة الإلكترونية، المؤرخ في 10 ماي 2018 الموافق ل24 شعبان 1439، ج ر عدد28، 2018.

[2]- القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018 الموافق ل 25 رمضان عام 1439، ج ر عدد 34، 2018.

نفسه أو شخص آخر، كما تساهم في التغطية على مختلف الجرائم الأخرى نتيجة صعوبة اكتشافها، كما أن استخدام وسائل الدفع الإلكتروني سيؤدي إلى صعوبة في تطبيق التنظيمات والقوانين المطبقة على المصارف.

الإشكالية:

أصبح التحدي الحقيقي لتطوير القطاع المصرفي وبالخصوص تطوير وسائل الدفع هو مدى توفر الحماية الجنائية عند استخدام وسائل الدفع الإلكتروني، لأن الأمن المعلوماتي رغم تأكيد المختصين على يوفره من حماية تقنية يبقى غير كاف لوحده، ولا يحل بأي حال من الأحوال محل الحماية القانونية عموما(المسؤوليات بمختلف أنواعها)، والجنائية خصوصا لأن (**المساءلة الجزائية**) هي الملاذ الأخير الذي يلجأ إليه المشرع.

وبالتالي نتساءل عن مدى كفاية نصوص قانون العقوبات الحالية، والنصوص الجزائية بقانون النقد والقرض ومختلف القوانين الجزائرية ذات الصلة بهذا المجال للمساءلة الجزائية عن استخدام وسائل الدفع الإلكتروني، أم أنه يلزمنا تدخل تشريعي سريع لتدارك مخاطر هذه الوسائل حيث يتوجب علينا خلق قواعد قانونية خاصة بالمسؤولية الجزائية تتلاءم وطبيعة وسائل الدفع الإلكتروني نظرا لما يحفها من صعوبات وللتوفيق بين متطلبات القانون الجنائي والتقنيات الحديثة؟

أهمية الموضوع:

بالعودة إلى قانون النقد والقرض وقانون العقوبات وقانون تبييض الأموال وقانون مكافحة التهريب نلاحظ أنها تبقى قاصرة عن ملاحقة هذا النوع من الإجرام، وحتى بالنسبة لتعديل القانون التجاري الخاص بوسائل الدفع فالمشرع لم يورد عقوبات عن سوء استخدامها، زيادة على غياب النصوص التشريعية التي تعاقب على الجرائم الجديدة الناشئة عن استخدام وسائل الدفع الإلكتروني فالدول المتقدمة تكنولوجيا عالجت هذه الجرائم المستحدثة، وأمام هذا الفراغ سيجد القاضي الجزائي نفسه مضطرا لترويض النصوص القانونية العقابية الحالية.

موضوع المسؤولية الجزائية عن استخدام وسائل الدفع الإلكتروني موضوع دقيق وشائك يثير مشكلات جديدة بالنسبة للقانون الجنائي نظرا للتقنية الفنية والبرمجة التي يستخدمها الجاني في ارتكاب الجريمة، ومن ثمة يأتي هذا البحث كمحاولة لإلقاء الضوء على بعض الجوانب من الإشكالات المثارة في هذا المجال.

الإجرام في هذا المجال يهدد الأعمال التجارية بخسائر فادحة تنال من الأمن القومي والسيادة الوطنية للدول ويشيع فقدان الثقة في التعاملات المصرفية الإلكترونية، وأصبح ساحة إجرامية نموذجية تتحدى الأجهزة الأمنية والقضائية بثغرات قانونية وفراغ تشريعي

وهذا دفع بالعديد من مشرعي دول العالم إلى إصدار قوانين جديدة لمواجهة هذه الجرائم بينما فضلت بعض الدول إجراء تعديل في بعض قوانينها القائمة.

يجب أن تواكب التشريعات الوطنية المختلفة هذا التطور الملحوظ في هذا المجال فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانونية غير تقليدية لهذا النوع من الجرائم المستحدثة خاصة وأننا نفتح الباب للتجارة الإلكترونية ووسائل الدفع الجديدة والتشجيع على استخدام بطاقات الدفع الإلكتروني وبالتالي ستتسع دائرة هذا الإجرام.

إذا كانت هذه الوسائل قد حققت رواجا كبيرا فإنها للآن تثير العديد من المسائل القانونية في حقل المسؤولية الجزائية مع تحديات المفهوم الجديد للمال الإلكتروني ولوسائل الدفع، وهنا تظهر أهمية المصارف كمؤسسات ذات أثر في توجيه المؤسسة التشريعية إلى تبني تشريعات متوائمة مع مفاهيم (المال، المحرر، طرق الاحتيال، طرق التزوير، طرق التبييض) الإلكتروني وقواعد وأحكام التعامل مع مشكلاته القانونية المثارة.

كما تظهر الأهمية في تهيئة بناء قانوني لإدارات المصارف يتيح لها إمكانية التعامل مع تحديات المصارف الإلكترونية إن اختارت دخول هذا الميدان، ولا نبالغ إذا قلنا أن جاهزية التعامل القانوني مع تحديات هذا النمط المستجد تمثل أهم ضمانة لنجاح المسيرة، لأنه إن كان يعتقد أن وسائل التقنية ستمنع مشكلات القانون فإنه محض وهم، إذ تخفي عوالم المصارف الإلكترونية وتحديدا مشاكل الدفع الإلكتروني ومشاكل تقديم الخدمة وما

تثيره من مسؤوليات، حزمة معتبرة من المشكلات والنزاعات المتوقعة تتطلب جاهزية تتفق مع هذه الأخطار.

التعريف بظاهرة جديدة من الجرائم التي ارتبطت بتكنولوجيا الإعلام والاتصالات المتطورة والاتجاه نحو الطابع الإلكتروني لتحديث المعاملات المصرفية التي تسعى لخدمة الزبون والوصول إليه في أي مكان وفي أي زمان والمتميزة بخصائص جعلتها تختلف عن غيرها وبالتالي ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية.

سوف نعالج موضوعا يكون محل اهتمام من طرف المشرع والقضاء الجزائري لأنه لا يمكن له بأي حال من الأحوال تجاهله في حياتنا اليومية، مما يستلزم التدخل التشريعي.

وأخيرا ربما يكون من المفيد أن نتذكر أن القوالب الجاهزة من الاتفاقيات والعقود والتعليمات والقوانين المنقولة عن نظم قانونية أخرى ومؤسسات أخرى لا تفي دائما بالغرض لما لكل ساحة من خصوصياتها ولما لكل دولة من اعتباراتها وأولوياتها الخاصة، وبقدر أهمية الاطلاع على تجارب الغير فإن الأهمية في قدرها الأكبر تكمن في فهم الاحتياجات الداخلية وموائمة الحلول مع هذه الاحتياجات مستفيدين مما لدى الغير من حلول.

نطاق البحث:

يتمحور حول تحول الجريمة التي تتم بوسائل الدفع الإلكتروني من صورتها التقليدية المادية إلى صورة معنوية ونتج عن ذلك مشكلة تفسير النصوص القانونية وحضر القياس

في المواد الجنائية ومبدأ الشرعية الجنائية وهذه العوامل تؤدي إلى إفلات عدد كبير من المجرمين من العقوبات، والمشكلة تكمن في قصر الحماية الجزائية على بعض الجرائم التي تتم بهذه الوسائل كجريمة تبييض الأموال تاركة البقية دونما أية حماية الأمر الذي يستوجب إيجاد حلول لهذه الثغرة القانونية خاصة إذا تكلمنا عن (تجارة و توقيع ومال ووسائل دفع ومصارف) إلكترونية.

يمكن أن تثار المسؤولية المدنية والتأديبية عن استخدام هذه الوسائل وقد آثرنا من خلال هذه الدراسة أن نتناول المسؤولية الجزائية عن استخدام وسائل الدفع الإلكتروني لما لها من أهمية كبرى في ميدان قانون الأعمال، والقانون الجنائي للأعمال والقانون الجنائي المعلوماتي والقانون المصرفي وكل القوانين المتداخلة معه حيث نحدد في (الباب الأول) المسؤولية الجزائية للفاعل الأصلي عن استعمال وسائل الدفع الإلكتروني، وفي (الباب الثاني) المسؤولية الجزائية عن الاشتراك في استعمال وسائل الدفع الإلكتروني في القانون الجزائري.

الباب الأول

المسؤولية الجزائية للفاعل الأصلي

عن استخدام وسائل الدفع الإلكتروني

المشرع الجزائري كما هو الحال في معظم التشريعات لم يضع تعريفا للفاعل الأصلي وتحديد الشخص المسؤول جزائيا باعتباره فاعل أصلي لا يثير الكثير من الصعوبات، فالفاعل هو الجاني الذي يرتكب الفعل المادي المكون للجريمة وبالتالي من يرتكب فعلا خارج نطاق الركن المادي المحدد لتكوين الجريمة لا يعد فاعلا ويمكننا القول أن الجرائم التي يرتكبها الفاعل الأصلي عند استخدام وسائل الدفع الإلكتروني غالبيتها تتجه فيها نيته إلى الاستيلاء على المال المتداول عن طريق هذه الوسائل.

غزت اللامادية مختلف نواحي الحياة اليومية وغدت طبيعة الأشياء لامادية خصوصا في مسألة الدفع الإلكتروني التي رافقت الاستجابة لطبيعة التجارة الإلكترونية، ومواكبة لهذه الحركية غزت وسائل الدفع الإلكتروني العمل المصرفي وأصبحت البنوك تتنافس في تقديم وتوفير هذا النوع من الخدمات، وهذا استجابة لمتطلبات الزبون وإرضاء لرغباته، واستقطابا لرؤوس الأموال.

لكن بالرغم من المزايا والايجابيات التي توفرها وسائل الدفع الإلكتروني نتيجة تطورها بشكل سريع تطورت معها الأساليب الاجرامية إلا أن الملاحظ دائما أن النصوص القانونية غالبا لا تتطور بنفس السرعة وخاصة النصوص الجنائية مما يجعلنا نصطدم بمبادئ القانون الجنائي وخاصة مبدأ الشرعية الذي يعد حجر الزاوية في هذه المسألة، ويهدف هذا الباب إلى بيان الأحكام العامة لوسائل الدفع الالكتروني(الفصل الأول) مع الاشارة إلى أنه تم اختيار عنوان

وسائل الدفع الإلكتروني عن قصد لأن الفقه غالبا ما يركز عليها أكثر من تركيزه على عملية الدفع الإلكتروني.

ونبين من خلال الفصل الثاني من هذا الباب مدى الحاجة إلى نصوص قانونية جنائية خاصة وجديدة في القانون الجزائري لترتيب المسؤولية الجزائية للفاعل الأصلي، وهذا تفاديا للخوض في الآراء الفقهية- وإن كنا لا ننكر أهميتها - التي ركزت على مناقشة النصوص التقليدية ومدى انطباقها على هذا النوع الجديد من الجرائم المرتكبة بواسطة وسائل الدفع الإلكتروني أم عدم انطباقها لهذا تم التركيز على الجرائم المنصوص عليها في القوانين المقارنة ليتم التأسيس للركن الشرعي لهذه الجرائم لأنه سجلت العديد من حالات سوء استعمالها وعدم التقيد بالأنظمة المتبعة في مجالها سواء من قبل الحامل أو الغير.

بقدر ما كان لوسائل الدفع الإلكتروني ايجابيات انعكست على العمل المصرفي والزبون إلا أنها بالمقابل كانت لها سلبيات عمقت من اشكالية السرية المصرفية في العمل المصرفي الإلكتروني.

الفصل الأول

الأحكام العامة لوسائل الدفع الإلكتروني

يركز الفقه القانوني عند معالجته للوفاء الإلكتروني على وسائل الدفع الإلكتروني Instrument de paiement أكثر من التركيز على الوفاء (le paiement) كتصرف قانوني، وأصبحنا أمام ظاهرة جديدة تتميز بها وسائل الدفع الإلكتروني وهي ظاهرة التطوق[1] أو اللامادية أو ما يعرف ب(dématérialisation[2])، **وهي عبارة عن نظام يسمح بالانتقال من الشكل الورقي إلى الشكل القيدي أي الغاء إثبات الأطراف للملكية في الشكل الورقي والانتقال إلى قيدها في الحساب** فأول ما تتميز به المعلوماتية هو عنصر اللامادية بحكم فقدان المعلومة لوعائها المادي، وهو النهج الذي انتهجه المشرع الجزائري حيث باشرت الجزائر إصلاحات لتطوير النظام البنكي وتحسين نظام الدفع واختارت ما يعرف بتطوق وسائل الدفع (dématérialisation des instrument de paiement)، و التطوق هو تحويل الشيء المادي (physique) إلى شيء غير مادي ويشمل التطوق جانبين أساسيين في وسائل الدفع وهما:

الأول تطوق السند الورقي ويتمثل بإلغاء السند الورقي تماما في التبادلات بين البنوك لغرض تحصيل قيمها وتعويضها بسند إلكتروني، والثاني **تطوق تبادلات التحصيل** ويعني

---

[1]- مصطلح التطوق مأخوذ عن بحيح عبد القادر، إشكالية التحكم في وسائل الدفع البنكية وأثرها على الخدمات المصرفية حالة الجزائر (1962-2010)، مجلة الباحث، العدد09، لسنة 2011، ص31.

[2]-Dématérialisation :Système permettant de substituer à une forme papier des titres, une forme scripturale, Conseil national du crédit et du titre, annexes au rapport problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mai 1997, transferts électroniques de fonds les paiement par wap, actes des journées d'études le 18 /11/1999-05/10/2000, organisé par l'association luxembourgeoise des juristes de banque, le centre de recherches informatique et droit (CRID) la faculté de droit de Namur et l'association européenne pour le droit bancaire et financier belgium (ABDBF-belgium), cahiers aedbf /evbfr-belgium, bruyant Bruxelles, 2001, p218.

إلغاء التبادلات المادية لوسائل الدفع وتعويضها بالتبادلات الإلكترونية للمعلومات المالية هذه الإصلاحات التي شرعت فيها المنظومة البنكية وخصت نظام الدفع أهلتها لوضع **نظام الدفع الإلكتروني** للقضاء على سلبيات نظام الدفع الكلاسيكي[1].

بالنتيجة تطوق وسائل الدفع الإلكترونية: هو إجراء يسمح بتجنب النقل المادي للتحويلات بين البنوك أو بين البنك وزبائنه في الشكل الورقي كالشيك أو التحويل مثلا وتسجيل التحويل على دعامة إلكترونية[2]، وعليه سنركز في هذا المبحث على التعريف بالدفع الإلكتروني (المبحث الأول)، ثم نخصص (المبحث الثاني) المفهوم القانوني لوسائل الدفع الإلكتروني والمبحث الثالث سنتناول من خلاله أنواع وسائل الدفع الإلكتروني.

المبحث الأول

التعريف بالدفع الإلكتروني

يعد الدفع الإلكتروني Le paiement électronique نظام أكثر سهولة وأقل تكلفة مقارنة بالدفع اليدوي لذا نجد أن وسائل الدفع الإلكتروني في تزايد وتطور مستمرين، ولأن وسائل الدفع التقليدية أصبحت لا تلائم التطور الكبير الحاصل في التجارة الإلكترونية ظهرت وسائل إلكترونية للدفع ونظرا لأهمية الدفع الإلكتروني على شبكة الانترنت من الضروري بيان آلية الوفاء بالبدل المالي المتجسد في الدفع الإلكتروني المتفق مع خصوصية التجارة

[1]- بحيح عبد القادر، المرجع السابق، ص31.

[2]-Annexes au rapport problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mai 1997, op, cit, p219.

الإلكترونية ومقتضيات السرعة، لهذا نتناول من خلال (المطلب الأول) بيان مفهوم الدفع الإلكتروني، ثم في (المطلب الثاني) أطراف الدفع الإلكتروني، وفي(المطلب الثالث) مبدأ عدم جواز التراجع عن الدفع الإلكتروني بين التوسيع والتقييد.

المطلب الأول

مفهوم الدفع الإلكتروني

يكتسي مفهوم الدفع الإلكتروني باعتباره مفهوم حديث نوع من الغموض نظرا لاختلاف المصطلحات المستعملة من دولة إلى أخرى، وغياب هذا المفهوم تماما في دول أخرى كالجزائر مثلا فالدفع الإلكتروني في الحقيقة ليس سوى الأمر بالتحويل الإلكتروني، أو الأمر الصادر عن طريق بطاقة بنكية ويخضعان لنفس النظام القانوني[1]، إلا أن هناك من يرى أن كلمة التحويل الإلكتروني أشمل من عبارة الدفع الإلكتروني لأن الدفع هو مجرد عملية من جملة عمليات التحويل[2] كما يقصد بالدفع الإلكتروني مجموع الأدوات والتحويلات الإلكترونية التي تصدرها المصارف والمؤسسات كوسيلة دفع وتتمثل في البطاقات البنكية والنقود الإلكترونية والشيكات الإلكترونية والبطاقات الذكية[3]، لهذا سنحاول من خلال (الفرع الأول)

[1]- pierre Bresse, guillaume Beaure D'Augères et Stéphanie Thuillier, paiement numérique sur internet, international Thomson publishing, 133.

[2]- علي كحلون، الأدوات المصرفية في التحويل الإلكتروني للأموال، مجلة القضاء والتشريع، صادرة عن وزارة العدل التونسية، جانفي 2011، ص19.

[3]- منصوري الزين، وسائل وأنظمة الدفع والسداد الإلكتروني عوامل الانتشار وشروط النجاح، مداخلة في الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الإلكترونية في الجزائر، المركز الجامعي خميس مليانة 26-27أفريل 2011.

تبيان مفهوم الدفع الإلكتروني في القانون الفرنسي، ثم في الفرع الثاني نناقش مفهوم الدفع الإلكتروني في القانون الجزائري (الفرع الثاني).

الفرع الأول

مفهوم الدفع الإلكتروني في القانون الفرنسي

يستعمل المشرع الفرنسي مصطلح خدمات الدفع الإلكتروني أو عمليات الدفع الإلكتروني و عملية الدفع حسب المادة L133- 3 الفقرة الأولى من قانون النقد و المال الفرنسي

L133-3 - 1 « Une opération de paiement est une action consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire, ordonnée par le payeur ou le bénéficiaire ... »

هي التصرف المنشئ للتحويل أو سحب الأموال المستقل عن الالتزامات التابعة للأطراف سواء الدافع (الآمر) أو المستفيد[1]، وتعرف خدمات الدفع بأنها الخدمات الجديدة المرافقة ل"حساب الدفع[2]" وعمليات الدفع المرتبطة والمرافقة لحساب الدفع تشمل: الأوامر بالاقتطاع، عمليات الدفع المنفذة عن طريق بطاقة الدفع أو أي وسيلة مماثلة، أو التحويلات وتشمل أوامر الدفع المتكررة، إضافة إلى خدمة الدفع المؤدية لعمليات الدفع الصادرة عن أي وسيلة اتصال رقمية أو معلوماتية[3]، ونستنتج استقلال العلاقات بين الأطراف سواء الآمر أو

[1]-Stéphane Piedelièver, Doit bancaire, Thémis droit privé, presses universitaires de France, 1er édition, 2003, p328.

[2]- مصطلح حساب الدفع إلى غاية يومنا هذا لم يحدد معناه في التشريع الفرنسي.

[3]-Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 7edition, lexis Nexis, 2009, p02.

المستفيد عن وسيلة الدفع بعبارة أخرى عملية الدفع تتضمن ثلاث عناصر أولا التصرف القانوني (تصرف الدافع (الآمر) أو نشاط مقدم خدمة الدفع، ثانيا التصرف القانوني (الأمر بالدفع)، ثالثا استعمال أجهزة تقنية شخصية (وسائل الدفع)[1].

تنقسم عمليات الدفع في القانون الفرنسي إلى ثلاث أنواع الأولى **خدمات الدفع البنكية** وتشمل منح الشيكات واصدار وتسيير شيكات السفر وكذلك اصدار وتسيير وسائل الدفع من غير خدمات الدفع واصدار وتسيير النقود الإلكترونية، والثانية **خدمات الدفع المرافقة لحساب الدفع** وتتمثل في ايداع النقود في حساب الدفع، السحب للنقود من حساب الدفع، تنفيذ عمليات الدفع (الاقتطاع، الدفع بالبطاقة أو أي وسيلة مشابهة، التحويل)، تنفيذ عمليات الدفع السابقة عندما تكون مرافقة لفتح الاعتماد، اصدار و/أو قبول وسائل الدفع، تحويل الأموال، تنفيذ الدفع من طرف مستخدمي الاتصالات، والثالثة **الخدمات الحرة** وتشمل الدفع بين المجموعات، الدفوعات الخاصة، الدفع عن طريق الهاتف أو الانترنت وهي ليست وسائل دفع[2].

الفرع الثاني

غياب مفهوم للدفع الإلكتروني في القانون الجزائري

يمكن تعريف عملية الدفع الإلكترونية بأنها كل عملية تحويل أموال خلاف العمليات المنشأة بموجب شيك أو سند أو أية أوراق أخرى وتجري إنفاذا لتعليمات بواسطة نقطة إلكترونية عبر

[1]- Stéphane Piedelièver, Doit bancaire, op, cit, P 328.
[2]- Cathie-Rosalie Joly, le statut de prestataire de services de paiement, www.ulys.net. www.droit-technolodie.org,www.droitdesjeux, consulté le 25/09/2017.

أية وسيلة اتصال، ويقصد بالنقطة الإلكترونية الجهاز الإلكتروني الذي يسمح بإنشاء عملية تحويل أموال إلكترونيا[1]، وعرف المشرع الجزائري النقطة الطرفية بأنها "نقاط وصل مادية تستجيب لمواصفات تقنية ضرورية للنفاذ إلى شبكة الاتصالات الإلكترونية والاتصال بفعالية عن طريقها وهي جزء لا يتجزأ من الشبكة..." في القانون الجديد رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية وعرف مصطلح جهاز مطرفي ضمن المادة العاشرة فقرة 06 من نفس القانون بأنه كل تجهيز مخصص لأن يكون موصولا بطريقة مباشرة أو غير مباشرة بنقطة طرفية ويرسل أو يستقبل أو يعالج إشارات الاتصالات الإلكترونية دون أن يشمل التجهيزات التي تمكن من الوصول إلى خدمات البث الإذاعي، وعرفت الفقرة الأولى من نفس المادة الاتصالات الإلكترونية بأنها كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرو مغناطيسية، فالدفع بوسيلة إلكترونية يجري في بيئة غير مادية تبرم التصرفات القانونية بداخلها عن طريق استخدام وسائل الاتصال الحديثة وعلى وجه الخصوص شبكة المعلومات الدولية المسماة بالأنترنت[2].

يتم الدفع الإلكتروني بالاستناد إلى دعامات إلكترونية وهو اسم نوعي لنوع من الدفع من بين الدفوع الأخرى تميزه خاصية الوسيلة أو الدعامة الخاصة التي تشكل في مجموعها آلية للدفع

---

[1]- زهير بوشناق، العمليات المالية المصرفية الإلكترونية، اتحاد المصارف العربية، لبنان 2006.

[2]- عرفت المادة 05/10 من القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية الأنترنت بأنها شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتكول الاتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها.

تتم كلها أو في جزء منها إلكترونيا[1]، وهناك من يعرف الدفع الإلكتروني على أنه عبارة عن وسيلة يمنحها مصدرها لشخص طبيعي أو اعتباري بناء على عقد بينهما تمكنه من شراء السلع أو الخدمات ممن يعتمد هذه الوسيلة دون دفع الثمن نقدا أو حالا[2]، مثلا التزام المصرف المصدر للبطاقة بسداد قيمة الالتزام محل الأداء، في حين هناك من يرى أن للدفع الإلكتروني معنيان الأول واسع والثاني ضيق[3]:

1-الدفع الإلكتروني بالمعنى الواسع: هو كل عملية دفع لمبلغ من النقود تتم بأسلوب غير مادي لا يعتمد على دعامات ورقية بل بالرجوع إلى آليات إلكترونية.

2-الدفع الإلكتروني بالمعنى الضيق: ينحصر فقط في عمليات الوفاء التي تتم دون وجود اتصال مباشر بين الأشخاص الطبيعيين كالذي يتم عبر شبكة الانترنت والحقيقة أن الدفع الإلكتروني هو دفع أو وفاء ولكن بوسائل إلكترونية وقد يكون تحويلا لمبلغ ما بالنقد الوطني أو بالنقد الأجنبي وفي جميع الأحوال هو وفاء بالنقد ولكن بوسائل إلكترونية[4].

---

[1]- Étienne Wéry, facture, monnaie et paiement électronique, litec groupe lexis Nexis, édition du juris-classeur, p44.

[2]- حسين عبد الله عبد الرضا الكلابي، الوفاء الإلكتروني كوسيلة لتنفيذ الالتزام دراسة قانونية، مجلة كلية الحقوق، جامعة النهرين، العدد الرابع عشر، 2012، ص181.

[3]- فالدفع الإلكتروني لا يشكل في ذاته ثورة في مجال الوفاء أو آلياته، بل هو في حقيقته نتيجة إلزامية للتطور التكنولوجي المستمر، أنظر عدنان ابراهيم سرحان، الوفاء(الدفع) الإلكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الأول، ص268، 269.

[4]- فياض ملفي القضاة، الجوانب القانونية للتعاقد والدفع الإلكتروني في التجارة الإلكترونية، المجلة الأردنية في القانون والعلوم السياسية، مجلة علمية محكمة، المجلد (1)، العدد الثالث، شوال 1430 الموافق ل تشرين الأول 2009، ص101.

يمكننا في الأخير تعريف الدفع الإلكتروني بأنه وفاء قيدي بأي وسيلة قانونية إلكترونية مهما كان شكلها التقني يستخدمها الفرد وتقوم مقام النقود، حيث لا تظهر النقود الإلكترونية للوجود إنما هي عبارة عن مجموعة من القيود، فالدفع الإلكتروني ليس هدفا في حد ذاته وإنما وسيلة ابتدعها العمل لمواكبة التطور الذي لحق بوسائل الاتصال لأن التصرفات أصبحت تتم إلكترونيا وبالتالي الدفع يجب أن يتم إلكترونيا.

المطلب الثاني

أطراف الدفع الإلكتروني

تعدد الأطراف شرط للتعامل بوسائل الدفع الإلكترونية و رغم أن هذه الفكرة لا تثور بالنسبة للوفاء بواسطة النقود القانونية (الأوراق النقدية) التي يتم الدفع بها بتصرف منفرد من حائز هذه الأوراق، أما الوفاء القيدي (باستخدام نقود الودائع) فإنه يقتضي تدخل طرفين[1]، ونظرا لخصوصية تقنية الدفع الإلكتروني لابد من تدخل أطراف حتى تتم هذه العملية عبر دعامات إلكترونية حيث يشترك فيها البنك أو المؤسسة المالية المقدمة لخدمة الدفع الإلكتروني، وهذه الأخيرة محتكرة من طرف البنوك والمؤسسات المالية في القانون الجزائري(الفرع الثاني) في حين تم انهاء مرحلة احتكار البنوك تقديم خدمات الدفع الإلكتروني في القانون الفرنسي(الفرع الأول)، والزبون المرخص له باستعمال وسائل الدفع الإلكتروني (الفرع الثالث) ورغم اختلاف دور كل منهما في إدارة عملية الدفع الإلكتروني إلا أن تدخلهما معا يعد أمرا لا غنى عنه

[1]– الشيك على سبيل المثال يقتضي تدخل كل من الساحب والمصرف المسحوب عليه.

منذ بدء عملية الدفع حتى انتهائها فلا يستطيع أحدهما أن يستعمل هذه الوسائل بمفرده، وهما الطرفان اللذان سنركز عليهما في هذا المطلب، كما لا تتم عملية الدفع الإلكتروني إلا بتدخل التاجر المرخص له التعامل بهذه التقنية.

الفرع الأول

انهاء احتكار البنوك لتقديم خدمات الدفع الإلكتروني في القانون الفرنسي

يلاحظ في نطاق قوانين التجارة والمعاملات الإلكترونية أن البعض منها لم يشر إلى الكيفية التي تتم بها عملية اصدار ومنح وسائل الدفع الإلكتروني، فالنقود الإلكترونية مثلا لا يشترط أن تكون مرتبطة بحساب بنكي ومع ذلك يبقى السؤال قائما حول الجهة التي يمكن أن تقوم بإصدار هذه الوسائل وهل يشترط أن تكون مصرفا أم أن أية مؤسسة مالية يحق لها اصدار وسائل الدفع الإلكتروني[1]، و يثور التساؤل خاصة في مجال البطاقات حول مدى جواز قيام بعض المؤسسات غير المصرفية بإصدار وإدارة أنوع من بطاقات الدفع والحقيقة أن المسألة تحتاج لإيضاح بسيط.

بالنسبة للاتحاد الأوربي نجد أن المفوضية الأوربية وفي تقريرها لعام 1994 الصادر عن المؤسسة النقدية الأوربية أكدت على أن اصدار النقود الإلكترونية يجب أن يبقى مقيدا ومحصورا فقط بالمؤسسات المالية[2]، وهذا لأنها كانت ترى ضرورة حماية الزبائن وعدم فتح

[1]– سلام منعم مشعل، وسائل الدفع الإلكترونية، مجلة كلية الحقوق، جامعة النهرين، العدد العشرون،2008، ص199.

[2]– سلام عبد المنعم مشعل، المرجع نفسه، ص 200.

الباب على مصراعيه بالسماح لغير المصارف بالمشاركة في اصدار وسائل الدفع الإلكتروني.

انتهت مرحلة احتكار اصدار وتسيير النقود الإلكترونية من طرف البنوك في فرنسا منذ سنة 2009[1]، مما يشير إلى إمكانية اصدار النقود الإلكترونية من قبل المؤسسات غير المصرفية ولكن بشرط أن تمنح إذن أو رخصة[2]، حيث تم اصدار الأمر المتعلق بالشروط المنظمة لتقديم خدمات الدفع والمتضمن إنشاء مؤسسات الدفع[3] وهو الأمر رقم 2009/866 المؤرخ في 15 جويلية 2009 وتم التعديل للقانون الفرنسي بإدراج النصوص الأوربية التي تنظم تقديم خدمات الدفع والمنصبة على إنشاء مؤسسات الدفع التي أصبحت سارية المفعول عن طريق هذا الأمر الذي سيغير بعمق وسائل الدفع، خصوصا الدفع، السحب، الدفع عن طريق البطاقات لأن الهدف من النص هو خلق أكبر قدر من المنافسة بين هذه المؤسسات وبالنتيجة خفض تكاليف المعاملات في مجال الدفع[4] وتم تعديل معظم مواد قانون النقد والمال الفرنسي حيث عدلت المجموعة الأولى من الكتاب الأول المتعلق بالعملة والنقود وكذا تعديل النصوص الأخرى المتعلقة بخدمات الدفع، اتفاقيات الحساب، وأخيرا مقدموا الخدمات.

[1]- Pierre Storrer, La monnaie électronique en droit français : en fin un nouveau départ ?, revue banque de France, N° 753 novembre, 2012, p53.

[2]- سلام عبد المنعم مشعل، المرجع السابق، ص200.

[3]- Ordonnance relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement (ord ne 2009 /866 du juill. 2009, Jo, 16juill.

[4]- Dominique legeais, crédit et titre de crédit, revue trimestrielle de droit économique, octobre, ne4, 2009, p784.

يفهم من نص المادة L521-1[1] من قانون النقد والمال الفرنسي على أن مقدمي خدمة الدفع(PSP)[2]هم أشخاص معنوية وتشمل ثلاث أنواع من المؤسسات، مؤسسات الدفع(EP[3])، و مؤسسات النقود الإلكترونية (EME)[4]، و مؤسسات القرض.

مؤسسات الدفع المشار إليها في المادة L 522/ 1[5]، هي أشخاص معنوية من غير مؤسسات القرض ومؤسسات النقود الإلكترونية، بالتالي نستنتج أن مصطلح مقدمي خدمات الدفع أشمل من مصطلح مؤسسات الدفع الذي يعد نوع من المؤسسات المقدمة لخدمة الدفع وبالتالي فمؤسسات خدمات الدفع تعتبر شخصيات معنوية من غير مؤسسات القرض والتي تقدم خدمات الدفع بصفة مهنية واعتيادية[6].

---

[1]-ART L521/1 CMF « I. - **Les prestataires de services de paiement sont les établissements de paiement, les établissements de monnaie électronique et les établissements de crédit.**
II. - Lorsqu'ils fournissent des services de paiement, les institutions et services suivants sont également considérés comme des prestataires de services de paiement, sans être soumis aux dispositions du chapitre II du présent titre et dans les limites des dispositions législatives qui, le cas échéant, les régissent :
a) La Banque de France, l'Institut d'émission des départements d'outre-mer et l'Institut d'émission
D'outre-mer ;
b) Le Trésor public ;
c) La Caisse des dépôts et consignations. »

[2] - (PSP) : Les prestataires de services de paiement.

[3] -(EP) : établissements de paiement.

[4]-(EME) : Les établissements de monnaie électronique.

[5] -ART L522-1 CMF « Les établissements de paiement sont des personnes morales, autres que les établissements de crédit, les établissements de monnaie électronique et les personnes mentionnées au II de l'article l.521-1, qui fournissent à titre de profession habituelle les services de paiement mentionnés à l'article l.314-1 ».

[6] - Dominique legeais, op, cit, p789.

فمؤسسات القرض في فرنسا يمكنها القيام بكل العمليات (العمليات البنكية، اصدار وتسيير النقود الإلكترونية وتقديم خدمات الدفع) ومؤسسات النقود الإلكترونية (EME)[1] أيضا تقوم بإصدار وتسيير النقود الإلكترونية ويمكنها "أن تزود بخدمات الدفع "، أما مؤسسات الدفع فلا يمكنها إلا تقديم خدمات الدفع[2]، ومؤسسات الدفع سيكون لها كزبائن أشخاص طبيعيون أو معنويون والذين سيقومون بالمدفوعات أو سيكونون هم المستفيدين[3] وتعرف خدمات الدفع بأنها الخدمات الجديدة المرافقة ل"حساب الدفع " وعمليات الدفع المرتبطة والمرافقة لحساب الدفع تشمل: الأوامر بالاقتطاع، وعمليات الدفع المنفذة عن طريق بطاقة الدفع أو أي وسيلة مماثلة، أو التحويلات وتشمل أوامر الدفع المتكررة، إضافة إلى خدمة الدفع المؤدية لعمليات الدفع الصادرة عن أي وسيلة اتصال رقمية أو معلوماتية[4]، وبالتالي نستنتج أن المشرع الفرنسي أنشأ مؤسسات خاصة بتسيير واصدار النقود الإلكترونية وهي المؤسسات الجديدة (EME) مع احتفاظه للبنوك بكل العمليات ومنها الترخيص لها بممارسة عمليات الدفع واصدار وتسيير النقود الإلكترونية في حين أن مؤسسات الدفع يحظر عليها القيام بإصدار النقود الإلكترونية وإنما مسموح لها فقط القيام بعمليات الدفع الإلكتروني.

القانون الفرنسي يسمح لمؤسسات القرض القيام بكل العمليات، أما مؤسسات النقود الإلكترونية وهي المؤسسات الخاصة التي أنشأها المشرع الفرنسي لتسيير واصدار النقود

[1]-(EME) : Les établissements de monnaie électronique.
[2]-Pierre Storrer, La monnaie électronique en droit français : en fin un nouveau départ ?, revue banque de France, N° 753 novembre, 2012, p52.
[3] - Dominique legeais, op, cit, p789.
[4]-Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 7edition, lexis Nexis, 2009, p02.

الإلكترونية فيمكنها القيام بعمليات اصدار وتسيير النقود الإلكترونية في حين مؤسسات الدفع تقوم فقط بعمليات الدفع فقط ويحظر عليها القيام بإصدار النقود الإلكترونية.

بالتالي منذ سنة 2009 شرع لعهد جديد لوسائل الدفع الإلكتروني وذلك بظهور متعاملين جدد هم مؤسسات الدفع[1] في القانون الفرنسي، فالمصارف بعدما كانت هي التي تستطيع دون سواها مباشرة مثل هذه العمليات وتنفيذ أوامر الدفع لأنها هي المرخص لها بذلك أصبحت وفق القانون الفرنسي تتشارك في هذه العمليات مع مؤسسات أخرى هي مؤسسات النقود الإلكترونية ومؤسسات الدفع.

الفرع الثاني

تكريس احتكار الدفع الإلكتروني في القانون الجزائري

على عكس القانون الفرنسي لايزال القانون الجزائري حبيس النظرة التقليدية لتقديم خدمات الدفع الإلكتروني وحصرها في البنوك والهيئات المالية وبريد الجزائر وإن كان لهذا الموقف ما يبرره باعتبار أن الجزائر تعمل على تطوير نظامها البنكي أولا، و لم يظهر أي وجود لمصطلح مقدم خدمة الدفع الإلكتروني من خلال القوانين المعدلة.

مقدمي (مزودي) خدمات الدفع الإلكتروني كناية عن شركات تقوم بعمليات الدفع بدلا من المصرف وهي أكثر مرونة من البنوك في انجاز عملياتها كما أنها تستخدم تقنيات حديثة

[1]– وبالنسبة للولايات المتحدة الأمريكية من خلال التشريعات والقوانين الاتحادية هناك يبدو أن الكيانات والمؤسسات المالية وحتى غير المالية يحق لها اصدار وسائل الدفع الإلكترونية، أنظر سلام عبد المنعم مشعل، المرجع السابق، ص202.

جعلت خدماتها أسرع من البنوك ومتنوعة أكثر[1]، وعرف المشرع العراقي مزود خدمات الدفع الإلكتروني[2] بأنه الشخص الذي حصل على ترخيص من البنك لتقديم خدمات الدفع الإلكتروني، و يمكننا أن نعرف مقدم خدمة الدفع الإلكتروني بأنها المؤسسة التي تمنح للزبون وسيلة الدفع الإلكتروني بشروط محددة، والحاصل على ترخيص من البنك المركزي في كل دولة والمصرح له بالتعامل بوسيلة دفع إلكتروني معينة مهما كانت وسيلة الاتصال سواء معلوماتية أو رقمية.

أولا/ الاحتكار الضمني من طرف البنوك والهيات المالية في القانون التجاري

بالعودة للقانون التجاري الجزائري نستنبط **حصر اصدار وسائل الدفع الإلكتروني لدى المصارف و الهيئات المالية** أن المصارف والمؤسسات المالية فقط هي المسموح لها بإصدار وسائل الدفع الإلكتروني وهذا طبعا بعد حصولها على الترخيص من بنك الجزائر هذا ما يفهم ضمنيا من خلال المواد 543مكرر19، والمادة 543 مكرر21، والمادة 543 مكرر23 من القانون التجاري حيث يشترط لإتمام الأمر بالتحويل ضرورة توفر حسابين، وفي الأمر بالاقتطاع يستلزم تقديم البيانات المصرفية، واشتراط أن تصدر بطاقات الدفع عن البنوك والهيات المالية المؤهلة قانونا.

[1]- أحمد سفر، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2008، ص20.

[2]- تنص المادة 01 /ثالثا النظام رقم 03 لسنة 2014، قرار مجلس الوزراء رقم 186السنة 2014، الوقائع العراقية، العدد4326، الصادر في 2014/06/23.

وإن كان مصطلح الهيات المالية غير واضح المعنى لأنه بالنسبة لقانون النقد والقرض نستعمل مصطلح مؤسسات مالية.

ثانيا/تكريس الاحتكار الصريح للبنوك وبريد الجزائر في قانون التجارة الإلكتروني

كرست المادة 27 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية احتكار البنوك وبريد الجزائر لإصدار وسائل الدفع الإلكتروني حيث جاء في نصها " يتم الدفع في المعاملات التجارية الإلكترونية إما عن بعد أو عند تسليم المنتوج، عن طريق وسائل الدفع المرخص بها، وفقا للتشريع المعمول به.

عندما يكون الدفع إلكترونيا فإنه يتم من خلال **منصات دفع مخصصة لهذا الغرض، منشأة ومستغلة حصريا من طرف البنوك المعتمدة من قبل بنك الجزائر وبريد الجزائر** وموصولة بأي نوع من أنواع محطات الدفع الإلكتروني عبر شبكة المتعامل العمومي للمواصلات السلكية واللاسلكية.

يتم الدفع في المعاملات التجارية العابرة للحدود، حصريا عن بعد عبر الاتصالات الإلكترونية".

أوجبت المادة 28 أن يكون موقع الأنترنت الخاص بالمورد الإلكتروني[1] موصولا بمنصة الدفع الإلكترونية مؤمنا بواسطة نظام تصديق إلكتروني.

[1]- المادة 27 من القانون 18-05 المتعلق بالتجارة الإلكترونية عرفت المورد الإلكتروني بأنه كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الإلكترونية.

وأخضعت المادة 29 من نفس القانون منصات الدفع الإلكتروني لرقابة بنك الجزائر لضمان استجابتها لمتطلبات التشغيل البيني وسرية البيانات وسلامتها وأمن تبادلها.

الفرع الثالث

الزبون المرخص له استعمال وسائل الدفع الإلكتروني

عند إصدار وسيلة الدفع الإلكتروني يلتزم المصرف بتنفيذ أوامر زبونه بخصوص عملية الدفع وبالتالي ففكرة الإدارة المشتركة لعملية الدفع الإلكتروني ترتكز على وجود حساب مصرفي حسب القانون الجزائري لأن وسائل الدفع الإلكتروني هي الأدوات والأساليب التقنية والعمليات الفنية التي يتم بها تحريك الأموال المودعة في الحسابات، سواء بمقتضى ايداع من قبل الزبون أو بموجب ائتمان أسند له من قبل المصرف، ويعد الحساب موضوعا أساسيا لحركة وسائل الدفع الإلكتروني لأنه بمقدار ما يحرص البنك بالتثبت الذي يبذله بقدر ما يقوم بالتزامه في جمع المعلومات الكافية من صاحب الحساب.

فالزبون المسموح له باستعمال وسائل الدفع الإلكتروني(حامل وسيلة الدفع الإلكتروني) يجب أن تتوفر فيه جملة من الشروط والالتزامات يلاحظ عليها في أغلب الحالات أنها تراعي مركزه الضعيف وتتمثل في:

- أن يكون زبونا لبنك أو مؤسسة مالية مرخص لها بإصدار وتوزيع هذه الوسائل.
- تمنح وسيلة الدفع الإلكتروني بناء على طلب الزبون بعد التأكد من توافر شروط معينة.
- على الزبون تقديم ضمانات شخصية وعينية لاستصدار وسيلة الدفع الإلكتروني.

- استعمال وسيلة الدفع الإلكتروني في حدود سقف مالي معين لا يحق للزبون تجاوزه.

- يتكون رصيد الحساب (حساب الدفع) للزبون إما من مجموع ايداعاته وإما من الائتمان الممنوح له من قبل المصرف وفي هذه الحالة الثانية تظهر أهمية الاتفاق المبرم بين المصرف والزبون في تكوين الرصيد الذي يسمح بتشغيل الحساب حيث يستطيع الزبون أن يصدر أوامر الدفع على الرصيد القائم (أيا كان مصدره).

نخلص في الأخير حسب المشرع الجزائري إلى أن اتفاق المصرف وزبونه هو الذي يسمح بتشغيل وسيلة الدفع الإلكتروني بالمشاركة الكاملة لكل منهما، كما يمكن أن يتم تشغيل وسيلة الدفع الإلكتروني بطريقة قانونية كما في حالة تطبيق الاقتطاعات على أجور الموظفين من طرف الدولة.

ويقع على الزبون مجموعة من الالتزامات عند استعمال وسيلة الدفع الإلكتروني منها:

- استعمال وسيلة الدفع الإلكتروني حسب الشروط القانونية والتعاقدية التي تنظم تسليمها واستعمالها واتخاذ الاحتياطات لضمان المحافظة عليها، وعلى الوسائل التي تمكن من استعمالها والامتناع عن تدوين الهوية الشخصية أو أي رمز آخر بطريقة يسهل اكتشافها على وسيلة الدفع نفسها أو على الأشياء والمعدات التي تحفظ أو تحمل معها.

- على الزبون اعلام المصرف بالعمليات وبالأخطاء التي تم تثقيلها بالحساب دون موافقته وتقديم الاعتراض في حالة الضياع أو السرقة لوسيلة الدفع الإلكتروني، أو الوسائل أو البيانات التي تمكن من استعمالها.

المطلب الثالث

مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني بين التوسيع والتقييد

الأصل العام المطبق في الدفع الإلكتروني هو عدم قابلية الرجوع في الأمر بالدفع الإلكتروني، ويعتبر هذا المبدأ من ضمن القواعد الهامة التي حرص القانون على وضعها حيث اعتبر أن أمر الدفع الإلكتروني وبمجرد صدوره أصبح قطعيا وساري المفعول ولا يجوز الرجوع فيه[1].

عدم رجعية أوامر الدفع يعتبر مبدأ لتأمين الدفع في الأنشطة التجارية وتأمين أنظمة الدفع وتعني مسألة تأمين الدفع عدم رجعية الأوامر وهي خاصية لقواعد أنظمة الدفع الإلكتروني وتعتبر مسألة أساسية بالنسبة للسلطات الأوربية (البنك المركزي، اللجنة الأوربية والبرلمان الأوربي)[2]، وهذا يبين مدى أهمية هذا المبدأ ومدى الاهتمام به أوربيا لحماية مستعملي وسائل الدفع الإلكتروني ومنه تم توسيعه في القانون الفرنسي ليشملها كلها(الفرع الثاني) وهو نفس النهج الذي انتهجه المشرع الجزائري حيث أقر المبدأ لكن بنوع من التقييد بالنسبة لبطاقات الدفع (الفرع الثالث)، وقبل كل هذا يجب علينا تحديد مفهوم الأمر بالدفع الإلكتروني في القانون الجزائري(الفرع الأول).

---

[1]- خنفوسي عبد العزيز، قانون الدفع الإلكتروني، مركز الكتاب الأكاديمي، الطبعة الأولى 2018، الأردن، ص8.

[2]- réponse de la fédération bancaire française à la consultation de la commission européenne pour un « nouveau cadre juridique pour les paiements dans le marché intérieur », fédération bancaire française, 13 février2004, Fed-bancaire-Fr, le 25 /05/2017, http://fbf.Fr.

الفرع الأول

مفهوم الأمر بالدفع الإلكتروني في القانون الجزائري

يصدر الزبون المستعمل لوسيلة الدفع الإلكتروني أمرا ينفذه المصرف مقدم خدمة الدفع، أما اذا لم يكن للزبون رصيد بالحساب أو لا يتمتع بأي ائتمان فلا مجال لإصدار أوامر الدفع الإلكتروني (ثانيا)، و لابد من تنفيذ الأمر لإتمام عملية الدفع الإلكتروني (ثالثا)، وقبل كل ذلك ينبغي تعريف الأمر بالدفع الإلكتروني في القانون الجزائري حسب ما هو وارد في أنظمة بنك الجزائر (أولا).

أولا/تعريف الأمر بالدفع الإلكتروني في أنظمة بنك الجزائر

عرف المشرع الجزائري الأمر بالدفع من خلال تعريفه لقائمة من المصطلحات الواردة بالملحق المرفق بالنظام رقم 06/05 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى بأنه **عبارة عن تعليمة تطابق المواصفات الخاصة بوسائل الدفع**، كما يعرف في التشريع الفرنسي بالمفتاح المنشئ لعملية الدفع ونميز بين حالتين الأولى في حالة صدور الأمر عن الدافع (الآمر)، أما الثانية في حالة صدور الأمر عن المستفيد وتتحقق بتدخل وسيط أو بعد استلام الأمر بالدفع من طرف الدافع، أو على أساس القبول الصادر من طرف الدافع[1]، كما عرف المشرع العراقي الأمر بالدفع الإلكتروني بأنه الأمر الصادر من الدافع أو المدفوع له إلى مزود خدمة الدفع الإلكتروني المعني يطلب فيه

[1]-Stéphane Piedelièver, Doit bancaire, op, cit, P329.

تنفيذ معاملة الدفع[1] والأمر بالدفع بالنسبة لوسائل الدفع الإلكترونية لم يعد يصدر في شكل مادي ملموس بل في صورة معلومة مختزنة في أشرطة ممغنطة ويتم إعداد هذه الاشرطة عادة في البنوك أوفي بعض الشركات ذات الإمكانيات الكبيرة بحيث تعبأ وتجمع ثم يتم تداولها بين ذوي الشأن[2]، **فالأمر بالدفع عبارة عن معلومات تمت معالجتها لتصدر في شكل معطيات في صورة تعليمات.**

ثانيا/اصدار الأمر بالدفع الإلكتروني

الأمر بالدفع تصرف قانوني يصدر وفقا لوسيلة الدفع المستخدمة، وينبغي على الصيرفي الموجه إليه الأمر بالدفع التثبت من وجود الأمر[3]، ولابد أن ينتقل إلى الجهاز المصرفي لتنفيذه، فبالنسبة لأمر التحويل المصرفي يرسل الزبون الأمر مباشرة إلى المصرف الذي يحتفظ لديه بحساب الوديعة الجارية، وبالنسبة لبطاقة الدفع فيقوم التاجر بتجميع الايصالات التي تحمل توقيعات حاملي البطاقات ويرسلها إلى الجهة المصدرة للبطاقة[4] واعتبر المشرع الجزائري الأمر بالدفع عبارة عن تعليمة تطابق المواصفات الخاصة بوسائل الدفع وبالنسبة للأوراق التجارية الإلكترونية فيقوم (المسحوب عليه) بإرسال أمر الدفع أو بالأحرى التوقيع

---

[1]- أنظر المادة 01 /سابعا من النظام رقم 03 لسنة 2014، قرار مجلس الوزراء رقم 186لسنة 2014، الوقائع العراقية، العدد4326، الصادر في 2014/06/23.

[2]- عصام ابراهيم القليوبي، تطور أدوات الوفاء ومشكلاته القانونية، الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، لبنان، الطبعة الثانية، 1999، ص113.

[3]- عادل البراهمي، مسؤولية الصيرفي في وسائل الدفع، مداخلة مقدمة ضمن ملتقى مسؤولية الصيرفي، المنظم من طرف مركز الدراسات القانونية والقضائية بالاشتراك مع الجمعية المهنية لبنوك تونس، 18 فيفري 1999، منشورات مركز الدراسات القانونية والقضائية، 2000، تونس ص 44.

[4]- عصام ابراهيم القليوبي، المرجع السابق، ص109.

على أمر الدفع وإرساله إلى المصرف الذي يقوم بالوفاء بعد وصول الأمر إليه، في القانون الفرنسي يتم إصدار الأمر بالدفع عن طريق خياران:

الأول: إصدار الأمر بالدفع إلى مقدم الخدمات عندما يتعلق الأمر بالتحويل.

الثاني: إصدار الأمر بالدفع عن طريق وسيط المستفيد وهذا الأخير أي وسيط المستفيد بعد أن استقبل من الآمر (الدافع) الأمر بالدفع يرسله حينئذ إلى مقدم الخدمات الدافع لهذا الأخير ويمكنه أن يقدم عن طريق وسيط أو وساطة الشخص الملزم بالدفع نفسه وهي الحالة المتعلقة بالبطاقات البنكية، كما يمكنه تنفيذ عملية الدفع أيضا عن طريق إصدار أمر من المستفيد الذي يعطي الأمر لمقدم خدمات الدفع وهذا الأمر قائم على الموافقة التي أبداها الدافع للمستفيد والأمر نفسه يمكن أن يصدره وسيط مقدم الخدمات نفسه وهي الحالة المتعلقة بالاقتطاع[1]، وفي الأنظمة بوسيط المؤسسة التي تقوم بالوساطة لا يكون لها أبدا علاقة مباشرة بالأموال إنما هي مجرد وسيط بين البائع والمشتري والمصرف الذي يسمح بالدفع بعدما تأكد المصرف أن حساب المشتري كان ممونا[2].

ففي البطاقات الإلكترونية تم استدال التوقيع اليدوي للآمر بتوقيع إلكتروني عبارة عن رقم كودي سري يحتفظ به الحامل ثم يقوم بتسجيله على جهاز خاص لدى المتجر وهو ما يثبت هوية الآمر بالدفع ويترتب على تسجيل الرقم على الجهاز للقراءة ميلاد أمر بالدفع غير قابل للرجوع فيه من الزبون إلى الجهة المصدرة للبطاقة والتزام الزبون بأن يسدد لهذه الجهة المبلغ

[1]- Dominique legeais, op, cit, p785.
[2]- Pierre Bresse, Guillaume Beaure d'Augères et Stéphanie Thuillier, op, cit, p 136.

الذي أدته نيابة عنه للتاجر[1]، ومنه نستنتج أنه على المصرف الذي يتلقى الأمر بالدفع أن يتثبت من نموذج توقيع صاحب الحساب المودع لديه عند فتح الحساب لأول مرة مهما كانت وسيلة الدفع[2] وبالخصوص إذا كانت الوسيلة إلكترونية، وقد لا يحتاج الأمر إلى اصدار أي محرر أو أشرطة ممغنطة بالنسبة للمؤسسات التي تمتلك أجهزة حاسبات آلية ذات اتصال دائم بأجهزة حاسبات مركزية سواء في المصارف أو الشركات حيث يتم اصدار الأمر بمجرد الضغط على الأزرار وتسجيل المعلومات المطلوب تنفيذها من قبل الطرف الآخر.

ثالثا/تنفيذ الأمر بالدفع الإلكتروني

بعد وصول الأمر إلى المصرف القائم بالتنفيذ لأمر الدفع الصادر عن زبونه تتم عملية الدفع بعدد من القيود الحسابية بين مصرف الآمر ومصرف المستفيد من الأمر وعادة ما يتم ذلك من خلال غرف المقاصة (نظام المقاصة في القانون الجزائري) حيث يقدم كل بنك إلى البنوك الأخرى في جلسة المقاصة قائمة بحقوقه لديهم ويتلقى منهم أوامر الدفع المسحوبة عليه ولما كانت كل البنوك تحتفظ بحساب لدى بنك الجزائر **بحساب جار دائن بعنوان نظم الدفع**[3] فتتم تسوية الديون والحقوق بأوامر تحويل على هذه الحسابات بحيث لا تنتهي الجلسة إلا وكل طرف قد حصل على حقوقه لدى الطرف الآخر وأدى ما عليه من ديون لصالحهم،

[1]- عصام ابراهيم القليوبي، المرجع السابق، ص113.

[2]- عادل البراهمي، المرجع السابق، ص 46.

[3]- المادة 52 من الأمر المتعلق بالنقد والقرض المعدل والمتمم "يجب على كل بنك يعمل في الجزائر أن يكون له حساب جار دائن مع بنك الجزائر لتلبية حاجات عمليات التسديد بعنوان نظم الدفع ".

وهذه العملية تتم بصفة منتظمة ويوميا وإذا لم يكن أحد البنوك عضوا في غرفة المقاصة فإنه يكون ممثلا عن طريق أحد البنوك الأخرى الأعضاء لينوب عنه في تنفيذ العمليات ثم يقوم المصرف سواء بالخصم أو الاضافة لحساب زبونه.

ينبغي أن يقع تنفيذ أوامر الدفع بالسرعة اللازمة والمعقولة وهنا سيجد الصيرفي نفسه مجبرا على التوفيق بين عنصري ضغط أساسيين فمن ناحية عليه التثبت والتدقيق في عمليات الدفع حتى لا يرتكب خطأ موجبا لمسؤوليته، ومن ناحية أخرى يقع عليه واجب الاسراع في تنفيذ أمر الدفع لأن التأخير المفرط فيه قد يكون بدوره موجبا لإثارة مسؤوليته[1].

يتم إخطار ذوي الشأن بنتيجة تنفيذ الأمر بالدفع وهذا يتم عمليا من خلال كشف الحساب الذي يرسل للزبون بصفة دورية أو باخطارات مستقلة فور الانتهاء من أي عملية تنفذ من خلال حساب الزبون[2]، وحرصا من القانون على حفظ الدليل في عمليات الدفع الإلكتروني أوجب على منفذ أوامر الدفع الإلكتروني أن يحتفظ في كشف داخلي بكل العمليات التي تمت في الدفع الإلكتروني بواسطة إحدى وسائل الدفع الإلكتروني وذلك لمدة زمنية ترك تحديدها لكل مشرع وطني[3].

[1]– عادل البراهمي، المرجع السابق، ص 46.

[2]– عصام ابراهيم القليوبي، المرجع السابق، ص110.

[3]– خنفوسي عبد العزيز، المرجع السابق، ص 08.

الفرع الثاني

توسيع مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني في القانون الفرنسي

عدم جواز التراجع عن الأمر بالدفع الإلكتروني يعتبر في الوقت الحالي مبدأ يحكم كل وسائل الدفع في القانون الفرنسي، فوسائل الدفع التقليدية بمجملها اكانت حاصلة بالعملة النقدية أو بالشيكات أو بواسطة السندات فهي جميعها لا تقبل مبدئيا الرجوع أو التراجع عنها وذلك عملا بالمبدأ العام المعمول به في شأن وسائل الدفع القائل بعدم جواز نقض الدفع أو التراجع عنه (principe de l'irrévocabilité du paiement)[1]، وتنص المادة 69 من القانون المتعلق بالتجارة الإلكترونية الفرنسي[2] (Irrévocabilité des instructions de paiement) أو عدم رجعية تعليمات الدفع التي تمت بأي وسيلة دفع إلكترونية، فالملاحظ أن الدفع بوسائل الدفع الإلكتروني تخضعه غالبية القوانين إلى المبدأ ذاته الثابت في القانون الفرنسي حاليا وهو أن الحامل لا يستطيع التراجع عن التعليمة التي أعطاها بواسطة وسيلة الدفع الإلكتروني[3].

هذا المبدأ ثابت بالنسبة لكل وسائل الدفع الإلكتروني في القانون الفرنسي حاليا في حين كان سابقا يخص فقط الأمر الوارد في بطاقة الدفع لأن القانون الفرنسي كان يقر المبدأ ذاته

---

[1]– طوني عيسى، حول الدفع الإلكتروني بالبطاقة الائتمانية في شبكة الانترنت، بحث مقدم إلى أعمال المؤتمر السنوي لكلية الحقوق بجامعة بيروت العربية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، الجزء الأول الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى 2007، ص253.

[2]- loi du 14 aout 2000 relative au commerce électronique.

[3]- ART L69CMF Irrévocabilité des instructions de paiement « le titulaire ne peut révoquer une instruction qu'il a **donnée au moyen de son instrument de paiement électronique,** l'exception de celle dont le montant n'est pas connu au moment où l'instruction est donnée.

صراحة في المادة 57-2 من المرسوم التشريعي الصادر سنة 1935 والمعدل سنة 1991 "...أمر الدفع بالبطاقة هو غير قابل للرجوع عنه ...ولا يمكن الاعتراض على الدفع إلا في حالة فقدان البطاقة أو سرقتها أو في حالة التصفية القضائية للمستفيد"[1]، أو في حالة الاستعمال غير المشروع للبطاقة أو المعطيات المرتبطة باستعمالها[2]، مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني كان يطبق على كل عمليات الدفع التي تتم بواسطة البطاقات البنكية ومهما كانت الدعامة التي تستعمل للاتصال، وانتقل هذا المبدأ للتطبيق على الدفع الرقمي من خلال شبكة الانترنت وهذا بهدف حماية المستهلكين عبر الانترنت[3].

يبدوا هذا المبدأ مهما لإضفاء طابع التجريد على أمر الدفع وجعله مستقلا عن العلاقات الأساسية بين أطراف عملية الدفع وهي البيع أو تقديم الخدمة، حيث تشكل مسألة عدم جواز التراجع عن الأمر بالدفع عنصرا أساسيا سواء بالنسبة لمصدر البطاقة أو المستفيد من الأمر بالدفع[4].

الفرع الثالث

تقييد مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني في القانون الجزائري

نلاحظ أن المشرع الجزائري تبنى نفس الاتجاه القديم للمشرع الفرنسي وهو حصر تطبيق مبدأ عدم جواز التراجع عن الأمر بالدفع على الأمر الصادر بموجب بطاقة الدفع وحبذا لو

[1]- طوني عيسى، المرجع السابق، ص 253.

[2] -Étienne Wéry, paiement et monnaie électroniques, op. cit, p74.

[3]-pierre Bresse, guillaume Beaure D'Augères et Stéphanie Thuillier, op, cit, p119.

[4] -Étienne Wéry, paiement et monnaie électroniques, op, cit, p72.

وسع الأمر ليشمل كافة وسائل الدفع الإلكتروني، حيث تنص المادة 543 مكرر24 من القانون التجاري الجزائري"...الأمر أو الالتزام بالدفع المعطى بموجب بطاقة الدفع غير قابل للرجوع فيه، ولا يمكن الاعتراض على الدفع إلا في حالة ضياع أو سرقة البطاقة المصرح بهما قانونا أو تسوية قضائية أو افلاس المستفيد "، فالتاجر[1] هو الشخص الذي يتمتّع بقاعدة عدم جواز الرجوع في الأمر بالدفع وعدم المعارضة بالاحتجاجات وللاعتراف بصحة الدفع الإلكتروني عبر الانترنت بمختلف وسائل الدفع الإلكترونية، وبالتالي تطبيق مبدأ عدم جواز التراجع عن الدفع الإلكتروني يشترط القيام بإجرائيين شكليين محددين في نفس الوقت هما: أولا ابراز البطاقة، وثانيا إدخال الرقم أو الرمز السري[2]، ونفس الشي بالنسبة لوسائل الدفع الإلكترونية الأخرى التي يجب أن تقيدها اجراءات شكلية محددة لكن الأمر يختلف إذا حصل الدفع بالبطاقة ووقع حاملها إلكترونيا عن بعد طبقا لآلية تعريف وتصديق فعليين أي أن تستخدم أدوات التشفير في التوقيع وأن يصادق على الدفع طرف ثالث هنا لا يبقى براينا أي مجال لاستبعاد تطبيق مبدأ عدم قابلية التراجع عن الدفع على أساس أن التوقيع الإلكتروني يعتبر في هذه الحالة مماثلا للتوقيع اليدوي[3]، إن لم نقل أكثر أمانا من التوقيع اليدوي لأنه معزز بالتصديق الإلكتروني، وبالنسبة للنقود الإلكترونية فهي تتناقص كلما تم استخدامها في

[1]–هذا المبدأ قد لا يكون في صالح حامل البطاقة الذي قد يقتني البضاعة من التاجر ويتولّى خلاص ثمنها عن طريقها وحين يتبيّن أنها غير التي اختارها أو أنّها معيبة فأنّه لا يمكن له إثارة هذا العيب أو الخطأ في المبيع والرجوع في الأمر بالدفع، ولا يمكنه معارضة البنك بالدفوعات المتعلّقة بعمليّة البيع.

[2]– طوني عيسى، المرجع السابق، ص255.

[3]– طوني عيسى، المرجع نفسه، ص 255.

عملية تسوية الديون فإذا نفذ المخزون أعيد شحنها من جديد ولا رجوع في الدفع بها[1]، لأن النقود الإلكترونية تمثل نقودا عادية يتم تحويلها إلكترونيا فإن المبدأ العام يجيز نقض الدفع في عمليات التحويل وإمكانية التراجع عنها إذا لم تقيد قيمة التحويل في حساب التاجر بمعنى أن العملية لم تصبح نهائية ولكن البنوك والهيات المصرفية في اتفاقاتها مع الزبائن تؤكد مبدأ عدم جواز التراجع عن الدفع في كل التحويلات الإلكترونية بحجة أن عملية الدفع الإلكترونية عملية لحظية لا يمكن التراجع عنها[2].

يترتب على قطعية الأمر بالدفع وعدم قابليته للرجوع فيه نتيجة هامة مفادها أنه لا يتأثر بموت من صدر منه أو بفقدانه الأهلية أو سحب البطاقة من حاملها، وحامل وسيلة الدفع الإلكتروني يستطيع الاحتفاظ بدليل اثبات على تمام عملية الدفع على عكس ما تنص عليه القواعد العامة الخاصة بأمر الدفع أو أمر التحويل التقليدي الذي يعتبر أمر قابل للمعارضة أو الرجوع فيه[3].

---

[1]- سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية، القاهرة، ص 65.

[2]- نضال اسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الاصدار الأول، 2005، ص،126، ص127.

[3]- واقد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة لنيل درجة الماجيستير، فرع القانون العام، تخصص قانون التعاون الدولي، جامعة مولود معمري تيزي وزو، تاريخ المناقشة 2011/05/09، ص 95،96.

نستنتج أن مبدأين اثنين يشاركان في تأمين المستفيد هما عدم رجعية الأمر بالدفع الذي يترتب على مصدره، وضمان الدفع الذي يعتبر خدمة مكملة تترتب على المؤسسات المقدمة لخدمة الدفع[1]، فهذا المبدأ يعتبر كذلك قاعدة جوهرية للتعامل بوسائل الدفع الإلكتروني.

المبحث الثاني

المفهوم القانوني لوسائل الدفع الإلكتروني

نظرا لسلبيات النقود ابتكر التجار وسائل دفع أيسر بداية بالسندات التجارية Effets de commerce إلا أن مسألة التعامل بها تعد أمرا اختياريا، غير أن تدخل البنوك في الحياة الاقتصادية صاحبه ابتداع وسائل أكثر يسرا وهي نقود الودائع (النقود الائتمانية أو النقود القيدية)، وتتحكم فيها البنوك كوسيلة وفاء موازية للنقود القانونية أو بديل عنها[2]، وتجردت النقود من كل مظهر مادي ولم تعد تظهر في شكل معدني أو ورقي وإنما في شكل قيود كتابية في الحسابات المصرفية المختلفة ويعتبر قبول التعامل بها أمرا اختياريا كذلك.

غزت الحياة ظاهرة المعلوماتية وبدأ نظام تحويل الأموال إلكترونيا من قبل المصارف التي تتبادل الأموال فيما بينها فتنتقل الديون المحفوظة في سجلات مخزنة في الحواسيب الآلية من مصرف إلى آخر وتنتقل المعلومات بسرعة وكفاءة ويعاد تصحيح السجلات في ظل تلك

[1]-réponse de la fédération bancaire française à la consultation de la commission européenne pour un « nouveau cadre juridique pour les paiements dans le marché intérieur », fédération bancaire française, 13 février2004, Fed-bancaire-Fr,

[2]- عصام ابراهيم القليوبي، المرجع السابق، ص98.

التحويلات[1]، ووسائل الدفع الإلكتروني ترتبط بشدة بالتقنية[2]، وهي ترتبط ارتباط وثيق بموضوع النقود التي تلقى قبولا عاما كوسيلة للتسديد، بالتالي إزالة للغموض وتوضيحا وإلماما بمفهوم وسائل الدفع الإلكتروني نتطرق في المطلب الأول إلى (تمييز مفهوم وسائل الدفع الإلكتروني عن غيرها من المفاهيم)، ونخصص المطلب الثاني لتوضيح (مفهوم وسائل الدفع الإلكتروني في القانون الجزائري).

المطلب الأول

تمييز مفهوم وسائل الدفع الإلكتروني عن غيرها من المفاهيم

مفهوم وسائل الدفع الإلكترونية كان ولا يزال موضع أخذ ورد من قبل العاملين في القطاعات القانونية والاقتصادية والتقنية[3]، لهذا نجد أن مفهوم وسائل الدفع الإلكتروني يرتبط بالعديد من النواحي وهذا ما سنسلط عليه الضوء في (الفرع الأول)، كما نلاحظ ارتباط هذا المفهوم بالعديد من المفاهيم الأخرى لذلك نحاول التمييز بين المصطلحات المشابهة ونبين معنى كل مصطلح حتى يتجلى لنا مفهوم وسائل الدفع الإلكتروني في (الفرع الثاني).

الفرع الأول

[1]– أحمد سفر، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2008، ص5.

[2] - Étienne Wéry, facture, monnaie et paiement électronique, op, cit, p44.

[3]– حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2014،2015، ص16.

المفاهيم المرتبطة بوسائل الدفع الإلكتروني

وسائل الدفع الإلكترونية عبارة عن أدوات وتقنيات لتحريك الأموال بشكل إلكتروني، وهناك من يعرف وسائل الدفع على أنها كل الأدوات التي مهما كانت الدعائم والأساليب التقنية المستعملة فيها تسمح لكل الأشخاص بتحويل الأموال[1]، ولتحريك الأموال إلكترونيا لابد أن نرتبط بنظام للمعالجة الآلية للمعطيات وهو ما سنتناوله (أولا)، ثم نوضح ارتباط مفهوم وسائل الدفع الإلكترونية بالتجارة الإلكترونية (ثانيا).

أولا/ارتباط مفهوم وسائل الدفع الإلكتروني بالمعالجة الآلية للمعطيات (البيانات)

الخاصية المميزة أساسا لنظام الدفع الإلكتروني هو الآلية وهذا يعني عمل النظام بالاستغناء أو دون حاجة لتدخل الانسان[2]، ويعد نظام المعالجة الآلية للمعطيات الشرط الأول الذي يلزم تحققه لكي نبحث بعد ذلك ما إن كان هناك اعتداء على نظم المعالجة الآلية للبيانات من عدمه، كما أن الضرر المترتب على تدمير نظم المعالجة الآلية للمعطيات يفوق الضرر الناجم عن إتلاف المعدات المادية الخاصة بنظم المعلومات وذلك لأن البيانات والمعلومات أصبحت ذات قيمة مالية واقتصادية[3]، فلكي نتحدث عن جريمة مرتبطة بوسائل الدفع الإلكتروني يجب أن يكون هناك بالطبع قاعدة معالجة آلية للبيانات أو المعلومات التي تتعلق بهذه الوسائل وبالمصرف، ومصطلح المعالجة الآلية يعني أن العمليات المنجزة كليا

[1]- Bonneau Thierry ,Droit bancaire,4éme édition ,Editeur Montchretien, Paris, 1994, P41.
[2]- Xavier Thunis, responsabilité du banquier et automatisation des paiements, travaux de la faculté de droit de Namur, presses universitaires de Namur, p291.
[3]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الطبعة الأولى سنة، 2002، مصر، ص 21.

أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها[1] فأوكل بذلك مهمة تعريفه كل من الفقه و القضاء فالفقه الفرنسي يجمع على أن نظام المعالجة الآلية ينصرف إلى المعلومات والنظام الذي يحتوي عليها وكذلك إلى الشبكات[2].

بالرجوع إلى المادة 2/ب من القانون رقم 04/09[3] نجدها عرفت المنظومة المعلوماتية على أنها "نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين" والملاحظ على المادة أنها أخذت بالمعلومات المعالجة تنفيذا لبرنامج معين سواء داخل نفس النظام، أو النظام ككل في حالة ارتباطه بأنظمة أخرى.

كما أن القضاء الفرنسي وسع من مفهوم نظام المعالجة الآلية واعتبر من قبيل أنظمة المعالجة الآلية (un disque dur و un radiotéléphone و le réseau de Carte bancaire)[4].

بالتالي نستنتج أن التعامل بوسائل الدفع الإلكتروني يعد من قبيل أنظمة المعالجة الآلية للمعطيات ويرد على منظومة معلوماتية.

---

[1]- أنظر المادة 03 من القانون رقم 07/18.

[2]- بوريابة صورية، قواعد الأمن المعلوماتي دراسة مقارنة، مذكرة لنيل درجة الدكتوراه في العلوم، تخصص علوم قانونية، فرع القانون الخاص، جامعة الجيلالي اليابس، سيدي بلعباس، السنة الجامعية 2015_2016، ص 89.

[3]- القانون رقم 04/09 المحدد للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، المؤرخ في 05أوت 2009،ج ر عدد47، 2009.

[4]- بوريابة صورية، المرجع السابق، ص 89.

ثانيا/ارتباط مفهوم وسائل الدفع الإلكتروني بالتجارة الإلكترونية

بالنظر لكون هذه الوسائل ترتبط ارتباطا مباشرا بالتجارة الإلكترونية فالتعريف القانوني لوسائل الدفع الإلكترونية يرتبط بتعريف التجارة الإلكترونية والتي تعني الاستعمال الأمثل لكل أنواع تكنولوجيا الاتصالات المتاحة من أجل تنمية النشاط التجاري للمشروعات[1]، وعرفت المادة السادسة الفقرة الأولى من القانون المتعلق بالتجارة الإلكترونية التجارة الإلكترونية بأنها النشاط الذي يقوم بموجبه مورد إلكتروني[2] باقتراح أو ضمان توفير سلع أو خدمات عن بعد لمستهلك إلكتروني[3] عن طريق الاتصالات الإلكترونية ، وخصص الفصل السادس بعنوان الدفع في المعاملات الإلكترونية من القانون السالف الذكر المواد من 27إلى 29 وبينت كيف تتم عمليات الدفع الإلكتروني بواسطة وسائل الدفع الإلكترونية عبر منصات الدفع الإلكتروني والتي تخضع لرقابة بنك الجزائر، فضلا عن تعريفه لوسيلة الدفع الإلكتروني في الفقرة الخامسة من المادة السادسة لأن وسائل الدفع الإلكتروني من ضمن الأشكال الحديثة للنقود التي يتم الوفاء عن طريقها في معاملات التجارة الإلكترونية وهذا المصطلح وسائل

---

[1]- التجارة الالكترونية (électronique commerce): تعني مجموع النشاطات التجارية التي تتم عبر الشبكة العالمية المكونة من الحاسبات ووسائل الاتصال التي يتم تبادل البيانات من خلالها.

[2]- المورد الإلكتروني حسب المادة 04/06: كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الالكترونية.

[3]- المستهلك الإلكتروني حسب المادة 03/06: كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الإلكترونية من المورد الإلكتروني بغرض الاستخدام النهائي.

الدفع الإلكترونية يشير إلى تلك العملية غير الملموسة ماديا والذي يتم استعماله والمتاجرة به من خلال ابرام العقود والتصرفات القانونية عن طريق شبكة المعلومات الدولية[1].

الفرع الثاني

تمييز وسائل الدفع الإلكتروني عن المصطلحات المشابهة

يقتضي تمييز وسائل الدفع الإلكتروني عن غيرها من المصطلحات المشابهة والكثيرة الاستعمال تمييزها عن أنظمة الدفع الإلكتروني(أولا)، والوسائط الإلكترونية (ثانيا).

أولا /وسائل الدفع الإلكتروني وأنظمة الدفع الإلكتروني

يشير مصطلح نظام الدفع الإلكتروني إلى مجموعة من القواعد الإلكترونية والاعلام الآلي المستعملة في عملية تحصيل ودفع قيم وسائل الدفع المتبادلة بين البنوك[2]، ويقصد بأنظمة الدفع الإلكتروني البرامج الإلكترونية المساعدة أو المتممة لعملية استخدام بطاقات الوفاء حيث تعتبر هذه الأنظمة بمثابة قنوات يتم بموجبها استعمال البطاقات من خلال تلقيم هذه البرامج بالبيانات الخاصة بالبطاقة لكي يتمكن المستخدم بواسطتها دفع أثمان السلع والخدمات بعد خصمها من رصيد بطاقته[3]، وأنظمة الدفع الإلكتروني هي كل الأنظمة التي تستخدم في تسوية العمليات المالية عبر الوسائط الإلكترونية إذ يتم اعتمادها بين المصارف أو الشركات أو الأفراد من داخل الوطن الواحد أو خارجه وتعمل هذه الأنظمة على أساس

---

[1]-سلام منعم مشعل، المرجع السابق، ص 191.

[2]-بحيح عبد القادر، المرجع السابق، ص 32.

[3]- نقلا عن حسين عبد الله عبد الرضا الكلابي، المرجع السابق، ص 185.

نظامين الأول معروف باسم نظام التحويل الإلكتروني للأموال (EFT)[1]، أما الثاني فيعرف باسم نظام التبادل الإلكتروني للبيانات المالي[2](FEDI)، حيث يختلف هذا الأخير عن الأول بأنه يحول بيانات وشروحات الصفقات التي تمت بمعنى تحويل كلي للبيانات بصورة آنية عكس الأول حيث لا يتم تحويل إلا معلومات عن قيمة الصفقة وتعتمد المصارف عدة أنظمة للتحويل الإلكتروني من أشهرها أنظمة التحويل الداخلي للأموال وتنقسم إلى أربعة أقسام: منها نظام التحويلات التلغرافية (Virement par télégramme)، ونظام غرفة المقاصة الآلية (Chambre de Compensation Automatisée) ونظام تكنولوجيا التحويل الإلكتروني للأموال عند نقاط البيع (Transfert Electronique de Fonds aux Points de Ventes)، ونظام السويتش الإلكتروني (E-SWITCH).

أنظمة التحويل الإلكتروني للمدفوعات الدولية فمنها: نظام تحويل الأموال في أوربا (Le système de transfert express automatisé transeuropéen à règlement brut en temps réel)، ونظام الدفع الدولي سويفت (SWIFT)، وأخيرا نظام الدفع عبر الانترنت ومن أشهر هذه الأنظمة نظام[3](SET)، وأغلب البنوك الجزائرية تعمل بنظام سويفت للتحويلات الخارجية.

---

[1]- نظام التحويل الإلكتروني للأموال (EFT) Electronic Funds Transfers.

[2]-نظام التبادل الإلكتروني للبيانات المالية (FEDI) Financial Eltronic Data Interchange.

[3] - Secure Electronic Transaction.

أنظمة الدفع المعتمدة في المصارف الجزائرية نظام التسوية الاجمالية الفورية [1] (RBTR) ، ونظام المقاصة الإلكترونية للمدفوعات (Système de Compensation électronique pour les Paiements de masse)، والذي يعرف في الجزائر باسم (ATCI .Algérie-Télé compensation Interbancaire)[2].

يمكن أن نخلص إلى تعريف أنظمة الدفع الإلكتروني بأنها البرامج الإلكترونية المساعدة لاستخدام وسائل الدفع الإلكتروني وإتمام عملية الدفع حيث تقوم نظم الدفع الإلكترونية بمعالجة العمليات في الوقت الحقيقي real time.

ثانيا/ وسائل الدفع الإلكتروني والنقود الإلكترونية

ارتبط مفهوم وسائل الدفع الإلكتروني بالنقود الإلكترونية من حيث أن وسائل الدفع الإلكتروني ماهي في الحقيقة إلا عبارة عن النقود الإلكترونية أو السيولة الإلكترونية أو العملة الرقمية والتي يتم تبادلها بشكل إلكتروني، فوسائل الدفع الإلكتروني أوسع من النقود الإلكترونية، والنقود الإلكترونية ماهي إلا وسيلة من وسائل الدفع الإلكتروني.

كثيرا ما يخلط البعض بين مفهوم وسائل الدفع الإلكتروني و النقود الإلكترونية التي تعتبر وسيلة من وسائل الدفع الإلكتروني حيث أن الدفع الإلكتروني من الممكن أن يتم بعدة وسائل أخرى تختلف عن النقود الإلكترونية وبالتالي استعمال مصطلح النقود الإلكترونية للدلالة على كل أنواع الدفع التي تتم بطريقة إلكترونية استعمال غير صحيح، فالنقود الإلكترونية تعد

[1]- النظام رقم 04/05.

[2]- النظام رقم 06/05.

شكلا جديدا من أشكال وسائل الدفع عبر الانترنت وتأخذ هذه النقود صورة وحدات إلكترونية تخزن على القرص الصلب لجهاز الحاسب الآلي في مكان يسمى محفظة النقود الإلكترونية، أما مصطلح الدفع الإلكتروني فهو تعبير واسع يجمع في طياته كل وسائل الدفع الإلكترونية التي تستخدم فيها تكنولوجيا متقدمة للوفاء[1]، وعلى هذا فإن علاقة النقود الإلكترونية بوسائل الدفع الإلكترونية تمثل علاقة الجزء بالكل أي أن النقود الإلكترونية تمثل إحدى وسائل الدفع الإلكتروني بينما لا تعد كل وسائل الدفع الإلكتروني نقودا إلكترونية[2]، وبالتالي هذا يتناقض مع استخدام البعض لمصطلح النقود الإلكترونية للتعبير عن كل أنواع وسائل الدفع الإلكتروني ويجب عدم الخلط باستعمال هذا المصطلح خاصة مع بداية اتضاح المفهوم الوظيفي للنقود الإلكترونية.

ثالثا/ وسائل الدفع الإلكتروني والوسائط الإلكترونية

يختلف مفهوم وسائل الدفع الإلكتروني كذلك عن الوسائط الإلكترونية المصرفية وهي مجموعة من الخدمات التي تقدمها المصارف يمكن بواسطتها للزبائن الاستفادة من خدمات المصرف عبر الانترنت مثل الهاتف المصرفي وخدمات المقاصة الإلكترونية والانترنت المصرفي[3]، ويجب أن نوضح أن الدفع الإلكتروني ليس مرادفا للدفع عبر الخط حتى ولو

---

[1]- نقلا عن ذكرى عبد الرازق محمد، النظام القانوني للبنوك الإلكترونية، المزايا – التحديات –الافاق، دار الجامعة الجديدة للنشر، مصر ،2010، ص41.

[2]- أحمد السيد لبيب ابراهيم، الدفع بالنقود الإلكترونية الماهية والتنظيم القانوني دراسة تحليلية ومقارنة، دار الجامعة الجديدة للنشر الاسكندرية، مصر، 2009، ص 23.

[3]- حسين عبد الله عبد الرضا الكلابي، المرجع السابق، ص192.

كان المستقبل يتجه إلى تدعيم العمليات عبر الانترنت[1]، والوسائط الإلكترونية هي التي تستخدم في عملية الدفع الإلكتروني حيث أن تطور وسائل الدفع في صورة وسائل إلكترونية فرض أشكال مختلفة لكيفية تداولها[2]، ومنه نستنتج أن الوسائط الإلكترونية هي عبارة عن أشكال تستخدم لتتداول من خلالها وسائل الدفع الإلكتروني.

المطلب الثاني

تعريف وسائل الدفع الإلكتروني في القانون الجزائري

يمكننا القول أن وسائل الدفع الإلكترونية هي مجموع الأدوات والتحويلات الإلكترونية التي تصدرها المصارف والمؤسسات المالية أو أنها إمكانيات وجدت قصد تبادل منتجات وخدمات بأبسط طريقة مع توفر عنصر الأمان، و بسبب تنوع هذه الوسائل و اختلاف خصائصها أصبح من الصعب وضع تعريف محدد ودقيق لوسائل الدفع الإلكترونية خاصة أنها تطورت وتتطور لمصاحبة انتشار عمليات التجارة الإلكترونية وتدعيما لوسائل الدفع العادية وعليه سنركز على النصوص القانونية الجزائرية فقط التي تناولت تعريف وسائل الدفع (الفرع الأول)، ثم نتناول تعريف وسائل الدفع من خلال أنظمة بنك الجزائر (الفرع الثاني).

[1]- Étienne Wéry, facture, monnaie et paiement électronique, op, cit, p46.

[2]- لوصيف عمار، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين مع الاشارة إلى التجربة الجزائرية، مذكرة لنيل شهادة الماجيستير في العلوم الاقتصادية، تخصص تحليل و استشراف اقتصادي، جامعة منتوري قسنطينة، 2008، 2009 ص 32.

الفرع الأول

تعريف وسائل الدفع الإلكتروني في النصوص التشريعية الجزائرية

تستلزم وسائل الدفع الإلكتروني اطار قانوني محكم لأجل الحصول على ثقة الزبائن والمؤسسات، وكذلك تستلزم تأمين الأمن القانوني و العملياتي لأنظمة ووسائل الدفع[1]، المشرع الفرنسي عرف في الفقرة الثالثة من المادة (L133-4) من قانون النقد والمال وسيلة الدفع[2] بأنها الأداة نفسها بالإضافة إلى أي جهاز شخصي أو رمز سري وكذلك جميع الإجراءات المتفق عليها بين الزبون ومقدم خدمات الدفع لتوصيل أمر الدفع لهذا الأخير، وعرفت جمعية البنوك الفرنسية وسائل الدفع بأنها كل وسيلة تسمح بتحويل الأموال مهما كانت الدعامة أو الاجراء التقني المستعمل[3].

استعمل المشرع الجزائري مصطلح "وسائل الدفع الإلكتروني" لأول مرة في الأمر 06/05 المتعلق بمكافحة التهريب[4] لأنه اعتبر تعميم استعمالها من بين التدابير والإجراءات الوقائية لمكافحة التهريب وهذا لأنها تمكننا من متابعة مصدر ومصير الأموال، كما أضاف المشرع

[1]- réponse de la fédération bancaire française à la consultation de la commission européenne pour un « nouveau cadre juridique pour les paiements dans le marché intérieur », fédération bancaire française, 13 février2004, Fed-bancaire-Fr.

[2] - L133-4 « un instrument de paiement s'entend, alternativement ou cumulativement, de tout dispositif personnalisé, et de l'ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement et auquel l'utilisateur de services de paiement a recours pour donner un ordre de paiement».

[3]-réponse de la fédération bancaire française à la consultation de la commission européenne pour un « nouveau cadre juridique pour les paiements dans le marché intérieur », fédération bancaire française, 13 février2004.

[4]- أمر رقم 05-06 المؤرخ في 18 رجب عام 1426 الموافق ل23 أوت سنة 2005، المتعلق بمكافحة التهريب، ج ر عدد59، 2005.

الجزائري عند تعديله للقانون التجاري بموجب القانون 02/05[1] إلى الباب الرابع، الكتاب الرابع، من القانون التجاري " السندات التجارية "، الفصل الثالث "**بطاقات السحب والدفع** " في المادة 543 مكرر 23.

أولا/ تعريف وسائل الدفع الإلكتروني في قانون النقد والقرض

قانون النقد والقرض يعتبر أول قانون جزائري تحدث عن التعاملات الإلكترونية حيث كانت تنص المادة 113 من القانون 10/90 المتعلق بالنقد والقرض[2] على أنه "تعتبر وسائل دفع جميع الوسائل التي تمكن من تحويل أموال مهما كان الشكل أو الأسلوب التقني المستعمل" وهي مادة منقولة حرفيا عن المادة الرابعة من القانون البنكي الفرنسي لسنة 1984[3]، وعدلت بالمادة 69 من الأمر 11/03 المتعلق بالنقد والقرض " تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل " حيث انتقل المشرع من وسائل الدفع التقليدية إلى وسائل الدفع الإلكترونية الحديثة، ولم يحدد المشرع الجزائري وسائل الدفع الإلكترونية وذلك من خلال عبارة "...**مهما يكن السند أو الأسلوب التقني المستعمل** " الواردة بالمادة 69 من الأمر 11/03.

---

[1]- القانون رقم02/05 المؤرخ في 27 ذي الحجة عام 1425 الموافق 06 فيفري 2005 المعدل والمتمم للأمر 59/75 المتضمن القانون التجاري، ج ر عدد11، 2005.

[2]-القانون رقم 10/90 المؤرخ في 19 رمضان عام 1410 الموافق ل14 أفريل 1990 المتعلق بالنقد والقرض، ج رعدد16، 1990.

[3]-voir, annexes au rapport problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, op, cit,p22.

المشرع الجزائري من خلال هذه العبارة لم يحدد وسائل الدفع، ولم يحصرها وإنما جاءت هذه الوسائل بمعنى واسع بحيث يمكن أن تستوعب أي وسيلة جديدة في ظل التطور الدائم لتقنيات ووسائل الدفع، وهذا الاتجاه وعدم التحديد كان مقصودا من المشرع الجزائري ليشمل وسائل الدفع التقليدية المطورة ووسائل الدفع المستحدثة وكذا المنصوص عليها قانونا وتلك التي لم تشملها النصوص القانونية بصريح العبارة وهذا أخذا بالمعنى الواسع لوسائل الدفع الذي تبناه المشرع الجزائري، فوسائل الدفع بالنسبة للمشرع الجزائري هي نفسها الأدوات حيث لا اختلاف من حيث المصطلحات أو أي أسلوب تقني يمكن أن يبتكر مستقبلا لتحويل الأموال.

ثانيا/ تعريف وسائل الدفع الإلكتروني في قانون التجارة الإلكترونية

عرفت المادة السادسة الفقرة الخامسة من القانون05/18 المتعلق بالتجارة الإلكترونية وسيلة الدفع الإلكتروني بأنها "... كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو بعد، عبر منظومة إلكترونية... " فالمشرع الجزائري استعمل لأول مرة عبارة وسيلة الدفع مضاف إليها كلمة إلكتروني وهذا بخلاف النصوص السابقة التي كان يكتفي فيها بمصطلح وسيلة الدفع فقط دون اضافة مصطلح إلكتروني، و من خلال هذه المادة اعتبر المشرع الجزائري وسائل الدفع الإلكتروني هي الوسائل المرخص بها طبقا للتشريع المعمول به وبالتالي يفهم أن الوسائل المقصودة هي الوسائل التي رخص

بنك الجزائر للعمل بها لأنه اشترط وجوب تقديم الطلب لبنك الجزائر قبل اعتماد التعامل بأي وسيلة كما سنرى لاحقا.

اعتبر المشرع الجزائري وسائل الدفع الإلكتروني كل الوسائل التي يتم الدفع بها عن قرب أو بعد عبر منظومة إلكترونية[1]، واستعمل عبارة المنظومة المعلوماتية في القانون رقم 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال السابق الاشارة إليها في حين عرف الاتصالات الإلكترونية من خلال نص المادة العاشرة من القانون رقم 04/18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية بأنها كل ارسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية، وبالتالي فطبيعة التراسل من الممكن أن تكون مالية.

الفرع الثاني

تعريف وسائل الدفع الإلكتروني من خلال أنظمة بنك الجزائر

ورد في الملحق المرفق بالنظام رقم 06/05 الصادر عن بنك الجزائر المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى[2] تعريف لبعض المصطلحات منها تعريف وسيلة الدفع **وسيلة الدفع** أنها أداة تسمح **بغض النظر** عن السند أو العملية الفنية المستعملة بتحويل الأموال، تتمثل وسائل الدفع الأساسية في الصكوك، والتحويل

[1]- مصطلح إلكتروني أشمل من مصطلح معلوماتي .

[2]- النظام رقم 06/05.

والبطاقة المصرفية ...الخ ومن خلال **التعريف نلاحظ أن المشرع لم يستعمل مصطلح سند ولا عملية لأن المشرع من خلال النظام 06/05 وظف مصطلح وسيلة الدفع التي تسمح بتحويل الأموال مهما كان السند أو العملية الفنية المستعملة**، ومنه حسما للإشكالات التي يمكن أن يثيرها مصطلح وسيلة الدفع أضاف المشرع عبارة مهما يمكن السند أو الأسلوب أو العملية الفنية.

المشرع الجزائري استعمل مصطلح وسائل الدفع عموما وعرفها ضمن نصوص قانون النقد والقرض ومن خلال أنظمة بنك الجزائر في حين لم يورد مصطلح إلكتروني إلا من خلال قانون التجارة الإلكترونية حيث استعمل مصطلح وسائل الدفع الإلكتروني وربط استعمالها بالمنظومة الإلكترونية، في حين أن نصوص القانون التجاري أضاف من خلالها فقط بعض الوسائل إلى باب السندات التجارية.

الفرع الثالث

الإجراءات المتخذة من بنك الجزائر لضمان التعامل الجيد بوسائل الدفع الإلكتروني

تنص المادة 56 من الأمر المتعلق بالنقد والقرض المعدل والمتمم على أن "ينظم بنك الجزائر غرفة المقاصة ويشرف عليها، ويسهر على حسن سير نظم الدفع وأمنها وفقا لنظام مجلس النقد والقرض.

يتأكد بنك الجزائر من سلامة وسائل الدفع، غير العملة الائتمانية، وكذا اعداد المعايير المطبقة في هذا المجال وملاءمتها.

ويمكنه رفض ادخال أي وسيلة دفع لاسيما إذا كانت تقدم ضمانات سلامة غير كافية، كما يمكن أن يطلب من مقدم طلب إدخال هذه الوسيلة اتخاذ التدابير لتدارك ذلك ويبلغ بنك الجزائر لممارسة مهامه من قبل أي شخص معنوي بالمعلومات المفيدة التي تخص وسائل الدفع والأجهزة و الأجهزة التقنية المتعلقة بها ".

وتنص المادة 62 من الأمر المتعلق بالنقد والقرض على أنه "يخول المجلس صلاحيات بصفته سلطة نقدية ...هـ- إعداد المعايير وسير وسائل الدفع وسلامتها ".

اتخذ بنك الجزائر عدة إجراءات وقام بالعديد من الاصلاحات لضمان التعامل الجيد بوسائل الدفع الإلكتروني وهذا من خلال اشراف بنك الجزائر على تسيير وتأمن وسائل الدفع الإلكتروني (أولا)، ضرورة تقديم طلب إدخال وسيلة الدفع الإلكتروني لبنك الجزائر (ثانيا)، ارتكاز وسائل الدفع الإلكتروني على تدخل مقدمي خدمات التصديق الإلكتروني (ثالثا).

