



جامعة دمشق

كلية الحقوق

قسم القانون التجاري

الحلول القانونية لمشكلات الدفع الإلكتروني

((دراسة تطبيقية على بطاقات الدفع الإلكترونية))

أطروحة أعدت لنيل درجة الدكتوراه في القانون التجاري

إعداد الطالب

محمد غسان يوسف

إشراف الدكتورة

حنان بادي مليكة

الأستاذ المساعد في قسم القانون التجاري

٢٠٢٠م / ١٤٤٢هـ

استناداً إلى قرار مجلس البحث العلمي والدراسات العليا رقم /٣٠٧٠/ م ب د تاريخ
٢٠٢٠/٩/٧ فقد تمت مناقشة هذه الأطروحة بتاريخ ٢٣/٩/٢٠٢٠ .

من قبل السادة الأساتذة:

الدكتور هيثم الطاس الأستاذ في قسم القانون التجاري بكلية الحقوق -جامعة دمشق

عضواً.....

الدكتور موسى خليل ميري الأستاذ في قسم القانون التجاري بكلية الحقوق -جامعة دمشق

عضواً.....

الدكتورة حنان مليكة الأستاذ المساعد في قسم القانون التجاري بكلية الحقوق -جامعة دمشق

عضواً مشرفاً.....

الدكتورة ميسون المصري الأستاذ المساعد في قسم القانون التجاري بكلية الحقوق -جامعة دمشق

عضواً.....

الدكتورة سهير الجندي المدرس في قسم القانون التجاري بكلية الحقوق -جامعة دمشق

عضواً.....

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

(فَإِذَا اسْتَوَيْتَ أَنْتَ وَمَنْ مَعَكَ عَلَى الْفَلَكَ فَقُلْ الْحَمْدُ لِلَّهِ الَّذِي نَجَّانَا مِنَ الْقَوْمِ الظَّالِمِينَ
وَقُلْ رَبِّ أَنْزِلْنِي مُنْزَلًا مُبَارَكًا وَأَنْتَ خَيْرُ الْمُنْزِلِينَ)

صدق الله العظيم

القرآن الكريم: الآية ٢٨ - ٢٩ من سورة المؤمنون

(اجْعَلُوا الشَّجَرَةَ جَيِّدَةً وَثَمَرَهَا جَيِّدًا، أَوْ اجْعَلُوا الشَّجَرَةَ رَدِيَّةً وَثَمَرَهَا رَدِيًّا، لِأَنْ مِنْ الشَّمْرِ تُعْرَفُ الشَّجَرَةُ)

انجيل متى ٣٣: ١٢



إلى من سعى وشقى لأنعم بالراحة والهناء

وعلمني بعبقريته كيف أحب العلم

وأن أرتقي بسلم الحياة بحكمة وصبر

والدي العزيز

إلى الوحيدة التي منحتني كل شيء

الينبوع الذي لا يمل العطاء

التي حاكت سعادتي بخيوط منسوجة من قلبها

والدتي الحبيبة

إلى من دعمني وشجعني طوال سني عمري، وحبته يجري في عروقي ويلهج بذكره فؤادي

أخي الغالي ساري

إلى من بحقها تعجز لغات العالم أجمع عن صياغة عبارات الشكر والامتنان

الدكتورة الفاضلة حنان مليكة

إلى من سرنا سويًا وتكاتفنا يدًا بيد ونحن نسقي زهرة علمنا

أصدقائي: د. أحمد مازن الحكيم،

أحمد القاسم، مكسيم حسين، عيسى سليمان

شكر وتقدير

بعد عناء البحث وتعب الأيام وجب عليّ الشناء على الرحمن الرحيم، فالحمد لله ولي النعمة ودافع النقمة، ما تعسر أمر إلا ويسره وما اشتد بلاء إلا أزاله، فله الحمد من قبل ومن بعد أن وفقني لإتمام هذا البحث، أسأل الله فيه التوفيق والنجاح وأن يجعله عملاً خالصاً لوجه الكريم.

قال رسول الله (ص): "لا يشكر الله من لا يشكر الناس"

لا يسعني وأنا أضع اللمسات الأخيرة لهذا البحث بعون الله تعالى إلا أن أتوجه بالشكر الجزيل وبالغ الامتنان والتقدير إلى أستاذتي الفاضلة

(الدكتورة حنان مليكة)

لتفضلها بالإشراف على هذه الأطروحة ولما بذلته من جهد مخلص، فقد كان لسعة صبرها وتدقيقها وإبداء ملاحظاتها السديدة الأثر الواضح في توجيه سير عملي نحو الاتجاه الصحيح، وفقها الله وجزاها عني خير الجزاء.

كما أتقدم بالشكر والامتنان إلى السادة أعضاء لجنة المناقشة لتفضلهم بمناقشة الأطروحة، وسيكون لملاحظاتهم القيمة الأثر الطيب في إخراجها بالصورة المثلى، وفقهم الله وجزاهم عني خير الجزاء.

كما أسدي شكري وعرفاني إلى جميع أستاذتي الذين نهلت من فيض علمهم ودماثة أخلاقهم، وأخص بالذكر أستاذتي في قسم القانون التجاري.

كما يمني عليّ واجب الاعتراف بالفضل لأهله أن أتقدم بالشكر والتقدير إلى كل من مد لي يد العون والمساعدة من قريب أو بعيد في انجاز هذا العمل ولو بالكلمة الطيبة والبسمة الصادقة وأخص بالذكر:

الدكتور محمد يوسف،

المعيد بلال الدغيم

الأستاذ أحمد نعيم جبارة

مخطط البحث:

الباب الأول: الإطار الموضوعي للمشكلات القانونية للدفع الإلكتروني

الفصل الأول: التعريف بالمشكلات القانونية للدفع الإلكتروني

المبحث الأول: المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية

المبحث الثاني: المشكلات التي تواجه الاقتصاد الوطني

الفصل الثاني: سبل معالجة المشكلات القانونية للدفع الإلكتروني

المبحث الأول: أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية

المبحث الثاني: أساليب معالجة المشكلات التي تواجه الاقتصاد الوطني

الباب الثاني: الإطار الموضوعي للمشكلات الأمنية للدفع الإلكتروني

الفصل الأول: التعريف بالمشكلات الأمنية للدفع الإلكتروني

المبحث الأول: المشكلات التي تمس أداة الدفع الإلكترونية

المبحث الثاني: المشكلات الناشئة عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية

الفصل الثاني: سبل معالجة المشكلات الأمنية للدفع الإلكتروني

المبحث الأول: التدابير الوقائية

المبحث الثاني: التدابير العلاجية

المقدمة

يشكل قطاع التجارة أحد الأنشطة الاقتصادية المهمة، حيث تلعب التجارة دوراً كبيراً في إنعاش الاقتصاد الوطني. ويقوم النشاط التجاري بشكل عام على تبادل سلعة بنقد بحيث يتم أداء ثمن السلعة أو الخدمة نقوداً في سبيل الحصول عليها. وقد شهد قطاع النقود تطورات مختلفة، وكان نظام المقايضة أول ما عرفته البشرية كمقابل للحصول على سلعهم وخدماتهم، ويتم بموجب نظام المقايضة مبادلة سلعة بسلعة (كمية من القمح مقابل كمية من الشعير)، ولكن سرعان ما اكتشفت الجماعات البشرية عدم فعالية هذا الأسلوب وعدم ملاءمته لحاجات التجارة، نظراً لعدم وجود مقياس مشترك للقيم وعدم قابلية بعض السلع للتجزئة وصعوبة تخزين بعضها. فكان النظام البديل هو نظام النقود.

حيث ظهرت النقود كوسيلة فعالة للحصول على السلع. وكانت هذه النقود تقوم في بدايتها على النقود المعدنية المصكوكة من الذهب أو الفضة أو البرونز، فتحمل كل قطعة معدنية فئة معينة وقيمة محددة يمكن من خلالها الحصول على السلع والخدمات. ثم ظهرت النقود الورقية التي كانت في بدايتها أمر صعباً على الناس تقبله كبديل عن النقود المعدنية وذلك بعد أن اعتادوا على النقود المعدنية كونهم لم يتمكنوا من تخيل الثروة ممثلة بقطعة ورق لا جدوى فيها ولا قيمة مالية لها. وبقيت النقود الورقية والمعدنية مستمرة في التعامل فترة طويلة من الزمن في ظل ملاءمة هذه النقود لحاجات التجارة الداخلية. لكن مع انتشار التعاملات الدولية أدرك الأفراد قصور النقود كأداة للتبادل وعجزها عن مواجهة احتياجات التجارة التي أخذت تستند بشكل أساسي على عنصر الائتمان. فالتجارة تفرض على المشتغلين بها الدخول في سلسلة من العلاقات مع الزبائن تارة تجعلهم مدينين

وتارة أخرى دائنين، ففي بعض الأحيان لا يملك التاجر النقود الكافية لشراء السلع أو أنه يملك النقود الكافية لكنه لا يرغب بتجميد جميع أمواله ثمناً لسلعة محددة الأمر الذي أدى إلى ظهور الأسناد التجارية كمقابل للحصول على السلع والخدمات. إذ تشكل الأسناد التجارية أحد أكثر الأدوات استخداماً في نطاق التجارة الدولية فهي تتميز بإمكانية الحصول على السلع والخدمات دون الحاجة لتسديد أثمانها فوراً (عنصر الائتمان)، كما تتميز بإمكانية نقل الحقوق الثابتة بهذه الأسناد إلى أشخاص آخرين من خلال مراعاة شكلية محددة (التظهير).

وبالتالي فقد شكلت النقود المعدنية والورقية الأساس الوطني للتعامل في ظل التجارة الداخلية، وذلك نظراً لقوة الإبراء المطلقة التي تتمتع بها هذه النقود في ظل احتكار إصدارها من قبل الدولة فضلاً عن الثقة المطلقة للأفراد بهذه النقود. في حين شكلت الأسناد التجارية والاعتماد المستندي أساس التعامل بالنسبة للتجارة الدولية نظراً لما تتطلبه هذه التجارة من عنصر الائتمان ولما تتمتع به هذه الأسناد من سهولة حملها وسهولة تداول الحقوق الثابتة بها وفقاً لشكلية معينة.

ولم يعد خافياً على أحد النقلة النوعية والثورة التقنية في قطاع المعلومات والاتصالات التي شهدتها عصرنا الحالي. فقد أدت التحولات التقنية الحديثة في مجال البرمجيات والاتصالات إلى فرض أشكال جديدة من المعاملات المرتبطة بالاقتصاد والمعلومات، ومن أبرز هذه الأشكال (التجارة الإلكترونية). ونقصد بالتجارة الإلكترونية عملية إبرام أو تنفيذ كل ما يتصل بعمليات شراء أو بيع السلع والخدمات عبر شبكة الإنترنت من خلال تبادل المعلومات إلكترونياً وتعيدها للحدود الزمنية والمكانية التي تقيد حركة المعاملات التجارية.

وينبغي أن نشير إلى أن أثر الثورة التقنية لم يقتصر على قطاع التجارة فحسب بل امتد ليشمل جميع القطاعات ومن ضمنها قطاع المصارف حيث ترتب على التزاوج بين قطاع المصارف والثورة التقنية ظهور ما يسمى بمصطلح (العمل المصرفي الإلكتروني). والذي يتجسد باستخدام الوسيلة الإلكترونية في نطاق تقديم الخدمات المصرفية التقليدية أو الإلكترونية. ولعل من أهم الأعمال المصرفية الإلكترونية عملية الدفع الإلكتروني التي نقصد بها بشكل عام كل عملية يتم بموجبها تأدية ثمن السلع والخدمات بوسائل إلكترونية. حيث كشف التطور التقني عن ظهور وسائل دفع جديدة تستخدم لسداد ثمن السلع والخدمات نذكر منها:

١- التحويل الإلكتروني للأموال: أصدرت لجنة الأمم المتحدة المعروفة باسم (الاونسترال) القانون النموذجي للتحويلات الدولية للأموال عام ١٩٩٢ والذي عرّف التحويل الإلكتروني للأموال بأنه: "مجموعة من الخطوات التي تبدأ بأمر التحويل الصادر عن الأمر، وتهدف من هذا الأمر وضع قيمة هذا الأمر بالتحويل تحت تصرف المستفيد ويشمل أي أمر صادر من مصرف وسيط بهدف تنفيذ هذا الأمر الذي صدر عن الأمر أي المحوّل".^١

٢- الشيك الإلكتروني: يعرف الشيك الإلكتروني بأنه: رسالة بيانات إلكترونية مزيلة بتوقيع إلكتروني مصدق يرسلها محرر الشيك إلى المستفيد ليتم تحويل قيمة الشيك إلى حساب المستفيد عن طريق أحد المصارف الإلكترونية.^٢

^١ ورد هذا القانون لدى ، محمد ذوابة، عقد التحويل المصرفي الإلكتروني، رسالة ماجستير ، منشورات دار الثقافة للتوزيع ، مصر، ٢٠٠٨ ، ص ٢١.

^٢ د. بسام شيخ العشرة و د. حنان مليكة، التجارة الإلكترونية، منشورات الجامعة الافتراضية، كلية الحقوق، جامعة دمشق، دمشق، ٢٠١١-٢٠١٢، ص ٨٩.

٣- النقود الإلكترونية : تعرف النقود الإلكترونية بأنها: وحدات إلكترونية ذات قيمة مالية مدفوعة مسبقاً ومخزنة على وسيلة إلكترونية ومستقلة عن أي حساب مصرفي تستخدم كوسيلة لسداد قيم السلع والخدمات كونها تتمتع بقوة إبرائية اتفاقية وتحظى بقبول واسع لدى أشخاص مستقلين عمن قام بإصدارها^١.

٤- البطاقات المصرفية: تُعرّف البطاقة المصرفية بأنها: أداة مصرفية يصدرها مصرف معين لصالح شخص طبيعي أو اعتباري يدون عليها اسم حاملها وتاريخ إصدارها وصلاحياتها وتستخدم في الحصول على النقد أو في شراء السلع والخدمات^٢.

وتتخذ البطاقة المصرفية أشكال متعددة حسب النوع أو الوظيفة أو الجهة المصدرة^٣.

وتتميز جميع وسائل الدفع الإلكتروني السالفة الذكر بانتقال النقود في لحظة واحدة من حساب لآخر دون استخدام الطريقة المصرفية التقليدية ودون استخدام أي شكل من أشكال النقود المعدنية أو الورقية. فالنقد هنا مبني على تتابع الأصفار والآحاد وينتقل عبر خطوط الشبكات الحاسوبية والهاتفية.

وقد وفرت وسائل الدفع الإلكتروني عدداً من المزايا بالنسبة للأفراد والمصارف، فبالنسبة للأفراد أدت هذه الوسائل إلى توفير الوقت والجهد فضلاً عن انخفاض التكلفة أما بالنسبة للمصارف فقد أدت هذه الوسائل إلى

^١ د. شريف غنام، محفظة النقود الإلكترونية، دار النهضة العربية، مصر، ٢٠٠٧، ص ١٠.

^٢ راجع الرابط: www.Ar.wikipedia.org/wiki

تاريخ الزيارة ٢٠٢٠/٩/٣١ الساعة ١٠،٣٠ a.m

^٣ رائد يوسف، النظام القانوني للدفع الإلكتروني، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري تيزي، الجزائر، ٢٠١١، ص ٦٩-٧٠.

ظهور فرص جديدة لأعمال المصارف الأمر الذي مكنها من تحقيق ميزة تنافسية تؤدي لتحقيق الربح على الأجل الطويل من خلال خلق فرص تسويقية جديدة وتوزيع واسع الانتشار الأمر الذي ينعكس بشكل إيجابي على الاقتصاد الوطني.

وبالرغم من المزايا العديدة التي وفرتها وسائل الدفع الإلكتروني فقد كانت في نفس الوقت وسائل محفوفة بالعديد من المشكلات والتحديات التي تتتاب العمل المصرفي الإلكتروني بشكل عام وعملية الدفع الإلكتروني بشكل خاص. حيث كشف التطبيق العملي للعمل المصرفي الإلكتروني عن ظهور مجموعة من المشكلات والتحديات التي قد تثير القلق لدى الأفراد وتدفعهم إلى الإحجام عن التعامل بهذا النوع الجديد من أعمال المصارف. وحيث أننا سوف نقتصر بدراستنا على أحد العمليات المصرفية الإلكترونية ألا وهي عملية الدفع الإلكتروني لذلك ينبغي التنويه للفكرة الآتية:

إن أي عمل مصرفي إلكتروني ينتابه أربعة أنواع من المشكلات (المشكلات القانونية والمشكلات الأمنية والمشكلات التشغيلية والمشكلات المالية). ولكن وحيث أننا نتحدث عن مشكلات الدفع الإلكتروني فإن نطاق الدراسة سوف يقتصر على نوعين من المشكلات التي تتتاب العمل المصرفي الإلكتروني وبالتحديد سوف نقتصر على المشكلات القانونية والمشكلات الأمنية ومرد ذلك إلى الاعتبارات الآتية:

أ- إن المشكلات التشغيلية والمشكلات المالية هي مشكلات تتتاب أي عمل مصرفي إلكتروني وليس عملية الدفع الإلكتروني فحسب فالمشكلات التشغيلية هي مشكلات ناتجة عن دخول الوسيلة الإلكترونية وتحدث نتيجة لوجود خلل في نظام التشغيل أما بالنسبة للمشكلات المالية فهي ناشئة عن طبيعة العمل المصرفي بحد ذاته

وبغض النظر عن دخول الوسيلة الإلكترونية (كمخاطر الائتمان ومخاطر أسعار الفائدة)، وبالتالي ليس هناك أحكام خاصة لهذه المشكلات تتعلق بعملية الدفع الإلكتروني إنما هي مشكلات عامة تصيب أي عمل مصرفي أو أي عمل يستخدم الوسيلة الإلكترونية.

ب- كثرة الدراسات والأبحاث التي عالجت المشكلات التشغيلية والمالية من الناحية القانونية والاقتصادية بالقدر الكافي، في حين وجدنا ندرة في الدراسات التي تناولت المشكلات القانونية والأمنية حيث أكتفت أغلب الدراسات بالإشارة لهذه المشكلات بشكل عام دون التعمق أو التخصص بالنسبة لعملية الدفع الإلكتروني.

لذلك وللاعتبارات السالفة الذكر آثرنا اقتصار الدراسة على الحلول القانونية لمشكلات الدفع الإلكتروني وخصوصاً المشكلات القانونية والمشكلات الأمنية وبالتحديد بالنسبة لبطاقات الدفع الإلكترونية باعتبارها أحد أهم وسائل الدفع الإلكتروني وأكثرها انتشاراً في سورية ونقصد ببطاقات الدفع في هذا الخصوص البطاقات المصرفية التي تصدرها المصارف بموجب ترخيص من المؤسسات والشركات العالمية وتقوم بوظيفتي: الوفاء بثمن السلع والخدمات لدى التجار (وإن كان استخدامها على نطاق ضيق في سورية حيث تقتصر على بعض المحلات التجارية الكبيرة) - كما تقوم بوظيفة سحب النقود من أجهزة الصراف الآلي - (باعتبار أن انتشار مثل هذه البطاقات واسع جداً في سورية) -

وفي سبيل أن تأتي هذه الدراسة هدفها المنشود سوف نتعرف بدايةً على المشكلات القانونية وسبل معالجتها ثم نتعرف على المشكلات الأمنية وسبل معالجتها.

حيث كشف التطبيق العملي لوسائل الدفع الإلكتروني وبالتحديد بطاقات الدفع الإلكترونية عن وجود مجموعة من المشكلات القانونية التي لا تقتصر على مستخدم أداة الدفع الإلكترونية فحسب بل تمتد لتشكل تهديداً للاقتصاد الوطني من خلال جملة من الأعمال غير المشروعة.

كما أن هواة الجريمة ومحترفيها لم يتوان قيد أنملة عن استغلال نقاط الضعف في بطاقات الدفع الإلكترونية بهدف المساس بهذه الأداة باعتبارها كيان مادي وتقني بنفس الوقت أو المساس بألية عمل هذه الأداة بغية الحصول على الأموال غير المشروعة باستخدام طرق وأساليب متعددة.

وأمام هذه المشكلات والتحديات التي تنتاب معاملات الدفع الإلكتروني كان لابد من البحث عن الحلول القانونية لمعالجة هذه المشكلات، وبالتالي كان مطلوباً من الجهات الرقابية في الدول أن تأخذ على عاتقها إيجاد الحلول لكافة المشكلات التي تنتاب الدفع الإلكتروني. وذلك على اعتبار أن مسألة تطور وسائل الدفع الإلكتروني وانتشارها متوقف على إيجاد الحلول لهذه المشكلات، باعتبار أن مثل هذه المشكلات تخلق نوعاً من الشك والتخوف لدى الأفراد في التعامل بوسائل الدفع الإلكتروني. ولكي يأتي البحث القانوني هدفه المنشود يفترض أن تكون أساليب المعالجة والحلول القانونية موجهة لكل مشكلة من المشكلات القانونية والأمنية التي تواجه نظام الدفع الإلكتروني بشكل عام وبطاقة الدفع الإلكترونية بشكل خاص بغية معرفة مدى نجاح هذه الحلول في وضع حد لانتشار مثل هذه المشكلات.

وتكمن أهمية البحث في أن وسائل الدفع الإلكتروني بأشكالها المختلفة تعد أحد نتائج الثورة التقنية في قطاع المعلومات والاتصالات. وقد لقيت هذه الوسائل رواجاً وانتشاراً كبيراً في بلدان العالم المتطورة والنامية، نظراً للمزايا التي تتمتع بها هذه الوسائل. حيث شكاى السرعة في الأداء، وانخفاض التكلفة، وتوفير الوقت والجهد أحد أهم العوامل التي دفعت الأفراد للتعامل بوسائل الدفع الإلكتروني. إلا أن وسائل الدفع الإلكتروني كأى عنصر تقني جديد ينتابه مجموعة من التحديات والمشكلات. فقد كشف التطبيق العملي لهذه الوسائل عن وجود مجموعة من التحديات والمشكلات التي تتنبأ بمعاملات الدفع الإلكتروني، الأمر الذي تطلب من الجهات الرقابية التدخل بشكل فعال بغية التصدي لهذه المشكلات، من خلال توفير مجموعة من الأساليب والوسائل القانونية التي تسهم في معالجة هذه المشكلات. الأمر الذي ينعكس بشكل إيجابي على انتشار وسائل الدفع الإلكتروني وذلك على اعتبار أن هذه المشكلات والتحديات من أكثر العوامل التي تؤرق المتعاملين بهذه الوسائل وتدفعهم إلى العزوف عن التعامل بها. وبناءً عليه تتجلى أهمية البحث من ناحيتين:

الناحية الأولى : تسهم الأطروحة في تسليط الضوء على مظاهر المشكلات القانونية والأمنية التي تتنبأ بنظام الدفع الإلكتروني سواء أكانت هذه المشكلات تواجه مستخدم الأداة أم تمتد لتشمل الاقتصاد الوطني وذلك بالنسبة للمشكلات القانونية وسواء أكانت هذه المشكلات تمس أداء الدفع باعتبارها عنصر تقني و مادي في آن واحد أم انها ناشئة عن آلية عمل هذه الأداة وذلك بالنسبة للمشكلات الأمنية .

الناحية الثانية: يسهم البحث في تحديد الأساليب والوسائل التقنية والقانونية الكفيلة بوضع حد لهذه المشكلات سواء أكانت هذه الوسائل

تدابير وقائية أم تدابير علاجية، وسواء كُرسيت بموجب قوانين خاصة بالمعاملات الإلكترونية أم بموجب القوانين العامة التي تطبق على المعاملات التقليدية.

ونتمحور إشكالية البحث حول بيان الحلول القانونية لمشكلات الدفع الإلكتروني، والبحث في مدى فعاليتها وملاءمتها لمعالجة تلك المشكلات، ويتفرع عن هذه الإشكالية عدة تساؤلات نذكر منها:

- ١- ماهي صور المشكلات القانونية التي تواجه نظام الدفع الإلكتروني؟
 - ٢- ما هي التدابير المتخذة لمعالجة المشكلات القانونية للدفع الإلكتروني؟
 - ٣- ما هي مظاهر المشكلات الأمنية للدفع الإلكتروني؟
 - ٤- هل كرس المشرع السوري أساليب معالجة للمشكلات الأمنية للدفع الإلكتروني بموجب أحكام خاصة أم أكتفى بالأحكام العامة؟
- هذه التساؤلات وغيرها سوف تكون مجال دراستنا في هذا البحث .

واتبعنا في هذا البحث المنهج التحليلي بحيث قمنا بإيراد المعلومة مدار البحث ومن ثم التعليق عليها إن كان هناك مجال للتعليق. وقد انصببت معظم دراستنا في هذا البحث على بطاقات الدفع الإلكترونية التي تقوم بوظيفتي السحب والوفاء وخصوصاً في الباب الثاني من هذا البحث باعتبارها أحد أهم وسائل الدفع الإلكتروني وأكثرها انتشاراً في سورية . كما حاولنا إغناء البحث القانوني بمجموعة من الأمثلة العملية والاجتهادات القضائية التي تسهم في إيضاح الفكرة القانونية مع تقديم المقترحات اللازمة عند الضرورة.

وتتمثل معوقات البحث في الآتي:

١- غياب تنظيم تشريعي خاص ينظم المسائل المتعلقة بالدفع الإلكتروني في سورية، الأمر الذي تطلب منا العودة للأحكام العامة الواردة في بعض النصوص القانونية التي نظمت المعاملات الإلكترونية أو المعاملات التقليدية.

٢- عدم قدرتنا على تأمين اجتهادات قضائية سورية بخصوص مشكلات الدفع الإلكتروني وأساليب معالجتها، الأمر الذي تطلب منا الاعتماد على الأمثلة والاجتهادات القضائية العربية والأجنبية.

٣- رفض الكثير من المصارف السورية التي تتعامل بوسائل الدفع الإلكتروني الإفصاح عن المشكلات التي تنتاب الدفع الإلكتروني خوفاً على سمعتها التجارية وفي إطار التزامها بالحفاظ على السرية المصرفية للعملاء لديها.

وفي سبيل الإحاطة الشاملة بالمشكلات الأمنية والقانونية لوسائل الدفع الإلكتروني وأساليب معالجة هذه المشكلات، قسمنا الدراسة إلى بابين حيث خصصنا الباب الأول للحديث عن الإطار الموضوعي للمشكلات القانونية للدفع الإلكتروني من خلال تقسيمه لفصلين تعرفنا في الفصل الأول على المشكلات القانونية للدفع الإلكتروني، ثم بينّا وسائل معالجتها في الفصل الثاني. أمّا بالنسبة للباب الثاني فعلى غرار الباب الأول، تحدثنا عن الإطار الموضوعي للمشكلات الأمنية للدفع الإلكتروني من خلال تقسيمه لفصلين تعرفنا في الفصل الأول منه على المشكلات الأمنية للدفع الإلكتروني، ثم انتقلنا للبحث في سبل معالجتها في الفصل الثاني.

الباب الأول

الإطار الموضوعي للمشكلات القانونية للدفع الإلكتروني

تعد عملية الدفع الإلكتروني كأحد العمليات المصرفية الحديثة التي شهدتها الحياة الاقتصادية نتيجةً طبيعيةً للتزاوج بين قطاع المصارف من جهة والثورة التقنية في نظم المعلومات ونظم الاتصالات من جهة ثانية.

وتعتبر المشكلات القانونية من أهم صور المخاطر التي تؤرق كل المتعاملين بالتجارة الإلكترونية بوجه عام وبعملية الدفع الإلكتروني بشكل خاص، ويتمثل مبعث هذا الأرق في اتجاهين:

الأول: تسببت الثورة التقنية في إحداث طفرة في أسلوب تقديم الخدمات المصرفية، فانعكس ذلك على طبيعة التنظيم القانوني الخاص بهذه الخدمات حيث باتت معظم القواعد المصرفية التقليدية غير قادرة على استيعاب هذه المستجدات.

الثاني: تتسم تقنية المعلومات بالتطور المستمر والمتلاحق الذي قد لا يستطيع المشرع أن يلحق بركابه على النحو الذي يسبب حالة من الفراغ التشريعي من خلال عدم قدرة القوانين القائمة على ملاحقة هذه التطورات واستيعاب الفروض المختلفة لها.