أولا/اشراف بنك الجزائر على تسيير وتأمن وسائل الدفع الإلكتروني

يقوم مجلس النقد والقرض بإعداد معايير سير وسلامة وسائل الدفع الإلكتروني، في حين يسهر البنك المركزي على تجسيد هذا النظام بإشرافه على سيرها وأمنها ويتأكد من سلامة الوسيلة، ويمكنه أن يطلب اتخاذ التدابير في حاله الشك في سلامة الوسيلة أو أن يتخذ قرار برفض إدخالها، و نجد أن المشرع الفرنسي يعتبر الوضع تحت التصرف لوسائل الدفع لدى

الزبائن من ضمن العمليات المصرفية حيث تشمل العمليات المصرفية استلام الأموال من الجمهور، عمليات القرض، والوضع تحت تصرف الزبائن لتسيير وسائل الدفع[1].

- أوجب الأمر 04/10 المتضمن تعديل[2] الأمر 11/03 المتعلق بالنقد والقرض على كل بنك أن يملك حساب دائن جاري[3] لدى بنك الجزائر لتلبية حاجات نظم الدفع وتسوية العمليات.

- يلتزم بنك الجزائر بالسهر على سلامة وفعالية نظم الدفع والسير الحسن لها[4]، وكذا مراقبة نظم الدفع وترك مسألة تحديد القواعد المطبقة على نظم الدفع لمجلس النقد والقرض من خلال الأنظمة التي يصدرها.

- يسهر بنك الجزائر على سلامة وسائل الدفع وإعداد معايير ملائمتها[5]، ويمكنه رفض ادخال أي وسيلة دفع لا تتضمن الضمانات الكافية أو أن يطلب اتخاذ التدابير الكافية إذا

---

[1]-Pierre Bresse, Guillaume Beaure d'Augères et Stéphanie Thuillier, op, cit, p 134.

[2]- أمر رقم 04/10 المؤرخ في 26أوت سنة 2010الموافق ل16 رمضان سنة 1431، المعدل والمتمم للأمر 11/03 المؤرخ في 27 اوت سنة 2003 والموافق ل27 جمادي الثاني سنة 1423 المتعلق بالنقد والقرض، ج ر عدد50، سنة 2010.

[3]- تنص المادة 04 من الأمر 04/10 المعدلة للمادة 52 من الأمر 11/03"يجب على كل بنك يعمل في الجزائر أن يكون له **حساب جار دائن** مع بنك الجزائر لتلبية حاجات عمليات التسديد بعنوان **نظم الدفع**".

[4]- تنص المادة 04 من الأمر 04/10 المعدلة للمادة 56 من الأمر 11/03 " يحرص بنك الجزائر على السير الحسن لنظم الدفع وفعاليتها وسلامتها.

تحدد القواعد المطبقة على نظم الدفع عن طريق نظام يصدره مجلس النقد والقرض.

يضمن بنك الجزائر مراقبة نظم الدفع ".

[5]- تنص المادة 05 من الأمر 04/10 المادة 56مكرر من الأمر 11/03" يتأكد بنك الجزائر من سلامة وسائل الدفع غير العملة الائتمانية وكذا إعداد المعايير المطبقة في هذا المجال وملائمتها، ويمكنه رفض ادخال أي وسيلة دفع، ولاسيما اذا كانت تقدم ضمانات سلامة غير كافية، كما يمكن أن يطلب من مقدم الطلب إدخال هذه الوسيلة واتخاذ كل التدابير لتدارك ذلك.

كانت وسيلة الدفع لا تتوفر عليها، ويجب على البنوك تقديم المعلومات التي تخص وسائل الدفع والأجهزة التقنية المتعلقة بها.

- تحميل المساهمين النفقات المتعلقة بتسيير نظم الدفع، كما يخول مجلس النقد والقرض باعتباره في الميدان إعداد المعايير المتعلقة بوسائل الدفع وسيرها وسلامتها[1].

- مسايرة لهذه التغيرات قام بنك الجزائر بإنشاء مديرية أنظمة الدفع (DSP)، والتي تندرج تحتها ثلاث مديريات فرعية والمتمثلة في المديرية الفرعية للعمليات، المديرية الفرعية لدعائم التقنية، المديرية الفرعية لرقابة أنظمة الدفع وتم انشاء مهام جديدة لبنك الجزائر خاصة فيما يتعلق بالتسيير اليومي والرقابة على أنظمة الدفع[2].

ثانيا/ ضرورة تقديم طلب إدخال وسيلة الدفع الإلكتروني لبنك الجزائر

تنص المادة 56 المعدلة سنة 2010 من الأمر المتعلق بالنقد والقرض على أنه يتأكد بنك الجزائر من سلامة وسائل الدفع، كما يمكنه أن يطلب من **مقدم طلب إدخال أي وسيلة** اتخاذ التدابير الكافية مما يفهم منه ضمنيا أن المصارف والمؤسسات المالية هي التي عليها تقديم طلب اعتماد وسائل الدفع الإلكتروني قبل إدخالها حيز التعامل، كما يحرص بنك

يبلغ بنك الجزائر لممارسة مهامه، من قبل أي شخص معني بالمعلومات المفيدة التي تخص وسائل الدفع والاجهزة التقنية المتعلقة بها ".

[1]- أنظر المادة 06 من الأمر 04/10 المعدلة للمادة 57 والمادة 62 من الأمر 11/03.

[2]- وتدخل بنك الجزائر من بين المشاركين في كل من بنك ATCIوARTS، وتم اعادة تقسيم العمليات أو نشاط مديريات البنك المركزي.

الجزائر على ضرورة توفر الأمن لاستعمال وسائل الدفع الإلكتروني بالتأكد من سلامة وسيلة الدفع أو الزام مقدم الطلب باتخاذ تدابير معينة لضمان سلامتها.

على المصدر واجب الاعلام المسبق قبل ابرام العقد المتعلق بتسليم و استعمال و سيلة الدفع الإلكتروني كتابيا أو إلكترونيا[1]، وضمان سرية الرموز ومراقبتها والتثبت منها و أن يقدم وصفا شاملا لوسيلة الدفع الإلكتروني ومميزاتها التقنية ووصفا شاملا لجميع الاستعمالات الممكنة لوسيلة الدفع الإلكتروني في الداخل والخارج عند الاقتضاء والسقف المحدد للعمليات المسموح بإجرائها بواسطة وسيلة الدفع الإلكتروني مع امكانية الزبون في اختيار السقف المحدد وكذلك في الحط منه في كل وقت ووصفا شاملا لواجبات الزبون والمصدر ومسؤولياتهما وكذلك المخاطر والاحتياطات المتعلقة باستعمال وسيلة الدفع الإلكتروني وأن يبين كيفية الاعتراض وإجراءاته وأجاله في حالة السرقة أو الضياع أو التزوير أو العدول عن استعمال وسيلة الدفع الإلكتروني والمصاريف المثقلة، وأن يضع على ذمة الزبون الوسائل اللازمة التي تمكنه من القيام بالإعلامات والسرقة وكذلك الوسائل التي تمكنه من اثبات قيامه بالعملية وأن يتخذ الاجراءات الفورية اللازمة لمنع استعمال وسيلة الدفع الإلكتروني موضوع الاعتراض، كما يجب اعلام الزبون بجميع العمليات المالية المنجزة بواسطة وسيلة الدفع الإلكتروني[2]، ويمنع على المصدر في غير حالات التجديد أو التعويض أن يسلم للزبون أو غيره وسيلة دفع لم يطلبها.

---

[1]- علي كحلون المرجع السابق، ص 56.

[2]- علي كحلون المرجع نفسه، ص57 .

ويحصل المصرف الذي يقوم بعملية الوفاء على عوائد مالية كبيرة سواء العائدة إلى تقديم خدماته الأساسية[1] المرتبطة بالدفع الإلكتروني أو الخدمات المتصلة والمساندة لعملية الدفع الإلكتروني وتتمثل العوائد المالية للخدمات الأساسية في الحصول على رسوم اصدار وسائل الدفع الإلكتروني التي تتفاوت من مصدر إلى آخر، وكذا النسبة المقتطعة من مبلغ كل عملية وفوائد التأخير وهذه الفوائد لتفادي المخاطر المرتبطة بوسائل الدفع الإلكتروني، وخاصة نسبة الفائدة وطريقة احتسابها وشروط المنازعة في العمليات المنجزة واجراءاتها والعنوان الذي توجه إلية الاعلانات والاعتراضات[2].

ثالثا/ارتكاز وسائل الدفع الإلكتروني على تدخل مقدمي خدمات التصديق الإلكتروني

تقوم معظم وسائل الدفع الإلكتروني على تدخل جهة ثالثة تتولى عملية تسوية المعاملات الإلكترونية ويقوم بهذا الدور عادة أحد البنوك أو غيرها من المنشات أو المؤسسات المالية التي يعهد إليها بهذه المهمة[3] وهناك من يسميه الوسيط الإلكتروني أو الموثق Certificateur لتأمين السرية والموثوقية لعمليات الدفع الإلكتروني، وفي القانون الجزائري يصطلح عليه مقدم خدمات التصديق الإلكتروني.

التصديق الإلكتروني بالنسبة لوسائل الدفع الإلكتروني يعني التوثيق الإلكتروني للرسائل المتبادلة بين البنك والزبون والخاصة بالبيانات والمعلومات المرتبطة بالعمليات التي تتم عن

---

[1]- حسين عبد الله عبد الرضا الكلابي، المرجع السابق، ص 175-ص219.

[2]- علي كحلون، المرجع السابق، ص 56.

[3]- ذكرى عبد الرازق محمد، المرجع السابق، ص 40.

طريق وسائل الدفع الإلكتروني، والتصديق لهذه البيانات يعني التأكد من صدور الأمر بالدفع من الشخص المنسوب إليه من خلال التحقق من هويته، وعدم وقوع تحريف أو تعديل في بيانات الوثيقة المتبادلة إلكترونيا باستخدام مفاتيح مشفرة يتم وضعها على الأمر بالدفع حتى يحتفظ بصحته ومصداقيته، وكذلك التوثق من سلامة الأمر بالدفع ومحرره ومن شهادة التصديق[1].

يتطلب السداد بوسائل الدفع الإلكتروني تدخل مقدمي خدمات التصديق الإلكتروني للتقليل من عدم قبولها أو عدم وجود رصيد كاف لسدادها، ويظهر ذلك جليا لو تتبعنا كيفية تمام السداد باستخدام الشيك الإلكتروني[2] وتدخل شخص ثالث لا يعد شرطا لازما لإتمام الدفع الإلكتروني **إلا أنه يجنب الكثير من المخاطر التي يمكن أن يتعرض لها المستفيد في حالة الدفع لو تمت التسوية بشيكات تقليدية لأنه بالنسبة للشيك التقليدي يغيب الارتباط بين عملية تحرير الشيك والتأكد من وجود الرصيد وهذا ما يعرضنا لخطر عوارض الدفع وانعدام**

---

[1]- غزالي نزيهة، تأمين وسائل الدفع الإلكترونية بآلية التصديق الإلكتروني في الجزائر على ضوء القانون الجديد 04/15، مداخلة قدمت في الملتقى الوطني حول الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر، المنظم من طرف كلية الحقوق والعلوم السياسية بجامعة محمد الشريف مساعدية بسوق أهراس، يومي 16و17 فيفري 2016.

[2]- مثلا شركة telecheck تعد خدمة قبول شيكات الانترنت من أهم الخدمات التي تقدمها وذلك على النحو التالي يقوم الزبون المشتري بزيارة موقع البائع ويتم تحويل الزبون بطريقة اوتوماتيكية الى مزود خدمة الشيكات الالكترونية الذي يرتبط اليا بمركز التسوية المؤقت ACH وذلك اذا ما قرر شراء منتج ويقوم البائع بإخطار مزود الخدمة باسم الزبون وعنوانه واجمالي قيمة الصفقة فيقوم مزود الخدمة بعرض نموذج للشيك الإلكتروني على الشاشة مبينا فيه البيانات التي حصل عليها المزود من البائع ويقوم الزبون بإضافة بعض البيانات الى هذا النموذج وعلى الأخص بيانات المصرف الذي يتعامل معه ورقم حسابه ورقمه الشخصي الذي زوده به الوسيط ويقوم المزود بالاتصال بمصرف الزبون عبر شبكة التسوية المؤقتة ACHليتأكد من مدى كفاية رصيد الزبون للوفاء بقيمة الشيك، ويقوم المزود بإيداع الشيك الإلكتروني لدى مركز التسوية المؤقت كما هو متبع تماما بالنسبة لشيك الورقي، أنظر سامي عبد الباقي أبو صالح، المرجع السابق، ص25،26.

الرصيد، على خلاف الحال بالنسبة للشيكات الإلكترونية غير المادية حيث يتوقف إتمام العملية التي حرر الشيك لتسويتها على التأكد من وجود رصيد كاف لتسويتها، وهذا هو دور التصديق بمعناه العام بالنسبة لوسائل الدفع الإلكتروني.

التصديق بمعناه الخاص بالنسبة لوسائل الدفع الإلكتروني يعني إجراء يقوم به طرف ثالث يقر بأن الشيء الذي بين يديه يتوافق مع معايير وشروط معينة كتوافق سلعة مع الشروط المطلوبة، أو توافق الخدمة مع المعايير المعمول بها وهذا ما يعرف بالتقييس حيث يشكل تقييس وسائل الدفع عنصرا مسبقا لإدخال التعامل الآلي على التبادلات ما بين البنوك ومنه عنصرا مسبقا لتحديث منظومة الدفع وتطويرها، وبالتالي فدور التصديق الإلكتروني بمعناه الخاص لوسائل الدفع ضروري لإثبات أن وسيلة الدفع الإلكتروني تتطابق مع المعايير والمواصفات والمقاييس العالمية[1].

وأشارت المادة 46 من قانون المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية لأول مرة في الجزائر بنص صريح إلى ضرورة تقييس الشيكات البريدية، وكذا وسائل السحب والدفع المسموح باستعمالها عند فتح حساب بريدي جاري، وأوجبت خضوع هذه الوسائل إلى المعايير والمواصفات التقنية التي يحددها بنك الجزائر.

[1]– غزالي نزيهة، تأمين وسائل الدفع الإلكترونية بآلية التصديق الإلكتروني في الجزائر على ضوء القانون الجديد 04/15، المرجع السابق.

المبحث الثالث

أنواع وسائل الدفع الإلكتروني في القانون الجزائري

أكثر المجالات التي استفادت من ثورة المعلومات القطاع المصرفي لأنه من البديهي أن ترافق وسائل الدفع الإلكتروني سواء الوسائل التقليدية المطورة أو الوسائل المستحدثة التجارة الإلكترونية، فتطور المعلوماتية وشدة الشكلية الصرفية(مبدأ الشكلية في قانون الصرف) كانا السبب وراء ظهور وسائل دفع إلكترونية جديدة والمحتوى العلمي تطور بسرعة والظاهرة التي كانت بعيدة اكتملت مع ظهور(النقود الإلكترونية)[1]، وتقسيم وسائل الدفع الإلكترونية إلى تقليدية ومطورة هو التقسيم هو المعتمد في الغالب، إلا أن المشرع الجزائري وخلافا لهذا الطرح عالج موضوع تقسيم وسائل الدفع الإلكتروني بنظرة مختلفة وبتقسيم مختلف، لذلك سنتناول في المطلب الأول(التحويل الإلكتروني للأموال، الأمر بالاقتطاع، بطاقات الدفع الإلكتروني) باعتبارها الوسائل المنصوص عليها في القانون التجاري الجزائري، وفي المطلب الثاني وسائل الدفع الإلكتروني المستخلصة من نصوص قانون النقد والقرض الجزائري وهي (الشيك الإلكتروني والنقود الإلكترونية).

[1] -Stéphane Piedelièver, Doit bancaire, op, cit, p265.

المطلب الأول

وسائل الدفع الإلكتروني في القانون التجاري

تضمن القانون التجاري الجزائري ثلاث وسائل دفع، الأولى هي التحويل الإلكتروني ورغم أنه عملية مصرفية قديمة و لكن الجديد اليوم هو الوسيلة الإلكترونية التي يتم بها وبالنظر إلى موضوع المذكرة سنتناوله في الشكل الإلكترون فقط (الفرع الأول)، والثانية الاشعار بالاقتطاع الذي يعتبر صورة من صور التحويل الإلكتروني للأموال (الفرع الثاني)، والثالثة بطاقات الدفع الإلكتروني باعتبارها وسيلة دفع إلكتروني مستحدثة (الفرع الثالث).

الفرع الأول

التحويل المصرفي الإلكتروني

التحويل المصرفي أداة الدفع الأساسية في النشاط الدفع البنكي، ووسيلة دفع مؤمنة ومفضلة الاستعمال من طرف الدولة[1]، يعد التحويل المصرفي الإلكتروني[2] أحد أشكال التطور في استخدام الوسائل الإلكترونية لنقل وتحريك الأموال من حساب إلى آخر تنفيذا لأوامر الدفع التي يتلقاها البنك من زبونه كما يعتبر من أهم وأخطر الموضوعات المؤثرة في حركة التجارة على الصعيدين الوطني والدولي وذلك لما تتمتع به هذه العملية من قدرة فائقة على تسوية المدفوعات فيما بين الأطراف عن طريق البنوك بشكل آمن وميسر ودون انتقال فعلي

[1]- Régine Bonhomme, instrument de crédit et paiement, LGDJ lextenso édition, 2013, 10 édition, p 329.

[2]- مفهوم التحويل الإلكتروني اشتق اسمه من الآلة المستخدمة في تنفيذه وهو الحاسوب، أنظر سليمان ضيف الله الزين، التحويل الإلكتروني للأموال ومسؤولية البنوك القانونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2012، ص43.

للنقود[1]، واستعمل المشرع الجزائري مصطلح التحويل في الفصل الأول من الباب الرابع من القانون التجاري ولم يقم بتحديد نوع التحويل وبالتالي نفهم أن المشرع الجزائري لم يحدد نوع التحويل إن كان تقليدي أو إلكتروني.

أولا /مفهوم التحويل المصرفي الإلكتروني

عملية التحويل المصرفي الإلكتروني هي مجرد أداة لتداول المبالغ المدونة في الحسابات المصرفية[2]، والتحويلات الإلكترونية للأموال تعتبر أساسا شكل لامادي للتحويل[3]، وهناك تشريعات قامت بالتوسيع أكثر من نطاق مفهوم التحويل الإلكتروني للأموال ليشمل جميع الحالات التي يتم بواسطتها استخدام أداة التحويل حتى ولو لم يؤدي ذلك إلى أثر على الذمة المالية للزبون كما في حالة استخدام أداة لمجرد الاطلاع على الحساب[4] ورغم أن التحويل المصرفي عملية مصرفية قديمة إلا أن المشرع الجزائري وبالنظر إلى مختلف التعديلات التي مست القانون الجزائري إلا أنه لم ينص على التحويل المصرفي إلا بتعديل سنة 2005 والجديد اليوم هو الوسيلة التي تتم بها العملية كما أن هناك فرق بين التحويل المصرفي التقليدي الذي يتم بنقل مبلغ من المال بين الحسابات(من حساب المدين إلى حساب

---

[1]- حوالف عبد الصمد، المرجع السابق، ص84.

[2]- نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، لبنان 2007، ص 186.

[3]- Christian Gavalda, Jean Stoufflet,instruments de paiement et crédit ,effet de commerce cheque, carte de paiement, transfert de fonds, 6edition ,lexis Nexis, p 424.

[4]- نقلا عن محمود محمد أبو فروة، مسؤولية البنك المدنية عن عمليات التحويل الإلكتروني دراسة مقارنة، الطبعة الأولى، 2014، دار وائل للنشر والتوزيع، الأردن، ص33.

الدائن)[1]، والحوالة التي يقوم فيها البنك بدور الوساطة بين طرفين لإنجاز عملية توصيل مبلغ معين من المال يسلمه أحد الأشخاص له في بلد أو في فرع معين على أن يتسلمها الطرف الآخر في بلد أو فرع آخر وتضمنت المادة 87 من القانون المتعلق بالبريد والمواصلات السلكية واللاسلكية[2] امكانية ارسال الأموال بالحوالات عن الطريق الإلكتروني[3]، وهي نفس المادة وردت ضمن القانون المتعلق بالقواعد العامة المطبقة على البريد والاتصالات الإلكترونية حيث تنص المادة 60 على امكانية ارسال الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن بريد الجزائر والمحولة بالبريد أو عن طريق الاتصالات الإلكترونية ونلاحظ بالمقارنة بين المادتين حذف مصطلحي عن طريق البرق أو الطريق الإلكتروني بالنسبة للمادة الأولى وتعويضه بمصطلح الاتصالات الإلكترونية وحسنا فعل المشرع لأنه سبق وأن عرف الاتصالات الإلكترونية ضمن المادة العاشرة من القانون المتعلق بالقواعد المطبقة على البريد والاتصالات الإلكترونية.

---

[1]- كان فقهاء القانون يعتبرون عند تعريفهم لعملية التحويل الإلكتروني للأموال أنها مرتبطة بفكرة المديونية ويقتصر الأمر في هذه العملية على نقل مبلغ من المال من حساب المدين إلى حساب الدائن ويقيد البنك المبلغ نفسه في الحسابين أي الجهة السلبية المدينة من حساب المدين ومن الجهة الايجابية الدائنة من حساب الدائن، أنظر سليمان ضيف الله الزين، المرجع السابق، ص37.

[2]- القانون 03/2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، المؤرخ في 05 أوت 2000 الموافق ل05 جمادي الأولى عام 1421، ج رعدد48، 2000.

[3]- المادة 87" يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني"

يجب التمييز بين تحويل المال إلكترونيا(EFT)[1]وتبادل المعلومات المالية إلكترونيا (F/EDT) فتحويل المال إلكترونيا هو (خدمة محددة) أو نظام لتبادل الأموال بين المصارف وتعني إسداء الخدمة لطرف واحد من أطراف الصفقة تتمثل في الدفعة المحولة (الأموال تنتقل على شكل معلومات) والتي تعتبر بحد ذاتها خدمة محددة، أما تبادل المعلومات المالية إلكترونيا (الخدمة الشاملة) فهو الإتمام الكامل للصفقة إلكترونيا ويعنى إيراد الشرح الكامل للصفقة بما فيه من تفاصيل وشروحات التحويل(مقدار الدفعة، عدد الفواتير، الخصومات بين الشركاء، والتعليمات والارشادات المحركة للأموال) وقبل أن يوجد نظام FEDI طورت المصارف أربعة أنظمة للتحويلات هي: التحويلات التلغرافية[2]WIRE TRACSFE، نظام CHIPS[3]، نظام SWIFT[4]، نظام ACH[5] ومنه فالتحويل الإلكتروني للأموال هو تحويل للمال بين الشركات نفسها أو بينها وبين الأفراد وذلك من خلال المصارف التي يتعاملون

---

[1]- نظام التحويلات المالية الإلكترونية EFT: هي عملية منح الإذن(permission) لمصرف ما للقيام بالتحويلات المالية الدائنة والمدينة إلكترونيا من حساب مصرفي إلى حساب مصرفي(débit or crédit) آخر، أي أن عملية التحويل تتم إلكترونيا عبر الهواتف وأجهزة المودم وأجهزة الحاسب الآلي عوض استخدام الأوراق، أنظر زهير بوشناق، المرجع السابق، ص55.

[2]- نظام يسمح بتسوية المدفوعات وتسديد التحويلات النقدية ذات المبالغ الكبيرة خلال نفس اليوم وبطريقة فورية بين الشركات والمستهلكين ويدير هذا النظام البنك الاحتياطي الأمريكي وبدأ استخدام التلغراف لإرسال واستلام التعليمات الخاصة بتحويل الأموال.

[3]-CHIPS: (Clearing House For International Payement System) عبارة عن غرفة مقاصة للتسوية في نهاية اليوم وهو ملك لجمعية نيويورك لبيوت المقاصة.

[4]-SWIFT: (Society for World Wide Interbank Financial Télécommunication) هو أكبر نظام عالمي للتحويلات المالية الإلكترونية والأسرع والأقل تكلفة يستعمل لتسوية التحويلات الخارجية والعالمية.

[5]- ACH: نظام بيت المقاصة المؤقت ويحكم عمل هذه الشبكة القواعد الصادرة عن مؤسسة NACHA وتختص بإجراء عمليات التحويل المالي صغيرة القيمة الخاصة بالمستهلكين إلى جانب إجراء المدفوعات المتوسطة والكبيرة.

معها باعتبار أن النظام المصرفي هو المعول عليه في تحويل وتحريك الأموال حيث أن جميع أنواع الدفوعات الجارية بالشيكات أو بالطرق الإلكترونية يتعين أن يتم تسويتها عن طريق المصارف ذات الصلة[1]، وبعد أن كانت البنوك تقوم بعملية التحويل بناء على أمر مكتوب وموقع من العميل، أصبح بالإمكان إعطاء الأمر بشكل إلكتروني نظرا لظهور أنظمة آمنة لاستخدامه[2] فبعدما كان يشترط أن يتم التحويل بإصدار أمر التحويل كتابة وإلا كان باطلا أصبح بالإمكان اصدار الأمر إلكترونيا وأصبح التحويل الإلكتروني للأموال يتم كليا أو جزئيا بوسيلة إلكترونية حيث يفوض الزبون المصرف المرخص له من بنك الجزائر لإجراء التحويل الإلكتروني للأموال أو إتمام قيد دائن أو مدين على حساب الأطراف، والحقيقة أن التحويل الإلكتروني لا يختلف عن التحويل التقليدي سوى أن الأمر بالتحويل يتم بطريقة الكترونية[3] وهناك اتجاه موسع يرى بأن التحويل المصرفي الإلكتروني يكون إلكترونيا إذا تمت أية خطوة من خطواته بشكل الكتروني، وهذا الاتجاه أوسع إذ اعتبر التحويل إلكترونيا متى كان أمر التحويل إلكترونيا أو تنفيذه إلكترونيا ويشمل كذلك الحالات التي يبدأ فيها أمر التحويل بشكل مكتوب على مستند ورقي إلا أن تنفيذه تم بشكل إلكتروني[4]، وهناك من يرى أن هذه الوسيلة ماهي إلا تطوير لاستعمال بطاقة الدفع خارج العلاقات بين البنوك

---

[1]- المصارف طورت أنواع من التحويلات هي : التحويلات التلغرافية _نظام التشيبس3_نظام السويفت4_ أي سي اتش، أنظر أحمد سفر، المرجع السابق، ص65.

[2]- حوالف عبد الصمد، المرجع السابق، ص84.

[3]- سامي عبد الباقي ابو صالح، المرجع السابق، ص31.

[4]- زينة غانم يونس العبيدي، مسؤولية المصرف عن أخطاء الكومبيوتر في النقل الإلكتروني للنقود، مجلة الرافدين، المجلد 11، العدد39، سنة 2009، ص06.

ويمكن إجراء تحويل للأموال وتتم العملية كلها بطريقة إلكترونية في البنك عن بعد أو البنوك دون شباك أو هي خاصة بالزبائن والمؤسسات التي تعمل على الخط[1].

المشرع الجزائري من خلال المادة 69 من الأمر 11/03المتعلق بالنقد والقرض المعدل والمتمم اعتبر وسائل الدفع كل الأدوات التي تمكن شخص من تحويل الأموال مهما يكن السند أو الأسلوب التقني المستعمل، فالمشرع اعتبر أن وظيفة وسائل الدفع هي تحويل الأموال ولا تشمل فقط تحويل الأموال من حساب إلى حساب آخر بل يشمل كذلك عمليات الإيداع والسحب التي تتم باستخدام وسائل الدفع واستعمل عند تنظيمه للتحويل من خلال المادة 543 مكرر19 الأمر بالتحويل هو الذي يوجهه صاحب الحساب إلى ماسك الحساب لتحويل الأموال أو القيم أو السندات المحددة القيمة إلا أن المشرع الفرنسي استخدم مصطلحين مختلفين للتمييز بين عملية التحويل بين الحسابات (virement) وعمليات التحويل التي تقوم بها وسائل الدفع التي تضعها البنوك رهن إشارة زبائنها (Transfer des fonds) والتي يقصد بها أساسا نقل الأموال من مكان إلى آخر.

وظائف وسائل الدفع هي نقل الأموال من وإلى الحساب بغض النظر عما إذا كانت وجهة أو مصدر تلك الأموال حساب آخر أم لا بل المهم في هذا الإطار أن يتم استخدام وسيلة الدفع لإصدار الأمر للبنك[2]، فالتحويلات الإلكترونية المتعددة والمختلفة في الولايات المتحدة الأمريكية تسمح للأشخاص استعمال بطاقة الدفع على الانترنت وتسوية مشترياتهم بطريقة

[1]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition, lexis Nexis, p424.

[2]- محمود محمد أبو فروة، المرجع السابق، ص37.

الكترونية[1]، أي القيام بالشراء عبر الانترنت وتحويل الأموال عن طريق استخدام بطاقة الدفع، أورد القانون النموذجي للتحويلات الدولية للأموال Model Law on (international crédit transfert) المعروف باسم(UNICITRAL) الصادر عن لجنة الأمم المتحدة سنة 1992 تعريف للتحويل الإلكتروني للأموال "بأنه مجموع العمليات التي تبدأ بأمر الدفع الصادر الآمر بهدف وضع قيمة الحوالة تحت تصرف المستفيد"[2] إلا أن هذه التقنية تستلزم استعمال حساب عبر الخط أو بطاقة دفع أو أي وسيلة دفع أخرى فالدفع يتم عن طريق رقم سري أو محفظة النقود الإلكترونية أو استعمال بطاقة افتراضية وكان استعمال أول بطاقة افتراضية سنة 2001عن طريق البنك على الشبكة (البطاقة الزرقاء) بمساعدة برنامج معبأ عبر الحاسب الآلي للزبون[3].

بالتالي حسب تحليلنا للمادة 543 مكرر19 والتي نصت على الأمر بالتحويل يمكن استعمال أي وسيلة من وسائل الدفع الإلكترونية التي تمكن أي شخص من تحويل الأموال كيفما كانت بشرط استخدام الوسيلة الإلكترونية لإصدار الأمر الذي يوجهه صاحب الحساب بشرط نقل الأموال من حساب إلى حساب آخر عكس بقية التشريعات التي يشمل فيها السحب والايداع وباقي العمليات.

[1] - Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, OPCIT, p424.

[2]- Article 2 de la loi type de la CNUDCI sur les transferts internationaux de crédit 1992 : « Aux fins de la présente loi:(A) «transfert de crédit» désigne la série d'opérations, à commencer par ordre de paiement du donneur d'ordre… ».

[3]- Christian Gavalda, Jean Stoufflet,instruments de paiement et crédit ,effet de commerce cheque, carte de paiement ,transfert de fonds, 6edition ,lexis Nexis,p424.

نرى بالنسبة للمشرع الجزائري أن نوع الكتابة لا يشكل أي مشكلة بعدما اعترف بالمساواة بين المستند المكتوب والمستند الإلكتروني[1]، كما أنه بالعودة إلى نص المادتين 543مكرر 19و543 مكرر 20 من القانون التجاري الجزائري لا نجد أي شرط يستلزم أن يكون أمر التحويل مكتوبا، وبالرغم من أن واقع العمل البنكي يظهر أن البنوك تقوم بطباعة أمر التحويل على الورق حتى يستطيع الزبون توقيعه إلا أنه في خضم التطورات التكنولوجية الحديثة سيكون الحديث عن الطباعة والتوقيع اليدوي أمرا متجاوزا[2]، إلا أن صدور الأمر بوسيلة إلكترونية يكون بالاتفاق بين الزبون والبنك على هذه الوسيلة[3].

يمكن أن نعرف عملية التحويل الإلكتروني للأموال بأنها تلك العملية التي يقوم فيها المصرف بقيد مبلغ معين في الجانب المدين من حساب الآمر بالتحويل وإجراء قيد دائن بذات المبلغ في حساب الشخص المراد التحويل له[4]، وتنفذ عمليات التحويل المصرفي عن طريق غرفة المقاصة أو ما يعرف عالميا بدار المقاصة العالمية وتخضع العملية للمقاصة الإلكترونية في الجزائر حسب نظام بنك الجزائر.

المشرع الجزائري وباستقراء نص المادة543مكرر19 من القانون التجاري الجزائري نلاحظ أنه لم يعرف التحويل الإلكتروني للأموال وإنما أورد العناصر والإجراءات الشكلية التي يجب أن تتقيد بها البنوك والتي يجب توفرها لإتمام هذه العملية والمتمثلة في:

---

[1]- رغم أن المشرع الجزائري لم يوضح المستند المكتوب المساوي للمستند الإلكتروني هل هو السند الرسمي أم السند العرفي وبمعنى آخر أن المشرع الجزائري لم يوضح موقع المستند الإلكتروني بين وسائل الاثبات.

[2]- محمود محمد أبو فروة، المرجع السابق، ص58.

[3]- أنظر سليمان ضيف الله الزبن، المرجع السابق، ص 78.

[4]- فياض ملفي القضاة، المرجع السابق، ص103.

1- الأمر الذي يوجهه صاحب الحساب إلى ماسك الحساب لتحويل الأموال والقيم والسندات المحددة القيمة.

2- بيان الحساب الذي يتم الخصم منه.

3- بيان الحساب الذي يتم إليه التحويل وصاحبه.

4- تاريخ التنفيذ.

5- توقيع الآمر بالتحويل ".

وبالنسبة للشرط الأول المتعلق بالأمر لم يحدد إن كان مكتوبا أم لا وبالتالي فإن المادة تستوعب كل أنواع التحويل ومنها التحويل الإلكتروني باعتبار أنه ليس هناك نص قانوني خاص بالتحويل الإلكتروني، كما أن ورود المادة ضمن الباب المتعلق ببعض وسائل الدفع يؤكد هذا، **وبالتالي يمكننا القول أن عملية التحويل المصرفي الإلكتروني في القانون التجاري الجزائري هي عملية القيد في حساب كل من الآمر بالتحويل والمستفيد بناء على الأمر بالتحويل سواء كان التحويل داخل نفس البنك أو بين بنكين أو أكثر وبحسابات لنفس الشخص (لا مانع من أن يكون الآمر بالتحويل هو المستفيد) أو لشخصين مختلفين مما يوحي بأن المشرع أخذ بالمعنى المقيد للتحويل وليس المعنى العام الذي يشمل استعمال كل وسائل الدفع الإلكتروني، فطبيعة التحويل وبعد التنازع الفقهي الدائر حول تكييفه وفق أحد العقود المعروفة تنتهي إلى نتيجة مهمة وهي أن التحويل المصرفي**

الإلكتروني عبارة عن وسيلة من وسائل الدفع الإلكتروني، وحسما للجدل قام المشرع الجزائري بإدراج التحويل ضمن الباب الخاص بوسائل الدفع في القانون التجاري الجزائري.

فالتحويل كتقنية يختص البنك بالقيام بها بناءا على الأمر الصادر من طرف زبونه وهذا الأمر قد يأتي في عدة أشكال فقد يسمح البنك لزبونه بإصدار بعض أوامر التحويل دون الحاجة إلى ابرام عقد خاص بخصوصها لأنه بمجرد قيام البنك بفتح الحساب للزبون يلزم بحد أدنى من الخدمات يقدمها له[1] وهو ما يؤكده القضاء المصري الذي اعتبر التحويل الإلكتروني للأموال ما هو إلا وسيلة من وسائل الفن المصرفي ابتكرتها المصارف مع تطور التكنولوجيا للوفاء بالديون لهذا لم يعتبر القضاء المصري عمليات التحويل عقودا بل اعتبرها عمليات مصرفية بحتة تحدث داخل جدران البنك ويحكمها الفن المصرفي[2]، وغياب قانون تشريعي إلزامي واضح في التحويل الإلكتروني للأموال و تكيف هذه التقنية مع التكنولوجيا الحديثة سمح بقبول التحويل في استعمالات جديدة[3].

[1]- محمود محمد أبو فروة، المرجع السابق، ص40.

[2]- سليمان ضيف الله الزين، المرجع السابق، ص 101،102 .

[3]-Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition, lexis Nexis, p 412.

ثانيا/اجراءات التحويل الإلكتروني للأموال

التحويل هو العملية المصرفية الأكثر سهولة معلوماتيا والأمر يمكن أن يصدر بطريق إلكتروني وهو الأكثر استخداما من طرف المؤسسات، و بدأ الخواص يقبلون عليه مع انتشار تقنية البنك المنزلي[1]، تتمثل إجراءات التحويل البنكي الإلكتروني في إجراءين:

1- الأمر بالتحويل (l'ordre de virement): أول ما يجب الإشارة إليه أنه يجب عدم الخلط بين التحويل كتقنية بنكية وبين الأمر بالتحويل virement لأن النظرية الحديثة للتحويل تقوم على فكرة النقود القيدية المتمثلة بالأرصدة المتيسرة معتبرة التحويل مجرد تقنية محاسبية يقوم فيها البنك بالقيد على الحساب تنفيذا لعقد الحساب أما الأمر الذي يصدر عن الزبون فهو مجرد وسيلة يستطيع الزبون أن يعبر من خلالها عن رغبته في اجراء التحويل[2]. خلافا للعادة المصرفية الجارية بوضع نماذج تحت طلب الزبائن يتم تعبئة فراغاتها لإتمام أمر التحويل، أصبح من الممكن أن يتم أمر التحويل بواسطة شريط ممغنط « Bande magnétique » وهو شريط تسجل عليه الأصوات والمعلومات في الحاسبات الإلكترونية[3]، فالأمر بالتحويل عبارة عن رسالة إلكترونية يتم إصدارها باستخدام الزبون لأداة التحويل التي

---

[1]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition, lexis Nexis, p414.

[2]- محمود محمد أبو فروة، المرجع السابق، ص29.

[3]- أحمد شكري السباعي، الوسيط في الأوراق التجارية "دراسة معمقة في قانون التجارة المغربي الجديد وفي اتفاقية جنيف للقانون الموحد وفي القانون المقارن، الجزء الثاني "في اليات الوفاء "الشيك ووسائل الأداء الأخرى، الطبعة الثالثة، 2010، ص384.

وضعها البنك رهن إشارته وتتضمن هذه الرسالة المعلومات المتعلقة بالعملية المراد من البنك تنفيذها وعادة ما يتوصل البنك بالأمر الصادر عن الزبون بشكل مباشر[1].

أمر التحويل يجب أن يستوفي الشروط المنصوص عليها في وجيز التقييس الصادر عن لجنة تقييس أدوات الدفع[2]، و يمكن أن يكون منفردا أو أن يعطى لمجموعة عمليات ويجب في هذه الحالة الأخيرة أن تكون حالة تحويل "مستمر" وأن صاحب الحساب الدائن يدفع نفس القيمة دوريا لمدينه[3].

عدم رجعية الأمر بالتحويل منذ القيد في حساب الآمر بالدفع التي كانت القاعدة التقليدية المقبولة لم تعد بعد الآن هي المبدأ، بل يجب العودة للمادة 133-8 من قانون النقد والمال الفرنسي الذي يفرض قاعدة عدم الرجعية منذ إدخال الأمر بالدفع من طرف بنك المستفيد[4]، وهذ الاتجاه الأخير هو الذي تبناه المشرع الجزائري باعتباره التحويل نهائيا منذ دخول المبلغ المحول إلى حساب المستفيد حسب نص المادة 543مكرر20 الفقرة الثانية من القانون التجاري الجزائري.

2-تنفيذ الأمر بالتحويل الإلكتروني: يتم تنفيذ التحويل بقيد المبلغ في الحساب الدائن لعملية المستفيد وليس من شأن المصرف التحقق من سبب اصدار أمر التحويل أو التحقق من

---

[1]- محمود محمد أبو فروة، المرجع السابق، ص65.

[2]- أنظر الملحق المرفق بالنظام رقم 05-06.

[3]- Régine Bonhomme, instrument de crédit et paiement, LGDJ lextenso édition, 2013, 10 édition, p 332.

[4]-Stéphane Piedelièvre, Emmanuel Putman, droit bancaire, corpus droit prive dirigé par Nicolas Molfessis, p340.341.

أهلية الآمر لمباشرة العملية، لكن مع ظهور الآلية والمعلوماتية للتحويلات كانت الحاجة للمقاصة بين البنوك[1].

ثالثا/صور التحويل البنكي الإلكتروني

يشكل التحويل الآلية الأكثر بساطة لتحويل الأموال عند اتمامها داخل نفس البنك، وفي حالة تدخل عدة بنوك يتعقد تنفيذ العملية ويتم تجزئتها على عدة مراحل[2].

1-التحويل المصرفي الإلكتروني من طرف بنك واحد: هي أبسط صور التحويل لأن كل من حساب الآمر والمستفيد موجودين بنفس البنك، ولا تعدو العملية مجرد قيد لمبلغ في حساب الآمر في الجانب المدين، وفي حساب المستفيد في الجانب الدائن، و لا مانع من أن يجتمع مركز الآمر والمستفيد في نفس الشخص بشرط وجود حسابين له، ويدخل ضمن هذه الصورة حالة كون الحسابين موجودين لدى فرعين للبنك نفسه أو أحد الحسابين موجود في المركز الرئيسي للبنك والآخر مفتوحا لدى فرع من الفروع ففي هذه الحالة يتم التحويل المصرفي الإلكتروني بتدخل بنك واحد[3]، وهي عملية داخلية بالنسبة للبنك.

2-التحويل المصرفي الإلكتروني عن طريق بنكين: تتم معظم حالات التحويل من خلال بنكين مختلفين يحتفظ كل من الآمر والمستفيد بحساب لدى هذين البنكين بحيث يقوم الآمر بإصدار أمر إلى بنكه ليقوم بتحويل مبلغ معين إلى حساب المستفيد في بنك آخر ويطب

---

[1] -Régine Bonhomme ,instrument de crédit et paiement ,LGDJ lextenso édition , 2013, 10 édition, p 332.

[2]-Régine Bonhomme, instrument de crédit et paiement, LGDJ lextenso édition, 2013, 10 édition, p329.

[3]-حوالف عبد الصمد، المرجع السابق، ص85.

البنك توقيع الآمر بالتحويل على هذه التعليمات المتضمنة لأمر التحويل بوسيلة إلكترونية، ويشترط التأكد من قبل البنك أن هذه التعليمات الصادرة بالوسيلة الإلكترونية صادرة من الزبون أم لا[1]، ويجب أن يمتلك كل بنك لدى الآخر حساب للتسوية لأن البنوك لا تنفذ العملية الواحدة وتجري المقاصة بل تنفذ عدة عمليات لعدة زبائن وفي النهاية تتم المقاصة في حسابات التسوية.

3-التحويل المصرفي الإلكتروني بين ثلاث بنوك: تتم هذه العملية بين ثلاث بنوك عند غياب حساب التسوية بين بنك الآمر وبنك المستفيد أو أن البنكين لا يشتركان في غرفة المقاصة لتسوية حساباتهما ومنه يتم اللجوء إلى البنك الوسيط لتنفيذ عملية التحويل.

ثالثا/اثار التحويل الإلكتروني

1- إخراج النقود من الذمة المالية للآمر والتسجيل في الجانب المدين في حسابه بمجرد تنفيذ أمر التحويل حيث تنص المادة 543 مكرر 20 من القانون التجاري الجزائري " يكون الأمر بالتحويل غير قابل للرجوع فيه ابتداء من **تاريخ الاقتطاع من حساب الآمر بالتحويل** ..." في حين يرى البعض أن أمر التحويل بحد ذاته لا يؤدي إلى إخراج النقود من الذمة المالية للآمر وبالتالي فإن الوقت الذي يتم فيه التسجيل في حساب المدين هو الوقت المعتد به للقول بتخلي الآمر عن النقود موضوع النقل بشكل حاسم[2]، ولكن المشرع الجزائري فصل في الوقت واعتبر التاريخ هو **تاريخ الاقتطاع من حساب الآمر بالتحويل** حسب نص المادة

[1]-سليمان ضيف الله الزين، المرجع السابق، ص 78.

[2]- محمود محمد أبو فروة، المرجع السابق، ص 58.

543 مكرر 20 من القانون التجاري الجزائري وبالتالي هل يمكن أن يتم التراجع عن أمر التحويل حتى ولو أرسلت الرسالة طالما أن البنك لم يقم بالعملية المطلوبة من كل ذلك يستنتج أنه يمكن دائما الرجوع عن أمر التحويل طالما لم يتم التقييد في الحساب[1] في حين نجد أن المشرع الجزائري في المادة 543 مكرر 21من القانون التجاري أكد على أن" تنتقل ملكية الأموال أو القيم أو السندات موضوع أمر الاقتطاع بقوة القانون بمجرد الخصم من الحساب لفائدة الدائن المرسل للإشعار بالاقتطاع "أما في القانون الفرنسي وتجنبا لهذه الاشكالات تنص المادة L 133-8-1 من قانون النقد والمال الفرنسي على عدم رجعية أوامر التحويل و حسب الأمر المتعلق بخدمات الدفع يمنع على الآمر بالدفع الغاء الأمر الذي أصدره من تاريخ استلامه من طرف البنكي أو مؤسسة الدفع[2].

2- المادة 543 مكرر20 من القانون التجاري الجزائري تنص "...يعتبر **الأمر بالتحويل نهائيا ابتداء من تاريخ دخول المبلغ المحول إلى حساب المستفيد** "، وبالتالي فإن مجرد ارسال رسالة المعلومات لا تؤدي بحد ذاتها إلى اخراج النقود من الذمة المالية للآمر بالرغم من دخولها تحت سيطرة البنك[3] لهذا فصل المشرع الجزائري في الموضوع واعتبر الأمر

2- الزبون لا يكون مسؤولا هن أي قيد على حسابه بواسطة تحويل إلكتروني للأموال تم بعد أن قام بإعلان البنك عن احتمال دخول الغير إلى حسابه أو فقدانه لرمزه السري، أنظر محمد محمود أبو فروة، المرجع السابق، ص 59.

[2]-Régine Bonhomme, instrument de crédit et paiement, LGDJ lextenso édition, 2013, 10 édition, p 335.

[3]- تنص المدة 5/ج من تعليمات البنك المركزي الاردني لعمليات التحويل الإلكتروني للأموال أن رسالة المعلومات التي تتضمن أمر التحويل تعتبر قد أرسلت من وقت دخولها إلى نظام معالجة معلومات لا يدخل في سيطرة المنشئ أو الشخص المرسل للرسالة نيابة عنه، أنظر محمد محمود أبو فروة، المرجع السابق، ص 58.

بالتحويل نهائيا من تاريخ دخول المبلغ المحول إلى حساب المستفيد وهذا برأينا يغطي حالة الاعطاب التقنية الخارجة عن سيطرة البنوك.

الفرع الثاني

الإشعار بالاقتطاع

الاقتطاع Le prélèvement " أو "تصريح بالاقتطاع"[1] و يسمى عمليا "الإشعار بالاقتطاع" وهو المصطلح المستعمل من المشرع الجزائري، وسن الاقتطاع في سنة 1956 لتطوير نظام الصندوق[2] إلا أن المشرع الجزائري لم ينص عليه إلا سنة 2005 في القانون التجاري حيث أضيف كآلية جديدة لوسائل الدفع الرسمية في النظام البنكي الجزائري، ويبقى استعمال التحويل والاقتطاع كوسيلة دفع ضئيل جدا بالمقارنة مع وسائل الدفع الأخرى ويشمل أساسا التحويلات الخاصة بأجور الادارات، وكبريات المؤسسات، والاقتطاعات الآلية في دفع فواتير (الماء، الكهرباء، الغاز، الهاتف) محدود جدا في الجزائر،

ضبط الأمر بالاقتطاع في القانون التجاري الجزائري بصيغة وجيزة من خلال مادتين فقط .

يساعد الإشعار بالاقتطاع على الاقتطاع المباشر من حساب الزبون، وحماية عملية دفع أقساط القروض البنكية التي يستفيد منها الزبائن الذين لهم توطين بنكي آخر domiciliation bancaire[3].

---

[1]-Régine Bonhomme, instrument de crédit et paiement, LGDJ lextenso édition, 2013, 10 édition, p 341.

[2]-Stéphane Piedelièver, Doit bancaire, op, cit, P284.

[3]- بحيح عبد القادر، المرجع السابق، ص 32.

أولا/تعريف الإشعار بالاقتطاع

الإشعار بالاقتطاع متفرع أو مشتق من التحويل وتطور دون سند تشريعي خاص[1] ومن حيث المصطلح في العادة نتكلم عن حوالة ولكن بالخلاف نتكلم عن مصطلح إشعار في الاشعار بالاقتطاع لأنه عبارة عن إشعار بالتوطين فالزبون يوطن الدفع عند الغير والذي هو البنكي[2] ويشكل الاقتطاع احدى صور التحويل البنكي إلا أنه يتميز عنه بتضمنه ترخيصا دائما من المدين بالأداء لفائدة المستفيد وذلك بالاقتطاع المباشر من الحساب الجاري للمدين بصفة متكررة ويستخدم عادة من الدائنين سواء كانوا مؤسسات أو أفراد يتقاضون دوريا مبالغ مستحقة من المدينين[3]، ويعمل به في حالة الدائن ومدينيه ويتضمن اتفاقين وبالتحديد حوالتين[4]، ويشبه الأمر بالاقتطاع التحويل حيث يسمح بتحويل أموال الزبائن من حساب إلى حساب آخر فهو تصريح مستمر يعطيه المدين إلى الدائن للاقتطاع من حسابه دائما وفي تواريخ منتظمة ويستلزم وجود هوية المستفيد البنكية أو ما يعرف ب(RIB)[5] **فالاقتطاع يعتبر وسيلة دفع إلكتروني عن بعد لديون لها خاصية التكرار، حيث يمكن من**

---

[1]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition, lexis Nexis, p422.

[2]-Cours-de-Droit des Instruments de paiement et de crédit sur le site mailto : cours-de-droit@outlook.Com.

[3]- محمد مومن، أحكام وسائل الأداء والائتمان في القانون المغربي دراسة لأحكام الكمبيالة والسند لأمر وفتح الاعتماد والخصم والشيك والتحويل البنكي والاشعار بالاقتطاع والبطاقات البنكية، المطبعة والوراقة الوطنية ،المغرب، الطبعة الأولى، 2013، ص 450.

[4]- Stéphane Piedelièver, Doit bancaire , op, cit, P284.

[5]-RIB : Relevé d'Identité Bancaire est un enregistrement informatique alphabétique et numérique permettant d'identifier le donneur d'ordre et bénéficiaire.

الاستخلاص الآلي للديون ويعتبر من الوسائل المفضلة في تسديد الفواتير والاقتطاعات الضريبية التي تتكرر بانتظام.

ثانيا/ البيانات الإلزامية للإشعار بالاقتطاع

تنص المادة 543مكرر21 من القانون التجاري على ستة بيانات إلزامية يجب توفرها لإصدار الإشعار بالاقتطاع وتتمثل في:

1-اسم مرسل الإشعار بالاقتطاع وبياناته المصرفية، وكذا رقمه كمرسل الممنوح له من قبل بنك الجزائر: وتتمثل في اسم ولقب مرسل الاشعار بالاقتطاع الدائن أو المستفيد من الأمر بالاقتطاع، وتشمل البيانات المصرفية رقم الحساب المراد تحويل مبلغ الاقتطاع إليه ورقم المفتاح الخاص به ورقم الاشعار بالاقتطاع الممنوح من قبل بنك الجزائر.

2-الاسم والبيانات المصرفية للمدين الآمر بالاقتطاع: وتتمثل في اسم ولقب المدين الآمر بالاقتطاع، وتشمل البيانات المصرفية رقم الحساب المراد الاقتطاع منه ورقم المفتاح الخاص به.

3-الأمر غير المشروط بتحويل الأموال أو القيم أو السندات محل الأمر بالاقتطاع: وهو الأمر الذي يوجهه المدين الآمر بالاقتطاع للبنك يسمح له من خلاله بالخصم من حسابه طبقا للأمر بالاقتطاع.

4-قيمة المبلغ المحول: ويقصد به المبلغ الاجمالي للأمر بالاقتطاع.

5-فترات الاقتطاع: ويقصد بها تحديد فترات الاقتطاع بيوم محدد من كل شهرا مثلا (تاريخ يتكرر دوريا للاقتطاع)، كما يجب تحديد تاريخ بداية سريان الاقتطاع باليوم والشهر والسنة.

6-توقيع المدين الآمر بالاقتطاع: باعتبارنا أمام وسيلة دفع إلكترونية فتوقيع المدين الآمر بالاقتطاع يكون إلكترونيا.

ثالثا/ مقارنة بين التحويل والإشعار بالاقتطاع

يجتمع كل من التحويل والاقتطاع في عدة نقاط فكلاهما عمليتين تسمح بتحويل النقود من حساب إلى حساب آخر وكل من التحويل والاقتطاع يمكن أن يكون بصفة دورية وآلية[1]، والتحويل والاقتطاع وسيلتين للدفع مختلفتين بالنظر إلى الشخص الذي يهتم بعملية تحويل النقود فالشخص المهتم بعملية التحويل والذي يصدر الأمر بالتحويل هو محول الأموال، أما الشخص المهتم بعملية الاقتطاع أو الذي يصدر الأمر بالاقتطاع فهو قابض الأموال ومنذ سنة 2009 ضبط المصطلح في فرنسا بالاقتطاع و تحديدا بالأمر الصادر عن المستفيد[2]، ويراقب عملية التحويل الشخص المستفيد من التحويل في حين يراقب عملية الاقتطاع الشخص المدين ويختلف التحويل عن الاقتطاع في عدة نقاط:

- **من حيث العقد:** التحويل هو أحد العمليات الواردة على الحساب أما أمر الاقتطاع فيشترط وجود عقد بين المصرف والزبون المدين وعقد بين المصرف والزبون الدائن.

---

[1]- متوفرة على الموقع Service-Public .Fr Le site officiel de l'administration Française تاريخ الاطلاع 04 جانفي 2016.

[2]-Régine Bonhomme ,instrument de crédit et paiement ,LGDJ lextenso édition , 2013, 10 édition, p 341.

- **من حيث الترخيص بالعملية:** الأمر بالاقتطاع يكون عادة لتسوية العمليات التي يتوفر فيها عنصر التكرار، بينما يتطلب الأمر بالتحويل باعتباره عملية انفرادية ترخيص دائم من المدين بالأداء لفائدة المستفيد.

- **من حيث الأشخاص:** في الأمر بالتحويل يمكن أن يكون الآمر والمستفيد نفس الشخص في حالة تعدد الحسابات لنفس الشخص، في حين أن الاقتطاع يكون غالبا لشخص آخر

- **من حيث المقاصة:** أمر الاقتطاع في الغالب أمر تحويل داخلي ولكن أمر التحويل يمكن أن يكون بمقاصة إلى الخارج.

رابعا/ إجراءات الإشعار بالاقتطاع

1-إصدار الأمر بالاقتطاع: لا يشترط أن يكون كتابة[1] من طرف المدين يسمح لدائنه بالاقتطاع من حسابه البنكي، حيث يطلب الزبون من البنك بأن يقوم بتحويل متكرر ومستمر لمبلغ معين من النقود المودعة لديه من حسابه إلى حساب آخر وذلك بصفة مباشرة لا تستدعي تدخل الزبون في كل مرة[2]، في حالة الإشعار بالاقتطاع الأمر يعطى مرة واحدة لكل العمليات من طرف المدين ودائم إلى غاية الغائه، والقواعد توضع من طرف البنك عن طريق تعليمات الدائن الذي يبين للبنكي قيمة وتاريخ الدفع[3].

[1]-Stéphane Piedelièver, Doit bancaire, op, cit ,P284.

[2]- محمد مومن، المرجع السابق، ص 450 .

[3]-Christian Gavalda, Jean Stoufflet,instruments de paiement et crédit , effet de commerce cheque, carte de paiement, transfert de fonds, 6edition , lexis Nexis, p422.

2-تنفيذ الأمر بالاقتطاع: حسب القانون التجاري الجزائري تنتقل ملكية الأموال أو القيم أو السندات موضوع أمر الاقتطاع بقوة القانون بمجرد الخصم من الحساب لفائدة الدائن المرسل للإشعار بالاقتطاع، وبالتالي من يوم الخصم من حساب الآمر بالاقتطاع لفائدة المرسل للإشعار بالاقتطاع يترتب عدم رجعية الأمر بالاقتطاع، وفي القانون الفرنسي عدم رجعية الأمر بالدفع في الاقتطاع تكون في نهاية يوم العمل المخصص لقيد الأموال " fin de jour "، حسب المادة L133-8 من قانون النقد والمال الفرنسي التي فرضت على مقدمي خدمة الدفع أنه يمكنهم ايجاد ساعة محددة أو موعد محدد أين تكون كل أوامر الدفع est[1] réputé reçu le jour ouvrable suivant.

القابلية للإلغاء للإشعار بالاقتطاع تعتبر رفض أو امتناع عن الدفع والإلغاء ممكن ويصبح ضروري في حالة قفل الحساب[2]، والمصرفي الذي يتجاوز معارضة الزبون الذي يكون بغياب الاشعار بالاقتطاع الصادر عن الزبون عليه إرجاع إلى هذا الأخير القيمة المقتطعة بصفة غير شرعية من الحساب[3].

[1] - Stéphane Piedelièver, Emmanuel Putman, droit bancaire, corpus droit prive dirigé par Nicolas Molfessis, p341.
[2]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit ,effet de commerce cheque, carte de paiement, transfert de fonds, 6edition ,lexis Nexis,p422.
[3]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition ,lexis Nexis,p422.

الفرع الثالث

بطاقات الدفع الإلكترونية

المصارف العربية لم يعد يقتصر دورها على قبول البطاقات المصرفية العالمية[1] بل أقدمت على اصدار بطاقات خاصة بها، والتي كلما تطورت تطور معها الإجرام مما اضطر المشرعين إلى اصدار قوانين لحمايتها، إلا أننا نلاحظ الفجوة القانونية بين الواقع وما ينجر عن استخدامها في الجزائر.

بطاقات الدفع الإلكترونية Cartes de paiement électronique هي وسائل مستحدثة دفعت إليها الحاجة لذلك تعاني بطاقات الدفع نقصا تشريعيا سواء على الصعيد الداخلي أو على الصعيد الدولي وإن تعرضت لها بعض التشريعات إلا أن أمر وضع تنظيم قانوني لهذه البطاقات لازال لم يكتمل[2].

وبتزايد بطاقات الدفع الإلكتروني تطور الاحتيال مع تطور التجارة الإلكترونية لهذا الغرض سن المشرع الفرنسي في 15نوفمبر 2001 قانون متعلق بأمن البطاقات البنكية المعدل لقانون النقد والمال وأنشأ مخالفات جديدة، وسمح لحامل البطاقة بالتعويض والمعارضة في

[1]- تعد بطاقات الدفع إحدى الخدمات المصرفية التي استحدثها القطاع المصرفي في الولايات المتحدة الأمريكية أنظر براق عبد الله مطر، النظام القانوني لبطاقات الدفع الإلكتروني، مجلة جامعة الانبار للعلوم القانونية والسياسية، العدد السابع، ص312.

[2] -Stéphane Piedelièver, Doit bancaire, op, cit, p265.

حالة الاستعمال الاحتيالي للبطاقة، ونلاحظ تطور لقانون بطاقات الدفع مقارنة مع قانون الشيك[1]، وهذا طبعا في القانون الفرنسي.

رغم التطورات التي عرفتها وسائل الدفع الإلكترونية عالميا وعربيا حيث أصبحت تستخدم في مختلف المجالات إلا أن الجزائر بقيت في منأى عن هذه المستجدات، وحرصا منها على مواكبة التطورات التكنولوجيا في العمل المصرفي شرعت في تبني البطاقات المصرفية، ومن بين الأهداف التي من أجلها أدخل نظام الدفع الإجمالي الفوري للمبالغ الكبيرة والمدفوعات المستعجلة هو تسوية عمليات البطاقات البنكية في وقت حقيقي ويمكن القول أن الدفع الإلكتروني في الجزائر يسير بخطوات منتظمة ومتباطئة من أجل تحقيقه بشكل تام وهذا العمل كان أثناء قيامها بالإصلاح المصرفي من أجل فتح المجال لتطوير التجارة الإلكترونية، وذلك بإصدار أول بطاقة هي " سي- بي – أي – فيزا – غولد". **"CBA VISA Gold Card"**[2] وهي بطاقة دفع إلكترونية عالمية تمكن صاحبها من شراء السلع عبر الإنترنت في أي مكان في العالم وتحويل الأموال إلى البائع عن طريق إرسال المعلومات البنكية عبر البريد الإلكتروني بشكل مشفر لضمان عدم قراءتها في حالة اعتراضها إلا أن ما يعيق هذه العملية في الجزائر هو بط إجراءات تحويل الأموال من بنك داخل البلاد إلى بنك آخر خارجه فهذا يتطلب وقتا أطول قد يتجاوز الشهرين.

---

[1]- Stéphane Piedelièver, Doit bancaire, op, cit , P267.268.

[2]- حوالف عبد الصمد، المرجع السابق، ص131.

تشجيع استعمال بطاقات الدفع الإلكتروني ألزم قانون المالية لسنة 2017 من خلال نص المادة 111 كل متعامل اقتصادي أن يضع في متناول الزبائن وسائل دفع إلكتروني تسمح لهم باستعمال بطاقات الدفع الإلكتروني[1] بناء على طلبهم تحت طائلة الغرامة عند المخالفة لأحكام هذه المادة.

تعددت البطاقات بتعدد الأغراض التي تسعى تلك المؤسسات والهيات تقديمها لزبائنها وفي مختلف المجالات وكذلك الاستفادة من الامكانات التي يقدمها الحاسب الآلي ولذلك تعددت أنواعها بتعدد أغراضها، فمنها ما يمكن أن يستخدمه في التعامل مع أجهزة التوزيع الآلي للنقود، ومنها ما يمكن أن يستخدمه في الوفاء، أو لضمان الشيكات، أو لدفع مشترياته على دفعات[2].

أولا/ تعريف بطاقة الدفع: هناك العديد من المصطلحات[3] التي تطلق على هذه البطاقات ولعل أكثرها شيوعا بطاقات الائتمان لأن هذه التسمية تعبر عن حقيقتها على أساس لفظ

---

[1]-المادة 111 من القانون رقم 17-11 المؤرخ في 8ربيع الثاني عام 1439 الموافق ل27 ديسمبر سنة 2017 المتضمن قانون المالية لسنة 2018 " يتعين على كل متعامل اقتصادي، بمفهوم القانون رقم 04-02 المؤرخ في 23 يونيو سنة 2004 الذي يحدد القواعد المطبقة على الممارسات التجارية المعدل والمتمم، يقدم سلع/أو خدمات للمستهلكين، أن يضع في متناولهم وسائل دفع إلكتروني بناء على طلبهم.

كل إخلال بهذا الالتزام يشكل مخالفة لأحكام هذه المادة ويعاقب عليها بغرامة قدرها خمسون ألف دينار (50.000 دج)..." ،ج ر عدد76، 2017.

[2]- محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الوفاء في مواجهة تصرفات حاملها، مجلة الشريعة والقانون، العدد الرابع والعشرون، رجب 1426هـ الموافق لسبتمبر 2005 ميلادي، ص387.

[3]- يطلق على بطاقات الدفع في الكتابات العلمية والاستعمال المصرفي مسميات عدة منها: بطاقة الائتمان، بطاقة الاعتماد، البطاقة البنكية، بطاقة الوفاء، بطاقة الاقراض، النقود الإلكترونية، والنقود البلاستيكية، أنظر براق عبد الله مطر، المرجع السابق، ص313،314.

crédit والذي يعني الائتمان والقرض وكل هذه التعابير تجمع عاملين رئيسيين هما الوقت والثقة[1]، تسميتها ببطاقة الدفع أو الوفاء يعبر عن وظيفة واحدة من وظائف البطاقة كما لا يدل على ما تحمله من معاني الثقة في حاملها و الائتمان الذي تقوم عليه، فضلا على أنه يمكن استخدامها في سحب النقود وهذه العملية ليس فيها دفع ولا وفاء بدين[2]، إلا أن هناك من يرى أن بطاقة الدفع(carte de paiement) ليست بطاقة ائتمانية وإنما تحمل تعهدا من البنك مصدر البطاقة بتسوية الدين بين حامل البطاقة والتاجر إن كان هناك رصيد دائن لحامل البطاقة ولا تنطوي على أي تعهد من البنك بتقديم تسهيلات ائتمانية[3]، وعلى أساس ما تقدم فإن المفاضلة بين المصطلحات تجعلنا نميل إلى تسميتها **ببطاقات الدفع** كونها التسمية الأكثر انسجاما مع طبيعتها ودورها وسواء تم الدفع بشكل فوري أو على دفعات فإنه لا يغير طبيعة البطاقة كونها أداة دفع، لذلك فبطاقة الائتمان ماهي إلا بطاقة دفع مقيدة بخط اعتماد متجدد، كما أن بطاقات الوفاء تخفي جانبا من جوانب الائتمان، وبطاقة الأداء (الدفع) المصطلح المستعمل والمقابل لها باللغة الفرنسية في القانون التجاري الجزائري (carte de paiement)، ومجرد اختلاف مسميات البطاقات رغم تماثلها الشديد من الناحية الشكلية – المادية أو المعلوماتية – لا يؤثر اطلاقا في كون المعروض في دراسة المسؤولية الجنائية

---

[1]– محمد محبوبي، أساسيات في أدوات الدفع والائتمان، الطبعة الأولى، دار ابي رقراق للطباعة والنشر، المغرب، 2012، ص 160.

[2]– حوالف عبد الصمد، المرجع السابق، ص 95.

[3]– محمد محبوبي، المرجع السابق، ص173.

عن الاستخدام غير المشروع لهذه البطاقات ينطبق عليها جميعا[1]، بغض النظر عن التسمية أو الوظيفة وإنما حاولنا فقط إزالة اللبس في هذه النقطة ولن نغوص في تعريفها لأننا لن نصل إلى تعريف شامل لها نظرا لحداثتها واختلافها باختلاف الوظيفة التي تقوم بها عرفها الفقه في أنها البطاقة التي ينحصر دورها في كونها أداة للوفاء يسمح بمقتضاها لحامها باتخاذ الإجراءات اللازمة لخصم وتحويل مبلغ محدد من المال من حسابه لدى البنك الذي أصدر البطاقة لمصلحة وحساب شخص آخر[2]، وتمكن الشخص من تحويل أمواله المودعة « de transférer des fonds » لدى البنك إلى دائنيه[3]، بطاقات الدفع هي كل بطاقة تسمح لصاحبها بسحب أو تحويل الأموال أما بطاقات السحب فهي لا تسمح لصاحبها إلا بالسحب للأموال[4]، وتنقسم هذه الطائفة من بطاقات الوفاء الإلكتروني بدورها إلى مجموعتين، الأولى لا تتمتع بخاصية الائتمان إذ لا تمنح الجهة المصدرة لها مستخدمها أي تسهيل ائتماني، ولهذايسمى هذا النوع من بطاقات الوفاء الإلكتروني، بالبطاقات المدينة، أما المجموعة الثانية فإن أساس الوفاء فيها هو ما يمنحه مصدره للمستخدم من ائتمان، ولهذا يسمى هذا النوع ببطاقات الائتمان[5]، والبطاقات البنكية عموما تعاني نقصا تشريعيا واضحا سواء على الصعيد الداخلي أو الصعيد الدولي.

---

[1]– محمد نور الدين سيد عبد المجيد، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقة الائتمان، دراسة في القانون المصري والاماراتي والفرنسي، دار النهضة العربية، القاهرة، دون طبعة، 2012، ص15.

[2]– محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الوفاء في مواجهة تصرفات حاملها، المرجع السابق، ص 392.

[3]–أحمد شكري السباعي، المرجع السابق، ص399.

[4] -Stéphane Piedelièver, Doit bancaire, op, cit, P267.

[5]– حسن عبد الله عبد الرضا الكلابي، المرجع السابق، ص 189.

ثانيا/تعريف بطاقة الدفع في التشريع الجزائري

ورد في الملحق المرفق بالنظام 06 / 05 الصادر عن بنك الجزائر المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى تعريف البطاقة المصرفية عموما وليس بطاقة الدفع فقط بأنها: **وسيلة دفع غير مادية تحددها تعليمة تصدر عن بنك الجزائر.**

وبالتالي فالمشرع الجزائري اعتبرها وسيلة دفع غير مادية بشرط أن يكون اصدارها مضبوطا وفق تعليمة تصدر عن بنك الجزائر، وأكدت التعليمة رقم 04/05 المتعلقة بتقييس البطاقات البنكية[1] أن البطاقات المزودة بالشريحة تستجيب للمقاييس العالمية وتسمح بالتحويل والدفع عبر نهائيات الدفع الإلكترونية، وتسمح بالسحب من أجهزة الموزعات الآلية والشبابيك الأوتوماتيكية.

المشرع الجزائري عرف بطاقة الدفع في المادة 543مكرر23 من القانون التجاري الجزائري "تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال..." ونلاحظ أن المشرع الجزائري عرفها بناء على الوظيفة[2] التي تقوم بها وهي السحب والتحويل للأموال كما أنه لم يحصرها في البطاقة

---

[1] -instruction n° 05/04 du 02 aout 2004, portant normalisation de la carte bancaire.

[2]– ويمكن تصنيف البطاقات إلى عدة أنواع بحسب الزاوية التي ينظر منها إليها فمن حيث المزايا تنقسم الى بطاقات عادية أو فضية أو ذهبية، ومن حيث تكوينها توجد البطاقات الممغنطة والبطاقات الذكية، وتنقسم بحسب إمكانية استعمالها إلى بطاقات محلية وأخرى إقليمية أو عالمية وبحسب كيفية التعامل بها إلى بطاقات الوفاء المباشر أو بطاقات الدفع المؤجل وبطاقات الائتمان .

البنكية فقط كما يطلق عليها ذلك البعض وإنما سمح بإصدارها من طرف البنوك والهيئات المالية المؤهلة قانونا فقط.

ثالثا/أساسيات في بطاقة الدفع

1- مكونات البطاقة: تتكون من كيان مادي وكيان معنوي:

أ-**الكيان المادي:** هو الجسم المادي للبطاقة

ب - بيانات البطاقة: مكونات أساسية يجب توفرها في كل أنواع البطاقات منها رقم البطاقة ، اسم حامل البطاقة، تاريخ الاصدار، تاريخ الصلاحية، اسم البنك المصدر، شعار الهيئة الدولية، حد السحب، الشريط الممغنط، الصورة المجسمة الثلاثية الأبعاد (الهولوجرام)، رقم التمييز الشخصي، شريط التوقيع.

رابعا/أطراف البطاقة

1-**المركز العالمي للبطاقة:** أو الهيئة الدولية وهي مؤسسة عالمية تتولى إنشاء البطاقة ورعايتها مفتوحة للبنوك والمؤسسات المالية للاشتراك وتعمل على تسوية النزاعات المتعلقة باستعمال البطاقة، وقد أسهمت منظمات (Visa)[1] و(MasterCard) في التطوير والتجديد في مجال بطاقات الدفع والائتمان والخصم مع شبكة سويفت العالمية التي ترعى التحويلات

[1]-منظمة (visa): هي صاحبة الترخيص باستعمال شعار (visa) وهي لا تقوم بإصدار البطاقات وليست مؤسسة مصرفية، بل هي ناد يساعد البنوك الأعضاء على إدارة خدماتهم، وتكون إدارتها من ممثلي البنوك الأعضاء، وترخص للبنوك إصدار البطاقات (visa) حسب الاتفاق المبرم بينها وبينهم.

الدولية بين المصارف وهي تتيح للزبائن فرص الاستفادة من الخدمات المالية عبر حدود العالم[1].

2-**بنك الزبون:** وهو الذي يملك حق إصدار البطاقات للزبون بعد أن يتعاقد مع الهيئة الدولية والاتفاق مع التجار لقبول البطاقة كوسيلة دفع.

3-**حامل البطاقة:** هو الشخص الذي تحصل على البطاقة من البنك المصدر، و يعد الحامل الأصلي والشرعي لها والذي يفتح الحساب في البنك باسمه.

4-**التاجر** : وهو الذي يقبل التعامل بالبطاقة.

خامسا/الطبيعة القانونية الخاصة لبطاقة الدفع الإلكتروني

تقوم البطاقات الائتمانية على اختلاف أنواعها بوظيفة السداد الإلكتروني و لكن لا يعني ذلك أن وظيفتها تقتصر على السداد لدى التجار، (Le Paiement électronique)فحسب، وإنما لها وظائف أخرى تتعلق بكونها وسيلة لسحب النقود أو أداة ضمان للشيكات أو أداة ائتمان ولكن ماهي الطبيعة القانونية لهذه البطاقات؟

أمام قصور النظريات[2] التي حاولت تكييفها على أساس عقدي كونها ذهبت إلى تفسير كل التزام ترتبه هذه البطاقات بعلاقتها المتشابكة على حدة اتجه الفقه الحديث وخاصة الفرنسي

---

[1]- براق عبد الله مطر، المرجع السابق، ص 312.

[2]- اختلف في مسألة السداد في بطاقات الدفع الإلكتروني الذي يقترب من حوالة حق أو وكالة الواقع وإن كان نظام العمل في هذه البطاقات يشبه النظم القانونية التي تحكم حوالة الحق أو تلك التي تحكم الوكالة فإنه لا يدخل ضمن هذه الأنظمة القانونية، لأن لهذه البطاقات طبيعة قانونية خاصة بها.

إلى تحديد الطبيعة القانونية لهذا النظام استنادا إلى كينونته كل لا يتجزأ[1] يقتضي البحث عنها وتكييفها في ضوء النصوص القانونية الحالية والمقترحة، وقد ذهب رأي آ خر إلى أن بطاقات الدفع الإلكتروني تعد نوعًا من النقود، تضاف إلى النقود الورقية والمعدنية المتداولة ولكن هذا الرأي منتقد، فهذه البطاقات لا تصلح أن تكون نقودًا، لأن نظامها يفتقد إلى خاصية التداول التي تتصف بها النقود، لذلك لا تطبق عليها النصوص الجزائية المتعلقة بتقليد النقود وتزييفها[2]، رغم اقتناعنا بأن هذه المحاولات ماهي إلا محاولة لإرجاع هذا النظام لبطاقات الدفع الإلكتروني إلى أحد القوالب القانونية التقليدية لا يتفق مع هذا النظام الحديث المتسم بالتعقيد، والذي يعتمد أساساً على الوسائل التكنولوجية الحديثة والمتشابك العلاقات[3]، مع تسليمنا بصعوبة وضع هذا النظام الجديد في إحدى هذه القوالب القانونية التقليدية، وحتى وإن كانت البطاقة تحل محل النقود في الوفاء إلا أنها كالتحويل ليست بعملة أو أداة نقدية وإنما هي أداة أو عملية يتم بمقتضاها انقاص الحساب البنكي للمودع أو صاحب البطاقة بقدر مبلغ يقيد في حساب المستفيد غير أن هناك من يرى أن بطاقة الدفع هي بطاقة وفاء بطبيعتها شأنها شأن الشيك[4]، إلا أنها تختلف عنه في أنها غير قابلة للتداول كما أن أحكام الوفاء في بطاقات الدفع لها أحكام خاصة ومختلفة بدليل أن بعض التشريعات أفردت حماية

---

[1]- معادي أسعد محمد صوالحة، بطاقات الائتمان النظام القانوني وآليات الحماية الجنائية الأمنية، دار الآفاق المغربية للنشر والتوزيع، المغرب، ص 136.

[2]-عبد الجبار الحنيص، الحماية الجزائية لبطاقة الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 24، العدد الثاني، 2008ص 153.

[3]-حوالف عبد الصمد، المرجع السابق، ص133.

[4]- محمد محبوبي، المرجع السابق، ص 170.

خاصة لبطاقة الائتمان ومن بين هذه التشريعات التشريع الفرنسي الذي لا يجيز الرجوع في أمر الدفع، ونفس المنهج تبناه المشرع الجزائري من خلال نص المادة 543 مكرر24 من القانون التجاري الجزائري " الأمر أو الالتزام بالدفع المعطى بموجب بطاقة الدفع غير قابل للرجوع فيه ولا يمكن الاعتراض على الدفع إلا في حالة ضياع أو سرقة البطاقة المصرح بهما قانونا، أو تسوية قضائية أو افلاس المستفيد "، كما أنها لا تخضع للتنظيم القانوني الخاص بوسائل الدفع التقليدية[1]، مما يعني عدم جواز تطبيق أحكام جريمة إصدار شيك بدون رصيد على بطاقة الوفاء[2]، لما فيه من تعارض مع مبدأ الشرعية المعروف في القانون الجنائي وما يؤكد الاختلاف هو إصدار المشرع الفرنسي سنة 1991 قانون تحت رقم (Relative à la Sécurité des chèques et des cartes de paiement 1382/91 المتعلق بتأمين الشيكات وبطاقات الدفع، ومنه نستنتج أن بطاقة الدفع وسيلة حديثة من وسائل الوفاء لا يمكن لأي قالب من القوالب القانونية التقليدية أن يفسر جميع العلاقات القانونية المتشابكة الناشئة عنها نظراً لارتباطها بالتطور الاقتصادي والتكنولوجي للمعاملات التجارية إذ تتم عملية التسوية من خلال إعطاء صاحب البطاقة أمرا بالدفع عبر وسيلة دفع تستخدم في الوفاء، وإن كان النقص التشريعي في مجال بطاقات الائتمان في المرحلة السابقة له ما يبرره، حيث أن هذه الوسيلة تعتبر في كثير من الدول من الوسائل الحديثة التي تتميز بالتجديد والتطور، فكان يجب الانتظار حتى يستقر النظام القانوني لهذه البطاقات

[1]– محمد محبوبي، المرجع السابق، ص173.

لبيان أحكامها الأساسية التي تقوم عليها، حتى يمكن وضع تشريع محدد لها يرتب التطورات التي قد تلحق عليها في المستقبل، حتى لا يكون هذا التشريع جامداً مما يعوق حركة التطور والسرعة والائتمان التي تتميز بها المعاملات التجارية لذلك وبعد استقرار النظام لهذه البطاقات وبيان أسس الأحكام التي يقوم عليها يجب على المشرع الجزائري وضع تنظيم قانوني للبطاقات، ولباقي وسائل الدفع الإلكتروني يبين أحكامها الأساسية وطرق حمايتها الجنائية والمدنية، مما يساعد على انتشار هذه الوسيلة السهلة كبديل عن حمل النقود وما تحمله من مخاطر، بالأخذ بالحسبان أنها تعتبر وسيلة حديثة للدفع.

المطلب الثاني

وسائل الدفع الإلكتروني وفق قانون النقد والقرض

يأخذ بنك الجزائر على عاتقه تطوير الجهاز البنكي بتحويله لنظام مصرفي إلكتروني باتخاذه عددا من النظم الرئيسية تحت رقابته المباشرة كبنك للتسوية منها نظام المدفوعات صغيرة القيمة عن طريق غرفة المقاصة الإلكترونية، حيث يتم تسوية الحقوق المتبادلة بين البنوك والناتجة عن التحويلات والشيكات حيث يتم خصم الحسابات المدينة من الحسابات الدائنة لكل بنك في مواجهة البنك الآخر فيسحب البنك المدين شيكا إلكترونيا لأمر البنك الدائن بهذا المبلغ لدى البنك المركزي وبالنظر لأهمية المقاصة الإلكترونية طورت البنوك السندات التجارية الإلكترونية ولكننا لن نتطرق للسفتجة الإلكترونية لأنها غير مشمولة طبقا للقواعد العامة في قانون الصرف بأية حماية جزائية وسنركز مباشرة على الشيك الإلكتروني (الفرع

الأول)، وبالنظر للمفهوم الموسع لوسائل الدفع الإلكتروني وفق قانون النقد والقرض الذي استعمل عبارة مهما يكن السند أو الأسلوب التقني المستعمل والتي من الممكن أن تستوعب أي وسيلة دفع إلكتروني جديدة ولا يوجد ما يمنع قانونا من التعامل بالنقود الإلكترونية في الجزائر (الفرع الثاني).

الفرع الأول

الشيك الإلكتروني

رغم الطبيعة المادية التي يمتاز بها الشيك والتي تتعارض للوهلة الأولى مع منطق الانترنت[1]، إلا أنه يبقى من وسائل الدفع التقليدية التي حافظت على مكانتها في البيئة الإلكترونية، وأهم مشكل واجهه الشيك باعتباره وسيلة من وسائل الدفع التقليدية هو مشكل الشيكات بدون رصيد ولضمان الوفاء وما ينتج عن الشيك التقليدي من مشاكل النصب والاحتيال جاء الشيك الإلكتروني كمكافئ أو بديل للشيك التقليدي ووسيلة أكثر أمانا لتفادي قلة الثقة في الشيك خاصة والأوراق التجارية عامة، و بدأت الدول تتسابق في اصدار القوانين الوطنية الخاصة بالاعتراف بوسائل الدفع الإلكترونية ومنها الشيكات الإلكترونية بشكل خاص مما شجع البنوك على الاعتراف بالشيك الإلكتروني في تعاملاتها وتبنيه[2].

أولا / تعريف الشيك الإلكتروني

[1]- ناهد فتحي الحموري، الأوراق التجارية الإلكترونية "دراسة تحليلية " دار الثقافة للنشر والتوزيع، الاردن، الطبعة الأولى، 2009، ص183.

[2]- عائض بن سلطان البقمي، النظام القانوني للشيك الإلكتروني وحجية التعامل به دراسة تحليلية مقارنة، دورية الادارة العامة، دورية علمية متخصصة ومحكمة يصدرها معهد الادارة العامة كل ثلاث أشهر، عمان الأردن، ص 4.

تقوم فكرة الشيكات الإلكترونية على تحويل الشيكات الورقية إلى شيكات رقمية تعتمد أنظمة الشيك الإلكتروني[1] بوجود وسيط يقوم بعملية التحقق والدفع الإلكتروني للشيك وغالبا ما يكون هذا الوسيط أحد البنوك الإلكترونية[2]، حيث تستخدم هذه الشيكات لإتمام عملية السداد الإلكترونية بين طرفين من خلال وسيط ولا يختلف ذلك كثيرا عن نظام معالجة الشيكات الحالي فيما عدا أنه يتم توليد الشيكات الإلكترونية عبر الانترنت وسيقوم الوسيط بالخصم من حساب الزبون ويضاف إلى حساب التاجر[3]، فالشيك الإلكتروني هو محرر ثلاثي الأطراف معالج إلكترونيا بشكل كلي أو جزئي يتضمن أمر من شخص يسمى الساحب إلى البنك المسحوب عليه بأن يدفع مبلغا من النقود لإذن شخص ثالث يسمى المستفيد[4].

---

[1]- توجد الكثير من الأنظمة للشيك الإلكتروني التي تستخدم للوفاء بالديون الناشئة عن المعاملات التجارية عبر شبكة الانترنت أهمها نظامي FSTC و Net chaix.

نظام FSTC:لاخلاف بينه وبين الشيك العادي ويستبدل فيه التوقيع العادي بالتوقيع الإلكتروني وبدلا من دفتر الشيكات يسلم للزبون دفتر شيكات إلكتروني ويتميز بتأمين الوفاء بالرجوع إلى آلية التشفير والانتقال بالشيك إلى دعامة غير مادية دون المساس ببياناته (نفس بيانات المادة 370 من القانون التجاري).

نظام Net chaix :هذا النظام يستلزم تدخل طرف ثالث وسيط الذي يسجل لديه كل من مستخدم النظام والتاجر يسمح للزبون بالتعامل على شيكاته من سحب وتظهير وتوقيع الضامنين الاحتياطيين انطلاقا من حسابه الشخصي .

[2]- محمد سعيد أحمد اسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى،2009، ص 323.

[3]- محمد عبد السلام سلامة، جرائم غسل الأموال إلكترونيا في ظل النظام العالمي الجديد للتجارة الحرة (العولمة)، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الرابع، ص1526.

[4]- مصطفى كمال طه، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، مصر دون طبعة، 2005، ص351.

1-تعريف الشيك الإلكتروني بالنظر إلى وظيفته: الشيك أهم السندات التجارية التي يمكن الاستفادة منها في مجال المعالجة الآلية للمعطيات لأن البنوك تعد طرفا أساسيا في الوفاء بها وتحصيلها، فالشيك الإلكتروني التزام قانوني بسداد مبلغ معين في تاريخ محدد لصالح فرد أو جهة معينة، ويحتوي على نفس المعلومات التي يحتويها الشيك التقليدي إلا أنه يكتب بواسطة أداة إلكترونية[1] وتكون جميع التوقيعات التي يتضمنها الشيك توقيعات إلكترونية ومن ثم فإنه يتمتع بنفس قوة الشيك الورقي في الدول التي تعتبر التوقيع الإلكتروني بمثابة التوقيع اليدوي وتعطيه حجية في الإثبات[2]، وكل هذه التعريفات التي وضعت للشيك الإلكتروني تنطلق من منظور وظيفة الشيك التقليدية وفي الواقع لا تعكس الصورة الحقيقية للشيك الإلكتروني ووظيفته الأساسية[3]، الذي يرى بأن الشيك الإلكتروني يعرف بالاعتماد على أن بيانات الشيك هي نفسها بيانات الشيك التقليدي لم يبين الطبيعة الإلكترونية للشيك كما لم يبين آلية عمل الشيك.

2-تعريف الشيك الإلكتروني بالنظر لآلية عمله: فالشيك الإلكتروني يعرف بأنه عبارة عن رسالة إلكترونية موثقة ومؤمنة ترسل من مصدر الشيك لمستلمه (حامله) يعتمده ويقدمه للبنك (الذي يعمل عبر الانترنت)حيث يقوم البنك بتحويل قيمة الشيك المالية لحساب حامل

---

[1]- نبيل صلاح محمود العربي، الشيك الإلكتروني والنقود الرقمية دراسة مقارنة، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الأول، ص 67.

[2]- محمد محمود أبو فروة، المرجع السابق، ص 50.

[3]- عائض بن سلطان البقمي، المرجع السابق، ص08.

الشيك وبعد ذلك يقوم بإلغاء الشيك واعادته إلكترونيا لمستلم الشيك (حامله) فيكون دليلا على أنه قد تم بالفعل تحويل المبلغ[1]، ويمكن لمستلم الشيك إلكترونيا مراقبة تحويل المبلغ لحسابه عن طريق مراقبة حسابه على الخط مباشرة ، فالشيك الإلكتروني يسمح بالقيام بالدفع بين طرفين مرورا بوسيط وطريقة الدفع هذه تختلف عن طريقة استعمال الشيك الكلاسيكي نظرا لما تحمله الشيكات المعالجة إلكترونيا والمتداولة عبر قنوات الاتصال من خصوصية فيقوم الوسيط بخصم مبلغ الشيك من رصيد المستعمل إلى رصيد الشركة[2] ورغم أن هذا التعريف جاء لبيان فكرة عمل الشيك والآلية التي يتم بها صرف قيمة الشيك الإلكتروني إلا أنه الأقرب في تعريفه للشيك الإلكتروني والأكثر موضوعية وواقعية[3].

3-الشيك الإلكتروني في القانون الجزائري: ورد في الملحق المرفق بالنظام 06/05 الصادر عن بنك الجزائر المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى تعريف لبعض المصطلحات منها تعريف الصكوك: بأنها وسائل الدفع المحددة مواصفتها في القانون التجاري وتحدد البطاقة المعلوماتية في وجيز تقييس وسائل الدفع الذي أحدثته لجنة التقييس، وقد تبنت البنوك الكبرى فكرة بناء مواصفات قياسية للشيكات الإلكترونية[4].

---

[1]- ناهد فتحي الحموري، المرجع السابق، ص199.

[2]-خنفوسي عبد العزيز، المرجع السابق 78.

[3]- عائض بن سلطان البقمي، المرجع السابق، ص09.

[4]- نقلا عن محمد محمود أبو فروة، المرجع السابق، ص 51.

وبالتالي فتعريف السندات التجارية يوجب علينا العودة إلى القانون التجاري سواء بالنسبة للسفتجة أو الشيك والتي يحكمها قواعد قانون الصرف وأصلها اتفاقيات دولية حددت مواصفاتها وتبنت التشريعات هذه الاتفاقيات وأدرجتها في قوانينها التجارية لتحافظ لها على خاصية أداء وظيفة الوفاء عالميا[1]، وهذا ما فعله المشرع الجزائري ففي تعديله للقانون التجاري الجزائري سنة 2005 حيث لم ينص على السندات التجارية الإلكترونية إنما نجد نظام المقاصة الإلكتروني الصادر عن بنك الجزائر هو الذي كرس فكرة مقاصة الصكوك إلكترونيا.

المشرع الجزائري لم يعرف الشيك في القانون الجزائري إنما اكتفى بالنص على بياناته في المادة 472 التي لم تتطرق إلى إمكانية إصداره إلكترونيا، غير أن المشرع الجزائري أقر امكانية تبادل الشيك وتقديمه للوفاء عبر الوسائط الإلكترونية من خلال المادة 502 الفقرة الثانية من القانون التجاري الجزائري "...يمكن أن يتم هذا التقديم أيضا بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول به "، ويمكن أن نستنتج ذلك ضمنيا من خلال قانون النقد والقرض ونظام المقاصة الإلكترونية لبنك الجزائر، كما أن المشرع الجزائري يستعمل كلمة توقيع من خلال المادة 472 من القانون التجاري الجزائري[2]، ولم يحدد نوع التوقيع (إذا كان يدوي أو إلكتروني)، وإذا أخذنا بهذه الحجج فإنه يمكننا الاعتراف بحجية الشيك الإلكتروني في التشريع الجزائري.

---

[1]- الأصل في وجود السفتجة هو تنفيذ عقد الصرف الذي وجد ليكون دوليا أساسا.

[2]- تنص المادة 472 من القانون الجزائري "... توقيع من أصدر الشيك...".

بالعودة إلى النظام المتعلق بالمقاصة الإلكترونية نجد صورتين للشيك الإلكتروني:

الأولى: عبارة عن شيك تقليدي يقدمه الساحب يدويا للمستفيد الذي بدوره يرسله بالبريد العادي إلى المتجر الإلكتروني الذي بموجب اتفاقية مع بنكه يمرر الشيك بصورته الورقية عبر آلية لتصوير بيانات الشيك الورقي ثم ارساله إلكترونيا إلى بنك المستفيد حيث يقوم البنك بالتأكد من صحة بيانات الشيك ووجود مقابل الوفاء لدى بنك الساحب.

الثانية: الشيك المحول (الصورة البديلة) تتطلب اختلاف بنك الساحب عن بنك المستفيد كما يتطلب وجود اتفاقية بين البنكين حيث بمجرد تقديم المستفيد للشيك لبنكه يتم تصويره إلكترونيا من الجهتين وارساله إلكترونيا إلى بنك الساحب الذي يتحقق من بيانات الشيك بصورته الإلكترونية ثم دفع قيمته من حساب الساحب، والغاية من هذه الصورة هو تقليل الاعتماد على غرف المقاصة بين البنوك لعمليات المقايضة التي تتم لقيمة الشيكات[1].

4- الفرق بين الشيك الإلكتروني و الشيك العادي: يخضع الشيك الإلكتروني إلى نفس الاطار القانوني المقرر في الشيكات الورقية، ودفتر الشيكات الإلكتروني دفتر آمن مقارنة بدفتر الشيكات العادي ولا يختلف كلاهما عن الآخر إذ أنهما يحققان الهدف نفسه والوظيفة نفسها[2]، فالشيك الإلكتروني يجب أن يحتوي على نفس البيانات التي يجب أن يحتويها الشيك التقليدي مع الأخذ بعين الاعتبار الطبيعة الإلكترونية التي توجب بعض البيانات الخاصة، لا

[1]- عائض بن سلمان البقمي ،المرجع السابق ،ص09.

[2]- نضال اسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الاصدار الأول، 2005، الأردن، ص125،124.

يختلف الشيك الإلكتروني عن الشيك التقليدي في الأحكام والأوصاف وعموما فإن الشيك الإلكتروني ما هو إلا صورة رقمية للشيك الورقي واجراء لتسهيل الوفاء بقيمة الشيك.

يلاحظ اختلاف بين الشيك الإلكتروني والتقليدي في ايراد بعض البيانات كرقم حساب الدافع، واسم البنك وتاريخ الصلاحية (هذه البيانات يرجع وجوب ورودها في الشيك الإلكتروني لاستخدام الوسائل الإلكترونية في التعامل بالشيكات وهنا نجد فراغا تشريعيا فيما يخص البيانات حيث لابد أن توضح طبيعة البيانات(إلزامية أم اختيارية) بالنسبة للشيك الإلكتروني والتي لا يمكن أن يتم التعامل بالشيكات الإلكترونية دونها.

ثانيا/ البيانات التي يحتويها الشيك الإلكتروني

يحتوي الشيك الإلكتروني على بيانات إلزامية[1] وبينات اختيارية[2] و بيانات خاصة بطبيعته الإلكترونية تشمل رقم الشيك (نفسه الذي يكون على الشيك العادي)، اسم الدافع، رقم حساب الدافع واسم البنك، اسم المستفيد ونلاحظ بالنسبة للشيك التقليدي لا وجود للشيك لحامله في اطار المتعامل بالشيكات الإلكترونية، لأنه من أهم الشروط في الشيك لحامله هو التسليم

---

[1]- حددت المادة 472 من القانون التجاري الجزائري البيانات الإلزامية في الشيك على سبيل الحصر وهي:
- ذكر كلمة شيك.
- أمر غير معلق على شرط لدفع مبلغ معين.
- اسم الشخص الذي يجب عليه الدفع وهو المسحوب عليه.
- بيان المكان الذي يجب فيه الدفع.
- بيان تاريخ الانشاء ومكانه.
-توقيع من أصدر الشيك وهو الساحب.

[2]-يمكن أن يشتمل الشيك على بيانات اختيارية تتمثل في : تعيين المستفيد(المادة 476من القانون التجاري الجزائري)، وتعيين موطن مختار (المادة 478 من القانون التجاري الجزائري)، الضامن الاحتياطي (المواد من 497-499 من القانون التجاري الجزائري)، وشرط الرجوع بلا مصاريف(المادة 515 من القانون التجاري الجزائري).

المادي الذي لا يمكن تخيله في اطار الشيك الإلكتروني[1]، القيمة التي ستدفع، وحدة العملة المستعملة، تاريخ الصلاحية، التوقيع الإلكتروني للدافع.

رابعا/كيفية العمل بالشيك الإلكتروني

-يصدر البنك للزبون دفتر شيكات إلكتروني بأرقام متسلسلة في الإطار المخصص له في موقع البنك أين يكون رصيده لديه ويمكنه استعمال الشيكات وارسالها على الخط مباشرة أو عن طريق نظام خاص بالمتعاملين[2]، غير أن الشيك التقليدي وما سار عليه العرف بأنه يحرر عادة على نماذج مصرفية وللبنوك اضافة ما يتلاءم مع المعالجة الإلكترونية للبيانات، لكن البنوك في الجزائر لازالت لا تقبل صرف الشيكات إلا على النماذج المسلمة من طرفها لزبائنها في انتظار أن يتم القبول والاعتراف بالشيك الالكتروني للتعامل به بين الزبائن والبنوك.

-عمليا يقوم الساحب بتحرير الشيك الإلكتروني بكتابة رسالة إلكترونية موثقة ومؤمنة على دعامة إلكترونية وتوقيعها إلكترونيا ثم ارسالها بالبريد الإلكتروني للمستفيد.

- يقوم المستفيد باستلام الشيك الإلكتروني والتوقيع عليه إلكترونيا بصفته مستفيد وهذا بيان الزامي في الشيك الإلكتروني عكس الشيك التقليدي ويقوم بإرساله إلى البنك.

- يقوم البنك بتحويل قيمة الشيك النقدية إلى حساب الشيك وبعد ذلك يقوم بإلغاء الشيك واعادته إلى المستفيد ليكون دليلا على أنه قد تم صرف الشيك فعلا ويقوم كذلك بإخطار كل

---

[1]- ناهد فتحي الحموري ،المرجع السابق ،ص208.

[2]-محمد خنفوسي، المرجع السابق، ص81.

من الساحب والمستفيد بتمام عملية الدفع والخصم من حساب الساحب والتحويل إلى حساب المستفيد ومن خلال هذه المراحل يتبين أن الوفاء بالشيك الإلكتروني هو تنفيذ للأمر بالدفع الإلكتروني المبعوث للبنك والذي يتم بالخطوات السابقة والمتتالية وتستلزم عملية دفع الشيكات الإلكترونية وضع نظام مركزي لمعالجتها يعرف بغرف المقاصة الإلكترونية والغرض منه تسهيل تسوية ومعالجة العمليات التي تستعمل فيها الأشرطة المغناطيسية التي تمثل دعامة إلكترونية لأوامر الدفع، والشيكات الإلكترونية، والسفاتج الإلكترونية .

- يتأكد البنك كذلك من صحة التوقيعات الإلكترونية والتي غالبا ما تكون مشفرة كما يتأكد من كفاية الرصيد، والتأكد من صحة التوقيع الإلكتروني شرط شكلي يترتب عليه البطلان فكيف يتم التحقق من التوقيع؟ يتم التأكد من صحة التوقيع عن طريق ادخاله في آلة لفك الشيفرات والرموز التي تعد خصيصا لذلك ويتم التأكد من التوقيع الإلكتروني في الشيكات الإلكترونية[1] عن طريق سلطات التصديق الإلكتروني.

- تدخل شخص ثالث لا يعد شرطا لازما لإتمام الدفع الإلكتروني، إلا أنه يجنب الكثير من المخاطر التي يمكن أن يتعرض لها المستفيد في حالة الدفع لو تمت التسوية بشيكات تقليدية لأنه بالنسبة للشيك التقليدي يغيب الارتباط بين عملية تحرير الشيك والتأكد من وجود الرصيد وهذا ما يعرضنا لخطر عوارض الدفع وانعدام الرصيد، على خلاف الحال بالنسبة

[1]- ناهد فتحي الحموري، المرجع السابق، ص206.

للشيكات الإلكترونية غير المادية حيث يتوقف إتمام العملية التي حرر الشيك لتسويتها على التأكد من وجود رصيد كاف لتسويتها من عدمه فإذا وجد الرصيد يتم إبرام العملية[1].

خامسا/ جزاء تخلف مقابل الوفاء

الراجح أن وجود مقابل الوفاء ليس شرطا لصحة الشيك ومن ثم لا يرتب على عدم وجوده بطلان الشيك لأن القاعدة الفقهية تنص على أن "لا بطلان إلا بنص" وبهذه المسألة لا يوجد نص يقرر البطلان، ويترتب على تخلف مقابل الوفاء في الشيك جريمة اصدار شيك بدون رصيد حسب المادة 374 من القانون التجاري، إلا أن الشيك الإلكتروني كان الهدف من وجوده هو تجنب مشكل انعدام الرصيد لأنه من البيانات التي يتم التحقق منها ثم القيام بعملية المقاصة (اقتطاع قيمة الشيك من حساب زبونه إلى حساب المستفيد).

سادسا/ نظام مقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض في الجزائر

بموجب النظام 06/05 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض في الجزائر تم تجسيد نظام ما بين البنوك للمقاصة الإلكترونية للصكوك والسندات والتحويلات والاقتطاعات، ودخل هذا النظام حيز التنفيذ يوم 15ماي 2006 في أول يوم للتبادلات وكانت البداية بمعالجة الصكوك على أن تتطور لتشمل باقي وسائل الدفع[2]، فالصكوك التي كان يتطلب لمقاصتها أشهر بين البنوك وحتى مع بريد الجزائر أصبحت تتم في دقائق من خلال الربط الآلي لجميع البنوك مع بنك الجزائر، وتتم المقاصة الإلكترونية

[1]- سامي عبد الباقي ابو صالح، المرجع السابق، ص26.

[2]-خنفوسي عبد العزيز، المرجع السابق، ص90.

بنسبة كبيرة للشيكات الإلكترونية وأصبحت تتم في وقت قياسي، ويحاول بنك الجزائر تحسين هذا النظام بالربط الشامل للبنوك المتواجدة في الجزائر به لتستفيد من السندات التجارية الإلكترونية.

الفرع الثاني

النقود الإلكترونية

النقود الإلكترونية تحتاج إلى اعتراف قانوني حتى يمكن عدها نقودا في الجزائر بالمعنى القانوني لأنها لاتعد شيئا مختلفا عن النقود الورقية أو المعدنية فهي رموز لقيمة واحدة، وأول ما يتبادر إلى أذهاننا هو غموض فكرة النقود الإلكترونية[1] لأن استعمالها وهي وسيلة دفع غير منظمة، ومبهمة كليا يعتبر مصدر خطر حقيقي لتبييض الأموال وتمويل الارهاب، كما تستعمل من طرف الجماعات الاجرامية للقيام بالتبادلات المتعددة للأموال والخدمات ضمن النظام المعلوماتي دون أن يتم تحويلها إلى نقود قانونية[2].

النقود الإلكترونية وسيلة من وسائل الدفع الإلكتروني الذي يتم عن بعد وتتميز عن التحويل الإلكتروني[3] كما أن تعبير نظم الدفع الإلكترونية أوسع من تعبير النقود الإلكترونية[1].

---

[1]- تستخدم عدة مصطلحات للتعبير عن مفهوم النقود الإلكترونية فقد استعمل البعض مصطلح النقود الرقمية Digital Money، أو العملة الرقمية Digital currency، بينما استخدم البعض الآخر مصطلح النقدية الإلكترونية Electronic cash(e-cash)، أنظر محمد إبراهيم محمود الشافعي، الآثار النقدية والمالية للنقود الإلكترونية، دار النهضة العربية، 2003، ص06.

[2]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit P89

[3]- التحويل المصرفي الإلكتروني: يعني تحويل قيمة نقدية من حساب إلى آخر بوسيلة إلكترونية وهو من ثم لا يتضمن قيمة نقدية معينة في كيان مادي بل هو عبارة عن رقم يتحول من حساب إلى آخر وكل ما في الأمر أن التحويل يتم طلبه بوسيلة إلكترونية دون أن يختلف عن التحويل العادي الذي يتم في المعاملات الورقية، أنظر حسين عبد الله عبد الرضا الكلابي، المرجع السابق،

أولا/ مفهوم النقود الإلكترونية

طورت النقود الإلكترونية ضمن اطار الألعاب التي تمارس على شبكة الانترنت، وتعتبر وسيلة دفع مناسبة لتسوية المدفوعات صغيرة القيمة حيث يعتبر التعامل ببطاقات الدفع غير مناسب نظرا لما يحمله للمستعمل من تكاليف واجراءات اضافية، فالنقود الإلكترونية تلائم المدفوعات صغيرة القيمة وأكثر اقتصادا في التكلفة، وهناك تعريفان للنقود الإلكترونية الأول موسع والثاني ضيق:

1-التعريف الموسع للنقود الإلكترونية: يشمل جميع أشكال التداول غير المادي للنقود[2]، منها: أنها **دفع أو تحويل الودائع المدخلة والمعالجة إلكترونيا ضمن أنظمة البنوك الإلكترونية** غير أن الملاحظ على هذا التعريف أنه يتطرق إلى وسيلة تحويل القيمة إلكترونيا دون أن يتطرق إلى تعريف القيمة النقدية نفسها فيما ذهب رأي آخر إلى أن النقود الإلكترونية **هي بطاقات تحتوي على مخزون إلكتروني أو أرصدة نقدية محملة إلكترونيا على بطاقة تخزين القيمة**، غير أن هذا التعريف هو الآخر لم يعرف النقود الإلكترونية بل عرف الوسيلة التي يتم فيها خزن أو حفظ تلك النقود[3]، فالنقود الإلكترونية بالمعنى الواسع

---

[1]- نظم الدفع يشمل جنبا إلى جنب نظم التحويل للأموال الكبيرة القيمة أما تعبير النقود الإلكترونية فيقتصر أساسا على المدفوعات منخفضة القيمة، أنظر أحمد عبد العليم العجمي، المرجع السابق، ص50.

[2]-أحمد السيد لبيب، الدفع بالنقود الإلكترونية الماهية والتنظيم القانوني (دراسة تحليلية)، دار الجامعة الجديدة، مصر، 2009، ص36.

[3]- نبيل مهدي زوين، النقود الإلكترونية دراسة مقارنة، ص03.

تتضمن عدة وسائل مثل محفظة النقود الإلكترونية، حسابات الدفع عبر الخط، البطاقات المسبقة الدفع[1].

2-التعريف الضيق للنقود الإلكترونية: بهدف الوصول إلى تعريف جامع مانع يكون أبلغ في الدلالة على حقيقة مضمونها مع الاختلاف حول العناصر التي يجب ابرازها في التعريف لتمييز النقود الإلكترونية عن غيرها من النظم التي تتشابه معها أو تختلط معها[2] فركز البعض على عنصر من هذه العناصر أو على الجمع بين بعضها منها التركيز على النواحي الفنية للنقود الإلكترونية، أو تمثل التزام على المصدر أو أنها لا ترتبط بأي حساب مصرفي، أو التركيز على وظائف النقود الإلكترونية، لذلك نكتفي بتعريف البنك المركزي الأوربي وتعريف المشرع الفرنسي.

أ- تعريف البنك المركزي الأوربي: هي مخزون إلكتروني لقيمة نقدية على دعامة تقنية يستخدم بصورة شائعة للقيام بمدفوعات لمتعهدين غير من أصدرها، دون الحاجة إلى وجود حساب بنكي عند إجراء الصفقة وتستخدم كأداة محمولة مدفوعة مقدما، ويعد هذا التعريف الأقرب إلى الصحة نظرا لدقته وشموله لصور النقود الإلكترونية واستبعاده للظواهر الأخرى التي يمكن أن تتشابه معها[3].

---

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit P80.

[2]- أحمد السيد لبيب إبراهيم، المرجع السابق، ص39.

[3]-محمد إبراهيم محمود الشافعي، أنظر محمد إبراهيم محمود الشافعي، الآثار النقدية والمالية للنقود الإلكترونية، دار النهضة العربية، 2003، ص07، 08.

ب-تعريف النقود الإلكترونية وفق قانون النقد والمال الفرنسي: عرفت المادة L 315-1 من قانون النقد و المال النقود الإلكترونية أنها قيم نقدية مخزنة في شكل إلكتروني بما فيها الممغنطة و تمثل دين على المصدر الذي يصدرها مقابل تخفيض الأموال لتنفيذ عملية الدفع المقبولة من طرف الأشخاص الطبيعيين أو المعنويين الآخرين كمصدر النقود الإلكترونية[1]، وهي عبارة عن نقود غير ملموسة وتخزن في مكان يسمى المحفظة الإلكترونية.

ثانيا/ العناصر المحددة لمفهوم النقود الإلكترونية: تتميز النقود الإلكترونية بمجموعة من العناصر والخصائص تتمثل فيما يلي:

1-النقود الإلكترونية تمثل قيمة نقدية: العملة رمز لقيمة محددة يكون القانون هو الفيصل في تحديدها فيمكن أن يكون هذا الرمز على قطعة معدنية، ويمكن أن يكون ورقة نقدية كما يمكن أن تكون مجموعة من البيانات المخزنة إلكترونيا، في الواقع يفتح الشخص لدى المصرف حسابين: واحد بالعملة النقدية والثاني بالعملة الإلكترونية فيقوم بتحويل أمواله من حسابه إلى الثاني وتكون النقود الإلكترونية عبارة عن بيانات جزافية ينتجها أحد البرامج لمرة واحدة بحيث لا يمكن أن تتطابق الأرقام في الاصدارات اللاحقة ويرسلها ذلك الشخص إلى البنك للمصادقة حيث يتم اضافة بيانات أخرى عليها وتعاد للزبون كوحدات دفع إلكترونية

[1]- ART L 315-1 CMF. « La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L133-3. Et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique ».

يحق للزبون استعمالها للدفع لدى التجار بعد تحققه من صحتها عبر توقيع البنك الإلكتروني الموضوع عليها[1].

يطرح التساؤل البسيط **هل بطاقة الهاتف تكون نقود إلكترونية أو وسيلة دفع** مع أنه لا يمكن الدفع بها ولكن يمكن إجراء مكالمات من خلالها فقط وهي ليست منظمة من طرف قانون النقد والمال الفرنسي بل منظمة من قبل قانون الاستهلاك وقوانين أخرى[2]، وبالتالي فبطاقات الهاتف لا تعتبر من قبيل النقود الإلكترونية لأن القيمة المخزنة عليها عبارة عن وحدات اتصال تليفونية وليست قيمة نقدية قادرة على شراء السلع والخدمات[3].

سؤال آخر يطرح **هل يعد كل دفع مسبق نقود إلكترونية؟** فكل دفع مسبق ليس نقود إلكترونية[4] فإذا كان كل نقد إلكتروني هو دفع مسبق إلا أن العكس غير صحيح فالدفع المسبق شرط ضروري لكنه ليس كاف لتصنيف النقود الإلكترونية وحسب عنوان الكتاب الثالث من قانون النقد والمال الفرنسي فإن النقد الإلكتروني هو وسيلة دفع " وسيلة للنقود القيدية" ويؤكد على أن القواعد المطبقة إصدار وتسيير وسائل الدفع الإلكتروني تنطبق على إصدار وتسيير النقود الإلكترونية حسب المادة L133-1-IV[5]، يجب الحصول على رأي بنك فرنسا قبل منح أي اعتماد و هذا راجع لأن النقد الإلكتروني نوع من الدفع الذي يجب أن

---

[1]– نادر عبد العزيز شافي، المرجع السابق، ص84، 85.

[2]- Pierre storrer, droit de la monnaie électronique, édition RB, p48.

[3]–محمد إبراهيم محمود الشافعي، أنظر محمد إبراهيم محمود الشافعي، الآثار النقدية والمالية للنقود الإلكترونية، دار النهضة العربية، 2003، ص08.

[4]- Pierre storrer, droit de la monnaie électronique, édition RB, p47.

[5]- ART L133-1- IV « Sans préjudice de l'application de la section 12, le présent chapitre s'applique à l'émission et la gestion de monnaie électronique ».

يكون مقبول من المستعملين وهذه الخاصية تكون مرتبطة بوجود "دفع مسبق " على دعامة إلكترونية والتي يمكن أن تكون قابلة للتعبئة مقابل تخفيض المال ومنه ليس هناك إنشاء للنقود[1]، لأن من يملك إنشاء النقود في أي دولة هو البنك المركزي ومنه النقود الإلكترونية هي مجرد وحدات لقيمة نقدية أنشأها البنك المركزي، تقوم النقود الإلكترونية بالوظائف التي تقوم بها النقود القانونية[2].

2- مخزنة على وسيلة إلكترونية: حيث يتم شحن القيمة النقدية بطريقة إلكترونية على بطاقة بلاستيكية أو على القرص الصلب للحاسب الآلي الشخصي وهو ما يميزها عن النقود القانونية والائتمانية التي تعد وحدات نقدية مسكوكة أو مطبوعة.

3-غير مرتبطة بحساب بنكي: تتضح أهمية هذا العنصر في تمييز النقود الإلكترونية عن وسائل الدفع الإلكترونية، إلا أن هناك من يرى أن هذه النقود تختلف عن النقود بمعناها القانوني إذ أن وصف النقود لا ينطبق إلا على النقود الصادرة عن الدولة والتي لها قوة ابراء فورية و الدليل على ذلك أنها لا ترتبط بحساب بنكي كالبطاقات أو التحويل المصرفي[3]، وتستعمل دون إدخال حسابات مصرفية في التعامل وتستخدم كسند لحامله مدفوع مقدما[4]، ودور المصدر يتمثل في تأكيد صحة وأصالة وحدات النقد الإلكتروني المستخدمة

---

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique , op, cit , P 80.

[2]- النقود الإلكترونية هي النقود التي أنشأها البنك المركزي.

[3]- سامي عبد الباقي، المرجع السابق، ص 64.

[4]- أحمد السيد لبيب إبراهيم، المرجع السابق، ص43.

في الدفع دون التأكد من شخصية الحامل وهذا ما يميزها عن التحويل المصرفي والبطاقات التي تتطلب تدخل المصرف لإتمام عملية الدفع.

تمتاز بنقص الشفافية لا وجود لشكلية خاصة لفتح محفظة نقود افتراضية أو حساب نقدي افتراضي، مقدمي خدمات الدفع ليس عليهم التزام قانوني وأيضا أكثر التحويلات تقع بالنقود الإلكترونية محفوظة في سجل عام وهي إضافة لذلك غير مسماة[1] وهي تسمح لمستعملي الانترنت الذين لا تتوفر لديهم بطاقات بنكية أو لا يريدون استعمالها وتمثل ميزة غير هينة لمجرمي المعلوماتية.

4-تحضى بقبول واسع من غير من أصدرها: يتعين أن لا يقتصر استعمال النقود الإلكترونية على من قام بإصدارها أو أشخاص معينين أو إقليم معين، أو فترة زمنية معينة، وتجدر الإشارة إلى أن معظم نظم النقد الإلكتروني لم تحظ حتى الآن بالقبول العام الذي تحظى به وسائل الدفع الأخرى، ومع ذلك لا يمكن إغفال حقيقة ما يؤكده الواقع من أن استخدام النقود الإلكترونية آخذ في النمو والتزايد[2].

5-وسيلة للدفع لتحقيق أغراض مختلفة: أي صالحة لشراء السلع والخدمات والقيام بمختلف الالتزامات.

---

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique , op, cit P 90 .

[2]-أحمد السيد لبيب إبراهيم، المرجع السابق، ص63.

رابعا/تنظيم النقود الإلكترونية في التشريع الفرنسي

بالنسبة لنا في الجزائر وحيث أننا سنستبق المشكلة قبل أن تدهمنا وهي لا محالة ستدهمنا وبالتالي ليس أمامنا إلا الرجوع إلى المشرع الفرنسي للوقوف على تنظيمه للنقود الإلكترونية وهذا حتى لا نغوص في الدراسات النظرية التي تناولت الموضوع، وحتى نعالج مختلف الإشكالات القانونية التي يثيرها موضوع النقود الإلكترونية.

1-غياب التنظيم القانوني للنقود الإلكترونية في الجزائر: نشير إلى المادة 117 من قانون المالية لسنة 2018 التي منعت شراء العملة الافتراضية وبيعها واستعمالها وحيازتها وكل مخالفة لأحكام هذه المادة معاقب عليها طبقا للقوانين والتنظيمات المعمول بها، وعرفت نفس المادة العملة الافتراضية بأنها تلك التي يستعملها مستخدمو الإنترنت عبر شبكة الأنترنت، وتتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو البطاقة، مما يوحي باستبعاد البطاقات من أشكال النقود الإلكترونية، وبالتالي المشرع الجزائري إلى غاية يومنا هذا لا يسمح باستعمال النقود الإلكترونية وكما نعلم أن قوانين المالية هي قوانين سنوية تتغير كل سنة فلا يوجد ما يمنع من إمكانية السماح باستعمال النقود الإلكترونية مستقبلا لأنه لا يوجد بقانون النقد والقرض ما يمنع من استعمالها.

2-التوجيه الأوربي حول النقود الإلكترونية: صدر التوجيه EC/46/2000 الخاص بالنقود الإلكترونية وصدر توجيه آخر EC/28/2000 عدل تعريف المؤسسات الائتمانية

الوارد في التوجيه الخاص بدمج البنوك ليدخل ضمنه مصدري النقود الإلكترونية كما أنه يوسع مضمون عمل الفقرة الثالثة من توجيه النقود الإلكترونية الخاصة بمسألة القابلية القانونية للتحويل لتشمل النقود الإلكترونية الصادرة عن البنوك[1] والذي أدمجته الدول الأوربية في قوانينها الداخلية.

3-إنهاء احتكار إصدار النقود الإلكترونية للمصارف في فرنسا: كانت النظرة الغالبة للنقود الإلكترونية ووسائل الدفع الإلكتروني عموما هو تقييد إصدارها فقط من قبل المصارف إلا أن هذه النظرة تغيرت عالميا.

بعد عشر سنوات من التأخير غيرت فرنسا أخيرا التوجيه المتعلق بالنقود الإلكترونية بالتوجيه الثاني في 16 سبتمبر 2009 و المسمى (DME2) بالقانون 28 جانفي 2013[2] الذي أقر إنهاء احتكار البنوك الفرنسية للنقود الإلكترونية و هو نفس الشيء الذي أقره الأمر 2009 المعدل للتوجيه المتعلق بخدمات الدفع لسنة 2007 (DSP)[3] التشريع الفرنسي الخاص بالنقود الالكترونية بمقتضى توجيه 2009/110/CE[4] الخاص بنشاط مؤسسات النقود الإلكترونية.

---

[1]- طارق محمد حمزة، النقود الإلكترونية كإحدى وسائل الدفع تنظيمها القانوني والمسائل الناشئة عن استعمالها، منشورات زين الحقوقية، الطبعة الأولى، 2011، ص 161.

[2]- Loi du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière économique et financière (JO du 29 janvier 2013)

[3]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, pratique de droit, collection dirigée par Nicolas Molfessis, economica, P78.

[4]- Directive 2009 /110/CE, concernant l'accès à l'activité des établissements de de monnaie électronique et son exercice ainsi que la surveillance prudentielle des établissements, du 16 septembre 2009.

4-دور القطاع الخاص في إصدار النقود الإلكترونية: إن اصدار النقود الإلكترونية من قبل غير البنوك أو المؤسسات غير المصرفية من الممكن أن يثير مسائل تتعلق بالتزوير وركزت المفوضية الأوربية على عوامل المنافسة والابتكار واعتبرت أن حصر إصدار وسائل الدفع الإلكترونية الحديثة بالبنوك دون سواها من شأنه أن يبطئ عملية الابتكار وبهدف ايجاد حلول لهذه المسائل أصدرت المفوضية الأوربية توجيها بشأن اصدار النقود الإلكترونية وقد قدم هذا التوجيه مؤسسة جديدة تدعى "مؤسسة النقود الإلكترونية" والتي تتميز بخضوعها لتنظيم أخف[1]، من ذلك الذي تخضع له البنوك كما أن مؤسسات الإصدار في باقي الدول الأعضاء لكن كان موقف البنك المركزي الأوربي مخالفا لذلك بضرورة حصر الإصدار بالبنوك فقط من حيث أنه لا حاجة لإنشاء بنى تحتية جديدة لأن البنوك تتوفر عليها، وبالتالي فضل البنك الأوربي المركزي انتهاج سياسة التمهل حول ضرورة أو عدم ضرورة وجود تنظيم مسبق لإصدار النقود الإلكترونية لأن حجم النقود الإلكترونية لم يكن لها أهمية كبيرة سنة 1998 في النهاية تم الركون إلى نتيجة مفادها أنه اذا ما بدأ العمل بالنقود الإلكترونية على نطاق واسع فسيكون من الصعب على المشرعين أن يقوموا بتغييره.

5-تعريف مؤسسات النقود الإلكترونية في التوجيه الأوربي: اعتبر التوجيه الأوربي مؤسسات النقود الإلكترونية أي متعهد أو أي شخص معنوي آخر غير المؤسسات الائتمانية وهي تصدر وسائل بشكل نقود إلكترونية، لكنها لا تخضع لنفس الشروط التي تخضع لها

[1]-طارق محمد حمزة، المرجع السابق، ص158.

البنوك بل تخضع لضوابط أخف فرأسمالها مثلا أقل من رأسمال البنوك ونشاطها العملي مقيد وهي ملزمة بتقديم تقرير دوري عن حركة النقود الإلكترونية، كما أن النقود الإلكترونية التي تصدرها هذه المؤسسات لا تكون إلا في مقابل أصول مالية ليست أقل من القيمة النقدية المصدرة وأدخلت مسألة القابلية للاسترداد أو التحويل.

سوق النقود الإلكترونية أفرزت بنية تنظيمية معقدة وتكون صعبة المراقبة لأنها تكون خارج البنوك وهذا التعقيد يستعمل لغاية السماح للمستعملين بالتخفي في هذه التحويلات المالية[1] تمثل مشكل كبير للفساد المالي وتكون الرقابة عليها مشكوك فيها وغير كافية لأن المجرمون يحسنون استغلال الثغرات.

خامسا/طبيعة النقود الالكترونية

يتساءل البعض بخصوص إطلاق مصطلح النقود الإلكترونية ويشكك بكونها نقود حيث يقر أن إطلاق مصطلح النقود لا يعني الاعتراف بكونها نقود من الناحية القانونية وهو يشبه إطلاق مصطلح النقود على العملة المزيفة رغم كونها ليست نقودا من الناحية القانونية لأنها ليست صادرة عن البنك المركزي[2]، فالفرق الجوهري بين النقود الإلكترونية وصور النقود التقليدية هو أن النقود لم تعد تأخذ الشكل المادي بل أصبحت تتمثل في مجرد انتقال المعلومات بين أطراف التبادل إذ أن المعلومات عن النقود أصبحت أكثر أهمية من النقود

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit P84

[2]– نبيل مهدي زوين، المرجع السابق، ص07.

ذاتها، ومنه تعتبر النقود الإلكترونية صيغة غير مادية للنقود الورقية إذ أن اصدار النقود الإلكترونية يتم من خلال تحويل شكل النقود من الصيغة الورقية إلى الصيغة الإلكترونية[1]، يعتبر البعض النقود الإلكترونية أداة تبادل[2] وليست أداة دفع حيث يكون الدفع نهائيا فقط إذا حاز المستفيد الأصول النقدية بدون مخاطر ويستدلون على ذلك بالشيك حيث يعتبرونه أداة للتبادل ولا يتم الدفع النهائي إلا بالحصول على المقابل النقدي وبالتالي النقود الإلكترونية تستوجب الرجوع للمصدر حتى يحصل من انتقلت إليه هذه النقود على حقوقه كاملة.

وتمر النقود الإلكترونية بثلاث مراحل أولها الإصدار لصاحب وسيلة الدفع ثم الانتقال من حامل وسيلة الدفع إلى طرف ثالث ثم تدمير النقود الإلكترونية بقيام الطرف الثالث باسترداد مقابلها من النقود التقليدية وبالتالي تعتبر النقود الإلكترونية مجرد صورة افتراضية للدورة الكاملة للنقود التقليدية، وخلافا للآراء السابقة هناك تقرير للبنك المركزي الأوربي يرى أن القيمة المختزنة في النقود الإلكترونية تتشابه مع الودائع البنكية[3]، وبالتالي هي تقوم على فكرة أساسها الدفع المسبق للمستهلكين للمصدر، وبالتالي وكما في الودائع فإن قيمة النقود الإلكترونية يمكن أن تتقلص أو تختفي بحسب السلامة المالية للمصدر.

---

[1]- نادر عبد العزيز شافي، المرجع السابق، ص90.

[2]– أداة تبادل لأنها لا تتوفر على خمسة شروط منها أن تكون مقبولة لدى العموم، أن تعد أداة دفع، أن تتم حوالتها بالتسليم أن تكون مغفلة التسمية، أن تتم الحوالة بدون أي تكلفة تقع على الحائزين السابقين لها، أنظر طارق محمد حمزة، المرجع السابق ، ص128.

[3]– طارق محمد حمزة، المرجع نفسه، ص133.

تشفير النقود ليس معروف من طرف البنوك المركزية الأوربية التي تخلق النقود وتراقبها عن طريق وحداتها المطورة ولا تقبل إلا من طرف أفراد من المجتمع وتستعمل من طرف السوق السوداء للجريمة المعلوماتية وهي حل يسمح بفضل محفظة النقود الافتراضية التي تستعمل في الشراء عبر الخط بدون تقديم معلومات بنكية[1].

البساطة، عدم التسمية، الكثافة، ضعف التأمين كلها مميزات للنقود الإلكترونية تسهل بشكل كبير تبييض الأموال المفضل لدى مجرمي المعلوماتية وهي ليست مراقبة من طرف أي مركز وتمثل تهديدا لاقتصاد الدول.

[1]-Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit, p 90

الفصل الثاني

حالات المسؤولية الجزائية للفاعل الأصلي عن استخدام وسائل الدفع الإلكتروني

نتج عن التحول من المادية إلى اللامادية في الجرائم المرتبطة باستخدام وسائل الدفع الإلكتروني انحصار السلوكات المادية، وتحول موضوع الجريمة من النطاق المادي إلى اللامادي لأن وسائل الدفع الإلكتروني أصبحت هي المسيطرة على التعاملات المصرفية.

الفاعل الأصلي في الجرائم المرتبطة بوسائل الدفع الإلكتروني من أتى منفردا سلوكا يعتبر ركنا ماديا في هذه الجرائم أو المخالفات المرتبطة بالدفع الإلكتروني يمكن أن تكون هي نفسها المرتبطة بالدفع التقليدي ولكنها مرتكبة بطريقة غير تقليدية[1]، والمخالفات[2] المتعلقة بالدفع الإلكتروني مفهوم غامض ومبهم يهدف إلى مواكبة الثورة الدائمة للتكنولوجيا الإجرامية والتي يوم بعد يوم تفرز أنواع جديدة من هذه الجرائم ولا يوجد تعريف قانوني محدد وواضح موضوع لهذه الجرائم المتعلقة بالدفع الإلكتروني[3]، بل تعد من الجرائم المعلوماتية في شكلها الحديث للجرائم المالية والاقتصادية التي ظهرت وتعددت أساليبها بتعدد وسائل الدفع الإلكتروني وتباينت الآراء حول المصطلح المستخدم للدلالة على ظاهرة الاعتداء على الحاسب الآلي والمرتبطة بالمال مرورا بمصطلح جرائم الحاسب الآلي، جرائم التقنية العالية وصولا إلى جرائم السيبركرايم، جرائم الياقات البيضاء انتهاء بالجريمة المعلوماتية وهو مترجم من اللغة الفرنسية informatique والذي يعتمد على المعالجة الآلية للبيانات.

الجريمة المرتبطة بالتطور التكنولوجي في ميدان وسائل الدفع من أخطر الجرائم وهذا بظهور آلية جديدة للتبادل بكافة صوره والتي تعتمد في عملها على أجهزة الحاسب الآلي

[1]-Hatem Adnan Bezzo, op, cit, p183.

[2]- مصطلح المخالفات يستعمل أكثر في قانون الأعمال للدلالة على الجرائم نظرا لطبيعتها الخاصة التي تعني المخالفة لأحكام القوانين المرتبطة بالجانب الاقتصادي فهي غالبا جرائم ذوي الياقات البيضاء.

[3]-Hatem Adnan Bezzo ,op, cit, p188.

الذي يتمتع بقدرة فائقة على تخزين المعطيات وإمكانية الوصول إليها في أسرع وقت وبارتباط الحواسب الآلية مع بعضها في فضاء تكنولوجيا المعلومات أصبحت الجرائم تطال الحق في المعلومة وتهدد الأمن الاقتصادي وبالتالي تتخذ مظهرين **الأول: يمثل الاعتداء على برامج ومعلومات الحاسب الآلي** باعتبار وسائل الدفع الإلكتروني هي إحدى تطبيقاته ولا يمكننا استخدامها إلا من خلال بيئة إلكترونية وباستعمال مدخلات ومخرجات الحاسب الآلي لإتمام التعامل أما **الثاني فيمثل: الاعتداء على وسائل الدفع بحد ذاتها من حيث استعمالها بطريقة غير شرعية** ويمكن تعريف الجرائم المرتبطة بوسائل الدفع الإلكتروني بأنها التصرفات غير القانونية المرتكبة عبر أي وسيلة من وسائل الاتصال الآلية التكنولوجية الموجهة للحصول أو التعديل أو المحو للمعلومات البنكية وتزوير وتزييف التصرفات والأنظمة البنكية للحصول على أرباح ومكاسب بنكية غير قانونية[1]، الجرائم المرتبطة بوسائل الدفع الإلكتروني تهدف الحصول على أرباح غير مشروعة و تشمل الجرائم الماسة ببرامج العمل وتشغيل هذه الوسائل، والجرائم المرتبطة بوسيلة الدفع الإلكتروني بحد ذاتها.

نتناول في المبحث الأول (المسؤولية الجزائية وتأثرها بوسائل الدفع الإلكتروني)، وفي المبحث الثاني نقف على حالات المسؤولية الجزائية للفاعل الأصلي.

[1]-Hatem Adnan Bezzo , op. cit, p183.

المبحث الأول

المسؤولية الجزائية وتأثرها بوسائل الدفع الإلكتروني

الشيء المؤكد أن القانون الجنائي لا يتطور دائما بنفس السرعة التي تتطور بها وسائل الدفع الإلكتروني التي أدخلت لجذب أكبر عدد من الزبائن وتطوير الخدمات المصرفية في ظل التنافس الحاصل بين المصارف، وإذا أصدرنا الحكم مسبقا بهذا الخصوص نعتقد أن نصوص القانون الجنائي لا تكفي من حيث المبدأ لمواجهة هذا الشكل الجديد من الجرائم ورغم التفنن في تطوير نظم الحماية التقنية إلا أن الحماية القانونية تبقى من بين المستلزمات التي علينا تبنيها لتحقيق الأمن المعلوماتي[1]، لذلك نتناول أولا الخصائص المميزة للمسؤولية الجزائية عن استعمال وسائل الدفع الإلكتروني (المطلب الأول)، ومدى انطباق المبادئ العامة على هذه المسؤولية (المطلب الثاني).

المطلب الأول

خصائص المسؤولية الجزائية عن استعمال وسائل الدفع الإلكتروني

أثرت الثورة التكنولوجيا على المسؤولية الجزائية عامة، وكان لوسائل الدفع الإلكتروني أثر خاص على المسؤولية الجزائية لذلك سنوضح في (الفرع الأول) المسؤولية الجزائية عن

[1]-عرف المشرع الجزائري الأمن المعلوماتي أو كما اصطلح عليه بالأمن السيبيراني من خلال المادة 03/10 من القانون 04/18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية بأنه "مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة".

يذهب رأي آخر إلى أن جهاز الحاسب الآلي لا يمكن أن يشكل أي نوع من الخطر على الزبائن فهذا الجهاز لم يضف أي جديد على التعامل المصرفي من حيث الفكرة فالإنسان منذ القدم يعرف فكرة الملفات والمحفوظات وإن كل ما أضافه هذا الجهاز هو تطوير الحياة المصرفية باستخدام الوسيلة الإلكترونية في تجميع المعلومات أو بعبارة أخرى إن الآلة حلت محل الذاكرة لإتمام العمليات المصرفية ومن ثم فإن الأمر لا يستدعي تطبيق قواعد قانونية خاصة[1].

أولا/الجرائم المرتكبة بوسائل الدفع الإلكتروني تتم على نظم المعالجة الآلية للبيانات

تشكل الجريمة الإلكترونية بالنسبة للقطاع المصرفي تحديا جديدا وتستلزم بذل عناية عالية من طرف المشرفين على الرقابة[2] حيث تتم في غالبية الأحيان داخل بيئة المعالجة الآلية للبيانات ونظام المعالجة الآلية أو (système de traitement automatisé de données) تعبير فني يصعب على المشتغل بالقانون ادراك حقيقته بسهولة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية ولذلك أسقط المشرع الفرنسي تحديد مفهوم هذا التعبير[3].

---

[1]– نقلا عن عبد المطلب بدوي، البنوك الإلكترونية ماهيتها معاملاتها والمشاكل التي تثيرها، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الخامس، ص1985، ص 1985.

[2] -Édouard fernandez-bollo, la Cybercriminalité risque Systémique pour le secteur financier, Revue Banque, N 793 février 2016, p22.

[3]– علي عبد القادر القهوجي، بحث بعنوان الحماية الجنائية للبيانات المعالجة إلكترونيا، مقدم إلى مؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة بالتعاون مع مركز الامارات للدراسات

تكنولوجيا الحاسب الآلي صاحبها تطور آخر هو تطور نظم الاتصالات عبر استخدام وسائل متعددة كالأقمار الصناعية والشبكات الأرضية دون اعتبار للمسافات وهو ما سهل استعمال وسائل الدفع الإلكتروني لتبادل هذه المعلومات ولابد من وضع مجموعة من قواعد الاتصال المعيارية المتفق عليها مسبقا والتي تسمى بروتوكولات protocolesلإرسال رسالة من جهاز ما إلى آخر عبر الشبكة حيث تجزأ هذه الرسالة في الطرف المرسل إلى وحدات وحزم ثم ترسل عبر خطوط الاتصال ليعاد تجميعها في الطرف المستقبل عبر مراحل وأجهزة معينة كالمودم[1]، والموزع الشبكي[2]، والمكرر[3]،والجسر[4]والموجة[5]، والبوابة[6].

الجرائم الإلكترونية تمثل خطرا حقيقيا على البنوك واستقرارها المالي في زمن هذا الربط بين الفاعلين في النظام المالي[7] وبالنسبة لوسائل الدفع الإلكتروني فالأموال كقيمة إلكترونية تخزن في شكل رموز في صيغة نقد إلكتروني ويكون لكل منهما رقم متسلسل محدد ومرتبط

والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة، المنعقد بتاريخ 01-03 ماي 2000، المجلد الثاني، الطبعة الثالثة 2004، ص593.

[1]- المودم modem :مهمته تحويل الاشارات الرقمية الصادرة عن خطوط الهاتف إلى تواصلية لأن أجهزة الحاسب الآلي لا تتعامل إلا مع الاشارات الرقمية فقط في بداية الأمر ثم تعديلها من رقمية إلى تواصلية عبر عملية التعديل وتحويلها مرة أخرى من تواصلية إلى رقمية في الطرف المستقبل عبر عملية فك التعديل.

[2]- الموزع الشبكي hub: يربط قطع الشبكة مع غيرها.

[3]- المكرر reporter يستعمل لانعاش الاشارة المرسلة عبر الشبكة لتبقى قوية دون تشويش إلى غاية وصولها للجهة المستقبلة لها.

[4]- الجسر bridge يستعمل لربط شبكتين محليتين ببعضهما البعض وهو مهم لتوسيع الشبكات .

[5]- الموجة router:تربط الشبكات مع بعضها بشكل اضخم بالاعتماد على العناوين المنطقية والعمل على نقل الحزم المعلوماتية الى هدفها عبر الشبكة الاخرى.

[6]- البوابة getway:عبارة عن اجهزة وبرامج تربط بين مختلف الشبكات لنقل المعلومات وتحويلها الى صيغة تتوافق مع بروتوكولات الشبكة الاخرى.

[7] -Édouard fernandez-bollo, la Cybercriminalité risque Systémique pour le secteur financier, Revue Banque, N 793 février 2016, p22.

بمسمى ثابت غير متغير وتتم المعاملات بنقل الرموز النقدية من جهاز إلى آخر ويكون مجموع مسمى هذه الرموز النقدية على الجهاز هو قيمة التحويل للموازنة المخزنة عليه باستخدام الشبكات بمختلف أنواعها ويختلف الأمر مثلا بالنسبة للبطاقات حيث يتم تحويل المدفوعات من حساب الزبون إلى حساب مقدم الخدمة أو السلعة وهذا يتوقف على نوعية الاتصال المنوط بجهاز الحاسب الآلي والمتعامل معه سواء كان نظام الاتصال مباشر online أو نظام اتصال غير مباشر offline.

الجريمة المعلوماتية تستهدف في جوهرها المعلومات بمفهومها الواسع من بيانات ومعلومات وبرامج تطبيقية بحيث تقوم الجريمة المعلوماتية على اعتبارين أولهما أن تكون المعلوماتية وسيلة للغش والتحايل والاعتداء وثانيهما أن تكون المعلومة نفسها محلا لهذا الاعتداء[1].

الجريمة المرتبطة بوسائل الدفع الإلكتروني تتسم بطبيعة خاصة على اعتبار أن معظمها يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء كان في تجميعها أم في تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات، يشترط لقيامها التعامل مع بيانات مجمعة ومجهزة للدخول إلى النظام المعلوماتي من أجل معالجتها إلكترونيا عبر مراحل: **مرحلة الادخال** حيث تترجم المعلومات إلى لغة مفهومة من قبل الحاسب الآلي يكون من السهل إدخال بيانات جديدة لا علاقة لها بالمعطيات القائمة ومحو البيانات الأساسية المطلوب إدخالها[2]، **حيث تعتبر هذه المرحلة جد مهمة للجناة لأنه يتم ارتكاب أكثر الجرائم**

[1]- معادي أسعد محمد صوالحة، المرجع السابق، ص 243.

[2]- خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008، ص50.

بواسطة استعمال وسائل الدفع الإلكتروني من خلالها كتغيير الأسماء أو الأرقام، أو المعلومات الشخصية، ...الخ، حيث يتم في هذه المرحلة الاستيلاء من طرف الجناة على بيانات شخصية غالبا ما تتعلق بعناصر الذمة المالية بغية تحويل الأموال لأنفسهم، إذ قد يتم إدخال إتلاف البيانات عن طريق استبدال رقم حساب بآخر أو إحلال بطاقة محل أخرى وهذا النوع على قدر كبير من الخطورة لأنه في حالة نجاح العملية يمكن أن تستمر لفترة من الزمن حتى يمكن كشف الفعل غير المشروع حيث أن هناك مجموعة من المستخدمين الاداريين على سبيل المثال استطاعوا خلال سنوات عديدة أن يضاعفوا من رواتبهم[1]، وحتى أن طريقة الكشف عنهم تمت بمحض الصدفة، لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيد بوجود حماية فنية[2]، رغم أن الواقع يؤكد أن غالبية الأنظمة الخاصة بالمصارف والتحويلات المالية تخضع للحماية الفنية ولا يتصور أن تغيب هذه الحماية.

مرحلة المعالجة حيث يمكن إدخال أي تعديلات على البرنامج فيتم **التلاعب ببرامج العمل المعتمدة من البنك وشركائه في عملية الدفع الإلكتروني (التاجر وصاحب وسيلة الدفع الإلكتروني أو بقية البنوك) فيتم إدخال بيانات غير مصرح بها واستبدالها بالبيانات الأساسية**، لأن أي برنامج عند إعداده له أخطاء وعيوب قد لا تكتشف كلها أو بعضها إلا

---

[1]- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2009، ص 145.

[2]- علي عبد القادر القهوجي، المرجع السابق، ص 595.

عند التطبيق ويستطيع المبرمج القيام بتصحيحها عن طريق الولوج إلى البرنامج الذي صمم للعمل بوسيلة الدفع الإلكتروني في أي وقت لتحقيق مكاسب مادية شخصية.

مرحلة الإخراج: يتم التلاعب في النتائج التي يخرجها النظام المعلوماتي بشأن بيانات غير صحيحة أدخلت فيها معالجة غير صحيحة، **وتقوم فكرة هذه المرحلة على السرقة من عدد كبير من الحسابات البنكية وبخصم قيمة ضئيلة عند استعمال أي وسيلة للدفع الإلكتروني وعادة تتم في حالة الإشعار بالاقتطاع**، حيث يتم الخصم من عدد كبير من الحسابات بكميات ضئيلة بحيث لا يتفطن لها صاحب الحساب الذي تم الخصم منه، أو يقدر اذا اكتشفها أن المسألة لا تستحق الابلاغ، إلا أن القائم بالخصم على مر السنوات تتراكم لديه مبالغ طائلة، أو إذا كانت الحسابات بأعداد كبيرة فإن المبالغ عند تجميعها تصبح كبيرة. **ومنه نستنتج امكانية ارتكاب الجرائم المرتبطة بوسائل الدفع الإلكتروني باعتبارها جريمة إلكترونية، في أي مرحلة من مراحل تشغيل نظام المعالجة الآلية للمعطيات (الإدخال – المعالجة –الإخراج)**، غير أن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر لطبيعتها ارتكاب الجريمة المعلوماتية إلا في وقت محدد يعتبر هو الأمثل بالنسبة لمراحل التشغيل[1].

ثانيا/تعدد صور الركن المادي للجريمة المتعلقة بوسائل الدفع الإلكتروني

[1]– عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية، مجلة مركز دراسات الكوفة، العدد السابع، 2008، ص 115.

تتعدد مظاهر الاعتداء على وسائل الدفع الإلكتروني فقد تكون الوسيلة نفسها موضوع الجريمة، أو تكون الوسيلة أداة لتنفيذ الجريمة، حيث يستهدف الاعتداء على وسائل الدفع الإلكتروني المعطيات الإلكترونية بدلالتها التقنية الواسعة من بيانات ومعلومات وبرامج، وفي حالة الاعتداء وسائل الدفع الإلكتروني مثلا وباعتبارها إحدى الصور الخاصة للاعتداءات التي تقع على الحاسب الآلي تتعدد صور الاعتداء، فقد يقع الاعتداء على نظام التشغيل الآلي لتحويل الأموال في حسابات البطاقات، أو قد يقع على ذات وسيلة الدفع الإلكتروني كالتزوير والاصطناع والتقليد من طرف حاملها أو من الغير كما قد يقع الاعتداء من قبل العاملين في المصارف أو من قبل التجار المتعاملين بهذه الوسائل أو أن يتم التحايل عبر الانترنت.

الفرع الثاني

الجرائم المتعلقة بوسائل الدفع الإلكتروني اقتصادية معقدة ولامادية

الجرائم المتعلقة بوسائل الدفع الإلكتروني جرائم اقتصادية[1]، معقدة ولامادية وتتميز بصفة عامة بالخطورة لأنها تمس البنوك المصدرة لهذه الوسائل في ذمتها المالية مما يؤثر عليها وعلى المؤسسات التي تتعامل بها في اقتصادها، وعلى سمعتها لأنها لم تتحكم في أمنها

[1]- يختلف الفقه حول مفهوم الجريمة الاقتصادية فالاتجاه الأول يضيق من مفهوم الجريمة الاقتصادية ليقصرها فقط على السلوكيات المخالفة للقواعد التي تحكم الأسعار في حين يأخذ اتجاه آخر بمفهوم واسع للجريمة الاقتصادية بحيث تشمل كافة النصوص الجزائية التي وضعت لحماية مصلحة الدولة في الامور الاقتصادية ومصالح الافراد الناتجة عن العلاقات الاقتصادية التي تربطهم مع بعضهم البعض، أنظر نائل عبد الرحمان صالح، الجرائم الاقتصادية في التشريع الاردني، دار الفكر للنشر والتوزيع، الطبعة الأولى، الجزء الأول، الأردن 1990، ص12،13.

المعلوماتي هذا من جهة، ومن جهة أخرى تمس البلاد ككل في أمنها القومي بمفهومه الحديث وهذا بالنظر إلى حجم الخسائر التي تخلفها، كما أن الاستعانة بالرقمية زادت الجريمة الاقتصادية والمالية تعقيدا لأن الجرائم الاقتصادية والمالية جرائم من الصعب ايقافها وتحديدها كما أصبحت أيضا معقدة بعد الآن لأن مرتكبيها يستهدفون الاستعانة بالشبكات والحاسبات الآلية والتكنولوجيا الرقمية متجاهلين الحدود الجغرافية للدول مما يصعب من مهمة قوانين الدول في ايقافها وتجد المؤسسات غموض قانوني على النطاق الدولي[1].

ومن المعلوم أن الحاسب الآلي يستخدم في الأنشطة الاقتصادية بكثرة، والنشاط الاقتصادي وجه من أوجه نشاط الفرد وأكثر هذه النشاطات فعالية في حياة الجماعة ولكن من أصعبها ضبطا إذ أن أمر احتوائه ضمن أنظمة تفصيلية من شأنه أن يكبله ويحد من اندفاعه، كما أن أي سلطة تعجز عن استباق أوجه النشاط الاقتصادي فلا تتمكن غالبا من الوقوف على سلبياته إلا بعد تحققها[2]، وباعتبار وسائل الدفع الإلكتروني لا يمكن العمل بها إلا من خلال الحاسب الآلي الذي يكون في العادة مرتبط بحاسبات مركزية ترتبط فروعها بشبكات داخلية أو خارجية (سواء كانت محلية أو دولية) بالتالي كثرت جرائم الحاسب الآلي التي تتم بوسائل الدفع الإلكتروني خاصة البطاقات لاستهدافها الاستيلاء على أموال المصارف وبالتالي المساس بجانب اقتصادي مهم وهو القطاع المصرفي، فكل سلوك ذا علاقة بالاقتصاد

[1]-Myriam Quéméner, criminalité économique et financière à l'ère numérique, op. cit, P19 ,20.

[2]- محمود داوود يعقوب، المسؤولية في القانون الجنائي الاقتصادي، دراسة مقارنة بين القوانين العربية والقانون الفرنسي، الطبعة الأولى، 2001، دمشق، سوريا، ص 18.

الوطني يعتبر متضمنا لجريمة اقتصادية فالجرائم المتعلقة بوسائل الدفع الإلكتروني كتزوير العملات الإلكترونية وتهريب الأموال عبر هذه الوسائل التقنية المتطورة وتبييضها كلها جرائم تخالف مصلحة الاقتصاد الوطني والقطاع البنكي القائمة على الثقة والائتمان.

هناك صعوبة في وضع رقم محدد واضح المعالم لحجم الخسائر في الجرائم المعلوماتية وهو ما يعبر عنه بالرقم الأسود[1] الذي يبقى الرقم الأكبر، والسبب الرئيسي لعدم ابلاغ البنوك عن هذه الجرائم يرجع إلى الخوف على سمعتها وكذا خوفها من التعرض إلى التشهير بها مما يصعب قياس الضرر الناتج عن استخدام البرامج الخبيثة على البنوك ووسائل الدفع الإلكتروني لأن الآثار تختلف حسب نوع الجريمة ونوع البيانات والأنظمة المعلوماتية المستهدفة سواء كان الضرر مباشرا باستهداف التجهيزات والبرامج، ويمكن أن يكون الضرر غير مباشر ينتج عنه توقف المنظومة عن العمل، كما يمكن أن يؤدي الابلاغ عن جرائم وقعت على وسيلة دفع معينة إلى احجام المستهلكين عن استخدام هذه الوسيلة في حين تسعى البنوك إلى تشجيع التعامل بوسائل الدفع الإلكترونية، وبالتالي تنفق مبالغ باهظة قصد تطوير الحماية التقنية.

اذا كانت المصارف موصولة بشبكة الانترنت فإن وسائل الدفع الإلكترونية ستضاعف من حجم هذه الجريمة لأنها تضمن السرية الكاملة وعدم كشف عن القائم بالجرم مما يجعل منها قناة مثالية لتنفيذ العديد من نشاطات الجريمة المنظمة.

[1]– الرقم الأسود يشير لعدم التبليغ عن الجرائم المعلوماتية الأمر الذي من شأنه أن يخفي الرقم الحقيقي.

ساهم انتشار أشكال الجرائم الإلكترونية خاصة مع تكرار سرقة بطاقات الائتمان في اضفاء حالة من الرعب على المؤسسات الاقتصادية العربية الضخمة وبدلا من معالجة الأخطاء وتفعيل القوانين وتفعيل وسائل الحماية والوقاية اكتفى الجميع بالجلوس في أماكنهم[1]، وإذا تطرقنا لأركان الجريمة الاقتصادية فإننا نجد الركن الشرعي فضفاضا ويمتاز أحيانا بالغموض وعدم الدقة فالجرائم الاقتصادية تشكل خطرا على النظام الاقتصادي للدولة وليس بالأمر السهل ولا اليسير تحديد هذه الأفعال ولذلك فإن النص غالبا ما يتسم بالعمومية[2]، وبالتالي نتساءل كيف سيكون الأمر إذا اختلط الجانب الاقتصادي بالجانب المعلوماتي التقني وبالعمليات المصرفية ووسائل الدفع الإلكتروني فكيف سيحدده القاضي؟ هذا ما يحتم علينا إعادة النظر في منظومتنا القانونية وتعديلها في هذا الجانب وإلا سنجد أنفسنا أمام فراغات تشريعية لا حصر لها.

الفرع الثالث

جرائم عابرة للحدود صعبة الإثبات

نبهت المفوضية الأوربية في تقريرها الصادر سنة 1999 أن هناك ضعف وتضارب في القوانين الموجودة في العديد من الدول الأعضاء التي تكافح الاحتيالات العابرة للحدود وهو ما سهل على العصابات الإجرامية الدولية استغلال هذه الاختلالات، فالجرائم المعلوماتية

---

[1]- نهلا عبد المومن، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ص51.

[2]- أنور محمد صدقي المساعدة، المسؤولية الجزائية عن الجرائم الاقتصادية، دراسة تحليلية تأصيلية مقارنة في التشريعات، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2009، ص 57.

عموما تتسم بهذه الميزة، الجرائم المعلوماتية لا تترك أثرا فليست هناك أموال مفقودة، وإنما هي أرقام تتغير في السجلات الإلكترونية للبنوك ولذا فإن معظم الجرائم المتعلقة بوسائل الدفع الإلكتروني يتم اكتشافها بالصدفة.

أولا/ الطبيعة العابرة للحدود للجرائم المتعلقة بوسائل الدفع الإلكتروني

يشكك البعض في مدى فعالية القوانين الحالية في التعامل مع هذا النوع الجديد من الجرائم المعلوماتية، فالجرائم المرتبطة بوسائل الدفع الإلكتروني تتميز بالطبيعة العابرة للحدود وهذا أثر طبيعي نتيجة الخاصية التي يتمتع بها الدفع الإلكتروني بأنه وسيلة مقبولة في جميع الدول هذه الطبيعة أفرزت عدة مشاكل كمشكل تحديد الاختصاص القضائي وبالتالي الدولة المختصة بالعقاب ومنه القانون الواجب التطبيق[1].

القدرة التي تتميز بها وسائل الدفع الإلكتروني في نقل وتبادل كميات كبيرة من الأموال إلى دول مختلفة وبسرية تامة وتتفادى هذه الوسائل اجراءات الرقابة المفروضة من الدول على تحويل الأموال بوسائل الدفع التقليدية، حيث أفرزت وسائل الدفع الإلكتروني في ظل التقنية الحديثة اقتصاد بلا حدود فجريمة بلا حدود وتم استغلال وسائل الدفع الإلكتروني أسوء استغلال فعن طريق الأنترنت يتم تحويل الأموال إلكترونيا وتبييضها، ويزدهر ويتزايد الجنوح

[1]– من أشهر القضايا في هذا المجال قضية " Rv Thompson" حيث قام أحد العاملين في أحد البنوك في الكويت بإجراء عمليات تحويل للأموال من حساب الزبائن إلى حسابه الخاص وبعد عودته إلى انجلترا بلده الأصلي قام بمراسلة البنك ومطالبته بتحويل حسابه الخاص إلى مجموع حسابات بنكية له في انجلترا وهو ما قام به البنك، وتم اكتشاف عملية الاختلاس هذه وتم تقديم المتهم للمحاكمة بتهمة السرقة إلا أنه دفع بعدم الاختصاص للقضاء الانجليزي إلا أن الطعن لم يقبل لأن نشاطه الاجرامي لم يكتمل إلا في انجلترا .

الاقتصادي في البيئة الرقمية فهذه الظواهر تساهم في انطلاق وتحليق الجريمة الاقتصادية والمالية عالميا[1]، وتصبح البلدان التي لا تعتمد تشريعات فعالة هدفا لمرتكبي هذه الجرائم الذين يستغلون غياب الأطر التنظيمية في هذا المجال، حيث ساهم اجراء المعاملات المصرفية بوسائل الدفع الإلكتروني في إضفاء الصبغة الدولية على الاعتداء المعلوماتي المتعلق بالمعاملات المصرفية الإلكترونية وأصبحت لا تعرف الحدود الجغرافية فالزبون يستطيع من أي بقعة على الأرض أن يجري معاملاته طالما توفرت له امكانيات الدخول على شبكة الانترنت[2]، وبالتالي فإن استخدام وسائل الدفع الإلكتروني في اتمام المعاملات المصرفية من مزاياه أنه لا يعرف قيودا زمانية أو حدودا جغرافية.

وأهم المشاكل تلك المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة بالإضافة إلى نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت، وجمع الأدلة عنها للإدانة فيها يشكل عائقا كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم[3]، اضافة التذرع بحجية السرية المصرفية واختلافها من دولة إلى أخرى يشكل عائقا آخر أمام مكافحة الجريمة المصرفية وخاصة إذا تمت هذه الجريمة في هيئتها الجديدة الخفية ألا وهي وسائل الدفع الإلكتروني التي أصبحت تنافس الوسائل التقليدية .

---

[1]-Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit, P17.

[2]- بلال عبد المطلب بدوي، المرجع السابق، ص 1935.

[3]- نهلا عبد المومن، المرجع السابق، ص34.

ثانيا/ صعوبة اثبات الجرائم المتعلقة بوسائل الدفع الإلكتروني

تزداد صعوبة اثبات الجرائم المتعلقة بوسائل الدفع الإلكتروني نتيجة عدم قيام البنوك بالإبلاغ عنها خوفا من احجام الزبائن على استعمال هذه الوسائل، والجريمة المرتكبة بوسائل الدفع الإلكتروني تتم في بيئة غير مادية أي في اطار افتراضي مما يزيد من صعوبة اجراءات التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة، فالجاني يستطيع تدمير أثر الادانة في أقل من ثانية، مما يصعب من اثباتها لعدم وجود أدلة مادية عليها كما يسهل اتلاف الأدلة الخاصة بها وارتكاب هذه النوعية من الجرائم يتم من مسافات بعيدة.

الجريمة عبر الانترنت أصبحت إحدى أشكال الاستغلال الاقتصادي الأكثر فائدة وغالبا مع خطر ضعف الاكتشاف وأكثر الميادين استهدافا هي الخدمات المالية والتجارية عبر الخط وأصبحت المصدر الأول لسرقة المال والمعلومات المالية[1]، وكذلك الرغبة في استقرار حركة التعامل ومحاولة اخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين يدفع المصرف المجني عليه إلى عدم مساعدة السلطات المختصة في إثبات الجريمة[2]، وحتى أثناء التحقيق فإنه لا يتعاون تخوفا مما يخلفه من اهتزاز لثقة الزبائن والمساهمين في المصرف. الجانب الأكبر من هذه الجرائم تحرص مجالس ادارات البنوك على اخفائها حتى

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit p37.

[2]- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول الجرائم الناشئة عن استخدام الحاسب الآلي، مكتبة دار النهضة العربية، مصر، ص 11.

بين موظفيها وتنتهي باتخاذ اجراءات داخلية عادة مما يؤثر سلبا في السياسة التي يمكن أن توضع لمجابهة هذا النوع من الاجرام، كما أن الاعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه[1] وهذا لأن البنوك تتخوف من خطر جديد يضاف للأخطار التي تتعرض لها أثناء أداء نشاطها، فالجناة من الصعب معرفتهم من الناحية التقنية وبالأخذ بالاعتبار الأرباح المهمة التي يحققونها فالأخطار الاقتصادية والعقابية متعلقة ببعضها البعض وضعيفة أمام هذا النوع من الأخطار[2].

المطلب الثاني

المبادئ العامة للمسؤولية الجزائية ووسائل الدفع الإلكتروني

المشرع الجنائي هو الوحيد الذي يتدخل ليتناول بالتجريم والعقاب ما يستجد من أفعال لم تكن تقع من قبل تحت سلطانه بالعقاب (الفرع الأول)، ولكن سرعة تطور الجرائم المرتبطة بوسائل الدفع الإلكتروني يستلزم تفويض الاختصاص(الفرع الثاني)، وبالتالي هل يمكننا التفسير للنصوص الجزائية المعاقبة على الجرائم المرتكبة بوسائل الدفع الإلكتروني (الفرع الثالث).

[1]- نهلا عبد المومن، المرجع السابق، ص37.

[2]- Myriam Quéméner, criminalité économique et financière à l'ère numérique , op, cit , p35.

الفرع الأول

وسائل الدفع الإلكتروني وأزمة الشرعية الجزائية في القانون الجزائري

تثير المسؤولية الجزائية عن استعمال وسائل الدفع الإلكتروني أزمة شرعية التجريم في التشريع الجزائري الذي يقتضي وجود نص تجريمي سابق على ارتكاب الفعل، ومبدأ الشرعية يعني حصر مصادر التجريم والعقاب في نصوص القانون ولهذا المبدأ شقان: الأول يعني شرعية وقانونية التجريم (تحديد الأفعال التي تعد جرائم)، والثاني يعني شرعية قانونية العقاب (بيان العقوبات المقررة للجرائم)، وليست هذه القاعدة من أصول قانون العقوبات فحسب وإنما هي من الأصول الدستورية فلا تستطيع السلطة التشريعية مخالفتها، بل ولو لم يرد بها نص في الدستور فهي من قواعد النظام الطبيعي التي لا تحتاج إلى نص يقررها[1]، ومن نتائج مبدأ الشرعية حصر التجريم والعقاب في يد السلطة التشريعية وكذا التزام القاضي بمبدأ التفسير الضيق للنص القانوني، وعدم سريان العقوبات إلا على المستقبل فالقاضي قبل أن يصدر حكمه عليه أن يشير في كل واقعة تعرض عليه إلى النص القانوني المجرم لها وقت ارتكابها، ومن هنا على المشرع الجنائي الجزائري أن يتدخل بالتجريم والعقاب على ما يستجد من الأفعال الإجرامية المرتبطة بوسائل الدفع الإلكتروني والتي لا تقع تحت سلطانه وذلك تطبيقا لمبدأ الشرعية، الذي يعد تجسيدا لمبدأ الفصل بين السلطات حتى تبقى السلطة التشريعية وحدها صاحبة الاختصاص بتشريع القوانين وتحمي من تعسف القضاة في إصدار

[1]-محمد محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، الجزء الثاني، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الثانية، 1979، ص61.

الأحكام، فالقاضي حتى ولو اقتنع بأن الفعل يشكل جريمة إلا أنه لا يملك سلطة العقاب على الأفعال التي لم يجرمها القانون ولا يملك سلطة اختيار العقوبات ماعدا تلك التي حددها القانون لأن العلة من إقرار مبدأ شرعية الجريمة والجزاء هو حماية الفرد حيال السلطة حيث أن الانسان لا يشعر بالأمان إذا كان لا يعلم ماهي التصرفات المباحة وتلك المحظورة والعقوبات المقررة لها[1] ومن أهم الانتقادات التي وجهت لمبدأ الشرعية أنه يقيد سلطات القاضي الجزائي ويقف حجرة عثرة أمام حق المجتمع وواجبه في مواجهة الأفعال الخطيرة التي تلازم التطور الاجتماعي والتقدم العلمي والتقني فالمشرع حين يجرم الأفعال الضارة أو الخطرة التي تمس بمصالح المجتمع إنما يضع في حسبانه المصالح القائمة وقت إصدار التشريع وكذلك صور الأفعال التي يمكن أن تضر بتلك المصالح حسب تصوراته وقت اصداره للقاعدة القانونية[2] لأن المشرع لا يجرم إلا لحماية المصالح القائمة ولا يأخذ بعين الاعتبار تطور المجتمع والمصالح المتطورة مما ينجر عنه عجز التشريع العقابي عن حماية المصالح المتطورة وبالتالي إفلات عديد المجرمين من طائلة العقوبة خاصة الذين يعرفون كيفية الاستفادة من ثغرات التشريع فيرتكبون أفعالا ضارة بالمصالح والحقوق محل الحماية الجنائية إلا أنها غير مطابقة للنموذج القانوني المنصوص عليه صراحة في القاعدة القانونية الجنائية، كذلك يوصف مبدأ الشرعية بأنه عنوان للجمود وعدم القدرة على شمول كافة التصرفات الضارة بالمصلحة العامة والمصالح الفردية التي يمكن أن يبتدعها العقل الإجرامي

[1]- نهلا عبد المومن، المرجع السابق، ص53.

[2]- عادل يوسف عبد النبي الشكري، المرجع السابق، ص119.

وتضر المجتمع في كافة المجالات[1]، وبالتالي على القانون الجنائي أن يواكب التطورات التكنولوجية التي تقدم فرصا واسعة لإساءة استخدام امكانيات الفضاء المعلوماتي، وأن يعمل على ردع هذه الأفعال الاجرامية[2] لذا نجد أن بعض التشريعات الجنائية قامت بإلغاء النص على مبدأ الشرعية الجزائية[3] إلا أن إلغاء هذا المبدأ ينتج عنه أضرار تفوق بكثير الأضرار التي قد تتحقق من الالتزام به وبالتالي هذه الانتقادات لم تنل من مبدأ الشرعية وإن كانت خففت من حدته وسمح فيه بنوع من المرونة للقاضي في الشق الثاني والمتعلق بتقدير العقوبة دون الشق الأول المتعلق بتحديد الجرائم، فأصبحت للقاضي سلطة في تقدير العقوبة التي تتفق مع ظروف الجريمة وطبيعة الجاني بين الحد الأقصى والحد الأدنى كما أعطيت له سلطة اختيار نوع العقوبة وأعطي للسلطة التنفيذية حق التدخل في تنفيذ العقوبة فقرر لها حق العفو والتخفيف والافراج المشروط، كما أن مبدأ الشرعية لم يبق على جموده بل تطور مع تطور المجتمع والدليل على ذلك تجريم العديد من التصرفات التي لم تكن تشكل في الماضي أية خطورة أو ضرر بالنسبة للمجتمع أو الأفراد ومن الأمثلة على ذلك جريمة الدعاية التجارية الكاذبة ومعظم الجرائم الاقتصادية[4].

---

[1]- نائل عبد الرحمان صالح الطويل، ناجح داود رباح، الأعمال المصرفية والجرائم الواقعة عليها، الجزء الأول، الطبعة الأولى، 2000، دار وائل للطباعة والنشر، الأردن، ص76.

[2]- طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلوماتية "، دار الجامعة الجديدة، 2009، ص14.

[3]- القانون السوفياتي الصادر سنة 1922وكذا قانون 1926، والقانون الالماني لسنة 1935، القانون الدانماركي لسنة 1933، أنظر عادل يوسف عبد النبي الشكري، ص120،119.

[4]- نائل عبد الرحمان صالح الطويل، ناجح داود رباح، المرجع السابق، ص28.

أصبحت وسائل الدفع الإلكتروني المفضلة للتعامل بها محليا ودوليا عن طريق الشبكات الإلكترونية إلا أن التطور أتاح الفرصة لإساءة استخدامها بمحاولة الاعتداء على نظام الدفع الإلكتروني، حيث تتم معظم التحويلات بالبطاقات التي تتم عبر الشبكات الإلكترونية المتصلة بالحاسبات الآلية بحيث أصبحت نظرا لوقوعها في غالبية الأحيان داخل بيئة المعالجة الآلية للبيانات من أخطر الجرائم مما دفع البعض إلى الاعتراف بأننا أمام ظاهرة اجرامية ذات طبيعة خاصة تحتاج إلى قانون جنائي معلوماتي خاص[1]، وحتى لا نصطدم بمبدأ الشرعية قامت العديد من الدول بسن القوانين لحماية البطاقات سواء من تلقاء نفسها أو بناء على ضغوطات مورست عليها من المؤسسات العالمية المنظمة لهذه البطاقات.

مما استعرضناه سابقا تثير وسائل الدفع الإلكتروني مسألة الحماية القانونية لأن ظهور المعلوماتية أدى إلى ظهور مشاكل قانونية مرتبطة بالمسؤولية الجزائية أي ظهور ما يسمى أزمة القانون الجنائي لتقيد القاضي بمبدأ الشرعية[2] والسؤال الذي يطرح نفسه هل تكفل النصوص الجنائية في القانون الجزائري حماية لوسائل الدفع الإلكتروني في نصوصها الحالية حيث أننا لسنا بحاجة إلى نصوص جديدة خاصة أم أن الأمر يحتاج إلى نصوص جديدة؟

---

[1]- معادي أسعد محمد صوالحة، المرجع السابق، ص 229.

[2]- بوعناد فاطمة الزهراء، مكافحة الجريمة الالكترو نية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول عام 2013، ص 63.

بالرجوع إلى قانون العقوبات الجزائري والقوانين المتعلقة بالنقد والقرض نلاحظ أنه لم ينص على الجرائم المتعلقة باستعمال وسائل الدفع الإلكتروني وهذا راجع حسب اعتقادنا إلى محدودية استعمال هذه الوسائل لدى المواطنين بالمقارنة مع الشيك ووسائل الدفع التقليدية لكن هذا لا يمنع البنوك من استعمال هذه الوسائل خاصة البطاقات وبالتالي نتصور إحالة هذا النوع من القضايا على القضاء وهنا لاشك أن القاضي سيجد نفسه في إشكالية تكييف فعل الاعتداء على النصوص القانونية.

في الواقع فإن ترك مرتكبي الجرائم التقنية دون التصدي لأفعالهم الجرمية ومساءلتهم سيؤدي إلى فقد الثقة بالمؤسسات الحكومية وهذا ما أدركته العديد من الدول التي اتجهت إلى وضع نصوص عقابية خاصة لمواجهة هذه الجرائم الحديثة ونصت على صورها صراحة ولم تترك الأمر إلى النصوص العقابية التقليدية التي لا يجوز القياس عليها في التجريم أو التوسع في تفسيرها تطبيقا لمبدأ الشرعية[1] وعلى المشرع الجزائري مادام يسعى إلى تجسيد مشروع الصيرفة الإلكترونية وكذا تعميم استعمال وسائل الدفع الإلكتروني وتحديث منظومة الدفع الانتباه إلى النصوص الجنائية وليس المنظمة للتعامل بهذه الوسائل فقط حتى لا نصطدم بمبدأ الشرعية، وحسنا فعل المشرع الجزائري بإصدار أنظمة بنك الجزائر التي تسير أنظمة الدفع الإلكتروني وتعديله لقانون النقد والقرض فيما يتعلق بالدفع الإلكتروني إلا أنه لحد الساعة اكتفى بتعديل قانون العقوبات دون أن يمس التعديل الجانب الجزائي من قانون النقد

[1]- نهلا عبد المومن، المرجع السابق، ص 54.

والقرض في الجانب الإلكتروني وبتعديله للقانون التجاري وادراجه لبعض وسائل الدفع الإلكتروني كذلك لم يدرج ضمنه عقوبات جزائية مصاحبة لهذه الوسائل.

على المشرع الجزائري السعي إلى وضع نصوص قانونية خاصة بالجرائم المرتبطة باستعمال وسائل الدفع الإلكتروني لا الاكتفاء بتعديل بعض مواد قانون النقد والقرض فقط خاصة بعد تصديقه على الاتفاقيات الدولية والعربية المتصلة بتكنولوجيا المعلومات وهذا حتى نتجنب أزمة الشرعية الجزائية عند التعامل بهذه الوسائل.

الفرع الثاني

ضرورة التفويض التشريعي في الجرائم المتعلقة بوسائل الدفع الإلكتروني

مبدأ الشرعية يجعل سياسة التجريم والجزاء من صلاحيات المشرع وحده ويمنع الهيات الأخرى من ممارسة هذه السلطة لضمان الحرية الكافية للأفراد ومن ثم فإنه يتعين على السلطة التشريعية وحدها القيام بسن النصوص التجريمية غير أن ما يمكن ملاحظته هو أن لفظ المشرع الجنائي له مدلول واسع يعني كل سلطة لها صلاحية التشريع وأنه بالرغم من وضوح الاختصاص في مجال التجريم بصفة أصلية لكل جهة فإن المشرع يتخلى عن سلطته في مجال التجريم والجزاء إلى السلطة التنفيذية بصفة مباشرة وإلى السلطة القضائية بصفة غير مباشرة ويلاحظ أن هذا التخلي قد يكون لأسباب ايديولوجية أو للضرورة بحيث أن تعقد

الحياة الاقتصادية والاجتماعية وما تقتضيه من تعدد وتنوع في التجريم يجعل المشرع في

إن التفويض التشريعي دليل على عدم جمود القاعدة القانونية الجزائية بل إنها تتطور مع تطور المجتمع[2] فعلى عكس القاعدة في القانون العام يتجه الفقه إلى تأييد تفويض السلطة التنفيذية في التجريم خروجا على أحكام القوانين الاقتصادية إذ لا يتسنى الرجوع إلى السلطة التشريعية بالسرعة اللازمة لمواجهة مشاكل التنفيذ[3]، وأمام دقة ميادين الجرائم الاقتصادية ألزم المشرع ضرورة اعتماد تقنية التفويض من أجل تحديد الجرائم نتيجة عدم تماشي المبادئ التقليدية لقواعد القانون الجنائي مع متغيرات السياسة الاقتصادية[4] لأن تفاصيل التجريم تحتاج إلى خبرات علمية وفنية، في حين يرى البعض بأن هذا الأسلوب فيه نوع من المخالفة لمبدأ شرعية الجرائم والعقوبات[5]، حيث ينبغي ألا يمس التفويض التشريعي بمبدأ الشرعية

يدخلوا تلك الدائرة مما يؤدي إلى استفادتهم من الجريمة، موضحا إفلاتهم من دائرة العقاب بنفس الوقت .

6- عدم تمكن السلطة التشريعية من التدخل في أي فترة تقتضي فيها الضرورة وضع نصوص لتنظيم بعض المسائل الاقتصادية لذلك يجب أن تمنح الإدارة المختصة بتنظيم الاقتصاد في كافة الميادين بصفتها الجهاز الوحيد الذي يبقى على صلة مستديمة بالمسائل الاقتصادية والمطلع على أهم المتغيرات التي ستطرأ مستقبلا على الوضع الاقتصادي في كافة الميادين، تمنح الحق في تحديد الجرائم الاقتصادية إذ أن إعطاءها هذا الحق هو الضمان الوحيد لحماية السياسة الاقتصادية بالسرعة المطلوبة[1] و عكس القاعدة في القانون العام يتسع نطاق التفويض التشريعي في تعيين الجرائم الاقتصادية ويقتصر دور المشرع على إصدار نصوص على بياض ويعهد إلى سلطات ثانوية بملئها وبعبارة أخرى يكتفي المشرع بوضع مبادئ عامة[2]، أي تحدد العقوبة ويترك للسلطة التنفيذية تحديد صور الجريمة وأشكالها وذلك لعدم قدرة السلطة التشريعية على متابعة الحركة الاقتصادية وبالتالي حصر وتحديد الجرائم الاقتصادية[3].

7-يعتبر مجلس النقد والقرض سلطة ادارية مستقلة في مجال النقد والقرض تنازلت له السلطة التنفيذية عن اختصاصها التنظيمي في مجال النقد والقرض نظرا لخصوصية هذا

---

[1]- نائل عبد الرحمان صالح، الجرائم الاقتصادية في التشريع الأردني، المرجع السابق، ص45.

[2]- مقني بن عمار، المرجع السابق، ص106.

[3]- محمد مخمخم، المرجع السابق، ص 27.

النشاط وتعقيده وكذا سرعته، فأمام عجز الحكومة عن مواكبة هذه المميزات اقتضت الضرورة الاقتصادية حلول مجلس النقد محل السلطة التنفيذية فهو الذي يصدر الأنظمة التي تؤطر النشاط المصرفي ويمارس رقابة فعالة على النظام المصرفي، فهو سلطة بمعنى الكلمة في النشاط المصرفي والمشرع في هذا المجال لأن التشريع في مجال النقد و القرض يتطلب دراية فنية لا تتوافر إلا لدى السلطة المفوضة، وهو مجلس النقد والقرض، كما أن أغلب نصوص قانون النقد والقرض تكون واردة بصيغة عامة حيث تحتاج إلى النصوص التنظيمية لوضع القواعد التفصيلية وبالتالي الحاجة إلى دعم التفويض التشريعي في مجال الجرائم الاقتصادية المصرفية المرتبطة بوسائل الدفع الإلكتروني ذلك أن التفويض ضرورة لازمة لتطور التشريع الاقتصادي والجزائي إضافة إلى الاستعجال والمرونة في إصدار النصوص التشريعية التي لا تستطيع السلطة التشريعية توفيرها، ومنه تصبح قواعد القانون الجنائي في خدمة السياسة الاقتصادية، فالمقصود بالنص القانوني كل قاعدة لها قوة الالزام تصدر عن السلطة التشريعية أو عن السلطة التنفيذية بناء على تفويض من السلطة التشريعية أو ضمن أحكام الدستور فمبدأ شرعية الجريمة والجزاء لا يشترط أن يكون النص قد صدر عن السلطة التشريعية بقدر ما يكون قد تقرر بموجب قانون صدر ضمن الاطار المحدد في الدستور وهذا المفهوم يقصد به مواجهة كافة الحالات التي تعوض فيها السلطة التشريعية حقها في

تحديد الجرائم والعقوبات ضمن شروط محددة إلى الجهة المكلفة بسن نظام أو اصدار التعليمات[1].

الفرع الثالث

التفسير الموسع وأثره في احتواء الجرائم المرتبطة بوسائل الدفع الإلكتروني

عندما تعرض قضية جزائية على القاضي فإن أول عملية يقوم بها هي تكييف الواقعة لمعرفة مدى تطابقها مع النص الذي يجرمها وللوصول إلى هذه الغاية يقوم القاضي باستخلاص عناصر الواقعة من النص وقد يصادف أثناء ذلك صعوبة أو غموض فيقوم عندئذ بتفسير النص الجزائي[2]، والمقصود بالتفسير معرفة المعنى الحقيقي لأحكام قانون العقوبات عند التطبيق للتأكد إذا كان هذا النص قابلا للتطبيق على الوقائع المادية المراد تطبيقه عليها[3]. تنعكس أهمية مبدأ الشرعية الجزائية على تفسير النصوص الجزائية ويضفي عليها ذاتية خاصة تميزه تتمثل في مبدأ التفسير الضيق للنص الجزائي إلا أن هذا المبدأ لا يعمل به أثناء تفسير نصوص التشريع الجزائي الاقتصادي المطبق على الجريمة الاقتصادية حيث يتم تطبيق مبدأ التفسير الواسع للنص الجزائي مما يعني توسيع نطاق تفسير النص إلى الحدود التي أرادها المشرع حتى تتطابق مع الواقع[4] أي البحث عن الغاية من وضع النص.

---

[1]– نائل عبد الرحمان الطويل، ناجح داود رباح، المرجع السابق، ص65.

[2]–بارش سليمان، المرجع السابق، ص 18.

[3]– نائل عبد الرحمان صالح، المرجع السابق، ص50.

[4]– محمد مخمخم، المرجع السابق، ص29.

على الرغم من أن القصور التشريعي قد أصبح واقعا ملموسا إلا أن هذا لا يحول دون الاجتهاد في تفسير النصوص العقابية التقليدية التي تعاقب على صور الاعتداءات المختلفة على المال بحيث يمكن تطبيقها على الجرائم المستحدثة التي أوجدها استعمال وسائل الدفع الإلكتروني بحيث يمكن أن ندخلها في اطارها متى أمكن اعتبارها من جنسها وأن المشرع يحميها بذات النصوص.

تفسير أحكام قانون العقوبات بشكل ضيق استنادا إلى مبدأ الشرعية يؤدي في بعض الأحيان إلى عجز القانون عن مواجهة المستجدات الجديدة، وخشية أن يؤدي التفسير إلى تجريم تصرفات لم تتجه إرادة المشرع إلى تجريمها عند صياغته للنص المفسر وفي الأساس ليس من وظائف المشرع التعريف والاتيان بأمثلة وتحديد عناصر أو صور الركن المادي بل تقتصر مهمة المشرع على وضع النص العام المجرد.

ضرورة قبول فكرة التفسير الموسع للنصوص في نطاق الجرائم الاقتصادية لأنها تصدر على وجه السرعة نظرا لما تمتاز به الجريمة الاقتصادية من حركية متسارعة وتتطلب استخدام مصطلحات عامة لمواكبة التطورات الاقتصادية المفاجئة داخل المجتمع، لذلك فهي لا تخلو من الأخطاء وعدم الدقة والوضوح في الصياغة كالتشريعات الأخرى التي يتم اعدادها في وقت طويل كقانون العقوبات أو الاجراءات الجزائية أو المدني.

التفسير يصبح أمرا حتميا وضروريا وحسب رأينا تزداد الحاجة إلى التفسير اذا اتصلت الميادين الاقتصادية بالجانب التكنولوجي كما يحدث في هذا الشأن بالنسبة لوسائل الدفع

أجل سن نص خاص بوسائل الدفع الإلكتروني أو تعديل قانون النقد والقرض بتجريم الأفعال المتصور أن تصيب وسائل الدفع الإلكتروني وهذا نظرا لخصوصية وسائل الدفع الإلكتروني، نذكر أن النصوص الجزائية المبتغاة لحماية وسائل الدفع الإلكتروني في القانون الجزائري هي الهدف المنشود الذي تقصده هذه الدراسة لعلاج القصور التشريعي الحالي في هذا الصدد.

المبحث الثاني

حالات المسؤولية الجزائية للفاعل الأصلي عن اساءة عن استخدام وسائل الدفع الإلكتروني

نتناول من خلال هذا المبحث حالات المسؤولية الجزائية للفاعل الأصلي عند اساءة استخدامه لوسيلة الدفع الإلكتروني ونركز على مسؤولية الحامل لوسيلة الدفع الإلكتروني باعتبارها تواجه إشكالية التكييف من الناحية القانونية وهو ما يبرز من خلال المطلب الأول (إشكالية التكييف للركن الشرعي لإساءة استخدام وسائل الدفع الإلكتروني)، ونبين الحالات المنصوص عليها قانونا من خلال المطلب الثاني (المسؤولية الجزائية لحامل وسيلة الدفع الإلكتروني).

المطلب الأول

إشكالية التكييف للركن الشرعي لإساءة استخدام وسائل الدفع الإلكتروني

أهم نتيجة نخلص إليها من محاولة تطويع النصوص التقليدية قصورها عن ملاحقة الجرائم المرتبطة بوسائل الدفع الإلكتروني لذلك نتناول من خلال الفرع الأول (ضرورة التخلي عن فكرة تطويع نصوص قانون العقوبات الخاصة بجرائم الأموال)، وبالتالي ضرورة التدخل التشريعي لأن نظريات وقواعد القانون الجنائي شيدت لملاحقة وحماية الأنشطة ذات المظاهر الخارجية وحماية الأموال المادية في حين نشأت وترعرعت حماية الملكية المعنوية في كنف القوانين المدنية وتشريعات حماية الملكية الفكرية[1]، وبالتالي نركز في الفرع الثاني على (تكييف الركن الشرعي لإساءة استخدام وسائل الدفع الإلكتروني).

الفرع الأول

ضرورة التخلي عن فكرة تطويع نصوص قانون العقوبات الخاصة بجرائم الأموال

اذا كانت التشريعات العقابية التقليدية قد تناولت الجرائم التقليدية التي تقع في الغالب على الأموال والتي لا تطال غالبية الجرائم التقنية المعلوماتية بالتجريم لاختلاف الأخيرة عن سابقاتها سواء في الطبيعية أو في الأركان أو في المحل[2]، ولعدم جدوى تضييع الجهد في تطويع النصوص القانونية في زمن أمست استجابات المؤسسات التشريعية فيه للتطور

[1]- يونس عرب، مقال بعنوان جرائم الكومبيوتر والانترنت، مجلة اتحاد المصارف العربية، عدد يناير 2002، ص65.

[2]- نهلا عبد المومن، المرجع السابق، ص52.

ضرورة رئيسية لتعزيز وجود الدولة وفعالية النظام القانوني[1]، يثبت الواقع أن القانون الجزائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري في تسخير المبتكرات للاستخدام السيء[2].

الدول المتقدمة تقنيا وصناعيا عالجت آليات الحماية الجنائية للمعلومات في ثلاث قطاعات منفصلة حماية المعلومة المال، وحماية البيانات الشخصية المتصلة بالحياة الخاصة، وحماية حقوق الملكية الفكرية لبرامج الحاسب الآلي مما أضعف آليات حماية المعطيات وحماية استخدام التقنية والذي يلح بوجوب أن تتجه أدوات الحماية إلى ترسيخ آليات عامة في نطاق نظرية عامة للحماية الجنائية للمعلومات تسقط الحدود والحواجز بين هذه القطاعات[3].

وبالتالي ضرورة التخلي عن فكرة تطويع النصوص الواردة في قانون العقوبات لمواجهة هذ النوع من الجرائم بل ندعو المشرع إلى الفهم العميق لهذه الجرائم وخصائصها، وكذا خصائص النظام المصرفي من أجل توفير الحماية الجزائية للمعلومات وكفالة استخدام الحاسب الآلي في البنوك واستخدام وسائل الدفع الإلكترونية في الدفع مع مراعاة التحديد الواضح لصور السلوك الاجرامي، والأثر التقني على الصياغة القانونية والاستعانة بذوي الخبرة والاختصاص في المجال التقني والمجال المصرفي وتنفيذ برامج جدية لتكوين القضاة

[1] يونس عرب، مقال بعنوان جرائم الكومبيوتر والانترنت، مرجع سابق، ص65.

[2] – نهلا عبد المومن، المرجع السابق، ص 52.

[3] – يونس عرب، مقال بعنوان جرائم الكومبيوتر والانترنت، المرجع السابق، ص65.

وتدريبهم من الناحية التقنية والمصرفية، وضرورة اهتمام الباحثين الحقوقيين المحامين والمصرفيين وجهات التشريع بالجرائم الماسة بوسائل الدفع الإلكتروني.

لعل هذه الصعوبة هي المشكل الرئيسي في مواجهة الأفعال غير المشروعة التي تتم بوسائل الدفع الإلكتروني فالنصوص الجزائية التقليدية المتعلقة بجرائم الأموال ونصوص المعالجة الآلية للمعطيات الورد ضمن قانون العقوبات، الجرائم المنصوص عليها في قانون النقد والقرض، جرائم الصرف، جرائم تبيض الأموال لا تكفي لمواجهة هذه الأفعال وزجرها خاصة لأن هذه النصوص وضعت لحماية الأشياء المادية مما يتعذر معه مواجهة صور التعدي المرتبطة بوسائل الدفع الإلكتروني(بطبيعتها غير المادية) هذا من جهة، ومن جهة أخرى إن تطبيق مثل هذه النصوص يتعارض مع الجريمة المعلوماتية التي تقع على الحاسب الآلي[1] وبالتالي نلاحظ عدم كفاية النصوص الحالية لمواجهة هذا النوع الجديد من الجرائم فهل يترك الفاعل يفلت دون عقاب أمام هذا الفراغ التشريعي، أم أننا سنسمح للقضاء بالتدخل لسد هذا النقص التشريعي بما ينطوي عليه ذلك من انتهاك لمبدأ الشرعية الجنائية أم على المشرع أن يتدخل لمراجعة النصوص القائمة[2] حتى تصبح كفيلة بحماية وسائل الدفع الإلكتروني وكذا ترتيب المسؤولية الجزائية عن استخدامها.

[1]-معادي أسعد محمد صوالحة، المرجع السابق، ص 253.

[2]-جميل عبد الباقي الصغير، المرجع السابق، مصر، ص12.

يتوجب على المشرع الجزائري إخضاع الجرائم المتصلة بوسائل الدفع الإلكتروني بنصوص مباشرة للعقاب[1].

خشية أن يفلت الجناة من أفعال تتسم بالخطورة من حيث اعتدائها على الذمة المالية للأفراد وخسائر اقتصادية كبيرة للمصارف ومساس باقتصاد الدولة ككل مما ينجر عنه فقدان الثقة بالمصارف وبالدولة.

نلاحظ أن مختلف التشريعات اختارت إضافة نصوص خاصة إلى قانون العقوبات ولم تختر طريقة سن تشريع خاص، كما قامت بالنص على مساواة الأموال المنقولة المادية بغير المادية لأغراض انطباق النصوص المتعلقة بالجرائم الواقعة على الأموال إلا أن هذا غير ممكن لوجود فرق بين جرائم المعلوماتية المتعلقة بوسائل الدفع الإلكتروني من حيث مبناها وطبيعة سلوكياتها عن الجرائم التقليدية وهذا ليس فقط من ناحية محل الجريمة.

الفرع الثاني

إشكالية تكييف الركن الشرعي لإساءة استخدام وسائل الدفع الإلكتروني

إن تجريم اساءة استخدام بطاقة الائتمان الإلكترونية الملغاة قد جاء النص عليه في بعض القوانين صراحة بنصوص مستقلة (خاصة)[2]، وهذا لأن النصوص الخاصة بجرائم الأموال

---

[1]- يلاحظ في التشريع الجزائري أن بطاقة الدفع من وسائل الدفع الإلكتروني الأكثر انتشارا وبالرغم من حاجة هذه البطاقة إلى تدخل سريع من المشرع الجزائري بوضع نصوص جزائية توفر الحماية الكاملة لها ولأطرافها إلا أنه حتى الآن لم يحدث مثل هذا التدخل ولا يوجد تشريع خاص لحماية هذه الوسيلة من وسائل الدفع الإلكتروني.

[2]- حسن حماد حميد، جاسم خريبط خلف، اساءة استخدام بطاقة الائتمان الإلكترونية الملغاة، جامعة بابل للعلوم الانسانية، المجلد 18، العدد الثاني، 2010، ص 599.