كلا هذين الاتجاهين يؤديان في النهاية إلى وجود جملة من المشكلات القانونية التي تشكل تهديداً لحقوق هؤلاء المتعاملين.

ومن خلال استعراض هذه المشكلات القانونية نجد أنها تتمحور حول شكلين أساسيين:

الشكل الأول: المشكلات التي تواجه مستخدم أداة الدفع سواء أكان بصفته عميلاً للمصرف لجأ إليه للاستفادة من إحدى الخدمات المصرفية التي يقدمها أم باعتباره مستهلكاً إلكترونياً تعاقد للحصول على سلعة أو خدمة.

الشكل الثاني: المشكلات التي تواجه الاقتصاد الوطني والتي بمجملها أنشطة غير مشروعة تهدف إلى استغلال نقاط الضعف في وسائل الدفع الإلكتروني بغية القيام بأنشطة غير مشروعة (غسيل الأموال والتهرب الضريبي).

وأمام هذه المشكلات والتحديات كان لابد للجهات الرقابية من أن تأخذ دورها وذلك من خلال اتخاذ مجموعة من السبل الكفيلة بمعالجة هذه المشكلات. وذلك على اعتبار أن مسألة تطور وانتشار عملية الدفع الإلكتروني تتوقف على مدى ثقة الأفراد بهذه العملية، فمع وجود الحلول القانونية للمشكلات المرتبطة بعمليات الدفع الإلكتروني تزداد ثقة الأفراد بتلك العمليات فيقبلون عليها دون خوف. ومن خلال البحث في سبل معالجة هذه المشكلات نجد أن معظمها عبارة عن تدابير علاجية موجهة بشكل مباشر لمعالجة هذه المشكلات سواء أكرست بموجب القوانين النازمة للمعاملات الإلكترونية أم بموجب القوانين النازمة للمعاملات التقليدية وذلك بغرض التعرف على مدى ملائمة هذه النصوص القانونية لمعالجة مشكلات الدفع الإلكتروني.

وفي سبيل الإحاطة الشاملة بالمشكلات القانونية للدفع الإلكتروني وسبل معالجتها كان لابد لنا من تقسيم هذا الباب إلى فصلين بحيث خصصنا الفصل الأول منه للتعريف بالمشكلات القانونية للدفع الإلكتروني أما الفصل الثاني فقد خُصص للبحث في سبل معالجة هذه المشكلات.

الفصل الأول

التعريف بالمشكلات القانونية للدفع الإلكتروني

ترتب على التعامل بنظام الدفع الإلكتروني مجموعة من التحديات والمشكلات القانونية، الأمر الذي أثار خوف الأفراد ودفعهم إلى الشك في مدى توفر الضمانات القانونية الكفيلة بمعالجة هذه المشكلات.

وتعرّف المشكلات القانونية بأنها: «المشكلات الناجمة عن عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الإلكترونية»^(١).

ويعاب على التعريف السابق أنه يعتريه جانب من النقص حيث اقتصر على تحديد المشكلات القانونية الناشئة عن عدم تحديد التزامات وحقوق الأطراف في إطار التعامل المصرفي، إلا أنه هناك جملة من المشكلات القانونية الناشئة عن إمكانية مخالفة بعض التشريعات كغسيل الأموال، أو المشكلات الناشئة عن النقص التشريعي.

في حين ذهب جانب آخر إلى تعريف المشكلات القانونية بأنها: «حالة من عدم التوافق بين التشريعات والعادات المستقرة والمعايير الأخلاقية، وبين نظام عمل المصرف وذلك على النحو الذي يجعل تعاملات المصرف مع عملائه يشوبها الغموض وعدم الاستقرار»^(٢).

^١ د. أحمد سفر، أنظمة الدفع الإلكترونية، ط١، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٨، ص ٢٧.

^٢ د. علاء التميمي، التنظيم القانوني للبنك الإلكتروني على شبكة الإنترنت، دار الجامعة الجديدة، مصر، ٢٠١٢، ص ٢٤٢.

كذلك يؤخذ على هذا التعريف بأنه اقتصر على جانب من المشكلات القانونية ألا وهو عدم انسجام التشريعات الحالية مع الأعمال المصرفية، في حين أن هناك مجموعة من الأعمال التي قد تشكل مخالفات قانونية كانتهاك السرية وغسيل الأموال، وبالتالي فإن هذا التعريف لم يكن تعريفاً جامعاً مانعاً للمشكلات القانونية.

ويمكننا أن نعرّف المشكلات القانونية بأنها: «جملة من الأعمال القانونية وغير القانونية التي لا تتسجم مع التشريعات والأعراف المستقرة في البلاد، مما يمس بحقوق مستخدم أداة الدفع أو يشكل تهديداً للاقتصاد الوطني».

فمن خلال استقراء التطبيق العملي نجد أن المشكلات القانونية تشكل نوعاً من المخالفة للقواعد القانونية والعرفية السائدة في البلاد والتي إما تشكل نوعاً من المساس بحقوق حامل الأداة أو أنها تشكل نوعاً من المساس بالاقتصاد الوطني للبلاد.

وبالتالي تتجلى المشكلات القانونية في نطاق الدفع الإلكتروني في صورتين:

الأولى: المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية وهذه مجال بحثنا في المبحث الأول.

الثانية: المشكلات التي تواجه الاقتصاد الوطني وهذه مدار بحثنا في المبحث الثاني.

المبحث الأول

المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية

يُقصد بمستخدم أداة الدفع الشخص الذي يحمل وسيلة الدفع الإلكترونية ويستخدمها في أنشطته المختلفة و يتجلى هذا الحامل في صورتين:

حيث تتمثل الصورة الأولى في إطار علاقته مع المصرف مصدر أداة الدفع وهنا يطلق عليه مصطلح العميل.

في حين تتجلى الصورة الثانية في إطار علاقته مع التاجر ويطلق عليه في هذه الحالة مصطلح المستهلك.

وفي سبيل الإحاطة بكافة المشكلات التي تواجه هذا المستخدم سوف نخصص المطلب الأول للبحث في المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف على أن ننتقل في المطلب الثاني للحديث عن المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً.

المطلب الأول

المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف

يحرص العميل وبشكل دائم على أن تكون جميع معلوماته الشخصية والمالية محاطة بسياج منيع من السرية بحيث لا يمكن لأي شخص أن يطلع على هذه الحسابات، وبالتالي تشكّل مسألة السرية المصرفية أحد أهم المشكلات التي تواجه العملاء، ويزداد الأمر خطورةً عندما ندخل في نطاق الدفع الإلكتروني وخصوصاً في ظل تعدد الحالات

والأساليب الإلكترونية التي يمكن من خلالها انتهاك السرية المصرفية.

لذلك وفي سبيل تسليط الضوء على مشكلة انتهاك السرية المصرفية بشكل إلكتروني كأحد أخطر المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية سوف نقوم بالتعريف بالالتزام بالسرية المصرفية وذلك في الفرع الأول على أن نعالج الأثر السلبي لتقنية المعلومات على الحياة الخاصة للأفراد وذلك في الفرع الثاني.

الفرع الأول

التعريف بالالتزام بالسرية المصرفية

إنّ الالتزام بالسرية المصرفية كغيره من الالتزامات لا بد فيه من طرفين هما المصرف والعميل، فالمصرف وبحكم عمله يطلع على أسرار عميله، والعميل مضطر للكشف عن هذه الأسرار لكي يتمكن من الاستفادة من خدمات المصرف وبالتالي ينبغي أن يكون المصرف مؤتمناً على هذه الأسرار وإلا كان مسؤولاً.

وقد عرّف جانبٌ من الفقه الالتزام بالسرية المصرفية بأنه: ((الموجب الملقى على عاتق المصرف بعدم إفشاء الأسرار المصرفية التي آلت إليه بحكم وظيفته أو في معرض هذه الوظيفة والمتعلقة بزبائنه وهذا الموجب فرضته نصوص عامة بالإضافة إلى تقاليد وأعراف عامة^(١))).

^١ د. روكس رزق، السر المصرفي، ط١، المؤسسة الحديثة للكتاب، لبنان، ١٩٩٩، ص ١٠.

نجد من التعريف السابق أنه خلط بين سر المهنة والسرية المصرفية، فسر المهنة لا يقتصر نطاقه على العمل المصرفي فحسب بل أي مهنة يوجد فيها هذا الالتزام، وهو يهدف لحماية المصالح الفردية وتدعيم الثقة بين العميل وموظف المصرف باعتبار أن ما عهد إليه من أسرار يمس الحياة الشخصية للعميل. في حين أن السرية المصرفية تهدف إلى تحقيق ثلاث مصالح (مصلحة العميل في حفظ أسرارهِ ومصلحة المصرف في زيادة نشاطه وحماية الائتمان الذي يعد عنصراً أساسياً في حماية المصالح الاقتصادية العليا في الدولة^١). إضافة إلى أن هذا التعريف كان مقبولاً عندما كان العمل المصرفي في بدايته محدوداً ولم يكن هناك انتشار للجرائم الخطيرة، أما اليوم وبعد انتشار الوسائل الإلكترونية لم يعد هذا المفهوم مقبولاً.

في حين ذهب جانب ثانٍ من الفقه إلى تعريف الالتزام بالسرية المصرفية بأنه: «الالتزام موظفي المصرف بالمحافظة على أسرار عملائهم وعدم الإفشاء بها للغير باعتبار المصرف مؤتمناً عليها بحكم مهنته وخاصة أن علاقة المصرف مع عملائه تقوم على الثقة التي يكون عمادها كتمان المصرف لأسرار عملائه المالية»^٢.

تجدر الإشارة إلى أن هذا التعريف أفضل من التعريف السابق إذ أخذ بعين الاعتبار أن السرية المصرفية نظام خاص ومستقل ويختلف عن بقية المهن التي تخضع لمفهوم سر المهنة، لكن بالمقابل أغفل هذا التعريف الحالات التي يمكن فيها خرق السرية المصرفية.

^١ د. بسام الزلمي، غسيل الأموال والسرية المصرفية، رسالة دكتوراه، كلية الحقوق، جامعة دمشق، ٢٠١٠، ص ١٢٠.

^٢ د. سمير بالي، السرية المصرفية، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٢، ص ١٠.

ونحن من جانبنا نعرّف الالتزام بالسرية بأنّه: «الالتزام على جميع العاملين في المصرف وعلى كل من أطلع بحكم صفته أو وظيفته على معلومة ما في هذا المصرف بأن لا يفشي هذه المعلومة لأي شخص كان إلا في الحالات التي يسمح بها القانون أو العميل».

إذاً يمكننا أن نستنتج مما تقدم أن الالتزام بالسرية المصرفية له نطاق شخصي ونطاق موضوعي:

أولاً: النطاق الشخصي للالتزام بالسرية المصرفية.

يتمثل النطاق الشخصي للالتزام بالسرية المصرفية بوجود طرفين هما المصرف والعميل، فالمصرف هو الشخص الذي يتحمل الالتزام والعميل هو الطرف الذي يُقرر الالتزام لمصلحته، ومع ذلك فإن المصرف وعلى الرغم من تحمله الالتزام إلا أنه بالنهاية هو أيضاً مستفيد من هذا الالتزام على اعتبار أن ثقة العميل بسرية المصرف سوف تدفع الكثير من العملاء للتعامل مع هذا المصرف الأمر الذي يزيد من نشاط المصرف ومن العمولات التي يتقاضاها.

١- المصرف: عرف المشرع الأمريكي في المادة الأولى من القانون التجاري الموحد (UCC) المصرف بأنّه: «شخص قانوني يحترف تقديم الخدمات المصرفية».

¹ (UCC): Uniform Commercial Code 1997

أمّا بالنسبة للمشروع السوري فقد بيّن في قانون التجارة أنه: «يطلق لفظ المصرف في هذا القانون على كل الأشخاص والمؤسسات التي تحترف الأعمال المصرفية»^(١).

وبناءً عليه نجد أن هذه التشريعات تبنت معياراً موضوعياً وذلك من خلال ربط وجود المصرف من الناحية القانونية بالخدمات التي يقدمها بغض النظر عن الشكل الذي يظهر فيه أو الأسلوب الذي يتعامل فيه مع عملائه، ويستوي أن يكون لهذا المصرف كيان مادي متمثل في أبنية ومعدات أم له كيان إلكتروني متمثل في الأجهزة والبرمجيات.

ونحن من جانبنا نعرّف المصرف بأنه: «شخص اعتباري يكتسب صفة التاجر ويقوم بالأعمال المصرفية كقبول الودائع وتنفيذ أوامر الدفع وفتح الحسابات»^(٢).

ونحن من جانبنا نرى أن اعتبار المصرف شخص اعتباري لا يعني ذلك أن المصرف مؤسسة وذلك لأن المؤسسة تحدث بمرسوم تشريعي أو قانون أما المصرف فيحدث بقرار من رئيس مجلس الوزراء وفق الضوابط التي يحددها مصرف سورية المركزي^٢.

٢-العميل: يقصد بالعميل في معرض هذه الدراسة ذلك الشخص المصرح له استخدام أداة الدفع الإلكترونية الصادرة من قبل أحد المصارف، وتكون هذه الأداة مطبوعة باسمه وموقعة بتوقيعه ولديه الرقم السري الخاص بها، ويلتزم حامل الأداة بالشروط التي يضعها

^١ المادة/٤٠٣/ من قانون التجارة رقم / ٣٣/ لعام ٢٠٠٧.

^٢ المادة(٤/أ) من القانون رقم /٢٨/ لعام ٢٠٠١ الخاص بتأسيس المصارف الخاصة.

المصدر. ولعل التساؤل الذي يثور في هذا المجال حول: هل يشترط أن يكون للشخص حساب لدى المصرف حتى يكتسب صفة العميل أم يكفي مجرد حصوله على إحدى الخدمات المصرفية التي يقدمها المصرف حتى يحظى بهذا الوصف حتى ولو لم يكن لديه حساب؟

ذهبت المحاكم الانكليزية في أحد أحكامها لتعريف المقصود بعميل المصرف بأنه: «الشخص الذي يوجد لديه حساب لدى المصرف»^(١).

وعلى صعيد آخر تبني جانب من الفقه القانوني^٢ رأياً مخالفاً لهذا الحكم القضائي حيث ذهب إلى أنه لا يمكن القول بقصر صفة العميل على من له حساب لدى المصرف، وبرّر ذلك بأن العمليات المصرفية الإلكترونية استحدثت التزاماً عاماً بالسرية يقع على عاتق من يحصل على أحد الخدمات التي يقدمها المصرف، لذلك لا يمكن قصر صفة العميل على من له حساب لدى المصرف.

ونحن من جانبنا نؤيد ما تبناه الرأي الفقهي السابق ونرى بأنه لا ضرورة لاشتراط أن يكون للشخص حساب حتى يطلق عليه مصطلح عميل وذلك للمبررات الآتية:

- هناك الكثير من الخدمات المصرفية التي يقدمها المصرف للشخص والتي لا تتطلب أن يكون لديه حساب لدى

^١ مشار إليه لدى: د. علاء التميمي، مرجع سابق، ص ٣١٧.

^٢ Ross Cranston. Principles of banking law, Second Edition, Oxford University Press, 2003, P130.

المصرف كالاستشارات المعلوماتية الخاصة بشؤون التجارة والاستثمار، وتحصيل الأوراق التجارية المعالجة بشكل إلكتروني... الخ.

- يمارس المصرف الإلكتروني وعلى خلاف المصرف التقليدي نشاطه على شبكة الإنترنت وهذا الأمر يتطلب منه مزيداً من الجهد في الحصول على كثير من المعلومات حول شخصية العميل ، ونظراً لحساسية هذه البيانات يلتزم المصرف أن يكتّم هذه الأسرار، والتزام المصرف بالسرية واجب عليه سواء أكان للشخص حساب أم لا وذلك بالنسبة لهذه المعلومات الشخصية وبغض النظر عن أي تعامل . وهذا ما أكدته قانون السرية المصرفية حيث جاء فيه:

أ - تعتبر معلومات سرية في معرض تطبيق هذا المرسوم التشريعي المعلومات التي تتعلق بهوية العملاء وحساباتهم وموجوداتهم ومعاملاتهم مع المؤسسات المالية بما في ذلك الحالات المذكورة في المادة (٣) من هذا المرسوم.

ب - لا يجوز لكل من اطلع على المعلومات المذكورة في الفقرة السابقة بحكم وظيفته أو بما تسمح به القوانين والأنظمة النافذة إفشاؤها بما يخالف أحكام هذا المرسوم^(١).

كما نص ذات القانون على أنه: «يتعين على المؤسسات المالية أن تتأكد من هوية وأسماء العملاء كافة وأن تحتفظ بالوثائق التي تثبت هويتهم^(١)».

^١ المادة الثانية من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

نستنتج من النصوص السابقة أن المشرع السوري ألزم المصرف التأكد من هوية العملاء وأسمائهم، واعتبر أن مثل هذه المعلومات (المعلومات الشخصية) محل للسرية ويقع على المصرف التزام بكتمتها وذلك سواء أكان للشخص حساب أم لا.

وبالنتيجة نجد أن العميل هو أي شخص له علاقة تعاقدية مع المصرف سواء أكان للشخص حساب أم لا.

ثانياً: النطاق الموضوعي للالتزام بالسرية المصرفية

اعتمد معظم المشرعين^٢ ومن ضمنهم المشرع السوري معياراً موضوعياً لتحديد النطاق الموضوعي للسرية المصرفية، وبموجبه يعد سراً كل ما يعلمه المصرف عن عميله إبان تعامله. أي يعد سر كل معلومة يعلم بها المصرف بسبب نشاط العميل أو أثناء ممارسة هذا النشاط. وبالتالي فإن المعلومات التي يطلع عليها موظف المصرف من مصدر آخر وليس من تعامله مع العميل كما لو حصل على هذه المعلومات من صديق أو قريب فلا تكون مشمولة بالسرية المصرفية^٣.

ومن خلال استقراء نصوص قانون السرية المصرفية السوري نجد أن المشرع السوري اعتبر أن المعلومات التي تتعلق بهوية

^١ المادة الرابعة من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٢ المادة الخامسة من قانون سرية الحسابات بالبنوك المصري رقم ٢٥٠/ لعام ١٩٩٠ و المادة الثانية من قانون سرية المصارف اللبناني رقم ٦ / لعام ١٩٥٦.

^٣ د. أديب ميالة و د. مي محرز، السرية المصرفية في التشريع السوري، بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٧، العدد الأول، دمشق، ٢٠١١، ص ١٤.

العملاء وحساباتهم وموجوداتهم ومعاملاتهم مع المؤسسات المالية بمثابة المعلومات السرية، وألزم كل من اطلع عليها بحكم وظيفته أو بما تسمح له القوانين النافذة أن لا يقوم بإفشاء هذه المعلومات إلا في الحالات المحددة في القانون^١. كما عمد المشرع السوري إلى ذكر بعض الأمثلة عن الحسابات والمعلومات التي تخضع للسرية المصرفية كحسابات الودائع المرقمة، تأجير خزائن حديدية خاصة، المعلومات الشخصية للعميل^٢.

كما تجدر الإشارة إلى أن المصرف لا يلتزم بالسرية إبان نشاط العميل أو بسبب ممارسة العميل لهذا النشاط بل أيضاً يلتزم بالسرية إبان نشاطه (نشاط المصرف). ففي حال طلب مصرف من مصرف آخر معلومة عن حسابات مدينة لعميل يلتزم المصرف طالب المعلومة بعدم إفشاء هذه المعلومة^٣.

وينبغي أن نشير إلى أن الالتزام بالسرية المصرفية ليس مطلقاً بل هناك مجموعة من الاستثناءات التي تحكم هذا الالتزام، حيث تعد هذه الاستثناءات بمثابة الضوابط والحدود للالتزام بالسرية المصرفية، وتهدف بالدرجة الأولى إلى تحقيق المصلحة العامة ومصلحة العميل. ومن خلال العودة إلى نصوص قانون السرية المصرفية نجد أن هذه الاستثناءات يمكن أن تتبلور في ثلاث مجموعات :

^١ المادة الثانية من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٢ المادة الثالثة من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٣ المادة السادسة من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

١- الاستثناءات المتعلقة بالعميل: بما أن السرية المصرفية هي مقررّة لمصلحة العميل أي أن العميل هو المستفيد من هذا الالتزام، لذلك يمكن للعميل أن يتنازل عن هذا الالتزام سواء بإرادته أم بغير إرادته.

أ - الاستثناءات المتعلقة بإرادة العميل: وهي الاستثناءات التي يحددها العميل بإرادته وبشكل مباشر وصريح ولا تشمل سوى حالة وحيدة وهي الإذن. فالعميل هو صاحب المصلحة في الالتزام بالسرية المصرفية وبالتالي يمكن أن ينزل عن هذا الحق وفي أي لحظة ويسمح للمصرف بإفشاء بعض المعلومات لشخص أو لأشخاص معينين أو غير معينين^١. وتجدر الإشارة إلى أنه هناك طائفة من الأشخاص الذين يحق لهم الاطلاع على حسابات العميل وأسراره وليس للمصرف الاحتجاج بالسرية في مواجهتهم (كالوكيل الخاص للعميل، ممثل الشخص الاعتباري، المصفي، وكيل التفليسة، كفيل العميل، الوصي والقيم، دائن العميل، الموصى لهم^٢).

ب- الاستثناءات المتعلقة بنشاط العميل: وهي الاستثناءات التي لا تتدخل فيها إرادة العميل فيها وتشمل:

^١ دبسم الزلمي، غسيل الأموال والسرية المصرفية، رسالة دكتوراه، كلية الحقوق، جامعة دمشق، ٢٠١٠، ص ١٣٤ - ١٣٥.

^٢ د. علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية، دراسة قانونية، لا يوجد دار نشر، ١٩٨٩، ص ١١٨٨.

أ- شهر إفلاس العميل أو المؤسسة المالية^١.

ب- المنازعات القضائية وتتجلى في صورتين:

- في حالة وجود نزاع بين المصرف وعميله يحق للمصرف وفي سبيل الدفاع عن حقوقه أن يقوم بالكشف عن أسرار العميل، إذ لا يعقل أن يحرم المصرف من هذا الحق لأنه في هذه الحالة أصبح من الضروري الكشف عن هذه الأسرار، وقد أشار المشرع السوري إلى ذلك في المادة (٥/ثانياً/هـ) (بطلب من المحاكم القضائية المختصة.....). أي أنه لا بد أن يبين المصرف للمحكمة أن هناك معلومات سرية عن خصمه (العميل) ويمكن أن تؤثر في مجرى الدعوى لكي يسمح له القضاء بكشفها وأن يكون هذا الكشف في حدود النزاع وهذا ما تقره الجهة القضائية المختصة.
- فيما لو كان هناك نزاع بين العميل وشخص آخر ودُعي ممثلي المصرف للشهادة أمام المحكمة، فممثلي المصرف ملزم بالشهادة أمام المحاكم في أي جريمة من الجرائم وذلك بعد طلب من المحكمة القضائية المختصة وتجدر الإشارة إلى أنه في جرائم غسيل الأموال وتمويل الإرهاب يتم الطلب الشهادة عن طريق هيئة مكافحة غسيل الأموال وتمويل الإرهاب وينبغي أن تقدم المعلومات إلى القضاء على وجه السرعة^٢.

^١ المادة (٥/ثانياً/ج) من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٢ المادة (٥/ثانياً/هـ) من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

ج-الاستثناءات المتعلقة بالحجز: يمكن للدائن أن يقوم بإلقاء الحجز التنفيذي على أموال مدينه (العميل)، وفي هذه الحالة يصبح المصرف ملزم بخرق السّرية المصرفية^١، أما بالنسبة للحجز الاحتياطي فقد تشدد المشرع السوري ولم يسمح لأي دائن بإلقاء الحجز الاحتياطي إلا إذا كان هناك دين للخرينة العامة أو فيما يتعلق بجرائم غسل الأموال وتمويل الإرهاب، وبالتالي باستثناء هاتين الجهتين لا يمكن إلقاء الحجز الاحتياطي وذلك بخلاف الحجز التنفيذي والذي يتاح لأي دائن دون استثناء^٢.

٢- الاستثناءات الموضوعية: وهي الاستثناءات التي لا علاقة للعميل بها فهي لا تنبثق عن إرادته ولا ترتبط بأعماله، وتشمل:

أ-الاستثناءات المقررة لمصلحة المصرف: أجاز المشرع السوري للمصارف الخروج عن مبدأ السّرية وبشكل جزئي عندما سمح لها بتبادل المعلومات مع بعضها البعض^٣، ولكن بشروط: أن يكون ذلك الأمر صيانة لتوظيف أموالها وأن يكون تحت طابع السّرية (أي أن المصرف طالب هذه المعلومات يلتزم بعدم إفشائها) وأن يكون تبادل المعلومات بين المصارف عن الحسابات المدنية فقط^٤.

ب-الاستثناءات المتعلقة بكشف جرائم معينة: أجاز المشرع السوري لهيئة مكافحة غسيل الأموال وتمويل الإرهاب الكشف

^١ المادة (٥/ثانياً/و) من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٢ المادة السابعة من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٣ المادة السادسة من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٤ د. بسام الزلمي، مرجع سابق، ص ١٤٨.

عن الحسابات الموجودة لدى المصارف إذا قام شك أو دلالة على استخدام هذه الأموال لغرض غسلها أو تمويل الإرهاب^١. وفي الواقع نجد أن المشرع السوري لم يكتفِ بخرق السرية المصرفية في جرائم غسل الأموال وتمويل الإرهاب، بل يمكن خرقها حتى في أي جريمة أخرى عندما نص في المادة (٥/ثانياً/هـ) (بطلب من المحاكم القضائية المختصة) وهذه العبارة تحتل تأويلين:

الأول: عندما يكون هناك نزاع بين المصرف والعميل أو بين العميل وشخص آخر ودُعي ممثلي المصرف للشهادة.

الثاني: عندما تكون هناك جريمة مرتكبة ويحتاج كشفها للاستعانة بالمصرف فهنا يمكن للمحاكم القضائية المختصة الطلب من المصرف كشف السرية عن أي حساب من أجل كشف جريمة معينة. ومع صدور قانون أحداث المحاكم المصرفية رقم /٢١/ لعام ٢٠١٤ نأمل من المشرع السوري استبدال عبارة (بطلب من المحاكم المختصة) بـ (بطلب من المحاكم المصرفية المختصة).

٣-الاستثناءات المتعلقة بالرقابة: ينبغي أن نشير إلى أنه هناك عدة جهات رقابية على أعمال المصارف ومن الطبيعي عدم التمسك بمبدأ السرية المصرفية تجاه هذه الجهات، ولو كان يجوز للمصارف التمسك بمبدأ السرية لتعذر على هذه الجهات ممارسة مهامها. فعندما يقوم كل من الجهاز المركزي للرقابة المالية والهيئة المركزية للرقابة والتفتيش بالرقابة على أعمال المصارف فلا يجوز لتلك المصارف

^١ المادة (٥/أولاً/ب) من قانون السرية المصرفية رقم /٣٠/ لعام ٢٠١٠.

التنزع تجاهها بالسرية المصرفية^١. ولكن المشرع السوري اقتصر في هذا الاستثناء على المصارف العامة فقط دون غيرها أي أن المصارف الخاصة يمكنها أن تحتج بمبدأ السرية في مواجهة تلك الجهات الرقابية.

كما اعتبر المشرع السوري أنه لا يجوز الاحتجاج بمبدأ السرية المصرفية في حال ممارسة (الهيئة العامة للضرائب والرسوم) لمهامها في تحصيل الضرائب وتقدير قيمتها، لأن هذه الجهة ملزمة بالكشف على الحسابات والأرصدة لكي تكون بياناتها المالية صحيحة. ولكن هذه السلطات التنفيذية (الهيئة العامة للضرائب والرسوم وجهاز مكافحة التهرب الضريبي) لا يمكنها أن تقوم بالكشف عن هذه الحسابات إلا بعد موافقة وزير المالية بالذات^٢.

كما يجوز الخروج عن مبدأ السرية عند ممارسة مجلس النقد والتسليف ومديرية مفوضية الحكومة لمهامهم المنصوص عليها في القوانين والأنظمة النافذة، فالمصارف ملزمة بموجب القانون الخاص بتشكيل مجلس النقد والتسليف بأن تقدم تقارير بجميع المعلومات التي يطلبها المجلس، كما أن لهذا المجلس الحق بتدقيق وتفنيش حسابات هذه المصارف الأمر الذي يفهم منه أن السرية المصرفية تخرق عند ممارسة هذه الجهات لمهامها الرقابية^٣.