التقليدية تبقى قاصرة عن استيعاب هذا الفعل مما يؤكد وجود فراغ تشريعي نتيجة لحداثة وسائل الدفع الإلكتروني، وجاءت بعض التشريعات الأجنبية بنصوص خاصة وواضحة تتناول تجريم إساءة استخدام بطاقة الائتمان وأبرز هذه التشريعات هو التشريع الفيديرالي الصادر عام 1984 في الولايات المتحدة الأمريكية[1]، وفي سويسرا كذلك جرم قانون العقوبات منذ عام 1995 الاستخدام غير المشروع لبطاقات الائتمان من قبل الحامل الشرعي لها اذ تقض المادة 148 من هذا القانون بمعاقبة كل من يستخدم بطاقة ائتمانية أو أي وسيلة أخرى للوفاء من أجل الحصول على أي خدمة ممكن أن تقدمها البطاقة اضرارا بالجهة المانحة للبطاقة خلافا للاتفاق المبرم بين الطرفين، وبذلك نرى أن التشريع السويسري قد جاء بنص خاص يدخل هذا الفعل ضمن قانون العقوبات إلا أنه لم يدخل الفعل تحت نطاق جرائم الأموال التقليدية (السرقة أو الاحتيال أو خيانة الأمانة)[2]، وهذا الموقف للمشرع السويسري أفرد جريمة خاصة لأنه رأى أن طبيعتها مختلفة عن كل جرائم الأموال التقليدية.

[1]- الذي تناول جريمة اساءة استخدام بطاقة الائتمان الإلكترونية (الاستخدام غير المشروع)، إذ نص في المادة 1029/أ من الباب الثامن عشر على تجريم الاستعمال التعسفي لوسائل الولوج أو السداد للبطاقات والأرقام السرية وكل ما يمكن استخدامه بصورة مفردة أو مترابطة من أجل الحصول على أموال أو بضائع أو خدمات أو أي شيء أخر له قيمة ويشمل إساءة استخدام البطاقة المسروقة أو المفقودة أو المنتهية الصلاحية وغيرها كما أنه يشمل تجريم إساءة استخدام بطاقة الائتمان الإلكترونية الملغاة، ومنه فإن المشرع الأمريكي قد جرم جميع الأفعال المتعلقة ببطاقة الائتمان الإلكترونية والتي يمكن عدها غير مشروعة.

[2]- حسن حماد حميد، جاسم خريبط خلف، المرجع السابق، ص 599، 600.

المشرع الفرنسي ومن خلال القانون رقم 1382/91 المتعلق بتأمين الشيكات وبطاقات الدفع[1] المكمل للمرسوم الصادر في 30 أكتوبر 1935 المتعلق بالشيك ومن خلال المادة 11 المعدلة للمادة 67 من قانون 30 أكتوبر أورد نصوص خاصة ببطاقة الدفع وأضاف المواد 2/1،67/67 ونص على جريمة التزوير والتقليد واستعمال بطاقة مزورة أو مقلدة وجريمة قبول الوفاء بواسطة بطاقة مزورة أو مقلدة وبالتالي فالمشرع الفرنسي ومن خلال هذه المواد لم يتطرق إلى باقي الحالات المتعلقة بإساءة استخدام البطاقة من قبل حاملها وبالنتيجة لم يتطرق إلى الحالات التي تخص وسائل الدفع عامة أما بالنسبة للأمر 866/2009 فترك ذلك لتطبيق المادة 313 /1 من قانون العقوبات الفرنسي والتي تتعلق بالاحتيال التي أضافت عبارة مالا ما « ou un bien quelconque »[2]، إلا أنها تشترط أن يتم الاحتيال على شخص ما وهذا غير متوفر في حالة السحب من جهاز الصراف الآلي.

[1]- voir l'article 11 de la loi n 91-1382 du décembre 1991 relative à la sécurité des chèques et des cartes de paiement, J.O.N °1du 01/01/1992.

[2] - l'article 313 /1 de code pénal français « L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs **ou un bien quelconque**, à fournir un service ou à consentir un acte opérant obligation ou décharge. … »

التشريعات العربية ومنها تشريع سلطنة عمان المتعلق بجرائم الحاسب الآلي[1] حيث تضمنت المادة 276 مكرر 4 منه جرائم خاصة بالبطاقات " يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تتجاوز خمسمائة ريال كل من:

1- استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له.

2- استخدم البطاقة بعد انتهاء صلاحيتها أو الغائها وهو عالم بذلك.

3- استعمل بطاقة الغير بدون علمه ".

وبذلك فإن هذا التشريع يعد من التشريعات السباقة في مكافحة الجرائم المعلوماتية (الإلكترونية) إذ أن النصوص جاءت صريحة بتجريم الأفعال محل البحث وغيرها من الأفعال وفق قوانين ونصوص خاصة وبذلك فإن القضاء في سلطنة عمان لن يكون مضطرا لتطبيق النصوص التقليدية[2]، إلا أنه يؤخذ على المشرع في سلطنة عمان أنه تقيد باصطلاحات مقيدة (البطاقة، بطاقة الدفع) في حين كان يمكنه أن يكون أكثر اتساعا وشمولا لتشمل صور الاعتداء المجرمة كل وسائل الدفع الإلكترونية الموجدة حاليا والمستقبلية، وبالتالي نحن في الجزائر سنواجه فراغا تشريعيا بخصوص هذه المسألة مما يحتم على القاضي تطويع النصوص التقليدية لجرائم الأموال لملاحقة حالات إساءة استخدام وسائل الدفع الإلكتروني.

---

[1]- تشريع سلطنة عمان متوفر على الموقع: https://www.rop.gov.om/pdfs/roplaws/ROPRULE-1.pdf

[2]- حسن حماد حميد، جاسم خريبط خلف، المرجع السابق، ص 596.

المطلب الثاني

المسؤولية الجزائية لحامل وسيلة الدفع الإلكتروني

تشجع وسائل الدفع الإلكتروني الحامل الشرعي نفسه على استعمالها بطريقة غير شرعية للتهرب من دفع المستحقات والاستفادة من المزايا التي توفرها هذه الوسائل مما يعرضه للمساءلة الجزائية عند استعماله لطرق معاقب عليها قانونا.

تقديم الحامل بطاقته إلى التاجر مع علمه بعدم وجود رصيد فيها يعد وسيلة من وسائل الاحتيال من شأنها الاقناع بوجود ائتمان وهمي وهو الذي تقوم به جريمة الاحتيال، غير أن هذا منتقد لأن القاعدة أنه لا يجوز القياس في مجال التجريم والعقاب، كما أن مسألة استخلاص القصد الجنائي لحظة تقديم الحامل للبطاقة يصعب اثباته، وعليه سنتناول المسؤولية الجزائية عن الحصول على وسيلة دفع إلكتروني بطريقة غير مشروعة (الفرع الأول)، واساءة استخدام وسيلة الدفع الإلكتروني خلال فترة صلاحيتها (الفرع الثاني)، وإساءة استخدام وسيلة دفع إلكتروني ملغاة أو منتهية الصلاحية (الفرع الثالث)، وأخيرا جريمة القبول لوسائل الدفع الإلكتروني المزورة والمقلدة (الفرع الرابع).

الفرع الأول

المسؤولية الجزائية عن الحصول على وسيلة دفع إلكتروني بطريقة غير مشروعة

الأصل أن يحصل الزبون على وسيلة الدفع الإلكتروني بطريقة قانونية من الجهة المصدرة إلا أن بعض الزبائن قد يستغلون هذه الوضعية لارتكاب جريمة الحصول على وسيلة دفع

إلكتروني بطريقة غير مشروعة ونبين أولا (الركن المادي)، وثانيا (إشكالية التكييف لهذه الجريمة في القانون الجزائري).

أولا/الركن المادي

ليحصل الزبون على وسيلة دفع إلكتروني عليه تقديم طلب إلى الجهة المصدرة بإبداء رغبته في الحصول على وسيلة الدفع الإلكتروني، وجرت العادة على أن توفر المصارف لزبائنها نماذج الطلبات المعدة مسبقا والتي يقوم الزبون بملء بياناتها والتي يفترض فيها أنها صحيحة، وأن المستندات المطلوبة المرفقة للحصول على وسيلة الدفع الإلكتروني صحيحة، فاذا قدم الطالب بياناته وتضمنت أسماء منتحلة وعناوين وهمية وضمانات غير حقيقية وعلى ضوئها أصدرت الجهة المختصة له وسيلة دفع فإنه ومما لاشك فيه يكون قد خدع وغش الجهة المصدرة المختصة بإصدار وسيلة الدفع فضلا عما ستتحمله من خسائر مادية ودون أن تتمكن فيما بعد من العثور عليه نتيجة المستندات المزورة، هذا ما دفع بمؤسسة فيزا كارد إلى القول بأن الطلبات المزورة للحصول على البطاقات هي الصدع والثغرة الكبيرة التي تعاني منها هذه الصناعة[1].

ثانيا/ إشكالية التكييف لهذه الجريمة في القانون الجزائري

[1]– ومثال ذلك ضبط تشكيل عصابي متخصص في الاحتيال في البنوك والاستيلاء على مبالغ مالية كبيرة لاستصدار بطاقات ائتمان صحيحة بموجب مستندات مزورة واعترفوا باتباعهم هذا النشاط منذ فترة واستخدامهم للبطاقات في الحصول على السلع والنقود دون سداد تلك المبالغ، ويعتبر هذا الأسلوب من الاعتداءات هو الشائع لدى حاملي البطاقة فعندما يحصل الزبون عليها يقوم باستعمالها ويمتنع عن الدفع فيرجع البنك فلا يجده، أنظر معادي أسعد محمد صوالحة، المرجع السابق، ص262.

هنا يثار التساؤل عن مدى إمكانية مساءلة الفاعل جزائيا، وما نوع الجريمة التي سيسأل عنها؟ فالأمر سيختلف إذا ادعى شخص بأن راتبه لا يقل عن مبلغ معين، وبين تقديم مستندات تثبت ذلك ففي الحالة الأولى نكون أمام احتيال وفي الثانية نكون أمام جريمة استعمال مستندات مزورة، ولكن البعض يرى مساءلة الحامل على أساس جريمة الاحتيال طبقا للمادة 372 /1من قانون العقوبات الجزائري حيث يحتج بأن الزبون الذي يقوم بالحصول على وسيلة دفع إلكتروني أيا كان نوعها غشا وخداعا منه باستخدامه لمستندات مخالفة للحقيقة والتي من شأنها إحداث الأمل بقدرته على تسديد قيمة المشتريات والعمليات التي سيقوم بها مستعملا تلك الوسيلة في الدفع[1].

الفرع الثاني

اساءة استخدام وسيلة الدفع الإلكتروني خلال فترة صلاحيتها

يفرق الفقه بين حالتين الأولى حالة استعمال البطاقة في السحب، أما الثانية فهي حالة استعمالها في الوفاء.

أولا/ المسؤولية الجزائية في حالة السحب عند عدم وجود الرصيد أو عدم كفايته

1-صور الركن المادي: تقوم البطاقات الإلكترونية للدفع بوظيفة السحب أيضا حيث تسمح للحامل بالسحب من الموزعات الآلية بمجرد ادخال الرقم السري في حدود القيمة المسموح بها من قبل الجهة المصدرة للبطاقة، إلا أن الحامل الشرعي لهذه البطاقة قد يتصرف بسوء نية

[1]- حوالف عبد الصمد، المرجع السابق، ص 536.

فيعمل على استخدام البطاقة لدى الموزعات الآلية سواء بالطريقة المعتادة أو بالتلاعب في معطيات الحاسوب ولكن هناك نوع آخر من الأساليب غير المشروعة التي قد يقوم بها حاملي البطاقات الملغاة، ولرغبتهم في الحصول على بطاقة ائتمانية جديدة عبر العصابات الاجرامية المتخصصة في ذلك والتي تطلق على نفسها عيادات الإصلاح الائتماني (Crédit Repair Clinics) بسبب امتناع الجهات المصدرة عن منح مثل هذه البطاقات إلى طالبيها نظرا لتاريخهم الائتماني السيء والتي تحصل على مبالغ تصل إلى ألفي دولار حتى تمكن طالب البطاقة من استخرج بطاقة ائتمان دون اعتراض البنك المصدر بعد تغيير المستندات التي تدل على سوء استخدامه للبطاقة.

2-تكييف فرضيات الركن المادي بين الإخلال بالشروط العقدية و المسؤولية الجزائية:

يجب التفرقة بين فرضيتين كذلك الأولى أن يتجاوز الحامل القيمة المسموح له بسحبها (لا تتعلق بالرصيد)، والثانية أن يتم السحب رغم انعدام الرصيد أو عدم كفايته (تتعلق بالرصيد)، إلا أنه وكما أسلفنا ولتفادي هذا الجدل الفقهي حول التكيفات فإنا نرى ضرورة تدخل المشرع بالنص الخاص للفصل في هذه المسألة خاصة مع تعدد وتنوع وسائل الدفع.

بالنسبة **للفرضية الأولى** يجمع الفقه على أنها تخضع للشروط التعاقدية، وقد حدد في بطاقة الدفع ما بين البنوك لبريد الجزائر اجراءات السحب من الموزعات الآلية، ويعتبر هذا اخلالا بالالتزام العقدي الذي يربطه بالجهة المصدرة، خاصة إذا لم يقم بتصحيح وضعيته من خلال

تغطية قيمة السحوبات المتجاوز فيها[1]، وبالتالي فالثابت في هذه الحالة أنها لا علاقة لها بانعدام الرصيد أو عدم كفايته إنما جرت العادة على أن تحدد البنوك حسب نوع البطاقة أو حسب شخص الزبون شروط العقد ولتفادي خطر السيولة[2] تحدد البنوك حدا معينا للسحب سواء يوميا أو أسبوعيا.

أما بالنسبة **للفرضية الثانية** والمتعلقة بالرصيد وتتمثل في حالة سحب مبالغ نقدية تتجاوز الرصيد الموجود بالفعل، أو حالة السحب مع انعدام الرصيد وهي حالات تشبه حالات المسؤولية الجزائية عن اصدار شيك بدون رصيد في حالة انعدام الرصيد أو عدم كفايته إلا أن حالة انعدام الرصيد بالنسبة لبطاقة الدفع الإلكترونية لا تشكل جريمة اصدار شيك بدون رصيد، حيث يجمع الفقه على أن هذه الحالة تثور بصددها المسؤولية الجزائية غير أن الآراء انقسمت حول الجريمة التي يمكن على أساسها مساءلة الحامل وحاولوا تطويع نصوص قانون العقوبات المتعلقة بالأموال فهناك من يرى أن هذه الحالة تشكل جريمة خيانة الأمانة، في حين هناك من يرى أنها جريمة سرقة وآخرون يرونها تشكل جريمة نصب واحتيال.

[1]- حوالف عبد الصمد، المرجع السابق، ص331.

[2]- خطر السيولة: يوجب على المصارف تطبيق قاعدة السيولة والتي تعني وجوب الاحتفاظ بمقدار من الأموال السائلة أو التي يمكن تحويلها إلى سيولة آنية لمجابهة المسحوبات.

الفرع الثالث

إساءة استخدام وسيلة دفع إلكتروني ملغاة أو منتهية الصلاحية

البطاقة المنتهية الصلاحية (périmée) غالبا ما يكون تاريخ الصلاحية مدون على البطاقة بأرقام بارزة وبانتهاء فترة الصلاحية يجب على الحامل تجديدها، وبالتالي رد البطاقة المنتهية الصلاحية وتسليمها إلى البنك المصدر الذي يسلم له بدوره مكانها بطاقة جديدة، أما البطاقة الملغاة (Annulée) فهذه البطاقة ألغيت لإخلال الحامل بالتزاماته التعاقدية مع البنك وبالتالي يقوم هذا الأخير بفسخ العقد وبالنتيجة إلغاء البطاقة التعاقدية.

أولا/صور الركن المادي لإساءة استخدام وسيلة دفع منتهية الصلاحية

1-اساءة استعمال بطاقة منتهية الصلاحية في السحب: إن استخدام البطاقة الملغاة في سحب النقود من أجهزة الصراف الآلي يعد مثلما يقول البعض أمر غير متصور وبالغ الصعوبة في ظل الاحتياطات التي تضعها البنوك على الأجهزة التابعة لها لأن هذه الأجهزة عادة ما ترفض القيام بعملية السحب أو تقوم بابتلاع البطاقة، إذ أن وسائل الرقابة على صلاحية بطاقات السحب الإلكترونية جعلت الاستعمال السيء(الاستخدام غير المشروع) بمقابل جهاز الصراف الآلي في حالة السحب يكون مرتكزا على السحب في حالة السحب المتجاوز للرصيد ولا يتضمن استعمال البطاقة الملغاة أو المنتهية الصلاحية إذ أن هذه

البطاقات يتم سحبها بطريقة آلية عن طريق الأجهزة التي تتم برمجتها من أجل القيام بهذا العمل بعد أن تزود بالذاكرة اللازمة لذلك[1].

2-إساءة استخدام وسيلة الدفع الإلكتروني الملغاة: الأصل أن البطاقة في هذه الحالة محل إلغاء وانتهت صلاحيتها نتيجة العقوبة المفروضة على الحامل من طرف البنك إلا أن الحامل وعوض رد البطاقة للمصدر يقوم باستخدامها مرة أخرى ويمكن له استعمالها إما في الوفاء أو في عملية السحب.

الاستخدام بعد الالغاء يؤدي إلى الزام البنك بدفع القيمة للتاجر ونميز بين حالتين:

الأولى **الامتناع عن رد البطاقة رغم طلبها من البنك المصدر:** فإن الغاء البطاقة من البنك المصدر لها وقيام الحامل باستخدامها يمثل جريمة خيانة الأمانة لأن التعاقد بينهما يشكل خيانة الأمانة.

الثانية **الاستخدام للبطاقة الملغاة في الوفاء:** يشكل جريمة الاحتيال.

الفرع الرابع

جريمة القبول لوسائل الدفع الإلكتروني المزورة والمقلدة

نصت المادة 18 فقرة 04 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على هذه الجريمة بقولها " كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك"، وتتشابه هذه الجريمة مع جريمة قبول شيك مزور أو جريمة قبول شيك بدون رصيد وعليه سنتناول

[1]- حسن حماد حميد، جاسم خريبط خلف، المرجع السابق، 559.

شمولية الركن الشرعي لكل وسائل الدفع الإلكتروني في القانون الفرنسي (أولا) صور الركن المادي (ثانيا)، الركن المعنوي (ثالثا).

أولا/شمولية الركن الشرعي لكل وسائل الدفع الإلكتروني في القانون الفرنسي

كان المشرع الفرنسي ينص في المادة 67 من القانون المتعلق بأمن الشيكات وبطاقات الدفع والسحب "كل من قبل الدفع عن طريق بطاقة الدفع مقلدة أو مزورة وهو يعلم بذلك "كما نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في الفقرة الرابعة من المادة الثامنة عشر على مايلي " كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك ".

إلا أن المشرع الفرنسي من خلال تعديله لقانون النقد والمال استبدل مصطلح بطاقة الدفع المقلدة أو المزورة بمصطلح وسيلة دفع من خلال نص المادة3-3-L163

« Est puni d'un emprisonnement de sept ans et d'une amende de 750 000 euros le fait pour toute personne :…

3-D'accepter, en connaissance de cause, de recevoir un paiement au moyen d'un chèque ou **d'un autre instrument** mentionné à l'article L 133-4contrefaisant ou falsifié ».

تناول المشرع المغربي نفس الجريمة في الفقرة الثالثة من المادة331 من مدونة التجارة "بقوله كل من قبل عن علم أداء بواسطة وسيلة أداء مزيفة أو مزورة ".

رغم أن المشرع الجزائري عدل القانون التجاري إلا أنه لم يدرج هذه الجريمة وهذا ربما حتى لا نصطدم بمبدأ الشرعية على أساس محدودية وسائل الدفع الإلكتروني الواردة بالقانون

التجاري الجزائري وتفضيل الأخذ بآخر تعديل للقانون الفرنسي، وحتى لا يولد النص ميتا لأنه تناول بالنص في القانون التجاري الجزائري بعض الوسائل فقط.

ثانيا/صور الركن المادي

هناك من أثار التساؤل حول جدوى هذا النص وبتعبير اخر الم تكن القواعد العامة في المساهمة الجنائية تؤدي الى نفس النتيجة ؟

قبل الاجابة على هذا التساؤل يتعين التنويه إلى أن المجني عليه في هذه الحالة لن يكون التاجر فقط وإنما البنك المسحوب عليه وربما صاحب الحساب الذي قلد بطاقة صاحبه ؟

للإجابة على هذا التساؤل يتعين التفرقة بين ثلاث فروض[1]؟

الفرض الأول: أن يقوم حامل البطاقة المزورة بتقديمها إلى التاجر ويفصح له عن طبيعتها ويقوم هذا الأخير بالاتفاق مع حامل البطاقة بقبولها ويتم الوفاء بواسطتها؟ وفي هذا الفرض لا يسأل حامل البطاقة عن جريمة الاستعمال لأنه لم يحتج بأن هذه البطاقة صحيحة، وإنما يسأل كشريك للتاجر الذي يحتج بها على البنك بأنها بطاقة صحيحة ولا يغير من ذلك التكييف أن التاجر سوف يحتج على البنك بصورة من البطاقة المزورة.

الفرض الثاني: أن يقوم حامل البطاقة المزورة بتقديمها للتاجر على أنها صحيحة ويعلم هذا الأخير أنها مزورة ولم يفصح لحاملها عن ذلك وقبل الوفاء بواسطتها، في هذا الفرض يعد

[1]- ضياء علي أحمد نعمان، النقود الإلكترونية أداة وفاء في التجارة الإلكترونية الأحكام والآثار، التجارة الالكترونية أية حماية، أشغال الندوة الوطنية التي نظمها مختبر الدراسات الجنائية وهيئة المحامين بمراكش أيام 29،30، ماي 2009، سلسلة الندوات والأيام الدراسية، الطبعة الأولى، 2010، المطبعة والوراقة الوطنية مراكش ،المغرب، ص211.

حامل البطاقة مرتكبا لجريمة استعمال محرر مزور ويعد التاجر كذلك مرتكبا لذات الجريمة اذ أنه سوف يحتج بصورة هذه البطاقة لدى البنك لاستيفاء دينه وهو يعلم أن البطاقة مزورة.

الفرض الثالث: أن يكون حامل البطاقة (وهو فرض نادر الوقوع) غير عالم بأن البطاقة مزورة ويقوم بتقديمها للتاجر ويعلم هذا الأخير بتزويرها وعلى الرغم من ذلك يقوم بقبولها وفي هذا الفرض لا يسأل حامل البطاقة عن جريمة الاستعمال لانتفاء القصد الجنائي ولكن يسأل التاجر عن جريمة الاستعمال إذا استخدمها واحتج بها في مواجهة البنك.

وبما أن هذا الفرض الثالث نادر الوقوع إلا أنه حتى تقع هذه الجريمة لابد أن تكون مصحوبة بوقوع عدة جرائم أخرى منها جريمة التزوير أو التقليد لوسائل الدفع الإلكتروني جريمة الاستعمال لوسيلة دفع إلكتروني مزورة أو مقلدة وبالتالي وقوع هذه الجريمة في الغالب تكون في صورة اتفاق جنائي للجرائم السابقة الذكر وخصها المشرع بالنص حتى لا يتذرع التاجر أو مقدم الخدمة للإفلات من العقاب الجنائي في الجرائم السابقة، فالأرجح أنه تنشأ عن جريمة استعمال بطاقات دفع مزورة أو مقلدة جريمة قبول لبطاقات دفع مزورة أو مقلدة وأن التاجر الذي يقبلها شريكا له في جريمة استعمال محرر مزور، وبالتالي هذه الجريمة تخص الفرض الذي يكون فيه التاجر متواطئا مع مستعمل البطاقة المزورة.

ثالثا/الركن المعنوي

هذه الجريمة من الجرائم العمدية فحسب نص الفقرة الرابعة من المادة الثامنة عشر من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات "كل من قبل أداة من أدوات الدفع المزورة

مع العلم بذلك "، ولتحقق هذه الجريمة يشترط العلم بتقديم وسيلة دفع إلكتروني مقلدة أو مزورة وقبولها وهذا حسب نص المادة L163-3-3 من قانون النقد والمال الفرنسي

« **D'accepter, en connaissance de cause, de recevoir un paiement** au moyen d'un chèque ou d'un autre instrument mentionné à l'article L 133-4**contrefaisant ou falsifié** ».

والذي يعد حسب رأينا أشمل من نص المادة الثامنة عشر من الاتفاقية العربية الذي اقتصر على مصطلح وسيلة دفع المزورة فقط وهو ما يحب على المشرع الجزائري الانتباه له لأننا في انتظار ادراجها من طرفه بنص تشريعي صريح.

المبحث الثالث

المسؤولية الجزائية عن إفشاء السر المصرفي لوسائل الدفع الإلكتروني

تزودت الجزائر على غرار العديد من البلدان بقانون يهدف إلى تأمين الحياة الخاصة للمواطن في جميع الميادين اليومية من تطور المعلوماتية وهو القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والذي حدد المبادئ الواجب اتباعها أثناء جمع ومعالجة وحفظ البيانات الشخصية وقواعد استعمالها، فخصوصية البيانات الشخصية هي مطالبة الأشخاص بأن لا تكون البيانات الخاصة بهم متوفرة تلقائيا لغيرهم من الأفراد أو المنظمات، حتى في حالة أن تكون البيانات مملوكة من

طرف آخر، فلهم القدرة على ممارسة قدر كبير من السيطرة أو التحكم بتلك البيانات وطريقة استخدامها وهذا ما يعرف "بخصوصية المعلومات أو خصوصية البيانات"[1].

نتيجة لطبيعة مهامه يضطر المصرفي إلى تجميع وحفظ المعلومات عن زبائنه على شكل ملفات ظلت هذه الملفات يدوية حتى بضع سنوات خلت حيث بدأت تمكنن يوما بعد يوم وهذا الأمر يزيد من مخاطر الاعتداء على الحريات الشخصية وعلى حياة الزبائن الخاصة فهي أداة فعالة في أيدي المصارف بشكل خاص والدولة بشكل عام لمراقبة نشاطات وتحريات الأشخاص المسجلين[2]، وفعالية مكافحة الغش تمر بالضرورة عبر تشكيل ملفات تحتوي على المعطيات الشخصية والتي توجد بهدف قمع الغش ومكافحته[3].

أنظمة الدفع الإلكتروني بدورها تستلزم التجميع والتحويل ومعالجة المعطيات شديدة الحساسية المتعلقة بحاملي وسائل الدفع[4]، وتعتبر إشكالية المحافظة على السرية المصرفية والمعلومات في المجتمع المعلوماتي من أهم القضايا التي توليها البنوك والزبائن أهمية كبرى لأنه من الواجب على البنوك المحافظة على هذه السرية والأمان للبيانات والمعلومات التي يرسلها

---

[1]-منى تركي، جان سيريل، الخصوصية المعلوماتية و أهميتها ومخاطر التقنية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013.

[2]-شايب عينو الهادي، بعض الجوانب القانونية لبطاقة الذاكرة والتبادل غير المستندي للشيكات والكمبيالة الإلكترونية، النص الأصلي باللغة الفرنسية قامت ماجدة القبيسي الجامعة اللبنانية بنقله إلى العربية، الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية،1999، الطبعة الثانية، لبنان، ص 183.

[3]-réponse de la fédération bancaire française à la consultation de la commission européenne pour un « nouveau cadre juridique pour les paiements dans le marché intérieur », fédération bancaire francaise,13 février2004,fed-bancaire-fr.

[4]-Henri delahaie et André grissonnanche, les nouveaux moyens de paiement ont –ils besoin a un cadre juridique spécifique l'expérience française, les cahiers de droit, vol 24, n°2, 1983, P279-304, disponible sur http://id.erudit.org, le 23/12/2016.

الزبون الإلكتروني للبنك من خلال العديد من التطبيقات التكنولوجية مثل التشفير رسائل البريد الإلكتروني بحيث لا يمكن قراءتها إلا بعد فك الشفرة وحلها بواسطة البنك[1] وهنا لا يستطيع أي شخص آخر قراءة الرسالة، لهذا سنتناول من خلال المطلب الأول(علاقة وسائل الدفع الإلكتروني بالسرية المصرفية) وفي المطلب الثاني(مفهوم السر المصرفي المعالج إلكترونيا).

المطلب الأول

علاقة وسائل الدفع الإلكتروني بالسرية المصرفية

إن الحاسب الآلي الذي يتم من خلاله استعمال وسائل الدفع الإلكتروني في المعاملات المصرفية الإلكترونية يمكن أن يمثل خطرا على الحياة الخاصة لمستعملي هذه الوسائل وعلى السرية المصرفية على وجه الخصوص، ومظاهر هذا الخطر تظهر في أكثر من جانب من أبرزها أن المعلومات الخاصة بالزبائن وبمجرد أن تنتشر فإن تبادلها يتم بسرعة مذهلة ولجهات غير محدودة وباتباع إجراءات إلكترونية بسيطة للغاية وتزداد خطورة هذا النشر إذا ما احتوى على معلومات غير صحيحة أو دقيقة بخصوص الزبون الذي تم نشر

[1]- هشام فتحي سيد حسن، وسائل حماية المستهلك الإلكتروني بين الشريعة والقانون، بحث مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات ص1205.

الاستئثار أو الخصوصية في مجال وسائل الدفع الإلكتروني يعني أن الدخول إلى المعلومات التي يتم عن طريقها التعامل بها أو الولوج إليها يكون مخصصا لمجموعة من الأفراد دون غيرهم وقد يكون متاحا لشخص بعينه بصفته صاحب السلطة للتصرف في المعلومة كأن يكون من العاملين بالبنك، أو من الحاملين لوسيلة الدفع الإلكتروني أومن التجار الذين يقبلون التعامل بوسائل الدفع الإلكتروني، كما أن سهر البنوك على تقديم وسائل الدفع الإلكتروني قد يتهدد بسبب احتمال إطلاع مقدمي الخدمات الإلكترونية[1] أثناء قيامهم بمهامهم على البيانات المصرفية، فمقدم خدمة الدخول للبنك على دراية بطبيعة الخدمات المصرفية[2].

وللخصوصية ثلاثة عناصر هي السرية والعزلة والتخفي ومنه نستنتج أن السرية تعتبر أحد العناصر المكونة للخصوصية، إلا أن عمليات الدفع عبر الانترنت تتطلب معلومات تفصيلية يغيب فيها القدرة على التخفي خلافا للعالم الواقعي.

لا يمكننا الحديث عن التعامل بوسائل الدفع الإلكتروني دون الحديث عن السرية عامة والتي تعتبر عنصر من عناصر الخصوصية، ولا دون السرية المصرفية خاصة والتي تعتبر التزام على عاتق مصدري وسائل الدفع الإلكتروني.

---

[1]- لا يوجد في الجزائر تنظيم قانوني خاص بمقدمي الخدمات الإلكترونية على شبكة الانترنت ماعدا القانون المنظم لخدمات المصادقة الإلكترونية.

[2]- علاء التميمي، التنظيم القانوني للبنك على شبكة الانترنت، دار الجامعة الجديدة للنشر، مصر، 2012، ص145.

ثانيا/ وسائل الدفع الإلكتروني وتفاقم مخاطر الخصوصية

وسائل الدفع الإلكتروني تعتبر أكثر عرضة لاختراق الخصوصية أو السرية عنها في وسائل الدفع الأخرى، والسبب في ذلك يعود إلى السهولة النسبية في الحصول على البيانات الإلكترونية في حال تعرضها للاختراق، ومع ازدياد التعامل بالنقود الإلكترونية فإن المستعملين سيزداد قلقهم بخصوص سرية معلوماتهم المتعلقة بالصفقات التي يجرونها[1]، لأن حماية خصوصية التعاملات المالية في بيئة الانترنت يعد من أهم ضمانات وجود الدفع الإلكتروني وتطوره، وكما قيل فإن نظام الدفع المالي على الأنترنت بدون نظام حماية للخصوصية سينقلنا من عالم الدفع النقدي المستتر إلى عالم مليء بوسائل الكشف والتعريف وتتزايد فيه قدرة تتبع الأشخاص ومشترياتهم وهو ما يتعارض مع واجب السرية المصرفية الملزم للبنوك اتجاه زبائنها، والذي يهمنا في هذه المسألة هو بيان كيف تكون وسائل الدفع الإلكتروني خطر في حد ذاته على أسرار الزبائن وخصوصياتهم.

الزيادة في عدد الأطراف المتدخلة في عملية الدفع بالوسائل الإلكترونية بما فيها المصدرين والعاملين لديهم، والموزعين والتقنيين، والعاملين لدى التجار، والحاملين لهذه الوسائل يمكن أن تزيد من عدد الأشخاص الذين يسمح لهم بالاطلاع على المعلومات الخاصة بالزبون، كذلك الاعتداءات على الخصوصية سوف تزداد كلما ازدادت استعمالات النقود الإلكترونية،

[1]- طارق محمد حمزة، المرجع السابق، ص34.

للإمداد بالخدمات البنكية تتعرض لمخاطر عدة سواء تشغيلية أو متعلقة بالسمعة أو قانونية لها علاقة باستخدام الشبكات المفتوحة[1].

يعتبر غالبية المصرفيين أن المخاطر الأمنية هي أحد المهددات الرئيسية في مجال المعلوماتية وتتسبب الوسائل الإلكترونية في خلق قضايا أمنية للبنوك فيما يتعلق بسرية وسلامة المعلومات والتحقق من هوية المستخدمين والتحكم في الدخول إلى الأنظمة والشبكات، وأصبحت البيانات الشخصية المسروقة تستعمل في الاحتيال وانتحال الهوية والغرض من وراء ذلك بالطبع مالي بحت حيث أن أكثر من 190 زبون بنك أوربي وجدوا أنفسهم أن حساباتهم قد أفرغت بما يعادل 500.000 يورو سنة 2014[2].

يمكن أن تهدد الحياة الخاصة للزبائن في ظل تزايد استعمال وسائل الدفع الإلكتروني ما يستلزم وضع قواعد خاصة للحماية لأن الاطلاع على المعلومات التي تحويها هذه الوسائل وتحليلها يمكن أن يعطي في النهاية فكرة عن الذمة المالية للشخص وهل هو في حالة يسر، أم أنه يواجه صعوبات وفي حالة توقف عن الدفع، كما لا تقتصر الخطورة على الحياة الخاصة للشخص في ما يمكن أن تحتويه من معلومات و امكانية نشرها إذا كانت معلومات صحيحة نتيجة تحليلها وتنسيقها، بل تظهر شدة الخطورة في حالة الخطأ أو التحوير للمعلومات التي تسجل على الشخص، فوجود خطأ عن الحياة والظروف المالية للشخص قد

[1]-Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit p48
[2]-Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit p48.

يؤدي إلى القضاء على المستقبل المالي له حيث توصد في وجهه أبواب المصارف وهيئات الائتمان دون أن يدري[1].

ثالثا/العلاقة الجدلية بين الحق في الخصوصية والمعلوماتية والسر المصرفي

السر المصرفي يعتبر من أحد مشتملات حق الخصوصية[2]، ونعود ونؤكد على حقيقة أن السماح بتخزين المعلومات المصرفية عن الزبون لا يعني أن هذه المعلومة قد انتقلت من دائرة الخصوصية إلى دائرة العلانية كما أن رضا الزبون بتجميع وتخزين بياناته لا يعني بحال حرية تداول ونقل المعلومات إلى الكافة[3] ويمكن اعتبار السر المصرفي من الحقوق المقدسة التي تعززت حمايتها باستعمال التكنولوجيا الحديثة، فهو من الحقوق التي لم تتأثر بالتكنولوجيا والمعلوماتية كما يمكن الجزم من جهة أخرى أن السر المصرفي من بين النواة الصلبة لحق الخصوصية الذي لا يمكن خرقه بالتقنيات الحديثة[4]، فالالتزام بالحفاظ على السر المصرفي لا يقف عند حد عدم الافشاء وإنما يمتد إلى ضرورة اتخاذ إجراءات الحيطة اللازمة لمنع تشويهها أو اتلافها أو تحويرها أو اطلاع أشخاص غير مأذون لهم عليها[5].

---

[1]- حسام الدين كامل الاهواني، المرجع السابق، ص53.

[2]- أوصديق فوزي، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الرابع، ص 1743.

[3]-عزيزة الشريف،، التوازن في المعادلة بين حق العميل في الخصوصية وحق البنك في مشروعية التعامل المالي، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الرابع، ص 1766.

[4]- أوصديق فوزي، المرجع السابق، ص1748.

[5]- عزيزة الشريف، المرجع السابق، ص1767.

الفرع الثاني

أنظمة بنك الجزائر وحماية الحق في الخصوصية

لأجل تحقيق أمن وسائل الدفع الإلكتروني استلزمت المادة 04 من النظام رقم 07/05 المتضمن أمن أنظمة الدفع أن يتضمن أمن أنظمة الدفع أمن البنية الأساسية لأنظمة الدفع، وكذا أمن وسائل الدفع بينما يسهر بنك الجزائر على الاشتغال الحسن لهذه الأنظمة وأمنها[1] كما يتأكد من توفير أمن وسائل الدفع من غير العملة النقدية وباحترام المعايير المطبقة في هذا المجال وإذا كانت وسائل الدفع لا تتوفر على الضمانات الأمنية الكافية يمكنه أن يطلب من الجهة المصدرة اتخاذ الإجراءات اللازمة لمعالجة الأمر، أو اتخاذ قرار توقيف ادخال وسيلة الدفع[2].

---

[1]-تنص المادة 04 من النظام 07/05 " يتضمن أمن أنظمة الدفع أمن البنية الأساسية لأنظمة الدفع وكذا أمن وسائل الدفع

تشمل البنية الاساسية لأنظمة الدفع مركبات الانظمة المركزية للإنتاج والنجدة ومركبات مختلف التجهيزات التقنية اي المكونات المادية والبرمجيات التي تم وضعها على مستوى المشاركين المعتمدين وكذا المصداقية العملية لخدمات البنية الاساسية التي تتوقف عليها هذه الأنظمة، لاسيما الاتصالات والطاقة الكهربائية .

تلقى مسؤولية وضع أجهزة أمن أنظمة الدفع على عاتق مسيريها والمشاركين في هذه الانظمة ، بينما يسهر بنك الجزائر على الاشتغال الحسن لهذه الانظمة وامنها".

[2]- المادة 12" يسهر بنك الجزائر على توفير الامن المادي والمنطقي للبنية الاساسية الخاصة بأنظمة الدفع كما يتأكد من توفير أمن وسائل الدفع من غير العملة النقدية وباحترام المعايير المطبقة في هذا المجال .

وفي حالة اذا ما اعتبر بنك الجزائر بأنه لا يتوفر في احدى وسائل الدفع على الضمانات الأمنية الكافية، يمكنه أن يطلب من الجهة التي تصدر اتخاذ اجراءات ملائمة لمعالجة الأمر ، وفي حالة عدم تطبيق هذه التوصيات يمكنه بعد استشارة السلطة المكلفة بالمراقبة اتخاذ قرار توقيف ادخال وسيلة الدفع المعنية في النظام .

يتعين على بنك الجزائر بصفة خاصة التأكد من أمن بطاقات الدفع ومتابعة اجراءات توفير شروط الأمن التي قامت بها الجهات التي تصدرها وكذا التجار ومتابعة احصاءات التدليس والتطورات في ميادين التكنولوجيا التي قد تؤثر على أمن بطاقات الدفع.

تضمنت المادة 05 من نفس النظام أن يشمل أمن البنية الأساسية لأنظمة الدفع، توفر الأنظمة، صحة المعطيات المتبادلة، رسم مخطط المعطيات المتبادلة، **السـريـة**[1]، قابلية المراجعة، و تعيين موظفين مؤهلين وأكفاء للقيام بعمليات الدفع، ويستوجب التعامل بوسائل الدفع الإلكتروني تقديمها في أنظمة الدفع وبالتالي على المشاركين في أنظمة الدفع احترام أنظمة بنك الجزائر المسيرة لأنظمة الدفع، واحترام الاتفاقيات المرتبطة بمختلف أنظمة الدفع، والتعليمات المتعلقة باستعمالها[2].

أخيرا يمكننا القول بأن الخصوصية في نطاق وسائل الدفع الإلكتروني تعني ارتباط البيانات والمعلومات بأطرافها (مصدر، حامل، تاجر) مما يستلزم عدم اطلاع الغير عليها، في إطار المحافظة على سلامة وسرية المعطيات على كل مصرف يقوم بمعالجة المعطيات الشخصية أن يتخذ جميع التدابير والاحتياطات اللازمة إزاء أطراف وسائل الدفع الإلكتروني المعنية بالمعالجة، وللمحافظة على أمان معطيات الدفع الإلكتروني ومنع الغير من تعديلها أو الإضرار بها أو الاطلاع عليها وإذا اختار المصرف طرف آخر يعهد إليه بأعمال

---

[1]- كما تنص المادة 10 من النظام رقم 07/05أنه " يتعين على المشاركين في نظم الدفع ضمان سرية وصحة المعلومات التي تمر عبر أنظمة الدفع ".

[2]- تنص المادة 09 من النظام رقم " يستلزم التبادل غير المادي لوسائل الدفع تقديمها المنطقي في أنظمة الدفع لاسيما تقنينها وهيئتها الموحدة.
يتعين على المشاركين الاحترام الصارم لأحكام الاتفاقيات المرتبطة بمختلف أنظمة الدفع والخصائص والتعليمات المتعلقة باستعمال هذه الأنظمة ".

المعالجة يجب أن يتحرى في اختياره الكفؤ للقيام بالمعالجة واحترام مقتضيات قانون معالجة المعطيات ذات الطابع الشخصي.

نحن في الجزائر بحاجة إلى هذا النوع من الحماية لأنه بالقدر الذي نتوسع فيه في مجال الحماية للمعطيات الشخصية بقدر ما نواجه بالتغيرات المهولة لشبكات الاتصال على الوصول إلى هذه الخصوصيات وإفشائها وهو ما جعل المشرع الجزائري يسعى إلى التوفيق بين ضرورة الحماية للمعطيات الشخصية والتطور التكنولوجي من جهة، ودخول هذه المعطيات عالم الدفع الإلكتروني والمعاملات المصرفية الإلكترونية.

يجب التوسع في مدلول حماية الحياة الخاصة لتشمل عنصرا مستحدثا يتمثل في حماية المعطيات الشخصية وبالتالي توسيع نطاق السر المصرفي ليشمل الأسرار المصرفية المعالجة إلكترونيا وكذا المعطيات الشخصية لأطراف وسائل الدفع الالكتروني.

المطلب الثاني

مفهوم السر المصرفي المعالج إلكترونيا

تظهر الخطورة بالنسبة لوسائل الدفع الإلكتروني في إمكانية استخدامها دون ترك أدنى أثر وبالتالي إمكانية أن تصبح المعلومات الشخصية والمالية للزبون موضع تشهير وإفشاء دون إمكانية التوصل إلى الفاعل، ويلتزم المصرف بحفظ سر المهنة عامة وليس سرية الحسابات فقط فهو يلتزم بعدم الادلاء بأسرار زبائنه، فطبيعة عمليات البنوك والعلاقة بين البنك وزبونه تقوم على ثقة الزبون في أن يكتم البنك ما يفضي به الزبون إليه من تصرفاته وأحواله

المالية[1]، وعلى هذا الأساس سنتناول تعريف السر المصرفي(الفرع الأول)، وتأثير وسائل الدفع الإلكتروني على مفهوم السر المصرفي (الفرع الثاني).

الفرع الأول

تعريف السر المصرفي المعالج إلكترونيا

تتأثر ماهية المعلومة الخاصة بالسر المصرفي بحق البنك في سلامة معاملاته المالية وسلامة الاقتصاد ككل من جهة وبين حق الزبون في الاحتفاظ بالسرية المصرفية لمعاملاته البنكية فالبنوك تطلب من الزبون أكبر قدر عن يساره هذا من جهة ومن جهة أخرى فإن البنوك تجمع معلومات كلها تتمتع بالسرية حيث لا يجوز للبنك البوح بها وإذاعتها.

السر المصرفي يشمل كافة البيانات الخاصة بالمعاملات المالية للزبون مع البنك دون تحديد لهذه البيانات وذلك لتغطية كافة أنواع البيانات التي قد يفرزها التطور في المعاملات المصرفية[2]، ويقصد بالسر المصرفي كافة البيانات والمعلومات الخاصة بالمعاملات المالية للبنك والتي يمكن أن تصاحب ثورة تكنولوجيا المعلومات وخاصة تلك التي تستعمل من خلال وسائل الدفع الإلكتروني التي يمكن استحداثها.

أولا/ تأثير المعالجة الآلية للعمل المصرفي على مفهوم السر المصرفي

لاعتبار المعلومة سرا يستحق الحماية يجب أن تكون ذات صلة بالفرد ويمكن أن تؤثر عليه ماديا أو معنويا وأن يكون حريصا على ابقائها طي الكتمان بعيدة عن علم الغير هذه

[1]- حسام الدين كامل الاهواني، المرجع السابق، ص51.

[2]- علاء التميمي، المرجع السابق، ص602.

المعلومات السرية يمكن أن تكون موجودة على جهاز الحاسب الآلي الخاص العائد للفرد سواء أكان الحاسب الآلي موجودا في البيت أو في مكان العمل الخاص، هذا الحاسب قد يكون منفردا وقد يكون مربوطا بشبكة اتصالات محلية أو عالمية كما يمكن أن تكون هذه المعلومات السرية لدى جهات أخرى يرتبط معها الفرد بعلاقة ما[1]، ومنها الحالة التي يرتبط بها الزبون بالمصرف من خلال استعماله لوسائل الدفع الإلكترونية بحيث يطلع المصرف على حساب الزبون وعلى وضعه المالي وهذا الوضع يعتبر في الغالب من الأسرار التي يرغب الزبون في ابقائها طي الكتمان والسرية وهو ما يعتبر اعتداء على الحياة الخاصة للأفراد وانتهاك لحرمة السرية الخاصة بهم، وغالبا ما يكون الاطلاع بهدف الإفشاء وسواء قام الفاعل والذي غالبا ما يكون عاملا في المصرف متاح له بحكم عمله الاطلاع على المعلومات والبيانات الخاصة بوسائل الدفع الإلكتروني وهذا يتم في العادة عن قرب من أحد أجهزة الحاسب الآلي في المصرف، أو أن يحدث هذا الفعل من شخص أجنبي عن بعد لأنظمه الاتصال المعلوماتية بمعونة أجهزة تحليل الشيفرات[2]، أو يتوصل بخبرته ودرايته بأنظمة المعلومات لتحقيق اختراقات واتصالات بعدية وهذه الطريقة الثانية هي التي يتم بواسطتها غالبا الاطلاع على المعلومات المتعلقة بوسائل الدفع الإلكتروني بحيث تسهل هذه التقنية عمليات الاختراق والاختلاس فيما بعد، أو أن يتمكن من الاطلاع على تلك الأسرار الخاصة بالزبائن وافشائها فيما بعد، وسواء تم الإفشاء لشخص واحد أو للعامة، كما يمكن أن

[1]– سهيل محمد العزام، بحوث قانونية، المملكة الاردنية الهاشمية، المكتبة الوطنية، الطبعة الأولى 2011، ص58.

[2]– سهيل محمد العزام، المرجع السابق، ص60.

يشكل الحاسب الآلي وسيلة أكثر فعالية في نشر وإفشاء الأسرار الخاصة بالزبائن بشمولية وتوسيع أكبر وبسرعة وكفاءة عالية لكافة أرجاء المعمورة.

لا يخفى على الكثير منا مدى الأضرار المادية أو المعنوية التي يمكن أن تلحق الزبون عند إفشاء الأسرار الخاصة به، ناهيك عن المنفعة التي يمكن أن يحققها الفاعل جراء ذلك الإفشاء كالتخلص من منافس في السوق أو مساس بسمعته التجارية أو التشهير بتوقفه عن الدفع وإنه في مرحلة الافلاس، أو حتى تهديد الزبون بالإفشاء والتشهير لسمعته في حال عدم تحقيق مطالب الفاعل.

ثانيا/ تأثير المعالجة الآلية للعمل المصرفي على الوضعية المالية للزبون

يلاحظ الفقه أن تخزين هذه المعلومات في الحاسب الآلي يؤدي إلى تقدير البنوك من خلالها لوضع الزبون المالي وعلى أساسها تحدد هل يمنح الائتمان أم لا وبالتالي يحظر تقدير مركز الزبون من خلال الحاسب الآلي لأن الزبون قد يفاجأ برفض الحصول على القرض لأن البنك الأول قد قدم هذه المعلومات المخزنة إلى البنك الآخر أو إلى بنك من بنوك المعلومات.

عند استعمال الزبون لأية وسيلة من وسائل الدفع الإلكتروني قد يسجل الحاسب الآلي عارض من عوارض الدفع وبالتالي هل يمكننا أن نستخلص أن الزبون معسر فهذا الرأي يرى أن هذا اضرار بالائتمان الشخصي دون وجه حق لأن التقدير يدخل في عموم حظر تخزين بيانات تنطوي على تقدير للشخصية باعتبار أن الذمة المالية جانب من جوانب الشخصية

لهذا تتجه التشريعات التي تستهدف توفير الحماية للمستهلك بمنحه حرية الرجوع في عقد القرض الذي أبرم مع البنك خلال فترة زمنية تحظر تخزين بيانات تتعلق بحالات الرجوع حتى لا تعطي عن الزبون فكرة غير صحيحة نتيجة عدم البحث في أسباب الرجوع مما يهدد ائتمان الشخص[1] وهذا حسبهم حتى لا يكون الحاسب الآلي عنصر من عناصر الخلل في التوازن بين البنك والزبون وبالتالي يكون من الصعب على الزبون أن يدافع عن نفسه لنفي الفكرة التي تكونت عنه من خلال الاطلاع على بيانات الحاسب الآلي.

الفرع الثاني

تأثير وسائل الدفع الإلكتروني على مفهوم السر المصرفي

تعني السرية بالنسبة للمعلومة المصرفية المتعلقة بوسائل الدفع الإلكتروني المعلومات التي تمثل القواعد التي تتحكم بإدارة بيانات ومعطيات وسائل الدفع كالمعلومات الشخصية للبطاقة المصرفية، أو المعلومات الخاصة بالتحويل الإلكتروني للأموال بصفة خاصة، وبصفة عامة السرية للمعلومات المتعلقة بوسائل الدفع الإلكتروني تشمل كل المعلومات المالية للأفراد.

قبل الخوض في مسألة تأثير وسائل الدفع الإلكتروني على مفهوم السر المصرفي إلكترونيا لابد لنا من أن نعرف البيانات والمعلومات **لأن السر** هو البيانات الشخصية والمعلومات التي تخص الأفراد وحساباتهم وكل ما يتعلق بهم في معاملاتهم مع البنك

أولا /بيانات ومعلومات وسائل الدفع الإلكتروني والسر المصرفي

[1]- عزيزة الشريف، المرجع السابق، ص1766.

تعرف البيانات بأنها المعطيات الأولية التي تتعلق بقطاع أو نشاط ما بينما تمثل المعلومات النتائج المبدئية أو النهائية المترتبة على تشغيل البيانات أو تحليلها أو استقراء دلالتها أو استنتاج ما يمكن استنتاجه منها وحدها أو متداخلة مع غيرها ومن هنا يظهر التمييز بين البيانات والمعلومات إذ تمثل البيانات المادة الخام للمعلومات ويجب احترام سرية البيانات الخاصة بالزبائن، واحترام حقهم في الخصوصية يقتضي الالتزام بعدم نشر أو بث أي بيانات تتعلق بشخصياتهم، أو حياتهم الخاصة وحتى البيانات المصرفية الخاصة بهم[1]، لأنه قد ينتج عن تحليل البيانات الخاصة بوسائل الدفع الإلكتروني استنتاج حقيقة الوضعية المالية للزبون، عرف النظام 06/05 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى من خلال الملحق المرفق به المعلومة **عملية مجسدة من خلال رسالة تعبر على مستوى نظام التسديدات** الخاصة بالجمهور العريض وتوجه لمشارك واحد أو لعدة مشاركين غير التقديم أو الرفض من الممكن أن يتعلق الأمر بالإعلام باستلام بيان خاص بالعمليات أو بالحساب اليومي واشعار بإقفال أو ختم، وتنص المادة 48 من النظام المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى" يلتزم المشاركون في النظام بالسر المهني، "واعتبر أن كل معلومة صادرة في أي شكل كان سرية ولا يمكن افشاؤها لطرف ثالث[2].

ثانيا /البيانات ذات الطابع الشخصي هدف للجرائم المرتبطة بوسائل الدفع الإلكتروني

[1]- حوالف عبد الصمد، المرجع السابق، ص 354.

[2]- أنظر المادة 48 من النظام رقم 06/05.

يعترف المصرفيون بهذا الخطر الجديد على البيانات الشخصية وهو ما تؤكده التقارير الرسمية المتعلقة بالنقود الالكترونية والخدمات المصرفية الإلكترونية بضرورة اتخاذ التدابير الاحترازية لأن الخدمات المصرفية الإلكترونية لا تغير بالأساس من دور البنوك وأنشطتها ولكنها تسمح بتوسيع أكبر لأسواقها غير أنها تعرضها لمخاطر جديدة[1].

القانون الدولي يبقى غير متساوي بخصوص حماية المعطيات ذات الطابع الشخصي لكن الأنترنت تلزم أن تكون حماية مع تعدد للمعايير[2]، لا يمكن التعامل بوسائل الدفع الإلكتروني عبر الأنترنت إلا من خلال البنك الإلكتروني حيث تشهد السرية والخصوصية في هذا الأخير أهمية خاصة لأنها لم تعد مقصورة على حسابات الزبائن وودائعهم لدى البنك فحسب بل يمتد الأمر أيضا ليشمل قاعدة البيانات الخاصة بالعملاء وتعاملاتهم مع البنك ككلمات السر الخاصة بالدخول على الموقع الإلكتروني للبنك أو دخول الزبون على حسابه والتعامل عليه، أيضا البيانات الخاصة بالتشفير وما يرتبط به من بيانات خاصة بمفاتيح التشفير والتوقيع الإلكتروني، فالبنك الإلكتروني العامل عبر شبكة الأنترنت ما هو إلا تدفق هائل من البيانات عبر مجموعة من الأجهزة والشبكات الأمر الذي يعظم من سرية وخصوصية هذه البيانات[3].

ثالثا/ المعالجة الآلية للمعطيات الشخصية مصدر للجريمة المرتبطة بوسائل الدفع الإلكتروني

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit p48

[2]-Francis baillet, le droit du cybercommerce, le guide pratique et juridique, 2001, P133.

[3]- علاء التميمي، المرجع السابق، ص 299، 300.

الاعتداءات في مادة المعالجة الآلية للمعطيات ذات الطابع الشخصي[1] للحسابات البنكية الناتجة عن دمجها وحصرها في الأنترنت أحدثت آثار مهمة في الجريمة الاقتصادية والمالية، في الواقع البنوك هي الضحايا الأولى للإجرام المعلوماتي المتحرك أساسا عن طريق باعث الربح مما يتطلب تطوير استراتيجيات خاصة بتركيز الأخطار الرقمية[2] وأصبح السر المصرفي وحماية البيانات الشخصية والأمن الإلكتروني عناصر جديدة تشكل ثقلا على مرونة المصارف[3]، وكذلك الجرائم المرتبطة بالمعالجة الآلية ذات الطابع الشخصي ناقلة للجريمة الاقتصادية والمالية فتطور الانترنت نتج عنه دوران المعطيات ذات الطابع الشخصي الجد حساسة في المادة البنكية التي لها قيمة اقتصادية وتخريبها هدف مرغوب فيه للمجرمين ويظهر أكثر في الجريمة الاقتصادية والمالية[4]، فالثورة الجديدة في وسائل الدفع تستعمل حاليا بواسطة الدفع عن طريق الأنترنت، والهاتف المحمول وكذلك المدفوعات دون الاتصال المباشر، وكذلك المدفوعات المتعلقة بالوسائل الجديدة غير المصرفية خاصة في أوربا وأصبح هناك نوع من المواجهة بين السلطات العمومية للمنافسة والبنوك والسياسات

---

[1]– كاليفورنيا قامت بتبني قانون في 12 فيفري 2002 دخل حيز النفاذ في جويلية 2003 حيث ابتكر مادة تلزم كل هيكل معالج للمعطيات الشخصية في حالة الاعتداء على أمن النظام المعلوماتي بإعلام مقيمي كاليفورنيا الذين معطياتهم الشخصية متضمنة في الملفات التي أفشيت أو يفترض أنها أفشيت لأشخاص غير مرخص، هذه المعطيات خاصة وتكون بأرقام أو أرقام تأمين اجتماعي وتسمح بتسيير بطاقة ترقيم حساب بنكي لبطاقة دفع أو ائتمان بتكملتها بكلمة مرور، المؤسسات كانت شفرت ملفاتها ولكن لم تكن خاضعة لهذا الالتزام، أنظر droit de pierre storrer, p262. édition RB, la monnaie électronique,

[2] - Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 153

[3] -Noémie Weinbaum, l'épineuse question de l'accès aux donnée de paiement, juillet-aout, 2017, N°810, p72.

[4]- Myriam Quéméner, criminalité économique et financière à l'ère numérique , op, cit 155.

المنتهجة حاليا تتمثل في نقل تكلفة الاحتيال من التاجر إلى بنك الزبون الذي يصدر وسيلة الدفع لأنه هو الذي من مصلحته الاستثمار لوضع ترتيبات أمنية مناسبة[1].

المطلب الثاني

أركان جريمة إفشاء الأسرار المصرفية الإلكترونية

الأصل أن جميع المصارف تحتفظ بخصوصيات الأفراد من خلال منع إفشاء السر المصرفي، أي عدم ذكر المعلومات حوله دون الرضى المسبق لحامل وسائل الدفع الإلكتروني.

ومنه يمكننا القول أن خصوصية المتعاملين بوسائل الدفع الإلكتروني يجب أن تكون موضوع حماية فيما يتعلق بمعلوماتهم الشخصية والمالية الموجودة على السجلات الإلكترونية أو على وسائل الدفع وخلال جميع العمليات التي تهدف إلى إجراء صفقات مالية في ظل عمليات الصيرفة الإلكترونية.

وهذه المعطيات أثرت في أركان جريمة إفشاء السر المصرفي وعليه سنرى كيف تأثر الركن الشرعي للسر المصرفي باعتباره صورة للخصوصية المعلوماتية في القانون الجزائري (الفرع الأول)، ثم تداخل الأركان المادية في الجرائم المتعلقة بالخصوصية والسر المصرفي (الفرع الثاني)، والركن المعنوي (الفرع الثالث) والاستثناءات على السر المرتبط بوسائل الدفع الإلكتروني (الفرع الرابع).

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit p48.

الفرع الأول

الركن الشرعي للسر المصرفي الإلكتروني باعتباره صورة للخصوصية المعلوماتية في القانون الجزائري

استحدث بموجب التعديل الدستوري الأخير في الجزائر حماية للحق في الخصوصية المعلوماتية (أولا)، مما ترتب عنه إمكانية الحماية الجنائية لسرية المعطيات ذات الطابع الشخصي بالقانون 07/18 (ثانيا)، ومع توافر حماية جزائية مسبقة للسر المهني في اطار قانون العقوبات (ثالثا)، وحماية جنائية للسر المصرفي (رابعا)، وكذا اقرار حماية جزائية جديدة لسرية المراسلات الإلكترونية (خامسا).

أولا/ حماية الحق في الخصوصية المعلوماتية بنص دستوري

نطاق حماية الحق في الخصوصية توسع في الجزائر ليشمل حماية الخصوصية المعلوماتية دستوريا حيث تم تعديل نص المادة 39 من الدستور كما يلي " لا يجوز انتهاك حرمة حياة المواطن، وحرمة شرفه، ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه[1].

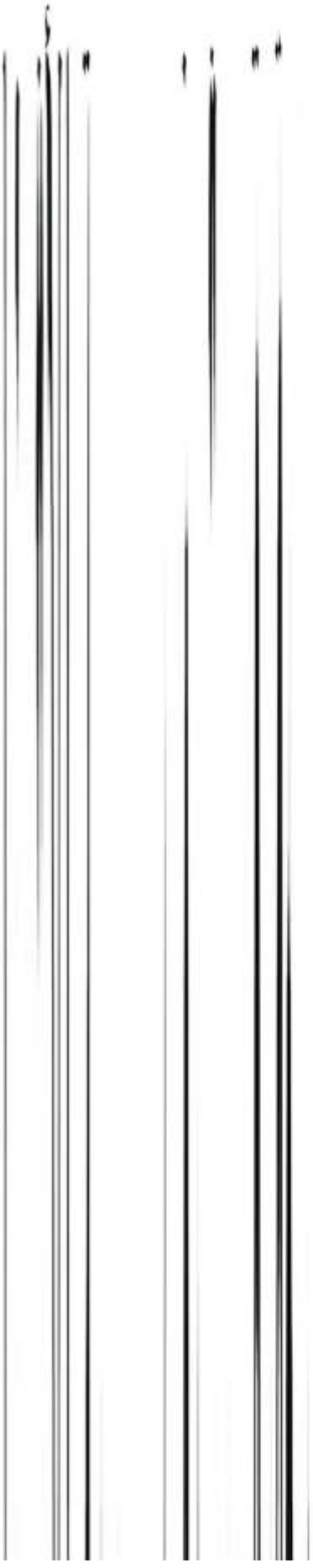
أقرت المادة 39 حماية دستورية لحق المواطن في الخصوصية بحرمة المساس بحياته الخاصة وحرمة المساس برشفه، وحقه في سرية مراسلاته بكل أشكالها، وأقرت الفقرة الثالثة المضافة سنة 2016 حماية الحق في الخصوصية المعلوماتية أي حماية الشخص الطبيعي عند معالجة المعطيات الشخصية الخاصة به، والمعطيات الشخصية هي تلك المشمولة بالحماية الجزائية التقليدية للأسرار بصفة عامة في جميع المجالات التي تخضع فيها للمعالج، وفي مجال حماية الأسرار المصرفية تظهر أهمية الحماية في حالة المعالجة للمعطيات بصفة خاصة، ويبدو أن المعطيات الشخصية المخزنة في جميع وسائل الدفع الإلكتروني والحاسبات الآلية للبنوك هي الأكثر تعرضا للإفشاء وبالتالي الأكثر حاجة للحماية.

ثانيا/الحماية الجنائية لسرية المعطيات ذات الطابع الشخصي بالقانون رقم 07/18

القانون الجديد رقم 07/18 يهدف حسب المادة الأولى منه إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وأكدت المادة

[1]– القانون رقم 16-01 المؤرخ في 06 مارس 2016، المتضمن نص التعديل الدستوري 2016 الصادر في الجريدة الرسمية، العدد 14، المؤرخة في 07 مارس 2016.

الثانية على وجوب احترام المعالجة للكرامة الإنسانية والحياة الخاصة والحريات العامة



هل تكفي هذه النصوص في ظل التطور الهائل للمعلوماتية ووسائل الدفع الإلكترونية لحماية المستعمل وبالتالي لا حاجة لتعديل المادة 117 من الأمر 03/11 أم لابد أن يعدل النص ليشمل أي صورة للإفشاء أو أي نوع للمعلومة، أو أشخاص جدد يمكن أن يشملهم الالتزام بالسر المصرفي.

الفرع الثاني

تداخل الأركان المادية في الجرائم المتعلقة بالخصوصية وافشاء السر المصرفي

يمكن تأمين حماية الحياة الخاصة للزبائن على الأقل ضد الإفشاء بالالتزام بالسر المصرفي الذي يدخل ضمن الاطار العام المفروض على البنكي للالتزام بسر المهنة، وتؤكد جميع النصوص المستحدثة في المجال الإلكتروني على هذا الالتزام وتتفق كلها على تجريم فعل الإفشاء إلا أن المشكل يمكن أن يثار حول المعلومات محل الإفشاء(أولا) وصعوبة تحديد الفاعل في حالة الإفشاء (ثانيا).

أولا/ الاتفاق عل فعل الإفشاء والتداخل في المعلومات محل السر المصرفي الإلكتروني

من الواجب المحافظة على خصوصية النظام المعلوماتي لوسائل الدفع الإلكتروني عن طريق وسائل فنية[1] تحجب معلومات هذه الوسائل عن أي شخص ليس له حق الاستفادة منها، وللحفاظ على الخصوصية لابد من التحكم بعملية التدخل لذلك تهتم غالبية التشريعات بموضوع سرية البيانات المشفرة احتراما للحق في الخصوصية وتجريم كل فعل من شأنه

[1]- كالتشفير مثلا أو الجدران النارية.

البطاقات المصرفية وتتأكد من أنها لا تخرق أحكام قانون المعلوماتية والملفات والحريات ثم تعطي رأيها على ضوء هذه الاختبارات[1].

عرفت المادة 01/03 من القانون 07/18 المعطيات ذات الطابع الشخصي بأنها "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه " الشخص المعني"[2] بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الاجتماعية ...".

يقصد بالبيانات الإسمية أو البيانات ذات الطابع الشخصي موضوع الجمع والمعالجة اليدوية أو المعلوماتية جميع المعطيات أو المعلومات التي تسمح بتعريف الشخص الطبيعي ولو بصفة غير مباشرة إذ يعتبر من قبيل البيانات الاسمية غير المباشرة للشخص الطبيعي، رقم الحساب المصرفي، أو رقم البطاقة المصرفية[3].

---

[1]-كل الاجراءات المشار إليها في المتن سواء التصريح بإمكانية المعالجة الآلية للمعلومات ذات الطابع الشخصي للزبائن كان موضوع مذكرة صادرة عن اللجنة الوطنية للمعلومات والحريات في فرنسا صادرة في08 يوليو 1980، وكذا عدة قرارات في ميدان البطاقات المصرفية حيث تبدي اللجنة رأيها في مدى احترام هذه البطاقات لقانون المعلوماتية والملفات والحريات منها القرار الصادر في أكتوبر 1987 الذي سمح بإيجاد معالجة ممكنة تمكن من استعمال بطاقات الذاكرة في أجهزة الهاتف العمومية، أنظر الهادي شايب عينو، المرجع السابق، ص184، 185.

[2]-عرفت المادة 02/03 من القانون 07/18 " الشخص المعني: كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة...".

[3]- حسين محمد الغول، جرائم شبكة الأنترنت والمسؤولية الجزائية الناشئة عنها، دراسة مقارنة، مكتبة بدران الحقوقية، الطبعة الأولى، 2017، لبنان، ص396.

النظام بالسر المهني " واعتبر أن كل معلومة صادرة في أي شكل كان سرية ولا يمكن افشاؤها لطرف ثالث[1].

3-التداخل بين معطيات إنشاء التوقيع الإلكتروني والبيانات ذات الطابع الشخصي: يشترط في التوقيع الإلكتروني أن يمكن من تحديد هوية الموقع[2]، وتنص المادة 68 من القانون 04/15 " يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث سنوات وبغرامة من مليون دينار(1.000.000 دج) إلى خمسة ملايين دينار(5.000.000 دج) أو بإحدى هاتن العقوبتين فقط، كل من يقوم بحيازة **أو إفشاء** أو استعمال **بيانات إنشاء توقيع إلكتروني** موصوف خاصة بالغير"، وكل وسائل الدفع الإلكتروني لا يمكن استعمالها إلا عن طريق توقيع إلكتروني خاص بالزبون وبالتالي يعتبر التوقيع الإلكتروني من بين المعلومات ذات الطابع الشخصي والبيانات الخاصة بإنشائه من بين البيانات التي تعرف الشخص الطبيعي. وبالتالي نتساءل في هذه الحالة عن النص الذي سيطبقه القاضي إذا عرض عليه النزاع هل هو نص المادة 68 من القانون 04/15 المتعلقة بإفشاء بيانات التوقيع الإلكتروني أو نص المادة 117 من الأمر 11/03 المتعلقة بإفشاء السر المصرفي، أو المادة 40 من القانون 07/18 المتعلقة بإفشاء البيانات ذات الطابع الشخصي، علما أن نصوص المواد الثلاثة الأخيرة جميعها تحيلنا إلى تطبيق العقوبة المنصوص عليها في المادة 301 من قانون العقوبات والتي لا تتعدى العقوبة بها الحبس لمدة ستة أشهر والغرامة 100.000 دج، في

[1]- أنظر المادة 48 من النظام رقم 06/05.

[2]- أنظر المادة 07 من القانون 04/15 .

حين أن المادة 68 من القانون 04/15 العقوبة المحددة بها تتراوح بين ثلاثة (3) أشهر إلى ثلاث سنوات حبسا، وغرامة مالية من مليون دينار(1.000.000 دج) إلى خمسة ملايين دينار(5.000.000 دج)، وللقاضي امكانية اختيار تطبيق إحدى العقوبتين فقط، فمن خلال هذه المادة يمكننا أن نتكلم عن حماية خاصة لبيانات انشاء التوقيع الإلكتروني وتجريم افشائها ولكن الإشكالية تبقى مطروحة بالنسبة للعمل البنكي والبيانات الخاصة بالتوقيع الإلكتروني لاستعمال وسائل الدفع الإلكتروني.

في الأخير وإن كنا نثمن اتجاه المشرع الجزائري بعدم حصره أو تعداده للمعلومات التي تعتبر سرية ولا يجوز إفشاؤها إلا أننا نرى إمكانية التعارض مع القوانين الجديدة في حالة تطبيق العقوبات ويبقى لقاضي الموضوع سلطة لتقدير المعلومات التي تدخل ضمن نطاق السر المصرفي وغيرها من المعلومات.

ثانيا/ صعوبة تحديد الفاعل في حالة الإفشاء

تضاعف وسائل الدفع الإلكتروني من احتمالات التعرض للحياة الخاصة نتيجة قدرتها التقنية على احتواء عدد من المعلومات عن حاملها، ونتيجة نقلها المادي بالنسبة للبطاقات مثلا، أو غير المادي كالنقود الإلكترونية إذ بمقدور حاملها تداولها عند الاستعمال بالإضافة إلى استطاعة التاجر المعتمد لها الوصول إلى الملفات المسجلة داخلها، ويصعب معرفة من الذي أفشى السر كما أن عقوبة الإفشاء للسر المصرفي الإلكتروني قد تقابلها صعوبات

ترجع إلى مبدأ التفسير الضيق في القانون الجنائي وبالتالي ضرورة وضع قواعد خاصة للمصرفي لحماية السرية في مجال المعلومات الآلية.

فلا يجوز أن تخضع الملفات التي أعدت يدويا لقواعد تختلف عن تلك التي أعدت إلكترونيا فالعملية أو الفكرة واحدة في الحالتين ومن ثم نحن لسنا بحاجة لإيجاد قواعد جديدة لتنظيم استعمال وسائل الدفع الالكترونية والقضاء قادر على تطويع النصوص والقواعد الخاصة بحماية الحياة الخاصة حتى يجعلها صالحة لمواجهة جميع المخاطر التي يمكن أن يثيرها استخدام الحاسب الآلي إلا أن هناك من يشكك في مواجهة التعدي على الحاسبات الآلية وفق القواعد العامة في الحماية إذا عرفنا أن السر المصرفي الالكتروني قد أصبح يعرفه عدد كبير من الموظفين العاملين في مجال الحاسب الآلي، فإذا عرف هذ السر كل هؤلاء الأشخاص في أماكن متعددة من العالم أي كل من يتصل بالنظام فهل يظل هذا سرا[1]، كما يجب علينا أن نأخذ في الحسبان إمكانية احتفاظ الفاعل بنسخة من المعلومات المطلع عليها كالاحتفاظ بالرقم السري للبطاقة سواء من العامل بالمصرف أو من الغير.

كما أن المشرع الجزائري من خلال نص المادة 117 من الأمر 11/03 نلاحظ أنها لا تخاطب موردي الخدمات الإلكترونية[2] صراحة بالالتزام بالسرية، إلا أنهم معنيون بهذا الالتزام

[1]-عزيزة الشريف، المرجع السابق، ص1756.

[2]-المشرع التونسي كان أكثر تحديدا حين نص في المادة 52 من قانون التجارة والمبادلات الإلكترونية التونسي على تجريم الاعتداء على السرية و الخصوصية بإفشاء معلومات عهدت إلى مورد الخدمات الإلكترونية، وذلك في اطار نشاطه باستثناء تلك التي رخص له صاحب الشأن بنشرها بمقتضى شهادة كتابية أو إلكترونية، أنظر عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية الكتاب الثاني الحماية الجنائية لنظام التجارة الإلكترونية، المرجع السابق، ص 276، 277.

حيث أن هذا النص لم يقصر هذا الالتزام على العاملين لدى البنك فقط ولكن كل المشاركين من أشخاص وجهات يخولها القانون الاطلاع على البيانات والمعلومات.

و بناءا عليه يلتزم موردي الخدمات الإلكترونية بالمحافظة على سرية البيانات التي يطلعون عليها بحكم عملهم لدى المصارف التي تقدم خدمة الدفع الإلكتروني عبر الأنترنت.

تدخل المشرع الجزائري وأكد على الالتزام بالسرية في مواجهة موردي الخدمات الإلكترونية حيث نصت المادة 26 من القانون المتعلق بالتجارة الإلكترونية أنه " ينبغي للمورد الإلكتروني الذي يجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن والزبائن المحتملين، ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية كما يجب عليه:

-الحصول على موافقة المستهلكين الإلكترونيين قبل جمع البيانات.

-ضمان أمن نظم المعلومات وسرية البيانات.

-الالتزام بالأحكام القانونية والتنظيمية المعمل بها في هذا المجال.

-يتم تحديد كيفيات تخزين المعطيات ذات الطابع الشخصي وتأمينها وفقا للتشريع والتنظيم المعمول بها"، فالمشرع راعى من خلال هذا النص اعتبارات حماية السرية واعتبارات تدخل مودي الخدمات الإلكترونية وما يتبعه من إمكانية الاطلاع على البيانات، يضاف إلى هذا ضرورة تبني البنك الإلكتروني لنظام رقابي محكم على أنشطة موردي الخدمات الإلكترونية فيما يتعلق بالاطلاع على البيانات الخاصة بالبنك وزبائنه وذلك على نحو يراعى فيه الحفاظ على السرية لهذه البيانات من ناحية، ويراعى من ناحية أخرى توفير مساحة من الحرية

هذه الوسائل كالتاجر وموظفيه المتدخلين في اتمام العمليات بهذه الوسائل ويجب النص على أن مخالفة قواعد العمل بهذه الوسائل يعتبر خطا جسيم ويرتب المساءلة الجزائية.

الفرع الثالث

الركن المعنوي في الجرائم المتعلقة بحماية الخصوصية وإفشاء السر المصرفي

يتمثل في العمد و ويترتب على ذلك نتيجة هي الاضرار بسمعة أو شرف الشخص و الاعتداء على حياته الخاصة، ولا يتصور وقوع الجريمة بمجرد الخطأ، نلاحظ أن النصوص عامة ولا يوجد ما يقيدها لأن لغرض من العقاب ليس المحافظة على المصلحة الفردية فقط وإنما المحافظة على المصلحة العامة لأن ضرر الإفشاء في هذه الحالة يقع على عموم الناس وليس صاحب السر وحده فلو أن البنك أفشى أسرار زبونه الإلكتروني لمنع ذلك بقية الزبائن من التعامل مع البنك[1].

إمكانية تطبيق نص المادة 117 من الأمر 11/03 على كل من أفشى بيانات سرية سواء كانت عادية أو كانت بيانات معالجة إلكترونيا، ولا يلزم تطبيق المسؤولية الجزائية عن إفشاء سرية المعلومات المصرفية المعالجة إلكترونيا أن يكون الزبون طالب بعدم إفشائه بل يكفي أن يصل السر إلى علم البنك أثناء المعالجة الإلكترونية للبيانات.

وتهتم البنوك بالوسائل الفنية للتحكم في الخصوصية وأكثرها انتشارا هي استخدام كلمات المرور والجدار الناري إضافة إلى شهادة الترخيص وبهذه الطرق يمكن منع حدوث جريمة

[1]- هشام فتحي سيد حسن، المرجع السابق، ص 1194، 1195.

إفشاء الأسرار المتعلقة بوسائل الدفع الإلكتروني فعلى حامل وسائل الدفع الإلكتروني أو أي شخص مخول له الدخول إلى النظام المعلوماتي لوسائل الدفع الإلكتروني الحفاظ على كلمة المرور هذا ما يقره قانون النقد والمال الفرنسي.

الفرع الرابع

الاستثناءات الواردة على جريمة إفشاء سرية بيانات وسائل الدفع الإلكتروني

استثنت المادة 48 من النظام المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى من الاحتجاج بالسر المصرفي اتجاهها وهي السلطات القضائية والمديرية العامة لبنك الجزائر في اطار وظائفها وفي حدود اختصاصها.

عمليا فإن الهدف من تخزين المعلومات عن الزبون يجب أن يكون من أجل استعمالها في النطاق الداخلي من قبل البنك ذاته المسؤول عن الحاسب الآلي و لأغراضه الداخلية ودون أن يدخل في الاستخدام نقل المعلومة إلى الغير، ولكن البنك قد ينقل المعلومات لجهة خارجية عن البنك ولكن لخدمة أهداف البنك ذاته[1] مثل جهات الرقابة وأبرزها بنك الجزائر باعتباره البنك المركزي أو جهات الرقابة التي تشرف على حركة تداول رؤوس الاموال في إطار عمليات تبييض الأموال وهي خلية الاستعلام المالي في القانون الجزائري.

أولا/الاستثناء برضا الزبون الكشف عن المعلومات الإلكترونية

[1]- عزيزة الشريف، المرجع السابق، ص1767.

معاملاتها القانونية والتوقيعات والسجلات الإلكترونية وكذلك عليها تطوير أنظمتها الداخلية والخارجية حتى تضمن سلامة وسرية السجلات المصرفية وبيانات الزبائن من الأخطار الإلكترونية، حيث أن التقصير في هذا المجال قد يعتبر اخفاق في توفير الحماية الكافية للمعطيات ذات الطابع الشخصي للزبائن مع ما يستتبع ذلك من أضرار قانونية أو حتى أضرار تتعلق بسمعة الزبائن، فمن شأن التدابير الأمنية الضعيفة أن تؤدي إلى بروز مخاطر سمعة أو مخاطر قانونية للبنوك إذ يمكن اتهام البنوك بالتقصير والاخفاق في توفير حماية كافية للبيانات الشخصية للزبائن مع ما يستتبع ذلك من أضرار قانونية وأضرار تتعلق بالسمعة[1].

[1]-سيف الدين السماتي عبد الكريم، العمليات المصرفية الإلكترونية والاطار الاشرافي، مجلة اتحاد المصارف العربية، العدد278، يناير 2004، ص71.

الباب الثاني

المسؤولية الجزائية للشريك في استخدام وسائل الدفع الإلكتروني

نوضح بداية أن هناك صور أخرى للمسؤولية الجزائية منها الشروع والتحريض إلا أننا اقتصرنا من خلال هذه المذكرة على توضيح فكرة المسؤولية الجزائية للفاعل الأصلي وهو ما تناولنه من خلال الباب الأول من هذه المذكرة، وسنخصص هذا الباب للمسؤولية الجزائية للشريك نظرا لخصوصية مسؤوليته في هذا النوع من الجرائم والتي غالبا ما تتم عن طريق الاشتراك.

الجريمة الإلكترونية يصعب الفصل فيها بين العمل التحضيري والبدء في التنفيذ أو النشاط الإجرامي لأن شراء برامج معدة للاختراق ومعدات لفك الشفرات، وكلمات المرور وحيازة أجهزة لصناعة الفيروسات ولو لم يتم إطلاقها يعتبر جريمة فالاشتراك فعل غير مجرم ولكنه متى ارتبط بفعل مجرم برابطة سببية أصبح مجرما بذلك الارتباط فتجريم الاشتراك في الفعل غير التنفيذي للجريمة يستلزم توافر التجريم في الفعل التنفيذي لها ونتيجته، وبالتالي فالفعل غير التنفيذي للجريمة يستعير صفته الإجرامية من الفعل التنفيذي وهو ما يعرف بنظرية استعارة التجريم لأن الشريك في الجريمة يستقل بمسؤوليته الجزائية عن الفاعل الأصلي غير أن مسؤوليته لا تتحقق إلا بتحقق مسؤولية الفاعل الأصلي للجريمة ويعاقب بنفس العقوبة المقررة للجناية أو الجنحة، ويعتبر الاشتراك والتعاون والتواطؤ على الاضرار أكثر تكرارا في الجرائم المعلوماتية عموما إلا أنه يعتبر السمة البارزة في الجرائم المرتبطة بوسائل الدفع الإلكتروني لأنه غالبا ما تكون هناك مساعدة من متخصص في الحاسبات الآلية، أو مساعدة من أحد العاملين بالمصرف المصدر لوسيلة الدفع الإلكتروني والمجني عليه في

نفس الوقت، أو من العاملين لدى التجار المعتمدين لهذه الوسائل في التعامل لتغطية عملية التلاعب والتحويل الإلكتروني للأموال بصفة غير قانونية.

يعد هدف تحقيق الربح المادي والاستيلاء على الأموال دافعا لارتكاب الجرائم المرتبطة بوسائل الدفع الإلكتروني وهو ما يميزها عن باقي الجرائم المعلوماتية وبالتالي المساعدة على ارتكابها وتسهيلها يحتاج إلى عدد أكبر من الشركاء وليس فقط الفنيين والمختصين بل من الممكن تصور تقديم المساعدة والعون للفاعل الأصلي من أي شخص يسعى لتحقيق الربح السريع، وغالبا ما تتيح الجرائم المعلوماتية التسهيل والمساعدة لارتكاب جرائم أخرى لتحصيل الأرباح المالية، ولم تستطيع المصارف إلى غاية يومنا هذا السيطرة والتحكم في التواطؤ المحتمل من العاملين لديها لمواجهة التعامل غير المشروع بوسائل الدفع الإلكتروني.

بالتالي فالاشتراك في الجرائم المرتبطة بوسائل الدفع الإلكتروني يشمل الاشتراك المنصوص عليه في المادة 42 من قانون العقوبات الجزائري والصورة الجرمية التي تبناها المشرع الجزائري في المادة 394 مكرر05 من نفس القانون والمتمثل في الاتفاق الجنائي باعتبار الجرائم المرتبطة بوسائل الدفع الإلكتروني من الجرائم المعلوماتية، أو الأعمال المسهلة أو التحضيرية والتواطؤ المنصوص عليه في المادة 389 من قانون العقوبات المتعلقة بتبييض الأموال.

وبالنتيجة يعاقب الشريك متى ساعد أو اتفق أو تواطأ مع غيره على ارتكاب الجرائم الناتجة عن استخدام وسائل الدفع الإلكتروني، وجعل المشرع الجزائري عقوبة الشريك كعقوبة الفاعل الأصلي في الجريمة.

نخلص في الأخير إلى أن جريمة الاشتراك يقوم فيها الشريك بدور ثانوي أو تبعي في الجرائم المتعلقة بوسائل الدفع الإلكتروني، كما أن الاشتراك في الجرائم المرتبطة بوسائل الدفع الإلكتروني يؤدي إلى زعزعة الثقة في العمل المصرفي الإلكتروني الذي هو الدعامة الجديدة التي تقوم عليها الخدمات المصرفية الإلكترونية الموجهة للزبائن.

يعتبر العمل تحضيريا القيام بشراء برامج لاختراق أنظمة عمل وسائل الدفع الإلكتروني، أو اعداد فيروسات، أو تزويد جهاز الحاسب الآلي ببرامج معدة لفك تشفير رموز الدفع الإلكتروني وعادة يتم الاعداد للفيروسات في جوانب خاصة غير مرتبطة بالأنترنت والحكمة من تجريم الاشتراك في الإعداد والتحضير لهذه الجرائم أنه عادة ما تتطلب المساعدة والتسهيل والعمل الجماعي.

لمعالجة حالات المسؤولية الجزائية عن الاشتراك في استعمال وسائل الدفع الإلكتروني لابد من توضيح المقصود بالفاعل الأصلي والشريك في الجريمة الذي تنازعته عدة نظريات[1]

[1]- **نظرية الاستعارة المطلقة:** يستعير الشريك تجريمه كاملا من الفاعل الأصلي، و يتساو معه في المسؤولية والعقاب
- **نظرية الاستعارة النسبية:** تميز بين الفاعل الأصلي و الشريك من حيث المسؤولية والعقاب، فالشريك باقترافه أفعال أقل خطورة من أفعال الفاعل يستحق عقابا أخف من عقاب الفاعل، أما من حيث الظروف فإن كل منهما يستقل بظروفه الشخصية في حين تسري الظروف العينية على جميع المساهمين.

ولكن ما يهمنا هو نهج المشرع الجزائري للتمييز بين الفاعل الأصلي والشريك حيث اتبع بشأن المساهمة الجنائية خطة يغلب عليها الأخذ بنظرية التبعية مع استقلال المساهمين: فمن حيث التبعية يعاقب الشريك بالعقوبة المقررة للجناية أو الجنحة التي اشترك فيها، كما تسري عليه الظروف الموضوعية اللصيقة بالجريمة إذا كان يعلم بها مع استقلال كل منهم بظروفه الشخصية كما أن معاقبة الشريك لا تستلزم إدانة ومعاقبة الفاعل الأصلي[2] و بين معنى الفاعل في المواد 41 و45 من قانون العقوبات حيث تنص المادة 41على أنه ' يعتبر فاعلا في الجريمة كل من ساهم مساهمة مباشرة في تنفيذ الجريمة، أو حرض على ارتكاب

– **نظرية التبعية:** إجرام الشريك بمادياته و معنوياته يختلف عن إجرام الفاعل، فالشريك ليس مستقلا عن الفاعل، إذ لا بد من علاقة بينهما، تقتصر على ضرورة وقوع الفعل المجرم من الفاعل الأصلي كشرط لعقاب الشريك فالفاعل متبوع والشريك تابع مع استقلال كل منهم حيث أن مسؤولية الشريك تقدر بمراعاة خطورته الخاصة بغض النظر عن خطورة الفاعل، و بالتالي عقوبة الشريك أشد أو أخف من عقوبة الفاعل بحسب الأحوال.

وإن مسؤولية الشريك تتحدد في نطاق قصده الجنائي، فلا يسأل عن جريمة اقترفها الفاعل و لو كانت جريمة محتملة إذا لم تدر في ذهنه عند الاشتراك.

ولا يتأثر الشريك بموانع المسؤولية أو موانع العقاب التي قد تلحق الفاعل الأصلي، و عليه فلا تسقط مسؤولية الشريك عندما تنقضي الدعوى الجنائية عن الفاعل الأصلي.

[2]– المشرع الجزائري وأيضا قانون العقوبات الفرنسي الجديد أخذ بنظرية استقلال مركز الشريك عن الفاعل الأصلي، بحيث أن إدانة ومعاقبة الأول لا تشترط إدانة ومعاقبة الثاني ولا قياس لوضعية أحدهما على الآخر، خلافا لنظرية استعارة العقاب التي كان يأخذ بها قانون العقوبات الفرنسي القديم الذي كان يستعمل في المادة 59 منه عبارة (مثل عقوبة الفاعلين) بقوله "إن المشاركين في جناية أو جنحة يعاقبون بالعقوبة نفسها مثل المرتكبين لتلك الجناية أو الجنحة أنفسهم، إلا إذا نص القانون على غير ذلك"

ART59 « les complices d'un crime ou d'un délit seront punis de **la même peine que les auteurs** même de ce crime ou ce délit, sauf les cas où la loi en aurait disposé autrement ».

في حين أن قانون العقوبات الجديد استعمل عبارة **كفاعل نكرة** بحيث يعاقب كأنه فاعل مستقل عن غيره.

ART 121-6 sera puni **comme auteur** le complice de l'infraction, au sens de l'article 127-7.

أنظر: نجيمي جمال، المبادئ العامة لقانون العقوبات الجزائري، مقارنة بقانون العقوبات الفرنسي، معلى ضوء الاجتهاد القضائي (المحكمة العليا ومحكمة النقض الدولية) مادة بمادة من المادة الأولى إلى المادة 60 مكرر، دار هومة للطباعة والنشر والتوزيع، الجزائر 2016، ص207.

الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو ولاية أو التحايل أو التدليس الإجرامي ' ونصت المادة 45 من نفس القانون على ' من يحمل شخصا لا يخضع للعقوبة بسبب وضعه أو صفته الشخصية على ارتكاب الجريمة يعاقب بالعقوبات المقررة لها ' فصور الفاعل في الجريمة متعددة فهو الفاعل المباشر أو المحرض أو الفاعل المعنوي.

يمكن التمييز بين حالتين للاشتراك في الجرائم المرتبطة بوسائل الدفع الإلكتروني الأول استغلال وسائل الدفع لصالح نشاط إجرامي من قبيل تبييض الأموال، التهرب الضريبي والثاني تعرض وسائل الدفع الإلكتروني ذاتها للهجوم بواسطة التزوير والتزييف والتي تعتبر حالات شائعة، ونفصل الاشتراك في الجرائم المرتبطة بوسائل الدفع الإلكتروني من خلال الفصل الأول (الاشتراك في الاحتيال المعلوماتي)، وفي الفصل الثاني (الاشتراك في التزوير والجرائم الخاصة ببيانات وسائل الدفع الإلكتروني)، وأخيرا الفصل الثالث نخصصه (للاشتراك في تبييض الأموال والتهرب الضريبي الإلكترونيين).

الفصل الأول

الاشتراك في الاحتيال المعلوماتي

يتمثل القصد الجنائي الخاص في الغاية التي يصبو الجاني إلى تحقيقها من وراء ارتكاب تلك لجريمة وتطلبت المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ضرورة توفر القصد الخاص في هذه الجريمة بقولها " لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة ".

يستثنى مما تقدم الأدوات المشار إليها إذا تم استخدامها من أجل الاختبار المصرح به أو لحماية جهاز الحاسب الآلي فإنها لا تدخل في نطاق تطبيق هذا النص وهذا ينطوي بالفعل في تعبير دون حق[1].

[1]- هلالي عبد اللاه أحمد، المرجع السابق، ص89.

تتميز الجرائم المرتكبة بوسائل الدفع الإلكتروني بحقيقة مؤداها أن دقة تنفيذ العمليات غير المشروعة تستلزم اشتراك أو مساعدة أشخاص آخرين سواء كانوا فنيين أو مجرد وسطاء، وغالبا ما يكون الاشتراك ايجابيا ويتمثل في مشاركة أو مساعدة فنية أو مادية، ومن جهة أخرى قد تبدو المساهمة الفنية أمرا حتميا بالنسبة لهؤلاء المجرمين الذين لا تتوافر لديهم هذه الكفاءة الفنية التي تؤهلهم للتلاعب بالحاسب الآلي وفقا لهواهم.

صاحب نشأة جريمة الاحتيال المعلوماتي انتشار استخدام التحويل الإلكتروني للأموال، وتزداد الحاجة إلى المساعدة والاشتراك إذا كانت جريمة الاحتيال مرتبطة باستخدام وسائل الدفع الإلكتروني للحاجة أكثر لمساعدة العاملين في البنوك الذين يملكون التقنية والكفاءة العالية للتلاعب بالبيانات المتعلقة بوسائل الدفع الإلكتروني، وكذا الخبرة في تسوية العمليات المصرفية الإلكترونية، والتجار والعاملين لديهم الذين يقبلون الدفع وتسوية ثمن المشتريات بوسائل الدفع الإلكتروني المتلاعب فيها حتى يتمكن الجاني من اتمام نشاطه الإجرامي، وإذا كان الجاني من العاملين في البنوك فإنه يحتاج إلى تعاون ومساعدة الزبائن أصحاب وسائل الدفع الإلكتروني وأصحاب الحسابات التي سيتم التحويل إليها ليتمكن من تحويل النقود أو ايداعها في هذه الحسابات أو إلى سحب النقود بأسماء الزبائن المتواطئين حتى يتمكن من تغطية عملية التلاعب وتحويل الأموال، أو مساعدة المبرمجين الذين تلجأ إليهم البنوك لتحديث برنامج عمل وسائل الدفع الإلكتروني وصيانتها، أو مصممي المواقع الإلكترونية للبنوك العاملة عبر شبكة الانترنت عند الدفع عبر هذه الشبكة، أو مساعدة موردي الخدمات

الإلكترونية المتدخلين لتنفيذ عملية الدفع الإلكتروني، فالتعاون والتواطؤ أكثر تكرارا في الجرائم الإلكترونية ولا سيما إذا كانت الجريمة الإلكترونية مرتبطة بوسائل الدفع الإلكتروني، وقبل التفصيل في جريمة الاحتيال المعلوماتي (المبحث الثاني)، نتناول مميزات الاشتراك في الجرائم المتعلقة بوسائل الدفع الإلكتروني (المبحث الأول).

المبحث الأول

مميزات الاشتراك في الجرائم المتعلقة بوسائل الدفع الإلكتروني

يثير الاشتراك في الجرائم المرتبطة بوسائل الدفع الإلكتروني والتي تعتبر الصورة الأكثر وقوعا في هذه الجرائم عديد التساؤلات لذلك سنحاول من خلال المطلب الأول بيان (الأحكام العامة للاشتراك في قانون العقوبات الجزائري)، ونتناول في المطلب الثاني (الاتفاق في الجرائم المرتبطة بوسائل الدفع الإلكتروني كصورة موسعة للاشتراك) استنادا إلى أحكام الاتفاق الواردة في القسم الخاص بالجرائم الماسة بالمعالجة الآلية للبيانات لأنه غالبا ما يقع الخلط بين جريمة الاتفاق الجنائي وبين الاتفاق الجنائي كصورة من صور الاشتراك في الجريمة.

المطلب الأول

الأحكام العامة للاشتراك في قانون العقوبات الجزائري

الاشتراك في الجرائم المرتبطة بوسائل الدفع الإلكتروني في غاية الأهمية وهو مطلوب نظرا لاعتبارات تقنية ذات صلة بإتمام الجريمة وتحقيق نتائجها وضمان حسن تنفيذها إذ غالبا ما

تحتاج الوسائل التقنية المشكلة لطبيعة السلوك إلى عمل أكثر من شخص من فنيين وعاملين في البنوك وتجار، من المقرر قانونا أن فعل الاشتراك لا تتحقق فيه الصفة الجنائية إلا بوقوع الجريمة التي حصل الاشتراك فيها[1]،

[1]– جمال عبد المجيد التركي، المساهمة التبعية في قانون العقوبات (دراسة تأصيلية تحليلية مقارنة)، المكتب الجامعي الحديث، الطبعة الأولى، 2006، ص48.

في الجريمة من لم يشترك اشتراكا مباشرا، و لكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك".

الاشتراك هو كل فعل لا تتنفذ به الجريمة ولكنه يرتبط بالفعل التنفيذي فالشريك هو من يرتكب فعلا تحضيريا لا تنفيذيا في الجريمة، ويتم الاشتراك عن علم بمساعدة أو معاونة الفاعل الأصلي أو الفاعلين بكل الطرق المادية أو المعنوية كتقديم معلومات وهي الحالة التي تظهر كثيرا في الجرائم المرتبطة بوسائل الدفع الإلكتروني، ويلاحظ أن الغالبية العظمى من الحالات المكتشفة لأفعال الجريمة الإلكترونية قد ارتكبت بواسطة مستخدم من المؤسسة التي تدار بنظام المعلوماتية أو على الأقل عن طريق اشتراكه فيها حيث يعد ذلك أمرا ضروريا وحتميا[1]، وهناك العديد من القوانين لم تدرج الحالات التي أوردنها ضمن المبحث الأول من الفصل الثاني للباب الأول المتعلقة بإساءة استخدام بطاقة الائتمان لأنها اعتبرتها جرائم تقليدية لا يمكن أن تتم إلا بتواطؤ حامل البطاقة مع العامل بالبنك أو التاجر وبالتالي فهي عبارة عن اشتراك أي من هؤلاء إما في الاحتيال، أو التزوير، أو استعمال المزور مثلا قيام حامل البطاقة بالاتفاق مع التاجر على الاحتيال على البنك عن طريق القيام بمشتريات بعد استنفاذ رصيد البطاقة، أو تواطؤ العامل بالبنك على مساعدة الزبون على استخراج بطاقة سليمة ببيانات مزورة، أو السماح للزبون بتجاوز حد السحب بالبطاقة، أو السحب ببطاقة منتهية الصلاحية، أو

[1]– ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المطبعة والوراقة الوطنية، الطبعة الأولى، 2011، ص 21.

بعد صدور قرار بسحبها، أو تواطؤ بين الحامل الشرعي والغير ويتحقق ذلك بقيام الأول

بإعطائه بطاقته للثاني لاستخدامها بدلا منه في السحب وتزوير توقيعه ثم يبادر

بالاعتراض على عمليات السحب ويطعن بتزوير توقيعه حتى لا يتحمل المبلغ[1].

ومن أشهر الحالات التي وقعت في التسعينات الهجوم الذي شنه شاب روسي على مصرف سيتي بنك فعن طريق استخدام حاسوبه الموجود في روسيا نجح في أن يخترق دون إذن وحدات خدمة حواسيب المصرف في الولايات المتحدة الأمريكية وقام بتجنيد عدد من المتواطئين لفتح حسابات مصرفية في شتى أنحاء العالم، ثم أصدر تعليمات إلى حاسوب سيتي بنك بتحويل أموال إلى تلك الحسابات وعند اكتشاف المخطط وتحديد هوية المتهم[2]

الفرع الثاني

أركان جريمة الاشتراك في القانون الجزائري

لمعاقبة الشريك يجب توفر الركن الشرعي والمادي والمعنوي، وجميع هذه الأركان تتضمن أحكام تطبق على كل الجرائم سواء تقليدية أو إلكترونية، فأفعال الاشتراك غير مجرمة بحد ذاتها ولكنها متى قدمت للمساعدة على ارتكاب جريمة من الجرائم المتعلقة

[1]- السيد عبد الحميد أحمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية والدولية، مكتبة الوفاء القانونية، مصر، الطبعة الأولى، 2018، ص66.

[2]- السيد عبد الحميد أحمد، المرجع نفسه، ص122.

الاشتراك في هذه الحالة، فالمبدأ هو أن جريمة الاشتراك لا تتحقق إلا إذا ساهم الشخص في مساهمة الفاعل الذي يقوم باقتراف عمل يعاقب عليه القانون، باستثناء الاشتراك في المخالفات، وأخيرا يكفي أن يكون الفعل معاقبا عليه لذاته للقول بمسؤولية الشريك، و لو كان فاعله لا يعاقب لظرف خاص به، لأن فعل الاشتراك يستمد تجريمه من الفعل الأصلي ولذلك كان توافر الصفة الاجرامية فيه معلق على توافرها في الفعل الأصلي أي أن تجريم فعل الاشتراك يتحقق بوجود نص يجرم الفعل الأصلي.

ثانيا/الركن المادي لإجرام الشريك

إذا كان مبدأ الشرعية في التجريم يجعل المشرع ملزما بتحديد الأفعال التي يكون التجريم فيها أصليا فإنه من باب أولى يجعله ملزما بأن يحدد الأفعال التي يكون فيها التجريم تبعيا[1]، ولأن المرجع في تجريم الأفعال هو القانون بينت المادتان 42 و43 من قانون العقوبات الجزائري الأفعال التي يعتد بها في المساهمة التبعية التي يأتيها الشريك وهي:

أ) أعمال المساهمة أو المعاونة.

ب) الأعمال التي تعد في حكم المساهمة (إيواء الأشرار)[2]، ونشير إلى أننا لن نبينها لأنها لا تتعلق بالاشتراك المراد الاعتداد به في هذه المذكرة.

---

[1]- جمال عبد المجيد التركي، المرجع السابق، ص99.

[2]- إيواء الأشرار اعتبره المشرع في حكم المساعدة التي تجعل من صاحبها شريكا في الجريمة وهو غريب عن الجريمة التي قام بها الأشرار، و يأخذ حكم الشريك فيها لتقديمه المساعدة اللاحقة كما نصت المادة 43، و ذلك باعتياده تقديم المسكن أو الملجأ أو مكان لاجتماع المساهمين في الجريمة.

كما أضافت المادة 91 من قانون العقوبات صور أخرى للمساعدة "...علاوة على الأشخاص المبينين في المادة 42 يعاقب باعتباره شريكا من يرتكب دون أن يكون فاعلا أو شريكا احد الأفعال التالية:

ج) حصر المساهمة في الأعمال الايجابية.

***المساهمة أو المعاونة:** ويقصد بها تقديم العون والمساعدة لمرتكب الجريمة على شرط أن تبقى هذه المساهمة في حدود الأعمال التبعية أي التحضيرية للجريمة، ولا تتعدى إلى الشروع في تنفيذ الجريمة، وسميت المساهمة التبعية لأنها تابعة للمساهمة الأصلية وجودا وعدما، بمعنى أن دور المساهم التبعي مرتبط بوجود فاعل أصلي للجريمة فيستمد نشاطه الاجرامي من المساهمة الأصلية[1]، وتعني اعانة الجاني على الجريمة بأي طريقة كانت[2] وما يعد من قبيل أعمال المساعدة غير محددة قانونا فهي أي عمل يرى المساهمون أنه ضروري لتحقيق مآربهم، وتتم بكل الطرق بشرط أن تنحصر في الأعمال التحضيرية أو الأعمال المسهلة أو المنفذة للجريمة[3].

***الأعمال التحضيرية:** و تتمثل في جميع الأعمال التي تسبق مرحلة التنفيذ، و من الصعب حصرها، إذ تتوقف على ظروف كل جريمة و ما يراه المساهمون من ضرورة التحضير لها.

1-تزويد مرتكبي الجنايات أو الجنح ضد امن الدولة بالمؤن أو وسائل المعيشة و تهيئة مساكن لهم أو أماكن لاختفائهم أو لتجمعهم و ذلك أو يكون قد وقع عليه إكراه ومع علمه بنواياهم .

2-حمل مراسلات مرتكبي هذه الجنايات و تلك الجنح و تسهيل الوصول إلى موضوع الجناية أو الجنحة أو إخفائه أو نقله أو توصيله و ذلك بأية طريقة كنت مع علمه بذلك... ".

[1]- فالمساهمة التبعية لا تتحقق وحدها إذ لا يتصور أن يسأل الشخص كمساهم تبعي دون أن يوجد إلى جانبه شخص آخر على الأقل يسأل عن الجريمة بوصفه فاعلا لها، أنظر، عبد الرحمان محمد السويلم، المساهمة في الجريمة المعلوماتية في النظام السعودي دراسة مقارنة بالقانون الاردني، رسالة ماجيستير في الشريعة والقانون، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، السعودية، 2014، ص 33.

[2]-جمال عبد المجيد التركي، المرجع السابق، ص101.

[3]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص125.

***الأعمال المسهلة أو المنفذة للجريمة:** لا تقتصر أعمال المساعدة على الأعمال التي تسبق ارتكاب الجريمة، فقد تكون أعمال المساهمة معاصرة أحيانا لارتكاب الجريمة.

وأعمال المساعدة المعاصرة نوعان: أعمال مسهلة، تقع مع بداية أعمال التنفيذ، و أعمال منفذة، تصاحب الخطوات الأخيرة في ارتكاب الجريمة.

وإذا كانت أعمال المساهمة التحضيرية لا تثير أي أشكال، فالأمر يختلف بالنسبة لأعمال المساعدة المعاصرة لارتكاب الجريمة، باعتبار أن أعمال المساهمة التي تعاصر ارتكاب الجريمة قد تعد عملا مباشرا أو ملتصقا بالجريمة وبالتالي فإنها تعد مساهمة أصلية ويعد من قام بها فاعلا أصليا لا مجرد شريك، بالرغم من أنها لا تدخل في تكوين الركن المادي للجريمة.

السؤال الذي يطرح نفسه هو كيف نستطيع أن نميز بين المساعدة المعاصرة لارتكاب الجريمة التي تعد مساهمة أصلية، و تلك المعاصرة لها أيضا و التي تعد مساهمة تبعية؟

أعمال المساعدة المعاصرة التي تجعل من صاحبها فاعلا أصليا هي المساهمة التي تحدث وقت ارتكاب الجريمة و في مكان وقوعها، أما المساعدة المعاصرة التي تجعل من صاحبها شريكا لا فاعلا فهي المساهمة التي تحدث وقت ارتكاب الجريمة ولكن في غير مكان وقوعها وهكذا فإن بعد المساهم بالمساعدة عن مسرح الجريمة يجعله شريكا ولو أنه قام بعمله في وقت يعاصر وقت ارتكابها وبالتالي لا يكفي أن يقدم أحدهم

مساعدته للفاعل لكي يعتبر شريكا ما لم يثبت أن مساعدته من العوامل التي ساهمت في ارتكاب الجريمة، أما أعمال المساعدة اللاحقة على تمام الجريمة فليست وسيلة من وسائل الاشتراك.

بهذا يكون المشرع الجزائري قد ضيق من أفعال المساهمة التبعية ووسع من نطاق الأفعال الخاصة بالفاعل الأصلي كالتحريض مثلا الذي اعتبره من قبيل المساهمة الأصلية، في حين اعتبره كلا من المشرعين الفرنسي والمصري من أعمال الاشتراك[1].

* **حصر المساهمة في الأعمال الإيجابية:** يذهب الرأي الراجح في الفقه إلى القول أن المساعدة في كل صورها تتطلب عملا إيجابيا يقوم به المساهم لمعاونة الفاعل على ارتكاب الجريمة، وقد حدد القانون أعمال المساهمة على سبيل الحصر، و لا يمكننا القول بأن الامتناع يصلح كسبب من أسباب الاشتراك.

يجب على القاضي في حالة الإدانة بالاشتراك أن يبين نوع المساعدة التي تم بها الاشتراك، وإلا كان حكمه معيبا، أما بالنسبة للشروع في الاشتراك فلا عقاب عليه لأن النص القانوني يقتضي تقديم المساعدة فعلا بقوله "كل من ساعد أو عاون..." وتستلزم إدانة الشريك إظهار طريق المساهمة وإبراز العلم فلا يكفي أن يفصل القاضي في حكمه على عبارات النص القانوني لبيان قيام الاشتراك بل يجب استظهار طريقة الاشتراك من بين الطرق المنصوص عليها قانونا بأن يأتي الشريك فعلا يندرج تحت طريقة من طرق

[1]-العيد سعدية، المسؤولية الجزائية للبنك عن جريمة تبييض الأموال، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق، جامعة مولود معمري، تيزي وزو، تاريخ المناقشة، 2016/02/20، ص135.

الاشتراك المحددة بالمادتين 42و43 من قانون العقوبات الجزائري[1]، وقد يعدل الشريك لسبب ما عن رغبته في تنفيذ الجريمة، فهل لعدوله هذا أثر على مساءلته عن الجريمة؟ نميز بين حالتين: الأولى حالة ما إذا قام الفاعل مستعينا بالمساعدة التي قدمها الشريك من عدوله و يسأل مسؤولية تامة عن جريمة الاشتراك، و الثاني حالة ما إذا بادر الشريك إلى سحب مساعدته قبل قيام الفاعل بتنفيذ أو محاولة تنفيذ جريمته، ففي مثل هذه الحالة يستفيد الشريك من عدوله بشرط أن يستطيع إزالة كل أثر لاشتراكه، بحيث يمكن أن يقال بأن الفاعل قد قام بجريمته بدون أي مساعدة من الشريك.

يسأل الشريك في حدود قصده، فلا يسأل عن جريمة لم تخطر له و لم يردها، فإذا اشترك أحدهم مع آخر بأن قدم له مفاتيح لتمكينه من دخول المنزل للسرقة ، فمقدم المفاتيح لا يكون مسؤولا كشريك إلا في حدود السرقة، فلا يسأل عن أي جريمة أخرى قام بها السارق.

أما بخصوص الشريك في الغش المعلوماتي فالملاحظ أن الغش المعلوماتي يستلزم اشتراك أو مساعدة أشخاص آخرين، سواء أكانوا فنيين أو مجرد وسطاء وغالبا ما يكون الاشتراك بفعل إيجابي يتمثل في مساعدة فنية أو مادية كتقديم الجسم المادي لبطاقات الدفع الإلكتروني للمجرمين ليس للدفع بها وإنما لتقليدها وبالتالي فصاحبها مشترك في جريمة التقليد، ويمكن أن نتصور المساعدة المعنوية في الجرائم المرتبطة بوسائل الدفع

[1]- نجيمي جمال، المرجع السابق، ص211.

الإلكتروني كتقديم معلومات تتضمن شرح كيفية الدخول إلى مواقع البنوك والمواقع المتعلقة باستعمال وسائل الدفع الإلكتروني وكيفية الاستيلاء على الأرقام وكلمات السر عند استعمال البطاقات عبر الانترنت.

ثالثا/الركن المعنوي للاشتراك

جريمة الشريك جريمة عمدية فالشريك يقوم بعمله عن علم و دراية ضمن سلسلة الأعمال الأخرى لتحقيق الجريمة، ولا يتصور قيام الاشتراك بعمل غير عمدي كإهمال القيام ببعض الواجبات والالتزامات مما يسهل ارتكاب بعض الجرائم، فالقصد الجنائي للشريك يتطلب علما بجميع عناصر الركن المادي للمساهمة التبعية فيتعين أن يكون عالما بالفعل الصادر عنه، ويتعين أن يكون عالما بالجريمة التي ستترتب عليه (الفعل الأصلي)[1] ولتحقق الاشتراك لابد من توفر العلم والارادة.

أ-العلم: إذا كانت أعمال الشريك قد حددت على سبيل الحصر، فإن علم الشريك يجب أن يمتد ليشمل كل الأعمال التي تؤدي إلى ارتكاب الجريمة، أي عمله هو وعمل غيره من المساهمين على حد سواء.

فالشريك يعلم أن عمله ليس إلا حلقة من الحلقات الأخرى التي يساهم بها الآخرون والتي بمجموعها ستؤدي إلى الواقعة الإجرامية، أما بالنسبة للنتائج المشددة، فالشريك يكون مسؤولا ولو أن إرادته لم تتجه إلى النتيجة المشددة التي حدثت أو التي لم يكن

[1]- جمال عبد المجيد التركي، المرجع السابق، ص128.

يتوقعها لا هو ولا الفاعل، فمن يشترك مع آخر في جريمة يكون مسؤولا عن النتائج التي تؤدي إليها هذه الجريمة.

ب-الإرادة: يجب على الشريك أن يكون مريدا للنتيجة الإجرامية أي مريدا للفعل الأصلي كأثر لفعل الاشتراك الصادر عنه، بمعنى أن يكون حالة قيامه بفعل الاشتراك المادي قد تمثل الجريمة أمرا واقعا بوصفها غاية له و مطلبا، وعليه فإذا اقتصر الجانب المعنوي لديه على مجرد العلم دون أن تنصرف إرادته إلى وقوعها فلا يعد شريكا و تخضع إرادة الشريك للأحكام العامة، إذ لا يعتد القانون إلا بإرادة واعية مدركة ومميزة وحرة الاختيار للقول بتوافر المسؤولية[1].

ومن الأمثلة التي تدل على ضرورة توافر نية ارتكاب الجريمة لدى الشريك المثال الذي أوردته المذكرة التفسيرية لاتفاقية بودابست، والذي مفاده أن النقل la transmission عبر الانترنت للبيانات المتعلقة بمحتوى ضار un contenu nuisible، أو كود عدواني un code malveillant كل ذلك يتطلب مساعدة مقدمي الخدمات[2].

المطلب الثاني

الاتفاق صورة موسعة للاشتراك في الجرائم المتعلقة بوسائل الدفع الإلكتروني

[1]- وهذا يعني أنه لا قيام لجريمة الاشتراك عند المجنون أو الصغير غير المميز أو المكره.

[2]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص207،208.

تبنى المشرع الجزائري مبدأ معاقبة الاشتراك بالاتفاق الجنائي من خلال نص المادة 394 مكرر 05 من قانون العقوبات بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية في إطار مجموعات، هذا التجريم للاتفاق تتمثل فائدته الرئيسية في الحفاظ على الأمن العام[1]، ومحاولة تفادي مشكلات الشروع في الجريمة وتحليل ما يدخل في الأعمال التحضيرية و ما هو بدأ في التنفيذ[2]، وتنص المادة 394 مكرر05 من قانون العقوبات الجزائري "كل من شارك في مجموعة أو اتفاق تألف **بغرض الإعداد** لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان **التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها** " فالمشرع لم يخرج عن القواعد العامة لعقوبة الشريك حيث رصد لها نفس عقوبة الجريمة التامة، والاتفاق يقتضي عدم المساهمة في التنفيذ بمعنى أن دور الشريك في حالة "الاتفاق "على ارتكاب الجريمة يجب أن يقف دوره عند حد الاتفاق فقط ولا يتعداه إلى ممارسة أي دور تنفيذي على مسرح الجريمة[3] فهذه الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر وإنما

[1]-Serge Losappio , la répression de l'entente en droit pénal français et son application à la lutte antiterroriste, disponible sur le site http://www.village-justice.com/articles/repression-entente-droit-penal,3356.html/17/07/2016.

[2]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 205.

[3]- منتصر سعيد حموده، المساهمة الجنائية في التشريع المصري والاسلامي وأحكام محكمة النقض المصرية، دار الفكر الجامعي، مصر، الطبعة الأولى، 2012، ص157.

يتصور الاتفاق الجنائي بمجرد انتقال كلمة السر من شخص إلى آخر وأن لم يكن بينهما معرفة سابقة[1].

جرم المشرع الجنائي الاتفاق الجنائي باعتباره جريمة مستقلة بذاتها من جهة ومن جهة أخرى جرم الاتفاق كصورة من صور الاشتراك، وثار جدل فقهي حول مدى ملائمة تجريم المشرع للاتفاق الجنائي من عدمه حيث ظهر اتجاهان كالآتي[2]:

ذهب اتجاه إلى القول أن الاتفاق الجنائي عزم إجرامي وتجريمه لا يعتبر استثناء يرد على قاعدة "عدم العقاب على العزم الاجرامي " ويستند هذا الرأي إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها وإنما يعاقب عليه في حد ذاته كجريمة خاصة تامة، وهذا طبقا لنص المادة 176[3]من قانون العقوبات الجزائري **وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل**، وهذه الحالة ليست من قبيل الاشتراك لأن المشرع بعدها مباشرة ينص على الاشتراك في جمعية الأشرار في المادة 177من قانون العقوبات الجزائري[4] وبالتالي الاتفاق المقصود في المادة 176 من قانون

---

[1]- خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر اساليب وثغرات، دار الهدى، الجزائر، طبعة 201، ص 129.

[2]- بوربابة صورية، المرجع السابق، ص 199.

[3]- تنص المادة 176 من قانون العقوبات الجزائري :" كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل وتؤلف بغرض الاعداد لجناية أو أكثر ، او لجنحة أو اكثر معاقب عليها بخمس(5) سنوات حبس على الاقل ، ضد الاشخاص أو الاملاك تكون جمعية أشرار ، **وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل** ".

[4]- أنظر المادة 177 من قانون العقوبات الجزائري " يعاقب على الاشتراك في جمعية الاشرار ...".

العقوبات الجزائري جريمة قائمة بذاتها وليست اشتراك، كما أنها لا تعني الاتفاق المنصوص عليه في الجرائم المعلوماتية.

فالأصل العام للاتفاق هو اجتماع ارادتين أو أكثر على موضوع معين **أو** التصميم المشترك للقيام بالفعل(الجريمة)، وحجة تبرير المعاقبة عليه أنه في الاتفاق الجنائي يظهر العزم الإجرامي الجماعي بمظهر خارجي مادي لأن كل عضو فيه يعلن عزمه إلى سائر الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، وليس هناك حاجة إلى إثبات الاتفاق في حد ذاته فاكتشاف وثائق تبين مخططات وعمليات مراقبة للمؤسسات البنكية التي من المحتمل أن تكون محل سرقة يعني ضمنيا وجود اتفاق[1].

ومن جهة ثانية الاتفاق الجنائي ظاهرة خطيرة تهدد الأمن العام تهديدا فعليا، كما أن هدف المشرع من العقاب على الاتفاق هو الوقاية حيث أن احباط الاتفاق الجنائي نتيجته هي الحيلولة بين الجناة وبين تحقيق خططهم الإجرامية ويرى أصحاب هذا الاتجاه أنه لا مجال للاعتراض على تجريم الاتفاق الجنائي بحجة أن في ذلك حث للجناة على الأقدام على ارتكاب الجرائم المتفق عليها مادام أن العقاب يقع لأول مبادرة بدرت منهم وهي اتفاقهم وأن باب العدول الفردي مفتوح وذلك بالتبليغ والاخبار وما يتبعه من اعفاء من العقاب.

[1]- A-VITU, participation à une association de malfaiteurs, 5 mais 2004, éditions du juris- classeur, 2004, p07.

في حين يرى اتجاه آخر أن تجريم مجرد الاتفاق فقط ستكون له انعكاسات سلبية ذلك لما يخلقه من دفع للمجرمين بإتمام ما تم الاتفاق عليه نظرا لأن اتفاقهم قد تم تجريمه حيث أن العدول عن هذا الاتفاق وفقا للرأي السابق غير قويم ويكفي لدحضها جميعا المقارنة بين خطورة الاتفاق الجنائي على نحو ما صوره أصحاب الاتجاه السابق، وبين خطورة الأعمال التحضيرية التي تصدر عن شخص يسعى إلى ارتكاب الجريمة بمفرده فالاتفاق الجنائي في مرحلة مبكرة بالنسبة للتحضير للجريمة إذ أنها ترد على المرحلة النفسية إلى مرحلة اتخاذ القرار وعقد العزم على ارتكاب الجريمة بينما يعقب التحضير للجريمة هذه المرحلة النفسية لهذا- يضيف أصحاب هذا الاتجاه – أنه لو صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة لوجب على المشرع أن يجرم مرحلة التحضير للجريمة من باب أولى.

مفهوم الاتفاق يستوجب التمييز بين مظهرين أساسيين حتى يصبح الاتفاق إجراميا أولا من الضروري وجود قرار بالتصرف المشترك، ومن جهة أخرى الاتفاق المبرم مجسد بأفعال مادية على الصعيد الخارجي[1] وهذا ما اشترطه المشرع الجزائري بأن يكون التحضير مجسدا بأفعال مادية أي لا عقاب على مجرد العزم لأنه حالة نفسية يصعب إدراكها وهذا ما يتجلى من خلال نص المادة 394 مكرر 05 من قانون العقوبات

[1] -A-VITU, participation à une association de malfaiteurs, 5 mais 2004, éditions du juris- classeur, 2004, p22.

الجزائري "...**وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية** ..."، فالاتفاق أساسه حالة نفسية يعبر عنها صاحبها بأي وسيلة كانت كقول أو كتابة أو ايحاء[1].

المشرع الجزائري بصفة عامة نص على الاتفاق لمقاومة ووضع حد لنوادي ومنظمات القراصنة المعلوماتيين أو الهاكرز « clubs et associations d'informaticien pirates ou hackers »، والمحاكم الفرنسية استعملت هذه الجريمة لمعاقبة أفعال المشاركة في الجريمة ضد الأنظمة المعلوماتية وليس الأعمال التحضيرية للجنحة وبالتالي القاضي الجزائي الفرنسي غير المعنى الذي كانت تذهب إليه الجريمة[2]، فتجريم الاشتراك في التحضير الجماعي كان بهدف القمع في حالة التزوير في المحررات الإلكترونية و استعمالها لأن هذا التجريم متخصص في الاستعمال الذي يتم محوه[3].

الفرع الأول

تمييز الاتفاق بوصفه طريق من طرق الاشتراك عما يشابهه

يختلط الاتفاق كصورة للاشتراك مع غيره من المفاهيم لذلك وللإحاطة بالمقصود من الاشتراك عن طريق الاتفاق في وسائل الدفع الإلكتروني سنميزه عما يشتبه به من مفاهيم، حيث نميز أولا (بين الاشتراك كأصل عام والاتفاق كصورة للاشتراك)، وكذلك

[1]– جمال عبد المجيد التركي، المرجع السابق، ص112.

[2]– دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل درجة الماجستير، شعبة القانون الجنائي، جامعة منتوري قسنطينة، 2012، 2013، ص46.

[3]-R.Gassin, informatique (fraude informatique), Rép, pén, p100, pén, paris, Dalloz, oct. 1995, P 39.

نميز بين الاتفاق كصورة للاشتراك والاتفاق الجنائي (ثانيا)، وأخيرا الاتفاق عن التحريض على الجريمة (ثالثا).

أولا/ تمييز الاشتراك كأصل عام عن الاتفاق كصورة للاشتراك

-الاشتراك والاتفاق كصورة للاشتراك الجنائي كليهما صورة من صور الاشتراك في الجريمة بل أن الاشتراك طريقة من طرق الاشتراك.

- الاشتراك في قانون العقوبات الجزائري عامة لا يتصور إلا بالفعل الايجابي ،في حين أنه في دول أخرى يمكن تصور الاشتراك بالفعل السلبي، أما الاشتراك بالاتفاق فلا يمكن تصوره بالفعل السلبي أي عن طريق الامتناع لأن الاتفاق يقتضي التجاوب بين ارادتين ولا شك أن ذلك يتطلب فعلا ايجابيا ولا يتصور بالامتناع.

- إن الاشتراك يمكن أن يكون سابقا على وقوع الجريمة أو معاصرا لها، أما الاتفاق كصورة من صور الاشتراك فلا يتحقق إلا سابقا على وقوع الجريمة لأن جوهره يقتضي ذلك بما يطلبه من تقابل الإرادتين بين الفاعل **والشريك بالاتفاق تقابلا صريحا على أركان الجريمة التي تكون محلا له**[1].

- لا يشترط في الاشتراك أن يتم الاتفاق بين الفاعل الأصلي والشريك على ارتكاب الجريمة بل يكفي علم الشريك بارتكاب الفاعل للجريمة وأن يساعده أو يسهل له ارتكابها.

[1]- ضاوي جزاع زين ضاوي المطيري، المسؤولية الجنائية للاشتراك بالمساعدة، دراسة مقارنة، رسالة ماجيستير، قانون عام، كلية الحقوق، جامعة الشرق الأوسط، 2011، الأردن، ص 33.

ثانيا/ التمييز بين الاتفاق كصورة للاشتراك و الاتفاق الجنائي

- الاتفاق كصورة من صور الاشتراك غير معاقب عليها ما لم تقع الجريمة المتفق عليها في حين الاتفاق الجنائي جريمة مستقلة قائمة بذاتها(مجرم بأصله) يعاقب على مجرد الانضمام ولو لم تقع الجريمة المتفق عليها، وإذا تمت الجريمة المتفق عليها نكون أما جريمتين جريمة الاتفاق والجريمة الأخرى.

- الاتفاق كصورة للاشتراك يستمد أو يستعير صفته غير المشروعة من جريمة الفاعل وبالتالي نكون أمام فاعل أصلي وشريك يستعير تجريمه من الفاعل الأصلي، بينما في الاتفاق الجنائي تكون صفته غير المشروعة أصلية وكل المشتركين فيه فاعليين أصليين.

- تجريم الاتفاق كصورة من صور الاشتراك يراد من خلاله تحديد المسؤولية الجزائية عن جريمة ارتكبت فعلا فيما بعد بناء عليه، إلا أن تجريم الاتفاق الجنائي يكون لما تنطوي عليه بعض الأفعال من خطورة على المجتمع اقتضت تجريم مجرد الاتفاق على ارتكابها.

- نظمت المادة 176 من قانون العقوبات الجزائري الاتفاق بوصفه جريمة مستقلة، بينما نظمت المادة 394مكرر05 من قانون العقوبات الجزائري الاتفاق بوصفه وسيلة للاشتراك في الجريمة المعلوماتية.

ثالثا/ التمييز بين الاتفاق والتحريض

يختلف الاتفاق على التحريض من حيث أن الاتفاق تتلاقى فيه إرادتي الطرفين على ارتكاب الجريمة المتفق عليها، أي أن لكل من الفاعل والشريك ارادة وتصميم على ارتكاب الجريمة محل الاتفاق، أما التحريض فتكون ارادة المحرض وشخصيته طاغية على إرادة وشخصية المحرض، حيث أن الأول هو الذي يخلق فكرة الجريمة والتصميم على ارتكابها لدى الثاني، وبذلك يكون المحرض أكثر خطورة اجرامية[1]، لأنه صاحب الفكرة الإجرامية وهو الذي يبذل الجهد في الاقناع.

كما أن المحرض في التشريع الجزائري يكون فاعلا أصليا أما الاتفاق فقد يكون صورة من صور الاشتراك كما قد يكون جريمة قائمة بذاتها.

الفرع الثاني

أركان الاتفاق الجنائي باعتباره صورة للاشتراك في الجرائم الإلكترونية

رغبة من المشرع الجزائري في مواجهة فعالة للجرائم الإلكترونية قام بتجريم الاتفاق بغرض التحضير لها نظرا لخطورة الأعمال التحضيرية، فالاتفاق مرحلة مبكرة بالنسبة للتحضير للجريمة إذ أنها ترد إلى المرحلة النفسية أي إلى مرحلة اتخاذ القرار وعقد العزم على ارتكاب الجريمة[2] في الجريمة وبالتالي من المهم أن نعرف الاتفاق الجنائي في الجريمة المرتبطة بوسائل الدفع الإلكتروني كصورة من صور الاشتراك وهذا ما يهمنا

[1]- منتصر سعيد حمودة، المرجع السابق، ص158.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر 2008، ص113.

(ثانيا) لكننا قبلا سوف نعرف الاتفاق الجنائي في الجريمة الإلكترونية (أولا) وبعدها نحدد الركن المادي للاتفاق الجنائي كصورة للاشتراك (ثالثا).

أولا/ تعريف الاتفاق في الجريمة الإلكترونية

يعني اشتراك شخص مع آخر في التحضير والإعداد للجريمة المعلوماتية دون الاشتراك في العمل التنفيذي للجريمة أي الاتفاق على الأعمال المجهزة والمسهلة لارتكاب الجريمة كما أنه من عادة من يمارسون الجرائم المعلوماتية تبادل المعلومات بصفة منتظمة حول أنشطتهم.

ثانيا/ تعريف الاتفاق في الجريمة المرتكبة بوسائل الدفع الإلكتروني

الاتفاق بين شخص وأكثر في التحضير للجرائم الماسة بوسائل الدفع الإلكتروني باعتبارها من قبيل الجرائم المعلوماتية، فالفاعل الأصلي في الجريمة المرتبطة بوسائل الدفع الإلكتروني هو كل من يساهم بعمل تنفيذي في ارتكاب جريمة تتعلق بوسائل الدفع الإلكتروني وبالتالي الفاعل الأصلي هو كل من يرتكب أفعالا يصح وصفها شروعا في حالة قيامه بها بمفرده.

فالمعيار السائد في التمييز بين الفاعل في الجريمة والشريك فيها هو معيار البدء في تنفيذ الجريمة، أو بعبارة أخرى معيار "الشروع "، فيعد الجاني فاعلا أصليا إذا صدر منه أفعالا يصح وصفها شروعا في حالة قيامه بها بمفرده، أما الأعمال التي لا يصح

وصفها بالشروع إذا قام بها لوحده فإنها تعد أعمالا تحضيرية، ويوصف في هذه الحالة بكونه شريكا في الجريمة[1]، فبالنسبة للمشرع الجزائري إن الاتفاق المنصوص عليه في نص المادة 394 مكرر5 من قانون العقوبات يقصد به الاتفاق كصورة للاشتراك "كل من شارك في مجموعة أو اتفاق تألف **بغرض الاعداد** لجريمة ...**التحضير**..."، ومنه نتساءل عن الشروع في الاتفاق هل يعاقب عليه أم لا فقد يعدل الشريك لسبب ما عن رغبته في تنفيذ الجريمة فهل لعدوله هذا أثر على مساءلته عن الجريمة أم لا؟

فالاتفاق الجنائي كصورة من صور الاشتراك لا عقاب عليه إلا بوقوع الجريمة المتفق عليها إما تامة أو في شكل شروع، لأنه يستمد وجوده من الجريمة المتفق عليها إما تامة أو في شكل شروع بعكس الاتفاق كجريمة قائمة بذاتها والتي يعاقب فيها الفاعل على مجرد الاتفاق بحد ذاته، كما نلاحظ حصر الاشتراك الجرمي للمشرع الجزائري لصالح المساهمة المادية التبعية (تعدد الفاعلين- مجموعة و اتفاق) حسب نص المادة 394مكرر5 من قانون العقوبات " كل من شارك في مجموعة أو اتفاق بغرض الإعداد لجريمة ...**وكان هذا التحضير مجسدا بفعل مادي أو عدة أفعال مادية**..."، يعود الاعتماد على الاشتراك والاتفاق في الجرائم المرتبطة بوسائل الدفع الإلكتروني إلى كون أن المخططين لهذا النوع من الجرائم خبرتهم تقليدية لا تسمح بتخطيط يحتاج إلى

[1]- أشرف عبد الله الضويحي، ملخص بحث المساهمة في الجرائم المعلوماتية المتعلقة بالاعتداء الشخصي، بحث تكميلي لنيل درجة الماجيستير، قسم السياسة الشرعية، سلسلة ملخصات الأبحاث القضائية، صادرة عن جامعة محمد بن سعود الاسلامية والجمعية العلمية القضائية السعودية، المملكة العربية السعودية، العدد الثالث، 1435، ص 214، ص 210.

تطورات جديدة وتجديد للمعلومات، وخبرة فنية لاسيما وأن الخدمات المصرفية الإلكترونية والأنترنت تقدم الجديد كل يوم، وعلى الفاعلين الأصليين المنفذين إشعار هؤلاء بالصعوبات والعقبات التي تعترضهم لإيجاد الحل، كما عليهم الاتصال بالعاملين في البنوك لإخبارهم بالمعلومات المالية عن وسائل الدفع الإلكتروني والزبائن وكذلك هذا الشرط الجديد مجموعة أو اتفاق الغرض من النص عليه هو تقرير نوع من الحماية المتقدمة الوقائية لنظم المعالجة الآلية للمعطيات ضد المخاطر التي تنشأ عن النشاط غير المشروع لبعض نوادي المعلوماتية التي قد تسهم بمعلوماتها الفنية في التحضير لارتكاب الجرائم المشار اليها وكذلك ضد قراصنة المعلومات[1]، تتميز الجرائم المتعلقة بوسائل الدفع الإلكتروني عادة بتعاون بين أكثر من شخص على ارتكابها وغالبا ما تتم بين متخصص في الجانب المعلوماتي والتكنولوجي للحاسب الآلي والانترنت يتولى اتمام الشق الفني للمشروع الإجرامي لأن الجريمة تتطلب خبرة ودراية واحتراف في مجال تقنية المعلومات فعلى سبيل المثال التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية وتقنية عالية من قبل مرتكبها، وشخص آخر عادة من ضمن العاملين بالمصرف المجني عليهم اطلع على أسلوب العمل بوسائل الدفع الإلكتروني، وشخص آخر من خارج البنك (قد يكون صاحب وسيلة الدفع الإلكتروني الحقيقي أو من الغير)،

[1]- علي عبد القادر قهوجي، المرجع السابق، ص 598.

أو شخص من العاملين بالمتاجر المرتبطة مع المصرف بقبول التعامل بوسائل الدفع الإلكتروني لتغطية عملية التلاعب وتحويل الأموال.

التعاون والتواطؤ على الاضرار أكثر تكرارا في الجرائم المعلوماتية منه في الأنماط الأخرى للجرائم المستحدثة أو الخاصة أو جرائم أصحاب الياقات البيضاء[1] ويعتبر التعاون والتواطؤ من أبر سمات الجريم المعلوماتية والأكثر تكرارا، وغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني للمشروع الاجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب وتحويل المكاسب إليه، كما أن من عادة من يمارسون التلصص والقرصنة على الحاسبات وشبكات المعلومات تبادل المعلومات بصفة منتظمة حول أنشطتهم بل ويعقدون مؤتمرات[2].

بل إنه يمكننا القول أن أغلب الجرائم المتعلقة بوسائل الدفع الإلكتروني لا يمكن أن تتم إلا عن طريق التعاون والتواطؤ بالاشتراك في إخراج هذا النوع من الجرائم والذي قد يكون سلبيا يترجم بصمت من يعلم بوقوع الجريمة في محاولة منهم لتسهيلها واتمامها وهذا غالبا من طرف العاملين بالمصارف، إلا أن هذه الحالة وهي الاشتراك السلبي تبقى

---

[1]- عادل يوسف عبد النبي الشكري، المرجع السابق، ص 115.

[2]- هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح انشاء الية عربية موحدة للتدريب التخصصي، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت الذي نظمته كلية الشريعة والقانون، جامعة الامارات العربية المتحدة بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة، من 01الى 03 ماي 2000، المجلد الثاني، الطبعة الثانية، 2004، ص 446،447.

غير معاقب عليها قانونا في التشريع الجزائري الذي يشترط اشتراك إيجابي بتقديم مساعدة فنية ومادية غالبا ما تكون من المختصين في المعلوماتية، وعليه فشروط توافر جريمة الاشتراك بالاتفاق الجنائي يمكن تلخيصها بأن يهدف الاتفاق التحضير لجريمة من الجرائم الماسة بوسائل الدفع الإلكتروني، تجسيد هذا التحضير بفعل مادي، وتوافر القصد الجنائي وهو ما سنبحثه.

ثالثا/الركن المادي للاتفاق الجنائي كصورة للاشتراك

يتمثل الركن المادي للاشتراك بفعل المساعدة والتسهيل والاتفاق الجنائي الذي تبناه المشرع الجزائري كصورة للاشتراك لا كاتفاق جنائي باعتباره جريمة مستقلة والاتفاق الجنائي هي الصورة التي تتم بها غالبا الجرائم المعلوماتية لأنه كثيرا ما يحتاج الفاعل الأصلي إلى مساعدة صغار نوابغ المعلوماتية لتنفيذ وتخطي إجراءات الحماية التي يفرضها المصرف على الدفع بوسائل الدفع الإلكتروني أو إلى اتفاق خاصة في جرائم الاحتيال، أو تبييض الأموال التي غالبا ما تتم بالتواطؤ من المصرفي خصوصا وأن مهمته هذه أصبحت جد سهلة في الدفع الإلكتروني نظرا لما توفره وسائل الدفع الإلكتروني من مزايا ويتطلب الركن المادي للاتفاق الجنائي توافر ثلاث عناصر:

1-فعل الاتفاق: نلاحظ أن المشرع الجزائري لم يقم بتجريم مجرد الاتفاق كحالة نفسية وإنما اشترط أن يتجسد الاتفاق بأفعال مادية مهما كان هذا الفعل المادي حسب نص المادة 394مكرر 05 من قانون العقوبات الجزائري وهذا لأنها مرحلة تحضيرية للجريمة،

والاتفاق هو صورة للاشتراك المباشر للجريمة[1]، ولا يتحقق الاتفاق إلا بإيجاب من أحد طرفيه واقترانه بقبول من الطرف الآخر[2] ويفهم من الاشتراك عن طريق الاتفاق في هذه الحالة وجود تصرفات مادية فعلية سابقة عن ارتكاب الجريمة أو هي صورة للمساهمة المادية في الجريمة ولا يكفي الاتفاق وحده (مجرد العزم) وإنما يجب أن يتبع بتحضير لجريمة أو أكثر ولا يعاقب عليه إلا بتجسيده بأفعال مادية ايجابية، وتتمثل الأفعال المادية بتبادل المعلومات والأرقام السرية الخاصة بوسائل الدفع مثل رموز الدخول (les codes d'accès)، أو اقتناء أشرطة أو كتب تشرح كيفية إساءة استعمال وسائل الدفع الإلكتروني أو اقتناء برامج اختراق يتم من خلالها الدخول غير المشروع إلى أنظمة التعامل بوسائل الدفع الإلكتروني كما أن الاتفاق الجنائي يعتبر مساهمة تبعية والمساهمة التبعية هي التي يتعدد فيها الجناة في مرحلة سابقة على مرحلة التنفيذ المادي للجريمة، ولا يقومون في تنفيذها بدور رئيسي أو أصلي وإنما بدور تبعي أو ثانوي[3]، فإذا كانت وسيلة الاشتراك هي الاتفاق وجب أن تقع الجريمة نتيجة لهذا الاتفاق فإذا لم تكن الجريمة نتيجة الاتفاق فلا اشتراك[4]، واشترط المشرع الفرنسي التجسيد في أفعال مادية في الحكم العام للاتفاق الجنائي وليس فقط التجسيد في الأفعال المادية في الجرائم الماسة بالمعالجة الالية للمعطيات فقط كما هو الأمر بالنسبة للمشرع الجزائري" **par**

[1]- عبد الرحمان محمد السويلم، المرجع السابق، ص28.

[2]- أشرف عبد الله الضويحي، المرجع السابق، ص 214.

[3]- عبد الرحمان محمد السويلم، المرجع السابق، ص33.

[4]- عبد الرحمان محمد السويلم، المرجع السابق، ص42.

un ou plusieurs faits matériels"[1]، أي للاشتراك في الاتفاق لا يكفي مجردا الانضمام أو الاتفاق بل يجب توافر فعل إيجابي للمشاركة، و اشتراط أن يتم الاتفاق بفعل مادي أو عدة أفعال مادية من السهل أن يتصور في الجرائم العادية و لكنه يصعب تصوره بالنسبة للغش المعلوماتي[2].

التطبيقات القضائية الخاصة تستلزم تحقق مجرد الاتفاق البسيط و ليس المنظم[3] فإذا صدر الايجاب من الطرف الأول لا يصح اعتبار سكوت الطرف الآخر اشتراك لأنه ليس نشاطا ايجابيا، وتضاعف العقوبة في القانون الفرنسي إذا كانت الجرائم مرتكبة ضمن جماعة منظمة واستهدفت معالجة المعطيات ذات الطابع الشخصي[4].

أثار مفهوم المادية جدلا فقهيا في ما مدى اعتبار الأعمال المادية قد تتحقق فقط في صورة بدأ تنفيذ الأعمال التحضيرية[5]؟

تبنى جانب من الفقه الفرنسي مفهوم واسع للمادية أي أن مجرد تبادل المعلومات في صورة مناسبة بحيث يؤدي ذلك إلى تحقيق الجرائم المنصوص عليها يعد كافيا لقيام

---

[1] -l'article 323-4 de code pénale Francis« La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée **par un ou plusieurs faits matériels**, d'une ou de plusieurs des infractions prévues par les articles 323-1à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. » Modifié par la loi N°2004/575 du 21 juin 2004- art 46 JORF 22juin 2004.

[2]-Raymond gassin , op sit ,p40

[3] Jean deveze, op site ,p16

[4]- L'article 323-4-1 de code pénale Francis -« Lorsque les infractions prévues aux articles 323-3 à323-3-1ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 150 000 € d'amende. »

[5]– بورباية صورية ، المرجع السابق ، ص 201 .

الجريمة كتبادل الرموز والكلمات السرية للدخول إلى النظام المعلوماتي، مع العلم أن المعاقبة على الاتفاق الجنائي يطبق فقط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات دون باقي الجرائم المعلوماتية المنصوص عليها في قوانين أخرى.

2- تعدد الجناة في الاتفاق الجنائي كصورة للاشتراك: الحد الأدنى للتعدد هو شخصان بينما لاوجود لحد أقصى حسب نص المادة 394 مكرر 5 من قانون العقوبات الجزائري بشرط أن يكون الجناة مسؤولين جنائيا فإن كان أحد الأشخاص غير مسؤول جنائيا لا يقوم الاتفاق.

3-الركن المعنوي للاتفاق الجنائي كصورة للاشتراك: الاشتراك في الاتفاق الجنائي فعل عمدي بأن يعلم كل عضو في الاتفاق بماهية الفعل أو الأفعال موضوع الاتفاق[1]، أي يشترط لقيام القصد الجنائي لدى أعضاء الجماعة توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية وأن تتجه إرادة ذلك العضو إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري، هذه الجريمة تفترض المساهمة الإرادية في الاتفاق وهذا يفترض أن المساهم يعلم بنشاط الجماعة وهدفها ومع هذا كانت له إرادة الاشتراك فيها و هذا لا يتطلب ضرورة أن يعرف كل فرد في المجموعة بكل نشاطات بقية الأطراف[2].

3-الاشتراك بالاتفاق في الجريمة المرتبطة بوسائل الدفع الإلكتروني :

[1]- أشرف عبد الله الضويحي، المرجع السابق، ص 226.

[2]-Jean deveze, op, cit.P17

- اتفاق شخصين أو أكثر على ارتكاب جريمة مرتبطة بوسائل الدفع الإلكتروني .

- وقوع الجريمة المرتبطة بوسائل الدفع الإلكتروني بناء على هذا الاتفاق إما كاملة أو شروع حتى يعتبر المتفق على الجريمة شريكا فيها، أي لابد أن يترتب على اتفاقه نتيجة يعاقب عليها القانون وتتمثل هذه النتيجة في وقوع الجريمة التي اتفق عليها تامة أو في صورة شروع وبالتالي يشترط لعقاب الشريك بالاتفاق أن تقع الجريمة بناء على الاتفاق.

الفرع الثالث

إشكالية تمديد الاشتراك بالاتفاق الجنائي لجرائم وسائل الدفع الإلكتروني

باعتبار التعامل بوسائل الدفع الإلكتروني يستلزم خلق نظام معلوماتي خاص ففي حالة وقوع أي جريمة من جرائم المساس بأنظمة المعالجة الآلية لمعطيات هذا النظام أو النظام المعلوماتي للبنك ككل عن طريق الاتفاق الجنائي لا تواجهنا أي إشكالية بصدد تطبيق حالة الاتفاق الجنائي المنصوص عليها ضمن المادة 394 مكرر05 من قانون العقوبات الجزائري، و لكننا نتساءل بخصوص مدى تطبيقها على باقي الجرائم الإلكترونية المتعلقة بوسائل الدفع الإلكتروني وهو ما سنناقشه (أولا)، ونتطرق إلى موقف المشرع الفرنسي الذي تبنى اضافة لأحكام الاتفاق العامة الواردة في قانون العقوبات، العصبة الاجرامية واعتبرها ظرفا مشددا ضمن نصوص قانون النقد والمال الفرنسي (ثانيا).

أولا/ إشكالية تمديد الاشتراك بالاتفاق الجنائي لباقي جرائم وسائل الدفع الإلكتروني

وسع المشرع الجزائري الاشتراك عن طريق الاتفاق الجنائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فقط، وبالتالي تثور الإشكالية بالنسبة للجرائم التي لم تشملها هذه النصوص كجرائم تزوير أو تبيض الأموال أو التهرب الضريبي عن طريق استعمال وسائل الدفع الإلكتروني وهي الجرائم التي سنفصلها من خلال هذا الباب من المذكرة، وإن كان بإمكان القاضي تطبيق نصوص المساس بمعالجة الأنظمة المعلوماتية إلا أنه سيواجه إشكالية على أساس اختلاف الغاية من التجريم لهذه الجرائم والتزوير وتبيض الأموال والتهرب الضريبي، فهل سيأخذ القاضي بمبدأ تفسير النصوص أو أنه سيحكم بالبراءة استنادا إلى مبدأ الشرعية، أم أنه سيضطر إلى العودة إلى الأحكام العامة للاشتراك في قانون العقوبات الجزائري وهو الحل الأنسب في اعتقادنا، وبالتالي نحن في الجزائر بحاجة إلى نص تشريعي لتوضيح هذه المسألة حتى لا يفلت المجرمون من العقاب، أو على الأقل النص على الاتفاق الجنائي كصورة للاشتراك في الجرائم المتعلقة بالدفع الإلكتروني لأنه صورة مهمة للاشتراك.

ثانيا/ العصبة الإجرامية ظرف مشدد لجرائم وسائل الدفع الإلكتروني في القانون الفرنسي

اعتبر المشرع الفرنسي العصبة الإجرامية ضمن نصوص قانون النقد والمال الفرنسي في الجرائم المرتكبة بوسائل الدفع الإلكتروني ظرفا مشددا لأن العلاقة بين الجرائم المرتكبة بوسائل الدفع الإلكتروني والإجرام المنظم تقتصر على الطريقة التي يتم بها ارتكاب هذه

الجرائم باعتمادها على التنظيم، بالعودة إلى نص المادة L163-4-2 من قانون النقد والمال الفرنسي نجد أن العقوبة تضاعف لتصل إلى عشر سنوات حبس ومليون أورو غرامة مالية عندما تكون الجرائم المحددة بالمواد L163-3 ،L163-4، L163-4-1 تشكل عصبة اجرامية وهذه الجرائم هي التي أوردناها في هذا الباب من المذكرة وتتعلق بالتقليد والتزوير لوسائل الدفع الإلكتروني، أو الاستعمال لوسائل الدفع الإلكتروني المقلدة والمزورة، أو القبول لوسائل دفع إلكتروني مقلدة أو مزورة...الخ، والتي سيأتي التفصيل بشأنها لاحقا في هذا الباب، وعرف المشرع الفرنسي العصبة الإجرامية في المادة 132-71 من قانون العقوبات

« Constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions. »

يشكل في مفهوم هذا القانون عصبة اجرامية كل تجمع أو اتفاق الغرض منه الاعداد لجريمة أو أكثر بفعل أو أكثر من الأفعال المادية.

المبحث الثاني

المسؤولية الجزائية عن الاشتراك في الاحتيال بوسائل الدفع الإلكتروني

تتعدد وتتباين التعاريف للاحتيال المعلوماتي، أو كما يسميه البعض غش الحاسب الآلي، ويرد هذا التباين إلى تحديد الأفعال المنطوية تحت هذا

الوصف، وعرفته في المملكة المتحدة لجنة (أوديت)، المكلفة بدراسة الاحتيال المعلوماتي على أنه سلوك احتيالي أو خداعي مرتبط بالحاسب يهدف شخص بواسطته كسب فائدة أو مصلحة مالية، وقد أثنى الباحثون والدارسون على تعريف لجنة أوديت باعتباره أفضل المفاهيم للاحتيال المعلوماتي لأنه ينصب على معطيات الحاسوب المخزنة في النظام والممثلة لأموال أو أصول أو خدمات ويهدف الجاني فيها إلى تحقيق مكسب أو مزية وتتم بالتلاعب وفق الدلالة التقنية الواسعة بمعطيات الحاسب الآلي المخزنة في نظام المعالجة الآلية[1].

ويمكن تعريفه بأنه التلاعب العمدي بمعلومات أو بيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أي وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات بهدف الحصول على ربح غير مشروع وإلحاق ضرر بالغير.

هذه الجريمة تقليدية كثيرة الوقوع في العمل المصرفي ولكن مع التقنيات الحديثة التي أدخلت على العمل المصرفي تنامت، بتجريم الاحتيال المعلوماتي يضمن المشرع حماية

[1]- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية، أطروحة دكتوراه في القانون، الجامعة الاسلامية، لبنان، لبنان، 2004، ص294.

لحق الملكية وحماية لحرية الإرادة وسلامتها[1]، أصبحت النصوص التقليدية قاصرة عن استيعاب جريمة الاحتيال المعلوماتي (مطلب أول)، وتحديد الركن المادي للاشتراك في الاحتيال بوسائل الدفع الإلكتروني (المطلب الثاني)، ومكانة الضرر والقصد في الاحتيال المعلوماتي (مطلب ثالث)، في (المطلب الرابع) نناقش إساءة استعمال وسائل تقنية المعلومات وإشكالية تسهيل العمليات الاحتيالية.

المطلب الأول

المسؤولية الجزائية عن الاشتراك في الاحتيال المعلوماتي

بين قصور النصوص التقليدية وضرورة التدخل التشريعي

إن تطوق (لامادية) وسائل الدفع الإلكتروني كانت الأصل لظهور نوع جديد من الجرائم[2]، ونشير إلى أن الشيك كأداة دفع قد بدأ في نفس الظروف حيث لم تكف المسؤولية المدنية وكذلك النصوص الجنائية الخاصة بالنصب والاحتيال لتحقيق الحماية الفعالة له مما استوجب تدخل المشرع في العديد من الدول لتقرير المسؤولية الجزائية

[1]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية ' دراسة نظرية '، منشورات الحلبي الحقوقية، ص 420.

[2] -Michel Espagnon, système carte bancaire « cb » et dématérialisation transferts électroniques de fonds les paiement par wap, actes des journées d'études le 18 /11/1999-05/10/2000, organisé par l'association luxembourgeoise des juristes de banque, le centre de recherches informatique et droit (CRID) la faculté de droit de Namur et l'association européenne pour le droit bancaire et financier belgium (ABDBF-belgium), cahiers aedbf /evbfr-belgium, bruyant Bruxelles, 2001, p218.

بنصوص جديدة (جريمة اصدار شيك بدون رصيد) وهي جريمة ظهرت نتيجة قصور فعل الاحتيال والنصب عن استيعاب فعل اصدار شيك بدون رصيد.

تبقى المسألة تحتم على المشرع التدخل بنصوص صريحة لتوفير الحماية الجنائية لوسائل الدفع الإلكتروني و بالتالي أول ما يتبادر إلى أذهاننا هو ما مدى إمكانية تطبيق النصوص القانونية للقانون الجنائي التقليدي المتعلقة بالاحتيال على الجرائم المرتكبة بوسائل الدفع الإلكتروني باعتبارها وسائل لاستعمال مال معنوي معلوماتي له خصوصياته التي تميزه عن الأشياء المادية؟ وهل يستطيع القاضي الجزائي من خلال النصوص العقابية لجريمة الاحتيال تحقيق حماية جزائية لوسائل الدفع الإلكتروني دون الإطاحة بالمبادئ التي يرتكز عليها القانون الجنائي(الفرع الأول)، وما مدى نجاعة نصوص المساس بالمعالجة الآلية للمعطيات وضرورة النص الجديد للحماية من الاحتيال المعلوماتي (الفرع الثاني)، والحاجة إلى نص تشريعي جديد لاستيعاب جريمة الاحتيال المعلوماتي في القانون الجزائري (الفرع الثالث)، وشمول المسؤولية الجزائية عن الاشتراك بالاحتيال المعلوماتي للاشتراك في الاحتيال بوسائل الدفع الإلكتروني (الفرع الرابع)، وأخيرا نناقش مدى تعارض العقاب عن الاحتيال المنظم بوسائل الدفع الإلكتروني مع المبادئ الأساسية للمسؤولية الجزائية (الفرع الخامس).

الفرع الأول

نصوص الاحتيال التقليدية قاصرة عن استيعاب الاحتيال بوسائل الدفع الإلكتروني

تم التركيز على جريمة الاحتيال المعلوماتي بوسائل الدفع الإلكتروني لأنه تم النص على هذه الجريمة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر وحتى نستطيع التأسيس للركن الشرعي لهذه الجريمة وتفاديا للغوص في الآراء الفقهية التي تناولت إمكانية التكييف للجرائم المتعلقة بوسائل الدفع الإلكتروني ضمن النموذج التقليدي لجرائم الأموال و إشكالية هل سنتمكن من تطبيق النص التقليدي أم لا بالمقارنة بين الاحتيال في صورتيه التقليدية والإلكترونية نجد أن جوهرهما واحد فكلاهما يهدف إلى الحصول على ربح غير مشروع باستعمال وسائل احتيالية إلا أن الاختلاف يكمن في نوع هذه الوسائل الاحتيالية وفي محل السلوك الاجرامي، و للتفرقة وعدم الخلط بين جريمة الاحتيال الإلكتروني بوسائل الدفع الإلكترونية التي يكون هدفها تحقيق ربح مادي غير مشروع في حين أن جريمة التلاعب بالبيانات تهدف إلى اظهار القدرات والمهارات التقنية وهذه الأخيرة تعتبر من أسباب ارتكاب الاحتيال الإلكتروني.

يمكن أن نقسم الاحتيال في العمليات المصرفية إلى نوعين الأول هو الاحتيال المصرفي التقليدي والثاني هو الاحتيال في مجال أنظمة المدفوعات وبطاقات الدفع[1]، والاحتيال في مجال الدفع الإلكتروني يعتمد على استخدام أساليب وتقنيات ومعارف وبرامج متطورة، وتولي المصارف أهمية بالغة لمكافحة هذا النوع من الاحتيال بتطوير الحماية

[1]- علي نحلة، النشاطات المشبوهة غسل الأموال الإلكتروني، اليات كشفها وكيفية التعرف عليها والتبليغ عنها، مجلة اتحاد المصارف العربية، يونيو 2005، ص71.

التقنية للحفاظ على ثقة الزبائن وتوعيتهم وارشادهم حول كيفية استخدام وسائل الدفع الإلكتروني.

قد يأتي الخطر من العاملين في هذه الخدمة والحقيقة أن احتيال العاملين يمكن أن ينشأ في العمل المصرفي التقليدي والإلكتروني معا إلا أنه يمكن أن يتم اكتشاف الاحتيال في العمل التقليدي واثباته بصورة أسهل عن تلك التي تكون في المجال الإلكتروني حيث يلجا بعض العاملين في المجال الإلكتروني لإجراء تغيير في البيانات من أجل سحب مبالغ من الحسابات البنكية أو الحصول على المعلومات من سجلات البنك تؤدي إلى الإضرار بوضع البنك[1].

ثار جدل فقهي[2]حول ضرورة استحداث نصوص عقابية لتجريم الاحتيال المعلوماتي من عدمه حيث أن هذا الأخير لا يختلف عن الاحتيال التقليدي وبالتالي امكانية تطبيق النصوص التقليدية على الاحتيال المعلوماتي هناك اتجاه عارض امكانية تطبيق وقوع فعل الاحتيال على الحاسب الآلي لأن جريمة النصب تستوجب أن يكون الجاني والمجني عليه أشخاص طبيعيين، في حين يؤيد اتجاه ثاني امكانية الاحتيال على

[1]- حسن شحادة الحسين، العمليات المصرفية الإلكترونية (الصيرفة الالكترونية)، بحث مقدم إلى الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، الجزء الأول الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، ص212.

[2]- نهلا عبد المومن، المرجع السابق، ص 168، يونس عرب، ورقة عمل "صور الجرائم الالكترونية واتجاهات تبويبها "، مقدمة الى ورشة عمل "تطوير التشريعات في مجال مكافحة الجرائم الالكترونية "، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 2-4أفريل 2006.

الحاسب الآلي وايقاعه في الغلط والواقع أن الاتجاه الثاني الذي قال بإمكانية وصلاحية البرامج والمعلومات للاحتيال هو الراجح.

تعد جريمة الاحتيال من جرائم الأموال والتي يهدف المشرع بتجريمه اياها إلى حماية حق الملكية، إن النصوص القانونية التقليدية التي وضعت لمواجهة جريمة الاحتيال تفترض بأن الطرق الاحتيالية لابد أن تقع بين شخصين طبيعيين[1]، مما يدفعنا إلى القول بأن الطرق الاحتيالية التقليدية نطاقها العلاقات الانسانية في حين أن الطرق الجديدة للاحتيال المعلوماتي لا يمكن أن تشملها النصوص التقليدية نظرا لطبيعة الآلات والبيانات والمعلومات والبرامج التي تقع عليها وليس الأشخاص الطبيعية، ولهذا لابد من استحداث نصوص عقابية تجرم الاحتيال المعلوماتي وبالتالي ضرورة النص الجديد على الاحتيال بوسائل الدفع الإلكتروني كجريمة مستقلة لأن محاولة تطويع النصوص التقليدية تجعلنا نصطدم بمبادئ القانون الجنائي، إلا أنه من الواجب الإسراع دون تباطأ نحو سن نصوص جزائية خاصة بتجريم هذا السلوك بصفة صريحة، أو السعي نحو تعديل النصوص الحالية بحيث تستوعب في إطارها التجريمي الاحتيال على الأموال المعلوماتية المعنوية والاحتيال المصرفي الإلكتروني والاحتيال بوسائل الدفع الإلكتروني بصفة خاصة حتى لا نصطدم بمبدأ الشرعية الجنائية.

[1]- نهلا عبد المومن، المرجع السابق، ص168.

بالعودة إلى نص المادة 372 من قانون العقوبات الجزائري نجدها نصت على المنقول دون تحديد لطبيعته ودون أن يقيده المشرع بأن يكون ماديا إلا أنه حتى وإن أخذنا بهذا التفسير نصطدم بعدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام وحتى على فرض أن التسليم قد تم فإن وسائل الدفع الإلكتروني تبقى بحوزة المجني عليه لا يحرم من حيازة وسيلة الدفع الإلكتروني التي تبقى خاضعة لسيطرته كما لا يحرم البنك من حيازة البرامج والبيانات التي تبقى تحت سيطرة البنك، ويعرف الاحتيال بالوسائل الإلكترونية بأنه كل تصرف احتيالي يهدف من خلاله أحد المجرمين تحقيق مكاسب مالية عبر الوسائل الإلكترونية.

ما مدى امكانية اعتبار الوسائل التقنية المستخدمة في الاحتيال المعلوماتي من قبيل الطرق التقليدية للاحتيال المنصوص عليها في المادة من قانون العقوبات الجزائري ؟

الاحتيال التقليدي يتم بالطرق التي حددتها المادة 372 من قانون العقوبات الجزائري وهي استعمال أسماء كاذبة، استعمال صفات غير موجودة، استعمال وسائل احتيالية (سلطة خيالية أو اعتماد مالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية ، الاستيلاء على الأموال عن طريق اللجوء إلى الجمهور بقصد إصدار أسهم أو سندات أو اذونات أو حصص أو أية سندات مالية سواء شركات أو مشروعات تجارية أو صناعية ...).

على فرض تسليمنا بأن الطرق الاحتيالية المستخدمة في الاحتيال المعلوماتي مشمولة بنص المادة السالف الذكر إلا أن ذلك لا يمكننا من تطبيقها لأن الطرق الاحتيالية وضعت لتكون في إطار العلاقات الانسانية فتسليم الشيء يجب أن يتم تحت تأثير الطرق الاحتيالية التي استعملها الجاني و بإرادة مؤثر عليها للمجني عليه.

فالطرق الاحتيالية يجب أن تكون في مواجهة إنسان آخر وليس آلة وذلك وفقا للمفهوم التقليدي لجريمة الاحتيال[1]، ومنه فإن تطبيق هذا النص قد يتعارض أحيانا والطابع الخاص للوسائل المعلوماتية المستحدثة لتنفيذ الجريمة[2].

بالتالي على المشرع الجزائري ونتيجة عجز النص التقليدي للمادة عن استيعاب طرق الاحتيال الإلكتروني لابد أن يقوم بالنص صرحة على تجريم هذا الفعل.

الفرع الثاني

مدى نجاعة نصوص المساس بالمعالجة الآلية للمعطيات

وضرورة النص الجديد للحماية من الاحتيال المعلوماتي

اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وعرفها بنص المادة 02 من قانون04/09 "بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة

[1]– نهلا عبد المومن، المرجع السابق، ص 171.

[2]– محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، 2008، مصر، ص99.

هذا النوع من الجرائم إذا ارتبطت بوسائل الدفع الإلكتروني لأنها غالبا ما تكون جرائم ذات طابع مالي، مختلف التكيفات الجنائية لفعل التاجر حول تصليف الاستعمال

الاحتيالي للمعطيات يمكن أن يشكل للحامل أو للمصدر دخول غير شرعي للمعطيات الموجودة في البطاقة حيث يمكن أن تشكل نصب واحتيال[1].

4-إعاقة أنظمة المعالجة الآلية للمعطيات المرتبطة بوسائل الدفع هو تخريب (عرقلة أو فتك) يمس خادم الإعلام الآلي للمعطيات التي تمكننا من استعمال هذه الوسائل، وهذا ينتج عنه استحالة تامة أو خاصة لاستعمال النظام خاصة في حالة التوقيف لرمز الدخول أو اعاقة عمل النظام، إعاقة عمل النظام يمكن أن يتحقق نتيجة إرسال الفيروسات، القنابل وهي أنظمة تظهر وتختلف من واحد لآخر من حيث المصطلحات والمحتوى أو النتيجة أو النوع الآلي[2].

مثلا: إرسال ضخم لرسائل الكترونية أو(mail bombing) بهدف وقف خادم (serveur) الإعلام الآلي المبعوث إلكترونيا يمثل إعاقة لعمل نظام المعالجة الآلية وبالنتيجة في هذه الحالة إعاقة النظام عن المعالجة الآلية للمعطيات سواء لمؤسسات الدفع أو زبائنها لا تستطيع الدخول للمعطيات البنكية المتعلقة بوسائل الدفع الإلكتروني[3].

---

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 261-262

[2]- Hatem Adnan Bezzo, op, cit , p196.

[3]– Hatem Adnan Bezzo, op, cit, p197.

تعرف المادة الحادية عشر من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر جريمة الاحتيال بأنها:

" **التسبب بالحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير**، عن طريق:

1-ادخال أو تعديل أو محو أو حجب للمعلومات أو البيانات.

2-التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3-تعطيل الأجهزة والبرامج والمواقع الإلكترونية ".

بالمقارنة بين هذه المادة والمادة 372 من قانون العقوبات الجزائري نجد أنها تتضمن وسائل الاحتيال الجديدة والتي هي عبارة عن جرائم متفرعة ورد ذكر بعضها في المواد المتعلقة بالمساس بالمعالجة الآلية للمعطيات، وبالعودة إلى هذه المواد لا نستطيع متابعة الفاعل على أساسها بجريمة الاحتيال عن طريق وسائل الدفع الإلكتروني لغياب عنصر الحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير، مما يستلزم على المشرع الجزائري وضع نص خاص للعقاب على الاحتيال المعلوماتي حتى لا نصطدم بمبدأ الشرعية الجزائية لأنه غالبا ما تكون نية تحقيق الربح هي الهدف الذي يتم لأجله المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بوسائل الدفع الإلكتروني.

والتلاعبات المعلوماتية الاحتيالية تكون مجرمة إذا سببت مباشرة للغير ضررا اقتصاديا أو ماديا أو يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير[1]

الفرع الرابع

شمول المسؤولية الجزائية عن الاشتراك في الاحتيال المعلوماتي للاشتراك في الاحتيال بوسائل الدفع الإلكتروني

الجرائم التي تستهدف أنظمة التحويل الإلكتروني للأموال والودائع المصرفية تمثل بإجماع الفقه أخطر جرائم غش الحاسوب وهذا يرجع إلى المبالغ الهائلة المتجسدة في هذه البيانات التي يجري نقلها بوقت قياسي وإلى شيوع استخدام تقنيات النقل الإلكتروني للأموال التي تهيء نشوء مجتمع التعامل دون نقود، ويثور بخصوص تطبيق جريمة الاحتيال على الاحتيال بوسائل الدفع الإلكتروني مسألتين: **الأولى** تتمثل في ما مدى جواز الاحتيال على الحاسب الآلي **والثانية** تتمثل في مدى اعتبار الأموال المتداولة عبر وسائل الدفع الإلكتروني من قبيل الأموال التي يرد عليها الاستيلاء، إلا أننا سنركز على المسألة الثانية ومناقشة الطرق الاحتيالية باعتبارها ذات صلة بالموضوع وباعتبار الجزائر صادقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مما يعني الاقرار ضمنيا بجريمة الاحتيال المعلوماتي وفي انتظار التدخل بالنص الصريح من طرف

[1]-هلالي عبد اللاه أحمد، المرجع السابق، ص103.

المشرع الجزائري والحسم نهائيا في مسألة مدى جواز الاحتيال على الحاسب الآلي، وحتى لا نطيل بسرد الآراء الفقهية المتعلقة بالمسألة و ننتهي بترجيح الرأي القائل بجواز الاحتيال على الحاسب الآلي، سنركز مباشرة على المسائل المتعلقة بوسائل الدفع الإلكتروني وجريمة الاحتيال المعلوماتي.

أثير التساؤل حول ما مدى جواز الاحتيال على الآلة ؟ونتساءل بدورنا عن مدى جواز الاحتيال على الحاسب الآلي باعتبار أنه هو من يعوض المجني عليه في الدفع عن طريق وسائل الدفع الإلكتروني ؟

أعمل القضاء الفرنسي فكرة الاحتيال على الحاسب الآلي عندما قضى بتوافر تلك الجريمة في حق المتهم الذي أعطى أمرا إلى الحاسب الآلي بتحويل مبالغ نقدية من الشركة التي يعمل بها لحساب شركة أخرى يسيطر عليها، وذلك للاستيلاء عليها لنفسه، كما استقر القضاء الفرنسي على وقوع جريمة الاحتيال إذا سحب المتهم مبالغ نقدية من حساب شخص غيره باستخدام بطاقة السحب الآلي لهذا الشخص، أو إذا قام بتسديد ثمن مشترياته باستعمال بطاقة غيره الخاصة بالسحب الآلي.

يثور التساؤل حول مدى اعتبار (القيد الكتابي) للأموال عن طريق وسائل الدفع الإلكتروني من قبيل التسليم المحقق لنتيجة السلوك في جريمة الاحتيال ؟

يجب التمييز بين حالتين أولهما إذا كان محل الاستيلاء نقودا أو أصولا كتوصل الجاني إلى معرفة الرقم السري لصاحب بطاقة ائتمان مسروقة ويستخدمها في السحب من

أجهزة الصرف الآلي للنقود ففي هذه الحالة لا يثور أي اشكال حول جريمة الاحتيال التقليدية، أما في الحالة التي يتم بها الاستيلاء عن طريق القيد الكتابي ومثالها تلاعب الجاني في البيانات المخزنة في الحاسوب أو في برامجه كي يحول كل أو بعض أرصدة الغير أو فوائدها إلى حسابه فهنا نتساءل بشأن تحقق نتيجة الجريمة باستلام المال والاستيلاء عليه مرهون بنطاق النص القانوني، إلا أنه وبالاستناد إلى اعتبار التسليم غير متطلب له المناولة المادية حسب ما هو مستقر في الفقه المصري والفقه الفرنسي ولأن محكمة النقض الفرنسية قد توصلت في بعض أحكامها بين تسليم النقود وبين الدفع الذي يتم عن طريق القيد الكتابي، فلقد ابتكرت نظرية جديدة تعرف باسم نظرية التسليم المعادل[1]، إلا أننا نرى أن التسليم المادي يتحقق بالنسبة لجرائم الاحتيال بواسطة وسائل الدفع الإلكتروني حسب المادة 372من قانون العقوبات الجزائري التي لم تشترط أن يكون التسليم مادي بل الاكتفاء بما يعادل التسليم.

ونظرية التسليم المعادل (التي أرستها محكمة النقض في فرنسا)، وقام الفقه بتطبيقها على جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسب الآلي والتي تؤدي إلى الغاء رصيد دائن، أو من باب أولى خلق رصيد دائن بمبالغ غير مستحقة وتتعدد الأساليب المستخدمة في هذا الشأن، فقد يحدث ذلك عن طريق التقاط أمر التحويل بواسطة الجاني، وتزييفه بالأمر بتحويل نفس المبلغ لحسابه الخاص، أو

[1]– والتي وضعت لمواجهة حالات الاحتيال الواقعة على ضريبة المبيعات وعلى عداد موقف السيارات وعلى الهواتف، أنظر نهلا عبد المومن، المرجع السابق، ص170.

عن طريق التلاعب في عملية البرمجة بغرض تحويل فوائد حساب شخص ما إلى حساب الفاعل، وأخيرا عن طريق انتحال الفاعل لشخصية الغير ومباشرته لعملية تحويل النقود[1].

ومن ثم رأى الفقه الفرنسي أن التسليم قد يكون محله مالا معنويا إلى جانب المال المادي، والأموال المعنوية أو الخدمات كلها نماذج لتطور المعلوماتية، وبذلك يهدف المشرع الفرنسي إلى حماية قيم أو كيانات ذات قيمة مالية، لكنها ليست نقودا مادية يمكن قبضها، لكن يمكن تحويلها إلى نقود مادية[2].

وننتهي إلى نتيجة مفادها أن نظرية التسليم المعادل la théorie remise par équivalent التي ابتدعها القضاء الفرنسي يمكن تطبيقها على الاحتيال الواقع بجميع وسائل الدفع الإلكتروني لأن محكمة النقض الفرنسية اعتبرت أن مجرد القيد الكتابي jeu d'écriture كاف لإتمام الدفع و لأن الدفع الإلكتروني يتم بمجرد القيد الكتابي وبالتالي فهو يعادل التسليم للنقود.

الفرع الخامس

مدى تعارض العقاب على الاحتيال المنظم بوسائل الدفع الإلكتروني

مع المبادئ الأساسية للمسؤولية الجزائية

[1]- محمد سامي الشوا، بحث بعنوان الجرائم المعلوماتية للتعدي على الذمة المالية للغير، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الرابع، ص1106.

[2]- محمد الشناوي، المرجع السابق، ص107.

تطورت أساليب الاحتيال الإلكتروني مع التطور التكنولوجي للمعلوماتية خاصة ما شهدته بطاقات الائتمان والدفع الإلكتروني بأنواعها المختلفة من تطور، فقد ازداد الاعتماد على هذه البطاقات خاصة بعد تنامي حجم الأعمال التي تتم من خلال التجارة الإلكترونية وظهور الأسواق الإلكترونية لتسويق وبيع السلع والخدمات وقد تحولت أساليب الاحتيال من مجرد جرائم فردية تعتمد على اقتناص الفرص إلى جرائم منظمة تعتمد على التخطيط المسبق والخبرات الفنية العالية في مجال المعلوماتية[1]، ويبقى الاحتيال عن طريق البطاقات وإن لم يكن له قانون خاص في الدول العربية على عكس الولايات المتحدة الأمريكية والدول الأوربية فإنه يتدرج تحت بند الاستيلاء على المال بطريقة غير شرعية مما ثبت من بعض الوقائع، كما هناك عصابات متخصصة في هذا المجال تتخذ من هذا النوع من الجرائم طريقة جديدة لتمويل عملياتها كغسيل الأموال وتجارة المخدرات والعمليات الإرهابية.

أولا / الاشتراك في عصابة غرضها الاحتيال بوسائل الدفع الإلكتروني

إذا أدخلنا تجريما للجريمة المنظمة بطريق الاحتيال أي عاقب المشرع على الانضمام لعصابة من أغراضها الاحتيال على الغير للاستيلاء على أمواله، لأن مجرد فعل الانضمام إلى تلك العصبة يكون معاقبا عليه دون اشتراط القيام الفعلي بالاحتيال على

[1]– مصطفى محمد بيطار، دور التشريعات الجنائية في الوقاية من الاحتيال المنظم، بحث مقدم إلى الندوة العلمية العلاقة بين جرائم الاحتيال والاجرام المنظم، مركز الدراسات والبحوث قسم الندوات و القاءات العلمية، جامعة نايف العربية للعلوم الأمنية، المنعقدة في 03-05 /1428/06 الموافق لـ18-20 /2007/06.

الغير ،ومن ثم إذا مارس أعضاء العصابة احتيالا بالفعل فإنهم يرتكبون جريمتين، الجريمة الأولى هي جريمة تكوين عصابة إجرامية يكون من ضمن هدفها الاحتيال على الغير وجريمة الاحتيال على الغير[1].

ثانيا / العقاب على الاحتيال المنظم ومبدأ الشرعية

يترتب على مبدأ الشرعية ضرورة وجود نص قانوني يجرم الفعل بشكل واضح يحول دون إبهامه أو اثارة الشكوك في التفسير حوله.

يثور التساؤل حول احترام مبدأ الشرعية في حالة النص على تجريم الاحتيال المنظم أو النص على الجريمة المنظمة التي من أغراضها ممارسة الاحتيال؟

تأتي المشكلة المتعلقة بمبدأ الشرعية من عدة أوجه:

أولا –هل يكفي في تجريم الانضمام إلى عصبة اجرامية تتخذ الاحتيال نشاطا رئيسيا لها أو يدخل الاحتيال ضمن أنشطتها الرئيسية أي هل تكفي واقعة الانضمام دون استلزام أن يرتكب المتهم العضو فعلا يجعله فاعلا أو شريكا في الاحتيال ؟

و تأتي الخشية من موقف التشريعات ما يكتفي بأن تشكل العصابة الاجرامية المنظمة دون اشتراط أن تقع أفعال اجرامية مادام أنها تكونت بقصد ارتكاب تلك الأفعال[2]، وهذا

---

[1]–غنام محمد غنام، طبيعة العلاقة بين جرائم الاحتيال والجريمة المنظمة، بحث مقدم إلى الندوة العلمية "العلاقة بين جرائم الاحتيال والاجرام المنظم، من تنظيم مركز الدراسات والبحوث قسم الندوات والقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، المنعقدة بتاريخ 03-05 /1428/06 الموافق ل18-20 /06/ 2008.

[2]- غنام محمد غنام، طبيعة العلاقة بين جرائم الاحتيال والجريمة المنظمة، بحث مقدم إلى الندوة العلمية "العلاقة بين جرائم الاحتيال والاجرام المنظم، من تنظيم مركز الدراسات والبحوث قسم الندوات والقاءات العلمية، المرجع السابق.

هو نفس النهج الذي انتهجه المشرع الجزائري من خلال نص المادة 176من قانون العقوبات الجزائري، إلا أن هناك من التشريعات ما يستلزم أن تقع أفعال مادية لارتكاب تلك الجرائم أي لا يشترط أن تقع في هذه الحالة جريمة الاحتيال والتزوير لوسائل الدفع الإلكتروني.

ولوضوح النص الجنائي وتطبيقا لمبدأ الشرعية يتعين على المشرع إدراج حالات الاحتيال والتزوير الإلكترونيين نظرا لخطورتهما ضمن الجرائم التي تدخل ضمن أنشطة الجريمة المنظمة لكي يمكن اعتبارها جرائم منظمة .فالوضع في القانون الجزائري يختلف عما هو مقرر في القانون الفرنسي حيث يجب ارتكاب فعل إجرامي وفقا للقانون الفرنسي للعقاب على الانضمام إلى العصابة الاجرامية بينما يكفي وفقا للقانون الجزائري مجرد الاتفاق.

لاحظنا أن الفقه والقضاء في الدول المتقدمة حاول تطويع النصوص التشريعية التقليدية في محاولة لمد سريانها على هذا النوع الجديد من الجرائم ولكن اتضحت صعوبة التطبيق قضائيا على جرائم الاحتيال المعلوماتي وبالتالي على المشرع الجزائري تعديل قانون العقوبات ليشمل جريمة الاحتيال المعلوماتي كما عليه اجراء تعديلات وإصدار قوانين خاصة لمواجهة هذا النوع من الاحتيال المتطور والخاص بوسائل الدفع الإلكتروني وهذا نظرا للطبيعة الخاصة التي تتميز بها هذه الجريمة في مجال الدفع الإلكتروني.

تظهر الطبيعة الخاصة لطرق الاحتيال المعلوماتي بوسائل الدفع الإلكتروني وهي التي سنفصل فيها باعتبارها طرق جديدة (الفرع الأول) ثم المحل في هذه الجريمة (الفرع الثاني).

المطلب الثاني

الركن المادي للاشتراك في الاحتيال بوسائل الدفع الإلكتروني

يمكن ارتكاب جريمة الاحتيال المعلوماتي بمساعدة العاملين في البنوك الذين يملكون التقنية والكفاءة العالية للتلاعب بالبيانات المتعلقة بوسائل الدفع الإلكتروني أو المبرمجين الذين تلجأ إليهم البنوك لتحديث برامج العمل بوسائل الدفع الإلكتروني، وتشير المذكرة التفسيرية لاتفاقية بودابيست إلى أنه مع حدوث الثورة التكنولوجية تضاعفت إمكانية ارتكاب جرائم اقتصادية، كالغش وخاصة النصب ببطاقات الائتمان كما أن الأصول الممثلة أو المتداولة عن طريق النظم المعلوماتية كالأموال الالكترونية أو الودائع أصبحت هدفا لتلاعبات بنفس الاشكال التقليدية للملكية[1]، هذه الجرائم تتم من خلال التلاعب بمدخلات النظام المعلوماتي لوسائل الدفع الإلكتروني أو البرامج التي تعمل بها هذه الوسائل أو من خلال التدخل في معالجة البيانات الخاصة بالدفع الإلكتروني.

الشريك المحتمل لارتكاب الاشتراك في الاحتيال بوسائل الدفع الإلكتروني يمكن أن يكون أحد العاملين بالبنك وغالبا ما يكون من الذين لهم سلطة على ادخال البيانات

[1]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 325.

على وسيلة الدفع الإلكتروني وهؤلاء يتم اكتشافهم عن طريق المراجعة للبرامج، أو معدي المعلومات وخبراء البرمجة (سواء برامج العمل المعلوماتية للبنك ككل وهو المبرمج العام ويتم اكتشافه عادة عند إجراء تعديل لجزء معين من البرنامج، أو مبرمج العمل بوسيلة دفع إلكتروني معينة) لهذا سنركز على الطبيعة الخاصة لطرق الاحتيال المعلوماتي بوسائل الدفع الإلكتروني (الفرع الأول) مع امكانية أن يتم الاشتراك من حامل وسيلة الدفع الإلكتروني أو أي شخص يسعى لتحقيق الربح، ثم نتطرق للإشكالات التي يثيرها المحل في الاحتيال بوسائل الدفع الإلكتروني (الفرع الثاني).

الفرع الأول

الطبيعة الخاصة لطرق الاحتيال المعلوماتي بوسائل الدفع الإلكتروني

صور الاحتيال المعلوماتي في ازدياد مستمر نتيجة زيادة الاعتماد على الأنظمة الإلكترونية في تحويل ونقل الأموال وتسارع وتيرة تحول المجتمع إلى مجتمع لا يتداول النقود ولا الشيكات[1] في ظل انتشار التعامل بوسائل الدفع الإلكتروني التي يتم من خلالها التحويل من حساب للآخر عبر الأنظمة المعلوماتية المتطورة للبنوك كما ساهم تطوير وظائف أجهزة الصرف الآلي والبنوك الإلكترونية في جعل المعاملات المالية في المجتمع بغير نقود.

[1]- غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص295.

المشرع الجزائري الذي لم يورد نصا خاصا بالاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات ولم يعتبرها جريمة مستقلة واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام، يمكن رد ذلك لأنه اعتبر برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية وتحدث عنها كظرف مشدد لجريمة الدخول والبقاء في المادة 394 مكرر الفقرة 03 من قانون العقوبات الجزائري[1]، فالتشريعات اتجهت اتجاهين هناك تشريعات أفردت لها نص خاص واعتبرتها جريمة مستقلة وهناك تشريعات اعتبرتها كظرف مشدد كما هو الحال بالنسبة للمشرع الجزائري والذي استعمل مصطلح التخريب.

الأكيد أن المشرع نص على الاعتداء على المعلومات كجريمة مستقلة في المادة 394 مكرر 01 من قانون العقوبات الجزائري "...كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[2]، ونلاحظ أن المشرع استعمل مصطلح المعطيات ولم يحدد نوعية المعطيات.

حصر المشرع الجزائري صور الركن المادي لهذه الجريمة والتي تؤدي إلى تغيير المعطيات في ثلاث صور (الإدخال، المحو، التعديل) في حين أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أضافت صور أخرى تتمثل في :الحجب للمعلومات أو

---

[1]- تنص المادة 394 مكرر فقرة 03 " تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج...".

[2]- نصت عليها المواد 04، 08، من اتفاقية بودابيست لسنة 2001 بشأن الاجرام المعلوماتي.

البيانات، التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها، التعطيل الأجهزة والبرامج والمواقع الإلكترونية وتعتبر هذه الأفعال المتعلقة بالاعتداء على البرامج والبيانات الخاصة بوسائل الدفع الإلكتروني من وسائل الاتلاف المعلوماتي ومن أفعال الإعاقة كما أنها قد تشكل جرائم متعلقة بالتزوير.

أولا/ فعل الإدخال L'intrusion

يتحقق **فعل الإدخال** بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم كان يوجد عليها معطيات من قبل[1]، أو هو تغذية النظام بالمعلومات المراد معالجتها أو بتعليمات لازمة لعملية المعالجة[2] ففي مرحلة المدخلات حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة يسهل إدخال معلومات غير صحيحة وعدم ادخال وثائق أساسية documents-clés وفي هذه المرحلة يرتكب الجانب الأكبر من الجرائم المعلوماتية ففي مرحلة المعالجة يمكن إدخال أية تعديلات تحقق الهدف الإجرامي عن طريق التلاعب ببرامج الحاسب الآلي كدس تعليمات غير مصرح بها أو تشغيل برامج جديدة تلغي جزئيا أو كليا عمل البرامج الاصلية[3] وتتطلب الجرائم المرتكبة في هذه الحالة توفر معرفة فنية لدى الفاعل ومركز في البنك وتعاون وتواطؤ بين أصحاب وسائل الدفع الإلكتروني والعاملين في البنك.

---

[1]- علي عبد القادر القهوجي، المرجع السابق، ص607.

[2]- نائلة عادل محمد فريد قورة، المرجع سابق، ص 437.

[3]- هشام محمد فريد رستم، المرجع السابق، ص 446.

يتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقة السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغ من النقود أكثر من المبلغ الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا للتاجر أو شخص يتعامل معه (أكثر من المبلغ المحدد له) وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من حاملها الشرعي أم من غيره في حالات السرقة أو التزوير.

يتحقق فعل الادخال بصفة عامة في كل حالة يتم فيها الاستخدام التعسفي لبطاقة السحب والدفع، ويعتبر هذا الفعل أكثر أساليب ارتكاب الاحتيال المعلوماتي وقوعا بساطة وأمنا، وصورة حية عن الاشتراك بالتواطؤ والاتفاق بين الحامل لوسيلة الدفع الإلكتروني والتاجر والعاملين بالبنك.

ثانيا / فعل المحو L'effacement

يقصد به إزالة جزء من المعطيات المسجلة على الدعامة الموجودة على وسيلة الدفع الإلكتروني أو داخل نظام العمل بوسيلة الدفع الإلكتروني أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات في المنطقة الخاصة بالذاكرة الموجودة داخل وسيلة الدفع، ومحو المعلومات من أسهل طرق الإتلاف لأنه من خصائص الجرائم المعلوماتية قدرة الجاني على محو آثار جريمته في فترة وجيزة جدا لا تتعد الضغط على زر بسيط في

لوحة المفاتيح أو البرنامج عن طريق الفأرة، فمثلا يقوم شخص بتحويل مبلغ مالي إلكترونيا من حساب ببنك إلى حساب آخر في بلد آخر مع محو آثار العملية فيسجل النظام المعلوماتي الخاص بالبنك فمن الصعب اكتشاف الجريمة خاصة في حالة عدم تقديم شكوى من طرف الضحية (صاحب الحساب).

ثالثا/ فعل التعديل La modification

يعني استبدال المعطيات الموجودة داخل نظام التعامل بوسيلة الدفع الإلكتروني بمعطيات أخرى، وبتوضيح صور التلاعب بالمعلومات يمكن ملاحظة أن هذه الأساليب قد ترتكب بها جريمة الاحتيال المعلوماتي بمختلف أشكاله بما في ذلك أنظمة التحويل الإلكتروني للأموال[1]، غير أنه لحل هذا التداخل لابد من التمييز بين التلاعب بالمعلومات بذاتها واتلافها دون أن يكون الهدف من وراء ذلك الحصول على منفعة مادية، وبين التلاعب بالبيانات المدخلة من أجل الحصول على فائدة مادية حيث تمثل هاته الأخيرة جريمة الاحتيال المعلوماتي ولقد قضت محكمة جنح باريس في حكم صادر لها بتاريخ 13فيفري 1990 على أن المتهمين الذين قاموا بتعديل ومحو المعلومات التي يحتوي عليها نظام المعالجة الآلية من أجل اجراء تحويلات غير مشروعة للأموال بتهمة النصب، وبتهمة إدخال أو محو أو تعديل المعلومات المبرمجة آليا على نحو غير مشروع[2].

---

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص 439.

[2]- بوربابة صورية، المرجع السابق، ص105.

وفي حالة تتسم بضخامة المبلغ المختلس تمكن خبير في الحاسبات الإليكترونية يدعى Rifkin من دخول حجرة الأسلاك البرقية المركزية لبنك Security Pacific Bank في لوس انجلس بكاليفورنيا الأمريكية، و أخذ يراقب عمليات التحويل الإلكتروني للأموال حتى إلتقط الشفرة التي يستخدمها البنك في إجراء هذه التحويلات، وعن طريق هاتف من خارج البنك تمكن Rifkin من الاتصال بشبكة معلومات البنك واستخدم الشفرة التي حصل عليها ليحول عبر نظام التغذية البرقية FEDWIRE من حساب البنك إلى حسابه في نيويورك مبالغ وصل مجموعها إلى 1,5مليون دولار ثم حول معظمها إلى حساب له بأحد البنوك السويسرية[1].

إن التعديل في البيانات أو الوظائف الخاصة بوسيلة الدفع يمكن أن يتم من خلال استغلال وجود ضعف أمني في النظام التشغيلي، أو من خلال اعتداءات مادية على الرقاقة ذاتها، أما في أنظمة النقود الإلكترونية ذات البرمجيات فيمكن تعديل البيانات المخزنة على الوسيلة التي يحوزها الحامل اذا لم تتوفر على حماية برمجية مناسبة[2]

رابعا/ حجب المعلومات والبيانات

[1]- هشام محمد فريد رستم، المرجع السابق، ص 462،463.

[2]- حوالف عبد الصمد، المرجع السابق، ص 340.

يتعلق بإجراءات منع وصولها إلى العنوان المرسلة إليه كحذف جزء منها على نحو لا يتيح وصولها إلى الموضع الفيزيائي المطلوب أو تصبح غير قادرة على ذلك أو منع الغير من الوصول إليها[1].