وبالنتيجة نجد أن السرية المصرفية هي عبارة عن التزام المصرف وكل من اطلع بحكم وظيفته أو بما تقضي به القوانين النافذة بحفظ المعلومات التي

^١ المادة (٥/أولاً/د) من قانون السرية المصرفية رقم ٣/ لعام ٢٠١٠.

^٢ المادة (٥/أولاً/هـ) من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

^٣ المادة (٥/أولاً/أ) من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

وصلت إلى علمه عن العميل بسبب ممارسة النشاط المصرفي أو أثناء ممارسة هذا النشاط، ولا يجوز الخروج عنه إلا في حالات محددة في القانون. ونكون بذلك قد بينا مفهوم الالتزام بالسرية المصرفية لننتقل إلى بيان أثر تقنية المعلومات على الحياة الخاصة بالأفراد في (الفرع الثاني).

الفرع الثاني

الأثر السلبي لتقنية المعلومات على الحياة الخاصة للأفراد

لا شك بأن استخدام الحواسيب في مجال جمع البيانات الشخصية المتصلة بالحياة الخاصة للأفراد ومعالجتها خلف آثاراً إيجابية وبخاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والعلمية والاجتماعية عن طريق تكوين قاعدة بيانات ومعالجتها بواسطة الوسائل الإلكترونية لإخراجها بصورة معلومات تعود بالفائدة على المستخدمين لأغراض معينة. وبالرغم من إدراك المجتمعات للإيجابيات الناجمة عن استخدام الحاسوب في شتى المجالات، إلا أنه تولد في الوقت نفسه الشعور بمخاطر تقنيات المعلومات التي تهدد الخصوصية، وازداد هذا الشعور بوجود كثير من حالات استخدام الحاسوب للبيانات الشخصية بطريقة غير مشروعة مما أدى إلى اتساع دائرة الاعتداء على الحياة الخاصة للأفراد. وهذا ما دفع الجهود الدولية والوطنية إلى إيجاد المبادئ والقواعد التي تحمي الحق في الحياة الخاصة مع ضرورة وجود التوازن بين حاجات المجتمع في جمع البيانات الشخصية وتخزينها ومعالجتها من جهة وضمان الحماية القانونية لهذه البيانات من مخاطر الاستخدام غير المشروع من جهة أخرى.

وفي سبيل معرفة الأثر السلبي لتقنية المعلومات على الحياة الخاصة للأفراد سنبين العوامل المتحكمة بمسألة الخصوصية (أولاً) ثم ننتقل لبيان المعالم الرئيسية لمخاطر الوسائل الإلكترونية على الحياة الخاصة (ثانياً) .

أولاً: العوامل المتحكمة بمسألة الخصوصية

يقصد بالخصوصية حق الفرد في حماية أسراره الشخصية والملاصقة للشخصية والعائلية ومراسلاته وسمعته وحرمة منزله وملكيته الخاصة في عدم اختراقها أو كشفها دون موافقته^١.

وقد حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية كبيرة في سورية لما للحياة الخاصة من أهمية قصوى على كيان الفرد والمجتمع ذلك أن الامر لا يخرج عن حالة من اثنتين لا وسط لهما إما هدر لحقوق الانسان في الحفاظ على حياته الخاصة أو احترام هذه الحقوق وإعلائها. ومن مظاهر الاهتمام بالحياة الخاصة للأفراد نذكر:

أكد الدستور السوري على أن: "الحياة الخاصة حرمة يحميها القانون"^٢.

كما نص القانون المدني على أنه: "لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر"^٣.

^١ المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادر بالمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢.

^٢ المادة /٣٦/ من الدستور السوري الصادر في ٢٧ شباط لعام ٢٠١٢.

^٣ المادة /٥٢/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

كما نص قانون الإعلام في هذا الخصوص على أنه: احترام خصوصية الأفراد وكرامتهم وحقوقهم والامتناع عن انتهاكها بأي شكل من الأشكال^١

كما نص ذات القانون على أنه: "يحظر على الإعلامي ان يتعرض للحياة الخاصة للأفراد ،ولا يعد مساساً بالخصوصية توجيه نقد أو نشر معلومات عن المكلفين بعمل أو خدمة عامة على ان يكون المحتوى الإعلامي وثيق الصلة بأعمالهم ومستهدفاً المصلحة العامة."^٢

نستنتج من النصوص السابقة أن للحياة الخاصة أهمية كبيرة ،حيث أكد الدستور على حرمة هذه الحياة ،كما نص القانون المدني على ضرورة وقف الاعتداء الذي يقع على حق من الحقوق الملازمة لشخصية الإنسان فضلاً عن المطالبة التعويض. كما أشار قانون الإعلام إلى حرمة الحياة الخاصة وإلى أن النقد البناء عن أي تقصير لا يعد نوعاً من انتهاك حرمة الحياة الخاصة للأفراد. كما تجدر الإشارة إلى وجود مجموعة من المؤيدات الجزائية في بعض القوانين التي نرجئ الحديث عنها إلى فقرة الحماية للحقوق الخاصة للأفراد.

وقد أورد التقرير الخاص بلجنة العمل الأمريكية حول وسائل الدفع الإلكترونية عدة عوامل تتحكم بمسألة الخصوصية نذكر منها :

١. إن الزيادة في عدد الأطراف المتداخلة في عملية الدفع بما فيهم المصدرين والموزعين والعاملين، يمكن أن تزيد من عدد الأشخاص الذين يسمح لهم الاطلاع على المعلومات الخاصة بالأفراد.

^١ المادة (٤/٤) من قانون الإعلام الصادر بالمرسوم التشريعي رقم ١٠٨/ لعام ٢٠١١.

^٢ المادة ١٣/ من قانون الإعلام الصادر بالمرسوم التشريعي رقم ١٠٨/ لعام ٢٠١١.

٢. تزداد الاعتداءات على الخصوصية كلما زادت استعمالات الدفع الإلكتروني وخاصة النقود الإلكترونية، كما أن التنوع في المعلومات ووجودها في أماكن مختلفة يمكن أن يضاعف القلق من هذه الاعتداءات.
٣. لا يحصل الشخص على إعلام أو اطلاع كافٍ حول نوع المعلومات المأخوذة عنه، والجهة التي تتلقاها وكيفية استخدامها.
٤. إن عدم وجود جداول تتضمن المعلومات الكافية حول كيفية صياغة الشخص لحقوقه يمكن أن يضاعف من فرضية الاعتداءات.
٥. قد لا يجري إخبار الشخص بمضامين الخصوصية بشأن التعامل بأدوات الدفع الإلكترونية لذلك من المفترض حصول جهد كبير لتتقيد العامل حول أمن المعلومات وكيفية استخدامها.
٦. يعتقد العاملون في قطاع صناعة الدفع الإلكتروني وخاصة النقود الإلكترونية، أن استخدام هذه النقود لا يزال في مراحله الأولى، وبالتالي من الطبيعي وجود بعض الجهل حول الآثار المترتبة على استخدامها.
٧. يفترض بالنظم التي تدير قطاع الدفع الإلكتروني وخاصة النقود الإلكترونية أن تطور نفسها بحيث تعمل على تقديم حماية تضمن أمن الشخص وخصوصيته بدلاً من تكريس الحماية له بعد ظهور المشكلة.

ثانياً: المعالم الرئيسية لمخاطر الوسائل الإلكترونية على الحياة الخاصة

هناك الكثير من المعالم التي تظهر بها مخاطر الوسائل الإلكترونية بشكل عام ومخاطر الحواسيب بشكل خاص على حياة الأفراد وتكمن في الآتي:

١- تقوم الكثير من المصارف العامة والخاصة بجمع البيانات المفصلة للأفراد والمتعلقة بالوضع المادي أو الصحي أو التعليمي أو العائلي أو غيرها وتستخدم في ذلك الحواسيب وشبكات الاتصال للقيام بتخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ونقلها. وهذا من شأنه أن يوفر الفرص للوصول إلى هذه البيانات بطريقة التحايل أو بشكل غير مأذون به، مما يفتح أوسع المجالات لإساءة استخدامها أو توجيهها بشكل خاطئ أو مراقبة الأفراد في خصوصيتهم أو الحكم عليهم من واقع السجلات المخزنة للبيانات الشخصية. فعلى سبيل المثال إن حكومة الولايات المتحدة وفق دراسات ١٩٩٠ جمعت ٤ بليون سجل مختلف حول الأمريكيين بمعدل ١٧ بند لكل رجل وامرأة وطفل. ومصلحة الضرائب IRS تمتلك سجلات لحوالي ١٠٠ مليون أمريكي على حواسيبها^١.

٢- تكمن مخاطر مصارف المعلومات على الحياة الخاصة في احتوائها على بيانات غير دقيقة أو معلومات غير كاملة أو معلومات لم يتم تعديلها أو تصويبها بما يكفل إكمالها وتصويبها. فعلى سبيل

^١ مشار إليه لدى: د. هشام رستم، قانون العقوبات ومخاطر المعلومات، ط ١، مكتبة الآلات الحديثة، مصر، ١٩٩٢، ص ١٨١.

المثال كلف مكتب تقييم التقنية في الولايات المتحدة OTA في عام ١٩٨١ الدكتور (لوردن) بإجراء دراسة حول قيمة بيانات التاريخ الإجرامي التي تحويها ملفات (وكالة الشرطة الفيدرالية FBI) وقد وجد أن نسبة عالية من البيانات غير كاملة وغير دقيقة ويتضمن العديد منها اعتقالات وتحقيقات إلا أنها لم تؤدي إلى إدانة. كما اعترفت أربع من خمس ولايات أمريكية تم الاتصال بها بواسطة مكتب التقنية أنها لم تتأكد أبداً من دقة البيانات في ملفاتها^١.

٣- من الصعب التوصل عادةً إلى المعلومات الشخصية بشكل كامل كونها متفرقة ومنعزلة، وبظهور قواعد البيانات الإلكترونية أصبحت مجمعة ومتوافرة ومتكاملة مما يتيح استخدامها لأغراض الرقابة على الأفراد أكثر من ذي قبل.

٤- شيوع النقل الرقمي للبيانات أدى إلى وجود مشكلة أمنية وطنية، ذلك أنه سهل استراق السمع والتجسس الإلكتروني فظهرت المخاطر التي تهدد الخصوصية بسبب عدم قدرة شبكات الاتصال على توفير السرية والأمان للبيانات المنقولة عبرها^٢.

٥- التعرض لالتقاط أرقام بطاقات الائتمان وسرقتها أثناء إرسالها عبر الشبكة إذا لم تستخدم الأساليب الفنية للتشفير.

^١ مشار إليه لدى: مادة معلوماتية حول الأعمال الإلكترونية وأمن المعلومات، المركز الوطني

للمعلومات، اليمن، ٢٠٠٥، ص ٧١ ومتاح على الرابط: www.arablawn.org

تاريخ الزيارة ٢٠١٨/٧/٢٠ الساعة ١٥:٠٦ P.M

^٢ المرجع السابق، ص ٧٣.

٦- التعرض لإمداد أطراف خارجية ليس لها علاقة بأعمال المصرف بالبيانات الخاصة بأحد عملائها. وخصوصاً في ظل غياب الساتر الأمني لحماية العملاء.

٧- بفضل التكامل بين عناصر الحوسبة والاتصالات والوسائط المتعددة أصبحت وسائل الرقابة السمعية والبصرية والمقروءة أكثر تطوراً وكذلك تطورت برمجيات التتبع وجمع المعلومات آلياً، وأتاحت شبكة الإنترنت القدرة الفائقة على جمع المعلومات ومعالجتها من خلال برنامج الذكاء الاصطناعي. الأمر الذي شكّل أرض خصبة لارتكاب الأنشطة غير المشروعة^١.

٨- التعرض لاختراق نظام المصرف بالدخول على شبكة الحاسب الآلي الخاص بها والتوصل إلى وسائل الاتصال بعملاء المصرف وإلى أجهزة الحاسب الشخصية بآماكن عملهم أو منازلهم، وهذا يمثل خطراً كبيراً ويؤدي إلى التعرف على رغبات العميل وميوله ومن ثم إغراقه بمنتجات دعائية على نحو قد يؤدي إلى إعاقة شبكة الاتصالات فضلاً عن تحمل المستهلكين نفقات باهظة بسبب الدعاية التي ترسل إليهم في صورة بريد إلكتروني^٢.

٩- اصطياذ البيانات الشخصية بواسطة تقنيات الكوكيز: تستخدم في بيئة الإنترنت العديد من الوسائل التقنية لتتبع المعلومات الشخصية

^١ يحيى حسن، التنظيم القانوني للعقود الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة النجاح الوطنية، فلسطين، ٢٠٠٧، ص ٤٠-٤١.

^٢ د. إبراهيم الدوي، التجارة الإلكترونية، دراسة تطبيقية على المكتبات، مطبوعات مكتبة الملك فهد الوطنية، السعودية، ٢٠١٠، ص ٥١.

وأشهرها رسائل الكوكيز التي تنتقل إلى نظام المستخدم بمجرد دخوله للموقع، وتتمكن من تسجيل بيانات تخص المستخدم. حيث إن تقنية الكوكيز يجري تخزينها بمجرد زيارة الموقع على القرص الصلب لجهاز المستخدم وبالتالي تتمكن التقنية من جمع المعلومات عن المستخدم (مثل المواقع التي قام المستخدم بزيارتها....الخ). ومع أن بداياتها ظهرت كوسيلة لغرض غير جرمي هو إرسال بريد إلكتروني من الشركات التجارية في إطار أنشطتها الدعائية إلا أنها تمكنت في ذات الوقت من الكشف عن بيانات لا يرغب المستخدمون الكشف عنها. وبالتالي فقد شكّلت رسائل الكوكيز وسيلة مهمة لملاحقة واقتفاء أثر المستخدمين وجمع المعلومات عنهم وتحليلها لغايات غير مشروعة^١.

١٠- اصطيد البيانات الشخصية بواسطة برمجيات التنبّع والشم: وهي وسيلة تتبّع لجمع أكبر قدر من المعلومات السرية والخاصة عن طريق ما يعرف بأنظمة جمع المعلومات (شمها). وكان الهدف من وراء هذه الاعتداءات في الغالب سياسياً حيث أن معظم البيانات المستهدفة كانت عائدة للمعارضة السياسية والصحفيين وناشطي حقوق الإنسان^٢.

وقد حصلت حوادث شهيرة في حقل الاعتداء على البيانات الخاصة من بينها:

^١ مادة معلوماتية حول الأعمال الإلكترونية وأمن المعلومات، مرجع سابق، ص ٧٢.

^٢ د. إبراهيم الدوي، مرجع سابق، ص ٥٦.

أ- حادثة حصلت عام ١٩٨٩ عندما تمكّن أحد كبار موظفي أحد المصارف السويسرية بمساعدة سلطات الضرائب الفرنسية بأن سرب إليها شريطاً يحتوي على أرصدة عدد من الزبائن، وقد تكررت مثل هذه الحادثة في ألمانيا^١.

ب- عرض نزاع على القضاء الروسي في قضية تتلخص وقائعها أن أحد العملاء أبرم عقد قرض مع أحد المصارف، ثم قامت السلطات الضريبية الروسية بطلب معلومات عن هذا العميل فلبى المصرف طلب هذه السلطات الأمر الذي اعتبره العميل نوع من انتهاك السرية المصرفية، فأقام دعوى قضائية أمام محكمة لينينسكي المحلية لمدينة كيميروفو على المصرف وانتهت المحكمة في حكمها إلى مسؤولية المصرف عن هذا الانتهاك وذلك على اعتبار أنه يمكن تقديم المعلومات التي تحتوي على السرية المصرفية لموظفي المؤسسات المرخص لها ولاسيما مصلحة الضرائب، فقط في حالة وجود مبرر وتأكيّد صحيح لضرورتها. ولم تتضمن نسخة الطلب المكتوب من مفتش الضرائب في القضية أي مبرر قانوني لطلب المعلومات المذكورة أعلاه. وبالتالي يمكن اعتبار تصرفات المصرف في إصدار هذه المعلومات غير قانونية، الأمر الذي يجعل المصرف مسؤول عن هذا الانتهاك^٢.

ونحن من جانبنا لا نؤيد هذه الحكم وذلك على اعتبار أن منح المصرف تقدير وجود مبررات لطلب معلومات سرية قد يشكاً نوعاً من المحاباة أو

^١ مشار لهذه الأمثلة لدى: مادة معلوماتية حول الأعمال الإلكترونية وأمن المعلومات، مرجع سابق، ص ٧٣.

^٢ القضية رقم ٢-٢٠١٢/٩٢٥ تاريخ ٢٠١٢/٢/٥ ومتاح على الرابط:

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>.

تاريخ الزيارة ٢٠١٩/٥/٢٢ الساعة ١٠،١٥ a.m.

عدم المساواة بين المستخدمين كما قد يفسح المجال لارتكاب الجرائم التي تمس الاقتصاد الوطني كجرائم التهرب الضريبي وغسيل الأموال من خلال رفض المصرف إعطاء هذه الجهات (جهاز مكافحة التهرب الضريبي أو هيئة مكافحة غسيل الأموال) بحجة عدم وجود المبرر. وحسناً فعل المشرع السوري في هذا الخصوص حيث سمح بالخروج عن السرية المصرفية في معرض ممارسة السلطات الضريبية لمهامها حيث نص قانون السرية المصرفية على أنه^١:

لا تطبق أحكام المرسوم التشريعي في الحالات الآتية:

بموجب موافقة تصدر عن وزير المالية بالذات في الحالات التالية:

١- في معرض ممارسة الهيئة العامة للضرائب والرسوم لمهامها بموجب القانون /٤١/ لعام ٢٠٠٧ وتعديلاته في سبيل تحصيل حقوق الخزينة العامة للدولة.

٢- في معرض ممارسة جهاز مكافحة التهرب الضريبي لمهامه بموجب القانون /٢٥/ لعام ٢٠٠٣ وتعديلاته.

٣- في معرض تبادل المعلومات المتعلقة بتطبيق أحكام الاتفاقية الدولية المبرمة بشأن تجنب الازدواج الضريبي.

٤- في معرض تطبيق أحكام المرسوم التشريعي /٤٤/ لعام ٢٠٠٥ وتعديلاته.

^١ المادة (٥/أولاً/هـ) من قانون السرية المصرفية رقم ٣٣/ لعام ٢٠١٠.

ج- عرض نزاع على القضاء الروسي في قضية تتلخص وقائعها أن أحد العملاء أبرم عقد قرض مع أحد المصارف وعهد المصرف بهذه الاتفاقية إلى أحد مقدمي الخدمات الإلكترونية ليصار إلى معالجة كافة البيانات المتعلقة بالقرض بشكل إلكتروني. ورغبةً من مقدم الخدمات في الحصول على مكافأة من المصرف أقدم على إرسال إشعار إلى العميل يطالبه بتسديد أقساط القرض وفق المواعيد المحددة الأمر الذي اعتبره العميل نوع من انتهاك البيانات الشخصية له. فأقام دعوى قضائية أمام المحكمة العليا للاتحاد الروسي على المصرف وانتهت المحكمة في حكمها إلى مسؤولية المصرف عن هذا الانتهاك، وذلك على اعتبار أن معالجة البيانات الشخصية تتم بموافقة صاحبها على ذلك. ولا يبدو من نص اتفاقية القرض أن هناك موافقة على نقل بياناته الشخصية إلى أطراف ثالثة لغرض معالجتها الأمر الذي يلزم المصرف بتحمل المسؤولية عن هذا الانتهاك^١

وفي ختام الحديث عن المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف، نصل إلى نتيجة مفادها أن دخول الوسيلة الإلكترونية كأحد العناصر التقنية الرئيسة في نظام الدفع الإلكتروني كان له أثرٌ سلبيٌّ على الحياة الخاصة بالأفراد. حيث كشف التطور التقني لعملية الدفع الإلكتروني عن وسائل عدة تستخدم لانتهاك البيانات الشخصية للأفراد الأمر الذي يشكل تحدياً قانونياً أمام المصارف ويدفعها للبحث عن علاج قانوني لهذه المشكلة.

^١ القضية رقم ٢-٢٠١٥/٩٣٦ تاريخ ٨ /٦/ ٢٠١٥ ومتاح على الرابط:

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>

المطلب الثاني

المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً

عندما يلجأ المستهلك إلى استخدام وسائل الدفع الإلكتروني في عمليات البيع والشراء فإنه يختصر على نفسه الكثير من الوقت كما أنه يوفر الكثير من النفقات، ولكن دخول هذا العنصر التقني (الوسيلة الإلكترونية) في عمليات الدفع بالنسبة للمستهلك كان له أثرين سلبيين:

الأول: أصبحت عمليات البيع والشراء لا تعرف الحدود الجغرافية الأمر الذي أفسح المجال لظهور المشكلات الناتجة عن عمليات الشراء عبر الحدود.

الثاني: لقد أسهمت الوسيلة الإلكترونية في ظهور المشكلات التي تواجه المستهلك التقليدي بصيغة جديدة أمام المستهلك الإلكتروني.

لذلك وفي سبيل التعرف على هذه المشكلات سوف نتحدث عن مشكلات الشراء عبر الحدود في الفرع الأول على أن ننتقل للحديث عن المشكلات التي تصيب المستهلك الإلكتروني كمتعاقد وذلك في الفرع الثاني.

الفرع الأول

مشكلات الشراء عبر الحدود

في ظل تجاوز عمليات الشراء الحدود الجغرافية للدول ظهرت مشكلات الشراء عبر الحدود كأحد التحديات التي تواجه المستهلكين في نطاق الدفع الإلكتروني وتتجلى هذه المشكلات في ثلاثة صور:

الأولى: مشكلة الدفع في أكثر من دولة وهي مجال بحثنا أولاً

الثانية: مشكلة القانون الواجب التطبيق والمحكمة المختصة وهي مدار بحثنا ثانياً

الثالثة: المشكلات المرافقة لانتشار النقود الإلكترونية وهي محور بحثنا ثالثاً

أولاً: مشكلة الدفع في أكثر من دولة

أدى التقدم الهائل في مجال الاتصالات إلى طرح مشكلات قانونية لم يخبرها رجال القانون من قبل فالواقع العملي يظهر أن عولمة وسائل الاتصال والمعلومات أدت إلى عولمة الاقتصاد. حيث أتاحت الوسائل الإلكترونية المتنوعة والمتطورة سوقاً هائلاً أمام الملايين من التجار والمستهلكين، حيث بات بمقدار الأشخاص شراء معظم احتياجاتهم عن طريق شبكة الإنترنت ومن ثم الدفع باستخدام أي وسيلة إلكترونية. ولعل من أبرز المشكلات التي صاحبت عملية الدفع الإلكتروني هي مشكلة الدفع في أكثر من دولة. وتتمثل هذه المشكلة في عدة مظاهر:

١- في نطاق عمليات الإصدار عبر الحدود التي تتجسد في قيام المصدر بإصدار وسيلة دفع إلكترونية لعميل موجود في بلد آخر مختلف عن بلد المصدر بهدف استخدام وسيلة الدفع في عمليات الشراء عبر الحدود. ويتوجب الأخذ بالحسبان أنه يجب الدفع للمصدر الثمن المقابل لاستخدام هذه الوسيلة. كما أنه قد يرغب مستلم وسيلة الدفع الإلكترونية بتحويل النقود الإلكترونية إلى نقود تقليدية (كاش أو

ودائع)^١ وهذه الإشكالية تتطلب من المصدر (المصرف) أن يكون موجوداً في الدول الأخرى التي تتعامل بالنقود الإلكترونية (بلد العميل أو البلد الذي يريد فيه تحويل المبلغ الإلكتروني لمبلغ تقليدي)، أو أن يعتمد على أنظمة الدفع العالمية المختصة بعمليات التجزئة والتي غالباً ما تكون مكلفة وغير فعّالة^٢.

٢- قد يقدم مصدر النقود الإلكترونية - على سبيل المثال - على الاستعانة بمنظمات بطاقات الائتمان بهدف تحويل النقود. وهذا الأمر من شأنه أن يتطلب الدفع إلى المزودين التقليديين لخدمات الدفع وهو ما يترتب تكاليف إضافية. إضافة إلى ضرورة وجود تعاون مشترك بين المصدر وأنظمة الدفع التقليدية. الأمر الذي يُظهر أنه حتى ولو تمكن مصدر والنقود الإلكترونية من التواجد في أي مكان في العالم (وهو أمر بالغ الصعوبة) فإنه في ذات الوقت ينبغي على المصدرين أن يجيدوا طريقة للربط بين دورات النقود الإلكترونية وأنظمة الدفع القانونية الموجودة في هذه الدول. وخصوصاً أن أنظمة الدفع الإلكترونية خلقت لتعمل في بيئة مفتوحة وليس في محيط مغلق^٣.

^١ د. حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ٢٠١٤ - ٢٠١٥، ص ٣٥٨.

^٢ المرجع السابق، ص ٣٥٩.

^٣ Malte Krueger, Off shore E- Money Issuers and Monetary policy, First Monday, December, 2005.

Available at:

[http:// www, first monetary – org issuer – 10/ kruger ? index – html.](http://www.firstmonetary-issuers-10/krueger?index=html)

تاريخ الزيارة ٢٠١٨/٨/١ الساعة ١٠,٣٠ a.m

٣- يترتب على الدفع في أكثر من دولة مشكلة تتعلق بالمنافسة حسب رأي أصحاب البطاقات الوطنية في فرنسا. حيث أقام أصحاب البطاقات الوطنية في فرنسا دعوى أمام القضاء معتبرين فيه أن انتشار البطاقات العالمية من شأنه أن يلغي ويحتكر المنافسة في السوق وذلك في ظل عدم تحديد النطاق الجغرافي للبطاقات العالمية، واستندوا في ذلك إلى أن القانون الفرنسي يجرم احتكار المنافسة ويفرض الغرامة بحق المحتكرين. لكن القضاء رفض الدعوى واعتبر أن الجهات المصدرة لهذه البطاقات ذات صفة عالمية من جهة النشاط وبالتالي لا يمكن حصرها بمكان جغرافي محدد. فالسوق الذي يجب النظر فيه بالنسبة لهذه الجهات المصدرة ينبغي أن يتجاوز الحدود الوطنية فهو ذو بعد أوروبي ودولي. كما اعتبر القضاء الفرنسي أن أصحاب البطاقات العالمية لا يحتكرون السوق كما ادعى أصحاب البطاقات الوطنية وذلك على اعتبار أن المنافسة في ظل البطاقات الوطنية كانت ضعيفة، أما ومع انتشار هذه الجهات العالمية فإن المنافسة أصبحت قوية للغاية وبالتالي دخول هذه الجهات يقوي المنافسة ولا يحتكرها حسب رأي القضاء الفرنسي^١.

ونحن من جانبنا نؤيد ما ذهب إليه القضاء الفرنسي وذلك على اعتبار أن تعدد الجهات المصدرة في نطاق الدفع الإلكتروني من

¹Tribunal, 7ème Chambre, Arrêt du 30 juin 2016, Affaire n° T-491/07 RENV.

شأنه أن يلزم هذه الجهات بتقديم أفضل الخدمات وبأقل الأسعار وبضمانات وحوافز أكبر، الأمر الذي من شأنه أن يغذي المنافسة ويشجعها وبالتالي ينعكس ذلك بشكل إيجابي لجهة المستهلكين.

نخلص مما تقدم إلى أن مشكلة الدفع الإلكتروني في أكثر من دولة تتمثل في الآتي:

- يترتب على الدفع الإلكتروني في أكثر من دولة أن يتحمل المصدر أعباء وتكاليف إضافية سواء بهدف إنشاء فروع له في بلدان أخرى أو بغية التعامل مع أنظمة الدفع التقليدية لتسوية الوضع.
- يترتب على الدفع الإلكتروني في أكثر من دولة أن يعمل المصدر على إيجاد وسيلة للربط بين أنظمة الدفع الإلكتروني وأنظمة الدفع التقليدية وذلك على اعتبار أن شبكة الإنترنت هي شبكة عالمية وليست محددة بنطاق معين وبالتالي فإن وسائل الدفع الإلكتروني تدور في محيط مفتوح وليس في نطاق مغلق.

ثانياً: مشكلة القانون الواجب التطبيق والمحكمة المختصة

تتميز عملية الدفع في العقد التجاري الإلكتروني، بسمات تختلف عن مثلتها في العقود التجارية التقليدية. وذلك نتيجة لثورة المعلومات التي نعيشها، والتي أحدثت انقلاباً حقيقياً للمفهوم التقليدي لعقود التجارة الدولية. حيث تتسم غالبية المعاملات التي تتم عبر شبكة الإنترنت بطابعها الدولي لكونها تتم بين أفراد يقيمون أو ينتمون إلى دول مختلفة. الأمر الذي من شأنه أن يثير مشكلة الدفع عبر الحدود

بالنسبة للقانون الواجب التطبيق والمحكمة المختصة في حال قيام نزاع بين أطراف العلاقة. وتتكشف خطورة وأهمية موضوع الدفع الإلكتروني في مجال التجارة الإلكترونية عند البحث في القانون الواجب التطبيق خاصة وأن شبكة الإنترنت التي يتم التعاقد من خلالها إنما هي شبكة ممتدة ومفتوحة كما لو كانت "منطقة بلا قانون" من حيث النظرة السطحية للمتعامل مع هذه الشبكة، في حين أنها في الحقيقة تخضع للعديد من النظم القانونية تبعاً لتعدد أطراف هذا المعاملات واختلاف انتماءاتهم السياسية وأماكن إقامتهم^١. مع العلم أن أشخاص المعاملات الإلكترونية لا يشعرون بخطورة وأهمية تحديد القانون الواجب التطبيق والمحكمة المختصة إلا عندما يثار نزاع فعلي ويجري البحث عن حل لهذا النزاع. حيث أن نظام الدفع الإلكتروني عبر الحدود قد يواجه مشكلات متعددة فيما لو كانت تكلفته الاقتصادية مرتفعة بسبب عدم وحدة المعايير المتبعة في الدول الأطراف في الصفقات، فتوحيد المعايير من شأنه تقليص التكلفة وخاصة في حال وجود فروق في المزايا المتوافرة في شبكات الدفع المعتمدة لدى هذه الدول^٢.

ونحن من جانبنا نؤيد ما ذهب إليه الرأي السابق من ضرورة توحيد المعايير الاقتصادية وذلك على اعتبار أن بعض الدول تمنح إعفاءات أو امتيازات اقتصادية أو إعفاءات بخصوص شبكة الإنترنت، في حين أن دول أخرى لا تمنح مثل هذه الإعفاءات الأمر الذي ينعكس على المشكلات القانونية التي تصيب المعاملات الإلكترونية.

^١ د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة دكتوراه، كلية

الحقوق، جامعة عين شمس، مصر، ٢٠٠٧، ص ٢٢٣.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٤٨.

وتعد مشكلات الشراء عبر الحدود بشكلها (مشكلة الدفع في أكثر من دولة و مشكلة القانون الواجب التطبيق والمحكمة المختصة) محط اهتمام الكثير من الدول. حيث تناولت مجموعة الدول الصناعية العشر الكبرى (Group of ten G10)^١ هذا الموضوع وقامت بتقديم تقرير حول وسائل الدفع وخاصة النقود الإلكترونية. و تضمّن هذا التقرير وجود اتجاهين بخصوص استخدام وسائل الدفع الإلكتروني عبر الحدود. وكلاهما يتضمن فرضية إصدار نقود إلكترونية بعملة أجنبية^٢.

فبحسب الاتجاه الأول: يستخدم المستهلك النقود الإلكترونية المصدرة من قبل جهة داخلية في عمليات الشراء من تجار قد يقع مركزهم خارج البلاد (مثال الشراء خلال السفر في الطائرة). ففي هذه الحالة فإن المصدر والمستهلك يمكن أن يكونا موجودين في بلد واحد في حين أن التاجر يكون مركزه في بلد آخر. وذلك على الرغم من أنه قد يكون للمستهلكين حقوق قانونية مختلفة فيما لو حصلت الصفقات في ظل تشريعات مختلفة.

أما بالنسبة للاتجاه الثاني: فمن الممكن أن يقوم أحد المصدرين في دولة ما بإصدار نقود إلكترونية إلى مستهلكين في بلد آخر - وربما

^١ بالفرنسية Groupe des Dix G10 وتضم هذه المجموعة: كندا - بلجيكا - فرنسا - ألمانيا - إيطاليا - اليابان - هولندا - سويسرا - المملكة المتحدة - الولايات المتحدة الأمريكية.

^٢ Groupe Des Dix - Monnaies Electroniques; la protection des consommateurs. Application de la loi de surveillance et question en Transfrontalière, Rapport du Groupe de travail sur la monnaie électronique, 1997, p24.

Disponible sur:
www.bis.org.

يكون ذلك بالعملة المحلية لبلد المستهلك - على أن تستخدم للشراء بها إما من قبل تجار محليين أو من تجار في بلد ثان. وهذا من الممكن أن يثير مشكلات أكثر صعوبة سواء من ناحية الحد من إمكانية تطبيق القوانين والأنظمة الوطنية أو أن يخلق حالة من الغموض على مستوى الاختصاص المكاني خاصة بالنسبة للأمور المتعلقة بالمستهلك.

وكنتيجة لذلك، قد يثور قلق بعض الدول من أن بعض المصدرين سيفضلون الاندماج مع شركات أو أن يؤسسوا شركات في الدول الأقل تشدداً من ناحية المتطلبات التنظيمية.

ويضاف إلى ذلك أن جهات الإصدار قد تتعرض لمخاطر قانونية تترافق مع عدم التطابق بين القوانين والأنظمة الخاصة بكل دولة، بما في ذلك القوانين الخاصة بحماية المستهلك، حفظ السجلات، القوانين المتعلقة بالخصوصية وغسيل الأموال.

ومن ناحية أخرى، ترى مجموعة الدول العشر أن احتمال عمل منتجات النقود الإلكترونية في غير بلد المصدر هو أمر غير واقعي مالم يكن لديه فرع. وقد توصلت إلى هذا الاستنتاج بعد الأخذ بالحسبان مسائل البنى التحتية والمادية اللازمة من جهة، ومدى قبولها من قبل التجار والمستهلكين من جهة أخرى.

وبخلاف ذلك، فإن الكثير من نماذج النقود الإلكترونية ذات البرمجيات لا تتطلب وجود أنظمة كمبيوترية لدى المستهلك أو التاجر، كما لا تتطلب الحضور الشخصي لأي منهما، غير أنه في هذه الحالات فإن المصدرين عبر الحدود قد يلاقون نوعاً من الإغراض عن تقبل منتجاتهم مقارنة بالمؤسسات المحلية والتي اعتاد

المستهلكون على التعامل معها كونها ذات سمعة تجارية حسنة. كما أن المصدرين الذين يتعاملون مع مقدمي خدمات أو أطراف خارجيين يمكن أن يتعرضوا لخطر عدم إمكانية تنفيذ الالتزامات القانونية من جانب الأطراف الخارجيين وذلك بسبب عوامل سياسية أو اجتماعية^١.

يضاف إلى ما تقدم، أنه من المحتمل أن يؤدي الاختلاف في التشريعات بين الدول إلى التأثير في مدى تطور وسائل الدفع الإلكتروني، فبالرغم من أن الدول تتشارك في عدد كبير من الأهداف السياسية فإن الآليات المعتمدة لتخفيفها يمكن أن تختلف فيما بينها فعلى سبيل المثال اختلاف القوانين وعدم تحديد المسائل المتعلقة بتطبيق أنظمة حماية المستهلك أو في مدى إلزامية العقود الخاصة بمنتجات الدفع الإلكتروني قد يعيق استخدامها عبر الحدود^٢.

ومن ناحية أخرى فإن المدى الذي يمكن أن تستخدم فيه وسائل الدفع الإلكتروني في ظل تشريعات مختلفة من شأنه أن يزيد من جاذبيتها كوسيلة لارتكاب الجرائم في حال استخدامها في إجراء الصفقات بين أفراد يخضعون لقوانين مختلفة، فالقرصنة عادة ما يركزون أهدافهم على عمليات الدفع التي لا تتطلب كمية كبيرة من المعلومات والبيانات التي ينبغي تأكيدها. فإن هذا النوع من الصفقات يمكن أن يزيد من نسبة المخاطر ومرد ذلك إلى اختلاف آليات التحقيق وإجراءاته باختلاف التشريعات النازمة لهذا النوع من المعاملات.

^١Ibid,p25.

^٢مشار إليه لدى: د. حوالف عبد الصمد، مرجع سابق، ص ٣٥٠.

حيث يستغل المجرمون تفاوت الحماية بين التشريعات المقارنة، فيميلون إلى الأسواق الأقل حماية. وبالتالي أصبحت هذه الجرائم تتخذ عمقاً دولياً أكثر فأكثر في حين أن إجراءات الحماية منها تتصف بالصفة المحلية الأمر الذي يثير صعوبة في مكافحة الجرائم عبر الحدود^١.

وبناءً على ما تقدم يمكننا القول بأن مشكلة القانون الواجب التطبيق والمحكمة المختصة تفوق خطورة وأهمية مشكلة الدفع في أكثر من دولة حيث تشكل الهاجس الأول الذي يشغل بال القانونيين من جهة وأطراف عملية الدفع الإلكتروني من جهة أخرى. وذلك على اعتبار أنه يترتب على هذه المشكلة جملة من المشكلات المرتبطة بها (الجرائم الإلكترونية - إعاقة تطور وسائل الدفع الإلكتروني....الخ) الأمر الذي يبرز مدى الحاجة الماسة لإيجاد الحلول القانونية السليمة لمثل هذه المشكلات.

ثالثاً: المشكلات المرافقة لانتشار النقود الإلكترونية

تشكل النقود الإلكترونية أحد أهم وسائل الدفع الإلكتروني وأكثرها انتشاراً في العالم، وقد كشف التطبيق العملي لهذه النقود عن وجود بعض المشكلات المرافقة لانتشارها وتتمثل هذه المشكلات في الآتي:

١- تحديد جهة الإصدار

المصدر هو عبارة عن الجهة التي تقوم بإصدار النقود الإلكترونية وفي سبيل إنجاز هذه العملية يبرم عدة عقود مع المستخدم والتاجر. ولعل التساؤل الذي

^١ المرجع السابق، ص ٣٥١.

يطرح نفسه في هذا المجال حول: من هو المصدر أو بمعنى آخر هل هو مؤسسة ائتمان أم مصارف خاصة أم عامة أم يقتصر الأمر على المصرف المركزي فقط دون غيره أسوة بالنقود التقليدية؟

إن المبدأ العام لدى معظم الدول هو أن يقوم المصرف المركزي بإصدار النقود الإلكترونية أسوة بالنقود التقليدية وذلك على اعتبار أن إصدار النقود من الحقوق الحصرية للمصارف المركزية كون الأمر يتعلق بسيادة الدولة، وبالتالي يحظر على أي جهة خاصة (مصارف أو مؤسسات ائتمان) أن تقوم بإصدار النقود الإلكترونية. ولكن اتجهت بعض التشريعات والتوجيهات الأوروبية إلى السماح لبعض المؤسسات الائتمانية بالقيام ببعض الأنشطة في مجال الدفع الإلكتروني.

حيث عرّف التوجيه الأوروبي المؤسسة المصدرة للنقود الإلكترونية بأنها: (كل جهة أو شخص معنوي بخلاف مؤسسات الائتمان تصدر وسيلة دفع تستخدم فيها نقود إلكترونية^(١)).

يلاحظ على تعريف التوجيه الأوروبي أنه لم يمنح هذه الجهات أي حق في إصدار النقود الإلكترونية وإنما أعطاهما الحق في أن تصدر وسائل دفع تستخدم فيها النقود الإلكترونية، وإصدار وسائل دفع أمر مختلف عن إصدار النقود الإلكترونية، الأمر الذي أدى إلى حدوث نوع من عدم الانسجام في تعريف التوجيه الأوروبي، حيث جاء المفهوم بمصطلح (المؤسسات المصدرة للنقود الإلكترونية) في حين جاء التعريف بمصطلح (إصدار وسائل دفع تستخدم فيها النقود الإلكترونية). كما أن التوجيه الأوروبي لم يقصر صفة

^١ التوجيه الأوروبي رقم ٤٦/ لعام ٢٠٠٠ المتعلق بالقيام بأعمال مؤسسات النقود الإلكترونية والرقابة الحصينة على تلك المؤسسات.

إصدار وسائل الدفع على مؤسسات الائتمان وإنما أجاز لأي جهة أو شخص معنوي بخلاف مؤسسات الائتمان أن تقوم بذلك.

في حين اتجه المشرع الفرنسي إلى تعريف مؤسسات الائتمان بأنها: (أشخاص اعتبارية تقوم بشكل معتاد بأعمال المصارف بعد حصولها على إذن مسبق، وتتمثل هذه الأعمال بصفة خاصة في تلقي الودائع وعمليات الائتمان وإدارة وسائل الدفع، كما حدد وسائل الدفع بأنها كل الوسائل التي تسمح للأشخاص بنقل أو تحويل الأموال أيًا كانت الدعامة التي تقوم عليها هذه الوسيلة وأياً كانت الطريقة الفنية التي تعمل بها^(١)).

يلاحظ على تعريف المشرع الفرنسي أنه على غرار التوجيه الأوروبي حيث أنه لم يمنح مؤسسات الائتمان أي حق حصري في إصدار النقود الإلكترونية إنما أجاز لهذه المؤسسات إدارة وسائل الدفع دون إصدارها وذلك على اعتبار أن إصدار النقود من الأنشطة المحصورة بنص القانون للمصارف^(٢).

كما جرى التقرير الخاص بمجموعة العمل في الاتحاد الأوروبي حول المؤسسات النقدية الأوروبية على وضع خمس نقاط تتعلق بكيفية إدارة المصرف المركزي لقطاع النقود الإلكترونية^(٣):

^١ مشار إليه لدى: د. شريف غنام، مرجع سابق، ص ٧٩.

^٢ د. حمود محمد غازي الحمادة، العلاقات التعاقدية الناشئة عن بطاقات الدفع الإلكترونية، المركز العربي للنشر والتوزيع، مصر، ٢٠١٧، ص ٩٠.

^٣ Electronic monetary institute working Group on Eui Emi 1994.

Available at:

[http\www.int\pub\pdf\annrep\ar 1994 en.pdf](http://www.int\pub\pdf\annrep\ar 1994 en.pdf).

أ- عدم تدخل المصرف المركزي أبداً: هذا ما تم تجاهله في ضوء مسؤوليات المصرف المركزي في المحافظة على سلامة ثبات وفعالية أنظمة الدفع وفي الإشراف على السياسة النقدية.

ب- عدم فرض قيود على مؤسسات الإصدار ولكن مع وجود رقابة من قبل المصرف المركزي: وهذا ما تم رفضه لأن الأصول التي تمثل القوة الشرائية في النقود الإلكترونية يجب أن تكون عبارة عن ودائع مالية مصرفية يمكن أن توجد فقط عن طريق مؤسسات ائتمانية تكون بطبيعة تأسيسها خاضعة لعدد من القيود من قبل المصرف المركزي.

ج- إصدار النقود الإلكترونية من قبل المصارف المركزية نفسها بالمنافسة مع القطاع الخاص معتمداً على البنية التحتية المصرفية لتوزيع النقود الإلكترونية: وقد تبين أن هذا الأمر لا يؤمن مصالح المصرف المركزي على المدى الطويل. إذ من شأن ذلك أن يرجح كفة القطاع الخاص دافعاً المصرف المركزي إلى الانسحاب من المنافسة والاكتفاء بمراقبة أنظمة الدفع والخدمات المصرفية الأخرى.

د- اعتبار عملية إصدار النقود الإلكترونية نشاطاً حصرياً خاصاً بالمصارف المركزية: وفقاً لهذا الأمر تقوم المصارف المركزية ببناء البنى التحتية بها لتوزيع النقود الإلكترونية وبذلك يمكن أن تعطى النقود الإلكترونية وصف العملة القانونية. غير أن ذلك لا يشكل الحل الأمثل بالنسبة لتقرير المؤسسات النقدية الأوروبية، فمعظم المصارف الأوروبية ليس لديها خطط لإصدار النقود الإلكترونية. فهي تؤمن بأن هذه النقود لن تكون مختلفة عن وسائل الدفع الأخرى غير النقدية، ومع ذلك فقد تم النص على أن المصارف المركزية يمكن أن تكون

ملزمة عند نقطة ما بإصدار النقود الإلكترونية كقيامها بإصدار بطاقات مسبقة الدفع خاصة به كطريق لمنع تكاثر نماذج النقود الإلكترونية ذات الأنظمة المختلفة.

هـ- حصر الإصدار بالمؤسسات الائتمانية والمؤسسات الائتمانية غير المكتملة التأسيس وذلك بشروط :

- أن يكون نظام عمل الدفع على الصعيد الداخلي فقط.
- أن تخضع المؤسسات المصدرة لتنظيم مناسب وخاصة فيما يتعلق بمتطلبات السيولة.
- أن يتم الإشراف على هذه المؤسسات من قبل المصارف المركزية.

وعلى الصعيد السوري فقد نص مشروع قانون النقد الإلكتروني على أنه: يصدر النقد الإلكتروني من قبل:

- مصرف سورية المركزي.

— المصارف العاملة في سورية بموجب ترخيص خاص بإصدار النقد الإلكتروني من مصرف سورية المركزي^١.

أي أن المشرع السوري حصر هذا الحق بمصرف سورية المركزي، وإن كان أجاز للقطاع الخاص إصدارها بموجب ترخيص خاص منه.

ونحن من جانبنا نرى أنه في نطاق الدفع الإلكتروني ينبغي التمييز بين نقطتين:

^١ المادة الثانية من مشروع قانون النقد الإلكتروني وهو عبارة عن مشروع أعدته لجنة من المصرف المركزي السوري وقدم إلى مجلس الوزراء وإلى الآن لم يبصر النور ويصبح قانون .

النقطة الأولى: فيما يتعلق بالجهة مصدرة النقود الإلكترونية فإننا نميل لحصر هذا الحق بالمصرف المركزي وحده أسوة بالنقود التقليدية والسبب في ذلك هو أن المصرف المركزي هو مصرف الدولة وهو المسؤول عن السياسة النقدية في البلاد، إضافة إلى إن السماح لمصارف أخرى إلى جانب المصرف المركزي بإصدار النقود الإلكترونية سوف يؤدي إلى خلل في السياسة النقدية من خلال عدم التوازن بين كل من النقود الإلكترونية والتقليدية وخصوصاً في ظل تعدد الجهات المصدرة. أما في حال حصر هذا الحق بالمصرف المركزي فهذا من شأنه أن يتحكم في عرض وإصدار النقود الإلكترونية بما ينسجم مع السياسة النقدية في البلاد.

النقطة الثانية: فيما يتعلق بإصدار وسائل الدفع الإلكتروني أو العمل في مجال الدفع الإلكتروني فإن هذا الأمر على خلاف مسألة إصدار النقود الإلكترونية فهو نوع من إصدار وسائل تسهم في تسهيل معاملات الأفراد كما الحال في إصدار الشيكات كوسيلة لتسهيل معاملات الأفراد. وبالتالي يجوز لأي جهة خاصة أن تقوم بإصدار وسائل دفع إلكترونية أو العمل في مجال الدفع الإلكتروني وهذا ما ينبغي على من يعد مشروع قانون الدفع الإلكتروني في سورية أخذه في عين الاعتبار، وخصوصاً أن المشرع السوري قد نص على إحداث الشركة السورية للمدفوعات الإلكترونية^١ والتي مهمتها توفير البنى التحتية اللازمة للدفع الإلكتروني، كما أن القرارات الصادرة

^١ راجع القانون رقم /١٣/ لعام ٢٠١٢ المتعلق بإحداث الشركة السورية للمدفوعات الإلكترونية.

عن مصرف سورية المركزي^١ أجازت الترخيص لشركات سورية تعمل في مجال الدفع الإلكتروني بالتعاون مع المصارف العاملة والمؤسسات المالية المصرفية كما حدد مصرف سورية المركزي أن غاية هذه الشركات تنحصر في مجال نشاط الدفع الإلكتروني وفقاً للشروط والضوابط التي يحددها المصرف المركزي.

٢- القوة الإبرائية للنقود الإلكترونية.

نظراً لأهمية هذا الموضوع سوف نتحدث عن القوة الإبرائية للنقود التقليدية ومن ثم ننتقل للحديث عن القوة الإبرائية للنقود الإلكترونية.

أ- القوة الإبرائية للنقود التقليدية:

نص قانون النقد الأساسي على أنه: "إصدار الأوراق النقدية والمسكوكات الذهبية والفضية والقطع النقدية المعدنية امتياز ينحصر بالدولة ويمارس مصرف سورية المركزي هذا الامتياز وفقاً لأحكام هذا القانون^٢.

كما نص ذات القانون على أنه: "تعتبر أوراقاً نقدية بموجب هذا القانون الأوراق لحاملها المحررة بالليرات السورية التي يصدرها مصرف سورية المركزي تنفيذاً لأحكام هذا القانون.

^١ راجع القرار رقم ٥٢/ تاريخ ٢٠١٩/٨/٢ المتضمن شروط الترخيص لتأسيس شركات تعمل في مجال الدفع الإلكتروني.

^٢ المادة/١٤/ من قانون النقد الأساسي رقم ٢٣/ لعام ٢٠٠١.

يكون لهذه الأوراق صفة التداول القانوني وقوة إبرائية غير محددة لتسديد جميع الديون العامة والخاصة^١.

نستنتج من النصوص السالفة الذكر أن المشرع السوري أعطى حق إصدار النقود التقليدية للمصرف المركزي وأعتبر هذا الحق من الحقوق الحصرية التي لا يمكن المساس بها تحت طائلة المسؤولية الجزائية^٢ وقد منح المصرف المركزي هذا الحق باعتباره مصرف الدولة والمسؤول عن السياسة النقدية في البلاد. وقد ترتب على منح المصرف المركزي هذا الحق إعطاء النقود التقليدية المحررة بالليرة السورية بفئاتها المختلفة صفة التداول القانوني أي أنه يحظر على أي شخص أن يتعامل داخل الأراضي السورية بغير الليرة السورية كما تتمتع هذه النقود بقوة إبرائية غير محددة لتسديد كافة الديون العامة والخاصة.

ولكن تجدر الإشارة إلى أن النقود التقليدية تفقد قوتها الإبرائية وتنزل من التداول في حال لم تقدم للتبديل قبل انتهاء المهلة المحددة وذلك بالنسبة للأوراق المنقوصة أو المشوهة وفقاً للشروط والضوابط التي حددها القانون^٣.

ب- القوة الإبرائية للنقود الإلكترونية:

يسعى كل من المستهلك والتاجر في نطاق استخدام النقود الإلكترونية إلى حصول كل طرف على حقه، لذلك كثيراً ما يهتم المستهلك بالقوة

^١ المادة/١٥/ من قانون النقد الأساسي رقم /٢٣/ لعام ٢٠٠١.

^٢ المادة(٣/١٤) من قانون النقد الأساسي رقم /٢٣/ لعام ٢٠٠١.

^٣ المواد(١٨-١٩-٢٠) من قانون النقد الأساسي رقم /٢٣/ لعام ٢٠٠١.

الإبرائية للنقود الإلكترونية بغية تمكنه من الحصول على السلعة أو الخدمة ولعل التساؤل الذي يطرح نفسه في هذا المجال يتجلى حول: هل تعد النقود الإلكترونية وسيلة دفع نهائية تبرئ ذمة المستهلك من دينه تجاه التاجر أم أن السداد يتوقف على عمل آخر يلي انتقال الوحدات الإلكترونية من المستهلك إلى التاجر؟

لقد ظهر لدينا في هذا الخصوص اتجاهين:

الأول^١: انتقال الوحدات الإلكترونية لا يعد دفعاً بالمعنى الصحيح أي أنه لا تبرأ ذمة المستهلك بمجرد انتقال الوحدات إلى التاجر. استناداً إلى أن انتقال الوحدات من المستهلك إلى التاجر لا يكون بغرض الدفع النهائي بل بغرض تحويلها بعد ذلك لنقود حقيقية مباشرة بعد كل عملية أو بعد فترة تخزين فيها هذه الأموال لدى التاجر في حسابه لدى المصرف، ولا تتمتع هذه الوحدات قبل تحويلها لنقود حقيقية بأي قوة إبراء قانوني. وبالتالي تظل ذمة المستهلك مشغولة بالدين إلى أن يتم تحويل هذه الوحدات إلى نقود حقيقية، فالوفاء النهائي لدى أنصار هذا الاتجاه لا يكتمل إلا بالتحويل لنقود حقيقية.

الثاني^٢: انتقال الوحدات الإلكترونية يعد دفعاً بالمعنى الصحيح يتجه أنصار هذا الاتجاه إلى القول بأن انتقال الوحدات الإلكترونية من المستهلك إلى التاجر يعد دفعاً نهائياً وحالاً لدين المستهلك،

^١ مشار إليه لدى: نورا الجزراوي، أثر استعمال النقود الإلكترونية على العمليات المصرفية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط للدراسات العليا، الأردن، ٢٠١١، ص ٥٠.

^٢ د. شريف غنام، مرجع سابق، ص ١٢٣.

فكما أن النقود التقليدية وسيلة دفع نهائية في حال انتقالها من المدين إلى الدائن يجب النظر إلى الوحدات الإلكترونية بنفس الكيفية. حيث أن انتقال الوحدات من أداة الدفع الموجودة لدى المستهلك وهذه الزيادة في رصيد التاجر تعني أن الأخير أصبح مالك لهذه الوحدات وليست ملك للمستهلك، والتاجر بإمكانه أن يستبدلها بنقود حقيقية أما المستهلك لا يمكنه ذلك.

أما بالنسبة لموقف المشرع السوري فقد نص قانون المعاملات الإلكترونية على أنه: «يعد الدفع الإلكتروني وسيلة مقبولة لانقضاء الالتزام وفق القواعد العامة»^(١).

وبذلك يكون المشرع السوري قد اعترف بوسائل الدفع الإلكتروني كأداة وفاء ولكن هذا لا يعني أنه ناصر أيّاً من الاتجاهين السابقين، فقد نص ذات القانون على أنه: «يخضع الدفع الإلكتروني إلى قانون النقد الأساسي والقوانين الناظمة لعمل مصرف سورية المركزي وقوانين العمل المصرفي والإجراءات والضوابط التي يضعها مصرف سورية المركزي»^(٢).

ومن المعلوم أن قانون النقد الأساسي حصر إصدار العملة بالمصرف المركزي وبذلك يكون قد استعد لإعطاء قوة الإبراء القانونية للنقود الإلكترونية، أما بخصوص مدى اعتبار الوفاء بالنقود الإلكترونية وفاءً نهائياً فإنه متروك لقرارات مصرف سورية المركزي لتعالج كل وسيلة على حدة.

^١ المادة /١٥/ من قانون المعاملات الإلكترونية رقم /٣/ لعام ٢٠١٤.

^٢ المادة /١٦/ من قانون المعاملات الإلكترونية رقم /٣/ لعام ٢٠١٤.

ونحن من جانبنا نؤيد الاتجاه الثاني ونرى أنه الأصح، حيث أن انتقال الوحدات الإلكترونية يعد دفعاً نهائياً ومبرئاً للذمة دون انتظار تحويلها لنقود حقيقية وذلك للحجج التي ساقها أصحاب هذا الاتجاه. ويضاف إليها أن الاتفاق ملزم لجميع الأطراف وبما أن الاتفاق المبرم بين المستهلك والتاجر (عقد بيع) ينص على قبول سداد الثمن بالوحدات الإلكترونية، فهذا يدل على أنه بمجرد انتقال الوحدات من المستهلك إلى التاجر يكون المستهلك قد نفذ التزامه وبرأت ذمته. كما أن النقود الإلكترونية قد وجدت لتكون أداة دفع جديدة كبديل عن النقود الحقيقية في إجراء الصفقات المنخفضة القيمة. وعلى ذلك إذا لم يؤخذ بهذا الإجراء فإن مستقبل النقود الإلكترونية سيكون في طور التراجع ولن يرى أي تطور إذا أخذنا برأي أصحاب الاتجاه الأول.

٣-وظائف النقود الإلكترونية.