خامسا / التدخل والتغيير والتعطيل لأنظمة التشغيل والاتصالات

وذلك بارتكاب الأفعال المتعلقة بالتدخل في المعطيات لتعطيل أداء وعمل الأنظمة بالتدمير والحذف والتعطيل مضاف إليها وسيلة البث أو الارسال[2] فبمجرد أن يكون الحاسب الآلي متصل بوحدة التشغيل المركزية عن طريق شبكة الهاتف أو أي وسيلة من وسائل الاتصال لتشغيل وسائل الدفع الإلكتروني يتمكن الجاني من خلالها إتمام عملية الاحتيال ويعتبر التلاعب بوسائل الاتصال عن بعد الوسيلة الأكثر شيوعا في التحويل الإلكتروني للأموال.

سادسا/تعطيل الأجهزة والبرامج والمواقع الإلكترونية

1-تعطيل البرامج: ويعرف البرنامج المعلوماتي على أنه مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما[3]، البرامج هي مجموعة من الأوامر الغرض منها جعل الحاسب ينفذ مهمة أو وظيفة معينة بمعنى هي

---

[1]- يونس عرب، ورقة عمل "قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان "، مقدمة الى ورشة عمل "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية "، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 2-4أفريل 2006.

[2]- يونس عرب، ورقة عمل "قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان "، المرجع السابق.

[3]- المادة الثانية فقرة 04 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

تعليمات وأوامر يستطيع الحاسب الآلي أن يترجمها ويفهمها تمهيدا لتنفيذها وتتنوع إلى برامج تشغيلية لأنها تمكن من تشغيل الحاسب الآلي وبرامج تطبيقية لأنها تقوم بأداء وظيفة محددة.

الشيء المشترك بين هذه الأنظمة (logiciel) أنها أنظمة محفزة تستخدم لتخريب النظام وتعطيل الملفات أو المعطيات والتي تستعمل لإعاقة عمل النظام ولتنفيذ تصرفات غير شرعية هي في النهاية تهدف للتأثير على الحاسب الآلي لتنفيذ تصرفات غير مصرح بها[1].

وتعتبر التدخلات في الكيان المنطقي البرامج من صور الاتلاف والاحتيال عبر وسائل الدفع الإلكتروني، فيتحقق فعل الإدخال بإدخال برنامج غريب (فيروس أو قنبلة) يضيف معلومات جديدة لبرامج عمل وسائل الدفع الإلكتروني، كما يعتبر المحو للبرامج جريمة اتلاف.

تتميز هذه الحالة بأن الفاعل يجب أن تكون لديه دراية كبيرة لأن التلاعب في البرامج يتميز بقدر كبير من التعقيد ومن أصعب الحالات اكتشافا ويتم التلاعب في برامج عمل وسائل الدفع الإلكتروني بصفة عامة عن طريق احدى الوسائل التالية:

الوسيلة الأولى: استخدام البرامج لتخطي أنظمة الحماية الفنية في الحالات الطارئة

من أمثلة ذلك ما حدث في بنك نيوجرسي عندما تمكن مدير تشغيل حاسب البنك عقب استخدامه أحد البرامج لتخطي الاجراءات الأمنية التي تكفل حماية ملفات حسابات

[1]-Hatem Adnan Bezzo, op, cit , p196.

الزبائن من أجل اصلاح بعض الأخطاء التي نجمت عن عطل في بعض أجزاء نظام الحاسب المركزي للبنك بتحويل مبالغ مالية من حسابات بعض الزبائن قدرت بثمانية وعشرون ألف دولار، ووضعها في حساب ثلاثة من أصدقائه واكتشف أمره بعد فحص البنك لشكاوي بعض الزبائن من نقص أرصدتهم دون أن يقوموا بسحب الأموال[1]، وهذه الجريمة تمت بتقديم المساعدة من الأصدقاء عن طريق السماح بتقديم أرقام حساباتهم وسحب المبالغ المالية من حساباتهم.

الوسيلة الثانية: استخدام البرامج الخبيثة للعبث بوسائل الدفع الإلكتروني

البرامج الخبيثة أو الفيروسات تهدف إلى الاحتيال والاستيلاء بواسطة وسائل الدفع الإلكتروني على الأموال، ويعتبر برنامج حصان طراودة الطريقة الغالبة في الاحتيال والتخريب بواسطة الحاسوب[2].

ومن أشهر حالات الاحتيال التي تمت باستخدام برنامج طراودة ما حدث لشركة متخصصة في اصدار وبيع بطاقات الدفع عندما رغبت في تحديث نظامها المحاسبي

---

[1]-غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص 300.

[2]-عملية حصان طراودة :هي تغطية لأوامر الحاسب الالي لتمكينه من الاتيان بوظائف غير المصرح بها مع ترك البرنامج على حاله للاستثمار فيه وتحقيق الاهداف، فالأوامر توضع في برنامج الحاسوب المنتج بحيث تعمل تلك الأوامر في المجال الممنوع أو المحمي من البرنامج ويكون له القدرة في الوصول إلى جميع الملفات، ويمكن اكتشاف عمليات حصن طراودة بمقارنة البرنامج المشتبه فيه مع الأصل أو صورة من الأصل الخالي من الثغرات القانونية، أنظر محمد الامين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت الذي نظمته كلية الشريعة والقانون، جامعة الامارات العربية المتحدة بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة، من 01 إلى 03 ماي 2000، المجلد الثاني، الطبعة الثانية 2004، ص 1063.

فتعاقدت مع احدى الشركات المتخصصة في إعداد وتطوير النظم المعلوماتية لتزويد شركة اصدار البطاقات بأنظمة متطورة، وتنفيذا لهذا التعاقد قام مبرمج يدعى (جون ماكلاود) بتصميم وإعداد البرنامج المحاسبي المطلوب ثم فصل من عمله وعندما بدأت الشركة في استعمال هذا البرنامج ظهرت فيه بعض العيوب فاستعان مديرها بمصمم البرامج مما ولد في ذهنه فكرة تحويل البرنامج الذي يتولى تصحيح عيوبه الى حصان طراودة كي يتاح له الاستيلاء على الأموال عند تشغيله فقد كان يقوم بسرقة بيانات بطاقات الدفع وادخالها في رمز معد لتنفيذ الأوامر الوهمية، ثم تعبئتها ببياناته الخاصة والتوجه إلى البنك لتحصيلها[1].

-الوسيلة الثالثة: ادخال تعديلات غير مرخص بها على عمليات الدفع الإلكتروني

تتمثل في تغيير البرامج المطبقة داخل البنك المجني عليه وذلك بإدخال تعديلات غير مرخص بها على البرامج المستخدمة في الدفع الإلكتروني فالثغرات المكتشفة بعد مدة من تشغيل البرامج تتيح للجاني إدخال تغيرات عن طريق الفيروسات (البرامج الخبيثة)، وبالتالي تعطيل عمل البرنامج الحقيقي لوسيلة الدفع الإلكتروني.

-الوسيلة الرابعة: إدخال برامج إضافية على وسائل الدفع الإلكتروني

تتمثل في إدخال برامج اضافية معدة مسبقا تهدف إلى تعديل المعلومات الخاصة بوسائل الدفع الإلكتروني الموجودة في ذاكرة الحاسب الآلي ومن خلال هذه الطريقة يتم

[1]- غازي عبد الرحمان هيان الرشيد، المرجع السابق، لبنان ص302.

الاستيلاء بالاقتطاع لمبالغ ضئيلة من المال من حسابات متعددة في البنك قد لا يثير نقصانها انتباه صاحب الرصيد وتحويلها إلى حساب الفاعل.

2-تعطيل الأجهزة: قد يمتد الاحتيال المعلوماتي إلى التلاعب بالمكونات المادية للحاسوب أو الدوائر المختلفة المكون منها ولاشك أن هذا الاحتيال يتطلب كسابقه درجة كبيرة من العلم بتقنية الحاسب الآلي، أثير التساؤل حول مدى امكانية عد التعطيل والاتلاف الذي قام به التاجر جريمة نصب وذلك باتباعه طرقا احتيالية للاستيلاء على أموال البنك والمتمثلة بتعطيل الالة في جزء منها لكي تقوم الالة بقيد الحساب بطريقة مغايرة ؟

وتطبيقا على ذلك فإن قيام التاجر بالاستيلاء على النقود بالاحتيال وباستعمال طرق احتيالية تتمثل في قيامه بتعطيل الآلة في جزء منها، لكي تقوم الآلة بقيد الحساب بطريقة مغايرة للحقيقة وبذلك يكون سند الدين على البنك غير صحيح مما يستوجب تطبيق جريمة النصب والاحتيال[1].

وقد يتم التلاعب في المكونات المادية لوسائل الدفع الإلكتروني كخطوط الاتصال أو أجهزة السحب وهذا لإدخال أو تعديل أو محو البيانات الخاصة بعمليات التحويل أو التلاعب بالسجلات الخاصة بوسائل الدفع الإلكتروني للاحتيال على المصرف.

[1]- عبد الكريم الردايدة، جرائم بطاقات الائتمان (على البنوك الأردنية)، دراسة تطبيقية ميدانية، الطبعة الأولى، 2013، دار الحامد للنشر والتوزيع، عمان الأردن، ص 226.

وجاء استخدام الماكينات الإلكترونية لتعزيز التعامل بالبطاقات والتمكن من الاتصال المباشر بالبنك نظرا لعدم فعالية الماكنات اليدوية وسهولة التلاعب بها من قبل التجار، أو موظفيهم بالاشتراك مع أصحاب البطاقات الحقيقين أومن الغير في حالة فقدان البطاقة أو سرقتها للاحتيال على البنوك وللحيلولة دون وقوع هذا الاحتيال تم استبدال الماكينات اليدوية بالإلكترونية، إلا أنه في أحيان أخرى يلجا التجار أنفسهم لعملية التلاعب والاعتداء عليها يدويا وتعطيلها إلكترونيا أثناء فترة قراءة البطاقة وكذلك استخدام الأرصدة غير الكافية[1].

3-تعطيل المواقع: ويعرف الموقع بأنه مكان اتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد[2]، الاحتيال عبر المواقع وتعطيلها كانت من أشكال الاحتيال الأولى في الظهور ويعتمد أغلبها على:

-تقنية تفجير مواقع البنوك التي تعمل على شبكة الانترنت وبالتالي تشتت المعلومات والبيانات المخزنة فيه حتي يتمكن الجاني من حرية التجول في الموقع المستهدف وبالتالي الحصول على البيانات والمعلومات الخاصة بوسائل الدفع الإلكتروني.

ويوجه مجرمو البطاقات هذا الأسلوب إلى الحواسب المركزية للبنوك بهدف تحصيل أكبر عدد ممكن من أرقام البطاقات.

---

[1]- عبد الكريم الردايدة، المرجع السابق، ص 226.

[2]- المادة الثانية فقرة 07 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

-الاحتيال بالبطاقة عن طريق المواقع الكاذبة على شبكة الانترنت من الغير وسرقة أرقام حسابات:

ويتم ذلك سواء بالتقليد والتزوير لهذه البطاقات أو من خلال اعتراض الرسائل البريدية والتي يقوم بها المخترقون بكسر أو فتح صناديق البريد بحثا عن رسائل تتضمن معلومات البطاقة والتي تأتي في العادة عندما تتم الموافقة على طلب الشراء لسلعة أو فاتورة مدفوعة فيتعامل معها المحتالون وكأنهم أصحابها ويقومون بالاحتيال عن طريق المواقع الكاذبة وسرقة هوية الشركات بمحاكاتها من ناحية التصميم والخصائص إلى درجة يقتنع بها الضحية بإدخال معلوماته الشخصية فيها ورقم بطاقته وفي الغالب يتخذ هؤلاء المحتالون من مواقعهم صفة أنها تابعة للموقع الأم[1].

ليس هناك وسيلة تقنية يمكن تطبيقها وتحول تماما دون تدمير المواقع أو اختراق الموقع بشكل دائم، فالمتغيرات التقنية والمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء سواء كان ذلك في مكونات نقطة الاتصال أو النظم أو الشبكة البرمجية جعلت الحيلولة دون الاختراقات صعبة جدا اضافة إلى أن هناك مؤسسات يدخل ضمن عملها اختراق المواقع[2].

---

[1]- حسين محمد الشبلي، مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، سلسلة الجرائم المالية والمستحدثة، دار مجدلاوي للنشر والتوزيع، الطبعة الأولى، 2009، الأردن، ص86.

[2]-عبد الرحمان بن عبد الله السند، أحكام تقنية المعلومات "الحاسب الالي وشبكة المعلومات الانترنت "، رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن، جامعة الامام محمد بن سعود الاسلامية، السعودية، 1424،1425، ص 265.

الاحتيال بأمر دفع غير صحيح من الاحتيالات الكبيرة التي اتسعت دوليا وتسمى الاحتيال بأمر دفع غير صحيح وتسمى (FOVI)[1] وتستهدف منذ عامين فروع المؤسسات الكبيرة الفرنسية الموجودة في الاتحاد الاوروبي أو المؤسسات الأجنبية المعتمدة في فرنسا[2]، وتعتبر هذه التقنية جديدة للاحتيال المستهدف بصفة خاصة لوسائل الدفع الإلكتروني.

الفرع الثاني

المحل في الاحتيال بوسائل الدفع الإلكتروني

يتمثل في نقود كتابية أو مصرفية بتلاعب الجاني في البيانات والبرامج كي تحول بعض أرصدة الغير أو فوائدها لحسابه فالعبرة بوضع الشيء في متناول يد الجاني أو تحت أمره[3].

ويتمثل كذلك في قيم مالية داخل نظام إلكتروني لمعالجة البيانات فإما أن تكون هذه القيم غير ملموسة كالودائع، سعر الفائدة، نتائج الحسابات للأرصدة، المرتبات، الفواتير، الأرصدة المصرفية، ويعد من المجالات الخصبة للاحتيال المعلوماتي خاصة مع

---

[1]- FOVI : Faux ordre de virement international.

[2]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 66

[3]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص163.

الاتجاه إلى ما يسمى بمجتمع اللانقود حيث أصبح نظام الدفع سواء في قطاع الأعمال أو في محيط الأفراد يعتمد بشكل أساسي على ما يسمى أوامر التحويل، كما قد تمثل **المعلومات** محل الاحتيال المعلوماتي قيما مادية ملموسة يستولي عليها بعد التلاعب بنظام الحاسب الآلي وتتمثل بصفة أساسية في الأموال النقدية، السلع والبضائع، ويعتبر التلاعب في هذه القيم قليل بالمقارنة مع القيم غير الملموسة ففي الأموال الملموسة تقدر الخسائر بالقدر الحقيقي للأموال والبضائع في حين يستطيع الجاني خلق هذه الأموال الإلكترونية بنفسه بالإضافة إلى الحجم الضخم للأموال التي يتم تخزينها أو تحويلها عن طريق الحاسبات الآلية[1].

في معظم الحالات يقوم مجرمي المعلوماتية بالتحكم في المواقع بعد اختراقها والتلاعب بأصول الحسابات البنكية والاستيلاء على الأموال والأرقام الخاصة بوسائل الدفع الإلكتروني.

المطلب الثالث

الضرر والقصد والعقوبة في الاشتراك للاحتيال بوسائل الدفع الإلكتروني

إذا كيفت الجريمة على أنها احتيال بوسائل الدفع الإلكتروني فإن الإشكالية تدور حول هل القصد من هذه الجريمة هو الاضرار، أم أن الضرر ركن في هذه الجريمة؟ وعليه سنقوم بتوضيح مكانة الضرر عند الاشتراك في الاحتيال بوسائل الدفع الإلكتروني(

[1]– نائلة عادل محمد فريد قورة، المرجع السابق، ص 421 .

للغير ومصطلح الضرر الاقتصادي أو المادي يتصل بمفهوم واسع جدا يشمل النقود والأشياء المادية وغير المادية ذات القيمة الاقتصادية[1].

تولي شركات البطاقات أهمية كبرى لمكافحة هذا النوع من الاحتيال فهذه الشركات تجري بصفة مستمرة أبحاثا نشطة للغاية لإيجاد السبل الكفيلة بتحسين عناصر وضوابط الأمن في بطاقات الائتمان خاصة ولأن المسألة ليست مجرد تجنب الخسائر المالية أو الحد منها بل الحفاظ على ثقة العملاء التي يعتمد عليها نظام بطاقات الدفع اعتمادا كليا[2].

الفرع الثاني

الركن المعنوي في الاشتراك للاحتيال بوسائل الدفع الإلكتروني

تعد جريمة الاحتيال المعلوماتي من الجرائم العمدية شأنها شأن جريمة الاحتيال إذ أنه من المفترض أن أفعال العرقلة و التعطيل لا تكون إلا عمدية وتنص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال المادة 11" التسبب بالحاق **الضرر** بالمستفيدين والمستخدمين **عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة ،للفاعل أو للغير** ..." فيكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، وتتطلب الجريمة نية خاصة،

[1]–هلالي عبد اللاه أحمد، المرجع السابق، ص104.

[2]– علي نحلة، النشاطات المشبوهة "غسل الأموال الإلكتروني آليات كشفها وكيفية التعرف عليها والتبليغ عنها "، مجلة اتحاد المصارف العربية ،عدد حزيران /يونيو 2005، ص 71.

عبرت عنها الاتفاقية بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير.

ويتمثل القصد العام في أن يعلم المتهم(سواء كان المصرفي، أو التاجر، أو حامل وسيلة الدفع، أو المختص في المعلوماتية) أنه من خلال التلاعب الذي يحدثه بالمعلومات التي يحتوي عليها نظام الحاسب الآلي أو أن المعلومات التي يقوم بإدخالها إلى النظام يقدم تسهيلات للمتهم الذي يرتكب فعل من أفعال الاحتيال، وهذه التسهيلات من شأنها أن تجعل الحاسب الآلي يستجيب وفقا لهذه المعلومات فيقوم بتنفيذ ما عهد إليه من تعليمات، فيجب أن ينصرف علم الفاعل أولا إلى أن ما يقوم بإدخاله من معلومات إلى نظام التعامل بوسائل الدفع الإلكتروني و أنظمة البنك يعد من قبيل التلاعب بهذه المعلومات، فمن يعتقد أن التعديل الذي يلحقه بالمعلومات داخل هذه الأنظمة ضروري حتى تقوم هذه المعلومات بدورها على نحو صحيح لا يتوافر لديه القصد المتطلب لقيام الجريمة، وكذلك من يعتقد أنه من حقه إدخال المعلومات ولا يلزم أن يعلم المتهم بأن الوسيلة المستعملة هي إحدى الوسائل المنصوص عليها في القانون وأن يعلم أن المال المستولى عليه ملك للغير لا إلى شخص محدد بالذات ففي التحويل الإلكتروني للأموال غالبا ما لا يعلم الفاعل شخص الضحية[1].

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص 488،489.

كما تتطلب جريمة الاحتيال المعلوماتي توفر القصد الخاص ويتمثل بنية المتهم أن يباشر على الشيء المستولى عليه مظاهر السيطرة التي يخولها حق الملكية[1].

و يمكن القول بتحقق مسؤولية التاجر عن اشتراك في الاحتيال ذلك لتسهيله للغير – حامل البطاقة المزورة –عملية الوفاء بمشترياته المنفذة بهذه البطاقة بحيث يمكن القول أنه لولا مساعدة التاجر لما تمت الجريمة وخاصة اذا كان التزوير بينا أو غير متقن أو إذا كان التاجر مزودا بآلات الوفاء الحديثة، ولقد أكدت محكمة استئناف باريس هذا الاتجاه فيحكم صادر لها في 17 أكتوبر 1991 حيث أدانت تاجر بالاشتراك في جريمة الاحتيال لمساعدة الفاعل الأصلي على الوفاء ببطاقات ائتمان مقلدة ومزورة مع علمه بذلك[2]، لا يمكننا تصور قيام جريمة الاحتيال المعلوماتي بوسائل الدفع الإلكتروني لقيام البنكي أو التاجر أو حامل وسيلة الدفع لوحده بهذه الجريمة، انما غالبا ما تتم حالات الاحتيال بالاشتراك والمساعدة والتواطؤ.

الفرع الثالث

إشكالية العقوبة المقررة في القانون الجزائري

[1]– كما أن المجلس الأوربي في توصيته رقم 89/09 الصادرة في شان جرائم الحاسب الآلي قد تطلب في جريمة الاحتيال المعلوماتي أن يترتب على نشاط الفاعل خسارة اقتصادية تلحق الضحية.

[2]– محمد نور الدين سيد عبد المجيد، المرجع السابق، ص427.

تبقى الإشكالية مطروحة في القانون الجزائري والعقوبة التي تطبق على الاحتيال المعلوماتي لأن المشرع الجزائري لازال لم يجرم الاحتيال المعلوماتي، حيث نتساءل هل يمكننا تطبيق المادة 372 من قانون العقوبات الجزائري على الاحتيال المعلوماتي حيث تتراوح العقوبة بين الحبس من سنة إلى خمس سنوات وغرامة من 500الى 2000 دج، والحرمان من الحقوق الواردة بالمادة 14 كلها أو بعضها والمنع من الإقامة لمدة خمس سنوات حسب المادة 372 من قانون العقوبات ويجوز الحكم على المصرف حسب المادة 382 من قانون العقوبات أم أنه لابد لنا أن ننتظر تعديلها بحيث تتلاءم وطبيعة المال المعلوماتي حتى لا نصطدم بمبدأ الشرعية، ومبدأ التفسير الضيق للقانون ومبدأ حظر القياس في المادة الجزائية أم أنه يمكننا اعتبار وضع المشرع الجرائم الماسة بالأنظمة المعلوماتية ضمن الكتاب الخاص بالجنايات والجنح ضد الأموال أنه اعتبر ضمنيا المعلوماتية مالا، أم أننا ملزمون فقط بتطبيق نص المادة 394 مكرر 1 : " يعاقب بالحبس من ستة (6) أشهر إلى (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، وكذا نص المادة 394 مكرر 5 " كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان التحضير

مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها"[1] في انتظار تعديل المشرع الجزائري بالنظر إلى مصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تضمن جريمة الاحتيال المعلوماتي بنص صريح.

المطلب الرابع

إساءة استعمال وسائل تقنية المعلومات واشكالية تسهيل العمليات الاحتيالية

أشارت المذكرة التفسيرية لاتفاقية بودابيست إلى أن هذه الجريمة تعتبر جريمة جنائية منفصلة ومستقلة الارتكاب عمدا لأفعال غير مشروعة خاصة ترتبط ببعض الأجهزة وبيانات الولوج من حيث اساءة استخدامها[2]، وهي من الصور التي خرج فيها المشرع عن القواعد العامة ولم يعتبرها اشتراك بل أعتبرها جرائم قائمة بذاتها وهذا لتكريس الطابع الاحتياطي والوقائي في مكافحة الجريمة الإلكترونية إلا أنه كثيرا ما تستغل الوسائل التقنية لتسهيل العمليات الاحتيالية بوسائل الدفع الإلكتروني والتي يكون الغرض منها تحقيق الربح، وبالتالي هذه الحالة تتضمن تداخل بين عديد النصوص القانونية في الجزائر وعليه سنتطرق إلى الركن الشرعي لإساءة استخدام وسائل تقنية المعلومات (الفرع الأول)، ونخصص الفرع الثاني (للركن المادي للاشتراك في إساءة استخدام وسائل تقنية المعلومات).

الفرع الأول

[1]– غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 166.

[2]– هلالي عبد اللاه أحمد، المرجع السابق، ص84.

الركن الشرعي لإساءة استخدام وسائل تقنية المعلومات

تنص المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جريمة إساءة استعمال وسائل تقنية المعلومات :

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير :

أ- أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب-كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأي من الجرائم المبينة في المادة السادسة الى المادة الثامنة.

2- حيازة أية أدوات أو برامج مذكورة الفقرتين أعلاه بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة الى المادة الثامنة ."

وتنص المادة 394 مكرر 2 من قانون العقوبات الجزائري على أنه "يعاقب بالحبس من شهرين (2) إلى ثلاث سنوات وبغرامة من 1.000.000 دج الى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي :

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 افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها في هذا القسم ".

اتفاقية بودابيست من خلال المادة السادسة نصت على :"يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية اجراءات يرى أنها ضرورية لتجريم - تبعا لقانونه الداخلي - القيام عمدا ودون حق لما يلي :

أ- انتاج أو بيع أو الحصول من أجل الاستخدام، أو استيراد أو نشر، أو أي أشكال أخرى للوضع تحت التصرف.

1-أي جهاز يحتوي على برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض ارتكاب احدى الجرائم المنصوص عليها وفقا للمواد من 2-5 السابق الاشارة اليها .

2-كلمة المرور، أو شيفرة الدخول، أو أي بيانات مماثلة تسمح بالولوج إلى كل أو جزء من نظام الحاسب بنية استخدامها لغرض ارتكاب جريمة من الجرائم المشار اليها في المواد من 2-5.

ب- حيازة أي عنصر من العناصر المشار اليها في البندين أ-1،أ-2 بنية استخدامه في ارتكاب أي جريمة من الجرائم الواردة في المواد من 2-5.

ويمكن لأي طرف أن يشترط في قانونه الداخلي وجود بعض هذه العناصر من أجل تقرير المسؤولية الجنائية ".

بالملاحظة والمقارنة لنصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ونصوص اتفاقية بودابست ونص المادة 394 من قانون العقوبات الجزائري نلاحظ أن المشرع الجزائري حصر هذه الجريمة في الوسائل المعنوية من خلال مصطلح معطيات معلوماتية أما نصوص الاتفاقيتين فجاءت شاملة للوسائل المادية والمعنوية من خلال مصطلحات "جهاز "وأداة "برنامج "وهو نفس النهج الذي انتهجه المشرع الفرنسي[1] وبالتالي سيكون أشمل من القانون الجزائري.

الفرع الثاني

الركن المادي للاشتراك في إساءة استخدام وسائل تقنية المعلومات

أولا /البنود المشتركة بين قانون العقوبات والاتفاقية العربية لمكافحة جرائم تقنية المعلومات

1-التصميم conception: ويقصد به القيام بخلق وايجاد معطيات صالحة لارتكاب جريمة[2] التصميم لمعطيات معلوماتية مقرصنة في برمجتها « sa programmation » بواسطة المعلوماتية ومثال ذلك الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية ضد الأنظمة المعلوماتية أو الأنظمة المعلوماتية

[1]- بوربابة صورية، المرجع السابق، ص 123.

[2]- محمد خليفة، المرجع السابق، ص200.

في حد ذاتها[1]، وبالتالي التصميم لأية وسيلة بإمكانها المساس بالأنظمة أو المعطيات المعلوماتية السليمة لوسائل الدفع الإلكتروني.

البحث: ويقصد بها البحث في كيفية تصميم هذه المعطيات وإعدادها[2] كلمة بحث لا نجدها في نص المادة 06 من اتفاقية بودابيست ولا في نص المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وعموما البحث يتم في أغلب الأحيان عبر شبكة الأنترنت من خلال عملية الاستنساخ « le téléchargement » إن الأخذ بالتفسير الواسع لهذه العبارة يوسع من نطاق التجريم ويشكل تهديدا فليس كل من يبحث عن معلومات يمكن أن ترتكب بها جريمة يعد قد ارتكب جرما، وإنما من يبحث عن معلومات لتصميم ما يمكن أن ترتكب به هذه الجرائم يكون قد ارتكب جريمة اساءة استعمال معلومات أو تقنية المعلومات لارتكاب جريمة ولعل هذا ما جعل المشرع الجزائري يستتبع كلمة بحث بعد كلمة تصميم[3].

2-النشر: ورد فعل النشر في نص المادة 394 مكرر 2 من قانون العقوبات الجزائري وهي مأخوذة من نص المادة السادسة الفقرة الثانية من اتفاقية بودابست، ويقصد بالنشر (diffusion la) اذاعة المعطيات محل الجريمة ونقلها للآخرين، وينبغي أن يمتد ليشمل كل نشاط من شأنه نقل بيانات للآخرين[4]، والنشر غالبا ما يتم عبر شبكة

---

[1]- دردور نسيم، المرجع السابق، ص 43.

[2]- محمد خليفة، المرجع السابق، ص201.

[3]- بورباية صورية، المرجع السابق، ص 122.

[4]- هلالي عبد اللاه أحمد، المرجع السابق، ص85.

الأنترنت لمعطيات معلوماتية مقرصنة يمكنها المساس بالأنظمة المعلوماتية لوسائل الدفع الإلكتروني ،سواء بنشرها عن طريق البريد الإلكتروني أو عن طريق مواقع الانترنت القابلة للنسخ ويتم الاستيلاء على البرامج ونسخها من أجل بيعها والمتاجرة بها ولعل النشر من أخطر الأفعال التي يمكن أن ترد على المعطيات المجرمة إذ أن هذا السلوك كفيل بأن ينقل هذه الأخيرة لعدد كبير من الأشخاص مما يجعل احتمال استعمال هذه المعطيات في الجرائم أكبر[1].

3-الاتجار: ولم يرد هذا المصطلح لا ضمن اتفاقية بودابيست ولا في التشريع الفرنسي، الاتجار بالمعطيات هو تقديمها للغير بمقابل وينص المشرع الفرنسي على مصطلحي التوفير أو العرض والوضع تحت التصرف وما يميز هذين المصطلحين عن الاتجار هو حصول الأخير بدون مقابل والظاهر أن المشرع الفرنسي لا يقيم اعتبار للمقابل فيعتبر تقديم المعطيات مجرما سواء تم بمقابل أم بغير مقابل، بينما أراد المشرع الجزائري أن يشمل بالنص الحالتين معا[2].

4-محل الجريمة جهاز يحتوي على برنامج معلوماتي: تعرضت المذكرة التفسيرية لاتفاقية بودابيست لطبيعة الأجهزة محل التجريم وهل تقتصر على الاجهزة المصممة خصيصا لارتكاب الجرائم المعلوماتية، أم أن مضلة التجريم تمتد لتشمل الأجهزة ذات

[1]- محمد خليفة، المرجع السابق، ص203.

[2]- محمد خليفة، المرجع السابق، ص204.

الاستخدام المزدوج المشروع وغير المشروع وفقا لقصد الشخص من استخدامها وتوظيفه لها[1].

واتفق على الاعتماد على العنصر الشخصي أي قصد ارتكاب جريمة معلوماتية وبالتالي يتحدد نطاق تطبيق المادة بالأجهزة التي يمكن القول أنها مصممة أساسا لأجل ارتكاب جريمة معلوماتية.

وبالتالي فإن هذا النص يستبعد عادة الأجهزة ذات الاستخدام المزدوج[2].

5-كلمة المرور un mot de passe: أو كلمة السر وهي عبارة عن مجموعة من الحروف والأرقام المتتالية يقوم المستخدم بإدخالها للحاسب الآلي أو موقع شبكة الأنترنت للوصول إلى النظام المعلوماتي لوسائل الدفع الإلكتروني وتظهر كنجوم عند كتابتها، وتمثل المفتاح السري الذي يمكن من خلاله استعمال وسيلة الدفع الإلكتروني فيما أعدت له من أغراض فمن خلال هذا الرقم يمكن الولوج إلى الأجهزة الآلية ومخاطبتها بحيث على أساسه تستجيب تلك الأجهزة لأوامر الشخص المستعمل لوسيلة الدفع الإلكتروني ويمكنه تنفيذ جميع العمليات المصرح له بها، وتعتبر وسيلة للتحقق من هوية الحامل، وبالتالي استخدام كلمة المرور أو كلمة سرية سواء من نهاية طرفية معينة أو لإدخال بيانات معينة إلا بذكرها حتى يمكن التعامل مع النظام المعلوماتي، والأصل أن يلتزم الزبون بالمحافظة على وسائل الدفع الإلكتروني واستعمالها استعمالا شخصيا

[1]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 320.

[2]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 321.

وحتى في حالة ضياع الوسيلة أو سرقتها فهو ملزم بتقديم الاعتراض للبنك حتى يوقف استعمال وسيلة الدفع الإلكتروني، فالغير في حالة حصوله على وسيلة الدفع الإلكتروني لن يتمكن من استعمالها إلا إذا كان يعلم كلمة السر الأمر الذي يفترض إخلال الزبون بواجب المحافظة عليها، كما يلزم بعدم البوح بكلمة السر أو كتابتها على أي وثيقة حتى يتمكن الغير من الاطلاع عليها وبالتالي إذا لم يكن للزبون أي علاقة بضياع كلمة المرور فإنه لا يسأل عن ما يجري من سحب للنقود، ومن الأفضل تغيير كلمة السر بصورة دورية لتجنب إمكانية الاطلاع عليها من قبل أشخاص غير مسموح لهم بذلك[1].

ويجب أن تكون سهلة التذكر بالنسبة للمستخدم المصرح له بالدخول إلى النظام المعلوماتي لوسائل الدفع الإلكتروني، وأن تكون صعبة التعرف عليها بواسطة المتطفلين عن طريق التخمين وكلما زاد عدد الحروف كلما قل احتمال التعرف عليها.

6-شيفرة الدخول un code d'accès: تمثل المفتاح المشفر الذي يمكن من خلاله استعمال وسيلة الدفع الإلكتروني وتختلف عن كلمة المرور في أن هذه الأخيرة للزبون حرية انشائها، في حين أن شفرة الدخول عادة ما تمنح من البنك للزبون لاستعمال وسيلة الدفع وتعد بأنظمة مشفرة لا يمكن فك تشفيرها إلا من طرف البنك الذي يملك مفتاح فك

[1]- نهلا عبد المومن، المرجع السابق، ص183.

التشفير، ومفاتيح الشفرات المدونة بها الأوامر أو الرسائل المكتوبة بالشفرة تحتاج إلى ترجمة لحلها وتساعد الشفرات على إخفاء البيانات حتى لا تفتح إلا لمن يملك الشفرة.

7- بيانات معلوماتية تسمح بالولوج إلى كل أو جزء من النظام المعلوماتي: وغالبا ما تتعلق هذه البيانات بمعلومات أخرى للمشترك[1] ماعدا المعلومات المتعلق بنوع الخدمة، وهوية المشترك وعنوانه أو أية معلومات أخرى عن موقع تركيب معدات الاتصال وكلمات المرور وشيفرة الدخول.

8- وسيلة الولوج: يقصد بوسيلة الولوج كل بطاقة أو اسطوانة أو شيفرة أو رقم حساب أو أي وسيلة يمكن استخدامها بمفردها أو بالاشتراك مع غيرها من الوسائل الأخرى للحصول على نقود أو أموال أو أي شيء آخر له قيمة أو يمكن استخدامها لمباشرة تحويل نقود، وتعني **وسيلة الولوج المصطنعة** كل وسيلة ولوج مزورة أو صورية أو مقلدة[2].

---

[1]- تنص المادة الثانية الفقرة 09 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات "معلومات المشترك :أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:

أ- نوع خدمة الاتصالات المستخدمة و الشروط الفنية و فترة الخدمة.

ب- هوية المشترك وعنوانه البريدي أو الجغرافي، أو هاتفه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.

ج- أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

[2]- محمد سامي الشوا، بحث بعنوان الجرائم المعلوماتية للتعدي على الذمة المالية للغير، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الرابع، ص1094.

ويتطلب ارتكاب هذه الجرائم غالبا حيازة وسائل الولوج la possession de moyen d'accès ومثال ذلك أدوات القرصنة outils de piratage أو أي أدوات أخرى ، فإن هناك دافعا قويا للحصول عليها لأغراض اجرامية، الأمر الذي يمكن أن يؤدي في النهاية إلى خلق نوع من السوق السوداء لإنتاج وتوزيع مثل هذه الأدوات[1].

ثانيا / بنود انفرد بها المشرع الجزائري

تنص المادة 394 /2 من قانون العقوبات الجزائري بقولها "يعاقب...**حيازة**[2] أو **افشاء** أو **نشر** أو استعمال لأي غرض كان **المعطيات المتحصل** عليها من احدى الجرائم المنصوص عليها في هذا القسم ".

وهذه الصورة نلاحظ أن المشرع الجزائري تفرد بها حيث لا نجدها قد ذكرت في نص المادة 06 من اتفاقية بودابست وكذلك المشرع الفرنسي لم يتطرق إليها.

والأفعال التي تتحقق بها هذه الصورة هي:

1- الإفشاء: نصت المادة394 مكرر02من قانون العقوبات الجزائري على تجريم افشاء المعطيات المتحصلة من جريمة من جرائم المساس بالمعالجة الآلية للمعطيات ، ولا يتطلب قانون العقوبات الجزائري حدوث نتيجة معينة من وراء فعل الافشاء بل يجرم هذا الأخير في حد ذاته والفرق بين الحيازة والإفشاء أو النشر أن الحيازة تقتصر على وجود

[1]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 319.

[2]- بالنسبة لفعل الحيازة سيتم شرحه في جريمة التزوير لوجود نص خاص بوسائل الدفع الإلكتروني كما أنه لا يعد صورة انفرد بها المشرع الجزائري إنما منصوص عليها ضمن الاتفاقيتين.

المعطيات غير المشروعة لدى الحائز فحسب دون قيامه بتقديمها للغير أما الإفشاء والنشر فهما يفترضان انتقال هذه المعطيات من حيازة هذا الشخص الى غيره من الأشخاص، أي أنه يقوم بتقديم هذه المعطيات غير المشروعة لأشخاص غيره ولا يقصرها عليه والذي يقوم بفعل الإفشاء هنا ليس شخصا ملزما بكتمان هذه المعطيات[1] بمقتضى عمله وإنما هو شخص تحصل على المعطيات بطريقة غير مشروعة وتعمد المشرع منع افشائها فلسنا هنا أمام حالة الزام الشخص بالمحافظة على السر المصرفي.

3-محل الجريمة: يتمثل في حيازة العناصر المشار اليها سابقا.

الفرع الثالث

الركن المعنوي لإساءة استخدام وسائل تقنية المعلومات

يتمثل في القصد بنوعيه العام و الخاص.

أولا / القصد العام

في كل الحالات يشترط في الجريمة أن ترتكب عمدا وبدون وجه حق.

بالنسبة للتصميم يجب أن يكون عمدا واراديا لمعطيات معلوماتية مقرصنة، أو أن يتم النشر عمدا لمعطيات معلوماتية مقرصنة، كما أن تعداد العناصر التي يتم حيازتها تخدم مباشرة إثبات النية الإجرامية[2].

ثانيا/ القصد الخاص

---

[1]-محمد خليفة، المرجع السابق، ص208.

[2]-هلالي عبد اللاه أحمد، المرجع السابق، ص88.

يتمثل القصد الجنائي الخاص في الغاية التي يصبو الجاني إلى تحقيقها من وراء ارتكاب تلك لجريمة وتطلبت المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ضرورة توفر القصد الخاص في هذه الجريمة بقولها " لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة ".

يستثنى مما تقدم الأدوات المشار إليها إذا تم استخدامها من أجل الاختبار المصرح به أو لحماية جهاز الحاسب الآلي فإنها لا تدخل في نطاق تطبيق هذا النص وهذا ينطوي بالفعل في تعبير دون حق[1].

[1]- هلالي عبد اللاه أحمد، المرجع السابق، ص89.

الفصل الثاني

الاشتراك في التزوير والجرائم الخاصة

ببيانات وسائل الدفع الإلكتروني

نظرا للتطور الذي حصل في و سائل الدفع الإلكتروني، فقد صاحب هذا التنامي ظهور نمط جديد من الجريمة ونسل جديد من المجرمين وصاحب انتشارها الواسع مجموعة من التحولات على جرائم التزييف والتزوير سواء في الأساليب أو الطرق أو في المحتوى والمضمون[1]، ويجب عدم الخلط بين جريمة التلاعب بالمعلومات المدخلة إلى النظام المعلوماتي أو المخزنة فيه (تغيير الحقيقة في البيانات المسجلة في دائرة النظام المعلوماتي) وبين تغيير الحقيقة في مستندات النظام المعلوماتي (التلاعب بالمستند المعلوماتي واستخدامه من أجل فائدة معينة التزوير المعلوماتي)، وحسن فعل المشرع الفرنسي حينما أخرج جريمة تزوير المستندات المعالجة آليا من جرائم الاعتداء على نظم المعالجة الآلية إذ يعتبر ذلك أمر منطقي لاختلاف المصلحة المحمية بالقانون والتي تقف وراء تجريم كل منهما وبذلك يكون المشرع الفرنسي قد فصل بين تغيير الحقيقة في المكونات غير المادية في نظام المعالجة الآلية للمعطيات (المساس بسلامة المعلومات أو التلاعب بالمعلومات المخزنة بالنظام المعلوماتي في المادة 323-3 من قانون العقوبات الفرنسي والتي تقابلها المادة 394مكرر 1 من قانون العقوبات الجزائري، وبين تغيير الحقيقة في محررات نظام المعالجة أو مستخرجاته (الاعتداء على أصالة المعلومات) التي شملها بالمادة 441-1[2] من نفس قانون العقوبات الفرنسي والتي لا توجد مادة تقابلها في قانون العقوبات الجزائري مما يوحي بفراغ تشريعي على المشرع الجزائري تداركه لتفادي الخلط بين جرائم المساس بسلامة

[1]- حوالف عبد الصمد، المرجع السابق، ص 323.

[2]- أصبحت المادة 441-1 من قانون العقوبات الفرنسي تشمل التزوير المعلوماتي .

المعطيات المعالجة آليا وبين جريمة التزوير المعلوماتي، وحتى في حالة هذا التعديل نبقى بحاجة إلى نص خاص في قانون النقد والقرض لتجريم تزوير وتزييف وتقليد وسائل الدفع الإلكتروني نظرا لخصوصيتها كما سنرى لاحقا ونظرا لأن المشرع الجزائري وإلى حد اليوم لم يجرم التزوير المعلوماتي رغم أنه خصص فصل كامل لجرائم التزوير (المواد 197-241 من قانون العقوبات الجزائري) وكذا عدم وجود نص خاص بالتزوير في قانون النقد والقرض الجزائري سنركز دراستنا على القوانين الفرنسية، من قانون العقوبات، والقانون المتعلق بأمن الشيكات وبطاقات الدفع والسحب، وقانون النقد والمال المعدل والمتمم.

كما أن المشرع الفرنسي استحدث بنص المادة 1/441 من قانون العقوبات الفرنسي لسنة 1994 أمرا هاما جديدا وهو أن طريق تغيير الحقيقة (أي طرق التزوير) لم تعد محددة قانونا على سبيل الحصر كما كان قديما[1].

على المشرع الجزائري واجب التعديل والتحديث لما تفرضه المستجدات من نصوص تتعلق بالتزوير الإلكتروني عموما وتزوير وسائل الدفع الإلكتروني خصوصا حتى لا تتأخر تشريعاتنا في الجزائر عن مواكبة العصر، فبالنسبة للمشرع الفرنسي فالمواد 323-1 و ما يليها في قانون العقوبات الفرنسي المتعلقة بأنظمة المعالجة الآلية للمعطيات يمكن أن يتم تطبيقها من أجل معاقبة بعض الممارسات الاحتيالية المتعلقة باستعمال بطاقات الدفع بقدر ما تكون العمليات التي تتم بواسطة البطاقات مسيّرة بعملية حاسوبية، فحكم محكمة الجنح

[1]- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي،2005، ص574.

في باريس سنة 2000 أكد أن نظام البطاقة الزرقاء هو نظام معالجة آلية للمعطيات و اعتبرت المحكمة أن كل تزوير لنهاية دفع إلكتروني مرتبط بالنظام يمكن أن يكون مصنف في نظام المعالجة الآلية للمعطيات، ويترجم بمعنى واسع للدخول أي يشمل كل أنواع الاختراق للنظام نظام المعالجة الآلية للمعطيات[1].

نظرا لخصوصية تزوير وسائل الدفع الإلكتروني نتناول في المبحث الأول (الاشتراك في التزوير واستعمال وسائل الدفع الإلكتروني المزورة، وفي المبحث الثاني (الاشتراك في الجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني).

المبحث الأول

الاشتراك في التزوير والاستعمال لوسائل الدفع الإلكتروني المزورة

توجد في قانون النقد والمال الفرنسي نصوص تجريمية أكثر خصوصية تتعلق بالاحتيالات المريعة على نحو متزايد والمقترفة بالبطاقات خصوصا[2]، وهذا حسب رأينا لأن المشرع الفرنسي ينظر إلى طبيعة ومكونات وسائل الدفع الإلكتروني التي ينبغي أخذها بعين الاعتبار في موضوع تزوير وتقليد وسائل الدفع الإلكتروني.

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 261

[2]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit ,effet de commerce cheque, carte de paiement, transfert de fonds, 6edition,2006,lexis Nexis,p385 .

رغم أن المصارف لاتزال تصر على توافر الأمان الذي تتمتع به البطاقات في حين تزايدت حالات التزوير ولا تعترف المصارف بذلك علنا أمام الجمهور[1]، حفاظا على سمعتها وعلى استعمال وسائل الدفع الإلكتروني.

هاتين الجريمتين غالبا ما تتم بتواطىء المصرفي مع الزبائن لأنها غالبا ما تتم باستعمال الأوراق التجارية ووسائل الدفع، أو استعمال المزور بهدف الدخول في عمليات مصرفية والحصول على قروض باستعمال وثائق مزورة[2]، المطلب الأول (المسؤولية الجزائية على أساس الاشتراك في تزوير وتزييف وتقليد وسائل الدفع الإلكتروني)، وفي المطلب الثاني (المسؤولية الجزائية عن الاشتراك في استعمال وسائل الدفع الإلكتروني المقلدة والمزورة).

المطلب الأول

المسؤولية الجزائية عن الاشتراك في تزوير وتزييف وتقليد وسائل الدفع الإلكتروني

يقوم الجناة بتزوير وسائل الدفع الإلكتروني بطريق التقليد أو الاصطناع لاستعمالها في عمليات السحب وتحمل هذه الجرائم في الوقت الحالي أهمية كبرى خاصة في عمليات الدفع الإلكتروني والتحويل الإلكتروني للأموال بعد دخول الحاسب الآلي كأداة رئيسية يقوم عليها العمل المصرفي إلا أن المصارف عموما تخفي أو لا تفصح عن جرائم تزوير وسائل الدفع

[1]-علي نحلة، النشاطات المشبوهة غسل الأموال الإلكتروني، آليات كشفها وكيفية التعرف عليها والتبليغ عنها، مجلة اتحاد المصارف العربية، عدد حزيران /يونيو 2005، ص72.

[2]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 136.

المحرر ليشمل المحررات الإلكترونية كما فعل المشرع الفرنسي الذي عدل المادة 441-1[1] من قانون العقوبات الفرنسي بإضافة عبارة " ou tout autre support " لتشمل كل صور التزوير ومهما كانت الوسيلة أو الدعامة التي تم عليها، وطرق التزوير لم تعد محددة على سبيل الحصر فالمادة 441 من قانون العقوبات الفرنسي عدلت سنة 2000 ورغم أن المشرع الجزائري عدل قانون العقوبات بعدها إلا أنه لم يعدل من النصوص المتعلقة بالتزوير، كما أنه وبتعديله لقانون النقد والقرض لسنة 2010 لم يعدل الشق الخاص بالجرائم ولم يتكلم عن تزوير وسائل الدفع الإلكتروني، رغم أنه عدل اختصاص بنك الجزائر في مجال وسائل الدفع الإلكتروني إلا أنه لم يعدل الشق الجزائي، كما أنه لم يصاحب هذه الوسائل بالحماية الجزائية في القانون التجاري كما فعل المشرع المغربي مثلا ولا ندري لماذا غياب الربط بين التعديلات التي حصلت في الجانب الإلكتروني وغيابها بالنسبة للجانب الجزائي.

تنص المادة L163-3 من قانون النقد والمال الفرنسي على جرائم تزوير وتقليد وسائل الدفع الإلكتروني كجرائم مستقلة وجديدة في مجال تكنولوجيا المعلومات ومجال الدفع الإلكتروني وهذا رغبة من المشرع الفرنسي بالتصدي لهذا النوع من الجرائم وحسما للجدل القائم سابقا بخصوص مدى امكانية تطبيق النص العام في قانون العقوبات على هذه الجرائم، وكذا حسما للنزاع الذي كان يتمحور سابقا حول الفرق بين التزوير والتقليد حيث هناك من يعتبر

[1]- ART 441/1 « Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit **ou tout autre support** d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende ».

معطيات مصمّمة أو معدّة خصيصا من أجل تزوير بطاقة دفع أو سحب[1]، فالتجريم الجديد مس التصرفات التحضيرية للقيام بالغش[2]، وبالتالي هي عبارة دائما عن وسائل للاشتراك في جرائم أخرى والقمع اليوم مركز على نصوص خاصة بوسائل الدفع الإلكتروني أكثر من النصوص العامة في قانون العقوبات الفرنسي في الفعالية[3].

وتنص المادة L163-4 من قانون النقد والمال الفرنسي على ما يلي:

L163-4« Est puni de sept ans d'emprisonnement et de 750 000 euros D'amende le fait, pour toute personne, **de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour Commettre les infractions** prévues au 1° de l'article L163-3».

وانتهجت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال المادة الثامنة عشر نفس النهج الذي انتهجه المشرع الفرنسي من خلال نصها على تمديد الاستخدام غير المشروع لوسائل الدفع الإلكترونية بنصها على التزوير والتقليد وهذا من خلال الفقرة الأولى على مايلي : "كل من زور أو اصطنع أو وضع أجهزة أو مواد **تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت** ..."، فالاتفاقية اعتبرتها من قبيل

[1]- Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition, 2006, lexis Nexis, p385.
[2]-Pierre storrer, droit de la monnaie électronique, édition RB, p247.
[3]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit, 258.

المواد والصور المساعدة والمسهلة لارتكاب الجرائم الخاصة بتقليد وتزوير وسائل الدفع الإلكتروني.

-**الاصطناع (de fabriquer):** كتصنيع واجهات مزورة للموزعات البنكية أو أجهزة لقرصنة أرقام البطاقات البنكية[1]. يتحقق بخلق محرر لم يكن له وجود من قبل ونسبته كذبا إلى غير مصدره ويصحب غالبا بطريقة أخرى من طرق التزوير[2] كما يعد من الطرق المادية التي يقع بها التزوير[3] يعني خلق وسيلة دفع لم تكن موجودة من قبل ونسبتها إلى المصدر، فقد يقوم المعتدي بخلق بطاقة يمكن أن تعمل كالبطاقة الأصلية لكنها تحتوي أرصدة وهمية أو احتيالية لم يجر الدفع مقابلها إلى المصدر كي يقوم بعملية التحميل[4] وبالتالي ليس هناك ما يمنع من اصطناع بطاقة بنكية جديدة دون أن تكون على غرار بطاقة أخرى وفي هذه الحالة يدخل الاصطناع تحت مدلول التزوير[5].

-**الوضع تحت التصرف:** للمواقع المخصصة لتصنيع أرقام البطاقات الكاذبة أو قرصنتها بمناسبة التحويلات على الأنترنت أو وضع تحت تصرف مواقع متخصصة مسمات carding[6]، أو بالوضع تحت التصرف على الانترنت لبرامج مضاهاة أرقام البطاقات البنكية، أو المعلومات المرتبطة بتشفير معطيات الأمان المتبادلة خلال التحويلات على

---

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit, 258.

[2]- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص144.

[3]- محمد حماد مرهج الهيتي، المرجع السابق، ص297.

[4]- طارق محمد حمزة، المرجع السابق، ص296، 297.

[5]- ضياء أحمد علي نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص 199.

[6]-pierre storrer, droit de la monnaie électronique, édition RB, p247.

-التوفير و الوضع تحت التصرف لأجهزة أو مواد أو برامج معلوماتية أو معطيات مساعدة على التزوير والتقليد «céder d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données».

ومصطلح التوفير أو الوضع تحت التصرف يقتضي اتاحة المعلومات وجعلها تحت تصرف الغير وفي حيازته أي توفير كل ما من شأنه تسهيل ارتكاب الجرائم[1]، وبالتالي تشمل هذه الحالة كل توفير لكلمات المرور أو شفرات الدخول خاصة وأن هناك برامج تساعد على فك الشفرات وتخمين كلمات السر للدخول إلى نظام استعمال وسائل الدفع الإلكتروني وبالتالي يشمل كل توفير للأجهزة والوسائل والبرامج المعلوماتية أو المعطيات التي تمكن الشخص من الدخول أو البقاء أو التلاعب بأنظمة تشغيل وسائل الدفع الإلكتروني، والفرق بين التوفير والتجميع أنه في هذا الأخير لا تتعدى حيازة المعطيات والتصرف فيها على من يقوم بالتجميع، بينما في التوفير فإن دائرة الأشخاص الذين سيحصلون على المعطيات ويتصرفون فيها تتعدى ذلك الشخص وتتسع بذلك وتزيد الخطورة بازدياد هؤلاء[2]، وتعاقب عليه المادة 394مكرر 02من قانون العقوبات الجزائري ومصطلح الوضع تحت التصرف « La mise à disposition » يشير إلى وضع أجهزة على الخط en ligne ليتم استخدامها بواسطة الغير، كما يضم هذا المصطلح من ناحية أخرى انشاء وتجميع الروابط بين الخطوط

[1]- بوربابة صورية، المرجع السابق، ص124.

[2]- محمد خليفة، المرجع السابق، ص203.

المتشعبة la compilation d'hyperliens من أجل الوصول إلى هذه الأجهزة[1] وذلك عن طريق الاحالة لبرنامج يتصل ببرامج مصممة على سبيل المثال لا تلاف بيانات وسائل الدفع الإلكتروني أو التدخل في عمل نظام تشغيل الدفع الإلكتروني أو تصميم فيروسات للتدخل في عمل نظام البنك ككل، أو الوضع على الأنترنت لبرامج إنشاء أرقام بطاقات على مواقع مخصصة تسمى carding[2] و تنص المادة الثامنة عشر من الاتفاقية "كل من زور أو اصطنع أو وضع مواد تساعد على تزوير أو تقليد أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت ..." مما يدل على أنها أخذت بالاتجاه القاضي بتمديد القمع في جرائم تزوير أو تزييف أو تقليد وسائل الدفع الإلكتروني.

الفرع الثالث

علاقة تزوير وسائل الدفع الإلكتروني بالجريمة المنظمة

أكد تقرير مقدم للجنة الفرعية لمجلس النواب الأمريكي بأن نسبة كبيرة من النشاط الاجرامي السنوي المتعلق بتزوير بطاقات الائتمان داخل الولايات المتحدة الأمريكية وخارجها يتم عن طريق جماعات اجرامية دولية والتي يصعب على أي شخص – لا ينتمي إليها –الدخول في تنظيمها، الشيء الذي يصعب مهمة التحقيق ومعرفة الأساليب والطرق الحديثة في عمليات التزوير للبطاقات[3].

---

[1] – هلالي عبد اللاه أحمد، المرجع السابق، ص320 .

[2] - Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit, 258.

[3] – كما أكد التقرير أن العصابات الاجرامية الاسيوية هي التهديد الرئيسي لأمن البطاقات، أنظر معادي أسعد محمد صوالحة، المرجع السابق، ص 467.

استغلت عصابات الجريمة المنظمة "الامكانيات المتاحة في وسائل الأنترنت في تخطيط وتمرير وتوجيه المخططات الاجرامية وتنفيذ وتوجيه العمليات الاجرامية بيسر وسهولة" ومثال ذلك إنشاء مواقع خاصة بها على شبكة الأنترنت لمساعدتها في إدارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع أعمال تبييض الأموال[1]، والجريمة المنظمة المرتبة باستعمال وسائل الدفع الإلكتروني أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان وإنما أصبح انتشارها على نطاق واسع، ويمكن القول أن هناك علاقة تبادلية بين وسائل الدفع الإلكتروني والجريمة المنظمة فكلما انتشر استعمال وسائل الدفع الإلكتروني انتشرت الجريمة المنظمة فإن أعضاء التنظيمات الاجرامية هم الذين يبادرون الى اختراق إجراءات الحماية التي يتم ابتكارها لحماية وسائل الدفع الإلكتروني من أجل المحافظة على مداخيل التنظيمات.

والملاحظ أن طبيعة تزوير البطاقة البنكية يرتبط بالجريمة المنظمة حيث أن هذه الجريمة من الجرائم العابرة للحدود وفي هذا المجال تم رصد العديد من جماعات الجريمة المنظمة التي تتخذ من هذا النشاط أسلوبا لها[2]، وفعالية التدبير القمعي للتزوير يصبح من الصعب تقديره

---

[1]-صالح بن سعود الصالح، مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي، مداخلة مقدمة إلى الدورة التدريبية لمكافحة الجرائم الاقتصادية، المنظم من طرف كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض ،خلال الفترة من 20 -1428/2/24هـ الموافق لـ10-14 /2008/3.

[2]-ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص 218.

الاشتراك في التزوير المعلوماتي لوسائل الدفع الإلكتروني هم العاملين بالبنوك، وحاملي وسائل الدفع الإلكتروني الذين يتعمدون تقديم وسائل الدفع الإلكتروني للغير الذي يقوم بالتزوير، أو التجار الذين يتفقون مع الغير في حالة سرقة البطاقات أو فقدانها أو اساءة استعمالها للمساعدة على تزوير عملية الدفع.

تتفاوت الأساليب هنا من حيث قدرتها على النفاذ الى نظام المعلومات في المصرف فبعضها أقوى من الاخرى كما أن بعضها قد يعتمد على المتاح من المعلومات الشخصية عن أصحاب أرقام الحسابات، وبالتالي توجيه أوامر الدفع، أو الحصول على بطاقات بنسخ ثانية أو بما يتقاطع مع البطاقات الصحيحة[1]، سنتناول من خلال هذا الفرع أولا(التغيير للحقيقة)، ثانيا (تقليد وسائل الدفع الإلكتروني)، ثالثا (اشكالية المحل في وسائل الدفع الإلكتروني كمحررات إلكترونية لجريمة التزوير)، ورابعا (مدى اشترط توفر عنصر الضرر في مختلف القوانين).

أولا /المساعدة على تغيير الحقيقة في بيانات وسائل الدفع الإلكتروني

يتمثل الركن المادي للاشتراك في التزوير بالمساعدة على تغيير الحقيقة دون أن يشمل هذا التغيير الحقيقة برمتها إنما جزء فقط منها[2].

يعتبر تغيير الحقيقة جوهر الركن المادي في جريمة التزوير حيث لا يتصور قيام جريمة التزوير دونها وتعرف المادة العاشرة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

[1]- علي نحلة، المرجع السابق، ص72.

[2]- غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص138.

جريمة التزوير المعلوماتي على أنها " استخدام وسائل تقنية المعلومات **من أجل تغيير الحقيقة في البيانات** تغييرا من شأنه احداث ضرر، وبنية استعمالها كبيانات صحيحة "[1] ونخلص إلى نتيجة مهمة من خلال إضافة الاتفاقية لعبارة تغيير الحقيقة في البيانات وهذا حسب رأينا تفاديا للنقاش الذي كان يدور حول أنواع التزوير هل المقصود به التزوير المادي أو التزوير المعنوي وحسما للجدل استعملت الاتفاقية هذا المصطلح وتقع جريمة التزوير بتغيير الحقيقة سواء كان هذا التغيير كليا أو جزئيا ويلاحظ أن المقصود بتغيير الحقيقة ليس تغيير الحقيقة المطلقة وإنما تغيير الحقيقة النسبية[2] وبالتالي من لم يغير في البطاقة الصحيحة شيئا وإنما عند استعمالها وضع توقيعا مزورا يكون قد ارتكب جريمة التزوير في وسائل الدفع الإلكتروني وكذلك اعتراض الجاني لأمر الدفع الإلكتروني الموجه من بنك لآخر وتزويره حتى يتم الدفع لحسابه، ويتخذ التزوير في وسائل الدفع الإلكتروني باعتبارها من المحررات الإلكترونية إحدى الصورتين: الأولى تتمثل في التلاعب في معلومات المحرر داخل نظام الحاسب الآلي وذلك لتغيير الحقيقة في وسيلة الدفع الإلكتروني سواء بتعديل المعلومات أو محوها أو جزء منها، والثانية تتمثل في إدخال معلومات غير صحيحة لخلق وسيلة دفع إلكتروني غير صحيحة وكلتا الطريقتين تتم بنية استعمال وسيلة الدفع الإلكتروني فيما زور من أجله.

---

[1]- أنظر المرسوم الرئاسي رقم 14-252، المؤرخ في 13ذي القعدة عام 1435 الموافق ل 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج ر عدد 57، 2004.

[2]-جميل عبد الباقي الصغير، المرجع السابق، ص135.

الملاحظ كذلك أن المشرع الفرنسي ونظيره المغربي ذكرا لفظ التزوير دون أن يحددا الطرق الخاصة به[1]، وهذا يعني أن أي تغيير في وسيلة الدفع الإلكتروني سواء بتغيير الأرقام، أو الامضاءات أو الأسماء أو أي طريقة من طرق التزوير للمعطيات الإلكترونية الخاصة بوسيلة الدفع الإلكتروني مشمولة بالنص[2] فمثلا في حالة وضع إمضاءات وأختام مزورة إذا نظرنا لإمكانية وقوع التزوير في المحررات الإلكترونية بهذه الطريقة وجدناه أمرا واردا فعند استخدام البطاقة داخل ماكينة السحب الآلي للنقود فإنه سيطلب منك إدخال الرقم السري الخاص بالبطاقة ففي حالة البطاقة المزورة والقيام بإدخال الرقم السري يكون قد وضع إمضاء مزور لأنه يعتبر توقيعا إلكترونيا.

وكذلك بالنسبة للنقود الإلكترونية والتي يقوم الموقع الخاص بها بتسليم حافظة نقود إلكترونية في شكل برنامج يتم تخزينه عبر الحاسب الآلي للزبون، بحيث إذا رغب الزبون في الشراء أو الدفع يتم سداد القيمة دون الحاجة إلى استخدام البطاقة، فإذا تمكن أحد الهاكرز من

---

[1]- ضياء أحمد علي نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص200.

[2]- علما أن المادة 216 من قانون العقوبات الجزائري نجد تحدد طرق التزوير و تتمثل فيما يلي:

- إما بتقليد أو تزييف الكتابة أو التوقيع.

-إما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات، وضمن الفقرتين 1و2 ما يصطلح عليه بالتزوير المادي ويشمل وضع توقيع مزور أو حذف أو إضافة أو تغيير لمضمون السند أو اصطناع هذا المحرر (السند).

في حين تنص الفقرتين 3و4 على:

- إما بإضافة أو إسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو إثباتها.

- وإما بانتحال شخصية الغير أو الحلول محلها.

الاستيلاء على هذا البرنامج وتغيير قيمته بالأعلى ثم استخدامه في الاستيلاء على الأموال بطريقة غير مشروعة وقع التزوير في هذا المحرر الإلكتروني[1].

ثانيا / المساعدة على تقليد وتزييف وسائل الدفع الإلكتروني

في 15 نوفمبر 2001 تبنى المشرع الفرنسي مخالفات أكثر اختصاصا في مكافحة تزوير و تقليد البطاقات البنكية و عدل بأمر 15 جويلية 2009 و تم إنشاء قسم مخصص في قانون النقد والمال الفرنسي للمخالفات المتعلقة بالشيك ووسائل الدفع الأخرى[2] حيث تبنى تدابير تسمح بالتجريم بطريقة متخصصة لتقليد أو تزوير وسائل الدفع الإلكترونية.

يمكن أن يتم التغيير سواء بالتقليد أو التزوير أو التزييف ويقصد بالتقليد عموما صناعة شيء على غرار الآخر أي صناعة وسيلة دفع إلكتروني كاذبة تشبه وسيلة دفع إلكتروني صحيحة أي محاكاة وسائل الدفع الإلكتروني الصحيحة ولا يشترط أن تكون على درجة عالية من الإتقان وإنما يكفي أن تكون الوسيلة في شكل ينخدع به الناس ويوهمهم بأصالتها أو يتمكن عند استخدامها من سحب النقود رغم أن أجهزة الصراف الآلي تزود ببرامج لكشف التقليد ولا تقبل وسائل الدفع الإلكتروني المشكوك فيها، كما يعد التقليد من الطرق المادية

---

[1]– ومثال ذلك ضبط عملية قرصنة تعرضت لها البنوك بدولة الامارات العربية المتحدة حيث قامت عصابة من المحترفين في علوم الحاسب الالي بإدخال جهاز skimming في فتحات ادخال البطاقة بماكينات السحب الالي للنقود وتمكنت من خلال هذا الاسلوب من تسجيل بيانات جميع البطاقات التي تعاملت مع هذه الماكينات، مع القيام بتصوير العملاء حاملي البطاقات عن طريق كاميرا صغيرة ملصقة في الماكينة فوق فتحة الصراف مصوبة على لوحة المفاتيح لمعرفة الرقم السري ، وعندما حصلت العصابة على ذلك، قامت باستخدام البطاقات المزورة الحاملة للبيانات الصحيحة ،وادخال الأرقام السرية الصحيحة دون ارادة حاملي البطاقات والاستيلاء على مبالغ تقدر ب22مليون درهم اماراتي أي ما يقارب 6ملايين دولار، أنظر ايهاب فوزي السقا، المرجع السابق، ص 67.

[2]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 255.

التي يقع بها التزوير[1] ويقصد بالتقليد التزييف أيضا فالتزييف هو كل اصطناع لأية عملة صحيحة أو تقليدها وكل تلاعب في قيمة العملة الصحيحة وكل ترويج أو إدخال من الخارج لعملة مزيفة متى كان ذلك بقصد وضع العملة المزيفة في التداول أو بقصد الغش أو الإضرار[2]، وغالبا ما يكون التقليد مصحوبا بإحدى طرق التزوير المادي الأخرى[3]، ويبدو أن السبب الذي دفع المشرع إلى النص على التقليد بالذات أنه الوسيلة الوحيدة –حتى الآن– التي تحقق للمتهم غرضه في استعمال البطاقة بعد ذلك فاستخدام البطاقة المقلدة يستلزم معرفة الرقم السري الخاص بها، ولكن ليس هناك ما يمنع من اصطناع بطاقة بنكية جديدة دون أن تكون على غرار بطاقة أخرى وفي هذه الحالة يدخل الاصطناع تحت مدلول التزوير[4] وبالتالي فالمشرع الفرنسي عندما نص على تزوير وتقليد وتزييف وسائل الدفع الإلكتروني كان يقصد الإلمام بكل صور المساس بوسائل الدفع الإلكتروني لأن التزوير غالبا يكون بالنسبة للأوراق التجارية، والتزييف يكون بالنسبة للعملة كما هو الحال بالنسبة للنقود الإلكترونية، و التقليد يعني الاصطناع الكلي لوسيلة الدفع والتي تحوي شقين أحدهما مادي والآخر معنوي[5] الدخول الغير شرعي للبطاقة عن طريق استعمال البرامج و سحب

---

[1]– محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقات الائتمان الممغنطة، دار الكتب القانونية، دار شتات للنشر والبرمجيات،2009، ص199.

[2]–أنظر عبد الفتاح سليمان، طرق اكتشاف تزوير الشيكات والمسؤولية عنه، دار الكتب طبعة 2005، ص 09.

[3]– جميل عبد الباقي الصغير، القانون الجنائي والتكنلوجيا الحديثة، المرجع السابق، ص143.

[4]– ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص 199.

[5]– رغم اقرارنا بأنه يصعب التمييز من الناحية الواقعية والفصل بالنسبة لوسائل الدفع الالكتروني هل نحن أمام تزوير أو تقليد أو تزييف لتداخل مفهوم الأوراق التجارية مع العملة مع البرامج التي تحكم سير وسائل الدفع الإلكتروني.

معلومات يمكن أن يكون مشكل لجريمة التقليد[1]، كما يجب أن نأخذ بعين الاعتبار أننا انتقلنا من التزوير والاحتيال المحلي إلى التزوير والاحتيال العالمي التأثير حيث أن تقليد وقرصنة وسائل الدفع يمثل تهديدا مباشرا وفوريا وسريعا للاقتصاد العالمي والمحلي وحقوق الأفراد بغض النظر عن موقعهم في العالم[2]، وقد يفسر منهج المشرع بالرغبة في الفصل بين التزوير الذي يقع على البطاقة ذاتها كمحرر، والتزوير المادي الذي يأخذ صورة اصطناع بطاقة على غرار أخرى[3]، وهو ما يأخذ مفهوم التقليد **لذلك خص المشرع الفرنسي تقليد وسائل الدفع الإلكتروني بالذكر حتى لا يحتج بمبدأ حظر القياس في المادة الجزائية وبأن النص العام يشمل التزوير فقط دون التقليد.**

أما تزييف العملة الإلكترونية : يعني الاعتماد الكامل على برنامج الحاسب الآلي و إمكانية نسخ البرنامج بما يعني مضاعفة قيمة النقد الإلكتروني المصدر بصورة احتيالية أي تزييف العملة الإلكترونية[4].

ثالثا /إشكالية المحل في وسائل الدفع الإلكتروني كمحررات إلكترونية لجريمة التزوير

المحل في جريمة التزوير هو المحرر[1] ومناط الحماية في المحرر هو مضمونه إذ لابد أن يكون مضمونه ذو طابع قانوني بحيث إذا خلا من هذا الطابع لا يمكن وصف ما تم تنظيمه

---

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 162

[2]- حوالف عبد الصمد، المرجع السابق، ص 324.

[3]- نقلا عن ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص 198.

[4]- نبيل صلاح محمود العربي، الشيك الالكتروني والنقود الرقمية، دراسة مقارنة،، دراسة مقارنة ، مقدم لمؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون ،المنظم من طرف كلية الشريعة والقانون وغرفة تجارة وصناعة دبي ،المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الأول، ص 37.

بالمحرر في إطار جريمة التزوير[2] لذلك ينبغي بيان إشكالية المحل بالنسبة لوسائل الدفع الإلكتروني لأنه الوعاء الذي يتضمن الحقيقة التي يتم التلاعب فيها وتغييرها خاصة وأن مدلول المحرر لم يتم تعريفه من طرف المشرع الجزائري، لكن تجدر الإشارة إلى أن بعض الفقه الفرنسي يرى إمكانية تغليب روح النصوص واعتبار ما يظهر على شاشة الحاسب شكلا مستحدثا للمحرر[3].

بالنسبة للتحويلات الإلكترونية يتم ذلك بتوجيه أمر من المدين إلى بنكه بالوفاء من حسابه إلى دائنه إلكترونيا باتخاذ الإجراءات المصرفية اللازمة لتحويل مبلغ معين لحساب بنك المستفيد، أو بتوجيه الدائن أمر إلى بنكه بتحصيل مبلغ من حساب مدينه بناء على تفويض مسبق بواسطة رسالة إلكترونية، وهذه الأوامر تعتبر من قبيل المحررات أو المستندات التي من شأنها أن تحمل أثرا قانونيا بين أطراف التعامل[4].

أما بالنسبة للبطاقات المصرفية فإن الإشكالية أثيرت من ناحيتين الأولى تتعلق بالجسم المادي للبطاقة والثانية بالنسبة للشريط الممغنط باعتباره الكيان المعنوي للبطاقة وهذا نظرا لاستخدام البطاقات المصرفية في وسط إلكتروني، فإن البيانات المسجلة عليها تكون على دعامة بلاستيكية يمكن رؤيتها بالعين، وكذلك هناك من البيانات التي يتم تشفيرها داخل شريط مغناطيسي أسود لا يمكن قراءته إلا بواسطة أجهزة الحاسب الآلي، وهذه البيانات

---

[1]- يسمي الفقه المحرر الإلكتروني بالوثيقة المعلوماتية والمستند الالكتروني.

[2]- محمد حماد مرهج الهيتي، المرجع السابق، ص251.

[3]- أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثانية، 2007، ص137.

[4]- ايهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، مصر، 2008، ص 44،45.

تتضمن معلومات عن الزبون حامل البطاقة والبنك المصدر لها، وحدود المبلغ المسموح به للتعامل بها وتاريخ انتهاء صلاحيتها وغيرها من البيانات التي تنظم عملية التعامل بها ومنه فجسم البطاقة ينطبق عليه وصف المحرر لأنه يتضمن بيانات خاصة عن حاملها وعن الجهة التي أصدرتها وعن تاريخ صلاحيتها أو انتهائها وهذه البيانات في مجملها تجعل البطاقة مستندا[1] يمكن استخدامه فيما أعد له[2]، فالرأي الراجح يرى أن بطاقات الائتمان تعد من المحررات الإلكترونية التي يتم استخدامها في بيئة إلكترونية[3].

إن التغيير الذي يمس بيانات البطاقة وإن كانت مصنوعة من مادة بلاستيكية في الغالب أو يتعرض لشكلها من شأنه أن يحقق التغيير المتطلب لتحقق جريمة التزوير لأنه ليس هناك ما يمنع من انطباق وصف المحرر عليها إلا أن تغيير الحقيقة المدمجة بالشرائط الممغنطة بطريقة غير مرئية أثار في الفقه خلافا بشأن تحقق وصف المحرر باعتباره المحل الذي يضع فيه الناس ثقتهم، والذي تتعرض الحقيقة الثابتة فيه للتغيير وبشكل خاص البيانات والمعلومات المدمجة بالشريط الممغنط[4] لذلك نلاحظ أن الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات عندما عرفت التزوير استعملت مصطلح "**من أجل تغيير الحقيقة في**

---

[1]– يقصد بالمستند في الاصطلاح القانوني كل دعامة مادية (مكتوب أو أي شيء) يصلح لأن تكون عليه معلومات أو آراء والتي هي غير مادية، أو هي الشيء المادي الذي يمكن أن يدون عليه شيء معنوي ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص، أو شريط ممغنط أو خلافه) يصلح لأن يكون د عامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة وتم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله ، أنظر أمال قارة، المرجع السابق، ص134.

[2]– محمد حماد مرهج الهيتي، المرجع السابق، ص 275.

[3]– ايهاب فوزي السقا، المرجع السابق، ص 45.

[4]– محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقات الائتمان الممغنطة، المرجع السابق، ص278.

البيانات"، ولمعالجة إشكالية مدى انطباق جريمة التزوير على التغيير الواقع على المعلومات المقروءة، وعدم انطباق جريمة التزوير على التغيير الواقع على المعلومات غير المقروءة كحل جزئي يثير إشكالية أخرى تترتب على مدى تحقق جريمة استعمال محرر مزور إذا تم استعمال البطاقة بعد وقوع التغيير على المعلومات المقروءة، وعدم انطباق وصف جريمة استعمال محرر مزور على البطاقة بعد التغيير الذي يصيب التلاعب بالمعلومات غير المقروءة، الأمر الذي يؤدي إلى نتيجة غير منطقية وهي عدم إمكانية تجزئة مكونات البطاقة مع إقرارنا بأهمية التغيير في الجزء غير المقروء، إلا أنه لا يمكن التعلل بأنه من غير الممكن رؤية المعلومات المتضمنة في الشريط الممغنط لأن هذا فيه نوع من الخلط بين ضرورة معرفة مدلول المحرر بحاسة العين ومدى ظهور هذا المعنى أو المدلول كما أن وجود المعلومات ضمن الشريط الممغنط واحتياجنا إلى أجهزة خاصة للتعرف على مضمونها لا ينفي وجود المحرر.

رابعا / مدى اشترط توفر عنصر الضرر في مختلف القوانين

بالرغم من أن المشرع الفرنسي لم يشترط الضرر لقيام جريمة تزوير وتقليد وسائل الدفع الإلكتروني إلا أن الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات اشترطت توفر الضرر في جريمة التزوير الإلكتروني[1] لأنه من المستقر عليه ضرورة توفر هذا الشرط ويبقى التزوير الإلكتروني من معوقات تطبيق التجارة الإلكترونية عموما ووسائل الدفع

[1]– اشترطت المادة العاشرة من على توفر الضرر بنصها "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه احداث ضرر ...".

خصوصا لذلك يسعى القائمون على تطوير تقنيات المعلومات إلى إيجاد طرق للحد منه، كما أن الخسائر المادية التي تترتب على إثبات التزوير تكلف مبالغ مالية كبيرة، ولا يعد تغيير الحقيقة تزويرا إلا إذا نشأ عنه ضرر أو كان من شأنه إحداث ضرر[1]، بل إن احتمال وقوع الضرر يكفي لقيام جريمة التزوير وهذا ما عبرت عنه الاتفاقية العربية بعبارة **من شأنه إحداث ضرر** وهذا يفسر أن المشرع الفرنسي أخذ بفكرة الخطر بدلا من فكرة الضرر لأنها تتميز بكونها أعم وأشمل وأوسع مدى من فكرة الضرر لأن مجرد الخطر خاصة في جرائم التقنية قد يسبب الكثير من الضرر[2] وهذا لأن الفكر الراسخ كان يرى أن النتيجة الإجرامية دائما ما تشكل ضرر معين محدد وهو ما يظهر في صورة ضرر مادي ملموس في العالم المادي، ظهرت فكرة الخطر لتضيف معنى جديد لمدلول النتيجة الإجرامية فلم تعد فكرة الضرر هي المكون للنتيجة الإجرامية وإنما أضيفت إليها الخطر لكي تشكل تهديدا للمصالح المحمية، وبالتالي المصالح المحمية في وسائل الدفع الإلكتروني ومصلحة البنوك والمصالح المالية والاقتصادية يبرر إزالة اشتراط الضرر بالنسبة للجرائم المتعلقة بتزوير وسائل الدفع الإلكتروني.

بالنتيجة نحبذ ما اتجه إليه المشرع الفرنسي وهو عدم اشتراط عنصر الضرر في جرائم تزوير وتزييف وتقليد وسائل الدفع الإلكتروني لأن هذه النصوص الإجرامية جديدة وتعبر عن

---

[1]- محمد خليفة الملط، المرجع السابق، ص 544.

[2]- ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالأنترنت والمعلوماتية دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، 2017،1438، ص487.

أفكار جديدة ليس لها علاقة بالأفكار التقليدية التي تشترط الضرر كعنصر للمعاقبة على جرائم التزوير إلا أنه بالنسبة للمشرع الفرنسي وحتى عندما استعمل هذه المصطلحات الثلاثة وهي التزوير والتقليد والتزييف حيث أنها وخاصة التزييف (ترتبط بالعملة والمتمثلة بالنقود الإلكترونية) حتى في مسألة التزييف للنقود التقليدية لا يشترط فيها كجريمة وقوع الضرر وبالتالي هذا يوحي بسلامة موقف المشرع الفرنسي.

يرجى من المشرع الجزائري التنبه لهذه المسألة عند صياغته لهذا النوع من الجرائم إذا تم استحداث نص خاص بتزوير وتقليد وتزييف وسائل الدفع الإلكتروني في قانون النقد والقرض الجزائري وبنائها على فكرة الخطر المتوافق مع الجرائم التقنية الحديثة وهو الاتجاه الذي تبنته القوانين الحديثة لأن الخطر ينصب على المجرم وليس على الفعل أو النشاط فخطر المستخدم لوسائل الدفع الإلكتروني المزورة والمقلدة والمزيفة هو ما يحدد حجم الجريمة.

الفرع الخامس

الركن المعنوي و العقوبات المقررة للجريمة

نتناول الركن المعنوي والعقوبات المقررة حسب ما هو وارد في مواد قانون النقد والمال الفرنسي:

أولا / الركن المعنوي

هذه الجريمة عمدية تقتضي اتجاه النية إلى الاشتراك في تزوير وسائل الدفع الإلكتروني وتغيير الحقيقة وهو قصد عام ويتطلب قصدا خاصا يتمثل في تحقيق غاية معينة من

ارتكاب الركن المادي تتمثل في نية استعمال المحرر و تعني الاحتجاج بالمحرر على أنه محرر صحيح، واشترطت المادة العاشرة من اتفاقية مكافحة جرائم تقنية المعلومات نية استعمال البيانات[1] التي مسها التغيير على أنها بيانات صحيحة، وتطبيقا لذلك لا يسأل الشخص متى ثبت أنه لم يكن يقصد سوى اختبار قدرته على التقليد وأن نيته كانت متجهة إلى اعدام المحرر في الحال[2].

ثانيا/ العقوبات

حسب المادة L163-3 من قانون النقد والمال الفرنسي تصل العقوبة الى سبع سنوات شجنا و750 ألف أورو غرامة مالية، ويقضى بنفس العقوبة لكل الصور التي مدد لها القمع حسب المادة L163-4 من نفس القانون، كما يقضى بمصادرة الشيكات ووسائل الدفع في حالة التزوير والتقليد ومصادرة الأدوات والآلات والبرامج المعلوماتية وكل المعطيات الموجهة لخدمة الغرض أو الموجهة لخدمة صنع وسائل الدفع L163-5 من قانون النقد والمال الفرنسي كما يحرم الفاعل من حقوقه المدنية والعائلية L163-6 من النقد والمال الفرنسي.

كما نشير إلى أنه يعاقب على الشروع في هذه الجرائم في القانون الفرنسي[3]، وتصل العقوبة في القانون الفرنسي لمدة عشر سنوات سجنا في حالة الجماعة المنظمة[4] وبالتالي على

---

[1]- أنظر المادة العاشرة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات " ...بنية استعمالها كبيانات صحيحة".

[2]- ايهاب فوزي السقا، المرجع السابق، ص 59.

[3]- L 163-4-1 « La tentative des délits prévus au 1° de l'article L163-3et à l'article L163-4est punie des mêmes peines ».

[4] -L 163-4-2 « Les peines encourues sont portées à dix ans d'emprisonnement et un million d'euros d'amende lorsque les infractions prévues aux articles L163-3 ,L163-4 et L163-4-1 sont commises en bande organisée ».

المهتمين بوسائل الدفع الإلكتروني السعي للحد من هذه الظاهرة (التزوير والتقليد والتزييف) حتى ينتشر ويعمم استعمال وسائل الدفع الإلكتروني بشكل واسع لأن الخوف من التزوير الإلكتروني سبب عدم ثقة كثير من الناس بالتعاملات الإلكترونية ومن باب الاحتياط يجري الأفراد تعاملاتهم بالطرق اليدوية العادية كما يعد السبب في عدم تطبيق التجارة الإلكترونية الصيرفة الإلكترونية وحتى الحكومة الإلكترونية.

الفرع السادس

ضرورة التدخل التشريعي في الجزائر لمواجهة تزوير وسائل الدفع الإلكتروني

نحن بحاجة إلى تدخل تشريعي في القانون الجزائري بالنص على التزوير الإلكتروني في قانون العقوبات عموما لأن المشرع الجزائري أغفل النص على تجريم الاعتداءات الواردة على منتوجات الإعلام الآلي رغم تجريمه للاعتداءات الواردة على الأنظمة المعلوماتية.

لم يتبنى المشرع الجزائري كذلك الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث[1].

ضرورة النص على تجريم تزوير وسائل الدفع الإلكتروني في قانون النقد والقرض الجزائري لتوفير الحماية الجزائية لوسائل الدفع الإلكتروني كلها ومن بينها البطاقات؟ لأن الطبيعة الخاصة للبطاقات واحتوائها على بيانات ومعطيات غير مرئية وغير مقروءة تدفعنا إلى الجزم بأن قانون العقوبات الجزائري الحالي بنصوصه المتعلقة بالتزوير غير قادر على

[1]- السيد عبد الحميد أحمد، المرجع السابق، ص393.

مواجهة مشكل التلاعب بها عن طريق التزوير كما أنه وبالعودة إلى النصوص المتعلقة بالمساس بنظام المعالجة الآلية للمعطيات لا يمكننا تطبيقها في حالة التزوير لاختلاف الهدف والغرض من الجريمتين وبالتالي على المشرع الجزائري وتفاديا لهذه الاشكالات النص على تزوير وسائل الدفع الإلكتروني صراحة حتى لا يبقى مجال للشك في تفسير النصوص الجزائية لأنه وحتى في حالة ادراج نص خاص بالتزوير المعلوماتي في القسم الخاص بالتزوير ضمن قانون العقوبات أو بالنسبة لوسائل الدفع الواردة ضمن القانون التجاري والذي تكلم عن بعض وسائل الدفع فقط سنصطدم بمبدأ الشرعية الجنائية.

بالتالي وحلا للإشكالية ومواجهة لكل الاحتمالات المحتملة للتنصل من المسؤولية لابد من الأخذ بالتعديل الأخير للمشرع الفرنسي بالنص على وسائل الدفع الإلكتروني عامة وليس البطاقات فقط وعدم الاكتفاء بتعديل مدلول المحرر ليشمل المحررات الإلكترونية، كما أن وسائل الدفع الإلكتروني ليست محررات لأنها لا تقوم حتى بوظيفته كونها غير معدة للتداول بين الناس والتي تعتبر من بين وظائف المحرر، ويعزز هذا النفي أن وسائل الدفع الإلكتروني لا تعدو أن تكون مجرد وسيلة للوصول إلى نظام المعالجة الآلية للمعطيات، كما أنها وسائل تقوم على الاعتبار الشخصي وخاصة بالزبون الذي صدرت الوسيلة أو منحت لمصلحته نتيجة الملاءة أو الثقة التي يتمتع بها، كما أنه لا يوجد نص يفرض على الأفراد التعامل بها إنما تبقى مقبولة فقط ممن اختار التعامل بها والجهة المصدرة لها.

نشير إلى أن تزوير المحررات العرفية و المصرفية يكيف على أساس جنحة، ويعاقب عليها المشرع الجزائري بالمادة 219 من قانون العقوبات بالحبس من سنة إلى خمس سنوات أو بغرامة من 500 إلى 20.000 د ج والحرمان من حق أو أكثر من الحقوق المنصوص عليها في المادة 14 وبالمنع من الإقامة من سنة إلى خمس سنوات، كما نستخلص من المادة كذلك أن صفة المصرفي ظرف مشدد للعقوبة، لأن التزوير هو كذب مكتوب بنية الإخلال بالضمان والغير والاستقرار الذي ينبغي أن يحيط بالعمليات المصرفية بمختلف أنواعها الأمر الذي يزعزع الثقة العامة في النظام المالي[1]،

ما يلفت انتباهنا كذلك هو أن المشرع الجزائري أفرد عقوبة خاصة لتزوير الشيك[2] وجعلها مشددة تصل إلى عشر سنوات، فهل كان القصد من هذا حمايته باعتباره أداة وفاء؟ في حين لا تتجاوز العقوبة عن التزوير لباقي الأوراق التجارية والمحررات المصرفية خمس سنوات، وهذا بنظرنا يحتم على المشرع الجزائري الانتباه للمسألة عند صياغة النصوص المتعلقة بوسائل الدفع سواء التقليدية أو الإلكترونية باعتبار الشيك أحد هذه الوسائل.

[1]- غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص136.

[2]- أنظر المادة 374 من قانون العقوبات المتعلقة بتزوير الشيك والمادة 219 من نفس القانون المتعلقة بتزوير المحررات التجارية والمصرفية.

المطلب الثاني

المسؤولية الجزائية عن الاشتراك في استعمال

وسائل الدفع الإلكتروني المقلدة والمزورة والمزيفة

استعمال المحرر المزور في حد ذاته لم يبينه القانون فلا يعد مجرد تقديم المحرر لفرد أو جهة من الجهات استعمالا إنما يراد بالاستعمال إرادة الاحتجاج بهذا المحرر المزور في التعامل باعتباره صحيحا، ولا يشترط أن يكون الاحتجاج من مقدم المحرر، فتسهيل المصرفي للزبون الحصول على قرض باستعمال وسائل دفع إلكتروني مزورة يعتبر اشتراك في استعمال وسائل دفع إلكتروني مزورة أو مقلدة، وتفترض جريمة الاستعمال وجود محرر مزور وتبعا لذلك وقوع جريمة تزوير[1]، نتناول الركن الشرعي للجريمة (الفرع الأول)، الركن المادي (الفرع الثاني)، وأخيرا (الركن المعنوي والعقوبات المقررة للجريمة).

الفرع الأول

الركن الشرعي لجريمة استعمال وسائل الدفع الإلكتروني المقلدة أو المزورة

يشترط لقيام هذه الجريمة توافر جريمة تزوير وسيلة دفع إلكتروني أو تقليدها وليس شرطا أن من يزور هو من يستعمل الوسيلة إنما الغالب أن هذه الوسائل المزورة في حالة استعمالها أنها تتطلب تدخل عدة أطراف سواء المختصين في مجال المعلوماتية أو العاملين في البنوك أو التجار، فالمستقر عليه هو عدم مسؤولية المصرفي عن التزوير المتقن لأنه يستوجب

[1]–جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص 148.

اكتشافه خبير متخصص في اكتشاف التزوير ويلزمه اختيار أدوات علمية وهذا الأمر غير متيسر عند المصارف ولا يتفق مع طبيعة العمل المصرفي وسرعة الأداء المطلوبة فيه، ومسؤولية المصرفي المطلقة على التزوير المفضوح والتزوير العادي الذي يمكن للمصرفي اكتشافه بسهولة ففي هذه الحالات يكون المصرفي شريك في جريمة استعمال المزور[1].

أولا / استقلال جريمة استعمال بطاقة دفع أو سحب مزورة أو مقلدة بنص خاص

استقلال جريمة استعمال بطاقة دفع أو سحب بنص خاص في القانون المتعلق بأمن الشيكات وبطاقات الدفع فالمشرع الفرنسي انفرد بموقف خاص بالنسبة لاستعمال البطاقة المزورة أو المقلدة حيث جعل من هذا الاستعمال جريمة مستقلة عن جريمة استعمال المحررات الخاصة المزورة[2]، وهي (جريمة استعمال أو محاولة استعمال بطاقة دفع أو سحب مزورة) وذلك من خلال نص المادة 67-1 المنشأة بالمادة 11[3] من القانون رقم 1382-91 المتعلق بأمن الشيكات وبطاقات الدفع.

تنص المادة من 67-1 -2 من القانون المتعلق بأمن الشيكات وبطاقات الدفع الفرنسي على الاستعمال بمعرفة السبب لبطاقة الدفع أو السحب المقلدة أو المزورة . **Usage** « **d'une carte de paiement ou retrait contre fait ou falsifiée ...** »

ثانيا / تمديد القمع ليشمل استعمال وسائل الدفع الإلكتروني المقلدة أو المزورة

---

[1]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 140.

[2]- محمد نور الدين سيد عبد المجيد، المرجع السابق، ص414.

[3]-Art 11 « ...2-ceux qui en connaissance de cause, auront **fait usage d'une carte de paiement ou retrait contre fait ou falsifiée ...** » .JORF, de1° janvier 1982.

أدرك المشرع الفرنسي أن الاستعمال لا ينحصر في البطاقات فقط وتفاديا للاصطدام بمبدأ الشرعية ومبدأ حضر القياس في المادة الجزائية عدل قانون النقد والمال الفرنسي ليشمل كل وسائل الدفع الالكتروني حيث تنص المادة

L163-3« Est puni d'un emprisonnement de sept ans et d'une amende de 750 000 euros le fait pour toute personne : …

2. De faire ou de tenter de faire usage, en connaissance de cause, d'un chèque ou **un autre instrument mentionné à l'article L.133-4contrefaisant ou falsifié** … ».

وبالتالي لا يمكن أن تقبل وسائل الدفع الإلكتروني أو أن يتم الدفع أو السحب بها إلا إن كان هناك تواطىء وتسهيل من المصرفي أو التجار، لأن الواجب الواقع على المصارف هو اكتشاف عمليات التزوير لما يسببه من ضرر للزبون وزرع للخوف في نفوس الزبائن على أموالهم المودعة بالمصرف مما يدفعه إلى سحبها، كما أنه على التجار التأكد من سلامة وسائل الدفع وعد تزويرها قبل قبولها وهم مزودون بتجهيزات وآلات وربط مباشر بالمصارف للتأكد من هذه الاجراءات إلا عمليات التزوير التي تقع في العمل المصرفي ووسائل الدفع الإلكتروني بشكل شبه يومي، فبمجرد إدراك هذه الحقيقة من المصرفي وعدم اتخاذ الاحتياطات اللازمة يكون قد ساهم بشكل غير مباشر في تسهيل ارتكاب عمليات التزوير ولو أننا لا نستطيع الاستناد إلى عدم اتخاذ الاحتياطات لأن الاشتراك لا يكون إلا بعمل ايجابي، وكذلك من النادر أن يتم استعمال وسائل الدفع الإلكتروني المقلدة أو المزورة إلا إن كان هناك اتفاق مسبق بين التجار والزبائن أو الغير.