لعل السؤال الذي أثار الجدل الفقهي هو: هل تؤدي النقود الإلكترونية ذات الوظائف التي تؤديها النقود الحقيقية؟

وفي سبيل الإجابة عن هذا السؤال ظهرت لدينا عدة نظريات:

أ- النقود الإلكترونية صيغة غير مادية للنقود الورقية:

تتعلق هذه النظرية^١ من مبدأ أن النقد هو رمز يمثل القيمة ذاتها، حيث تطور التمثيل المادي للنقود عبر التاريخ من المقايضة إلى

^١ ناهد الهندي، النظام القانوني للنقود الإلكترونية، رسالة ماجستير، كلية الحقوق، منشورات جامعة دمشق، دمشق، ٢٠١١، ص ١٣٧ + فراس بلحة، محفظة النقود الإلكترونية، رسالة ماجستير، منشورات كلية الحقوق، جامعة دمشق، دمشق، ٢٠١٥، ص ٣٧.

العملات المعدنية ثم إلى الورقية وظهر في العصر الحاضر استخدام النقود الإلكترونية والتي تعتبر أكثر صور النقود حداثة وتعقيداً. حيث يفسر أصحاب هذا الرأي أن الفرق الجوهرى بين النقود الإلكترونية وصدور النقود التقليدية هو أن النقود لم تأخذ الشكل المادي بل أصبحت مجرد انتقال المعلومات بين أطراف التبادل. وبناءً على ذلك تعتبر هذه النظرية أن النقود الإلكترونية صيغة غير مادية للنقود الورقية. إذ أن إصدار النقود الإلكترونية يتم من خلال تحويل شكل النقود من الصيغة الورقية إلى الصيغة الإلكترونية فهي إحلال شكل للنقود محل شكل آخر^١.

في الحقيقة تنتقد هذه النظرية كونها تثير مشاكل واقعية، إذ أن النقود التقليدية التي تدفع لشحن البطاقة بالنقود الإلكترونية وفقاً للنظرية السابقة - تبقى داخل النظام النقدي وتضاف إلى أصول مصدر تلك النقود الإلكترونية مما يؤدي إلى وجود ازدواج في الكتلة النقدية بحيث يمكن لكل من صاحب النقود ومصدرها استعمالها بشكل متزامن مما يؤدي إلى مشاكل جمة.

ب- النقود الإلكترونية أداة تبادل وليست أداة دفع:

يعتبر أصحاب هذا الرأي^٢ أن الاختلاف الجوهرى بين النقود التقليدية والنقود الإلكترونية يكمن في أن النقود الإلكترونية تصدر عن مؤسسات خاصة بينما النقود التقليدية تصدر من قبل

^١ Dave Chaffey, E. business and E. commerce Management, strategy, implementation and practice, third Edition, prentice Hall, New jersey, U.S. 2006,p15 .

^٢ مشار إليه لدى نادر شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس،

لبنان، ٢٠٠٧، ص ٩٦+ نور الجزراوي، مرجع سابق، ص ٤٥.

المصرف المركزي. وتستند هذه النظرية إلى التفرقة بين أدوات الدفع (means of payment) وأدوات التبادل (medium of exchange) انطلاقاً من أن استخدام أدوات التبادل يؤدي إلى إتمام عملية البيع إلا أنه يتطلب عملية إضافية تتمثل بالدفع النهائي بين مختلف عمليات التبادل.

حيث تعتبر هذه النظرية أن إصدار النقود الإلكترونية نوع من بيع أصول المصدر لأنها تشتري من المصدر مقابل مبلغ معادل من النقود التقليدية. أي يتم شراء إصدارات النقود الإلكترونية بما يعادل من النقود التقليدية الصادرة عن المصرف المركزي. أي بمعنى آخر هي عملية شراء نقود بنقود أخرى. وتنتهي حياة النقود الإلكترونية حينما يقوم باستردادها وذلك بالتصرف كمشتري لها من البائعين الذين تلقوها نظير مبيعاتهم.

وتتقد هذه النظرية كونها تلزم مؤسسات الإصدار أن تحتفظ (بالنقود التقليدية) التي تلقتها مقابل بيع النقود الإلكترونية وهذا ما يشكل تقييداً لقدرة تلك المؤسسات على إصدار هذه النقود.

ج- النقود الإلكترونية أداة ائتمان:

يعتبر أصحاب هذه النظرية^١ أن كافة صور النقود الإلكترونية هي شكل من أشكال الائتمان التي تستخدم كأداة تبادل. أي أن العملة تعتبر أداة ائتمان لأنها تشكل ديناً على الحكومة التي أصدرتها وتعتبر النقود الإلكترونية ائتمان لأنها عبارة عن رصيد مسجل

^١ د. أحمد سفر، مرجع سابق، ص ٦٨.

إلكترونياً ويصبح الالتزام القانوني على مصدر هذه النقود هو المقابل بين الوحدات النقدية وبين الوحدات الإلكترونية وهذا يشبه الالتزام القانوني الواقع على الحكومة في مواجهة حائز العملة المتمثل في قطعة العملة ذاتها.

يؤخذ على هذه النظرية أنها تجاهلت وظيفة النقود الأساسية سواء أكانت نقود إلكترونية أم تقليدية بأنها أداة وفاء قبل كل شيء.

د- النقود الإلكترونية صورة افتراضية لتدقق ثلاثي الأقطاب:

يعتبر أصحاب هذا الاتجاه^١ أن الأموال التي يتلقاها مُصدرو النقود الإلكترونية هي عبارة عن ودیعة مصرفية لدى طرف ثالث إذ أن إصدار النقود الإلكترونية والإيداع لدى مصدرها لا يشكلان عملية واحدة بل يجب التمييز بين عمليتين هما: عملية تقديم الوديعة وعملية إصدار النقود الإلكترونية. فصاحب الحساب يقرض الأموال لمصدر النقود الإلكترونية حيث يعتبر هذا الأخير مدينًا للأول. وعندما تصدر النقود الإلكترونية لا تعطى لصاحب الحساب على سبيل الحيابة النهائية وإنما على سبيل القرض.

حيث يعتبر أصحاب هذا الرأي أن حياة النقود الإلكترونية تمر بثلاثة مراحل:

المرحلة الأولى: الإصدار لصالح صاحب الحساب أو لصالح صاحب البطاقة.

^١ مشار إليه لدى: ناهد الهندي، مرجع سابق، ص ١٣٩ + نور الجزراوي، مرجع سابق، ص ٤٦.

المرحلة الثانية: الانتقال من صاحب البطاقة إلى طرف ثالث (البائع) الذي انتقلت إليه النقود الإلكترونية.

المرحلة الثالثة: تدمير النقود الإلكترونية عن طريق قيام الطرف الثالث باسترداد مقابلها من النقود التقليدية من مصدر النقود الإلكترونية^١.

وعليه لا تعتبر النقود الإلكترونية أصلاً مالياً حسب هذه النظرية وإنما صورة افتراضية للدورة الكاملة التي تشكل إيداع النقود التقليدية وإصدار نقود إلكترونية ثم تدميرها عند إجراء كل عملية من عمليات الدفع النقدي^٢.

ونحن من جانبنا نرى أن النقود الإلكترونية لا تختلف بجوهرها الوظيفي عن النقود التقليدية. فهي تؤدي ذات الوظائف التي تؤديها النقود التقليدية فالنقود الإلكترونية يمكن أن تكون:

— وسيطاً للتبادل: بحيث يمكن لحاملها أن يقوم بمبادلتها بالسلع والخدمات التي يرغب بشرائها.

— مقياس للقيم: إذ يمكن قياس السلعة بكمية النقود الإلكترونية التي يجري الدفع للحصول عليها.

— مخزن للقيمة: على الرغم من أنها لا تدر فوائد وبالتالي غير قابلة لأن توضح كوديعة إلا أن مستخدميها يعدونها مخزن للقيمة

^١ نادر شافي، مرجع سابق، ص ٩٤ - ١٠٠.

^٢ Dave Chaffey .op .cit, p 25

فمن الممكن تأجيل تبادلها في مقابل السلع والخدمات إلى وقت لاحق في المستقبل.

إذاً يمكن القول أن النقود الإلكترونية تقوم بذات الوظائف التي تقوم بها النقود التقليدية على الرغم من وجود بعض الفوارق الشكلية بين النوعين فالنقود التقليدية تصدر عن المصرف المركزي مما يمنحها قوة إبرائية قانونية بخلاف النقود الإلكترونية التي تصدر من قبل جهات خاصة مما يمنحها قوة إبرائية اتفاقية فضلاً عن كون النقود التقليدية تحظى بقبول واسع وعام لدى الجميع بخلاف النقود الإلكترونية التي ما زال التعامل بها محدود في ظل حادثة انتشارها. وبالنتيجة يمكننا أن نجد أن النقود الإلكترونية هي باختصار حسيطة التزاج بين القطاع المصرفي وثورة تكنولوجيا المعلومات والاتصالات فهي عبارة عن المكافئ الإلكتروني للنقود التقليدية.

٤- مركز النقود الإلكترونية.

لعل السؤال الذي يطل بظلاله في هذا المجال هو هل تعد النقود الإلكترونية نوعاً جديداً يضاف إلى جانب النقود الورقية والنقود الكتابية أم أنه يندرج ضمن هذه الأنواع؟

تتجلى أهمية الإجابة على هذا السؤال في تحديد النظام القانوني الذي ينطبق على النقود الإلكترونية فإذا كانت تنتمي إلى نوع معين من هذين النوعين انطبق عليها النظام القانوني الخاص بهذا النوع. أما إذا كانت تشكل هذه النقود نوعاً جديداً يخرج عن النوعين المعروفين فيجب أن يحكمها نظام قانوني يتماشى مع

طبيعتها الخاصة. بدايةً ينبغي أن نشير إلى أن الفقهاء الذين تناولوا هذه المسألة كانوا متفقين على أن النقود الإلكترونية تقوم بذات وظائف النقود التقليدية لكن نقطة الخلاف تركزت حول مكانة هذه النقود.

حيث يرى بعض الفقه^١ أن النقود الإلكترونية ليست سوى نقود مكتوبة فهي لا تكون في صورة مادية وإنما في صورة أرقام تقيّد في الجانب المدين للعميل الذي يسدد بها وتقيّد في الجانب الدائن للتاجر الذي قبل السداد بها، وهي بذلك تتشابه مع التحويلات البنكية ولكن تختلف النقود الإلكترونية عن التحويلات البنكية في أن النقود تصدر وتتداول بشكل إلكتروني بينما التحويلات البنكية تتم بنقود حقيقية.

في حين اتجه جانب آخر من الفقه^٢ إلى أن النقود الإلكترونية نوع جديد من النقود ويتمتع بخصوصية تجاه النقود الورقية والنقود المكتوبة وهذه الخصوصية تعود إلى أمرين:

الأول: أن التاجر بعد أن يحصل على الوحدات الإلكترونية من العميل يطلب من المصدر تحويلها إلى نقود ورقية أو مكتوبة الأمر الذي يعني وجود اختلاف بين هذه النقود.

الثاني: التاجر يعتبر دائن للعميل وبوصول الوحدات الإلكترونية إلى التاجر، يكون الأخير قد استوفى حقه فالتاجر ليس دائن

^١ نهى الموسوي وإسراء الشمري ، النظام القانوني للنقود الإلكترونية، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية، العراق، المجلد ٢٢، العدد الثاني، ٢٠١٤، ص ٦٩.

^٢ شريف غنام، مرجع سابق، ص ٣٩.

للمصدر وليس له الحق بمطالبة المصدر بالسداد بل كل ما هنالك أن للتاجر الحق في مطالبة المصدر بتحويل الوحدات الإلكترونية إلى نقود ورقية أو مكتوبة.

ومن جانبنا نميل إلى الاتجاه الذي يعتبر النقود الإلكترونية نوع جديد وذلك استناداً للحجج التي أوردها أنصار هذا الاتجاه إضافة إلى أن النقود الإلكترونية تتم بشكل إلكتروني وتقبل التحويل إلى نقود ورقية وهذا الشكل الإلكتروني يعتبر الفيصل في تمييز النقود الإلكترونية عن النقود التقليدية الأمر الذي يتطلب خضوعها لنظام قانوني خاص بها شأنها في ذلك شأن العقد الإلكتروني وفضلاً عن ذلك فإن من أهم خصائص العقد الإلكتروني ظهور وسائل دفع خاصة به. (محفظة النقود الإلكترونية - الشيك الإلكتروني ...الخ) والتي تعتبر إحدى أهم نتائج الثورة التقنية وثورة الاتصالات. وبما أن هذه الوسائل خاصة بالعقد الإلكتروني فهذا يعني أن لها نظام قانوني خاص ومستقل عن كافة أنواع النقود الأخرى.

إذاً وبعد أن تعرفنا على مشكلات الشراء عبر الحدود كأحد المشكلات القانونية التي تواجه المستهلك ننقل للحديث عن شكل آخر من هذه المشكلات ألا وهي المشكلات التي تواجه المستهلك الإلكتروني كمتعاقد.

الفرع الثاني

المشكلات التي تواجه المستهلك الإلكتروني كمتعاقد

يُقصد بالمستهلك: ((كل شخص طبيعي أو اعتباري يشتري سلعاً استهلاكية بأنواعها المختلفة غذائية كانت أو زراعية أو صناعية بهدف التغذية أو لاستخدامها لأغراضه الشخصية أو المنزلية أو الذي يستفيد من أي خدمة مقدمة من فرد أو مجموعة من الأفراد أو من شخص اعتباري في مختلف المجالات المنصوص عليها في هذا القانون^(١))).

هذا فيما يتعلق بتعريف المشرع السوري للمستهلك بشكل عام، ولكن المشرع السوري لم يكتف بهذا التعريف فقد عرف قانون المعاملات الإلكترونية المستهلك الإلكتروني بأنه: ((كل شخص طبيعي يشتري أو يستأجر سلعاً أو يستفيد من خدمة بوسائل إلكترونية وذلك لأغراض لا تدخل في نشاطه الاقتصادي الاحترافي^(٢))).

نستنتج من التعريفين السابقين أن المستهلك الإلكتروني يتميز عن المستهلك التقليدي من ناحية الوسيلة الإلكترونية المستخدمة، وقد كان لهذا العنصر التقني أثرٌ سلبيٌّ بالنسبة للمستهلك الإلكتروني. حيث كان من شأن هذه الوسيلة الإلكترونية أن تضعه أمام جملة من التحديات والمشكلات التقنية الناتجة عن هذا العنصر التقني. وحيث أن المستهلك الإلكتروني هو المكافئ الإلكتروني للمستهلك التقليدي فكان من الطبيعي أن يتعرض المستهلك الإلكتروني لجملة من المشكلات

^١ المادة الأولى من قانون التجارة الداخلية وحماية المستهلك رقم ١٤/ لعام ٢٠١٥.

^٢ المادة الأولى من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

والتحديات الناتجة عن عقد الاستهلاك أو عقد البيع. وبالتالي نجد أن المستهلك الإلكتروني أمام نوعين من المشكلات:

❖ مشكلات تقنية خاصة به ناتجة عن دخول العنصر التقني ومثالها (الجانب السلبي للتطور التقني وافتقار المستهلك للتطوير المعلوماتي).

❖ مشكلات قانونية عامة تصيب أي مستهلك سواء أكان مستهلك إلكتروني أم تقليدي كونها ناشئة عن عقد الاستهلاك بحد ذاته (كالمشكلات المتعلقة بالشروط التعسفية وانتشار الإعلانات التجارية المضللة).

لذلك وفي سبيل تسليط الضوء على هذه المشكلات سوف نتحدث عن المشكلات التقنية (أولاً) على أن نتعرف على المشكلات القانونية (ثانياً).

أولاً: المشكلات التقنية

تتمثل بالمشكلات التي تواجه المستهلك في إطار التعاقدات الإلكترونية كونها ناتجة عن دخول العنصر التقني، والتي من شأنها أن تزعزع ثقة المستهلك بالتعاملات الإلكترونية وتدفعه إلى الإحجام عن هذه التعاملات. وتتجلى في الآتي:

١- الجانب السلبي للتطور التقني: أفرز التطور التقني العديد من الوسائل الإلكترونية المتطورة وعلى رأسها الإنترنت، والتي من خلالها يمكن للمستهلك الوصول إلى العديد من السلع والخدمات بطريقة سهلة توفر الوقت والجهد. ويمثل التطور التقني في هذا الجانب واقعاً علمياً يأتي كل لحظة بالجديد مما ينبغي أن يقود إلى

تحسين الروابط التجارية بين التاجر والمستهلك بهدف الحصول على أفضل الأداء للممارسات التجارية الإلكترونية. غير أن الجانب السلبي لهذا التطور التقني يتجسد في قهر المستهلك بطريقة تبدو عدائية مما ينبغي أن يؤثر على الوصف القانوني لعقد التجارة الإلكترونية مقارنة بالبيع الذي يتم في موطن ومحل إقامة المستهلك. ويتمثل هذا الجانب السلبي في عدم قدرة المستهلك على معاينة السلعة أو المبيع بطريقة حقيقية أو الالتقاء مع التاجر في مجلس عقدي تقليدي^١.

٢- حاجة المستهلك إلى الخدمات الإلكترونية: يؤدي افتقار المستهلك للخدمات الإلكترونية إلى جعله عاجزاً عن التفاعل مع المواقع التجارية عبر شبكة الإنترنت، والمقصود بذلك عدم اكتراث المستهلك بالمواقع التجارية عبر شبكة الإنترنت بسبب قلة الحاجة لهذه المواقع. ولكن مع التطور التقني الحاصل أصبح لهذه المواقع أهمية كبيرة ذلك أنها قدمت للمستهلك العديد من الخدمات (كالخدمات العقارية والسياحية والمصرفية وبيع تذاكر الطيران والفنادق). فحاجة المستهلك إلى الخدمات الإلكترونية الضرورية تنبع من كونها توفر منتجات وخدمات ذات جودة عالية وأسعار معقولة بسبب كثرة المواقع الإلكترونية التجارية وبالتالي زيادة المنافسة بين هذه المواقع لتقديم الأفضل بالإضافة إلى الخدمات الممتازة لعمليات ما بعد البيع^٢. فأهمية الخدمات الإلكترونية الموجودة على شبكة الإنترنت تزيد من إقبال

^١ سهام إمدالو و ليلي الحسن، حماية المستهلك الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميره - بجاية، الجزائر، ٢٠١٢-٢٠١٣، ص ٢٢.

^٢ د. طارق كميل، حماية المستهلك في التعاقد عبر شبكة الإنترنت، بحث منشور في مجلة الجامعة العربية الأمريكية للبحوث، المجلد الأول، العدد الأول، الجزائر، ٢٠١٤، ص ٦٨.

المستهلكين على هذه الخدمات وتجعل منها محور طلب الكثير منهم ومن هنا كانت الحاجة إلى تأمين الحماية للمستهلك بشكل واضح وصريح.

٣-افتقار المستهلك إلى التنوير المعلوماتي التقني: تعتبر شبكة الإنترنت المنتشرة حول العالم نافذة مفتوحة أمام الملايين من الناس، فهذه الشبكة تمثل صالة عرض لكافة المنتجات والخدمات، فالبريد الإلكتروني ومواقع الإنترنت ووسائل التفاعل المباشر تتجه جميعها لتحقيق هدف واحد ألا وهو عرض أنواع متباينة من المنتجات والخدمات للمستهلك والتعاقد معه من خلالها. ف قدرة المستهلك على التعامل مع جهاز الحاسوب وشبكة الإنترنت تسهل عليه الوصول إلى المنتجات والخدمات التي يريدها. وهنا يجب أن نفرق بين إعلام المستهلك الذي يعد من حقوق المستهلك وبين معرفة المستهلك المعلوماتية بشبكة الإنترنت، فهذه الأخيرة تمثل الحد الأدنى من أجل وصول المستهلك إلى معلومات عن الخدمات والمنتجات، وهي تعبر عن قدرة المستهلك على التعامل مع جهاز الحاسوب وشبكة الإنترنت^١. فافتقار المستهلك إلى المعرفة التقنية المرتبطة بشبكة الإنترنت بالإضافة إلى المشكلات التي قد تواجه المستهلك عند التعمق في هذه الشبكة يؤدي إلى وقوعه بحيل وخداع قراصنة الإنترنت من خلال المواقع الوهمية.

^١ عبد الله محمود، حماية المستهلك في التعاقد الإلكتروني، رسالة ماجستير، كلية الحقوق، جامعة النجاح الوطنية، فلسطين، ٢٠٠٩، ص ٣٢.

ثانياً: المشكلات القانونية

وهي عبارة عن مجموعة من التحديات القانونية التي تواجه أي متعاقد سواء أكان تقليدي أم إلكتروني كونها ناشئة عن عقد الاستهلاك أو البيع وبغض النظر عن الوسيلة المستخدمة في التعاقد وتتمثل هذه المشكلات في الآتي:

١- عدم كفاية القواعد القانونية العامة المتعلقة بنظرية الالتزام لحماية المستهلك الإلكتروني: إن التاجر هو الطرف القوي الذي يمتلك آليات إدارة السوق الإلكترونية بما يتضح أمامه من المعرفة التامة بمفردات السوق، وبما يتفوق به من مركز اقتصادي قوي ومركز معلوماتي فائق التصور، في حين أن المستهلك في موقف ضعيف ويسعى للحصول على أفضل المنتجات والتزود بأحسن أداء للخدمات. ويبدو الموقف دقيقاً على المستوى القانوني ولاسيما في ظل التعاقد بين طرفين أحدهما المستهلك الذي لا يعرف عن الطرف الآخر إلا ما تسمح به التقنيات التي يملكها هذا الأخير، فضلاً عن وجودهم في دولتين مختلفتين فيكون المستهلك هو الأولى بالحماية تبعاً لذلك^١.

ولا ينبغي أن تكون هذه الحماية نسبية سواء في مرحلة التعاقد أم في مرحلة التنفيذ وإذا كانت المقدمات تعقبها النتائج، فإن مرحلة تكوين الرابطة العقدية هي الأكثر وجوباً للحماية القانونية لأنها الأكثر حساسية ودقة باعتبار أن محل التعاقد هو ميدان إلكتروني. وما يلاحظ هو قصور النظرية التقليدية للالتزامات عن حماية المستهلك

^١ فلاح العجمي، الحماية المدنية للمستهلك في العقد الإلكتروني، رسالة ماجستير، كلية الحقوق،

في العقد الإلكتروني. فمن خلال تحليل الرابطة القانونية بين المستهلك والتاجر من منظور النظرية العامة للالتزامات نجد أن نصوص القانون المدني قد تفلح في حماية المستهلك ولكنها لا تقصده. فالنظرية العامة للالتزامات لا تعرف وصف المستهلك ولا تأخذ بالحسبان عدم التوازن الاقتصادي بين الأطراف. فهي تحمي أحد أطراف العقد أصلاً لا وصفاً^١. فإذا تصادف وجود المستهلك في مركز من مراكز الحماية العامة التي حددها القانون المدني وفقاً لضوابطه شملته الحماية بوصفه متعاقد وليس مستهلك ولعل خير مثال على ذلك ما يلي:

أ- تفسير الشك لمصلحة المدين: فإذا تصادف وجود المستهلك في مركز المدين يستفيد من هذا المبدأ^٢.

ب- نظرية عقود الإذعان: وهي الأكثر انتشاراً في نطاق التعاملات الإلكترونية بهدف توفير الحماية الفعالة للمستهلك^٣.

ج- نظرية الظروف الطارئة: تقوم فلسفة القانون المدني على حماية الطرف المتضرر من الظروف الطارئ من منظور الصفقة التي أبرم في شأنها العقد فحسب إذ لا عبرة للمركز المالي للمضرور فقد يكون هو الطرف القوي اقتصادياً^٤. وقد أثبت الواقع أن حماية الجانب الضعيف اقتصادياً في العقد ليس هدفاً لفلسفة النظرية العامة

^١ المرجع السابق، ص ٥٨.

^٢ المادة ١٥٢/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٣ المادة ١٥٠/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٤ المادة ١٤٨/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

للالترامات في القوانين المدنية في حد ذاته، مما يبرر عدم كفاية هذه النظرية لحماية المستهلك في العقد الإلكتروني. وأمام هذا الواقع لابد للمشرعين من التدخل بنصوص قانونية خاصة لحماية المستهلك الإلكتروني.

٢- وجود بعض الشروط التعسفية في العقود الإلكترونية: يطغى على أشكال العقود الإلكترونية نماذج معدة مسبقاً يتولى إعدادها مختصون يتمتعون بالنفوق الاقتصادي والكفاءة الفنية، الأمر الذي يؤدي إلى وجود بعض الشروط التعسفية في هذه العقود. وفي سبيل الإحاطة الشاملة بهذه الشروط سوف نقوم بتعريفها وتحديد معيار الشرط التعسفي و نطاق تطبيقها وفقاً للآتي :

أ-تعريف الشروط التعسفية:

في الحقيقة لم يعرف المشرع السوري الشروط التعسفية في القانون وإنما اكتفى بالحديث عن سبل الحماية منها من خلال منح القاضي سلطة اعفاء المتعاقد منها أو تعديلها (وسوف نرجئ الحديث عنها إلى سبل حماية المستهلك الإلكتروني كمتعاقد).

أما بالنسبة للفقهاء:

فقد عرف الفقه الفرنسي الشرط التعسفي بأنه: «الشرط المحرر مسبقاً من جانب الطرف الأكثر قوة، ويمنح هذا الأخير ميزة فاحشة عن الطرف الآخر^(١)»

^(١) إيناس بن غيده، الحماية المدنية للمستهلك في العقود الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أو بكر بلقايد- تلمسان، الجزائر، ٢٠١٤-٢٠١٥، ص ٥١.

في حين عرف المشرع الجزائري الشرط التعسفي بأنه: «كل شرط أو بند بمفرده أو مشترك مع بند واحد أو عدة بنود أو شروط أخرى من شأنه إخلال بالتوازن الظاهر بين حقوق وواجبات أطراف العقد»^(١).

بينما عرف التوجيه الأوروبي الشرط التعسفي بأنه: «الشرط الذي يرد في العقد وينطوي على تفاوت جلي خلافاً لما يقضي به مبدأ حسن النية، وضد مصلحة المستهلك بين حقوق والتزامات الأطراف فيه على حساب المستهلك»^(٢).

وبناءً عليه يمكننا تعريف الشرط التعسفي بأنه: «كل شرط يقوم التاجر بإدراجه في العقد مستغلاً قوة مركزه الاقتصادي أو قوة نفوذه بهدف الحصول على ميزة مجحفة على حساب المستهلك مما يشكل إخلالاً بالتوازن العقدي»^(٣).

ب- معيار الشرط التعسفي: حتى نعتبر الشرط تعسفياً لا بد من توافر أمرين متلازمين:

أ- التعسف في استعمال السلطة الاقتصادية: يعتبر الشرط تعسفياً عندما تكون الميزة المجحفة التي مُنحت للتاجر نتيجة لتعسفه في استعمال سلطته الاقتصادية. والسلطة الاقتصادية هنا ليست مرادف للقوة بل هي عبارة عن الحالة التي يمثل فيها الشرط عدم تعادل جسيم. وعليه لا يكون هذا التفوق اقتصادي فقط، بل يمكن القول أن التفوق الفني أو التقني هو

^١ المادة (٥/٣) من قانون الممارسات التجارية الجزائري رقم/٠٤-٠٢/ لعام ٢٠٠٤.

^٢ المادة (١/٣) من التوجيه الأوروبي رقم/١٣/ الصادر في ٥ نيسان ١٩٩٣ بشأن الشروط التعسفية في العقود المبرمة مع المستهلكين.

الذي يمكن التاجر من فرض شروطه التعسفية^١. فالتاجر معتاد على إبرام هذه العقود ويعرف الحقوق والالتزامات المترتبة على العقد ويمتلك من الوسائل ما يمكنه من تحديد الالتزامات التي يستطيع تنفيذها، بالإضافة إلى الشروط التي يستطيع فرضها على من يتعاقد معه. ومثال ذلك الشروط المطبوعة مسبقاً والصيغ الموحدة للعقود المعدة من قبل التاجر ومن في حكمه. وفي هذا الصدد نص قانون الاستهلاك الفرنسي^٢ على أنه: (في العقود المبرمة بين المهنيين والمستهلكين تكون هذه العقود تعسفية في الحالات الآتية:

١- النص على التزام قاس على عاتق المستهلك في حين أن واجبات التاجر يتوقف تنفيذها على إرادته المنفردة.

٢- السماح للتاجر بالاحتفاظ بالمبالغ التي دفعها المستهلك الذي عدل عن تنفيذ أو إبرام العقد دون النص على حق المستهلك في الحصول على تعويض من التاجر يعادل ضعف المبلغ الذي دفعه المستهلك إذا كان التاجر هو من عدل عن العقد.

٣- فرض تعويض مبالغ فيه على المستهلك الذي لا يلتزم بالوفاء بالتزاماته.

٤ - إعطاء التاجر الحق بإنهاء العقد دون إشعار معقول.

^١ فلاح العجمي، مرجع سابق، ص ٨٤.

^٢ المادة (٢/١٣٢) من قانون الاستهلاك الفرنسي المعدل بتاريخ ٣٠ يناير ٢٠٢٠ وقد عدلت هذه المادة عام ٢٠٠٩ وألغيت الفقرة الثامنة منها عام ٢٠١٦.

٥- السماح للتاجر في التنازل عن عقده دون إرادة المستهلك مما يؤدي إلى انخفاض حقوق المستهلك.

٦- إعطاء التاجر الحق بتعديل العقد من جانب واحد فيما يتعلق بحقوق والتزامات الطرفين.

٧- تحديد تاريخ إرشادي لتنفيذ العقد من الحالات التي يسمح بها القانون.

٩- الحد دون مبرر من الأدلة المتاحة للمستهلك.

١٠- عرقلة ممارسة المستهلك لحقه في اتباع الإجراءات القانونية وسبل الانتصاف.

يستنتج من النص السابق أن الشروط التي تنشئ من حيث موضوعها أو الآثار المترتبة عليها اختلالاً عقدياً بما يحقق مصلحة التاجر على حساب المستهلك نتيجة تعسف التاجر في استعمال سلطته هي شروط تعسفية. كما أن هذه الأحكام تعد محلاً للتطبيق مهما كان شكل العقد أو الوسيط الذي يتم من خلاله حيث جاء النص بصيغة عامة أي أن الشرط التعسفي يمكن أن يرد في العقد الإلكتروني والعقد التقليدي على حد سواء.

ب- وجود الميزة المجففة: لنكون أمام شرط تعسفي لا بد من حصول التاجر على ميزة مجففة عند استخدامه لنفوذته الاقتصادية في تعاقدته مع المستهلك، وهذا يعني أن الميزة المجففة هي نتيجة لهذا الاستخدام التعسفي. وقد انتقد مصطلح

الميزة المجففة واعتبر غامضاً وليس محدداً ولكنه يبقى قريباً من النصوص العامة التي تعاقب على الغبن، فكلاهما يعبر عن الفكرة نفسها وهي الضرر اللاحق بالعلاقة العقدية غير أن الاختلاف يكمن في محل التعسف، ففي الغبن يتجسد محل التعسف بالثمن بينما في الشروط التعسفية ينصب على شروط تبعية تتعلق بتنفيذ العقد^١. وفي هذا الصدد نص قانون الممارسات التجارية الجزائري^٢ على أنه: «تعتبر بنوداً أو شروطاً تعسفية في العقود بين المستهلك والبائع ولاسيما البنود أو الشروط التي تمنح الأخير:

- ١- أخذ حقوق و/أو امتيازات لا تقابلها حقوق و/أو امتيازات مماثلة معترف بها للمستهلك.
- ٢- فرض التزامات فورية ونهائية على المستهلك في العقود في حين أنه يتعاقد هو بشروط يحققها متى أراد.
- ٣- امتلاك حق تعديل عناصر العقد الأساسية أو مميزات المنتج المسلم أو الخدمة المقدمة دون موافقة المستهلك.
- ٤- التفرد بحق تفسير شرط أو عدة شروط من العقد أو التفرد في اتخاذ قرار البت في مطابقة العملية التجارية للشروط التعاقدية.
- ٥- إلزام المستهلك بتنفيذ التزاماته دون أن يلزم نفسه بها.
- ٦- رفض حق المستهلك في فسخ العقد إذا اخل هو بالالتزام أو عدة التزامات في ذمته.

^١ فلاح العجمي، مرجع سابق، ص ٨٥.

^٢ المادة ٢٩/ من قانون الممارسات التجارية الجزائري رقم ٠٤/٠٢ لعام ٢٠٠٤.

- ٧- التفرد بتغيير آجال تسليم المنتج أو آجال تنفيذ خدمة.
- ٨- تهديد المستهلك بقطع العلاقة العقدية لمجرد رفض المستهلك الخضوع لشروط تجارية جديدة غير متكافئة.
- نستنتج من النص السابق أن الشروط التي تمنح البائع (التاجر) أية مزايا لا يقابلها مزايا مماثلة بالنسبة للمستهلك تشكل نوعاً من الشروط التعسفية كون هذه الشروط تجعل التاجر منفرداً بميزة محفة بحق المستهلك نتيجة استغلال التاجر لقوة نفوذه الاقتصادي.

ويثور التساؤل حول مدى التشابه بين عقد الإذعان والشرط التعسفي وذلك على اعتبار أن كل من عقد الإذعان والشرط التعسفي بصيغة قالب موحد وجاهز؟

ينبغي أن نشير إلى أن معظم عقود الإذعان تحتوي شروط تعسفية حيث تظهر في قالب جامد وموحد وليس للطرف الآخر أي حرية في التفاوض أو تعديل بنود العقد. فإما أن يقبل العقد بشكل كامل أو أن يرفضه كاملاً. ولكن يتميز عقد الإذعان عن الشرط التعسفي بأن عقد الإذعان عقد قائم بحد ذاته، أي يتعلق بتوافق إرادتي الطرفين حيث يهيمن الطرف القوي اقتصادياً على شروط العقد دون أن تكون للطرف الضعيف فرصة أن يعدل شرط من شروطه، أما الشرط التعسفي فهو شرط وارد في العقد المراد إبرامه يغطي المسائل المتعلقة به أو يقتصر على بعضها أي أنه لا يعتبر عقد حقيقي قائم بذاته^١.

^١ عبد الله محمود، مرجع سابق، ص ٧٢.

أضف إلى ذلك أن معيار عقد الإذعان هو توفر ثلاثة شروط تتمثل
ب:

- أن يظهر بصيغة موحدة لكافة الجمهور.
- أن يتعلق بسلعة ضرورية.
- وجود احتكار فعلي أو قانوني للسلعة أو الخدمة مما يجعل المنافسة محدودة الأمر الذي يجعل الطرف الآخر أمام أحد خيارين إما القبول أو الرفض دون حق التعديل.

أما الشرط التعسفي فهو يتطلب عنصرين هما:

- التعسف في استعمال السلطة الاقتصادية.
- وجود الميزة المجحفة.

ج- نطاق تطبيق الشرط التعسفي: يقتضي تحديد مفهوم الشرط التعسفي تحديد مجال تطبيقه، فهل يسري الشرط التعسفي على عقد معين (كعقد البيع فقط) أم يمتد إلى باقي العقود؟

نص قانون الممارسات التجارية الجزائرية على أنه: «تعتبر بنوداً أو شروطاً تعسفية في العقود بين المستهلك والبائع.....الخ»^(١).

كما نص قانون الاستهلاك الفرنسي على أنه: «في العقود المبرمة بين المهنيين والمستهلكين تكون هذه العقود تعسفية.....الخ»^(٢).

^١ المادة /٢٩/ من قانون الممارسات التجارية الجزائري رقم /٠٢-٠٤/ لعام ٢٠٠٤.

^٢ المادة (٢/١٣٢) من قانون الاستهلاك الفرنسي المعدل بتاريخ ٣٠ يناير ٢٠٢٠ وقد عدلت هذه المادة عام ٢٠٠٩ وألغيت الفقرة الثامنة منها عام ٢٠١٦.

وعليه يمكن القول أن المشرع الجزائري قد قصد عقود البيع المبرمة بين المستهلك والبائع (التاجر) أي أنه استبعد العقود المبرمة بين التاجر أنفسهم، وفي هذا حماية واضحة للمستهلك، وهو نفس الموقف الذي اتجه إليه المشرع الفرنسي الذي يشترط لاعتبار الشرط تعسفياً أن يظهر في عقد مبرم نهائي بين المهني (التاجر) والمستهلك.

وبهذا الصدد فقد صدر حكم من محكمة النقض الفرنسية بتاريخ ١٠/١٠/١٩٩٦ في قضية فحواها: أن مؤسسة (Chrompost) لم تقم بتقديم الطرد المرسل عن طريقها في الوقت المناسب، وقد أدرجت هذه المؤسسة في عقودها النموذجية شرطاً محدداً للمسؤولية وحيث أن الزبون كان مؤسسة، فإن محكمة النقض لم تعتبر هذا الشرط تعسفياً، وإنما اعتبرته شرط محدد للمسؤولية^١.

كما أن كلا المشرعين الجزائري والفرنسي جاء بصيغة عامة أي أنهم لم يشترطوا شكلاً معيناً في العقد فقد يكون تقليدياً أو إلكترونياً وأياً كان محله منقول أو عقار.

ولكن من جهة أخرى، فإن المشرع الجزائري قد حصر نطاق تطبيق المادة ٢٩/ على عقود البيع فقط دون العقود الأخرى وذلك من خلال استخدام مصطلح في العقود بين البائع والمستهلك، على خلاف المشرع الفرنسي الذي عمم تطبيق المادة ١٣٢/ على كل العقود سواء أكانت بيعاً أم إيجاراً أم قرض... الخ وذلك من خلال استخدام مصطلح في العقود بين المهنيين والمستهلك.

^١ مشار إليه لدى: إيناس بن غيده، مرجع سابق، ص ٥٤.

وفي ظل عدم تنظيم المشرع السوري لمفهوم الشروط التعسفية فإننا نأمل من المشرع السوري إدراج مادة قانونية في قانون المعاملات الإلكترونية تتعلق بمفهوم الشرط التعسفي وذلك لخطورة مثل هذه الشروط وبغية توفير الحماية القانونية للمستهلك الإلكتروني من خلال بيان مفهوم هذا الشرط مع إعطاء بعض الأمثلة عن الشروط التعسفية أسوة بالمشرع الجزائري والفرنسي، كما نأمل من المشرع السوري ان يحذو على خطا المشرع الفرنسي من خلال عدم تحديد شكل معين للعقود التي تتضمن شروط تعسفية. وفيما يلي نص هذه المادة:

أ- الشرط التعسفي هو كل شرط يقوم المزود بإدراجه في العقد مستغلاً قوة مركزه الاقتصادي أو قوة نفوذه بهدف الحصول على ميزة مجحفة على حساب المستهلك بما يشكل إخلالاً بالتوازن العقدي.

ب- من صور الشروط التعسفية التي يمكن أن تدرج في العقد على سبيل المثال لا الحصر:

- الشروط التي تؤدي إلى الاختلال في الالتزامات المتقابلة

-الشروط التي تمنح المزود حق الانفراد بتعديل العقد

-الشروط التي ترفض حق المستهلك بفسخ العقد

-الشروط التي تهدد بقطع العلاقة التعاقدية

ج- هذه الأحكام الواردة في الفقرتين السابقتين تعد محلاً للتطبيق مهما كان شكل العقد أو الوسيط الذي يتم من خلاله

٣- انتشار الإعلانات التجارية عبر شبكة الإنترنت: تُسبق الأعمال التجارية الإلكترونية بصفة عامة بشكل من أشكال الدعاية والإعلان عبر شبكة الإنترنت أو أي وسيلة إلكترونية أخرى. ولا شك أن الإعلان أصبح من أهم آليات النشاط التجاري في المنافسة وتحقيق الربح عبر شبكة الإنترنت. لذلك وفي سبيل تسليط الضوء على الإعلانات التجارية سوف نتحدث بداية عن تعريف الإعلانات التجارية ثم ننتقل للحديث عن المشكلات التي تصيب المستهلك من جراء الإعلانات التجارية.

أ-تعريف الإعلانات التجارية الإلكترونية.

يُعرّف الإعلان بأنه: «مجموعة من الجهود غير الشخصية التي تهدف إلى توجيه انتباه الأفراد إلى سلعة ما لحثهم على شرائها»^(١). وحيث أننا في نطاق التعاملات الإلكترونية، فقد عُرف الإعلان الإلكتروني بأنه: «عبارة عن أنواع من الأنشطة المختلفة التي يتم من خلالها نشر أو إذاعة الرسائل الإعلانية المرئية أو المسموعة على أفراد المجتمع بهدف حثهم على شراء السلعة أو الخدمة المعلن عنها»^(٢).

كما عرّف المشرع السوري الإعلان بأنه: «أي طريقة تهدف إلى ترويج أو بيع أو تسويق منتج أو سلعة أو خدمة سواء كان ذلك

^(١) فلاح العجمي، مرجع سابق، ص ٦٤.

^(٢) عبد الله محمود، مرجع سابق، ص ٣٦.

بطريقة مباشرة أم غير مباشرة مفرداً أو مسموعاً أو مرئياً أو بالترميز^(١).

يلاحظ من التعاريف السابقة أن الإعلان هو كل فعل أو تصرف يهدف إلى التأثير النفسي على جمهور المستهلكين بغية إقناعهم بالسلعة أو بالخدمة وما يمكن أن تحققه من فوائد بغض النظر عن الوسيلة المستخدمة في ذلك.

وبالتالي لا يختلف الإعلان الإلكتروني عن الإعلان التقليدي إلا من ناحية الوسيلة المستخدمة سواء أكانت هذه الوسيلة من خلال شبكة الإنترنت أم غيرها من الوسائل كالهاتف الجوال. وتنقسم الإعلانات إلى أنواع مختلفة منها إعلانات بحسب الهدف أو إعلانات بحسب المنطقة الجغرافية التي يغطيها أو بحسب نوعية نشاط المعلن أو بحسب الأداة المستخدمة أو بحسب السلعة محل الإعلان^٢.

ومن التطبيقات العملية للإعلان الإلكتروني نذكر:

- الإعلانات المختصرة عبر الإنترنت، فعند فتح صفحة الإنترنت من خلال شاشة الحاسوب تظهر عناوين بعض المواقع التجارية و يتم الدخول إلى أي موقع بشكل مباشر، وتظهر هذه الإعلانات أعلى صفحة محركات البحث بشكل عشوائي أو بمظهر ثابت.

^١ المادة الأولى من قانون التجارة الداخلية وحماية المستهلك رقم ١٤/ لعام ٢٠١٥.

^٢ عبد الله محمود، مرجع سابق، ص ٣٧.

^٣ المرجع السابق، ص ٣٧.

- تمثل الرسائل القصيرة المرسلة إلى الهواتف المحمولة العائدة للمستهلكين أو إلى بريدهم الإلكتروني صورة من صور الإعلان الإلكتروني.

ب- المشكلات التي تصيب المستهلك من جراء الإعلانات الإلكترونية.

نظراً لما تتمتع به الإعلانات الإلكترونية من القدرة على التأثير النفسي للمستهلك وبالتالي تنعكس على حرية اختياره السلع والخدمات، لذلك كثيراً ما يصيب المستهلك نوع من الخلط في المفاهيم والمصطلحات التي يتضمنها الإعلان، كما أن الإعلان قد يكون عبارة عن إعلان مضلل أو موقع وهمي مما قد يسبب للمستهلك ضرراً كبيراً لذلك يمكننا أن نجمل المشكلات التي تصيب المستهلك جراء الإعلانات الإلكترونية في نوعين:

أ- الخلط بين الإعلان الذي يمثل دعوة للتعاقد وبين الإيجاب.

لا يعد الإعلان الموجه إلى المستهلك عبر شبكة الإنترنت إيجاباً، وإنما هو دعوة للتعاقد حيث أن عرض السلع في واجهات المحلات التجارية دون بيان أسعارها لا يعد إيجاباً. كما أن عرض البضائع والخدمات عبر الإنترنت يشبه إلى حد كبير نافذة المتجر الحقيقي، فإذا تضمن عرض السلع والخدمات عن طريق الإنترنت ثمن المبيع يعد هذا العرض إيجاباً شأنه في ذلك شأن عرض البضائع على واجهات المحلات مع بيان أثمانها. ففي الحالتين يتحقق للمستهلك رؤية الشيء المبيع سواء أكانت رؤية حقيقية أم افتراضية. ويأتي اعتبار الإعلان الإلكتروني الموجه إلى المستهلك دعوة للتعاقد من خلال عدم احتواء الإعلان على

الشروط الأساسية للتعاقد، حيث أن بيان أسعار السلع عبر الإنترنت يعتبر إيجاباً لكون السعر من المعلومات الجوهرية في التعاقد.^١ وتطبيقاً لذلك فقد قضت محكمة النقض المصرية بأن الإعلان الموجه إلى الجمهور الصادر من شركة النصر لصناعة السيارات عن فتح باب الحجز للسيارات التي تنتجها لا يعدو أن يكون دعوة للتعاقد وليس إيجاباً.^٢

كما قضت بأن طرح مناقصات التوريد وغير ذلك من البيانات الموجهة للجمهور كالنشرات والإعلانات ليس إيجاباً وإنما دعوة للتعاقد فالإيجاب هو الاستجابة لهذه الدعوة، ويتم التعاقد بقبول الجهة صاحبة المناقصة.^٣

ونحن من جانبنا نرى أن الإعلان التجاري الإلكتروني الموجه إلى المستهلك قد يكون إيجاباً أو دعوة للتعاقد. فإذا كان الإعلان واضحاً ومفصلاً لكافة الشروط الأساسية للتعاقد وموجهاً لأشخاص محددين عُدَّ إيجاباً، أما إذا كان هذا الإعلان خالياً من ذلك عُدَّ دعوة للتعاقد. وبالتالي فإن مسألة وضوح الإعلان الإلكتروني هي أحد أساليب معالجة المشكلة (وهذا ما سيتم بحثه لاحقاً).

^١ د. فواز صالح، مصادر الالتزام، الجزء الأول، كلية الحقوق، منشورات جامعة دمشق، ٢٠١٢، ص ١٧٢-١٨٢.

^٢ طعن نقض مدني رقم ١٩٨ جلسة ٣/١٢/١٩٧٦ ومشار إليه لدى: عبد الله محمود، مرجع سابق، ص ٣٩.

^٣ طعن نقض مدني رقم ١٨٦٥ جلسة ١/٢٣/٢٠٠١ ومشار إليه لدى: المرجع السابق، ص ٣٩.

ب- وجود بعض الإعلانات المضللة: عرّف بعض شراح القانون الإعلان المضلل بأنه: «الإعلان الذي يكون من شأنه خداع المستهلك أو يمكن أن يؤدي إلى ذلك»^(١).

كما عرّف التوجيه الأوروبي الإعلان المضلل أو الخادع بأنه: «كل إعلان يحتوي في طريقة تقديمه بأي طريقة كانت على تضليل أو قد يؤدي إلى تضليل الأشخاص الموجه إليهم أو الذين يصل إليهم الإعلان وبالتالي يؤثر على سلوكهم الاقتصادي»^(٢).

كما بين التوجيه الأوروبي أن الإعلان المضلل قد يقع عن طريق إغفال إحدى الخصائص المهمة أو الجوهرية في السلع والخدمات^(٣).

أما بالنسبة للمشرع السوري فقد عرّف الإعلان المضل بأنه: «الإعلان الذي يتم بأي وسيلة كانت ويتناول سلعة أو خدمة أو يتضمن عرضاً أو بياناً أو ادعاء كاذب أو مصوغاً بعبارات من شأنها أن تؤدي بشكل مباشر أو غير مباشر إلى خداع المستهلك»^(٤).

نستنتج من التعاريف السابقة أنها جميعها تدور حول فكرة واحدة وهي أن الإعلان المضلل يتم بأي وسيلة من شأنها أن تؤثر على حرية اختيار المستهلك بحيث لولا هذا الإعلان المضلل لما اختار المستهلك هذه السلعة.

^١ عبد الله محمود، مرجع سابق، ص ٤٢.

^٢ المادة (٢/٢) من التوجيه الأوروبي رقم (٨٤/٤٥٠) الصادر في ١٠/٩/١٩٨٤ الخاص بالإعلان الكاذب أو المضلل.

^٣ المادة الثالثة من التوجيه الأوروبي رقم (٨٤/٤٥٠) الصادر في ١٠/٩/١٩٨٤ الخاص بالإعلان الكاذب أو المضلل.

^٤ المادة الأولى من قانون التجارة الداخلية وحماية المستهلك رقم ١٤/ لعام ٢٠١٥.

ونحن من جانبنا نعرّف الإعلان المضلل بأنه: «الإعلان الذي يؤدي إلى خداع أو تضليل المستهلك بأي وسيلة كانت من خلال تضمينه معلومات خاطئة تتعلق بعناصر وأوصاف جوهرية في المبيع والتي من شأنها التأثير في حرية اختيار المستهلك للسلعة أو الخدمة».

وتجدر الإشارة هنا إلى أن الإعلان المضلل جريمة معاقب عليها بموجب القانون (وهذا ما سيتم بحثه لاحقاً).

٤- وجود بعض العيوب سواء في المنتج أم في الإرادة.

كثيراً ما يُفاجأ المستهلك بوجود عيوب خفية في المنتج أو الخدمة لم يتمكن من اكتشافها وخصوصاً في ظل العقود الإلكترونية، والتي يغيب فيها الحضور المادي للأطراف وأحياناً الحضور المادي للمنتجات كما لو كان المبيع عبارة عن منتجات رقمية. حيث تعد العيوب الخفية في المنتج أحد المشكلات الأساسية التي تصيب المستهلك في نطاق التعاملات الإلكترونية. لذلك كان لابد من تسليط الضوء على مفهوم هذا العيب بغية التمكن من الوصول إلى حل قانوني لهذه المشكلة.

فقد عرّف جانبٌ من الفقه العيب الخفي بأنه: «العيب الذي يلحق بالمبيع حيث يصيب المنتج أو الخدمة سواء في الأوصاف أو الضمانات بحيث يجعلهم غير صالحين للهدف المعدين لأجله أو يؤدي وجودها إلى إتلاف في المبيع»^(١).

^(١) عبد الله محمود، مرجع سابق، ص ١٠٩.

في حين عرّف المشرع المصري العيب بأنه: «كل نقص في قيمة أي من المنتجات أو نفعها بحسب الغاية المقصودة ويؤدي بالضرورة إلى حرمان المستهلك كلياً أو جزئياً من الاستفادة بها فيما أعدت من أجله، بما في ذلك النقص الذي ينتج من خطأ في تنزيل السلعة أو تخزينها وذلك كله ما لم يكن المستهلك تسبب في وقوع هذا النقص»^(١).

يلاحظ على التعاريف السابقة أنها جاءت واضحة ومفصلة لأشكال ومظاهر العيوب التي تصيب المنتج (نقص في قيمة المنتج، النقص في الضمانات) كما بينت الآثار السلبية التي تترتب على العيب (حرمان المستهلك من الاستفادة من المبيع)، ولكن يعاب على تعريف المشرع المصري اقتصره على وجود عيب في المنتج فقط ولم يشمل الخدمة.

ونحن من جانبنا نرى أنه لا يمكن وضع تعريف موحد للعيب فهو يختلف باختلاف الناحية التي ننظر من خلالها:

فمن الناحية المادية نعرّف العيب بأنه: «كل ما يؤدي إلى حدوث تلف في المنتج أو الخدمة أو يلحق به الهلاك أو ينقص من قيمته ومنفعته»^(٢).

أما من الناحية الوظيفية نعرّف العيب بأنه: «كل ما يصيب المنتج أو الخدمة في خصائصه ليصبح غير صالح للغرض المعدّ من أجله»^(٣).

أما من الناحية العقدية فالعيب هو: «تخلف صفة في المنتج أو الخدمة التزم البائع بوجودها فيه»^(٤).

^(١) المادة الأولى من قانون حماية المستهلك المصري رقم ١٨١/ لعام ٢٠١٨.

وبشكل عام يمكن تصنيف العيوب التي تنشأ عنها الأضرار إلى ثلاثة أنواع: عيوب التصميم وعيوب التصنيع والتعليمات والتحذيرات المعيبة، ويلاحظ أن عيبي التصميم و التصنيع مرتبطان بالخواص الذاتية للمنتج بينما العيوب التي تتعلق بالتعليمات والتحذيرات فهي تتصل بعوامل خارجية لا تدخل في تركيب المنتج كعدم الإدلاء بالبيانات التي يفترض أن تكون مصاحبة للمنتج^١.

وإلى جانب العيوب الخفية في المنتج كثيراً ما تظهر عيوب في إرادة المستهلك المتعاقد. حيث أنه وفي ظل عدم الحضور المادي للأطراف كثيراً ما يقع المستهلك في عيوب الغلط في شخص المتعاقد، كما لو أقدم أحد التجار (مستغلاً شهرة تاجر آخر) على تصميم موقع إلكتروني يحمل اسم التاجر المشهور. فيدخل المستهلك على الموقع ويقوم بشراء سلعة ظناً منه أنه يتعامل مع التاجر المشهور، ثم يُفاجأ بأنه يتعامل مع شخص آخر وبالتالي يكون المستهلك قد أصابه أحد عيوب الإرادة (عيب الغلط في شخص المتعاقد)، وذلك على اعتبار أن المستهلك ما كان ليتعاقد لو علم أن هذا الموقع لا يعود لهذا التاجر المشهور.

وإلى جانب عيب الغلط قد يقع المستهلك ضحية أساليب احتيالية في التعاقد (التدليس) كما لو قام أحد الأشخاص بنشر إعلانات كاذبة ومضللة عن منتجاته قاصداً من وراء ذلك خداع المستهلك وتضليله. فيقوم المستهلك وتحت تأثير هذه الإعلانات بقبول التعاقد ثم يُفاجأ بأنه وقع ضحية تدليس هذا الشخص لأن المنتج ليس على ذات

^١ سهام إمدالو و ليلي حسن، مرجع سابق، ص ٤٦.

المواصفات التي ذكرت في الإعلان. وخصوصاً أن المستهلك ما كان ليتعاقد لولا هذه الطرق الاحتيالية التي أوقعت المستهلك في التدليس ودفعته للتعاقد.

وبالنتيجة يمكننا القول أن دخول الوسيلة الإلكترونية في نطاق الدفع الإلكتروني كان له أثر ذو طبيعة خاصة ومزدوجة بالنسبة للمشكلات التي تصيب المستهلك الإلكتروني كمتعاقد:

فمن جهة أسهمت الوسيلة الإلكترونية في ظهور مشكلات جديدة لم تكن معروفة من قبل (كمشكلات الشراء عبر الحدود بأشكالها المختلفة-التحديات التقنية).

ومن جهة أخرى أسهمت الوسيلة الإلكترونية في ظهور المشكلات القديمة التي تواجه المستهلك التقليدي بصيغة جديدة لم نعرفها من قبل أمام المستهلك الإلكتروني (كالمشكلات القانونية المتعلقة بالعيوب الخفية والشروط التعسفية...الخ).

وأمام هذه التحديات والمشكلات التي تواجه المستهلك جراء التعاقدات الإلكترونية كان لا بد من البحث عن أساليب وحلول قانونية تساهم في علاج هذه المشاكل وتوفير الحماية للمستهلك الإلكتروني سواء أكانت هذه الحماية مقررة بموجب أحكام قانون المعاملات الإلكترونية أم بموجب أحكام القانون المدني.

المبحث الثاني

المشكلات التي تواجه الاقتصاد الوطني

لا تقتصر الآثار السلبية لوسائل الدفع الإلكتروني على الأفراد المتعاملين بهذه الوسائل فحسب سواء أكانوا عملاء أم مستهلكين، بل على العكس من ذلك كثيراً ما تمتد الآثار السلبية لتواجه الاقتصاد الوطني للبلاد. فكلما كشف التطور التقني عن مجموعة من الوسائل التي تستخدم في سبيل تطور المجتمع وتقدمه كلما لجأ محترفو الجريمة وهواتها إلى تطويع هذه الوسائل في سبيل ارتكاب الجرائم. حيث تعد مشكلة التهرب الضريبي وغسيل الأموال باستخدام وسائل الدفع الإلكتروني من أخطر المشكلات التي تواجه الاقتصاد الوطني وذلك لسببين:

الأول: الطابع الجرمي الذي يكتنف هذه المشكلات.