الفرع الثاني

الركن المادي للاشتراك في استعمال وسائل الدفع الإلكتروني المقلدة والمزورة

يتمثل الركن المادي في هذه الجريمة في فعل الاستعمال أي إبراز وسيلة الدفع الإلكتروني المزورة والاحتجاج بها على أنها صحيحة، ففي مجال السحب أو الوفاء فإن الاستعمال يعني ابراز وسيلة الدفع الإلكتروني وتقديمها والاحتجاج بها على أنها صحيحة بمعنى أن يقوم المتهم باستخدام وسيلة الدفع الإلكتروني في الدفع أي دفعها إلى التعامل لتحقيق الغرض الذي خصصت من أجله وهو استخدامها في الدفع لدى التجار أو في السحب من أجهزة السحب النقدي الآلي أو استعمالها كوسيلة في الحصول على الخدمات مع علم من استخدمها بأنها مزورة ومؤدى ذلك أن مجرد وجود وسيلة الدفع الإلكتروني المزورة في حيازة المتهم دون ابرازها لا يقوم به فعل الاستعمال، ويتعين أن يقوم المتهم بإبراز وسيلة الدفع الإلكتروني والاحتجاج بها على أنها صحيحة ويكون ذلك عندما يستخدمها في الدفع لدى التجار، وبالتالي فمن يقدمها للاستعلام عن مدى قبول التاجر للدفع بها لا يحقق فعل الاستعمال وإنما يجب أن يراد الاحتجاج بها أي أن يتم التمسك بوسيلة الدفع أو أن يطلب ارشاده على كيفية استخدامها وغالبا في هذه الحالة يكون هناك اتفاق بين المتهم والتاجر بأن يقبل التاجر الدفع بوسيلة إلكترونية وإبرازها إن كان لها كيان مادي كالبطاقات وأن يطلب إتمام العملية الثانية وهي الدفع عن طريقها أي إرادة التمسك بالبيانات التي تتضمنها وهي بيانات غير حقيقية للتأثير على من يقبل الدفع بها أي استعمال الوسيلة ككل باعتبارها

صحيحة وهذا ما يفرقها عن جريمة استعمال بيانات وسائل الدفع الإلكتروني المزورة أو المقلدة ويكون في هذه الحالة مرتكب لجريمة قبول الدفع ببطاقة مقلدة أو مزورة وشريكا في جريمة استعمال بطاقة مزورة أو مقلدة، وأثير الإشكال حول مدى تحقق فعل الاستعمال عندما يتم السحب من خلال أجهزة السحب النقدية الآلية؟

للإجابة على هذا التساؤل نشير إلى أن تعبير الاحتجاج بها على أنها بطاقات صحيحة قد يكون غريبا في حالة السحب الآلي، إلا أن المشرع الفرنسي ونظيره المغربي قد ذكر تعبير من "استعمل "، والاستعمال سواء بالوفاء بها لدى أحد التجار أو عند استخدامها في السحب من الآلة مما يؤكد ذلك أن المشرع قد جرم المحاولة وأعطاها حكم الجريمة الكاملة وتبدو أهمية المحاولة –بصفة خاصة –عند استعمال البطاقة المزورة في السحب من أجهزة السحب النقدي[1]، ومن صور الاشتراك بين التجار طباعة أرقام بطاقته على اشعارات بالبيع خيالية دون طباعة رقم الماكينة الخاصة به عليها ويوقع عليها الزبون و يأخذها التاجر إلى تاجر آخر ويبيعها اياه بشرط اقتسام قيمة العملية المحصلة من البنك بالإشعار المزور فيتابع الأول بالتزوير والثاني بالاشتراك في التزوير، فحالة شراء فواتير مزورة تكون **جريمة استعمال محرر مزور** لأن التاجر الثاني الذي يشتري الاشعار المزور ويقوم بتحصيل الأموال من بنكه يكون قد استعمل بطاقة مزورة مع علمه بذلك.

[1]– ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص 208.

الفرع الثالث

الركن المعنوي والعقوبات المقررة للجريمة

أولا /الركن المعنوي

هذه الجريمة عمدية وهذا حسب نص المادة L163-3-2 من قانون النقد والمال الفرنسي سواء للاستعمال أو محاولة الاستعمال لوسيلة دفع إلكتروني مع العلم بالسبب « **De faire ou de tenter de faire usage, en connaissance de cause...** »، يتخذ القصد الجنائي صورة العلم بأن وسيلة الدفع مزورة أو مقلدة والاحتجاج بها على أنها صحيحة، أي أن يعلم كل من المصرفي أو التاجر أو الزبون أنه يسهل الاستخدام لمستعمل وسائل الدفع الإلكتروني التي يعلم أنها مزورة أو مقلدة كما يعلم باتجاه إرادة المستعمل إلى التمسك بها باعتبارها صحيحة.

ثانيا / العقوبات المقررة لجريمة الاستعمال لوسيلة دفع إلكتروني مقلدة أو مزورة

يعاقب على استعمال وسيلة دفع الكتروني مقلدة أو مزورة أو محاولة استعمالها بالسجن مدة سبع سنوات وغرامة قدرها 750 ألف أورو حسب المادة L163-3-2 من قانون النقد والمال الفرنسي، وفي الأخير نذكر أن مرتكب أي جريمة يعاقب عليها القانون بعقوبة الحبس وتطبيقا للمادة 131-6 من قانون العقوبات الفرنسي الجديد يمكن أن يتم حرمانه من حق استعمال بطاقة دفع، على سبيل عقوبة بديلة، لمدّة لا تتجاوز خمس سنوات وفقا للمادة

131-20[1] من قانون العقوبات الفرنسي، كما يشمل حظر استعمال البطاقات بالنسبة للمدان أمرا بإعادة البطاقات التي بحوزته للبنك الذي قام بتوزيعها وتلك الخاصة بوكلائه وهذا الشكل من أشكال العقوبة يمكن أن يتم تطبيقه بوضوح في حالات المخالفة المتعلقة ببطاقات الدفع أو السحب أو الائتمان[2].

المبحث الثاني

الاشتراك في الجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني

في الوقت الذي تشكل فيه بيانات الدفع "ذهب" الاقتصاد اقتحم فاعلون جدد الساحة لاستغلال منجم كان تقليديا مخصص للبنوك فهذا النشاط الجديد يقوم بنسج شبكته الشيء الذي لاشك يطرح مسائل قانونية شائكة[3].

كما تتمتع وسائل الدفع الإلكتروني بالحماية فإن البيانات والمعطيات الموجودة داخلها كذلك تتمتع بالحماية بالنظر إلى طبيعتها المعلوماتية، إلا أنه قبل النص على هذه الجرائم كان الأمر في غاية التعقيد بخصوص الاستيلاء على الأرقام والبيانات والمعلومات التي تحويها وسائل الدفع الإلكتروني وهل تصلح لأن تكون محلا للسرقة أم لا وهي أن هذه الأرقام والبيانات يصلح أن تأخذ وصف المال وبالتالي تفاديا لهذه الاشكالات خص المشرع الفرنسي

---

[1]-Art 131-20 de code pénal français« L'interdiction d'utiliser des cartes de paiement comporte pour le condamné injonction d'avoir à restituer au banquier qui les avait délivrées les cartes en sa possession et en celle de ses mandataires. Lorsque cette interdiction est encourue à titre de peine complémentaire pour un crime ou un délit, elle ne peut excéder une durée de cinq ans. »

[2]-Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 6edition,2006, lexis Nexis,p385 - p385.

[3] - Noémie Weinbaum, op, cit, p72.

هذه الجرائم بنص خاص لذلك سنتناول في المطلب الأول(الركن الشرعي للاشتراك في جرائم الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني)، المطلب الثاني(صور الأركان المادية لجرائم الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني)، (المطلب الثالث) نخصصه لاستعمال الشبكة المعلوماتية ووسائل تقنية المعلومات للوصول إلى بيانات وسائل الدفع الإلكتروني، ثم نتطرق إلى عنصر الضرر والركن المعنوي لهذه الجرائم (المطلب الرابع).

المطلب الأول

الركن الشرعي للاشتراك في جرائم الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني

تم وضع هذا النص الذي يجرم الحصول على البيانات عن طريق الشبكة المعلوماتية أو أي نظام معلومات كما هو الحال في تعقب المعاملات المالية أو قواعد البيانات الخاصة بوسائل الدفع الإلكتروني والحصول منها على رموز ومعلومات استخدامها، حيث يمكن أن يتم الاستيلاء أو الاستعمال لبيانات وسائل الدفع الإلكتروني ويكون هذا من خلال استغلال الضعف الأمني في الأنظمة التشغيلية للبنوك فبيانات وسائل الدفع الإلكتروني هي عبارة عن كلمات وأرقام ورموز وحقائق أو إحصاءات خام لا يوجد أي صلات بينها، وهي صالحة لتكوين فكرة أو معرفة بمعرفة الانسان أو الادوات والأجهزة التي يسخرها الانسان لذلك وهي ما يسمى بعملية المعالجة الإلكترونية و كثيرا ما تستخدم البيانات كمرادف للمعلومات رغم

الاختلاف في المعنى والمفهوم والدلالة فالمعلومة هي المعنى المستخلص من البيانات بعد معالجتها لذلك يرى البعض أن البيانات ليس لها قيمة بخلاف المعلومات فالمعلومات يمكن أن يكون لها قيمة اقتصادية.

الوزن المالي للغش المرتبط بوسائل الدفع الإلكتروني يجب أن يكون على عاتق المؤسسات المصدرة لها و يجب أن يمر عبر تطوير التكنولوجيا الموجهة لتدعيم تأمين الدفع لهذه الوسائل ويجب على المؤسسات وضع أجهزة قارة لآليات التعريف غير قابلة للرجوع فيها خاصة عن طريق الإرسال ل(SMS أو الرسائل القصيرة) للرقم السري الذي يكون للاستعمال الشخصي بهدف احباط الغش و تعويض و تأمين الضحايا ويحتاج أيضا إلى تنظيم عقوبات قمعية وفعالة[1].

استكمالا لما تبذله المؤسسات المصدرة لوسائل الدفع الإلكتروني لتطوير الحماية التقنية على المشرع الجزائري تبني نصوص تجريمية للاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني (الفرع الأول)، وضرورة استحداث نص قانوني لتجريم انتحال الهوية الرقمية.

الفرع الأول

الحاجة لنصوص تجريمية للاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني في التشريع الجزائري

نصت المادة 276 مكرر (1) المضافة بموجب المرسوم السلطاني رقم 2001/72 من قانون الجزاء العماني " يعاقب بالسجن مدة لا تقل عن ستة اشهر ولا تزيد عن سنتين

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 65

وبغرامة لا تقل عن مائة ريال ولا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين كل من **استولى أو حصل على نحو غير مشروع على بيانات** تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات " وتضاعف العقوبة إذا ارتكبت هذه الأفعال من طرف مستخدمي الكومبيوتر[1]، وبالتالي يمكن للقاضي في سلطنة عمان الاستناد إلى هذا النص في حالة الاستيلاء على البيانات وأرقام وسيلة الدفع الإلكتروني، كما جرم صورة أخرى تتعلق بالالتقاط غير المشروع للمعلومات أو البيانات والذي يمكن أن يشمل وسائل الدفع الإلكتروني أيضا[2]، ونلاحظ أن المشرع العماني استعمل مصطلح الاستيلاء بدل الاختلاس الذي يوحي بالطبيعة المادية والذي يصعب اثباته في هذه الحالة حيث أن الاختلاس يوحي بأخذ الشيء ونقله من شخص لآخر إلا أن هذه الحالة لا تتحقق في حالة استيلاء الشخص على معلومات وبيانات وسائل الدفع الإلكتروني لا يعني أنها انتقلت من حاملها إلى المستولي عليها وهذه الإشكالية التي كانت تثار بخصوص تطبيق فعل الاختلاس فتبقى المشكلة قائمة بشأن احتفاظ صاحب وسيلة الدفع الإلكتروني ببياناتها الأصلية قائمة لأن استيلاء الجاني على المعلومة لم يؤد إلى فقدان صاحب الوسيلة لها، إن حل هذه الاشكالية كما يتصور البعض هو أنه إذا كان الشيء الذي يرد عليه الاختلاس شيئا ماديا فإن انقاص الذمة لا يكون إلا بخروج الشيء من ذمة المجني عليه ودخوله في ذمة الجاني، أما إذا كان الشيء غير مادي فإننا لا نكون بحاجة إلى مثل ذلك

[1]- أنظر المادة 276 مكرر (2) من قانون الجزاء العماني .

[2]-أنظر المادة 276 مكرر من قانون الجزاء العماني .

حيث لا يتطلب الاختلاس نقل الشي لأن هذا الأخير ما هو في الحقيقة إلا انقاص لذمة المجني عليه وانقاص ذمة الأخير قد تمت بانتقاص قيمة المعلومات لأن صاحب المعلومة على الرغم من أن أصل المعلومة لازال بين يديه إذ أن هناك من يزاحمه في ذلك فهو لم يبق صاحب الحق الوحيد في احتكار المعلومة واحتكار استغلالها[1] وبالتالي كان الاستيلاء على المعلومات والبيانات المتعلقة بوسائل الدفع الإلكتروني دون استعمالها فعل غير معاقب عليه لأن النية للاستغلال غير المشروع غير موجودة إذ لابد لوجودها من مظهر خارجي يؤيد ذلك، لذلك انتبه المشرع لهذه الحاجة وجرم الاستيلاء والحصول علة المعلومة دون استعمالها وكذلك استعمل مصطلح الاستيلاء عن قصد حتى لا يحتج بعدم امكانية التطبيق لفعل الاختلاس وبالتالي عدم تطبيق أحكام فعل السرقة.

يتوجب على المشرع الجزائري أن يتدخل ليشمل بالتجريم ما يستجد من أفعال لم تكن مجرمة من قبل.

الفرع الثاني

الحاجة لنص قانوني مستحدث لتجريم انتحال الهوية الرقمية

مختلف التصنيفات الجنائية لرفع النزاع حول تصنيف الاستعمال الاحتيالي للمعطيات يمكن أن يشكل للحامل أو للمصدر دخول غير شرعي للمعطيات المحتوات في البطاقة حيث يمكن أن تشكل نصب واحتيال، أو استلاء على الهوية الرقمية التي تفترض أيضا استعمال

[1]-محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الائتمان الممغنطة، ص504، 505.

لمعطيات تم التحصل عليها بطريق الغش[1]، والهدف من خلق جريمة انتحال الهوية الرقمية هو القمع المعنوي للجرائم المرتكبة على الأنترنت في حالة غياب الضرر المالي، يمكن أن تتأثر وسائل الدفع الإلكترونية على اختلاف أنواعها بهذه الجريمة التي تتأقلم مع الشكل الجديد من الاجرام المعتبر و المتطور بسبب الدفع عبر الانترنت[2]، يعتبر انتحال الهوية الرقمية (اغتصاب الهوية الرقمية usurpation d'identité numérique) من التصرفات غير الشرعية الجديدة على الانترنت[3]، وجريمة العصر المستحدثة وتستخدم أساليب انتحال الشخصية أو التسلل الإلكتروني للدخول إلى المناطق المؤمنة والمحمية إلكترونيا أو الوصول إلى مراكز الحاسب الآلي والدخول على قواعد المعلومات وقد يكون الدخول شخصيا[4] أو إلكترونيا والهدف من خلق جريمة انتحال الهوية الرقمية هو السماح بالقمع المعنوي في حالة غياب الضرر المالي[5].

يمكن تعريف انتحال الهوية الرقمية بأنه سوء استعمال لوثائق أو بيانات شخصية بهدف انتحال شخصية أو صفة أفراد آخرين للقيام بنشاطات غير مشروعة[6]، ومنه يمكننا تعريف انتحال الهوية بأنها الفعل القصدي الذي بموجبه يقوم شخص باستعمال أو استغلال

[1]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 261-262.

[2]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 65

[3]-Céline CASTETS-RENARD, droit de l'internet, LGDJ-Montchrestien Lextenso éditions, 2010, p543.

[4]- فالدخول الشخص يتم عن طريق انتحال شخصية أحد العاملين في المكان المؤمن أنظر، محمد الأمين البشري، المرجع السابق، ص1069.

[5]-Céline CASTETS-RENARD, op, cit, p545.

[6]- طارق محمد حمزة، المرجع السابق، ص303.

معلومات أو بيانات شخصية للغير لأهداف غير مشروعة من قبيل ارتكابه لأفعال مجرمة أو لتحقيق منافع مالية[1].

وكان القضاء قبل خلق هذه الجريمة يلجأ إلى تكيفات لجرائم أكثر عمومية كالتزوير والنصب والاحتيال على الانترنت[2]، ونصت عدد من تشريعات الولايات المتحدة الأمريكية على سرقة الهوية ووسائط العريف فاعتبرت من قبيل الجريمة متى توفر العلم وقصد تحقيق منافع مادية – الحصول على أو حيازة أو نقل أو استخدام أو محاولة الحصول أو الحيازة أو النقل أو الاستخدام لواحدة أو أكثر من وثائق التعريف الشخصية أو الأرقام الشخصية أو أية وسائل تعريفية للشخص أو لشخص آخر غير مصرح له قانونا بحيازتها – وهذه التشريعات لا توصف عموما كجزء من تشريعات جرائم الحاسب الآلي ومع ذلك يتم إدخالها ضمن نطاق تشريعات جرائم الحاسب الآلي بسبب اتصال سرقة الهوية بأنشطة الاختراق والدور الرئيسي الذي تلعبه هذه الأنشطة في هذا الحقل[3]، وفي أوربا قمع انتحال الهوية على الانترنت كان محل اقتراحات متعددة ومشاريع قانونية منذ سنة 2005ويبدو أن هذا السؤال قد وجد جوابه بإقرار النص المنشئ لهذه الجريمة من خلال قانون التوجيه والبرمجة من أجل ترقية الأمن الداخلي المسمى (L O P P S I) loi d'orientation et de programmation pour

---

[1]– زياد سويدان ،انتحال الهوية الرقمية، متوفرة على الموقع: www.urdri.fdspt.rnu.tn/.../zied-souiden-usurpation-identite.ppt، تاريخ الاطلاع: 09/07/ 2017.

[2] - Fabrice Mattatia, l'usurpation d'identité sur internet dans tous ses états, revue de science criminelle et de droit pénal comparé, avril-juin 2014.

[3]– يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، المرجع السابق، ص11.

la performance de la sécurité intérieure. المؤرخ في 14 مارس 2011، والمادة 226-4-1 من قانون العقوبات الذي تمت المصادقة عليه في 24 جويلية 2013 قدم النائب "مارك لوفر" مشرع قانون يعدل فيه المادة 226-4-1 من قانون العقوبات من أجل مضاعفة مقدار العقوبة إلا في حالة الانتحال فقط الذي تم على الانترنت[1].

تتكون الهوية الرقمية من جميع العوامل والمفردات التي تعبر عن وجود شخص في فضاء الانترنت مثل عنوان برتوكول الانترنت التابع لجهاز حاسوبه على الشبكة (IP) أو عنوان بريده الإلكتروني وكلمة السر واسم المستخدم أو الاسم الذي يعرف به عبر غرف المحادثة والمنتديات الحوارية أو اسم حسابه الإلكتروني على مواقع الانترنت "كالفيس بوك "وغيرها من المواقع الإلكترونية التي يكون للشخص فيها نشاطات ومشاركات بحساب إلكتروني فتحه وسجل به على تلك المواقع وهناك أنواع أخرى من الوجود الإلكتروني أخطر وأهم للشخص على الانترنت منها أرقام الحسابات البنكية التي تخول التعامل مع حسابه البنكي إلكترونيا من خلال موقع البنك على الانترنت أو تحويل الأموال إلكترونيا أو الشراء على الانترنت ببطاقات الائتمان وجميعها تعد من الأمثلة على الهوية الإلكترونية[2] ونفس الأمر بالنسبة للنقود الإلكترونية التي يمكن أن تكون محلا لهذه الجريمة ويحدد التوقيع الرقمي هوية مصدر هذه النقود الإلكترونية ويعطي ضمانا بتحويل هذه السلسلة من البياناتbits إلى نقود مادية (دينار، يورو، دولار ...)، ونتصور امكانية حدوث التزوير المعنوي في وسائل الدفع

[1] -Fabrice Mattatia, op cit, p331.

[2] – زياد سويدان، انتحال الهوية الرقمية،

الإلكتروني عن طريق تزوير الأمر بالدفع سواء من طرف صاحب وسيلة الدفع الإلكتروني أو من طرف الغير، كقيام العاملين في البنك بتزوير الأمر بالدفع بواسطة إدخال التوقيع الرقمي للبطاقة وانتحال شخصية صاحبها، ويمكن أن يتم استعمال المعلومات الشخصية لشخص آخر بهدف غير شرعي، والمعطيات الشخصية التي تحتاج للتحفظ خاصة في حالة المعطيات البنكية[1].

ولكن هل يتصور وقوع تزوير معنوي في بطاقة الدفع البنكية ؟

للإجابة على هذا التساؤل نشير إلى أنه من المعروف أن البطاقة البنكية تصدر ويتبعها رقم سري معين ويفترض وجود حساب خاص للزبون الذي يحمل البطاقة، وهذا يعني صعوبة وقوع التزوير المعنوي دون استحالته، فاذا انتحل شخص شخصية صاحب حساب في أحد البنوك وهو يعلم أن هذا الأخير لم يحصل على البطاقة البنكية من البنك ثم قام بطلب هذه البطاقة فصدرت بالطبع باسم صاحب الحساب الحقيقي وقام المتهم بالحصول عليها، ففي هذه الحالة نكون بصدد تزوير معنوي اتخذ صورة جعل واقعة مزورة في صورة واقعة صحيحة وذلك بانتحال شخصية الغير[2]، أو اقناع الحامل بعد أخذ البطاقة منه وتمريرها بالماكينة الإلكترونية أن هذه الأخيرة معطلة ويجب تمرير البطاقة على آلة القراءة اليدوية

[1]-Céline CASTETS-RENARD, op cit, p544.

[2]- ضياء أحمد علي نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص 201.

حتى تتم العملية وهو في الحقيقة يدبر لأخذ موافقتين وبعمليتين مختلفتين وبعدها يقوم بتزوير توقيع الزبون على الاشعار الثاني للعملية الثانية ويرسلها للبنك للتحصيل[1].

يجب التمييز بين انتحال الهوية واستعمال الهوية الوهمية فهذه الأخيرة تتمثل في خلق شخصية وهمية بكل المعايير والحصول باسمها على مستندات تثبت الشخصية، أو بفتح حسابات على الأنترنت إذا كان اختراع أو اختلاق شخصية يمكن أن يكون قاعدة (أساسا) للمكتسبات غير المشروعة أو النصب والاحتيال على حساب الآخرين فهي تختلف عن الانتحال نفسه لغياب الضحية[2] هذا الفعل معاقب عليه ضمن المادة 226-4-1 من قانون العقوبات الفرنسي المعدل سنة 2011 «le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou sa considération est puni d'un an d'emprisonnement et de 15000^{e} d'amende, cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication ou public en ligne ».

بالتالي فقانون العقوبات الفرنسي يجرم فعل الانتحال أو الاستعمال لمعلومة أو عدة معلومات أيا كان نوعها تسمح بالتعرف عليه وتعكر هدوءه أو تمس مكانته، ويعاقب بسنة

[1]- ضياء أحمد علي نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المرجع السابق، ص275.

[2] - Fabrice Mattatia, op cit, p332.

حبسا وغرامة مالية قدرها 15000 أورو ويعاقب على هذا الفعل بنفس العقوبة إذا ارتكب على شبكة اتصال عامة على الانترنت.

المطلب الثاني

صور الأركان المادية للاشتراك في الجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني

من الصور التي تضمنتها الجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني الاشتراك في الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني(الفرع الأول)، والركن المادي لانتحال الهوية الرقمية (الفرع الثاني).

الفرع الأول

الأركان المادية للاشتراك في الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني

يثير الاستيلاء على أرقام وبيانات وسائل الدفع الإلكتروني جدلا حول تكييفها على أنها جريمة سرقة أم أنها تمثل نوع آخر من الاعتداء على الأموال، وتشترك المعلومات والبيانات الخاصة بوسائل الدفع الإلكتروني مع طبيعة برامج الحاسب الآلي كون هذه البرامج عبارة عن معلومات ذات طبيعة غير مادية وربما تعتمد على ذات الأسلوب في تسييرها وتكوينها بكونها معلومات مشفرة ولا يمكن للغير الأطراف الاطلاع عليها من خلال أجهزة تتولى قراءتها ونتناول مختلف الحالات تباعا:

أولا/ الركن المادي للاشتراك في الاستيلاء على بيانات وسائل الدفع الالكتروني

الأصل وراء تجريم الاستيلاء على بيانات وسائل الدفع الإلكتروني أنها تتميز بالسرية التي يقصد منها أنها محدودة العلم بها وبالتالي يستلزم أن يحصل عليها أشخاص محددين وهذه البيانات الأصل فيها أنها غير شائعة للغير وبالتالي الاستيلاء عليها من طرف الغير يشكل جريمة منفصلة بذاتها.

يتمثل الركن المادي لهذه الجريمة في الحصول على البيانات الخاصة بوسائل الدفع الإلكتروني بطريقة من غير الطرق التي يتم بها الحصول على المعلومات عن طريق شبكة الانترنت كأن يتم الحصول عليها بالتصنت أو الالتقاط أو الاعتراض للبيانات بطريق آخر غير شبكة الانترنت كأن يتم مشاهدة أرقام وسائل الدفع الإلكتروني عبر جهاز الحاسب الآلي بشرط أن يتم التلاعب في هذه البيانات أو أن يتم الاستيلاء من العاملين في البنك على المعلومات الخاصة بالعاملين الآخرين ويتمكنوا من الدخول إلى أنظمة لا يحق لهم الدخول إليها ويستولون على هذه البيانات.

جريمة الاستيلاء على بيانات وسائل الدفع الالكتروني تتحقق بطرق تعد جرائم معاقب عليها مما يعني اشتراك في جريمة الحصول على بيانات وسائل الدفع الإلكتروني.

يمثل الاعتداء على البيانات اختراق للحماية الخاصة بالاتصالات وأمن البيانات يتمثل السلوك الاجرامي بالمساعدة والتسهيل للاستيلاء والحصول ولا يشترط قيام الفاعل باستخدام هذه المعلومات لتطبيق العقوبة بحقه فمجرد الحصول على تلك المعلومات قصدا دون سبب

مشروع يعد جريمة قائمة بذاتها تستوجب العقوبة كما هو الحال في سرقة بطاقة الائتمان، فالمعلومات الخاصة ببطاقة الائتمان لا تقل أهمية عن البطاقة ذاتها ويستوجب حمايتها لمنح الثقة في المعاملات المالية الإلكترونية وحماية للحقوق المالية لمالكيه[1]، وبالتالي يتم الاستيلاء على البيانات المعالجة إلكترونيا دون أن يقترن ذلك باختلاس أوعيتها المادية[2]، كما قد يحاول المحتالون الاستيلاء على بيانات وسيلة الدفع عن طرق مراقبة سير الرسائل بين البنك والزبائن للقيام بهجمات تهدف إلى فك التشفير كما قد يتم الاستيلاء على البيانات من الغير عند ارسالها عبر خطوط الاتصالات من خلال شبكة الانترنت، ويمكن الاستيلاء على البيانات من خلال الاعتراض أو اعادة نقل الرسائل التي تبدو أوضح في أنظمة الدفع ذات البرمجيات التي تعتمد شبكة الانترنت في عملها، فهنا يمكن استخدام التقنيات الخاصة بالوسائل المعدة للانتقال عبر البريد الإلكتروني[3]، كما أنه في مجال البنوك هناك برامج خاصة تقوم بحماية أنظمة البنوك من الاختراق وتحويل الأموال ونقلها عن طريق وسائل الدفع الإلكتروني وهذه البرامج تقوم بتغيير الشيفرة في البنوك بمعدل كل عشر ثوان تقريبا حتى لا يسمح باختراقها، كما أن هذه المعلومات والبيانات عند دمجها على الدعامات الممغنطة تتفعل ويتم تشغيلها ليس من خلال برنامج ليس من خلال برنامج يستطيع فك رموزها برنامج معين كتب بلغة معينة إنما لا يكون ذلك إلا من خلال الرقم السري الذي

[1]- عبد الرحمان محمد السويلم، المرجع السابق، ص 58.

[2]- طارق ابراهيم الدسوقي عطية، المرجع السابق، ص571.

[3]- حوالف عبد الصمد، المرجع السابق، ص329.

يختص به حامل وسيلة الدفع الإلكتروني والذي تطلب منه الجهة المصدرة لها المحافظة عليه حيث يمثل هذا الرقم السري المفتاح الذي يمكن من خلاله استعمال وسيلة الدفع الإلكتروني فيما أعدت له ومن خلاله يتم مخاطبة الأجهزة الآلية المستعملة في الدفع الإلكتروني حتى تستجيب لأوامر الشخص وهذا وجه الاختلاف بين هذه البيانات وبين برامج الحاسب الآلي التي تختلف طبعا حسب نوع البرنامج ووظيفته.

ثانيا/ الركن المادي للاشتراك في استعمال بيانات وسائل الدفع الإلكتروني

يجب التفرقة في نطاق البيانات والمعلومات بين المسؤولية الناشئة عن المساس بالأفراد والمؤسسات عند اساءة استعمال بياناتهم الشخصية المخزنة بالحاسب الآلي على نحو يمس أسرارهم وحقهم في الخصوصية والتي تطرقنا إليها من خلال الباب الأول والتي ترتبط بالسر المصرفي للأفراد والبيانات الخاصة وبياناتهم الخاصة اللازمة لاستعمال وسائل الدفع الإلكتروني وبين المسؤولية عن الأفعال التي تمس أو تعتدي على أموال الأفراد ومصالحهم وعلى حقهم في المعلومات ذات القيمة الاقتصادية التي نحن بصدد الكلام عنها في هذا المجال التي تحويها وسائل الدفع الإلكتروني.

الاستعمال يشير إلى ضرورة وجود نشاط مادي بعد الاستيلاء على المال المعلوماتي كبيعه أو استعماله في أنظمة النقود الإلكترونية ذات البرمجيات، وتتمثل النتيجة المحققة من خلال الركن المادي بحصول الجاني على البيانات والأرقام بحيث يمكن تعديل البيانات المخزنة على الوسيلة التي يحوزها المستهلك إذا لم تتوافر حماية برمجية مناسبة كما يمكن اجراء

تغيير في البرمجيات لتسمح للمستخدم اجراء تعديلات على نحو غير مرخص به[1]، فقد يحاول المزورون تغيير البيانات الخاصة بالوسيلة عن طريق الغاء الرسائل واعادة ارسالها مجددا أو ابدال الرسالة الأصلية بالرسالة المعدلة أو مراقبة سير هذه الوسائل بهدف القيام بهجمات لفك التشفير[2] والوجه الذي يثار بشأن الاستغلال هنا أن هذه البيانات والمعلومات الأصل فيها أنها محمية وبالتالي هي عبارة عن رموز وعلامات واشارات محددة ومخصصة لتبليغ أشخاص محددين ينحصر التعامل بها ضمنهم وأن من يتأثر بهذه البيانات شخص بمفرده لأنه له سلطة التصرف بها وهي تثبت لصاحب وسيلة الدفع أو شخص من المتدخلين في استعمالها.

الفرع الثاني

الركن المادي لجريمة انتحال الهوية الرقمية

يستوجب انتحال الهوية الرقمية مباشرة مرتكبه لفعلين متتابعين أولهما تجميع المعلومات والبيانات الشخصية للغير ثم القيام باستعمالها[3] وتهدف المادة 226-4-1 من قانون العقوبات الفرنسي إلى التجريم بصفة موسعة لكل استعمال لمعلومة أو عدة معلومات من أي نوع ويشمل التجريم سرقة كلمة السر، الاسم المستعار، البريد الالكتروني، وحتى العنوان الإلكتروني (IP) الذي يعني عنوان جهز الحاسب الآلي عند الربط على شبكة الانترنت وهي

---

[1]- حوالف عبد الصمد، المرجع السابق، ص329.

[2]- طارق محمد حمزة، المرجع السابق، ص 298.

[3]-زياد سويدان ،المرجع السابق .

ليست من حالات انتحال الهوية بالمفهوم الضيق، ولكن يمكنها أن تؤدي إلى الأضرار نفسها بالنسبة للضحية[1].

وبالتالي يستعمل الجناة عادة طريقة التصيد أي سرقة كلمة السر من أجل الدخول إلى الحسابات البنكية أو المعلومات الشخصية والتي تستهدف في أغلب الحالات استعمال البطاقات عبر الانترنت إلا أن المشكل أن هذا التصيد غير معاقب عليه بنص صريح، ولكن أحكام القضاء في فرنسا تبين أنه من الممكن المعاقبة عليه عن طريق جريمة النصب والاحتيال أو الدخول غير المسموح به إلى نظام المعالجة الآلية للمعلومات وهذه كذلك من الأمثلة التي تسمح بتجريم عدد معين عن حالات السرقة للهوية على الانترنت إضافة إلى المواد 226-4-1 و23 و434 من قانون العقوبات الفرنسي[2].

المطلب الثالث

استعمال الشبكة المعلوماتية ووسائل تقنية للوصول لبيانات وسائل الدفع الإلكتروني

تم اعتبار هذه الحالة حالة خاصة من الجرائم الماسة ببيانات وسائل الدفع الإلكتروني وهذا ما سيتوضح من خلال تحديد الركن الشرعي والركن المادي.

أولا/ الركن الشرعي

[1] - Fabrice Mattatia, op cit, p333.
[2]- Fabrice Mattatia, op cit, p334.

يستلزم الركن الشرعي لهذه الجريمة قيام الجناة باستغلال شبكة المعلومات ووسائل تقنية المعلومات للوصول إلى بيانات وسائل الدفع الإلكتروني فمن مخاطر الدفع بوسائل الدفع الإلكتروني عبر الانترنت أن هناك من يحاول اصطياد والتقاط بيانات البطاقة وأرقامها ليقوم باستعمالها خاصة وأن التعامل عبر الانترنت يوفر أهم خاصية لوسائل الدفع الإلكتروني وهي عدم كشف هوية مستعملها وغياب الحدود فالشخص الموجود في الجزائر يستطيع الاستيلاء على أرقام وبيانات لوسائل دفع الكتروني لأشخاص في أمريكا وبالتالي يمكنه استعمالها في عمليات الشراء عبر الانترنت

ثانيا/ الركن المادي

يتمثل الركن المادي لجريمة الحصول على بيانات وسائل الدفع الإلكتروني عن طريق استعمال الجناة لشبكة المعلوماتية والوسائل التقنية وبالتالي تخرج من نطاق هذه الجريمة الحصول على بيانات وسائل الدفع الإلكتروني عن طرق آخر غيرها وبالتالي الحصول على البيانات بالطرق التقليدية ولا يدخل في نطاق هذه الجريمة الافشاء من العاملين لهذه الوسائل أو عن طريق السرقة لوسيلة الدفع الإلكتروني أو أن يقوم الجناة بتصميم موقع مشابه لموقع البنك المقدم للخدمات الخاصة بوسائل الدفع الإلكتروني فيقوم صاحب الوسيلة بالدخول إلى هذا الموقع الوهمي وادخال البيانات الخاصة بتلك الوسيلة وتعد هذه الجريمة من أحدث وأخطر الصور الاجرامية المستحدثة التي تقع من قبل الغير بالاستيلاء على البيانات والمعلومات الخاصة بوسائل الدفع الالكتروني واستعمالها في أي وقت وفي أي مكان ويتم

استخدام الهوية في الاحتيال على الآخرين بما يجعل جريمة انتحال الهوية قائمة فقد أمكن لأحد المحتالين الحصول على أسماء وأرقام التأمين الاجتماعي لمجموعة كبيرة من العسكريين والقيام باستخدامها احتيالا على أحد المصارف[1] أو كان يقوم الشخص بملء استمارة ما تتضمن ما يدل على هويته، مثلا قد يتفق موظف البنك مع أفراد عصابة اجرامية منظمة على مدهم بدون وجه حق ببيانات بطاقات ائتمان صحيحة ومتداولة وذلك لاستخدامها في تقليد أو اصطناع هذه البطاقات ولاشك أن هذا الموظف يكون شريكا في جريمة منظمة مع أفراد العصابات بحيث يكون دوره هو الإمداد بالمعلومات ودورهم هو اصطناع البطاقات المزورة فيشكل هذا الأمر عدة جرائم متشابكة من حيث الإمداد بمعلومات عن حسابات العملاء وتزوير بطاقات الدفع والاستيلاء على أموال الغير بطريق غير مشروع، ولعل هذا ما يؤكد الخاصية التي سبق التطرق إليها بأن هذه الجرائم هي جرائم منظمة وغالبا ما تتحقق هذه الجريمة بأن يتم اتفاق مسبق بين الموظف بالبنك مع أحد الأفراد ويمدهم بدون وجه حق ببيانات بطاقات الدفع أو السحب الصحيحة والمتداولة وذلك لاستخدامها في تقليد واصطناع هذه البطاقات[2].

[1]– محمد الشناوي، المرجع السابق، ص 91.

[2]– عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص127.

المطلب الرابع

الضرر والركن المعنوي للجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني

نتطرق في هذا المطلب إلى عنصر الضرر والركن المعنوي لهذه الجرائم.

أولا/ الضرر

يعتبر الضرر عنصر ضروري يجب توفره لتجريم هذه الحالات السابقة نظرا لأهمية البيانات المتعلقة بوسائل الدفع الإلكتروني باعتبارها الذهب الذي تقوم عليه هذه الوسائل ومنجم جديد اكتشفه مجرمي المعلوماتية.

ثانيا/ الركن المعنوي: يتوفر الركن المعنوي لهذه الجرائم متى توفر القصد في الحصول على البيانات الخاصة بوسائل الدفع الإلكتروني وهي جريمة عمدية أي أن يكون الجاني عالما بأن هذه البيانات والأرقام التي سيستولي عليها مملوكة للغير ولا يجوز له الاستيلاء عليها ولكنه يسعى بإرادته إلى الاستيلاء عليها قصد تملكها أو استعمالها بدون وجه حق، وحتى لو لم يتحقق فعل الاستعمال إنما الحصول على هذه البيانات هو الهدف من هذه الجريمة، ولا يتصور حصول هذه الجريمة عن طريق الخطأ بل الغالب في صورها المختلفة العمد، في حين يتحقق فعل الاشتراك في الاستعمال لبيانات وسائل الدفع الإلكتروني بعد الحصول على البيانات واستعمالها في تحويل الأموال من حساب الضحية إلى حساب الجناة والاستعمال لهذه البيانات عند الشراء أو أي خدمة يتاح الحصول عليها عبر الانترنت أو أن يكون

القصد منها تقديمها لشخص آخر لتنفيذ عمليات الشراء وهذه هي الصورة الغالبة أي الحصول على مال الغير بدون وجه حق، لأن الغرض من هذه الجرائم هو تسهيل ارتكاب جرائم أخرى.

تعتبر وسائل الدفع الإلكتروني وتطورها من التحديات المستقبلية التي تواجه جرائم تبييض الأموال، لأن عملية التبييض عبر الانترنت تشكل خطرا يهدد كيان الدولة ويلحق ضرر بمنشئاتها الاقتصادية لإمكانية خروج كمية هائلة من الأموال في أي وقت مما يشكل عدم الاستقرار في الدولة نتيجة قابلية الأموال للحركة[1]، كما أن استعمال وسائل الدفع الإلكتروني يصعب من تطبيق الالتزامات التي تتقيد بها المصارف في أعمالها منها مبدأ اعرف عميلك، كما تسهل اخفاء مصدر الأموال وعمليات التبييض ومراحله غير المشروعة وتساهم في اخفاء آثار التبييض لهذا سنركز في هذا الفصل على الاشتراك في تبييض الأموال باستخدام وسائل الدفع الإلكتروني (المبحث الأول).

تساعد وسائل الدفع الإلكترونية في زيادة قيمة الأموال غير المشروعة بزيادة التهرب الضريبي للصعوبات التي تواجه إدارة الضرائب في مراقبة العمليات الإلكترونية والصفقات التي تتم عن طريقها مما يصعب من فرض الضرائب عليها (المبحث الثاني) التهرب الضريبي الإلكتروني.

المبحث الأول

الاشتراك في تبييض الأموال باستخدام وسائل الدفع الإلكتروني

كان لتفجيرات 11 سبتمبر 2001 أثر كبير في صدور العديد من اللوائح والتوصيات ذات العلاقة بمكافحة جريمة تبييض الأموال خاصة المتأتية من مصدر ارهابي، فاجتمعت

[1]-خالد ممدوح ابراهيم، المرجع السابق، ص 77.

مجموعة العمل المالي الدولي FATF[1] مباشرة بعد الحدث في أكتوبر 2001 وقامت بالتوسيع من نشاطها الذي كان يرتكز على مكافحة جريمة تبييض الأموال لتشمل أيضا تمويل الارهاب ووضعت بهذا الصدد تسع توصيات والتي تعنينا هي التوصية السادسة فقد نصت على أحكام تتعلق بأنظمة التحويل البديلة للنقود ووضعت من خلال هذه التوصية الاجراءات الضرورية لضمان التحويل القانوني للنقود وفقا للمعايير الدولية التي أتت بها توصيات FATF التي تسري على التحويلات عبر البنوك.

أثار استخدام وسائل الدفع الإلكتروني كبديل للتعامل بالنقود الورقية العديد من المشكلات ومنها ما يتعلق بتبييض الأموال ويلاحظ أن جريمة تبييض الأموال كجريمة منظمة تجد نفسها في عمليات الصيرفة الإلكترونية والتي يمكن لأي شخص ممارستها بما فيها الشباب والأحداث القادرين على ممارسة هذه المهمة في أي جزء من أجزائها[2]، وكذلك خلق وسائل جديدة سهلة الاستعمال على نطاق واسع تسهّل المدفوعات المجهولة الهوية في إطار المعاملات التجارية عبر الحدود[3]، وبالتالي استعمال وسائل الدفع الإلكتروني يجاذبه شقان الأول تسهيل المكافحة والثاني تسهيل التبييض وهذا ما سنتطرق إليه في (المطلب الأول)، ثم نبين كيف تأثرت أركان جريمة تبييض الأموال باستخدام وسائل الدفع الإلكتروني في (المطلب الثاني).

---

[1] -FATF(

[2]– عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دراسة الظاهرة الاجرامية المعلوماتية، دار الفكر الجامعي، مصر، الطبعة الأولى، 2008، ص52.

[3]– Anne –Marie Moulin, problématique dématérialisation et blanchiment,....., p112.

المطلب الأول

إشكالية جعل وسائل الدفع غير ملموسة وتبييض الأموال

استعمال وسائل الدفع الإلكتروني سهل للمصارف التخفي عند اشتراكها في التبييض لصعوبة تعقب عمليات التحويل الإلكتروني للأموال، ويعد هذا الأمر هاجسا للسلطات المختصة بمكافحة تبييض الأموال لأن سيطرة الجريمة المنظمة على المصارف سوف يعطيها حرية في تبييض كميات كبيرة ليس لنفسها فقط إنما للمنظمات الاجرامية الأخرى[1]، وبالتال فاستعمال وسائل الدفع الإلكتروني يجعلها ذات شقين هما تسهيل المكافحة وتسهيل التبييض (الفرع الأول)، مراحل تبييض الأموال هي الأخرى تأثرت باستعمال وسائل الدفع الإلكتروني (الفرع الثاني).

الفرع الأول

وسائل الدفع الإلكتروني بين تسهيل المكافحة وتسهيل التبييض

لعل وقوع هذه الجريمة (تبييض الأموال) بطريق الوسائط الإلكترونية ووسائل الدفع الإلكتروني أمر طبيعي مترتب على تحول الأعمال المصرفية إلى شكلها الإلكتروني وبالتالي ظهور مخاطر قانونية من هذا التحول تتمثل في انتهاك القوانين أو القواعد أو الضوابط

[1]– ففي روسيا وبعض دول شرق اوروبا يمكن شراء المصارف مقابل مبالغ زهيدة رغم أن هذه المصارف لديها القدرة على التحول لأعمال الصيرفة الإلكترونية العالمية –سويفت –وهي خدمة خاصة بنقل الأموال وإلى جانب المصارف فان خدمة سويفت المتعلقة بتحويل الأموال يمكن عن طريقها تقديم خدمات الية إلى الوسطاء وتجار السندات وشركات المقاصة والاسواق المالية الكبرى، أنظر عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دراسة الظاهرة الاجرامية المعلوماتية، المرجع السابق، ص53.

المقررة خاصة تلك التي تتعلق بمكافحة تبييض الأموال[1] فالأصل أن وسائل الدفع الإلكتروني وجدت لمحاربة تبييض الأموال (أولا)، لكن واقعيا يلاحظ العكس حيث استغلت في تسهيل تبييض الأموال (ثانيا).

أولا / طريقة جعل وسائل الدفع الإلكتروني غير ملموسة تسهل مكافحة تبييض الأموال

الأصل عموما أن جعل عملية السحب أو الدفع غير ملموسة مواتية تماما لمكافحة تبييض الأموال[2]، ومنه فطريقة جعل وسائل الدفع الإلكتروني غير ملموسة تعتبر عنصرا يسهل مكافحة تبييض الأموال، وهذا لأن أموال البنوك (تتداول عن طريق الكتابة) ولأن المال مسجل على حساب هذا يعني امكانية التعرف على الزبائن واعادة تسطير مسار العمليات وتتبعها[3]، و تشجع توصيات مجموعة العمل المالي GAFI على استعمال الأدوات الأخرى غير استعمال السيولة، وتعد النقود الإلكترونية من أهم التقنيات الحديثة التي حرفت عن مسارها الطبيعي، وحولت عن الهدف الذي وجدت من أجله وذلك من خلال استخدامها كأداة لارتكاب جريمة تبييض الأموال[4]، وبالتالي فالهدف الذي وجدت لأجله النقود الإلكترونية ووسائل الدفع الإلكتروني عامة ليس تسهيل ارتكاب جريمة تبييض الأموال، إنما تسهيل ملاحقتها وتتبعها كما تساهم وسائل الدفع الإلكتروني في التعرّف على الزبائن ليس فقط من

---

[1]- عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، المرجع السابق، ص13.

[2] – Anne –Marie Moulin, op, cit, p111

[3]–Anne –Marie Moulin, op, cit, p110.

[4]– بسام أحمد الزلمي، دور النقود الإلكترونية في عمليات غسل الأموال، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010، ص559.

قبل البنوك ولكن أيضا من طرف المؤسسات المالية الأخرى، وحتى بعض الشركات غير المالية[1]، وفي هذا الصدد الزمت المادة 11 من النظام رقم 03/12[2] الذي ألغى أحكام النظام رقم 05 /05[3]، المصارف والمؤسسات المالية والمصالح المالية لبريد الجزائر اتخاذ الإجراءات المناسبة للوقاية من تبييض الأموال عند استعمال الوسائل التكنولوجيا، كما ألزمت المادة 17 من نفس النظام في اطار التحويلات الإلكترونية مهما كانت الوسيلة المستعملة(SWIFT ,ARTS,ATCI...إلخ) بالتحقق بدقة من هوية **الآمر** بالعملية **والمستفيد**.

تعد وسائل الدفع بشكل عام والنقود الإلكترونية بشكل خاص أدوات حديثة للدفع سهلة الاستخدام وسريعة الحركة، ومن المفترض أن تشكل خطوة ايجابية على طريق تقدم الحياة الاقتصادية لكن مبيضي الأموال لم يرحموا هذه الوسيلة ولم يتركوها تؤدي غرضها الإيجابي الذي وجدت من أجله فعمدوا فور ظهورها لاستخدامها في ارتكاب جرائمهم مما جعلها ذات وجهين إيجابي وسلبي بدلا من أن تكون ذات وجه ايجابي فقط[4].

---

[1]-Anne –Marie Moulin, op, cit, p111.

[2]- النظام رقم 03/12 المرخ في 14 محرم عام 1434 الموافق ل 28 نوفمبر سنة 2012 المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما، ج ر عدد 12 لسنة 2013.

[3]- النظام رقم 05/05 المؤرخ في 13 ذي القعدة عام 1426 الموافق ل 15 ديسمبر سنة 2005، المعدل والمتمم للنظام 01/05 المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما، ج ر عدد 26، 2005.

[4]- حوالف عبد الصمد، المرجع السابق، ص377.

ثانيا / وسائل الدفع الإلكتروني تسهل تبيض الأموال

تتميز وسائل الدفع الإلكتروني بتسهيل خطر تبييض الأموال بطبيعتها اللامادية مما يجعل مراقبة هوية الأطراف أمرا في غاية الصعوبة[1] الملاحظ واقعيا أن وسائل الدفع الإلكترونية تسهل تبيض الأموال حيث يتم التعامل بوسائل الدفع الإلكترونية دون حاجة إلى ظهور الهوية الحقيقية للمتعاملين وأحيانا دون ظهور هويتهم اطلاقا وهذا ما يسهل على المجرم اخفاء شخصيته حتى ولو كان معتادا على تبييض الأموال، كما أن لوسائل الدفع الإلكترونية جانب من السرية يجعل مهمة خلية الاستعلام المالي بمراقبة تبييض الأموال جد صعبة حيث يصعب مراقبة السجلات والعمليات المالية والمصرفية التي تتم باستخدام وسائل الدفع الإلكترونية.

فضلا عن أن استخدام هذا النوع من النقود يعتمد بدرجة كبيرة على أنظمة الدفع الإلكتروني وأجهزة الحاسب الآلي التي تتوقف عن العمل نتيجة الإجرام المقصود أو التوقف التلقائي ليستحيل معه مراقبة العمليات التي تمت وبالتالي تسهيل ارتكاب جريمة تبيض الأموال.

بنك الجزائر مزود بالمركزيات وباللجنة المصرفية التي تؤدي دورا لا يستهان به في الكشف والتبليغ ومنع ارتكاب تبييض الأموال من خلال مراقبة السوق النقدي وكذا المراقبة الدائمة للبنوك وهنا يبرز خطر نمو النقود الإلكترونية التي تؤثر في ميزانية بنك الجزائر ومن ثم تقليص ميزانية البنك بسبب انخفاض القاعدة النقدية مما يقلص من دوره في مراقبة السوق النقدي، ومن ناحية أخرى فإن المدفوعات الإلكترونية أو الدفع بطريق إلكتروني يساعد

[1]-Étienne Wéry, op, cit, p47.

أطراف الصفقات التجارية في الحصول على مقابل السلعة أو الخدمة بطريقة سرية وآمنة ومناسبة فيما يتعلق بالتحويلات النقدية.

انتشار هذا النوع من وسائل الدفع يسهل الانتقال العالمي للأموال بطريقة غير مشروعة خاصة وأن السرعة التي تتسم بها هذه النظم تجعلها عالية الكفاءة، كما ترفع من عنصر السرية فيها حسب وجهة نظر أولئك الذين يعملون في حقل تبييض الأموال.

هذه المزايا لوسائل الدفع الإلكتروني تشكل عائقا أمام السلطات المختصة و الضبطية القضائية في تجميع الأدلة والبحث والتحري عن تبييض الأموال، خاصة وأن هناك أفاق للتبادل المباشر الممكن من وسيلة دفع إلى وسيلة أخرى وبالتالي من حامل إلى آخر، وكذا وجود وسائل غير مرتبطة بحساب بنكي[1] مما يصعب من مهمة السلطات المختصة بمكافحة هذه الجريمة.

أصبح تبييض الأموال إلكترونيا جريمة يسهل ارتكابها[2] ولكن يصعب اكتشافها كما أن استخدام وسائل الدفع الإلكتروني أثرت على المبادئ التي يقوم عليها العمل المصرفي ومنها مبدأ اعرف عميلك، لأنها ستقلل من تعامل الزبون الشخصي وجها لوجه مع البنك وبالتالي عدم تطبيق المبدأ الهام "تعرف على عميلك" كما أن استخدام هذه الأموال الإلكترونية سيسمح للطرفين بتنفيذ العملية المالية فيما بينهما مباشرة دون الحاجة لوسيط ثالث (بنك

[1]– Anne –Marie Moulin, op, cit, p111.

[2]– العيد سعدية، المرجع السابق، ص 233.

مثلا) وبالتالي عدم وجود مستندات ورقية يمكن اقتفاء آثارها وتعقبها[1] وعليه يجب على الدول اتباع منظومة محكمة لمراقبة وملاحقة هذه الجريمة بوسائل تتميز بالدقة والسرية، فالبطاقات المسبقة الدفع أصبحت من وسائل الدفع المفضلة من طرف الكارتل المتخصص في تجارة المخدرات في أمريكا لأن بعض العمليات الحالية تتحقق بمساعدة البطاقات المسبقة الدفع وتمثل خطر لرفع تبييض الأموال وتمويل الارهاب وتهرب كبير لمراقبة الهوية[2].

الفرع الثاني

مراحل تبييض الأموال و تأثرها بوسائل الدفع الإلكتروني

تتمتع وسائل الدفع الإلكتروني بمجموعة من المزايا تجعلها تنسجم أكثر مع فكر مبيضي الأموال(أولا)، ومكنت هذه المزايا من اعادة هندسة مراحل تبييض الأموال (ثانيا).

أولا / مزايا وسائل الدفع الإلكتروني في تبييض الأموال

تتصف وسائل الدفع الإلكتروني بميزات تخدم الوصفة الخاصة لعملية تبييض الأموال وتتمثل فيما يلي:

1-**السرية والكتمان:** حيث يمكن للمشتري أن يقوم بعملية الشراء دون أن يكون مضطر لتقديم اية معلومات[3] وهذه أهم ميزة تتطلبها عملية التبييض.

---

[1]- حسام العبد، غسل الأموال الإلكتروني، مجلة البنوك في الأردن، العدد السادس، المجلد التاسع عشر، أيلول 2000، ص 16.

[2]- Myriam Quéméner, criminalité économique et financière à l'ère numérique, op, cit 77

[3]- لسلوس مبارك، النقود الإلكترونية بين الكبح والتشجيع لجريمة غسل الأموال، مداخلة قدمت للملتقى العلمي الدولي الرابع حول نظام عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الإلكترونية في الجزائر (عرض تجارب دولية)، المنظم من طرف معهد العلوم الاقتصادية، المركز الجامعي خميس مليانة، يوم 26-27أفريل 2011.

2-**الدرجة العالية من الأمان:** تتيح وسائل الدفع الإلكتروني أعلى درجات الأمان الممكنة لحماية المعلومات المالية عبر الانترنت.

3-**انخفاض التكلفة:** فهذه الوسائل قيمتها أقل بكثير من قيمة وسائل الدفع التقليدية حيث تنعدم تكاليف المقاصة أو التسوية لأنها تتم آليا.

4-**التخطي للحدود:** بعدم الاعتراف بالحدود الجغرافية والسياسية للدول وهذا مرمى تبييض الأموال.

5-**السهولة في الاستخدام:** لأنها تغني عن الاستمارات واجراء الاستثمارات واجراء الاستعلامات البنكية.

6-**السرعة في عمليات الدفع:** تمكن المتعاملين بها من اتمام صفقاتهم وهم في المنزل أو المكتب دون الذهاب للمصرف وهذا ما يتيح اخفاء الأثر للمعاملات المالية فالعمليات الإلكترونية تتوافق مع هذا الغرض فتجري حركة التعاملات المالية ويتم تبادل المعلومات والتنسيق الخاصة بها فورا في الزمن الحقيقي دون الحاجة إلى أي نوع من الوساطة.

ثانيا/مراحل تبييض الأموال إلكترونيا

4-مرحلة التوظيف: الهدف منها هو المباعدة بين الأموال غير المشروعة ومصدرها الأصلي بالتوظيف للأموال القذرة عن طريق التحويل الإلكتروني الفوري للأموال إلى حسابات مصرفية خارجية، أو تغيير الأموال الإلكترونية إلى سندات أو شيكات سياحية أو تحويل النقد الإلكتروني من وسيلة دفع إلكتروني إلى وسيلة أخرى، أو تحويل الأموال القذرة إلى نقود إلكترونية، وباستخدام النقود الإلكترونية يمكن تنفيذ عملية التوظيف من خلال جهاز حاسب آلي شخصي وبدون أية آثار يمكن تعقبها.

5-مرحلة التغطية(التمويه): يتم اخفاء طبيعة الأموال القذرة واضفاء صفة المشروعية عليها بطريقة مباشرة وبدون أن يتم في هذه الحالة شراء أصول مادية ودفع ثمنها عن طريق وسائل الدفع الإلكتروني إلا أنه في واقع الأمر قد يتم استخدام أساليب غير مشروعة والتلاعب في عملية التسديد[1] ومن صور عملية التمويه بالوسائل الإلكترونية التواطؤ بين المصارف الوطنية والأجنبية واستخدام بطاقات الدفع والبطاقات الذكية والحسابات الرقمية المتغيرة[2]، تبدو هذه الصورة ملائمة لملاحقة الوسائل المتطورة والتقنيات المصرفية بالغة التعقيد التي تساهم على نحو أو آخر في عملية التبييض وتيسر لها[3] ومنها وسائل الدفع الإلكتروني.

---

[1]-حوالف عبد الصمد، المرجع السابق، ص376.

[2]-عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، المرجع السابق، ص115.

[3]-سليمان عبد المنعم، مسؤولية المصرف الجنائية عن الأموال غير النظيفة، دار الجامعة الجديدة، مصر، 2002، ص 19 .

6-في مرحلة الدمج: يقوم الحائز بإجراء التحويلات الإلكترونية إلى دول أخرى ليست فيها عملية التبييض ثم يعيد تحويلها إلى دول أخرى ليدخلها في الدورة الاقتصادية دون أن تتعرض لكشف مصدرها، ففي مرحلة الدمج يتم خلق الاحساس بمشروعية الأموال القذرة بمحاولة دمجها بالدورة الاقتصادية من خلال:

-الايداع الإلكتروني للنقود والأرباح المتأتية من الصفقات والشركات المشبوهة والوهمية في المصارف الإلكترونية.

-الدخول إلكترونيا إلى الأسواق المالية الثانوية والقيام بعمليات البيع والشراء للأسهم والسندات.

-القيام بعمليات التجارة الإلكترونية.

المطلب الثاني

أثر وسائل الدفع الإلكتروني في أركان الجريمة

من وجهة نظر قانونية تعد النصوص التي شرعت لمكافحة تبييض الأموال التقليدي قاصرة على أن تشمل بالتجريم والعقاب تبييض الأموال كصورة مستجدة ومغايرة للصورة التي تقع بها جريمة تبييض الأموال التقليدية، وبالتالي فإن وسائل الدفع الإلكتروني أثرت في ضرورة إعادة بلورة أركان جريمة تبييض الأموال من ضرورة تعديل الركن الشرعي لتبيض الأموال إلكترونيا (الفرع الأول)، وكذا بالنظر إلى تغير أساليب التبييض وتغير محل التبييض كلها أثرت في الركن المادي لجريمة تبييض الأموال إلكترونيا(الفرع الثاني).

الفرع الأول

ضرورة تعديل الركن الشرعي لتبييض الأموال إلكترونيا

وسع المشرع الجزائري من مفهوم الاشتراك في تبييض الأموال (أول)، ورغم هذا التوسع إلا أننا نلاحظ عدم كفاية النصوص الحالية (ثانيا)، مما يحتم علينا إعادة الصياغة للركن الشرعي لتبييض الأموال إلكترونيا (ثالثا).

أولا/ مفهوم الاشتراك في تبييض الأموال من الضيق إلى التوسع

تنفيذا من الجزائر لالتزاماتها الناتجة عن مصادقتها على الاتفاقيات الدولية المتعلقة بتبييض الأموال، وتكريسا لمبدأ الشرعية أدرج المشرع الجزائري قسم خاص بتبييض الأموال في قانون العقوبات بموجب القانون 15/04 المؤرخ في 2004/11/10 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات، و يشتمل على المواد 389 مكرر إلى 389 مكرر 7، كما نص في المادة 389 مكرر على تجريم فعل تبييض الأموال[1]، وأهم ما جاء به المشرع الجزائري هو التوسع في مفهوم الاشتراك في تبييض الأموال مقارنة بالقواعد العامة للاشتراك في القانون الجزائري.

وفقا للمادة 389 مكرر[2] من قانون العقوبات "يعتبر تبييضا للأموال:...

---

[1]- إن الجزائر بذلت ما في كل ما في وسعها لاستيفاء شرط الانضمام للمنظمة العالمية للتجارة بإدخالها جريمة تبييض الأموال في قانون العقوبات، و إصدار قانون الوقاية من تبييض الأموال وتمويل الإرهاب تكون قد التزمت بالاتفاقيات التي صادقت عليها وطبقت النصائح التي قدمتها GAFIمن خلال 49 توصية.

[2]- تنص المادة 389 مكرر من قانون العقوبات الجزائري" يعتبر تبييض للأموال:

– المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو تواطؤ أو التآمر على ارتكابها و محاولة ارتكاب أو المساعدة و التحريض على ذلك و تسهيله وإسداء المشورة بشأنه " **فوفقا لهذه المادة يعتبر الاشتراك من قبل الجريمة نفسها**[1]، وهذه الفقرة نفسها أوردها المشرع الجزائري في المادة 03مكرر من القانون المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتها المعدل والمتمم[2] ولو أنها تضمنت تناقض في المصطلحات وعدم التناسق بين النص الفرنسي والنص العربي، حيث بالعودة إلى النص باللغة الفرنسية[3] ومن خلال قراءتنا له نفهم بأن كل من participation – association – entente tentative– complicité هي من صور تبييض الأموال والتي تحصل بالوسائل التالية assistance – conseil لورود العبارة بالفرنسية par la fourniture de وبالتالي نتساءل عن مفهوم مصطلح مشاركة فهل تعني participation أم أن المقصود به هو فعل

أ/ تحويل الممتلكات أو نقلها مع علم الفاعل أنها عائدات إجرامية بغرض إخفاء أو تمويه المصادر غير المشروعة لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته.

ب/ إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيه أو حركتها أو الحقوق المتعلقة بها مع علم الفاعل أنّها عائدات إجرامية.

ج/ اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنّها تشكل عائدات إجرامية.

د/ المشاركة في ارتكاب أي من الجرائم المقررة. وفقا لهذه المادة. أو تواطؤ أو التآمر على ارتكابها و محاولة ارتكاب أو المساعدة و التحريض على ذلك و تسهيله. وإسداء المشورة بشأنه '.

[1]– ولو أن المشرع الفرنسي ينص مباشرة على اشتراك المصارف في عمليات التبييض.

[2]– القانون رقم 06/15 المؤرخ في 15 فيفري 2015 الموافق ل25 ربيع الثاني 1436 هـ، المعدل والمتمم للقانون رقم 01/15 المؤرخ في 06 فيفري 2005 الموافق ل27 ذي الحجة 1425 هـ، المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما، ج ر عدد08، 2015.

[3]– دلندة سامية، ظاهرة تبييض الأموال مكافحتها والوقاية منها، نشرة القضاة، العدد 60، ص251.

الاشتراك في الجريمة المنصوص عليه في المادة 42 و ما بعدها من قانون العقوبات إلا أن الراجح أن هذا لا يعدوا أن يكون من باب الخلط والتناقض الذي وقع فيه المشرع[1] وكذلك قصد المشرع إضافة صور أخرى للاشتراك قصد التوسع في التجريم[2] مثل التواطىء- التآمر - التسهيل - إسداء المشورة خلافا للقاعدة العامة المتضمنة في الاشتراك والذي يقتصر على المساعدة والمعاونة[3]، كما لا يمكننا تصور أن كل من كان له ضلع في الجريمة من قريب أو بعيد يعتبر فاعل أصلي وجوبا، وهذا تأكيدا من المشرع على محاصرة هذا النشاط ومن توصيات إعلان بازل تقرير المسؤولية الجنائية للمصارف والشركات باعتبارهم شخصيات معنوية بالإضافة إلى إيقاع المسؤولية الجنائية على العاملين فيها واعتبارهم شركاء في الجريمة في حال وقوع عملية تبييض للمال[4].

---

[1]- والدليل على ذلك أن ما يلاحظ على هذه المادة أنها نقلت حرفيا من المادة 06 من الاتفاقية الأممية لمكافحة الجريمة المنظمة حيث لا يمكننا تصور أن كل من كان له ضلع في الجريمة من قريب أو بعيد يعتبر فاعل أصلي وجوبا، الدليل على أن هذه المادة نقلت حرفيا أنها تضمنت فعل التحريض والذي يعد حسب المشرع الجزائري فاعل أصلي (الفاعل المعنوي) خلافا لبعض التشريعات التي تعتبره من قبيل الاشتراك، عملا بالقواعد العامة فان المشرع قصد في هذه الفقرة الاشتراك في تبييض الأموال والدليل على ذلك أنه لم يتبع هذه الفقرة بعبارة ' مع علمه بأنها تشكل عائدات إجرامية مثلما فعل في الفقرات الثلاثة الأولى.

[2]- خلافا لما يراه البعض من أن الاشتراك المقصود في هذه المادة ليس الاشتراك بمعناه الاصطلاحي إنما المقصود الاشتراك بالمصطلح الشرعي أي الاشتراك في التنفيذ كفاعل أصلي ويطبق وصف الشريك على من يقوم بذات الفعل المكون للركن المادي أو بجزء منه أو بدور تنفيذي أو بدور رئيسي على مسرح الجريمة، أنظر بهذا الخصوص نبيل صقر، قمراوي عز الدين، الجريمة المنظمة، دار الهدى، ص 171.

[3]- يعتبر الاشتراك عمل مساهمة في الجريمة وحصره المشرع الجزائري في المساعدة والمعاونة على ارتكاب الأعمال التحضيرية أو المسهلة أو المنفذة لها فالشريك هو من يساهم بصفة عرضية أو ثانوية في الجريمة، علما أن المادة 43 تضيف لحكم الشريك من يقدم مسكنه مأوى للمجرمين.

[4]- غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 179.

تبييض الأموال عن طريق وسائل الدفع الإلكتروني غالبا كجريمة ترتكب عن طريق مساعدة المصرفي لمرتكب جريمة تبييض الأموال وبالتالي و بالتالي صور الاشتراك هي غالبا الصورة التي يتم على أساسها متابعة المؤسسات المالية والمصرفية والعاملين فيها إذا ما تورطوا في تبييض الأموال.

ثانيا / عدم كفاية النصوص الحالية رغم التوسع

الوسائل الحديثة –بلا شك– مهدت الطريق للمجرمين وجعلت من قابلية استغلال تلك الأدوات المالية الجديدة في عمليات التبييض للأموال ممكنة بسبب غياب النصوص التشريعية التي تجرم وتعاقب على اساءة استخدام تلك الوسائل الإلكترونية وكذلك غياب الضوابط الرقابية التي تنظم عملية اصدار تلك الوسائل الحديثة واستخدامها[1] وبالتالي فغياب تنظيم ممارسة الرقابة على وسائل الدفع الإلكتروني وتنظيم عملية اصدار هذه الوسائل، وكذا غياب النصوص التشريعية الجنائية الخاصة بتبييض الأموال إلكترونيا كلها ثغرات تفسح المجال للمجرمين لممارسة نشاطهم بكل أريحية وبلا شك سينتشر بسرعة في ظل الفراغ التشريعي القاضي بتجريمه، وهذا ما يثير قلق المنظمات الدولية والسلطات المختصة في مختلف الدول المعنية بوضع المعايير والضوابط لمكافحة استغلال النظام المالي لغرض جنائي، وتعد قوانين مكافحة تبييض الأموال في صورته التقليدية قاصرة عن مواجهة النمو المتزايد لأساليب تبييض الأموال المصاحب لتطور وسائل الدفع الإلكتروني.

[1]– سعود بن عبد العزيز المريشد، المرجع السابق، ص 217.

وبالتالي من الناحية القانونية فإن قوانين تبييض الأموال المحلية في صورتها التقليدية لا تستوعب وسائل الدفع الإلكتروني إذا ما استغلت لغرض جنائي، وبالتالي فإن ارتكاب جريمة تبييض الأموال باستغلال المزايا التي توفرها هذه الوسائل يمكن أن تفلت من العقاب الجنائي لأن من سمات القانون الجنائي عدم جواز التوسع في تفسير نصوصه لكي تشمل أفعالا لم يقصدها المشرع صراحة بالنص على تجريمها، فعندما ترتكب هذه الجريمة باستعمال وسائل الدفع الإلكتروني فهي من وجهة نظرنا جريمة إلكترونية وبالتالي حتى عندما عدل المشرع الجزائري قانون العقوبات أغفل تعديل النص الخاص بتبييض الأموال إلكترونيا.

ثالثا / الحاجة إلى إعادة صياغة الركن الشرعي لتبييض الأموال إلكترونيا

تعتبر جريمة تبييض الأموال من الجرائم المنظمة والمدروسة بإتقان حيث أخذت تشهد عمليات التبييض دخول مجموعة من الأفراد المهنيين والمتخصصين في هندسة نظم المعلومات، كما أنها تتماشى مع الوسائل التكنولوجيا الحديثة[1] وبالنسبة لعالمنا العربي فالدول مدعوة للمبادرة إلى إجراء التعديل التشريعي لقوانينها الخاصة بمكافحة جرائم تبييض الأموال كي تستوعب تلك الأساليب الإلكترونية المستحدثة أو إلى سن قوانين جنائية خاصة بمكافحة الجرائم المعلوماتية وتضمينها نصوص قانونية تجرم إساءة استخدام وسائل التقنية لغرض تبييض الأموال غير المشروعة أو ما يعرف بتبييض الأموال الإلكتروني[2].

---

[1]- رافعة ابراهيم الحمداني، أثر استخدام التكنولوجيا المصرفية في ظاهرة غسيل الأموال والجهود الدولية لمكافحتها، المؤتمر العلمي الرابع، الريادة والابداع – استراتيجيات الأعمال في مواجهة تحديات العولمة – بجامعة فيلادلفيا كلية الحقوق والعلوم الادارية والمالية، يومي 15،16 مارس 2005.

[2]– سعود بن عبد العزيز المريشد، المرجع السابق ، ص218.

يجب سن نصوص عقابية جنائية خاصة بجريمة تبييض الأموال باعتبارها جريمة من جرائم اساءة استخدام تكنولوجيا المعلومات وتحديد صور النشاط المكون لها بشكل واضح ومحدد منعا للاجتهاد والقياس وامتثالا لمبدأ الشرعية.

فجريمة تبييض الأموال الإلكتروني هي مزيج بين مقومات جريمة غسل الأموال التقليدية وبين التقنية التي أثرت في أساليب ارتكاب جريمة تبييض الأموال العادية نتيجة اعتمادها على نظم اقتصادية ومالية إلكترونية كطرق الدفع الذكية ونحو ذلك[1]، وتنص المادة 16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات على تجريم " 1-القيام بعمليات غسل الأموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال...".

نصت المادة 19 من القانون الاتحادي الإماراتي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات على أنه : " مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال يعاقب بالحبس مدة لا تزيد عن سبع سنوات وبالغرامة التي لا تقل عن ثلاثين ألف ولا تزيد على مائتي ألف درهم كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو اخفائه أو قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بأنها من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات وذلك مع العلم بمصدرها غير المشروع **عن**

[1]- سعود بن عبد العزيز المريشد، المرجع السابق ، ص 233.

طريق استخدام الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات بقصد اضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعا لارتكاب أي من هذه الأفعال ".

يلاحظ على المادة 19 من القانون الاماراتي في شأن مكافحة تبييض الأموال أن المشرع قد أحال إلى قانون مكافحة غسل الأموال في شأن الأحكام الخاصة بهذه الجريمة متى وقعت عن طريق وسائط إلكترونية[1] ومن ثم يمكننا القول أن تبييض الأموال الإلكتروني يمثل العملية أو العمليات التي تتم بواسطة استخدام الانترنت من خلال استغلال نظم مالية ذات تقنية متطورة لإخفاء أو تمويه الطبيعة غير المشروعة لتلك الأموال بسبب مصدرها الإجرامي[2]، وبالتالي فأغلبية الدول انتبهت إلى أهمية مكافحة تبييض الأموال إلكترونيا وبدأت بالمكافحة التشريعية كخطوة أولى، يتحتم على المشرع الجزائري اضافة مصطلح التبييض عن طريق استعمال الوسائل الإلكترونية وشبكة الأنترنت ووسائل تقنية المعلومات.

رابعا/ إنشاء مواقع لنشر أساليب تبييض الأموال كصورة جديدة

بعد مصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات يستوجب على المشرع الجزائري تعديل نصوص تبييض الأموال وإضافة صورة جديدة للتبييض وهي نشر طرق القيام بتبييض الأموال.

---

[1]-عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، المرجع السابق، ص152.

[2]-سعود بن عبد العزيز المريشد، المرجع السابق، ص 234.

يقوم المبيضون بإنشاء وتصميم مواقع[1] على الشبكة العالمية الانترنت تبين كيفية تبييض الأموال عن طريق وسائل الدفع الإلكتروني، والموقع عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تشمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العالمية ويقوم بحل رموز HTMLواصدار التعليمات لإظهار الصفحات المكتوبة لهذا فإن معظم المبيضيين لهم مواقع إلكترونية وهي بمثابة المقر الافتراضي لها وإذا ظهر موقع للتبييض اليوم فانه يختفي غدا لأنه سيغير من نمطه الإلكتروني ثم يختفي ليظهر مرة أخرى بشكل جديد مغاير وعنوان إلكتروني مختلف بل نجد لعض المنظمات المختصة في التبييض آلاف المواقع حتى يضمنوا انتشارا أوسع وحتى ولو تم منع الدخول على بعض هذه المواقع وتعرضت بعضها للتدمير تبقى المواقع الأخرى يمكن الوصول إليها، وبالتالي لا مفر من إدانة أصحاب هذه المواقع بالاشتراك في تبييض الأموال في الجزائر نتيجة غياب النص عليها قانونا ويعتبر عملهم من قبيل المساعدة للمبيضين.

الفرع الثاني

وسائل الدفع الإلكتروني وتسهيل اخفاء الجريمة المصدر

على خلاف بعض التشريعات المقارنة أخذ المشرع الجزائري بالأسلوب المطلق في تحديد الجريمة المصدر فلم يحصرها في مجموعة من الجرائم بل وضع نصا عاما ليشمل كافة

[1]-عرفت المادة 07/02 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات "...الموقع : مكان اتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد...".

الجنايات والجنح وهذا مسلكا محمودا من المشرع الجزائري حتى لا يفلت الجاني من العقاب في الكثير من الجرائم، إلا أنه بالرجوع لنص المادة 389 مكرر من قانون العقوبات نجده يتكلم عن تبييض العائدات الإجرامية[1]" يعتبر تبييضا للأموال تحويل الممتلكات أو نقلها مع علم الفاعل أنّها عائدات إجرامية...".

كما عرّف في المادة 02 /ز قانون06 /01المتعلق بمكافحة الفساد العائدات الإجرامية أنّها: كل الممتلكات المتأتية و المتحصل عليها **بشكل مباشر أو غير مباشر في ارتكاب الجريمة** أن ترجمة المادة 389[2]مكرر لم تكن سليمة لأن" le produit d'un crime "أي عائدات جناية يختلف عن عائدات إجرامية التي تعني"le produit d'une infraction" .

ساهمت وسائل الدفع الإلكتروني في إخفاء الجرائم المصدر والتستر عليها فقد مكنت النقود الإلكترونية المجرم الذي كدس مليارات الدولارات من تجارة المخدرات وغيرها من الجرائم التي ارتكبها، والتي كان يصعب عليه في الماضي اخفاؤها لضخامتها من تحويلها إلى نقود إلكترونية مما يسهل عليه استثمارها في الاقتصاد المشروع، فضلا عن عرقلة اكتشاف الجرائم الأولية التي تحصلت منها[3].

---

[1]- أن مصطلح عائدات إجرامية هو مصطلح من علم الإجرام، و لا يصلح صبّه في نص تجريمي يحكمه مبدأ شرعية الجرائم و العقوبات من جهة و مبدأ التفسير الضيق للنص الجزائي من جهة أخرى، أنظر غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 180.

[2]- المادة 389من قانون العقوبات '...مع علم الفاعل بأنها عائدات إجرامية ..." يقابلها باللغة الفرنسية « l' auteur sait qu'il sont le produit Dun crime »،

[3]-بسام أحمد الزلمي، المرجع السابق، ص546.

الفرع الثالث

الركن المادي لجريمة تبييض الأموال إلكترونيا

تختلف صور الركن المادي لتبييض الأموال إلكترونيا ومراحله عن تلك التقليدية (أولا)، كما أنها توسع من محل تبييض الأموال (ثانيا).

أولا/ السلوك المادي للاشتراك في تبييض الأموال بوسائل الدفع الإلكتروني

تأثر القطاع المصرفي كغيره من القطاعات بالتكنولوجيا وطور خدماته المصرفية ووسائل الدفع الإلكترونية، وبالمقابل فإن عصابات الجريمة المنظمة ومبيضي الأموال استفادوا من هذه التكنولوجيا وبالتحديد من المخاطر المصاحبة لاستخدامها وبذلك فقد تطورت وتغيرت أساليب وطرق تبيض الأموال وأصبحت تبتعد تدريجيا عن الأساليب التقليدية التي تكون عرضة للاشتباه فيها وكشفها بسهولة[1] بل إن العصابات أصبحت تتفنن في طرق الاستفادة غير المشروعة من الخدمات التي توفرها وسائل الدفع الإلكتروني، ومن خصائص جريمة تبييض الأموال إلكترونيا أنها جريمة عالمية لا ترتكب في اطار دولة فحسب بل إن عولمة المال والاقتصاد الناجمة عن زيادة الروابط الإلكترونية والاعتماد المتزايد على التقنية الحديثة قد أسهم في تدويل الجريمة، ويتلخص السلوك الاجرامي للشريك في جريمة تبييض الأموال بواسطة وسائل الدفع الإلكتروني في كل فعل أو تصرف إيجابي للمساعدة يسمح بقطع الصلة بين الأموال المتحصلة عن جريمة ومصدرها غير المشروع، فالشريك هو من لا

[1]– رشيد بوعافية، مزيود بوعلام، المرجع السابق.

يرتكب العناصر المادية المكونة للجريمة وإنما يأتي أقوالا وأفعالا ذات أهمية قانونية لتسهيل ارتكاب الجريمة ويجب أن يكون الاشتراك سابقا أو معاصرا لأفعال التبييض[1] تضمنت المادة 389 مكرر من قانون العقوبات الجزائري أربع صور محددة بصفة حصرية:

1- تحويل الممتلكات أو نقلها:

أ-**التحويل:** يقصد به إجراء عمليات مصرفية كإيداع الأموال أو الممتلكات بالمصارف أو بالإقراض أو المبادلة ...الخ و قد يتم التحويل عن طريق بطاقات ائتمان مزورة و السحب بها من حسابات الزبائن ثمّ إيداع تلك الأموال في حسابات عادية بالمصارف وقد يكون تحويل إلكتروني وهي تقنية أصبحت تشكل منفذا جيدا لعمليات تبييض الأموال بتحويلها إلى أي مصرف في العالم في وقت قياسي و يفترض في تبييض الأموال بأغلب صوره تواطؤ المصرفي و مساهمته و كذا العاملين معه على نحو أو آخر باستخدام العديد من الأساليب و الحيل المصرفية المشروعة في ذاتها[2]، وتحويل الأموال كذلك قد يتم من عملة وطنية إلى عملة أجنبية في ظل عدم وجود قيود تشريعية على هذه التحويلات[3]، وخاصة الإلكترونية .

ب-**النقل:** فإنه حسب رأينا ليس من الجرائم التي تتم بمساهمة المصرفي أو مساهمة عدة أطراف، وليس من الجرائم التي تتم بوسائل الدفع الإلكتروني، كما أن مصطلح نقل قد يشكل

[1]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص182.

[2]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 183.

[3]-عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، المرجع السابق، ص152.

سلوك مادي لتبييض الأموال في غير المجال المصرفي في صورتها التقليدية[1] فالشائع استخدامه هو التحويل الإلكتروني، يتم التعامل عن طريق البطاقات مع أجهزة ATM مباشرة دون الحاجة إلى الدخول للمصرف و استخدام هذه الأجهزة في عملية سحب وايداع النقود في الحسابات المصرفية يهدف إلى التخلص من الاجراءات المصرفية التقليدية[2]، هذه الأخيرة تتضمن تعبئة نماذج ورقية والتي من الممكن أن تكشف مصدر الأموال المشكوك فيها، يتم استخدام وسائل الدفع الإلكتروني في تبييض الأموال بإجراء العديد من عمليات السحب والايداع لضمان عدم الكشف ولفت الانتباه وتحاشيا للالتزامات القانونية المترتبة على البنوك بالبلاغ عن عمليات الايداع والسحب المشكوك فيها والتي تتجاوز المبالغ المحددة رقابيا من طرف بنك الجزائر، وأكثر عمليات تبييض الأموال خطورة التي حدثت باستخدام البطاقة الائتمانية هي التي قام بها مبيضو الأموال في أمريكا حيث قام المجرمون ببناء ماكنة صرف آلي مزورة استطاعوا من خلالها معرفة الأرقام السرية للعملاء الذين استخدموها ثم قاموا بتزوير هذه البطاقة واستخدامها في السحب عن طريق المنافذ الحقيقية للسحب الآلي وبالتالي الاستيلاء على مبالغ هؤلاء العملاء وفي الغالب بعد سحب مرتكبي جريمة تبييض الأموال من النوافذ الإلكترونية يقومون بإيداعها في حسابات متعددة بالبنوك ثم يقومون بتحويلها إلى عدة فروع في بلدان مختلفة بحيث يتم التمويه أساسا عن مصدر هذه الأموال

[1]– العيد سعدية، المرجع السابق، ص74.

[2]_مصطفى كافي، النقود والبنوك الإلكترونية، دار مؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2012، ص329.

غير المشروعة[1]، والنقود الإلكترونية من أهم الأدوات الإلكترونية لمبيضي الأموال لاستحالة تعقبها وسريتها وسرعتها، حيث يمكن تحويل أي مبلغ من خلالها في فترة قصيرة من دون أية اعاقات جغرافية أو قانونية أو مصرفية وبدون الحاجة للوسيط المالي[2].

فالعلاقة بين النقود الإلكترونية وعملية تبييض الأموال تتجلى باستغلال النقود الإلكترونية كوسيلة لارتكاب الجريمة فهي تعد وسيلة مثالية لاختزان قيمة نقدية لأموال متحصلة من مصدر غير مشروع تمهيدا لغسلها، وهنا يبرز الجانب السلبي لهذه الوسيلة المتطورة من وسائل الدفع الإلكتروني بحيث تتحول إلى وسيلة لارتكاب جريمة تبييض الأموال على اعتبار أن مراقبتها مسألة في غاية الصعوبة[3]، وهذا بالنظر لأنها تسهل عملية نقل الأموال من بلد لآخر دون خضوعها لإجراءات وقيود التحويل التي تكون مفروضة في بعض البلدان[4] فيستطيع مبيض الأموال القيام بعملية إخفاء الأموال غير المشروعة بما يشاء من العمليات المصرفية لأن النقود الإلكترونية ليست مادية محسوسة يمكن مراقبة حركتها.

وتستعمل النقود الإلكترونية في مرحلتي الايداع والدمج فيبدأ بإيداع الأموال المراد تبييضها بطريقة الايداع الرقمي ليتفادى المحاسبة الورقية فعملية التحويل الإلكتروني لهذه الأموال لا

---

[1]-آيت عكاش سمير، سعيد الهواري، مداخلة بعنوان البنوك الإلكترونية وعمليات غسيل الأموال، قدمت للملتقى العلمي الدولي الخامس حول الاقتصاد الافتراضي وانعكاساته على الاقتصاديات الدولية.

[2]-مصطفى كافي، النقود والبنوك الإلكترونية، ص330.

[3]-يسام أحمد الزلمي، المرجع السابق، ص552.

[4]-صفوت عبد السلام عوض الله، بحث بعنوان الاثار الاقتصادية لعملية غسيل الأموال ودور البنوك في مكافحة هذه العملية، مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الرابع، ص1548.

يشوبها أي تلاعب إلا أن صفة عدم المشروعية يرجع إلى مصدر الأموال بحد ذاتها، حيث يلجا مبيضي الأموال بشراء السلع في بلد معين باستخدام البطاقات وبعدها يقوم البنك الذي تمت عملية الشراء في بلده بطلب تحويل القيمة من فرع البنك مصدر البطاقة الذي يقوم بعملية التحويل التلقائي ويخصم القيمة من حساب زبونه الذي يقوم بعملية البيع للسلع دون المرور عبر قنوات وقيود التحويل ثم يقوم بعملية ايداعها بالبنوك مما يصعب معرفة مصدر الأموال.

2-إخفاء أو تمويه الطبيعة الحقيقية للممتلكات: هي غرض السلوك الأول (الإيداع) و تعني حيازة الأموال و المتحصلات في الجريمة المصدر حيازة مستترة أو علنية و يقتضي **الإخفاء** أن يصدر من المصرفي سلوك ايجابي يتمثل في حيازة الأموال أو تسلمها و لو لم تكن له السيطرة المادية عليها[1] وعلى هذا فان الدور الذي يقوم به المصرفي من قبول لإيداع أو تحويل أو استخدام الأموال أو المتحصلات الناتجة عن نشاط إجرامي باستخدام أي وسيلة من وسائل الدفع الإلكتروني ينطوي تحت فعل الإخفاء، أما **التمويه** فهو تغيير طبيعة هذه الأموال بعدد من التحويلات الداخلية والخارجية بحيث يتعذر الوصول إلى مصدرها تبدو هذه الصورة ملائمة لملاحقة الوسائل المتطورة والتقنيات المصرفية بالغة التعقيد التي تساهم على نحو أو آخر في عملية التبييض وتيسر لها[2]. ومنها وسائل الدفع الإلكتروني لما تمتاز به من تطور كل يوم وتعمد المشرع التوسع في نطاق الجريمة لأن أساليب الإخفاء

[1]- غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 184.

[2]- سليمان عبد المنعم، المرجع السابق، ص 19.

والتمويه متعددة ومتنوعة ومتطورة بتطور النشاط المصرفي، وتطور وسائل وأساليب الدفع الإلكتروني.

كما تمكن المبيضين من تهريب الأموال لأي دولة باستخدام البطاقة عوضا عن النقود الورقية، ومما يزيد من خطورة البطاقة الذكية في عمليات تبييض الأموال أن لها خاصية الاحتفاظ بملايين الدولارات مخزنة على القرص الخاص بها ثم يمكن بعد ذلك بسهولة نقل هذه الأموال إلكترونيا على البطاقة الذكية بواسطة التيليفون المعد لذلك بدون تدخل أي بنك من البنوك وبهذا تكون البطاقة الذكية بمنأى عن ملاحقة أو اشراف أي جهة[1]. حيث يمكن لمبيضي الأموال تحريك القيم النقدية المشحونة على البطاقات إلى أي مكان في العالم و بمنأى عن أي اشراف.

3-اكتساب أو حيازة أو استخدام الأموال المتحصلة عن الجريمة: تتعلق هذه الصورة بتجريم مجرد اكتساب أو حيازة الأموال مع ضرورة توافر علم مرتكب الفعل أن تلك الممتلكات أو الأموال المتحصلة من عائدات إجرامية.

ولكن أغفل المشرع الجزائري أن يتبع هذه الصور بعبارة أن تتم بوسائل إلكترونية لذا كان من الأفضل إدراج هذه العبارة خاصة وأن المشرع الجزائري أخذ بالمفهوم الموسع لمحل الجريمة ليشمل الأموال الالكترونية ولا ندري إن كان المشرع بأخذه بالمفهوم الموسع للمال ومنه الإلكتروني والرقمي استغني عن اتباع أساليب التبييض بعبارة تدل على الوسائل

[1]- صفوت عبد السلام عوض الله، المرجع السابق، ص1549.

الإلكترونية ومنها وسائل الدفع لذا يمكن القول أن قوانين جرائم تبييض الأموال التقليدية سنت وفقا لمعايير معينة لا تتناسب مع مقومات الجرائم الإلكترونية وطبيعتها مثل تبييض الأموال الإلكتروني لأن طرق اتيان السلوك المادي لتلك الجريمة يختلف عن ذلك الموجود في صورتها التقليدية لذا كان لزاما أن يتواكب القانون الجنائي ويتطور بشقيه الموضوعي والاجرائي لينسجم مع ثورة المعلومات بشتى أنواعها ومجابهة الجديد في عالم الاجرام[1].

4-تسهيل التبرير الكاذب لمصدر الأموال أو المداخيل حسب القانون الفرنسي: لم يورد المشرع الجزائري هذه الصورة (تسهيل التبرير الكاذب لمصدر الأموال أو المداخيل المتحصلة من جناية أو جنحة) ضمن صور تبييض الأموال في حين أن المشرع الفرنسي جعل هذه الصورة من أهم الصور التي تتحقق بها جريمة التبييض للأموال[2]، حيث تنص الفقرة الأولى من المادة الأولى من القانون الفرنسي رقم 392/96[3] المؤرخ في 13 ماي 1996 المعدلة للمادة 324 من قانون العقوبات الفرنسي.

« Le blanchiment est le fait de faciliter **par tout moyen**, la justification Mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré a celui-ci un profit direct ou indirect ».

---

[1]- سعود بن عبد العزيز المرشد، المرجع السابق، ص 235.

[2]- العيد سعدية، المرجع السابق، ص77.

[3]-Loi n°96-392 du 13 mai 1996 relative à la lutte contre le blanchiment et trafic des stupéfiants et à la coopération internationale en matière de saisie et de confiscation des produits du crime, JORF, 14 mai 1996.

فالمشرع الفرنسي لم يحدد الوسيلة التي يتم بها التبرير الكاذب لمثل هذا التصرف وإنما تركه مفتوح ليشمل كل الوسائل والتي من بينها وسائل الدفع الإلكتروني.

كما استعمل المشرع الفرنسي مصطلح التسهيل بأي وسيلة التبرير الكاذب لمصدر الأموال ونعتقد بأن هذه الصورة تشمل الاشتراك بالتسهيل لتبييض الأموال بوسائل الدفع الإلكتروني.

ثانيا/ وسائل الدفع الإلكتروني توسع محل جريمة تبييض الأموال

محل السلوك الاجرامي يتمثل في الأموال المتأتية من ارتكاب جريمة سواء تعلقت بحقيقتها أو مكانها أو طريقة التصرف فيها أو حركتها أو الحقوق المتعلقة بها أو ملكيتها وتشمل الأموال المنقولة و غير المنقولة، وهذا ما ذهب إليه المشرع الجزائري بتوسيعه لمحل السّلوك الإجرامي ليشمل كافة صور المتحصلات دون قصرها على الأموال النقدية فقط أو المنقولة. ويتجلى ذلك في اكتفائه بلفظ العائدات الإجرامية عند تحديده لمحل جريمة التبييض خلافا لبعض التشريعات[1]، وعرفت المادة 04 من القانون المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتها المعدل والمتمم[2] المال بأنه " أي نوع من **الأموال** المادية أو **غير المادية**، لاسيما المنقولة التي يحصل عليها بأي وسيلة كانت والوثائق والصكوك القانونية أيا كان شكلها **بما في ذلك الشكل الإلكتروني أو الرقمي** أو التي تدل على ملكية تلك الأموال أو أي مصلحة، بما في ذلك الائتمانات المصرفية، وشيكات السفر، والشيكات المصرفية

[1]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 185.

[2]- القانون رقم 01/05 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق ل 06 فيفري سنة 2005، المتعلق بالوقاية من تبييض الأموال و تمويل الارهاب ومكافحتهما المعدل والمتمم بالقانون رقم 06/15، ج ر عدد 11، سنة 2005.

والحوالات والأسهم والأوراق المالية والسندات والكمبيالات وخطابات الضمان " وبالتالي هذا يبين تبني المشرع الجزائري لفكرة **الأموال غير المادية** أيا كان شكلها بما في ذلك **الشكل الإلكتروني** ومنه تندرج وسائل الدفع الإلكترونية تحت هذا المفهوم، وترتيبا على ما سبق فإن النقود الإلكترونية والوسائط الإلكترونية المخزن عليها معلومات ذات قيمة مالية يجوز أن تكون محلا في جريمة تبييض الأموال طالما أن المعلومات ذات قيمة وهذه مسألة استقر عليها الفقه والقضاء سيما وأن جريمة تبييض الأموال ذاتها قد تتم في كافة أركانها عن طريق الوسائط المعلوماتية[1]، وهذا يعني أن المشرع أراد مواجهة –المتحصلات المباشرة وغير المباشرة – التي قد تستخدم كمحل في جريمة تبييض الأموال وتكون نتاجا من الجرائم الأصلية ونحن نؤيد هذا التوسع ليشمل الصور المستحدثة للجريمة.