الثاني: تعد وسائل الدفع الإلكتروني البيئة الخصبة والملائمة لارتكاب هذه المشكلات وخصوصاً في ظل عدم تحديد هوية النشاط أو هوية المتعامل بهذه الوسائل.

وبالتالي ونظراً لخطورة هذه المشكلات سوف نتحدث عن مشكلة التهرب الضريبي باستخدام وسائل الدفع الإلكتروني في مطلب الأول على أن نتعرف على مشكلة غسيل الأموال باستخدام وسائل الدفع الإلكتروني وذلك في المطلب الثاني.

المطلب الأول

مشكلة التهرب الضريبي باستخدام وسائل الدفع الإلكتروني

تعد الضرائب على الأنشطة التجارية أحد الموارد الرئيسية لاقتصاد الدولة، إلا أن زيادة نسبتها من شأنه أن يحد من حجم النشاط التجاري وخصوصاً التجارة الإلكترونية نظراً لأن التعاملات الإلكترونية هي تعاملات حديثة العهد، الأمر الذي يشكل صعوبة في تطبيق التشريعات المطبقة على التعاملات التقليدية بهذا الصدد. ومن المتوقع أن يصاحب انتشار وسائل الدفع الإلكتروني تزايد كبير في جرائم التهرب الضريبي حيث سيكون من الصعب على الجهات المكلفة بتحصيل الضرائب القيام بفرض الضريبة على الصفقات الإلكترونية لكون أغلب هذه الصفقات تتم خفية عبر شبكة الإنترنت، وعليه فإن الإدارة الضريبية في كافة أنحاء العالم تواجه صعوبة في حماية عائداتها الضريبية نتيجة تطور النشاط التجاري الإلكتروني إلا أنها وفي الوقت نفسه تسعى إلى تطبيق التقنيات الحديثة التي تساهم بشكل إيجابي في مجال التنمية.

ولتسليط الضوء على هذه المشكلة نبين مدى خضوع معاملات الدفع الإلكتروني للضريبة وذلك في الفرع الأول ثم ننقل لبيان التحديات التي تواجه فرض الضريبة على معاملات الدفع الإلكتروني في الفرع الثاني.

الفرع الأول

مدى خضوع معاملات الدفع الإلكتروني للضريبة

أدى انتشار وسائل الدفع الإلكتروني كوسيلة لتسوية الالتزامات الناشئة عن التعاملات الإلكترونية إلى تأثيرات مختلفة مالية واقتصادية واجتماعية، مما أثار تساؤلات كثيرة حول الآليات المناسبة للتعامل معها، ومن أهم هذه الموضوعات المثارة (المعاملة الضريبية لمعاملات الدفع الإلكتروني) والتي أوجدت مواقف متباينة يمكن إجمالها في موقفين:

أولاً: الاتجاه المعارض لفرض الضريبة على هذه المعاملات

أكد أنصار هذه الاتجاه في العديد من كتاباتهم^١ على رفض فكرة فرض الضريبة على معاملات الدفع الإلكتروني وساقوا لتبرير موقفهم العديد من الحجج نذكر منها:

١-- سيكون فرض الضريبة على معاملات الدفع الإلكتروني الآن من أكثر العوامل المعيقة لنمو هذه المعاملات وانتشارها، وهو ما

^١ د. طارق حمزة ، النقود الإلكترونية كإحدى وسائل الدفع (تنظيمها القانوني-المسائل الناشئة عن استعمالها)، ط١، منشورات زين الحقوقية، لبنان، ٢٠١١، ص ٣١٩. و د. عبد الباسط أبو الوفاء، سوق النقود الإلكترونية (الفرص - المخاطر - الآفاق) بحث منشور في مجلة مصر المعاصرة ، العدد ٤٧١-٤٧٢، مصر، ٢٠٠٣، ص ٢٩٣.

عبر عنه أحد الفقهاء بقوله (أني قلق جداً من أن الضريبة على الدفع الإلكتروني ستعيق نمو هذا القطاع و هو مالا يمكن تحمله الآن^١).

٢- يؤدي فرض الضريبة على معاملات الدفع الإلكتروني إلى المساس بخصوصية المستخدم وذلك على اعتبار أن المعلومات المطلوبة لتقدير الضريبة و تحصيلها (كأسماء المستخدمين، عناوينهم، طبيعة مشترياتهم) قد تهدد إمكانية الاستخدام السري للإنترنت، الأمر الذي يحد من الشراء عبر الإنترنت.

٣- إن فرض ضريبة على معاملات الدفع الإلكتروني سيزيد من حركة المصارف العاملة في هذا المجال و تنقلها إلى بلدان ذات ضرائب منخفضة و ذلك على اعتبار أن رأس المال في مجال الدفع الإلكتروني متقلب بسرعة لكافة الاختلافات الضريبية، لذلك من الأولى أن يتم التركيز على إنشاء بيئة عمل جاذبة لهذه المعاملات بدلاً من التفكير في كيفية فرض ضريبة عليها.

٤- التكاليف الإدارية العالية المرافقة لفرض ضريبة على هذه المعاملات، وما يشبه ذلك من حساب للضريبة ونسبها المختلفة في الدول وتحصيلها والتدقيق عليها، فمتطلبات فرض هذه الضريبة وتحصيلها في ضوء ما تواجهه من صعوبات (قانونية و تقنية) ستكون مكلفة جداً، الأمر الذي من شأنه رفض فرض الضريبة على معاملات الدفع الإلكتروني.

٥- لقد كان للإنترنت دوراً و أثراً كبيراً على الاقتصاد ككل، فعلى سبيل المثال قفز الاقتصاد الأمريكي إلى أكثر من ٠.٤ في السنة

^١ المرجع السابق، ص ٣١٩.

خلال عامين متتاليين ١٩٩٧، ١٩٩٨، كما زادت حصيلة ضرائب المبيعات من ١٤٧ مليار دولار عام ١٩٩٧ إلى ١٥٥ مليار دولار عام ١٩٩٨^١. ذلك فإن إنشاء التزام بتحصيل ضرائب على معاملات الدفع الإلكتروني على حد تعبير أحد الباحثين بمثابة قتل الإوزة التي تبيض ذهباً^٢.

^١Marvin Kirsner , Taxation Of Electronic Commerce's, Internet Tax Advisor , Vol 1 , Issue12, USA,p.9.

^٢ مشار إليه لدى :د. حوالف عبد الصمد، مرجع سابق، ص٣٦٢.

وفي هذا الخصوص فقد كان التشريع الأمريكي من التشريعات التي عارضت مسألة فرض الضريبة على معاملات الدفع الإلكتروني. حيث أصدر قانون حرية الضرائب في عام ١٩٩٨. وقد كان هذا القانون أول قانون اتحادي حظر إنشاء الضرائب على الأنشطة الرقمية بشكل عام ومعاملات الدفع الإلكتروني بشكل خاص. وقد كان يهدف المشرع الأمريكي من وراء هذا الحظر تشجيع مستقبل معاملات الدفع الإلكتروني وذلك على اعتبار أن فرض الضرائب على هذه المعاملات من شأنه أن يقوض مسألة انتشار هذه المعاملات، كما أن فرض ضرائب على معاملات الدفع الإلكتروني أمر صعب في ظل الافتقار لمتطلبات الأمن الداخلي والخارجي لهذه المعاملات. ولكن وخلال فترة قصيرة لقي هذا القانون انتقاداً واسعاً داخل مجلس الشيوخ. ففي عام ١٩٩٩ أجريت دراسة حوله داخل مجلس الشيوخ حيث كان فليب ماريني رئيس اللجنة المالية في المجلس أول من رأى أن عدم فرض ضرائب على الأنشطة الرقمية بكافة أشكالها نوع من تنازل الدول المستهلكة عن إيرادات الضرائب، وهذا الأمر سوف ينعكس سلباً على الاقتصاد الوطني للدول وذلك على اعتبار أن الشركات والمصارف التي تتعامل بالأنشطة الرقمية لا تنهرب من الضريبة فحسب بموجب القانون الاتحادي، إنما تسعى تلك الشركات والمصارف لخلق قارة افتراضية بلا حدود. ويرى فليب ماريني أن قطاع الإنترنت استخدم منذ نشأته المنصة العالمية للتنهرب الضريبي ومرد ذلك لعدة عوامل هي:

١- تولد الأنشطة الرقمية منافسة غير عادلة: حيث تدفع شركة apple / ٢ سنت/ من ضريبة القيمة المضافة في لوكسمبورغ لقاء تنزيل أغنية بينما يدفع منافسوها

١٩سنت/وبالتالي سوف تتأثر جميع الأنشطة بالمنافسة غير العادلة من قبل الشركات والمصارف العاملة في مجال الأنشطة الرقمية.

٢-وجود الملاذات للتهرب الضريبي: ومثالها (موناكو-سويسرا-برمودا-هونغ كونغ)
 ٣-استخدام المصارف في التهرب الضريبي: حيث أظهر تقرير مجلس الشيوخ رقم ٢٩٨/٢٠٠٨ حول دور المصارف في التهرب الضريبي أن ٥٠٠ من أصل ٧٥٠٠ شركة تابعة مملوكة للمصارف الفرنسية تستخدم الإنترنت في سبيل تهريب أنشطتها من الضرائب.

٤-وجود شبكات اتصال إلكترونية فعالة لتحويل الأموال في أقل من نصف ثانية وخارج نطاق السيطرة.

٥-انتشار ثقافة الربح بأي ثمن: حيث خلف غياب دوريات الأخلاقيات في التعليم العالي أجيال من القادة المستعدين للتضحية بالإنسان والثقافة والوطن مقابل بضعة دولارات

ثانياً: الاتجاه المؤيد لفرض الضريبة على هذه المعاملات

في مواجهة الداعين لاستبعاد معاملات الدفع الإلكتروني من نطاق الضريبة، ظهرت آراء تدعو إلى فرض الضريبة عليها، وتقدم حججاً تدعم موقفها^١. يمكن حصر هذه الحجج في الآتي :

١- إن عدم فرض ضريبة على معاملات الدفع الإلكتروني سيثبته سلوك المستخدمين، فالأشخاص الذين يعيشون في دول ذات ضرائب مرتفعة سيقبلون على الشراء عبر الإنترنت للتهرب من دفع الضرائب، مما يشكل حافزاً للتجار لتقديم منتجاتهم عبر الإنترنت.

٢- إن فشل فرض الضريبة على معاملات الدفع الإلكتروني سيؤدي إلى عدم المساواة بين التجارة الإلكترونية والتجارة التقليدية، ولعل ذلك قد يبدو حجة مشروعة للباعة التقليديين الذين يشاهدون المستخدمين يحضرون إلى محلاتهم و يختارون السلع التي يريدونها ثم يشترونها عن طريق الإنترنت لتجنب دفع الضريبة وبالتالي فإن الأمر سيؤدي إلى سوء توزيع الموارد^٢.

^١ د. ابراهيم كامل الشوابكه، ضريبة المبيعات على التجارة الإلكترونية، بحث منشور في مجلة علوم الشريعة والقانون، المجلد ٣٤/، الجامعة الأردنية، عمان، ٢٠٠٧، ص ٥١٩، متاح على الرابط: www.Journals.ju.edu.jo/Disasat/Law/article/view/612/610

تاريخ الزيارة : ٣٠/١٠/٢٠١٨ الساعة ٣:٤٥ pm

و د. رمضان صديق محمد، مشكلات الضريبة على دخل التجارة الإلكترونية والحلول الممكنة، بحث منشور في مجلة الحقوق، العدد الثالث، السنة السادسة والعشرون، الكويت، ٢٠٠٣، ص ٣٤٠.

^٢ المرجع السابق، ص ٣٤٠.

٣- إن عدم فرض الضريبة على معاملات الدفع الإلكتروني سيؤدي إلى زيادة خسائر الدول من العوائد الضريبية. فعلى سبيل المثال يقدّر اقتصاديو جامعة تينيسي بأن خسارة الولايات المتحدة الأمريكية من جراء عدم فرض ضريبة على الإنترنت حوالي ١٠,٨ مليار دولار^١، مما دفع أحد الباحثين إلى أن يصف أثر إلغاء الضريبة على الإنترنت بمثابة النمل الأبيض الذي سيلتهم الضريبة^٢.

٤- إن عدم فرض الضريبة على هذه المعاملات سيعيد توزيع الدخل لمصلحة الأغنياء، كون الفقراء هم الأقل اهتماماً باستخدام الإنترنت، لذلك فإن الأشخاص الذين يقومون بالشراء عبر الإنترنت هم الأغنياء نظراً لما يتطلبه الشراء عبر الإنترنت من معدات و تقنيات مكلفة مادياً ولا يقدر عليها إلا الأغنياء.

وفي هذا الخصوص يرى الخبير الاقتصادي سيمون ووديسايد^٣ أن المعاملة الضريبية لمعاملات الدفع الإلكتروني ليست استثناء. ولعل جوهر الخلاف حسب رأيه إنما ينبع من بعض الأفكار الموجودة مثل

¹William Fox , E-Commerce In The Context Of Declining Sale+ Tax Bales, National Tax Journal , P 1375,

Disponible sur:

www.cber.bus.utk.edu/e-comm.pdf.

تاريخ الزيارة ٢٠١٩/١٠/٨ الساعة ١١,٣٠ a.m.

^٢مشار إليه لدى :د. حوالف عبد الصمد، مرجع سابق ، ص ٣٦٣.

³Simon Woodside, La fiscalité du commerce électronique, Une réalité virtuelle, Centre de politique et d'administration fiscales;

Disponible sur:

http://www.observateurocde.org/news/archivestory.php/aid/391/La_fiscalit_E9_du_commerce_E9lectronique:_Une_r-E9alit-E9-virtuelle.html.

تاريخ الزيارة ٢٠١٩/١٠/١١ الساعة ١٠,٣٠ a.m.

فكرة أن الدفع الإلكتروني له طابع خاص لدرجة أنه لا ينبغي إخضاعه للضريبة، حيث اعتبر أن هذه الحجة غير مقبولة لأنه لا يوجد سبب وجيه لإعطاء معاملة ضريبية أكثر ملاءمة لمعاملات الدفع الإلكتروني من التجارة التقليدية. حيث من شأن عدم إخضاع معاملات الدفع الإلكتروني للضريبة أن يشوه الاقتصاد الوطني وخصوصاً في ظل استمرار تآكل القاعدة الضريبية للدول من قبل هذه المعاملات الأمر الذي ينعكس سلباً على الاقتصاد الوطني. وبالنسبة ل سيمون ووديسايد أن فرض الضريبة على معاملات الدفع الإلكتروني يتطلب قاعدتين أساسيتين:

الأولى: ينبغي أن نحدد بوضوح مكان حدوث الضرائب في الفضاء الخارجي تجنباً لظاهرة الازدواج الضريبي.

الثانية: تحديد الوسائل العملية والمعقولة لتطبيق المعايير الضريبية المقبولة دولياً على معاملات الدفع الإلكتروني، ومن هذه الوسائل (تحديد القاعدة التي تعطي الدولة الحق في فرض الضريبة على الأرباح العائدة لشركة من دولة ما وتعمل في الفضاء الخارجي لدولة أخرى أي تحديد الوسائل الكفيلة بتحصيل الضرائب على المنتجات التي يتم تسليمها عبر الإنترنت كالمنتجات الرقمية.)

ودون هاتين القاعدتين فإن مسألة فرض الضريبة على معاملات الدفع الإلكتروني أمر بالغ في الصعوبة حسب رأي الخبير الاقتصادي.

و نحن من جانبنا نؤيد أنصار الاتجاه الثاني الذي نادى بفرض الضريبة على معاملات الدفع الإلكتروني وذلك للمبررات التي ساقها

أنصار هذا الاتجاه، كما أن وجود صعوبة في فرض الضريبة على معاملات الدفع الإلكتروني نظراً لحدثة ظهورها لا يشكل مبرراً لعدم خضوعها، بل لابد من تطويع الأحكام القانونية التقليدية لتلاءم هذا النوع من المعاملات أو العمل على سن تشريعات قانونية تعالج مسألة فرض الضريبة على هذه المعاملات. كما أننا لو نظرنا إلى الحجج التي ساقها أنصار الاتجاه الأول لوجدنا أنهم يرفضون فكرة فرض الضريبة بهدف منح معاملات الدفع الإلكتروني المزيد من الوقت للتقدم والازدهار، وبالتالي فإن موقفهم آني و مؤقت ويؤيد بشكل غير مباشر فرض الضريبة على هذه المعاملات على الرغم من وجود عدة صعوبات وتحديات تواجه فرضها.

وتأكيداً على ضرورة خضوع معاملات الدفع الإلكتروني للضريبة، فقد أشار حكم صادر عن المحكمة الإدارية في فرنسا بتاريخ ٢٥ كانون الأول ٢٠١٣ (رقم ١١٠١٤٢، TAPAU) إلى أن حسابات PayPal (أحد المصارف الرئيسة في فرنسا) تخضع للالتزام بالإبلاغ عنها لناحية الضريبة، وذلك على اعتبار أن لشركة PayPal (Europe) مكتب رئيس في لوكسمبورغ، كما أن فتح الحساب لدى هذه الشركة يشمل الوصول إلى خدمات الدفع الإلكتروني والمشتريات عبر الإنترنت باستخدام الأموال المتاحة في هذا الحساب. حيث جاء في حيثيات الحكم: إن الإدارة الضريبية في فرنسا تلزم بالإبلاغ عن الحسابات المحتفظ بها في الخارج، وقد تبين من الحسابات ذات الرموز الآتية: (٢٠١٣١١١٢-٢٠-٣٠-CPF -BOICF) و (CGI) (١١١ ANNS) العائدة لشركة PayPal (وكذلك المادتين (A344

¹ Guillaume Hublot :*Le dispositif FATCA applicable en France*, Droit et Patrimoine, N° 231, 1er Décembre 2013.

وB344) من قانون الضرائب الفرنسي أنه يجب إبلاغ السلطات الضريبية سنوياً بالحسابات المفتوحة في الخارج من قبل أشخاص طبيعيين وكذلك من قبل بعض الكيانات القانونية الموجودة في فرنسا. وبالتالي فإن الحكم الصادر بتاريخ ٢٥ كانون الأول ٢٠١٣ (رقم ١١٠١٤٢، TAPAU) يلزم بالإبلاغ عن حسابات (PayPal) لناحية الضريبة بالحد الذي يكون للشركة (PayPal Europe) مكتب رئيس في لوكسمبورغ طالما أن فتح الحساب لدى هذه الشركة يشمل الوصول إلى خدمات الدفع الإلكتروني والمشتريات عبر الإنترنت باستخدام الأموال المتاحة في هذا الحساب. كما أشار الحكم الصادر إلى أن الالتزام بالإبلاغ يطبق بالنسبة للأفراد الذين يستخدمون الحساب بشكل احترافي، أما الحسابات التي لا تتطوي على الوصول لخدمات الدفع الإلكتروني والمشتريات عبر الحدود فلا تخضع لشروط الإبلاغ المنصوص عليها في المادة ٦٤٩/ من قانون الضرائب الفرنسي. كما بين الحكم الصادر أن الإعفاء من الإبلاغ يتطلب ثلاثة شروط تراكمية :

- يجب أن يكون الغرض من الحساب هو إجراء مدفوعات أو إيصالات شراء عبر الإنترنت لمبيعات البضائع.
- أن ينطوي فتح الحساب على الاحتفاظ بحساب آخر يتم فتحه في فرنسا والذي يتم دعمه عليه.
- أن لا يتجاوز مجموع الإيصالات السنوية المقيدة في هذا الحساب والمتعلقة بالمبيعات التي قام بها حامل البطاقة (١٠٠٠٠ يورو)، ويتم تقييم هذه العتبة عند الاقتضاء من خلال جمع جميع الإيصالات التي تم إجراؤها على جميع الحسابات التي يحتفظ بها صاحب الحساب نفسه.

الفرع الثاني

التحديات التي تواجه فرض الضريبة على معاملات الدفع الإلكتروني

ينتاب مسألة فرض الضريبة على هذه المعاملات نوعين من التحديات:

أولاً: تحديات قانونية

و تتمثل هذه التحديات في الآتي:

١- تحديد الدولة صاحبة الحق في فرض الضريبة: لا شك أن تبادل السلع و الخدمات سواء المادية أم الرقمية من خلال معاملات الدفع الإلكتروني داخل الدولة الواحدة يعطي الحق لتلك الدولة في فرض ضريبة على تلك المعاملات، أما بالنسبة للسلع و الخدمات التي يتم تبادلها من خلال تلك المعاملات على المستوى الدولي، فلا بد من التمييز بين :

- سلع مادية: لا تثير هذه السلع أي إشكالية، حيث أنها تتعدى الحدود الدولية و تستطيع الدول من خلال إدارتها الضريبة فرض الضريبة و تحصيلها أثناء عبور السلع المادية حدودها الإقليمية.
- سلع و خدمات رقمية: لا تظهر في صورة مادية و تتعدى حدود الدول دون استئذان، حيث تسلم بطريقة إلكترونية يصعب تسجيلها أو تدقيقها على الحدود، فهذا النوع من السلع

يثير إشكالية حول أحقية الدولة في فرض الضريبة أهى دولة المقصد أم دولة المنشأ^١.

و تحتل مسألة فرض الضريبة على معاملات الدفع الإلكتروني و خصوصاً بالنسبة للسلع الرقمية أهمية كبيرة وذلك خوفاً من حدوث ظاهرة الازدواج الضريبي الدولي الذي يعرف بأنه: «فرض أكثر من ضريبة من قبل عدة دول على ذات المكلف و على المطرح نفسه خلال دورة مالية واحدة»^٢.

إن نظام الدفع الإلكتروني وما تضمنه من إلغاء للرسوم الجمركية والحدود الاقتصادية بين الدول يجعل من المعالجة الضريبية أمراً شائكاً، وذلك على اعتبار أن هناك تحديات موضوعية قانونية تواجه هذه المسألة ولاسيما ما يتعلق باعتماد مبدأ إقليمية الدخل أم مبدأ عالمية الإيراد، حيث أن الإنفاق على شراء سلعة كمالية تعتبر مطرحاً لضريبة الإنفاق و بالمقابل فإن قيمة مبيعات الشركة من هذه السلع تعتبر مطرحاً لضريبة من قبل الدولة التي يوجد فيها مقر الشركة وبالتالي تكون الصفقة قد خضعت لنوعين من الضرائب في ذات الوقت وعلى ذات المطرح^٣.

ولكن يبقى التساؤل الأهم حول من هي الدولة صاحبة السلطة في فرض الضريبة؟

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٦٤.

^٢ المرجع السابق، ص ٣٦٤.

^٣ د. محمد شريف توفيق و د. نعيم حنا، أساليب تنفيذ عمليات التجارة الإلكترونية والتحاسبات

الضريبي عنها، بحث منشور، ص ١٥ ومتاح على الرابط: www.kenana online.com

تاريخ الزيارة ١٠/١٠/٢٠١٨ الساعة ١٥، ١٠ a.m

في الحقيقة حتى نتمكن من الإجابة على هذا التساؤل لابد بدايةً من وجود اتفاق دولي بشأن معايير هذه الضريبة، ومن ثم يعهد بفرضها إلى أحد اقتراحين:

- إما أن يعهد بفرض الضريبة للدولة التي نفذ فيها العقد أي الدولة التي تم فيها تسليم المنتج أو الخدمة الرقمية أو المادية. وذلك على اعتبار أن هذه السلع هي منقولات تنتقل ملكيتها بالتسليم قياساً على قاعدة الحيازة في المنقول سند ملكية الحائز حسن النية. فالمنتجات المادية لها وجود مادي أما الرقمية فعلى الرغم أنها ليست مادية لكن يمكن تجسيدها بشكل مادي، حيث أنه بمجرد التسليم يكون العقد قد نفذ من قبل أطرافه وبالتالي يمكن فرض الضريبة بحق المكلف بها.
- أو أن يطبق مبدأ عالمية الإيراد (التبعية السياسية للمكلف)، أي أن الدولة التي يحمل المكلف جنسيتها هي صاحبة الحق في فرض الضريبة على دخل المكلف بغض النظر عن مكان تحققه داخل الدولة أو خارجها. وهو من أفضل الحلول لهذه المشكلة وخصوصاً إذا ما كان هناك توافق دولي بشأن معايير الضريبة وذلك تفادياً للازدواج الضريبي.

٢- تحديات مرتبطة بتحديد الهوية و تعيين النشاط: وتتمثل هذه التحديات في المظاهر الآتية:

أ- تتمتع التعاملات الإلكترونية بشكل عام ومعاملات الدفع الإلكتروني بشكل خاص بطابع من السرية والخصوصية، الأمر الذي يجعل من هوية أطراف العقد الإلكتروني غير معلومة إذ لا يرَ طرفا التعاملات الإلكترونية كل منهما الآخر. ولكن هذه الميزة أو الخاصية شكّلت تحدياً أمام السلطات الضريبية وذلك على

اعتبار أن أطراف معاملات الدفع الإلكتروني كثيراً ما يستغلون هذه الميزة لأغراض التهرب الضريبي من خلال عدم تسجيل هذه المعاملات في الدفاتر المحاسبية.

ب- كشف التطور التقني عن ظهور سلع وخدمات جديدة كالسلع الرقمية (ومثالها الصور الفوتوغرافية)، وتتميز هذه السلع بصعوبة تجسدها في كيان مادي حيث يتم الحصول عليها عبر الإنترنت. وقد شكلت الطبيعة الخاصة لهذه السلع صعوبة في تحديد هوية المعاملات أو الأنشطة التي تكون فيها هذه السلع محلاً للشراء عبر الإنترنت الأمر الذي انعكس سلباً بالنسبة لفرض الضريبة على هذه السلع.

ج- أصبح بإمكان الشركات أن تنشئ المتاجر الإلكترونية وتستطيع من خلالها أن تعرض و تبيع منتجاتها، كما أصبح بإمكان الزبائن أن يتجولوا في هذه المتاجر ويطلبوا ما يحتاجونه مع تحديد كافة التفاصيل المتعلقة (بطرق الشحن، الكلفة الإجمالية، طريقة الدفع). الأمر الذي يشكل صعوبة في كيفية فرض الضرائب على هذه المعاملات نظراً لانعدام الوجود المادي للعمليات التي تتم عبر المتاجر الإلكترونية وبالتالي صعوبة تقفي آثارها.

٣- القصور المعرفي لدى جهات التفتيش والتحقق الضريبي: لعل من أهم العوامل التي تساعد على التهرب الضريبي بشكل عام وفي نطاق معاملات الدفع الإلكتروني بشكل خاص هو عدم

د. علي عزوز، جباية المعاملات الإلكترونية (المشاكل والحلول)، بحث منشور في مجلة الردة لاقتصاديات الأعمال، العدد الأول، جامعة الشلف، الجزائر، ٢٠١٥، ص ٧٥.

المعرفة القانونية والتقنية لدى جهات التحقيق والتفتيش الضريبي، فضلاً عن غياب التعاون وتبادل المعلومات بين أجهزة الإدارة الداخلية في سبيل مكافحة التهرب الضريبي. وفي هذا الخصوص نشرت محكمة مراجعة الحسابات في فرنسا¹ بتاريخ ١٥ كانون الأول ٢٠١٣ ملخصاً لرئيسها الأول في الحرب ضد التهرب الضريبي الدولي - (تمت إحالة الملخص إلى أول رئيس لمحكمة الحسابات بشأن خدمات الدولة ومكافحة التهرب الضريبي الدولي) - حيث تساءل عن انخفاض معدل شكاوى التهرب الضريبي والتي تعتبر ضعيفة الاستهداف ومتأخرة؟

حيث تنتقد محكمة مراجعة الحسابات الاحتكار المنسوب للسلطات الضريبية لمقاضاة التهرب الضريبي وتعتبره ضاراً ولاسيما في الشؤون الدولية ووسائل الدفع الإلكتروني. وينبغي أن يكون الادعاء قادراً على الاستمرار دون تقديم شكاوى أولية من قبل السلطات الضريبية في بعض عمليات الاحتيال المعقدة، وبالتالي فإن احتكار عمليات التفتيش الضريبي غير مبرر من قبل محكمة مراجعة الحسابات. كما تأسف هذه المحكمة للقيود المفروضة على القائمة السوداء للدول والأقاليم غير المتعاونة والتي تحدد سنوياً ولكنها لا تشمل البلدان التي يلجأ إليها المتهربون من الضرائب لتنفيذ عملياتهم. وتدعو محكمة مراجعة الحسابات في هذا الصدد إلى تعزيز التعاون بين مختلف المديريات ولاسيما (المديرية العامة للمالية العامة DGFIP، المديرية العامة للجمارك والضرائب غير المباشرة

¹Frédérique Perrotin: Fraude fiscale : les exigences de la Cour des comptes, Droit et Patrimoine, N° 232, 15er Décembre 2013.