إلا أن مؤيدي الخصوصية يرون أن منافع استخدام النقود الإلكترونية يفوق بكثير السلبيات والاستخدامات الاجرامية المحتملة ولذلك يجب مقاومة أية اجراءات تقيد استعمال النقود الإلكترونية وإنما ضرورة تمكين الهيئات المختصة من مراقبة السجلات وكل العمليات والمبادلات التي تتم باستخدام النقود الإلكترونية، كما أن عدم توفر الأنظمة التي تتمتع بالسرية سيزيد من حذر الأفراد ويؤخر انتقالهم بشكل كامل نحو أنظمة الدفع الإلكترونية والنقود الرقمية، والغموض الذي يشوب التشريعات والأنظمة الموضوعة لمكافحة تبييض الأموال يشكل تهديدا مستمرا يعيق الابتكار المالي خصوصا في مجال تطور النقود

[1]–عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، المرجع السابق، 167.

الإلكترونية من هنا فإن الغاء قوانين مكافحة تبييض الأموال من شأنه الاسراع في استخدام النقود الرقمية[1] كما أن الجهود المبذولة للحد من ظاهرة تبييض الأموال لم تثبت جدواها الاقتصادية[2].

الفرع الثالث

الركن المعنوي لتبييض الأموال إلكترونيا

يجب توافر القصد الجنائي[3] لدى الشريك إذا كان يعلم أن هذا الفعل يساهم في تسهيل ارتكاب الجريمة فإن قام المصرفي بقبول إيداع مجزأ في عدة حسابات وهمية على أساس أن أموال الإيداعات هي عائدات إجرامية وذلك من أجل إخفاء الأصل الحقيقي لتلك الأموال ثم قام بعد ذلك بتحويل تلك الأموال لحسابات أخرى في دولة معنية قامت مسؤولية المصرفي الجزائية عن تبييض الأموال على أساس قواعد الاشتراك في الجريمة وهو أمر في غاية الصعوبة من الناحية العملية، إذ لا بد أن يثبت ارتكاب جريمة معاصرة أو لاحقة لأفعال الاشتراك "**التبييض** " ولا بد من ثبوت علم مرتكب فعل الاشتراك ليس فقط بحقيقة أفعاله، وإنما أيضا بثبوت الجريمة الأصلية التي ساهم فيها[4].

---

[1]- توفيق شنبور، أدوات الدفع الإلكترونية (بطاقة الوفاء – النقود الإلكترونية)، بحث مقدم إلى أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، الجزء الأول الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، لبنان الطبعة الأولى 2007، ص 115،116.

[2]-مصطفي كمال طه، عمليات البنوك، المرجع السابق، ص 138.

[3]- يمكن استخلاص القصد الجنائي من العلاقات الوطيدة العائلية وعلاقات الأعمال القائمة بين من يقوم بالتبييض ومرتكب الجريمة الأصلية ولا يشترط أن يكون الجاني على دراية تامة بوصف الجريمة أو مرتكبها.

[4]- غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص186.

المشرع الجزائري اعتبرها جريمة قصدية لا يمكن ارتكابها بطريق الخطأ الذي لم يعتد به مطلقا كجوهر للركن المعنوي لكافة صور تبييض الأموال.

يمكن استخلاص عنصر العلم من الأموال الطائلة التي يعجز المتهم عن تحديد مصدرها ومن الكذب الذي يحيط بأقواله وما يقدمه من تفسيرات و أن تتجه إرادة الشريك إلى المساهمة في إحدى الصور المحددة للسلوك الإجرامي، و أن يريد تحقيق النتيجة الإجرامية المترتبة عليه.

إن استخلاص النية الجرمية أمر صعب في حالة الإيداع أو التحويل لا سيما وأن الدفع الإلكتروني يتم وفق آليات و أساليب ووسائل جد متطورة، ويستلزم استخدام هذه الطرق تواطؤ المصرفي والسماح بمعاملة وسائل الدفع الإلكتروني المستغلة في تبييض الأموال معاملة عادية فلا تتكشف الصفة الحقيقية للمبيضين.

ويكون في غاية الصعوبة إن لم يكن من المستحيل الكشف عن عملية تبييض الأموال التي تتم بواسطة التواطؤ المصرفي، بسبب عدم امكانية تمييز هذه الصفات عن التحويلات التي تجري عادة بين مصرف وآخر لأغراض مشروعة تماما[1].

أما **القصد الجنائي الخاص** الذي تطلبه المشرع الجزائري من خلال المادة 389 مكرر من قانون العقوبات الجزائري، لكن ليس في كل الصور إذ نص على ذلك في الفقرة الأولى بقوله : "يعتبر تبييضا للأموال تحويل الممتلكات أو نقلها مع علم الفاعل بأنّها عائدات إجرامية

[1]-نادر عبد العزيز شافي، المرجع السابق، ص 279.

بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته..."، فإذا قصد الشريك تقديم المساعدة للجاني إما بإخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات و إما مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته في هذه الحالة نقول بتوافر القصد الجنائي الخاص[1].

يتم التواطؤ المصرفي من خلال تحويل المبالغ المالية من مصرف لآخر لإخفاء عمليات التبييض للأموال ويستطيع المبيضون اجراء هذه العمليات بسهولة عن طريق استخدام المصرف لتحويل المبالغ الكترونيا بين حساباتهم وحسابات مراسليهم في مصارف أخرى للإيهام بان المؤسسات المالية تجري تصفيات بين الفروع والمقر الرئيسي[2].

يلاحظ أن المشرع الفرنسي في نص المادة 1/324 قد جرم جميع صور المساعدة في عمليات تبييض الأموال تفصيلا فذكر أنها قد تكون تسهيل في الإيداع أو في الإخفاء أو تحويل الأموال غير المشروعة تأكيدا منه على ملاحقة نشاط تبييض الأموال بكل صوره، والمساعدة في الإيداع يعني الإيداع لدى مؤسسات مالية أو مصرفية أيا كانت صورة الإيداع كالإيداع عن طريق وسائل الدفع الإلكتروني أو مساعدة في الإخفاء والوسيلة المفضلة للمبيضين هي النقود الالكترونية، كما شمل التجريم المساعدة في عمليات التحويل

[1]-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، المرجع السابق، ص 186.

[2]- نادر عبد العزيز شافي، المرجع السابق، ص 278.

الإلكتروني فمتى ثبت علم المصرفي بما ينصب عليه التحويل فهي مسؤولية جنائية عن اشتراك في جريمة تبييض الأموال.

المبحث الثاني

الاشتراك في التهرب الضريبي الإلكتروني

تعتبر اشكالية التهرب الضريبي من المشاكل الناتجة عن استعمال وسائل الدفع الإلكتروني ومن بين الاشكالات التي تطرحها التجارة الإلكترونية بحدة إشكال تحصيل الضرائب على معاملات التجارة الإلكترونية في سوق افتراضي وعالمي لا يعترف بالحدود التي تفصل بلدان العالم حيث أدى الاستخدام التجاري للشبكات إلى خلق مشاكل جديدة للإدارة والأنظمة الضريبية فوسائل الاتصال الحديثة قلبت القواعد الناظمة للجباية رأسا على عقب فيما يخص مجال تحديد الوعاء الضريبي، وكذا صعوبة تعيين المكلفين بالضريبة والتعرف على مختلف التعاملات التجارية الناشئة في عالم التجارة الإلكترونية[1] كما أن طبيعة العمليات المصرفية الإلكترونية تطرح اشكالية تحديد النظام الضريبي الواجب التطبيق على تلك الأنشطة بسبب عدم امكانية تحديد مكان اجراء تلك العمليات ليتم على أساسه تحديد القانون الواجب التطبيق على هذه العمليات[2]، وانقسمت الدول بين مؤيد ومعارض لفكرة فرض الضريبة على التجارة

[1]- فارس فضيل، حمزة صويفي، مداخلة بعنوان الابعاد القانونية والضريبية للتجارة الالكترونية في ظل وسائل الدفع المعتمدة ،الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الالكترونية في الجزائر ، عرض تجارب دولية، المنعقد بالمركز الجامعي خميس مليانة يومي 26-27 أفريل 2011.

[2]- نادر عبد العزيز شافي، المرجع السابق، ص 151.

الإلكترونية، وعليه سنتناول إشكالية التهرب الضريبي الإلكتروني باستعمال وسائل الدفع الإلكتروني (المطلب الأول)، وفي المطلب الثاني (الحلول المقترحة للتهرب الضريبي الإلكتروني).

المطلب الأول

اشكالية التهرب الضريبي الإلكتروني

باستعمال وسائل الدفع الإلكتروني

يظهر جليا أن مختلف وسائل الدفع الإلكتروني تضمن ميزة الخصوصية وعدم التسمية للتحويلات المالية إن لهذه الميزة خطر عند استعمالها من طرف المنظمات غير الشرعية في الغش كتبييض الأموال و التهرب الضريبي[1].

خلق النقود الإلكترونية يمكن أن يؤثر في السياسة المالية للدولة من خلال تأثيرها على حجم الايرادات الضريبية المتوقعة ففي ظل غياب نظام قانوني دقيق ومحكم فإنه سيكون من الصعب على السلطات المالية المتخصصة أن تراقب الصفقات وكذلك المداخيل التي يتم دفعها من خلال النقود الإلكترونية ومن ثم فإن من شأن ذلك أن يفتح الباب أمام التهرب الضريبي وكذلك أمام تعميق ظاهرة الاقتصاد السري[2]، فالجباية الإلكترونية تعنى بفرض الضرائب على التعاملات التي تتم على شبكة الأنترنت[3] وبصدور قانون التجارة الإلكترونية

[1]- pierre Bresse, guillaume Beaure D'Augères et Stéphanie Thuillier, op, cit, p149.

[2]- محمد ابراهيم محمود الشافعي، المرجع السابق، ص 130.

[3]- حوالف عبد الصمد، المرجع السابق، ص 360.

ستواجه الجزائر مشكل التهرب الضريبي وبالتالي حرمان الخزينة العمومية من الإيرادات الضريبية الناتجة عن التجارة الإلكترونية والدفع الإلكتروني، لهذا نتطرق إلى مناقشة اشكالية وسائل الدفع الإلكتروني وتسهيل التهرب الضريبي (الفرع الأول)، كما تسهل وسائل الدفع الإلكتروني إخفاء التهرب الضريبي وحجمه (الفرع الثاني).

الفرع الأول

وسائل الدفع الإلكتروني تسهل التهرب الضريبي

بعد ظهور التجارة الإلكترونية كان لابد من ايجاد صورة تتوافق وخصائص التجارة الإلكترونية يتم فيها تسديد المستحقات المالية ظهرت وسائل الدفع الإلكتروني وهذه الوسائل يطلق عليها البعض مصطلح النقود الإلكترونية وتمثل هذه الوسائل مشكلة حقيقية باعتبارها تؤدي إلى حدوث التهرب الضريبي، خاصة وأنه يسهل اخفاء الصفقات التي تتم عبر شبكة الانترنت والمستخدم فيها وسائل الدفع الإلكترونية[1].

وبالتالي فرض هذا النوع من الضرائب يتطلب أنظمة ضريبية جديدة تختلف عن الأنظمة الضريبية التقليدية لتلائم النشاط التجاري الإلكتروني، وكذا المكلفين الجدد بالضريبة وكيفية تأديتها ومراقبتها في حين هناك دول أخرى ومنظمات (كالولايات المتحدة الأمريكية والمنظمة العالمية للتجارة) تنادي بترك التجارة الإلكترونية دون ضرائب وجعلها منطقة حرة لتشجيع هذا النوع من النشاط التجاري رغم ما يخلفه من فكرة عدم المساواة بين المكلفين

[1]-قيس حسن عواد، مقال بعنوان مشكلات فرض وتحصيل الضرائب في عقود التجارة الالكترونية، مجلة الرافدين للحقوق، المجلد 12، العدد43، سنة 2010.

بالضريبة على أرض الواقع والمعفيين منها إذا ما مارسوا نفس النشاط إلكترونيا، فالبنك عندما يعقد صفقة ما ويتم الدفع عن طريق التحويل المصرفي(التحويل المصرفي التقليدي) فإنه تفرض على العملية ضريبة، في حين أنه بالنسبة للصفقة ذاتها إذا تم الدفع عن طريق التحويل الإلكتروني للأموال فإنها تكون معفاة من الرسم والضريبة وهذا يخلق نوع من التمييز وتبقى إشكالية تحصيل الرسوم والضرائب في المجال الإلكتروني ذات أهمية خاصة بالنسبة للدول النامية إذ قد تؤدي لحرمانها من أهم مصادر الايرادات، وهذا يقتضي وضع قواعد تضمن حقوق هذه الدول بدون أن تؤدي للحرمان من مزايا التجارة الإلكترونية[1] ولا شك أن فرض الضريبة في كل الأحوال على نشاط التجارة الإلكترونية يتطلب تعاونا من طرفي العلاقة التعاقدية في هذه التجارة وعدم اخفاء تعاملاتها وإلا كانت هناك مشكلة قانونية فيما يتعلق بتحديد النشاط التجاري أو الوعاء الضريبي الخاضع لهذه الضريبة[2].

الاصرار على السرية المطلقة من طرف مصدري النقود الإلكترونية والمتعاملون فيها على أن تظل النظم المطبقة خالية من أية بيانات تسمح بتتبع مصادر الأموال وهو الأمر الذي يساهم في تسهيل عمليات التهرب الضريبي[3].

[1]- حسين شحادة الحسين، المرجع السابق، ص 210.

[2]-عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني الحماية الجنائية لنظام التجارة الإلكترونية، المرجع السابق، ص327.

[3]- نبيل صلاح محمود العربي، المرجع السابق، ص 37.

كما يتعهد مصدرو النقود الإلكترونية والمتعاملون فيها على أن تظل النظم المطبقة خالية من أية بيانات تسمح بتتبع مصادر الأموال وهو الأمر الذي يساهم في تسهيل عمليات التهرب الضريبي[1].

الملاحظ أن دفع ثمن الصفقة عن طريق النقود الإلكترونية يتم بطريقة غير محسوسة تحول دون تقدير نسبة الضريبة التي ينبغي دفعها، فالنقود الإلكترونية لا تحتاج إلى وسيط كبنك أو مؤسسة مالية مما يصعب معه التعرف على أساس المحاسبة الضريبية، وبالتالي فالنقود الإلكترونية هي وسيلة دفع لصفقة لا يعرف قيمتها سوى طرفيها أي البائع والمشتري وتظل هذه القيمة مجهولة بالنسبة لمصلحة الضرائب ما لم يتقدم أحد هذين الطرفين طواعية بإقرار إلى مصلحة الضرائب يبين فيه حجم مبيعاته أو مشترياته حتى يتم فرض الضريبة عليه[2]، علاوة على ذلك فإن جزءا من الدفع الإلكتروني المستخدم في السوق ولا ينطوي على أية معلومات عن مستخدميه[3].

وبهدف التصدي لأخطار هذه الوسائل أو الانقاص منها على الأقل اتخذت العديد من الدول اجراءات منها إلزام المؤسسات بإعداد تقارير للسلطات المختصة حول بعض العمليات المالية ففي الولايات المتحدة الامريكية مثلا التحويلات الإلكترونية التي تفوق 10000 دولار

[1]- ضياء نعمان، المرجع السابق، ص209.

[2]- ضياء نعمان، المرجع السابق، ص243.

[3]- حوالف عبد الصمد، المرجع السابق، ص 372.

تلزم المؤسسات بإعداد تقرير حولها كما تلزم بالاحتفاظ بنسخة إضافية للتحويلات التي تفوق قيمتها 100000 دولار[1].

الفرع الثاني

وسائل الدفع الإلكتروني تسهل اخفاء أثر التهرب الضريبي وحجمه

عادة لا تخلف المعاملات التجارية في عالم التجارة الإلكترونية والناشئة عبر الانترنت أي دليل مادي يثبتها، مما يسمح للأشخاص وباستخدام لتكنولوجيا الانترنت من تحقيق معاملات وصفقات تجارية بعيدا عن سلطة وعين الادارة الضريبية لأن عملية تسليم السلع لا تخضع لمراقبة جمركية وبتطور وسائل الدفع الإلكتروني فإن السلطات لا تملك الوسائل التي تمكنها من تتبع أثاره مما أدى إلى انقاص موارد خزائن الدول فيما يخص محاصيلها الجبائية ويزيد من استفحال ظاهرة التهرب الضريبي، لأن هناك صعوبة في تحديد حجم نشاط التجارة الإلكترونية الخاضع للضريبة لأن الممول لا يعطي إدارة الضرائب التشفير الخاصة بحجم تعاملاته على شبكة الانترنت لأنها من أسراره الخاصة، فضلا عن أن الجهات القائمة عليها لا تمتلك حل الشفرة في غير الأحوال المقررة قانونا وإلا عوقبت جنائيا ولهذا تبدو الصعوبة في وجود مشكلات قانونية واجرائية في مجال إثبات الوعاء الخاضع للضريبة في حالة نشوب نزاع قضائي بين الممول ومصلحة الضرائب الأمر الذي يقتضي تعديل القوانين

[1]- pierre Bresse, guillaume Beaure D'Augères et Stéphanie Thuillier, op, cit, p150.

المتعلقة بالتشريعات الضريبية أيا كان نوع الضريبة وكذلك تشريعات الجمارك حتى يمكن اخضاع نشاط هذه التجارة للضريبة[1].

ومن المستحيل على الأجهزة الضريبية اقتفاء أثر المنتجات الرقمية، وغالبا لا يدفع المشترون عبر الانترنت أية ضرائب، بل إنهم يحجمون – كما أسلفنا – عن الشراء في حال الزامهم بدفع ضرائب.

تزيد الانترنت حركة الشركات وتنقلها مع أنواع معينة من الأيدي الماهرة فالأعمال أو الأفراد العاملون على الشبكة يستطيعون الانتقال إلى البلدان المنخفضة الضرائب، كما أنها ستزيد من صعوبة تحديد هوية الأفراد أو الشركات العاملة في الأنشطة القابلة لفرض ضرائب عليه. تزيد الانترنت من الصعوبات التي تواجهها الأجهزة الضريبية وذلك عن طريق تعطيل قدرة التجار والمصرفيين وغيرهم من الوسطاء الذين يلعبون اليوم دورا هاما في جباية الضرائب أو في توفير معلومات التجارة الإلكترونية.

المطلب الثاني

الحلول المقترحة للتهرب الضريبي الإلكتروني

لكي يتم تجنب حالات التهرب الضريبي نتيجة استخدام النقود الإلكترونية كوسيلة للأداء فإنه يمكن لمصلحة الضرائب إيجاد منفذ إلى البيانات المخزنة على ذاكرة الحاسب الشخصي للممولين حتى يسهل معرفة حجم الصفقات التي تمت بين الأفراد رغم أن هذا الحل يعد

[1]-فارس فضيل، حمزة صويفي، المرجع السابق

انتهاكا للحرية الشخصية للمواطنين التي يكفلها الدستور على الرغم من الدوافع القوية التي سوف تسوقها الحكومة من أجل هذا التدخل مثل محاربة غسيل الأموال والتهرب الضريبي[1].

وظهرت العديد من الأفكار تتضمن تأسيس الضريبة منها :

أولا/ فرض الضريبة عن طريق مزودي خدمة الأنترنت

مضمون هذه الفكرة هو أن يقوم مزودي خدمة الأنترنت بإعداد محاسبة لزبائنهم تشمل المعاملات التي قاموا بها عبر الانترنت، إذ يتم فرض ضريبة على قيمة الصفقات المبرمة، ثم يقوم مزودي خدمة الأنترنت بدفعها لخزينة الدولة على غرار ما يتم بالنسبة للضريبة على القيمة المضافة، وهذا معناه أن يؤدي مزودي خدمة الأنترنت دور المكلف القانوني في نظر ادارة الضرائب، وبالتالي بالنسبة لوسائل الدفع الإلكتروني فإن تشغيلها والتعامل بها يتم عبر شبكة الانترنت يوجب على المصارف القيام بتبليغ زبائنها بحجم تعاملاتهم ومقدار الضريبة المفروض عليهم.

اشراك مزودي خدمات الأنترنت القادرين من الناحية الفنية على تتبع جميع تعاملات الانترنت لزبائنهم كطرف ثالث موثوق به للقيام بعملية فرض وتحصيل وتحويل ضريبة المبيعات المقررة على السلع والخدمات الرقمية وكنقطة بداية فلا بد من أن يسجل مزودو خدمة الأنترنت في دار المقاصة التي تتولى بدورها تحويل العائدات الضريبية للجهات ذات الأحقية[2].

[1]- ضياء نعمان، المرجع السابق، ص243.

[2]- حوالف عبد الصمد، المرجع السابق، ص 366.

من الانتقادات التي وجهت لهذه النوعية من الضرائب هي الطرق التي تستعمل لتتبع المعاملات الإلكترونية للزبائن التي تتنافى مع القوانين التي تضمن سرية المعاملات وخاصة التنافي مع السرية المصرفية بالإضافة إلى أن فرض هذه الضريبة سيؤدي إلى زيادة الأعباء الجبائية التي يتحملها الزبائن في البنوك[1].

وقد اقترح لمعالجة عملية تتبع التعاملات عبر الحدود استخدام عناوين بروتكول الانترنت والتي تستخدم في نقل البيانات من نقطة إلى أخرى، حيث تعتبر هذه العناوين جزءا أساسيا لكل نقطة وصول للأنترنت غير أنه يلاحظ حاليا أن العديد من عناوين بروتكول الانترنت تعين بصورة عشوائية مما يجعل من الصعب تتبع واقتفاء التعاملات التجارية للمستخدمين الأفراد، علاوة على ذلك فانه يمكن لعناوين بروتكول الانترنت أن تعالج لتخفي هوية المستخدم وموقع المستخدم[2].

ثانيا/ فرض رسم على وحدات التعداد الإلكتروني (TAXE SUR LES BITS)

في محاولة لوقف الخسائر عن تآكل وعاء الضريبة بسبب التحول إلى التجارة الإلكترونية، التي يتعذر متابعتها ضريبيا في ظل القوانين الحالية ظهرت فكرة ضريبة الوحدات الرقمية لأول مرة سنة 1994من خلال التقرير الذي قدمه الباحثان (THOMAS ARTHUR CORDEL, IDE) أمام نادي روما تحت عنوان "بناء المجتمع الأوروبي

[1]–حراق صباح، مداخلة بعنوان المعالجة الجبائية للتجارة الإلكترونية، الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الإلكترونية في الجزائر، عرض تجارب دولية، المنعقد بالمركز الجامعي خميس مليانة يومي 26-27 أفريل 2011.

[2]– حوالف عبد الصمد، المرجع السابق، ص 366، 367.

وضمان الاعلام للجميع"، يرى أصحاب هذا الاقتراح أنه من الضروري أن تعلم الدول أن مفهوما جديدا لثورة الأمم يأخذ في التبلور حاليا، يختلف عن المفهوم الذي ساقه آدم سميث إذ تتمثل هذه الثروة الجديدة في تريليونات الوحدات الرقمية من المعلومات التي تتداول عبر وسائل الاتصالات المتطورة والتي تشكل صورة جديدة من صور الإنتاج، التوزيع والاستهلاك في عصر الانترنت.

ضريبة البيتس (bits) تتمثل في فرض الضريبة على أساس الوحدات الرقمية المتعلقة بالاتصالات خلال الشبكة باعتبارها العنصر الوحيد الذي يمكن تتبعه وقياسه وتحديد الضريبة على أساسه وقد أيدت اللجنة الأوربية عام 1998 فرض هذه الضريبة مع تطبيق تسعيرات مختلفة بحسب مدى الاتصال ونوع الخط المستخدم[1]، ويعرف هذا النوع من الضرائب بأنه ضريبة تفرض على الانتقال الإلكتروني للمعلومات (انتقال رقمي) وهو لا يستهدف منتوجا محددا بل وحدة التعداد الإلكتروني وذلك مهما كانت الوسيلة المستخدمة لنقل هذه الوحدة التي تعبر عن التبادلات المحققة أو الصفقات الدولية المبرمة مثل المحاضرات عن بعد (Téléconférence)، البريد الإلكتروني، (E .mail) تحويل الملفات المقامة بين البنوك إلى غير ذلك من التبادلات التي أصبحت تنجز عبر شبكات الاتصال الإلكترونية[2].

[1]- حابت أمال، التجارة الإلكترونية في الجزائر، رسالة لنيل شهادة الدكتوراه في العلوم ، تخصص قانون، جامعة مولود معمري، تيزي وزو، تاريخ المناقشة 30 سبتمبر 2015، ص245.

[2]- حراق صباح، مداخلة بعنوان المعالجة الجبائية للتجارة الإلكترونية، المرجع السابق .

أساس هذا الرسم يتم تحديده من خلال عدد وحدات التعداد الإلكتروني وليس على أساس تكلفة وقيمة الاتصال في حد ذاته، التي هي متغير تابع للمسافة والزمن واقترح معدل هذا الرسم قدره (1% واحد في المئة ميقا بيت) أي من وحدة التعداد (bit). ويمكن أن يستعان في هذا العد بآلة قياس (عداد) كالتي تستعمل في قياس استهلاك الكهرباء مما يمكن المستهلكين والحكومة من التعرف على مقدار الوحدات التي نقلت[1].

من الانتقادات التي وجهت لهذا النوع من الضرائب أنها تفرض على كافة الاتصالات دون تمييز بين نوع الاتصال أو الغرض منه تجاريا أو غير تجاري.

يؤدي فرضها إلى ازدواج ضريبي، ضريبة تقليدية عند اقتناء التجهيزات وضريبة أخرى لدى استعماله كما سيؤدي تطبيق مثل هذه الضريبة إلى معاملة تميزية لغير صالح التجارة الإلكترونية عبر الأنترنت، فنقل البيانات عبر الهاتف أو الفاكس لا يخضع لها[2]

ثالثا/ تحصيل الضريبة عن طريق الوسطاء الماليين[3]

يمكن احتساب الضريبة واقتطاعها على المنتوجات والسلع الرقمية من خلال مؤسسات مالية موثوقة كشركات وسائل الدفع الإلكتروني، وذلك عند البيع وحسب نسبة الضريبة في بلد المشتري أو البائع ولاشك أن مثل هذا الاقتراح سيتطلب من تلك المؤسسات المالية الاحتفاظ بقاعدة بيانات للدول المختلفة، اضافة إلى تقديم الباعة المعلومات الضرورية حول مبيعاتهم

---

[1]- حراق صباح، مداخلة بعنوان المعالجة الجبائية للتجارة الإلكترونية، المرجع السابق.

[2]- حابت أمال، المرجع السابق، ص 246.

[3]- حوالف عبد الصمد، المرجع السابق، ص365، 366.

والأطراف المعنية بعملية البيع، كأرقام حسابات البائع والمشتري وقيمة المبيعات وقيمة الضريبة وعنوان المشتري وفي سبيل تحويل عوائد الضريبية الى النطاق الاستهلاكي فقد اقترح استخدام تلك المؤسسات المالية لدور مقاصة لهذا الغرض، وان كان انشاؤها بين الدول المستقلة سيواجه صعوبات سياسية جمة.

ولعل اقتراح استخدام شركات الدفع، سيصطدم بالتكلفة التي تتحملها البنوك لإنشاء النظام المناسب وانجاحه، اضافة إلى عدم جاهزية البنوك الآن من الناحية الفنية للتعامل مع هذا الكم الهائل من المعلومات مما قد يفتح المجال أمام البنوك في حالة القاء المهمة عليها لتقرير حقها في اقتضاء الرسوم على تقديم خدمات التحصيل ويلاحظ وان كان الدفع بواسطة بطاقات الدفع، هو الوسيلة المتبعة حاليا في مجال التجارة الإلكترونية إلا أن الأمر لم يدم طويلا في ظل انتشار النقود الإلكترونية مما زاد من صعوبة تتبع حسابات المكلفين بالضريبة والحجز عليها.

هل سيشكل مشكل فرض الضريبة في مجال التجارة الإلكترونية عقبة أمام انتشار استخدام وسائل الدفع الإلكتروني لعدم وضوح معايير حسابها وآليات فرضها؟ فرض الضرائب على هذا النمط الجديد يتطلب استراتيجيات ضريبية مختلفة في المتابعة والكشف والجمع والأهم تعاونا وتنسيقا اقليميا ودوليا، والزام البنوك والمؤسسات المالية بضرورة اخطار مصالح الضرائب بالتحويلات المالية التي تتم عن طريقها بوسائل الدفع الإلكتروني بين المشروعات سواء كان أطراف هذه التحويلات مقيمين داخل الدولة أو خارجها وهل سيؤثر على مبدأ

السرية المصرفية، والى حين تقرير نظام قانوني لفرض الضريبة على التجارة الإلكترونية في الجزائر سيمكننا تقرير حالات المسؤولية الجزائية للتهرب الضريبي الإلكتروني والذي دون شك ستساهم فيه وسائل الدفع الإلكتروني، ورغم أهمية هذا الإشكال إلا أن النصوص التشريعية لم تعالجه بعد.

UNIVERSITE SETIF2

خاتمـــــة

هذه الدراسة تعالج المخاطر المحتملة للجرائم الإلكترونية المرتبطة بوسائل الدفع الإلكتروني خصوصا وتأتي لتعزيز النظام المصرفي على مواجهة الجريمة الإلكترونية عموما، ويبقى الخوض في موضوع كهذا نوع من المجازفة لأن الأمر يتعدى المجال التقليدي للمسؤولية الجزائية الذي يمكن محاصرته بجميع جوانبه إلا أن أهمية هذه المبادرة في أنها ستخدم قطاعا عريضا من رجال القضاء والقانون وكذا العاملين بالمصارف وهذا لأننا غالبا ما نشعر بنوع من النقص أمام المستجدات العلمية.

إصلاح الجانب الجنائي لوسائل الدفع الإلكتروني يعتبر مطلبا مهما في عصرنة نظام الدفع الإلكتروني وبالنتيجة عصرنة القطاع المصرفي والاقتصادي ككل، لأنه يندرج ضن الاصلاحات العميقة التي على المشرع الجزائري القيام بها وذلك بإدخال جرائم جديدة ومعالجة فراغات تشريعية مازالت مطروحة على مستوى تشريعاتنا، وضرورة مراجعة النصوص التقليدية بمراعاة النزعة اللامادية لجرائم الأموال التقليدية ووسائله اللامادية في إطار عالم كله افتراضي وإن كنا نقر بعدم امكانية تطوير القانون الجنائي بنفس سرعة تطور الأساليب الاجرامية، إلا أن المهم بالنسبة لوسائل الدفع الإلكتروني أن نؤسس بصفة قوية وليس المهم الاسراع لتقليص المدة الزمنة التي ستنجز فيها الإصلاحات لأنها ستمس الجانب الإلكتروني للعمل المصرفي، وبالنظر للدور الذي تلعبه المصارف كمحرك للاقتصاد ستمس الاقتصاد الرقمي ككل.

حجم الجريمة المعلوماتية في الجزائر مقارنة مع المستوى الدولي منخفض لأنها غالبا ما ترتبط بسرقة بطاقات الائتمان وإن كانت هذه الجرائم ليست منتشرة بالحجم والوتيرة التي عرفتها باقي الدول، ومازال المسار في طور الانجاز يجب أن نبذل جهودا لتقييم الوضع وتوظيف الخبرة وتوجيه الجهود إلى تأمين وسائل الدفع الإلكترونية.

التشريعات في الجزائر تخلفت مقارنة مع التطور التكنولوجي السريع فتعديل قانون العقوبات سنة 2004 وبالرغم من ادراج كتاب خاص بموجب القانون 04 /15 المعدل والمتمم لقانون العقوبات والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية بعنوان المساس بأنظمة المعالجة الآلية للمعلومات بمرجعية فرنسية حرفية من خلال قانون GODFRAIN لسنة 1988 المدرجة في قانون العقوبات لسنة 1994، ولعل المشرع الجزائري لم يتعامل بفطنة مع هذا السلوك الإجرامي وإنما كان عليه أن تكون نظرته أكثر عالمية وشمولية في الطرح ولا يبقى تابعا للمشرع الفرنسي الذي هو في ذاته يحتاج إلى تنقيح مقارنة مع التشريعات المقارنة الأخرى وأنه كان يجب أن تكون من ضمن مصادره كتابات الفقه والاجتهادات القضائية في هذا الصدد.

على المشرع ألا يكتفي بتجريم المساس بأنظمة المعالجة الآلية للمعطيات بل يجب التطرق إلى مجمل الجرائم التي لا يقتصر مصرحها على الحاسوب بل يتعدها إلى الانترنت، الهواتف النقالة، وسائل الدفع الإلكترونية.

لقد أصبحت تنمية البنية التحتية والاطار القانوني لوسائل الدفع الإلكترونية ضرورة حتمية لمسايرة التطور التكنولوجي وتجهيز وتحول القطاع المصرفي الجزائري بمنظومة دفع عصرية ويمكننا مرافقة تطور وسائل الدفع الإلكترونية عن طريق معالجة سريعة ومؤمنة لهذه الوسائل بوضع الهياكل القاعدية ما بين المصارف والوسائل التقنية لمعالجتها ومواكبة الإطار القانوني والتنظيمي لوسائل الدفع الإلكترونية من خلال ترتيب المسؤولية المدنية و الجزائية عند التعامل بها، وعلى المشرع الجزائري استكمال وضع الإطار القانوني اللازم لضمان حقوق المتعاملين بوسائل الدفع الإلكتروني، واعتماد تنظيم قانوني للنقود الإلكترونية التي ستداهمنا لامحالة، ينظم التعامل بها ويجرم سرقتها وتزويرها، تحديد حد اقصى لقيمة النقود الإلكترونية حيث لا تزيد عن حد معين في كل صفقة.

إننا نحبذ ما انتهجه المشرع الجزائري من عدم ادراج مواد تعاقب على استعمال البطاقات أو وسائل الدفع الإلكتروني في القانون التجاري لأننا سنصطدم بمبادئ القانون الجنائي (مبدأ الشرعية ومبدأ حضر القياس في المادة الجزائية).

المشرع الفرنسي تفاديا لهذه الإشكالات قام بإلغاء القانون المتعلق بالبطاقات واستعمل مصطلح وسائل الدفع الإلكتروني في القانون المتعلق بالنقد والمال وعدل المواد المتعلقة بالعقاب على الجرائم المتعلقة بها ضمن هذا القانون.

أما بالنسبة للبطاقات فإن أغلبية القوانين تركت الأمر للاتفاقات بين البنوك وزبائنها إلا أن الإشكالية تبقى مطروحة بالنسبة للمسؤولية الجزائية عن استعمال هذه الوسائل في التشريع

الجزائري مما يحتم علينا ضرورة تعديل قانون النقد والقرض خاصة في الجانب الجزائي المرتبط بهذه الوسائل، وتعديل قانون العقوبات باستكمال الفراغات التي تخص باقي الجرائم الإلكترونية.

يبقى أن نذكر أن النصوص الجزائية المبتغاة لحماية وسائل الدفع الإلكتروني في القانون الجزائري هي الهدف المنشود الذي تقصده هذه الدراسة لعلاج القصور التشريعي الحالي في هذا الصدد.

ومن الأفضل أن يتناول المشرع الجزائري المشكلة بالفحص والدراسة والتمحيص من أجل سن نصوص خاصة بوسائل الدفع الإلكتروني تتناول كل الجوانب الخاصة بالدفع الإلكتروني تجنبا لأي خلل، أو تعديل قانون النقد والقرض بتجريم الأفعال المتصور أن تصيب وسائل الدفع الإلكتروني، لأنه يجب على التشريع العقابي أن يواكب دائما الثورة التكنولوجيا المصرفية وأن يضمن درجة عالية من الحماية القانونية ضد الجريمة المعلوماتية لأن غياب العقوبات الجزائية في ميدان الدفع الإلكتروني سيحفز المجرمين على تطوير قدراتهم وبالنتيجة سيساهم في زيادة هذا النوع من الجرائم الإلكترونية.

تعديل قانون النقد والقرض بالنص على الجرائم المرتبطة باستعمال وسائل الدفع الإلكتروني .

ضرورة النظر إلى الجرائم المرتبطة باستعمال وسائل الدفع الإلكتروني كجرائم مستقلة من حيث المبنى وطبيعة السلوك عن جرائم الأموال التقليدية وليس فقط من ناحية محل الجريمة.

ضرورة العقاب الجزائي للحامل على كل استخدام لوسيلة الدفع الإلكتروني مع علمه بعدم وجود الرصيد أو بعد انتهاء صلاحياتها أو إلغائها.

توسيع دائرة الأشخاص الملزمين بالسر المصرفي من مقدمي الخدمات الإلكترونية ومصممي المواقع الإلكترونية للبنوك العاملة عر الأنترنت.

ضرورة النص على توسيع نطاق الاشتراك بالاتفاق ليشمل الجرائم المتعلقة باستعمال وسائل الدفع الإلكتروني أو النص على اعتبار العصبة المنظمة ظرف مشدد في هذه الجرائم.

تجريم الاحتيال المعلوماتي كجريمة مستقلة بالنظر إلى الغرض منها.

وضع مواد خاصة في قانون النقد والقرض بالجرائم المتعلقة بتزوير وتقليد وتزييف وسائل الدفع الإلكتروني، استعمال وسائل دفع إلكتروني مزورة، اصطناع ، توفير، حيازة، والوضع تحت التصرف لأجهزة وبرامج معلوماتية أو معطيات مساعدة على التزوير والتقليد، وعدم الاكتفاء بتعديل المواد المتعلقة بالتزوير فقط في قانون العقوبات.

التناول بالتجريم لجرائم الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني، واستحداث نص خاص لتجريم انتحال الهوية الرقمية، وكذا استعمال الشبكة المعلوماتية والوسائل التقنية للوصول إلى أرقام وبيانات وسائل الدفع الإلكتروني.

اعادة الصياغة لنص المادة 389 مكرر من قانون العقوبات الجزائري لتشمل التبييض باستخدام الشبكة المعلوماتية ووسائل تقنية المعلومات، النص على إنشاء موقع لنشر أساليب التبييض للأموال باعتبارها صورة جديدة للتبييض.

تجريم التهرب الضريبي إلكترونيا والذي تساهم في تفاقمه استعمال وسائل الدفع الإلكتروني .

ضرورة إيلاء الدولة أهمية خاصة لتطوير البنية التحتية للاتصالات والاهتمام بالحماية التقنية لوسائل الدفع الإلكتروني وتطويرها من قبل المصارف باعتباره خطر جديد عليها مواجهته.

تدريب العاملين في المصارف على التعامل بوسائل الدفع الإلكتروني والتجار المعتمدين لها وكذا التعامل مع النقود الإلكترونية واكتشاف حالات الاستعمال غير المشروع.

توفير الوسائل التي تمكن من اكتشاف التزوير الخاص بوسائل الدفع الإلكتروني الجديدة.

التزام البنوك بتقديم تقارير دورية لبنك الجزائر وهيئة الاستعلام المالي.

إن نضج الوعي لدى الزبائن بالنسبة للعمل المصرفي الإلكتروني وبالنسبة لاستعمال وسائل الدفع الإلكتروني يحتاج إلى وقت ليس بالقصير، ويعتقد على المديين القريب والمتوسط فإن العمل المصرفي الإلكتروني سيكون مقتصرا على المصارف الكبرى والطبقة الثرية من الزبائن والتي لديها معارف معلوماتية بمعنى أن يصبح لدى المصارف نوعين من الزبائن زبائن المصرف الفوري وزبائن المصرف التقليدي ، وهذا من الأمور التي يجب التنبه لها عند اطلاق وسائل الدفع الإلكترونية وعلى المدى الطويل وبنمو الثقافة المعلوماتية سيعي الزبائن أهمية التحول إلى الخدمة الإلكترونية نظرا للفوائد الجمة المتمثلة في الاتصال المباشر بالمصرف وتوفير الوقت والمال.

وعلى المصارف أن تدرك أهمية الاستثمار في الأنظمة المعلوماتية واعتماد التقنيات الحديثة في مجال الاتصالات وتطوير الرقابة الداخلية والخارجية وتطوير وسائل الأمان والحماية

وتدريب الكوادر البشرية في مجال المعلوماتية، كما أن اعتماد التعامل بوسائل الدفع الإلكتروني سيساهم في بقاء السيولة في المصارف.

للمصارف الدور الهام في منع ارتكاب جرائم وسائل الدفع الإلكتروني بشتى أنواعها فيجب عليها الحد من الثغرات التي يمكن من خلالها ارتكابها من خلال عدة وسائل منها:

1-الاستعلام الجيد والدراسة المتأنية للزبائن من طالبي الحصول على وسائل الدفع الإلكتروني والتأكد من صحة وسلامة المستندات المقدمة.

2- حسن اختيار العاملين فيها ومراقبتهم بصورة دورية وتدريبهم بصورة جيدة لكيفية التعامل مع هذه الوسائل.

3- متابعة التطورات التقنية التي تحصل في حقل اصدار وسائل الدفع الإلكتروني ووسائل تأمينها.

4- مراقبة التجار المتعاقدين مع المصارف من خلال فواتير البيع والشراء لذات المصارف لمنع أي تلاعب.

5- التنسيق مع الأجهزة الأمنية لرصد معدلات الجريمة والعمل على مواجهتها.

6- ايجاد نوع من المتابعة والتنسيق بين المصارف العاملة في هذا المجال لتبادل المعلومات الخاصة بالعملاء والتجار سيئ السمعة ليتم وضعهم في القائمة السوداء التي يتم ايقاف التعامل معهم على المستوى الدولي.

المطالبة بتكوين متخصص للقضاة في هذه الجرائم بخصوصياتها المتعلقة بالجانب المصرفي لفهم تقارير الخبراء الفنية والتقنية في هذا المجال وتكوين مصالح الشرطة القضائية باستقدام خبراء مختصين قانونيا وتقنيا لتكوين الشرطة القضائية، خاصة باعتماد قانون التجارة الإلكترونية الذي سيرسخ التعامل بالدفع الإلكتروني والذي بدوره سيساهم في بعث الاقتصاد الرقمي.

قائمـــــــــة

المراجـــــــع

أولا/المراجع باللغة العربية

أ- الكتب:

1-أحمد السيد لبيب ابراهيم، الدفع بالنقود الإلكترونية الماهية والتنظيم القانوني دراسة تحليلية ومقارنة، دار الجامعة الجديدة للنشر الاسكندرية، مصر، 2009.

2-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، 2005.

3-أحمد سفر، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، الطبعة الأولى.

4-أحمد شكري السباعي، الوسيط في الأوراق التجارية "دراسة معمقة في قانون التجارة المغربي الجديد وفي اتفاقية جنيف للقانون الموحد وفي القانون المقارن، الجزء الثاني "في اليات الوفاء "الشيك ووسائل الأداء الأخرى، الطبعة الثالثة، 2010.

5-أنور محمد صدقي المساعدة، المسؤولية الجزائية عن الجرائم الاقتصادية، دراسة تحليلية تأصيلية مقارنة في التشريعات، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2009.

السيد عبد الحميد أحمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية والدولية، مكتبة الوفاء القانونية، مصر، الطبعة الأولى ،2018، ص66.

6-امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثانية، 2007.

7-ايهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، مصر، 2008.

8-بارش سليمان، مبدأ الشرعية في قانون العقوبات الجزائري، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2006 .

-بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2009.

-بوعناد فاطمة الزهراء، مكافحة الجريمة الإلكترو نية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول عام 2013.

9-جمال عبد المجيد التركي، المساهمة التبعية في قانون العقوبات (دراسة تأصيلية تحليلية مقارنة)، المكتب الجامعي الحديث، الطبعة الأولى، 2006.

10-جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول الجرائم الناشئة عن استخدام الحاسب الآلي، مكتبة دار النهضة العربية، مصر.

11-حسام الدين كامل الاهواني، حماية أنشطة البنوك من مخاطر استخدام الحاسبات الإلكترونية، الجوانب القانونية الناتجة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، الطبعة الثانية، بيروت، لبنان، 1999.

12-حسين محمد الشبلي، مهند فايز الدويكات، التزوير والاحتيال بالبطاقات الائتمانية، سلسلة الجرائم المالية والمستحدثة، دار مجدلاوي للنشر والتوزيع، الطبعة الأولى، الاردن، 2009.

13-حسين محمد الغول، جرائم شبكة الأنترنت والمسؤولية الجزائية الناشئة عنها، دراسة مقارنة، مكتبة بدران الحقوقية، الطبعة الأولى، لبنان، 2017.

14-خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008.

15-خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر اساليب وثغرات، دار الهدى، الجزائر، طبعة 2010.

16-خنفوسي عبد العزيز، قانون الدفع الإلكتروني، مركز الكتاب الأكاديمي، الطبعة الأولى الأردن، 2018.

17-ذكرى عبد الرازق محمد، النظام القانوني للبنوك الالكترونية، المزايا – التحديات – الافاق، دار الجامعة الجديدة للنشر، مصر، 2010.

18-ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالأنترنت والمعلوماتية دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، 2017.

19-رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الاسكندرية، مصر، 2007.

20-زهير بوشناق، العمليات المالية المصرفية الإلكترونية، اتحاد المصارف العربية، بيروت، لبنان، 2006.

21-طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلوماتية "، دار الجامعة الجديدة، 2009.

ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المطبعة والوراقة الوطنية، الطبعة الأولى، 2011،

22-محمد الشناوي، جرائم النصب المستحدثة (الانترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة) دار الكتب القانونية، مصر، 2008.

23-منتصر سعيد حموده، المساهمة الجنائية في التشريع المصري والاسلامي وأحكام محكمة النقض المصرية، دار الفكر الجامعي، مصر الطبعة الأولى، 2012.

24-محمد إبراهيم محمود الشافعي، الآثار النقدية والمالية للنقود الإلكترونية، دار النهضة العربية، 2003.

25-محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقات الائتمان الممغنطة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2009.

26-معوان مصطفى، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية، قواعد الاثبات المدني والتجاري، دار الكتاب الحديث، 2009.

27-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، مصر، 2007.

28-محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2008.

29-مصطفى كافي، النقود والبنوك الإلكترونية، دار مؤسسة رسلان للطباعة والنشر والتوزيع، سوريا، 2012.

30-محمد نور الدين سيد عبد المجيد، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الائتمان، دراسة مقارنة في القانون المصري والاماراتي والفرنسي، دار النهضة العربية، 2012 .

31-محمود داوود يعقوب، المسؤولية في القانون الجنائي الاقتصادي، دراسة مقارنة بين القوانين العربية والقانون الفرنسي، الطبعة الأولى، دمشق، سوريا، 2001.

32-مصطفى كمال طه، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، مصر دون طبعة، 2005.

33-محمد سعيد أحمد اسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2007.

34-محمد حماد مهرج الهيتي، الحماية الجنائية لبطاقات الائتمان الممغنطة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، 2009.

35-معادي اسعد محمد صوالحة، بطاقات الائتمان –النظام القانوني واليات الحماية الجنائية والأمنية، دار الافاق المغربية للنشر والتوزيع، الطبعة الأولى، 2008.

36-محمد محبوبي، أساسيات في أدوات الدفع والائتمان، دار ابي رقراق للطباعة والنشر، المغرب، الطبعة الأولى، 2012.

37-محمد محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، الجزء الثاني، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الثانية، 1979.

38-محمود محمد أبو فروة، مسؤولية البنك المدنية عن عمليات التحويل الإلكتروني، دراسة مقارنة، دار وائل للنشر والتوزيع، الطبعة الأولى، 2014، الأردن.

39-نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2005.

40-ناهد فتحي الحموري، الأوراق التجارية الإلكترونية دراسة تحليلية مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009.

41- نادر عبد العزيز شافي، المصارف والنقود الالكترونية، المؤسسة الحديثة للكتاب، لبنان، 2007.

42- نائل عبد الرحمان صالح، الجرائم الاقتصادية في التشريع الأردني، دار الفكر للنشر والتوزيع، الطبعة الأولى، الجزء الأول، الأردن، 1990.

42-نائل عبد الرحمان صالح الطويل، ناجح داود رباح، الأعمال المصرفية والجرائم الواقعة عليها، الجزء الأول، الطبعة الأولى، دار وائل للطباعة والنشر، الأردن،2000 .

43-نسرين عبد الحميد نبيه، الجانب الالكتروني للقانون التجاري، منشاة المعارف بالإسكندرية، 2008.

44-نضال اسماعيل برهم، أحكام عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع، الطبعة الاولى، الاصدار الأول، 2005.

45-عادل البراهمي، مسؤولية الصيرفي في وسائل الدفع، مداخلة مقدمة ضمن ملتقى مسؤولية الصيرفي المنظم من طرف مركز الدراسات القانونية والقضائية بالاشتراك مع الجمعية المهنية لبنوك تونس، 18 فيفري 1999، منشورات مركز الدراسات القانونية والقضائية، 2000.

46-عبد الحكيم زروق، التنظيم القانوني للمغرب الرقمي، مكتبة الرشاد _ساطات، الطبعة الأولى، 2013.

47-عبد الفتاح بيومي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية، 2004 .

48-عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دراسة الظاهرة الاجرامية المعلوماتية، دار الفكر الجامعي، مصر، الطبعة الأولى، 2008.

49-عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، دار الكتب القانونية، مصر، 2008.

50-عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني الحماية الجنائية لنظام التجارة الاليكترونية، دار الفكر الجامعي، الطبعة الأولى سنة، مصر، 2002.

51-عبد الفتاح بيومي حجازي، طرق اكتشاف تزوير الشيكات والمسؤولية عنه، دار الكتب، طبعة 2005، مصر.

52-عصام ابراهيم القليوبيِ، تطور ادوات الوفاء ومشكلاته القانونية، الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، لبنان، الطبعة الثانية .

53-علاء التميمي، التنظيم القانوني للبنك على شبكة الانترنت، دار الجامعة الجديدة للنشر، مصر، 2012.

54-عبد الكريم الريايدة، جرائم بطاقات الائتمان على البنوك الأردنية، دراسة تطبيقية ميدانية، دار الحامد للنشر والتوزيع، عمان الأردن، الطبعة الأولى،2013.

55-سامي عبد الباقي أبو صالح، الوفاء الالكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية، القاهرة.

56-سليمان ضيف الله، التحويل الإلكتروني للأموال ومسؤولية البنوك القانونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2012.

57-سليمان عبد المنعم، مسؤولية المصرف الجنائية عن الأموال غير النظيفة، دار الجامعة الجديدة، مصر، 2002.

58-سهيل محمد العزام، بحوث قانونية، المملكة الأردنية الهاشمية، المكتبة الوطنية، الطبعة الأولى 2011.

نبيل صقر، قمراوي عز الدين، الجريمة المنظمة، دار الهدى، الجزائر.

59-نجيمي جمال، المبادئ العامة لقانون العقوبات الجزائري مقارن بقانون العقوبات الفرنسي على ضوء الاجتهاد القضائي، المحكمة ومحكمة النقض الدولية مادة بمادة من المادة الأولى إلى المادة 60، دار هومة للطباعة والنشر والتوزيع، الجزائر 2016.

60-نضال اسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الاصدار الأول، 2005.

ثانيا/الرسائل والمذكرات الجامعية

أ-الرسائل الجامعية

1-العيد سعدية، المسؤولية الجزائية للبنك عن جريمة تبييض الأموال، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق، جامعة مولود معمري، تيزي وزو، تاريخ المناقشة، 2016/02/20.

2-بوربابة صورية، قواعد الأمن المعلوماتي دراسة مقارنة، مذكرة لنيل درجة الدكتوراه في العلوم، تخصص علوم قانونية، فرع القانون الخاص، جامعة الجيلالي اليابس، سيدي بلعباس، السنة الجامعية 2015_2016.

3-حوالف عبد الصمد، النظام القانوني لوسائل الدفع الالكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية، 2014،2015.

4-عبد الرحمان بن عبد الله السند، أحكام تقنية المعلومات "الحاسب الالي وشبكة المعلومات الانترنت "، رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن، جامعة الامام محمد بن سعود الاسلامية، السعودية، 1424،1425.

5-غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية، أطروحة دكتوراه في القانون، الجامعة الاسلامية ، لبنان، 2004.

ب-المذكرات الجامعية

1-دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل درجة الماجستير، شعبة القانون الجنائي، جامعة منتوري قسنطينة، 2012،2013.

2-ضاوي جزاع زبن ضاوي المطيري، المسؤولية الجنائية للاشتراك بالمساعدة، دراسة مقارنة، رسالة ماجيستير، قانون عام، كلية الحقوق، جامعة الشرق الأوسط، 2011، الأردن.

3-عبد الرحمان محمد السويلم، المساهمة في الجريمة المعلوماتية في النظام السعودي دراسة مقارنة بالقانون الاردني، رسالة ماجيستير في الشريعة والقانون، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الامنية، السعودية، 2014.

4-غزالي نزيهة، المسؤولية الجزائية للمصرفي في القانون الجزائري، بحث مقدم لنيل درجة الماجيستر، فرع قانون الأعمال، القانون الخاص، جامعة منتوري قسنطينة .

5-لوصيف عمار، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين مع الاشارة الى التجربة الجزائرية، مذكرة لنيل شهادة الماجيستير في العلوم الاقتصادية، تخصص تحليل و استشراف اقتصادي، جامعة منتوري قسنطينة،2009،2008.

6-محمد خميخم، الطبيعة الخاصة للجريمة الاقتصادية في التشريع الجزائري، مذكرة لنيل درجة الماجيستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، 2011/2010.

7-واقد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة لنيل درجة الماجيستير، فرع القانون العام، تخصص قانون التعاون الدولي، جامعة مولود معمري تيزي وزو، تاريخ المناقشة 2011/05/09.

ثالثا/المقالات

1-أشرف عبد الله الضويحي، ملخص بحث المساهمة في الجرائم المعلوماتية المتعلقة بالاعتداء الشخصي، بحث تكميلي لنيل درجة الماجيستير، قسم السياسة الشرعية، سلسلة

ملخصات الأبحاث القضائية، صادرة عن جامعة محمد بن سعود الاسلامية والجمعية العلمية القضائية السعودية، المملكة العربية السعودية، العدد الثالث،1435.

2-ايهاب الروسان، خصائص الجريمة الاقتصادية دراسة في المفهوم والأركان، دفاتر السياسة والقانون، العدد السابع، 2012.

3-بحيح عبد القادر، إشكالية التحكم في وسائل الدفع البنكية وأثرها على الخدمات المصرفية حالة الجزائر (1962_2010) ، مجلة الباحث، العدد09، لسنة 2011.

4-براق عبد الله مطر، النظام القانوني لبطاقات الدفع الإلكتروني، مجلة جامعة الانبار للعلوم القانونية والسياسية، العدد السابع.

5-بسام أحمد الزلمي، دور النقود الإلكترونية في عمليات غسل الأموال، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، 2010.

6- حسام العبد، غسل الأموال الإلكتروني، مجلة البنوك في الأردن، العدد السادس، المجلد التاسع عشر أيلول 2000.

7- حسن حماد حميد، جاسم خريبط خلف، اساءة استخدام بطاقة الائتمان الإلكترونية الملغاة، جامعة بابل للعلوم الانسانية، المجلد 18، العدد الثاني، 2010.

8- دلندة سامية، ظاهرة تبييض الأموال مكافحتها والوقاية منها، نشرة القضاة، العدد60.

9-حسين عبد الله عبد الرضا الكلابي، الوفاء الإلكتروني كوسيلة لتنفيذ الالتزام دراسة قانونية، مجلة كلية الحقوق، جامعة النهرين، العدد الرابع عشر، 2012.

10-زينة غانم يونس العبيدي، مسؤولية المصرف عن أخطاء الكومبيوتر في النقل الإلكتروني للنقود، مجلة الرافدين، المجلد 11، العدد39، سنة2009.

11-عائض بن سلطان البقمي، النظام القانوني للشيك الإلكتروني وحجية التعامل به، دراسة تحليلية مقارنة، دورية الإدارة العامة، دورية علمية متخصصة محكمة يصدرها معهد الإدارة العامة، فصلية، الأردن.

12-عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية، مجلة مركز دراسات الكوفة، العدد السابع، 2008.

13-عبد الجبار الحنيص، الحماية الجزائية لبطاقة الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 24، العدد الثاني، 2008.

14- علي كحلون، الأدوات المصرفية في التحويل الإلكتروني للأموال، مجلة القضاء والتشريع، صادرة عن وزارة العدل التونسية، جانفي 2011.

15-علي نحلة، النشاطات المشبوهة "غسل الأموال الإلكتروني آليات كشفها وكيفية التعرف عليها والتبليغ عنها "، مجلة اتحاد المصارف العربية، عدد حزيران /يونيو 2005.

16-فياض ملفي القضاة، الجوانب القانونية للتعاقد والدفع الإلكتروني في التجارة الإلكترونية، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة الأردن، المجلد الأول، العدد الثالث، 2009.

17-قيس حسن عواد، مقال بعنوان مشكلات فرض وتحصيل الضرائب في عقود التجارة الإلكترونية، مجلة الرافدين للحقوق، المجلد 12، العدد43، سنة 2010.

18-سعود بن عبد العزيز المريشد، غسل الأموال الإلكتروني في القانون السعودي والمقارن، مجلة الحقوق، الصادرة عن مجلس النشر العلمي، جامعة الكويت، العدد الثالث، السنة الخامسة والثلاثون شوال 1432هـ-سبتمبر 2011.

19-سلام منعم مشعل، وسائل الدفع الإلكترونية، مجلة كلية الحقوق، جامعة النهرين، العدد العشرون، 2008.

20-سيف الدين السماتي عبد الكريم، العمليات المصرفية الإلكترونية والاطار الاشرافي، مجلة اتحاد المصارف العربية، العدد278، يناير 2004.

21-محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الوفاء في مواجهة تصرفات حاملها، مجلة الشريعة والقانون، العدد الرابع والعشرون، رجب 1426هـ الموافق لسبتمبر 2005 ميلادي.

22-مقني بن عمار، مفهوم الجريمة الاقتصادية في القانون المقارن، مجلة القانون المغربي، مجلة قانونية شاملة تعنى بالشؤون القانونية والابحاث والدراسات القانونية والفقهية والاجتهادات القضائية، المغرب، عدد13، فيفري 2009

23-منى تركي، جان سيريل، الخصوصية المعلوماتية و أهميتها ومخاطر التقنية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013.

24-يونس عرب، جرائم الكومبيوتر والانترنت، مجلة اتحاد المصارف العربية، عدد يناير 2002.

رابعا/ مقالات في اطار الملتقيات و الندوات

1-ايت عكاش سمير، سعيد الهواري، مداخلة بعنوان البنوك الإلكترونية وعمليات غسيل الأموال، قدمت للملتقى العلمي الدولي الخامس حول الاقتصاد الافتراضي وانعكاساته على الاقتصاديات الدولية.

2-بلال عبد المطلب بدوي، البنوك الإلكترونية ماهيتها معاملاتها والمشاكل التي تثيرها، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الخامس.

3-بوعافية رشيد، ابراهيم مزيود، مداخلة بعنوان التحول إلى وسائل الدفع الإلكترونية وتحديات الجرائم المعلوماتية، الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الالكترونية في الجزائر، عرض تجارب دولية، المنعقد بالمركز الجامعي خميس مليانة، يومي 26-27 أفريل 2011.

4-توفيق شنبور، أدوات الدفع الإلكترونية (بطاقة الوفاء _النقود الإلكترونية) ، بحث مقدم إلى اعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، الجديد في

أعمال المصارف من الوجهتين القانونية والاقتصادية، الجزء الأول الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، لبنان الطبعة الأولى.

5-حسين شحادة الحسين، العمليات المصرفية الإلكترونية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، الجزء الأول، الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى، 2007.

6-حراق صباح، مداخلة بعنوان المعالجة الجبائية للتجارة الالكترونية، الملتقى العلمي الدولي الرابع حول، الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الالكترونية في الجزائر، عرض تجارب دولية، المنعقد بالمركز الجامعي خميس مليانة يومي 26-27 أفريل 2011.

7-رافعة ابراهيم الحمداني، اثر استخدام التكنولوجيا المصرفية في ظاهرة غسيل الأموال والجهود الدولية لمكافحتها، المؤتمر العلمي الرابع ، الريادة والابداع – استراتيجيات الأعمال في مواجهة تحديات العولمة – بجامعة فيلادلفيا كلية الحقوق والعلوم الادارية والمالية، يومي 15،16 مارس 2005.

8-طوني عيسى، حول الدفع الإلكتروني بالبطاقة الائتمانية في شبكة الانترنت، بحث مقدم إلى أعمال المؤتمر السنوي لكلية الحقوق بجامعة بيروت العربية، الجديد في أعمال

المصارف من الوجهتين القانونية والاقتصادية، الجزء الأول الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى، 2007.

9-ضياء نعمان، النقود الالكترونية أداة وفاء في التجارة الإلكترونية الأحكام والاثار، التجارة الإلكترونية أية حماية، أشغال الندوة الوطنية التي نظمها مختبر الدراسات الجنائية وهيئة المحامين بمراكش أيام 29-30 ماي 2009، سلسلة الندوات والأيام الدراسية 33-2010، المطبعة والوراقة الوطنية مراكش، المغرب.

10-محمد ابراهيم محمود الشافعي، الاثار القانونية والنقدية والاقتصادية والمالية للنقود الإلكترونية، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، المنعقد يوم 09_10ماي 2003، بالإمارات، الجزء الأول.

11-محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت الذي نظمته كلية الشريعة والقانون، جامعة الامارات العربية المتحدة بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة، من 01الى 03 ماي 2000، المجلد الثاني، الطبعة الثانية، 2004.

12-محمد سامي الشوا، بحث بعنوان الجرائم المعلوماتية للتعدي على الذمة المالية للغير، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية

الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09_10، ماي 2003، بالإمارات، الجزء الرابع.

13-مصطفى محمد بيطار، دور التشريعات الجنائية في الوقاية من الاحتيال المنظم، بحث مقدم إلى الندوة العلمية العلاقة بين جرائم الاحتيال والاجرام المنظم، مركز الدراسات والبحوث قسم الندوات و اللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، المنعقدة في 03-05 /1428/06 الموافق ل18-20 /2007/06.

14-منصوري الزين، وسائل وأنظمة الدفع والسداد الإلكتروني عوامل الانتشار وشروط النجاح، مداخلة في الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر، المركز الجامعي خميس مليانة 26-27أفريل 2011.

15-نبيل صلاح محمود العربي، الشيك الإلكتروني والنقود الرقمية، دراسة مقارنة، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10ماي 2003، بالإمارات، الجزء الأول.

16-صالح بن سع الصالح، مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي، مداخلة مقدمة إلى الدورة التدريبية لمكافحة الجرائم الاقتصادية، المنظم من طرف

كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، خلال الفترة من 20-1428/2/24هـ الموافق ل10-14 /2008/3.

17-صفوت عبد السلام عوض الله، بحث بعنوان الاثار الاقتصادية لعملية غسيل الأموال ودور البنوك في مكافحة هذه العملية، مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10 ماي 2003، بالإمارات، الجزء الرابع.

18-عدنان ابراهيم سرحان، الوفاء(الدفع) الإلكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10، ماي 2003، بالإمارات، الجزء الأول.

19-علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت الذي نظمته كلية الشريعة والقانون، جامعة الامارات العربية المتحدة بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة، من 01الى 03 ماي 2000، المجلد الثاني، الطبعة الثانية، 2004.

20-عزيزة الشريف، التوازن في المعادلة بين حق العميل في الخصوصية وحق البنك في مشروعية التعامل المالي، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة

والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09-10ماي 2003، بالإمارات.

21-غزالي نزيهة، تأمين وسائل الدفع الإلكتروني بآلية التصديق الإلكتروني في الجزائر على ضوء القانون الجديد 04/15 مداخلة قدمت في الملتقى الأول حول الاطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر، المنظم من طرف كلية الحقوق والعلوم السياسية ، بجامعة محمد الشريف مساعدية بسوق أهراس، يومي 16-17 فيفري 2016.

22-غنام محمد غنام، طبيعة العلاقة بين جرائم الاحتيال والجريمة المنظمة، بحث مقدم إلى الندوة العلمية "العلاقة بين جرائم الاحتيال والاجرام المنظم، من تنظيم مركز الدراسات والبحوث قسم الندوات والقاءات العلمية ، جامعة نايف العربية للعلوم الامنية ،المنعقدة بتاريخ 03-05 /1428/06/ الموافق ل18-20 /06/ 2008.

23-فارس فضيل، حمزة صويفي، مداخلة بعنوان الأبعاد القانونية والضريبية للتجارة الالكترونية في ظل وسائل الدفع المعتمدة، الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الالكترونية في الجزائر، عرض تجارب دولية، المنعقد بالمركز الجامعي خميس مليانة يومي 26-27 أفريل2011.

24-لسلوس مبارك، النقود الإلكترونية بين الكبح والتشجيع لجريمة غسل الأموال، مداخلة قدمت الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية

واشكالية اعتماد التجارة الالكترونية في الجزائر، عرض تجارب دولية، المنعقد بالمركز الجامعي خميس مليانة، يومي 26-27 أفريل2011.

25-هشام فتحي سيد حسن، وسائل حماية المستهلك الالكتروني بين الشريعة والقانون، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنظم من طرف كلية الشريعة والقانون جامعة الامارات العربية المتحدة وغرفة تجارة وصناعة دبي، المنعقد يوم 09_10ماي 2003، بالإمارات.

26-هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح انشاء الية عربية موحدة للتدريب التخصصي، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت الذي نظمته كلية الشريعة والقانون، جامعة الامارات العربية المتحدة بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة، من 01الى 03 ماي 2000، المجلد الثاني، الطبعة الثانية، 2004.

27-يونس عرب، التنظيم الضريبي والجمركي لصفقات التجارة الالكترونية، ورقة عمل مقدمة إلى برنامج الندوات المتخصصة حول التجارة الالكترونية، تنظيم معهد التدريب والاصلاح القانوني، الخرطوم، كانون الأول 2002.

28-يونس عرب، ورقة عمل "قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان "، مقدمة الى ورشة عمل "تطوير التشريعات

في مجال مكافحة الجرائم الالكترونية "، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 2-4أفريل، 2006.

29-يونس عرب، ورقة عمل "صور الجرائم الالكترونية واتجاهات تبويبها "، مقدمة إلى ورشة عمل "تطوير التشريعات في مجال مكافحة الجرائم الالكترونية "، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 2-4أفريل 2006.

30-ورقة عمل حول الاطار القانوني لنظم الدفع وتسوية الأوراق المالية، معدة من طرف اللجنة العربية لنظم الدفع والتسوية، أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، صندوق النقد العربي، 2012.

خامسا/النصوص القانونية

1-القانون رقم 10/90 المؤرخ في 14 أفريل 1990 الموافق ل19 رمضان عام 1410، المتعلق بالنقد والقرض، ج ر عدد16، 1990.

2-القانون رقم 03/2000 المؤرخ في 05 أوت 2000 الموافق ل05 جمادي الأولى عام 1421، المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر عدد48، 2000.

3-الأمر 07/03 المؤرخ في 10نوفمبر 2004 المعدل والمتمم للأمر 156/66 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات ج ر العدد 71 في 10نوفمبر 2004.

4-الأمر 11/03 المؤرخ في المتعلق بالنقد والقرض .ج ر العدد ،2003.المعدل والمتمم

5-القانون رقم 01/05 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق ل 06 فيفري سنة 2005، المتعلق بالوقاية من تبييض الاموال و تمويل الارهاب ومكافحتهما المعدل والمتمم بالقانون رقم 06/15، ج ر عدد 11، سنة 2005.

6-القانون 02/05 المؤرخ في 06 فيفري 2005 الموافق ل. المعدل والمتمم للأمر 59/75 المتضمن القانون التجاري ، ج ر عدد11،سنة 2005.

7-الأمر 06/05المؤرخ بتاريخ 23 أوت 2005 المتعلق بمكافحة التهريب ج ر عدد 59، 2005.

8-القانون رقم 04/09 المحدد للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ،المؤرخ في 05أوت 2009،ج ر عدد47، 2009.

9-الأمر رقم 04/10 المؤرخ في 26أوت سنة 2010الموافق ل16 رمضان سنة 1431، المعدل والمتمم للأمر 11/03 المؤرخ في 27 أوت سنة 2003والموافق ل27 جمادي الثاني سنة 1423 المتعلق بالنقد والقرض، ج ر، عدد50، سنة 2010.

10-القانون رقم 04/15 المؤرخ في 01 فيفري 2015، الموافق ل 11 ربيع الثاني عام 1436، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد06، 2015.

11-القانون رقم 06/15 المؤرخ في 15 فيفري 2015 الموافق ل25 ربيع الثاني 1436 هـ، المعدل والمتمم للقانون رقم 01/15 المؤرخ في 06 فيفري 2005 الموافق ل27 ذي الحجة 1425 هـ، المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما، ج ر عدد08، 2015.

12-القانون رقم 16-01 المؤرخ في 06 مارس 2016، المتضمن نص التعديل الدستوري 2016 الصادر في الجريدة الرسمية، العدد 14، المؤرخة في 07 مارس 2016.

13- القانون رقم 11/17 المؤرخ في 27 ديسمبر 2017 الموافق ل08 ربيع الثاني عام 1439، المتضمن قانون المالية لسنة 2018، ج ر عدد 76، 2017.

14-القانون رقم 18-04 المتعلق بالبريد والاتصالات الإلكترونية، المؤرخ في 10 ماي 2018 الموافق ل24 شعبان 1439، ج ر عدد27، 2018.

15-القانون رقم 18-05 المتعلق بالتجارة الإلكترونية، المؤرخ في 10 ماي 2018 الموافق ل24 شعبان 1439، ج ر عدد28، 2018.

16-القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018 الموافق ل 25 رمضان عام 1439، ج ر عدد 34، 2018.

د -المراسيم

-المرسوم الرئاسي رقم 14-252، المؤرخ في 13ذي القعدة عام 1435 الموافق ل 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج ر عدد 57، 2004.

هـ-نصوص قانونية لدول اخرى

1-قانون الجزاء العماني متوفر على الموقع:
https://www.rop.gov.om/pdfs/roplaws/ROPRULE-1.pdf

2-النظام رقم 03 لسنة 2014، قرار مجلس الوزراء رقم 186لسنة 2014، الوقائع العراقية، العدد4326، الصادر في 2014/06/23.

سادسا/أنظمة بنك الجزائر

1-النظام رقم 04/05 المتعلق بالتسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل، مؤرخ في 15 ديسمبر سنة 2005 الموافق ل13 ذو القعدة عام 1426، ج ر عدد26، 2006.

2-النظام رقم 05/05 المؤرخ في 13 ذي القعدة عام 1426 الموافق ل 15 ديسمبر سنة 2005 ، المعدل والمتمم للنظام 01/05 المتعلق بالوقاية من تبييض الاموال وتمويل الارهاب ومكافحتهما ، ج ر عدد 26، 2005.

3-النظام 06/05 المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى المؤرخ في 15 ديسمبر2005 الموافق ل13ذي القعدة 1426، ج ر عدد26، أفريل 2006.

4-نظام رقم 07/05 المتضمن أمن انظمة الدفع المؤرخ في 26ذي القعدة عام 1426الموافق ل28 ديسمبر سنة 2005، ج ر عدد 37 سنة 2006.

5-النظام رقم 03/12 المرخ في 14 محرم عام 1434 الموافق ل 28 نوفمبر سنة 2012 المتعلق بالوقاية من تبييض الاموال وتمويل الارهاب ومكافحتهما، ج ر عدد 12 لسنة 2013.

ثانيا/المراجع باللغة الفرنسية

Ouvrages :

1-Bonneau Thierry,Droit bancaire,4éme édition,Editeur Montchretien, Paris,1994.

2-Céline CASTETS-RENARD , droit de l'internet, LGDJ-Montchrestien Lextenso éditions, 2010

3-Christian Gavalda, Jean Stoufflet, instruments de paiement et crédit, effet de commerce cheque, carte de paiement, transfert de fonds, 7edition, lexis Nexis, 2009.

4-Étienne Wéry, facture, monnaie et paiement électronique ,litec groupe lexis Nexis ,édition du juris-classeur,p44

5-Etienne wéry, paiement et monnaie électronique, droit européen ,français et belge, droit des technologies, larcier, 2007, p72

6-Francis baillet,le droit du cybercommerce, le guide pratique et juridique, 2001.

7-Myriam Quéméner, criminalité économique et financière à l'ère numérique, pratique de droit, collection dirigée par Nicolas Molfessis, economica

8- pierre Bresse, guillaume Beaure D'Augères et Stéphanie Thuillier, paiement numérique sur internet , international Thomsonpublishing .

9-Pierre Storrer, La monnaie électronique en droit français en fin un nouveau départ?, revue banque de France, N° 753 novembre, 2012.

10-Régine Bonhomme, instrument de crédit et paiement, LGDJ lextenso édition, 2013, 10 édition.

11-Stéphane Piedelièver, Doit bancaire, Thémis droit privé, presses universitaires de France, 1er édition, 2003.

12-Stéphane Piedelièvre, Emmanuel Putman, droit bancaire, corpus droit prive dirigé par Nicolas Molfessis

13-Xavier Thunis, responsabilité du banquier et automatisation des paiements, t travaux de la faculté de droit de Namur, presses universitaires de Namur, p291

Thèses

1-Hatem Adnan Bezzo, le paiement électronique en matière d'opérations bancaires et de commerce en ligne, thèse en vue de l'obtention du doctorat, université de Toulouse, 2012.

Cours:

1-Cours-de-Droit des Instruments de paiement et de crédit sur le site mailto :cours-de-droit@outlook.com.

Articles :

1-Anne –Marie Moulin, problématique dématérialisation et blanchiment, membre de la délégation française ou groupe d'action financière (GAFI).

2-Cathie-Rosalie Joly, le statut de prestataire de services de paiement, www.ulys.net. www.droit-technolodie.org,www.droitdesjeux, consulté le 25/09/2015.

3-EL Hadi CHAIBAINOU, Informatique et sécurité bancaire les utilisation malveillantes des cartes bancaires, Revue banques et entreprises au Maroc, 6, Juin-Juillet-Aout 1986.

4-Henri delahaie et André grissonnanche, les nouveaux moyens de paiement ont –ils besoin a un cadre juridique spécifique l'expérience française, les cahiers de droit, vol 24,n°2,1983,P279-304,disponible sur http://id.erudit.org consulté le 23/12/2016.

5-réponse de la fédération bancaire française à la consultation de la commission européenne pour un nouveau cadre juridique pour les paiements dans le marché intérieur, fédération bancaire francaise, 13 février 2004,fedbancaire-fr, consulté le 25/05/2017, http://fbf.fr

6-Michel Espagnon, système carte bancaire « et dématérialisation transferts électroniques de fonds les paiement par wap, actes des journées d'études le 18 /11/1999_05/10/2000, organisé par l'association luxembourgeoise des juristes de banque, le centre de recherches informatique et droit (CRID) la faculté de droit de Namur et l'association européenne pour le droit bancaire et financier belgium (ABDBF-Belgium) , cahiers aedbf /evbf-belgium, bruyant Bruxelles, 2001

7-R.Gassin, informatique (fraude informatique), Répén, paris,dalloz, act 1995.

8-Serge Losappio, la répression de l'entente en droit pénal français et son application à la lutte antiterroriste, disponible sur le site http://www.village-justice.com/articles/repression-entente-droit-penal,3356.html/17/07/2016.

Lois:

1- loi n 91-1382 du décembre 1991 relative à la sécurité des chèques et des cartes de paiement, J.O.N °1du 01/01/1992 disponible sur.

2- Loi n°96-392 du 13 mai 1996 relative à la lutte contre le blanchiment et trafic des stupéfiants et à la coopération internationale en matière de saisie et de confiscation des produits du crime, JORF, 14 mai 1996.

3- loi du 14 aout 2000 relative au commerce électronique

4-Directive 2009/110/CE, concernant l'accès à l'activité des établissements de de monnaie électronique et son exercice ainsi que la surveillance prudentielle des établissements, du 16 septembre 2009.

5-Loi du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière économique et financière (JO du 29 janvier 2013)

الفهرس

مقدمة :..... 01

الباب الأول : المسؤولية الجزائية للفاعل الأصلي عن استعمال وسائل الدفع الإلكتروني 15

الفصل الأول: الأحكام العامة لوسائل الدفع الالكتروني.....18

المبحث الأول: التعريف بالدفع الإلكتروني 20

المطلب الأول: مفهوم الدفع الإلكتروني.....21

الفرع الأول: مفهوم الدفع الإلكتروني في القانون الفرنسي.....22

الفرع الثاني: غياب مفهوم للدفع الإلكتروني في القانون الجزائري.....23

المطلب الثاني: أطراف الدفع الإلكتروني.....26

الفرع الأول: انهاء احتكار البنوك لتقديم خدمات الدفع الإلكتروني في القانون الفرنسي.....27

الفرع الثاني: تكريس احتكار الدفع الإلكتروني في القانون الجزائري.....31

الفرع الثالث: الزبون المرخص له استعمال وسائل الدفع الإلكتروني.....34

المطلب الثالث: مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني بين التقييد والتوسيع.....36

الفرع الأول: مفهوم الأمر بالدفع الإلكتروني في القانون الجزائري.....37

الفرع الثاني: توسيع مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني في القانون الفرنسي.....42

الفرع الثالث: تقييد مبدأ عدم جواز التراجع عن الأمر بالدفع الإلكتروني في القانون الجزائري.....43

المبحث الثاني: المفهوم القانوني لوسائل الدفع الإلكتروني.....46

المطلب الأول: تمييز مفهوم وسائل الدفع الإلكتروني عن غيره من المفاهيم.....47

الفرع الأول: المفاهيم المرتبطة بوسائل الدفع الإلكتروني.....48

الفرع الثاني: تمييز وسائل الدفع الالكتروني عن المصطلحات المشابهة.....51

المطلب الثاني: تعريف وسائل الدفع الإلكتروني في القانون الجزائري.....55

الفرع الأول: تعريف وسائل الدفع في النصوص التشريعية الجزائرية.....56

الفرع الثاني: تعريف وسائل الدفع الإلكتروني من خلال أنظمة بنك الجزائر.....59

الفرع الثالث: الإجراءات المتخذة من بنك الجزائر لضمان التعامل الجيد بوسائل الدفع الإلكتروني....60

المبحث الثالث: أنواع وسائل الدفع الإلكتروني في القانون الجزائري.....68

المطلب الأول: وسائل الدفع الإلكتروني في القانون التجاري.....69

الفرع الأول: التحويل الإلكتروني للأموال.....69

الفرع الثاني: الإشعار بالاقتطاع.....84

الفرع الثالث: بطاقات الدفع الإلكترونية.....90

المطلب الثاني: وسائل الدفع الإلكتروني وفق قانون النقد 100

الفرع الأول: الشيك الإلكتروني.....101

الفرع الثاني: النقود الإلكترونية.....111

الفصل الثاني: حالات المسؤولية الجزائية للفاعل الأصلي عن استعمال

وسائل الدفع الإلكتروني في القانون الجزائري.....124

المبحث الأول: المسؤولية الجزائية وتأثرها بوسائل الدفع الإلكتروني.....126

المطلب الأول: خصائص المسؤولية الجزائية عن استعمال وسائل الدفع الإلكتروني 127

الفرع الأول: مسؤولية جزائية عن جريمة إلكترونية.....128

الفرع الثاني: مسؤولية عن جرائم اقتصادية معقدة ولامادية 134

الفرع الثالث: مسؤولية عن جرائم عابرة للحدود صعبة الإثبات.....137

المطلب الثاني: المبادئ العامة للمسؤولية الجزائية ووسائل الدفع الإلكتروني.....141

الفرع الأول: وسائل الدفع الالكتروني وأزمة الشرعية الجزائية في القانون الجزائري.....142

الفرع الثاني: ضرورة التفويض التشريعي في الجرائم المتعلقة بوسائل الدفع الإلكتروني.....147

الفرع الثالث: تفسير الموسع وأثره في احتواء الجرائم المرتبطة بوسائل الدفع الإلكتروني.....153

المبحث الثاني: حالات المسؤولية الجزائية للفاعل الأصلي عن إساءة استخدام وسيلة الدفع الإلكتروني 156

المطلب الأول: اشكالية التكييف للركن الشرعي لإساءة استخدام وسيلة الدفع الإلكتروني.....157

الفرع الأول: ضرورة التخلي عن فكرة تطويع نصوص قانون العقوبات الخاصة بجرائم الأموال.....158

الفرع الثاني: تكييف الركن الشرعي لإساءة استخدام وسائل الدفع الإلكتروني.....160

المطلب الثاني: حالات المسؤولية الجزائية عن استخدام وسيلة دفع إلكتروني معيبة 164

الفرع الأول: المسؤولية الجزائية عن الحصول على وسيلة دفع إلكتروني بطريقة غير مشروعة.....164

الفرع الثاني: المسؤولية الجزائية عن اساءة استخدام وسيلة دفع إلكتروني خلال فترة صلاحيتها.....166

الفرع الثالث: المسؤولية الجزائية عن اساءة استخدام وسيلة دفع إلكتروني ملغاة أو منتهية الصلاحية.....169

الفرع الرابع: المسؤولية الجزائية عن قبول وسيلة دفع إلكتروني مقلدة أو مزورة او مزيفة.....170

المبحث الثالث: المسؤولية الجزائية عن افشاء السر المصرفي لوسائل الدفع الالكتروني.....174

المطلب الأول: علاقة وسائل الدفع الإلكتروني بالسرية المصرفية **176**

الفرع الأول: وسائل الدفع وعلاقتها بالمساس بالخصوصية.....177

الفرع الثاني: أنظمة بنك الجزائر وحماية الحق في الخصوصية 183

المطلب الثاني: مفهوم السر المصرفي المعالج إلكترونيا.....185

الفرع الأول: تعريف السر المصرفي المعالج إلكترونيا.....186

الفرع الثاني: تأثير وسائل الدفع الإلكتروني على مفهوم السر المصرفي.....189

المطلب الثاني: أركان جريمة افشاء الأسرار المصرفية الإلكترونية.....190

الفرع الأول: الركن الشرعي للسر المصرفي الإلكتروني باعتباره صورة

للخصوصية المعلوماتية في القانون الجزائري.....194

الفرع الثاني: تداخل الأركان المادية في الجرائم المتعلقة بالخصوصية والسر المصرفي 199

الفرع الثالث: الركن المعنوي في الجرائم المتعلقة بالخصوصية و إفشاء السر المصرفي.....208

الفرع الرابع :الاستثناءات الواردة على إفشاء الأسرار المتعلقة بوسائل الدفع الإلكتروني.....209

الباب الثاني: المسؤولية الجزائية للشريك في استخدام وسائل الدفع الإلكتروني.....210

الفصل الأول :الاشتراك في قانون العقوبات و الاحتيال بوسائل الدفع الإلكتروني.....218

المبحث الأول: مميزات الاشتراك في الجرائم المتعلقة بوسائل الدفع الإلكتروني.....220

المطلب الأول: الأحكام العامة للاشتراك في القانون العقوبات الجزائري.....220

الفرع الأول : مفهوم الاشتراك في القانون العقوبات الجزائري.....222

الفرع الثاني : أركان جريمة الاشتراك في القانون الجزائري.....224

المطلب الثاني: الاتفاق صورة موسعة للاشتراك في الجرائم المتعلقة بوسائل الدفع الإلكتروني.....232

الفرع الأول: تمييز الاتفاق بوصفه طريقة من طرق الاشتراك عما يشابهه 236

الفرع الثاني: أركان الاتفاق الجنائي باعتباره صورة للاشتراك في الجرائم الإلكترونية 239

الفرع الثالث: إشكالية تمديد الاشتراك بالاتفاق الجنائي لجرائم وسائل الدفع الإلكتروني.....247

المبحث الثاني: المسؤولية الجزائية عن الاشتراك في الاحتيال بوسائل الدفع الإلكتروني.....250

المطلب الأول: المسؤولية الجزائية عن الاشتراك في الاحتيال المعلوماتي بين قصور النصوص التقليدية وضرورة التدخل التشريعي.....251

الفرع الأول: نصوص الاحتيال التقليدية قاصرة عن استيعاب الاحتيال بوسائل الدفع الالكتروني.....253

الفرع الثاني: مدى نجاعة نصوص المساس بالمعالجة الآلية للمعطيات وضرورة النص الجديد للحماية من الاحتيال المعلوماتي.....257

الفرع الثالث: الحاجة الى نص تشريعي جديد لجريمة الاحتيال المعلوماتي في القانون الجزائري....261

الفرع الرابع: شمول المسؤولية الجزائية عن الاشتراك في الاحتيال المعلوماتي للاشتراك في الاحتيال بوسائل الدفع الإلكتروني.....262

الفرع الخامس: مدى تعارض العقاب على الاحتيال المنظم بوسائل الدفع الالكتروني مع المبادئ العامة للمسؤولية الجزائية.....266

المطلب الثاني: الركن المادي للاشتراك في الاحتيال بوسائل الدفع الالكتروني.....269

الفرع الأول: الطبيعة الخاصة لطرق الاحتيال المعلوماتي بوسائل الدفع الالكتروني.....270

الفرع الثاني: المحل في الاحتيال بوسائل الدفع الإلكتروني.....282

المطلب الثالث: الضرر والقصد والعقوبة عن الاشتراك في الاحتيال بوسائل الدفع الالكتروني.....283

الفرع الأول: مكانة الضرر في الاحتيال بوسائل الدفع الإلكتروني.....284

الفرع الثاني: الركن المعنوي للاشتراك في الاحتيال بوسائل الدفع الإلكتروني.....285

الفرع الثالث: اشكالية العقوبة المقربة في القانون الجزائرية 287

المطلب الرابع: اساءة استعمال وسائل تقنية المعلومات وإشكالية تسهيل العمليات الاحتيالية 288

الفرع الأول: الركن الشرعي لإساءة استخدام وسائل تقنية المعلومات.....289

الفرع الثاني: الركن المادي للاشتراك في اساءة استخدام وسائل تقنية المعلومات.....292

الفرع الثالث: الركن المعنوي لإساءة استخدام وسائل تقنية المعلومات.....298

الفصل الثاني: الاشتراك في التزوير والجرائم الخاصة ببيانات وسائل الدفع الإلكتروني.....300

المبحث الأول: الاشتراك في التزوير والاستعمال لوسائل الدفع الإلكتروني المزورة.....303

المطلب الأول: المسؤولية الجزائية عن الاشتراك في تزوير وتزييف وتقليد وسائل الدفع الإلكتروني..304

الفرع الأول: جرائم التزوير والتزييف والتقليد مستقلة بنص خاص في قانون النقد والمال الفرنسي....305

الفرع الثاني: تمديد القمع للاشتراك بالوسائل والتجهيزات والبرامج في قانون النقد والمال الفرنسي....308

الفرع الثالث: علاقة تزوير وسائل الدفع الإلكتروني بالجريمة المنظمة.....313

الفرع الرابع: الركن المادي لجرائم الاشتراك في تزوير وتزييف وتقليد وسائل الدفع الإلكتروني.....315

الفرع الخامس: الركن المعنوي والعقوبات المقررة للجرائم.....326

الفرع السادس: ضرورة التدخل التشريعي في الجزائر لمواجهة تزوير وسائل الدفع الإلكتروني.....328

المطلب الثاني: المسؤولية الجزائية عن الاشتراك في استعمال وسائل الدفع الإلكتروني المزورة المزيفة والمقلد.....331

الفرع الأول: الركن الشرعي لجريمة استعمال وسائل الدفع الإلكتروني المزورة المزيفة والمقلدة 331

الفرع الثاني: الركن المادي للاشتراك في استعمال وسائل الدفع الإلكتروني المزورة المزيفة والمقلدة..334

الفرع الثالث: الركن المعنوي والعقوبات المقررة.....336

المبحث الثاني: الاشتراك في الجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني.....337

المطلب الأول: الركن الشرعي لجرائم الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني.....338

الفرع الأول: الحاجة لنصوص تجريمية للاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني في التشريع الجزائري.....339

الفرع الثاني: الحاجة إلى نص قانوني مستحدث لتجريم انتحال الهوية الرقمية.....341

المطلب الثاني: صور الأركان المادية للاشتراك في الجرائم المتعلقة ببيانات وسائل الدفع الإلكتروني.....347

الفرع الأول: الأركان المادية للاشتراك في الاستيلاء والاستعمال لبيانات وسائل الدفع الإلكتروني....347

الفرع الثاني: الركن المادي لجريمة انتحال الهوية الرقمية.....351

المطلب الثالث: استعمال الشبكة المعلوماتية ووسائل تقنية المعلومات للوصول لبيانات وسائل الدفع الإلكتروني.....352

المطلب الرابع : الضرر والركن المعنوي في الجرائم المتعلقة ببيانات وسائل الدفع الالكتروني 355

الفصل الثالث: الاشتراك في تبييض الأموال والتهرب الضريبي.....357

المبحث الأول: الاشتراك في تبييض الأموال باستخدام وسائل الدفع الإلكتروني.....358

المطلب الأول: إشكالية جعل وسائل الدفع الإلكتروني غير ملموسة وتبييض الأموال 360

الفرع الأول: وسائل الدفع الإلكتروني بين تسهيل المكافحة وتسهيل التبييض.....360

الفرع الثاني: مراحل تبييض الأموال وتأثرها بوسائل الدفع الإلكتروني 365

المطلب الثاني: أثير وسائل الدفع الإلكتروني في أركان الجريمة 369

الفرع الأول: ضرورة تعديل الركن الشرعي لتبييض الأموال إلكترونيا.....370

الفرع الثاني: وسائل الدفع الإلكتروني وتسهيل إخفاء الجريمة المصدر 377

الفرع الثالث: الركن المادي للاشتراك في جريمة تبييض الأموال إلكترونيا.....379

الفرع الرابع: الركن المعنوي لتبييض الأموال إلكترونيا.....388

المبحث الثاني: الاشتراك في التهرب الضريبي الإلكتروني.....391

المطلب الأول: إشكالية التهرب الضريبي الإلكتروني باستخدام وسائل الدفع الإلكتروني.....392

الفرع الأول: وسائل الدفع الإلكتروني تسهل إخفاء التهرب الضريبي.....393

الفرع الثاني: وسائل الدفع الإلكتروني تسهل إخفاء أثر التهرب الضريبي وحجمه.....396

المطلب الثاني: الحلول المقترحة للتهرب الضريبي الإلكتروني.....397

خاتمة:.....**404**

قائمة المراجع :.....**418**

ملخص: المسؤولية الجزائية عن استخدام وسائل الدفع الإلكتروني في القانون الجزائري

يثير موضوع المسؤولية الجزائية عن استخدام وسائل الدفع الإلكتروني في القانون الجزائري العديد من الإشكالات عمليا، وعلى الجزائر استكمالا لإصلاح أنظمتها المالية اتمام اصلاحات القطاع البنكي خاصة ما تعلق بأنظمة الدفع الإلكتروني ووسائل الدفع الإلكتروني لبقاء السيولة في البنوك، ومن أهم الجوانب التي نحتاج لإصلاحها المسؤولية الجزائية عن استخدام وسائل الدفع الإلكتروني وهذا نظرا لخصوصية الجرائم المرتكبة بهذه الوسائل لأننا عند تكييفها سنصطدم بمبادي القانون الجنائي ومنها مبدأ الشرعية، ومبدأ حضر القياس في المادة الجنائية مما يحتم علينا ضرورة القيام بالإصلاحات لإقرار هذه المسؤولية .

Résumé

La responsabilité pénale sur l'usage des moyens du paiement électronique dans le droit Algérien.

La question de la responsabilité pénale sur l'usage des moyens du paiement électronique dans le droit Algérien, soulève un nombre de problèmes sur le plan pratique et que l'Algérie dans le cadre de l'achèvement de son système financier, est appelée à compléter les réformes du secteur bancaire particulièrement en ce qui concerne le système du paiement électronique pour le maintien des liquidités dans les banques et parmi les aspects les plus importants dont nous avons besoin à réformer, celui de la responsabilité pénale sur l'usage des moyens du paiement électronique et ceci, en raison de la spécificité des infractions commise à l'aide de ces moyens, parce que, lors de son adoption, nous nous trouverons face aux principes du Droit pénale et, de ce fait, celuidu principe de l'interdiction de l'évaluation dans l'article pénale, ce qui oblige à la nécessité d'entreprendre des réformes pour l'adoption de cette responsabilité.

Summary:

The penal responsability on the use of the means electronic payment in Alg law.

The question of responsibility on use of means of electronic payment in Algerian law, raises a number of problems on the practical plan and, Algeria within, as part of the completion of its financial system, is appealed to complete the reforms banking sector, particulary as for as concerned the system of electronic payment for the maintenance of liquidities (cash) and among the most important aspects wich we need to reform, this of penal responsibility, on the means of electronic payment this because of the specificity of infractions commited with these means, because, during of its adaptation, be facing the principle of Algerian law, and, therefore, this of the principle of prohibition of the evaluation in the penal article, wich is to the necessity to indertake reforms for adoption of this responsibility.