(DCDDI) والتي ستستفيد من الوصول المنتظم والمتبادل بشكل أسرع لبياناتهم. كما توصي محكمة مراجعة الحسابات بضرورة اعتماد أبحاث الاستخبارات بشكل كبير على (المديرية المركزية للاستخبارات الداخلية DCRI وعلى وحدة مكافحة غسيل الأموال وتمويل الإرهاب TRACFIN).

ثانياً: تحديات تقنية

و تتمثل هذه التحديات في الآتي:

١ - آليات التحصيل: تواجه دول العالم تحدٍ رئيس لعدم وجود آليات محددة لإخضاع معاملات الدفع الإلكتروني للضريبة، حيث توجد إشكالية حول ماهية الأساليب التي سوف يتم على أساسها تحصيل الضرائب على هذه المعاملات.

وقد ظهر اتجاهين في هذا الخصوص :

الأول: يجعل تحصيل الضرائب على معاملات الدفع الإلكتروني من مهمة التاجر سواء أكانت الضريبة على هذه المعاملات تقوم على أساس دولة المنشأ أم دولة المقصد^١. ولكن من المتوقع أن يؤدي إلقاء هذا الدور على التاجر وحده إلى انخفاض مؤكد في الحصيلة الضريبة، وخصوصاً على اعتبار أن التاجر يعتبر شخص غير مؤهل لتحصيل ضرائب المعاملات الإلكترونية.

الثاني: يرى ضرورة وجود آليات جديدة لتحصيل الضرائب على معاملات الدفع الإلكتروني، وتتمثل هذه الآليات الجديدة باقتراح

^١ د. علي عزوز ، مرجع سابق، ص ٧٧

فرض ضريبة جديدة اسمها ضريبة البيت وتحسب على أساس كمية الإنترنت المستخدمة، وأن يعهد بتحصيل هذه الضريبة إلى طرف ثالث خارج عن أطراف عملية الدفع الإلكتروني كمزود خدمة الإنترنت أو أي وسيط مالي. وعلى الرغم من فعالية الاتجاه الثاني إلا أنه يبقى مجرد اقتراحات تحتل القبول والرفض^١.

وأمام عدم فعالية الأساليب التقليدية لفرض الضريبة على معاملات الدفع الإلكتروني من جهة، وعدم وجود قرار حتمي بخصوص الأساليب الجديدة للتحصيل تبقى آليات التحصيل أحد التحديات التقنية التي تواجه فرض الضريبة على معاملات الدفع الإلكتروني.

٢- تحديات ناشئة عن استخدام النقود الإلكترونية:

وتتمثل هذه التحديات في المظاهر الآتية:

أ- يرى بعض الاقتصاديين^٢ أن النقود الإلكترونية سوف تحل بمرور الزمن محل النقود الحقيقية في معاملات الأفراد، حيث ستحتوي الرقاقة الموجودة في البطاقات الإلكترونية على أرصدة الأموال الخاصة بالأفراد وسوف تستخدم في دفع المستحقات و تسوية الحساب، الأمر الذي يشكل تحدٍ أمام السلطات الضريبية وذلك نظراً لسهولة حمل النقود الإلكترونية ولسرعة تحويلها خارج الحدود إلى دول ذات نظم ضريبية أسهل مما يجعل مهمة تقفي معاملات الدفع الإلكتروني غاية في الصعوبة.

^١ د. محمد شريف توفيق، د. نعيم حنا، مرجع سابق، ص ١٦.

^٢ د. علي عزوز، مرجع سابق، ص ٧٤.

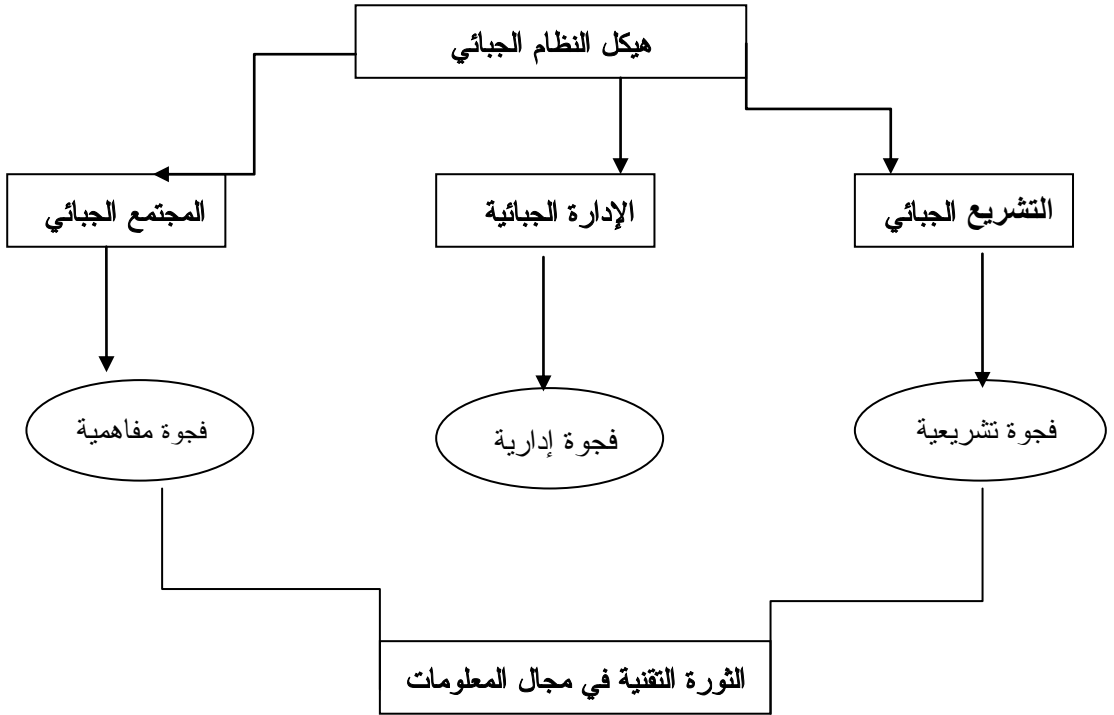
ب-تتفد المدفوعات الإلكترونية دون تسجيل محاسبي، وبالتالي فإن العمليات التي تتم تسويتها عن طريق النقود الإلكترونية لا تترك آثار محاسبية تدل عليها مما يمنح مجال واسع للتهرب الضريبي^١.

ج-التعامل بالنقود الإلكترونية كأى تعامل إلكتروني يتم تحت طابع من السرية والخصوصية بالنسبة لهوية الأطراف أو لهوية النشاط، الأمر الذي يستغله أطراف الدفع الإلكترونية بغية التهرب الضريبي وخصوصاً في ظل عدم وجود أساليب متطورة لدى السلطات الضريبية لتحديد الهوية أو تحديد النشاط بالنسبة لهذه التعاملات.

٣-قصور العلاقة بين هيكل النظام الجبائي و مستحدثات تقنيات المعلومات: يؤثر هذا القصور بشكل سلبي على كفاءة الأداء الجبائي، ويتحدد هذا القصور من خلال ثلاث فجوات رئيسة في العلاقة بين كل من مفردات الهيكل الجبائي و الثورة التقنية في مجال المعلومات. وهذا ما يوضحه الشكل الآتي^٢:

^١ المرجع السابق، ص ٧٥

^٢ د. رأفت رضوان و رشا عوض و ولاء الحسيني، الضرائب في عالم الأعمال الإلكترونية، بحث منشور في مجلة التنمية والسياسات الاقتصادية، المجلد ٢، العدد ٢، الكويت ، ٢٠٠٠،



إذاً ومما تقدم يمكننا القول إن مشكلة التهرب الضريبي باستخدام وسائل الدفع الإلكتروني أحد المشكلات القانونية الجديدة التي تواجه الاقتصاد الوطني. ونظراً للطبيعة الخاصة للوسيلة الإلكترونية (باعتبارها العنصر التقني الرئيس في نطاق عملية الدفع) فإن الحدود العامة للمشكلة المتعلقة بفرض الضرائب على معاملات الدفع الإلكتروني تتلخص في الآتي :

- إن عدم تحديد هوية الأطراف أو هوية النشاط في نطاق معاملات الدفع الإلكتروني شكّل أحد التحديات القانونية التي تواجه فرض الضرائب على هذه المعاملات.
- يتطلب فرض الضرائب على معاملات الدفع الإلكتروني البحث عن آليات جديدة لتحصيل الضرائب وجبايتها.

- قد تهاجر النقود الالكترونية من حيث خادmega التقنية المتحركة نحو الدول ذات النظم الضريبية الأسهل دون أن تترك أي أثر، الأمر الذي يشكل تحدٍ أمام السلطات الضريبية في سبيل تقفي معاملات الدفع الإلكتروني.
- يتطلب فرض الضريبة على هذه المعاملات تعاون و تنسيق دولي فعال حول معايير هذه الضريبة واستراتيجيتها.

وفي هذا الصدد فقد فرضت الولايات المتحدة الأمريكية قانون (FATCA)^١. حيث وقع بيبير موسكو فيتشي وزير الاقتصاد والمالية الفرنسي وتشارلز ريفكين سفير الولايات المتحدة في فرنسا الاتفاق على تطبيق قانون الامتثال الضريبي على الحساب الأجنبي (FATCA)، والذي يهدف لمحاربة ممارسات التهرب الضريبي بجميع أشكال الدفع الإلكتروني وتم التصويت عليه في ١٨ مارس ٢٠١٠. يستهدف هذا القانون دافعي الضرائب الذين يحملون الجنسية الأمريكية والذين لديهم حسابات خارج الولايات المتحدة الأمريكية و يستخدمون أدوات استثمارية خارجية معينة لتجنب تهريب دخلهم وأصولهم من الولايات المتحدة. حيث تسهل الاتفاقية إنشاء التبادل التلقائي للمعلومات بين فرنسا والولايات المتحدة وتحديد إطار هذا التبادل ولاسيما (وصف المعلومات التي يجب الحصول عليها وتبادلها من جهة فرنسا و الولايات المتحدة، تحديد الجدول الزمني والتفاصيل العملية لهذا التبادل)^٢.

^١ قانون (FATCA) قانون الامتثال الضريبي على الحساب الأجنبي بين فرنسا وأمريكا والذي يهدف لمحاربة ممارسات التهرب الضريبي بجميع أشكال الدفع الإلكتروني وتم التصويت عليه في ١٨ مارس ٢٠١٠.

^٢ Annabelle Pando: *Comptes PayPal : les précisions de Bercy*, LamilineDroit et Patrimoine, N° 231, 1er Décembre 2013, p. 10.

المطلب الثاني

مشكلة غسيل الأموال باستخدام وسائل الدفع الإلكتروني

مع ظهور التجارة الإلكترونية والتي تتجلى بإتمام المعاملات التجارية من خلال شبكة الإنترنت، كان لابد من إيجاد وسائل دفع جديدة تتناسب مع هذا النوع من التجارة. ولم تحمل وسائل الدفع الإلكتروني في طياتها ميزات ايجابية فقط، بل على العكس من ذلك أخذ الأشخاص يستعملون هذه الوسائل بشكل غير مشروع لغرض ارتكاب بعض الجرائم كجريمة غسل الأموال. فغاسل الأموال كأى مجرم آخر يبحث عن وسائل جديدة لم تكتشفها السلطات بعد لارتكاب جريمته. لذلك كانت وسائل الدفع الإلكتروني أحد الأساليب المتطورة والتي استخدمها الأشخاص لارتكاب جريمة غسيل الأموال، وذلك على اعتبار أن هذه الوسائل مازالت حديثة العهد الأمر الذي من شأنه أن يشكل صعوبة وارتباك لدى السلطات المختصة في التعامل معه.

وقد عُرِفَ مصطلح غسيل الأموال بأنه: «(استثمار أو تمويل آخر لتدفق الأموال من مصادر غير قانونية إلى قنوات شرعية، بحيث لا يمكن معه معرفة المصدر الأصلي كما هو الحال في صفقات المخدرات واحتجاز الرهائن والاتجار بالبشر، وتهريب الكحول والأدوية والتبغ والأسلحة والتهرب الضريبي وغيرها من الأنشطة غير المشروعة)^(١).

^١ د. شريف سعيد كامل، مكافحة غسيل الأموال في التشريع المصري، دار النهضة العربية،

في حين عرّف جانبٌ آخرٌ من الفقه غسيل الأموال بأنه: «عملية متتابعة ومستمرة في محاولة معتمدة لإدخال الأموال غير المشروعة الناتجة من الأنشطة غير المشروعة التي تمارس من خلال ما يسمى الاقتصاد الخفي»^(١).

بينما عرّف المشرع السوري غسيل الأموال بأنه: «سلوك يقصد به إخفاء أو تغيير هوية الأموال التي لها علاقة بعمليات غير مشروعة وذلك تمويتها لمصادرها الحقيقية ولكي تظهر على أنها ناجمة عن عمليات مشروعة»^(٢).

كما نص المشرع السوري على أنه: «يعد من قبيل ارتكاب جرم غسل الأموال كل فعل يقصد منه إخفاء أو تمويه الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأنها أموال غير مشروعة»^(٣).

يلاحظ على النص السابق أن المشرع السوري قد تنبه لمشكلة غسيل الأموال وأخذ بالحسبان إمكانية ارتكاب هذه الجريمة بوسيلة إلكترونية لذلك جاء النص بصيغة عامة ومطلقة دون تحديد وسيلة معينة لإخفاء أو تمويه الطبيعة الحقيقية للأموال آخذاً بالحسبان أن الثورة التقنية في مجال المعلومات قد تكشف على وسائل جديدة كوسائل الدفع الإلكتروني يمكن أن تستخدم

^١ د. عبد اللطيف عبد الحميد، العولمة و اقتصاديات البنوك، دار الجامعة الجديدة، مصر، ٢٠٠٣، ص ٢٣٤.

^٢ المادة الأولى من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥/ المتعلق بمكافحة غسيل الأموال و تمويل الإرهاب.

^٣ المادة (٢/أ، ١) من المرسوم رقم ٣٣/ لعام ٢٠٠٥/ المتعلق بمكافحة غسيل الأموال و تمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

لارتكاب هذا الجرم، وذلك بهدف إعطاء المرونة للنص التشريعي ليشمل أي شخص يرتكب غسيل الأموال مهما كانت الوسيلة المستخدمة.

إذاً يمكننا القول أن جميع التعاريف السابقة تدور حول فكرة واحدة وهي استبدال الأموال الملوثة بأموال نظيفة من خلال إدخالها في سلسلة من المشروعات والأنشطة دون تحديد أو التقيد بنشاط معين أو بوسيلة معينة.

وبما أننا في نطاق الدفع الإلكتروني فإنه يمكننا تعريف غسيل الأموال بأنه: «عملية تستهدف إضفاء الشرعية على أموال تم الحصول عليها من مصدر غير مشروع باستخدام الوسائل الإلكترونية».

إذاً لم تكن جريمة غسيل الأموال بمنأى عن التطور التقني الذي أصاب الحياة التجارية بل تطور السلوك الإجرامي للجنة فيها، ومن أهم صور هذا السلوك هو الاستعانة بالوسائل الإلكترونية في ارتكاب غسيل الأموال بمراحلها المختلفة. الأمر الذي أدى إلى زعزعة ثقة الأفراد بوسائل الدفع الإلكتروني نظراً لما يترتب على جريمة غسيل الأموال في نطاق الدفع الإلكتروني من آثار سلبية لا يمكن إغفالها.

لذلك وفي سبيل تسليط الضوء على مشكلة غسيل الأموال في نطاق الدفع الإلكتروني سوف نخصص الفرع الأول للحديث عن الأساليب الحديثة في ارتكاب غسيل الأموال على أن نتحدث في الفرع الثاني عن مراحل غسيل الأموال وآثارها السلبية.

الفرع الأول

الأساليب الحديثة في ارتكاب غسل الأموال

لقد تطور القطاع المالي والمصرفي كغيره من القطاعات مع تطور التقنيات المصاحبة للعولمة، فتطورت معه أساليب تقديم خدماته المالية والمصرفية. وبالمقابل فإن عصابات الجريمة المنظمة وغاسلي الأموال استفادوا من هذه التقنيات وبالتحديد من المخاطر المصاحبة لاستخدامها. وبذلك فقد تغيرت وسائل غسل الأموال وأصبحت تبتعد عن الأساليب التقليدية، حيث أخذت تتم بمجموعة من الأساليب الحديثة نظراً لما تتمتع به هذه الأساليب من سهولة في الأداء وسرعة في التحويل فضلاً عن طابع السرية والخصوصية الذي يكتنف الوسائل الحديثة، الأمر يجعل من اكتشاف هذه الجريمة أمراً صعباً.

لذلك وفي سبيل التعرف على الأساليب الحديثة لارتكاب غسل الأموال سوف نتحدث عن غسل الأموال بواسطة النقود الإلكترونية والبطاقات المصرفية (أولاً) ثم ننتقل للحديث عن غسل الأموال بواسطة بعض الأساليب المصرفية الأخرى (ثانياً).

أولاً: غسل الأموال بواسطة النقود الإلكترونية والبطاقات المصرفية

سوف نتحدث بداية عن غسل الأموال بواسطة النقود الإلكترونية ثم ننتقل للحديث عن غسل الأموال بواسطة البطاقات المصرفية.

١- غسل الأموال بواسطة النقود الإلكترونية: تتجلى العلاقة السلبية بين النقود الإلكترونية وجريمة غسل الأموال باستغلال غاسل الأموال لهذه النقود كوسيلة لارتكاب جريمته، فهي من أهم الأدوات الإلكترونية لغاسلي الأموال

وذلك لاستحالة تتبعها وسرعتها، حيث يمكن تحويل أي مبلغ من خلالها في فترة قصيرة دون أي إعاقات. إذ توجد إمكانية كبيرة لغسل الأموال باستخدام النقد الإلكتروني من خلال مرحلتي الإيداع والدمج ففي مرحلة الإيداع يبدأ حائز المال المراد غسله بتدوير هذا المال عن طريق إيداعه في المصرف سواء بالإيداع المادي أم الافتراضي وبذلك يتفادى القيود الورقية. أما في مرحلة الدمج يقوم الحائز بإجراء تحويلات رقمية إلى دول ليس فيها عمليات غسل أموال ثم يعيد تحويلها إلى أماكن أخرى تمهيداً لإدخالها في الحياة الاقتصادية.^١ ويتجلى دور النقود الإلكترونية في عملية غسل الأموال من ناحيتين:

أ- النقود الإلكترونية تسهل ارتكاب جريمة غسل الأموال:

ويتجلى ذلك من خلال ما يلي:

- يتم التعامل بالنقود الإلكترونية دون الحاجة إلى ظهور الهوية الحقيقية للمتعاملين وهذا الأمر يخلق فرصة لدى غاسل الأموال لاستخدامها في ارتكاب جريمته، وبالتالي لن يكن مضطراً للإفصاح عن شخصيته حتى ولو كان له تاريخ حافل في ارتكاب هذه الجريمة.
- تتمتع النقود الإلكترونية بطابع من السرية الأمر الذي يجعل مهمة السلطات المختصة بمراقبة جريمة غسل الأموال مهمة صعبة جداً، حيث يصعب مراقبة السجلات والعمليات التي تتم باستخدام هذه النقود، فضلاً على أن استخدام هذا النوع تلقائي وفي هذه الحالة

^١ د. أروى الفاعوري ود. ايناس قطيشات، جريمة غسل الأموال (المدلول العام و الطبيعة القانونية) دراسة مقارنة، دار وائل للنشر، الأردن، ٢٠٠٢، ص ٩٢.

يصبح من المستحيل مراقبة العمليات التي تتم باستخدام النقود الإلكترونية ويفسح المجال بشكل كبير لعمليات غسل الأموال^١.

- جرت العادة على أن المصارف المركزية تلعب دوراً في كشف عمليات غسل الأموال من خلال مراقبتها للأسواق المالية وهنا تبرز خطورة انتشار النقود الإلكترونية التي تؤدي إلى التأثير في ميزانية المصارف المركزية ومن ثم تنخفض الميزانية بسبب انخفاض القاعدة النقدية وهذا من شأنه أن يفقد المصارف المركزية القدرة على مراقبة الأسواق المالية و بالتالي يفسح المجال لارتكاب هذه الجريمة.

ب- النقود الإلكترونية توسّع محل جريمة غسل الأموال: يتمثل محل هذه الجريمة في الأموال غير المشروعة الناتجة عن ارتكاب الجرائم وقد تساعد النقود الإلكترونية على تأمين الأموال غير المشروعة وذلك على النحو الآتي:

- قد يؤدي استخدام النقود الإلكترونية إلى حدوث مشكلة التهرب الضريبي (وخصوصاً في ظل حالة التخبّط من مسألة فرض الضريبة على معاملات الدفع الإلكتروني)، حيث يصعب على الجهات المكلفة بتحصيل الضرائب مراقبة الصفقات التي تتم عبر الإنترنت وبالتالي يصعب فرض الضريبة عليها، ومما لاشك فيه أن الأموال التي تنتج عن التهرب الضريبي تعد أموال غير مشروعة وتحتاج للغسل.

^١ د. نادر عبد العزيز شافي، مرجع سابق، ص ٨٩.

- إن الطبيعة الخاصة للنقود الإلكترونية تجعل من الصعب التحقق من صحتها عند إبرام الصفقات. فقد يُكتشف بعد إتمام الصفقة أن النقود الإلكترونية مزيفة وبالتالي فالأموال الناتجة أموال غير مشروعة وتحتاج للغسل.
- تتعرض النقود الإلكترونية- على غرار النقود التقليدية - للسرقة، حيث يمكن الدخول إلى الأجهزة والأنظمة الخاصة بها، والمحفوظة على أجهزة الكمبيوتر ومن ثم فك شفرتها وسرقتها وهذه الأموال المسروقة هي أموال غير مشروعة وبالتالي أيضاً تحتاج للغسل^١.

كما كشف التطبيق العملي عن استخدام النقود الإلكترونية في نطاق الأعمال غير المشروعة الأمر الذي يجعل من هذه النقود محل لغسيل الأموال.

ومن الأمثلة على ذلك نذكر^٢:

- إن أحد الاستخدامات الجنائية الأكثر شيوعاً للنقود الإلكترونية هو في عمليات الحصول على فدية حيث يقوم مجرمو الإنترنت بتشفير بيانات الضحية وعدم الإفراج عنها إلا بعد أن يتم دفع مبلغ مالي بالعملة الافتراضية.

^١ المرجع السابق، ص ٨٩.

^٢ مشار لهذه الأمثلة لدى: جوشوا بارون، أنجيلا أوماهوني، دايفيد مانهايم، وسينثيا ديون -

سفارتس، تداعيات العملة الافتراضية على الأمن القومي، بحث منشور من قبل مؤسسة

RAND، الولايات المتحدة الأمريكية، ٢٠١٥، ص ٣٨. متاح على الرابط:

<http://www.rand.org/nsrd/ndri/centers/isdp.html>

تاريخ الزيارة ٢٠/١/٢٠٢٠ الساعة ١٢،٣٠ a.m

- قد تستخدم النقود الإلكترونية جنائياً لشراء البضائع غير المشروعة كالمخدرات.
- انتشار الإعلانات الإلكترونية لأنصار الدولة الإسلامية في العراق والشام (داعش) يحثون بها على جمع التبرعات بواسطة النقود الإلكترونية.

٢- غسيل الأموال بواسطة البطاقات المصرفية: يتم غسيل الأموال بواسطة نوعين من البطاقات المصرفية:

أ- بطاقات الدفع الإلكترونية: تتم عملية غسيل الأموال بواسطة بطاقة الدفع الإلكترونية من خلال ثلاث مراحل:

المرحلة الأولى: الإيداع و الإحلال: حيث يتم إيداع الأموال المشبوهة في أحد المصارف المحلية أو الخارجية والحصول على بطاقة بسقف يعادل الرصيد المودع.

المرحلة الثانية: الخداع والتمويه: حيث تستخدم هذه البطاقة فيما بعد بشراء الأصول المادية كالمعادن الثمينة واللوحات الفنية وتكون عملية الشراء مباشرة أو عن طريق الغير بتسليمه بطاقة الدفع أو بواسطة الإنترنت مع اللجوء إلى استخدام أنظمة الحماية والتشفير لضمان سرية العمليات.

المرحلة الثالثة: الدمج والإعلان: حيث يجري بيع الأصول المادية (المعادن أو اللوحات) نقداً أو لقاء شيك أو حوالة مالية مسحوبة على مصرف آخر^١.

^١ المرجع السابق، ص ٢٧.

ب- **البطاقة الذكية:** يستطيع العاملون في مجال غسيل الأموال استخدام البطاقة الذكية في جريمتهم إذ بمقدورهم تحريك القيم النقدية المشحونة على البطاقة إلى أي مكان في العالم، كما يمكنهم إضافة أي قيم نقدية على البطاقة. مما يشكل وسيلة سهلة لتغطية الأموال القذرة. حيث تسمح هذه البطاقة (كمحفظة النقود الإلكترونية) بنقل النقود دون الحاجة للاتصال بالمصرف وبالتالي يتم استخدام هذه البطاقة كوسيلة لتهريب النقود خارج البلد عوضاً عن النقود الورقية. وما يزيد خطورة البطاقة الذكية هو خاصية الاحتفاظ بالأموال على الرقاقة الإلكترونية والتقليل بها إلى أي مكان ليتم بعد ذلك نقل الأموال إلكترونياً على بطاقة أخرى أو تحويلها لنقود تقليدية الأمر الذي يستغله هؤلاء المجرمين وبمناى عن أي ملاحقة أو إشراف^١.

ثانياً: غسيل الأموال بواسطة بعض الأساليب المصرفية الأخرى

أدى التطور التقني في القطاع المصرفي إلى إحداث ثورة في الممارسات والنظم المصرفية الحالية، ومع نجاح استخدام هذه الأساليب الحديثة تزداد بشدة فرص نجاح غاسلي الأموال. ومن أبرز الوسائل الإلكترونية التي تستخدم في ارتكاب هذه الجريمة هي:

١- **أجهزة ATM:** يتم استخدام هذه الأجهزة في عمليات إيداع وسحب النقود القذرة من الحسابات المصرفية، بهدف التخلص من الإجراءات المصرفية التي تتضمن تعبئة نماذج خاصة لعمليات الإيداع والسحب، والتي قد تكشف عمليات غير شرعية. ويتم استخدام هذه الآلات في غسيل الأموال من خلال إجراء العديد من عمليات السحب والإيداع لضمان عدم الكشف ولفت الانتباه، وتماشياً

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٧٤.

مع الالتزامات القانونية المترتبة على المصارف بالإبلاغ عن عمليات الإيداع والسحب التي تتجاوز المبالغ المحددة رقابياً^١.

٢- مصارف الإنترنت: أدت شبكة الإنترنت إلى نشوء التجارة الإلكترونية، والتي يمكن عن طريقها إجراء العديد من الصفقات المشبوهة وغير القانونية والتي تسهم في عمليات غسل الأموال مستغلين صعوبة التعرف على البطاقة الشخصية وعناوين إقامة المتعاملين مع المصارف الدولية التي تتعامل عبر شبكة الإنترنت^٢. وتعتبر مصارف الإنترنت من أهم وأخطر الوسائل الحديثة لغسل الأموال، إذ يقوم المتعامل مع هذا النظام بإدخال الشفرة السرية من أرقام الحسابات والضغط على المفاتيح الملائمة لتحويل الأموال إلى أي مكان في العالم بالطريقة التي يختارها عبر الجهاز^٣. وتعد هذه الوسيلة أحدث الطرق المستخدمة في غسل الأموال لكونها أسهل استخداماً وأيسر في التعامل، وتتضمن نقل كميات كبيرة من الأموال بسرعة وأمان كبيرين وفي سرية كاملة، حيث لا هوية للمتعاملين فيها، وزيادة على ذلك لا تخضع هذه المصارف لأية قوانين رقابية نظراً لحدثة نشأتها ولل فراغ التشريعي في هذا المجال.

٣- الخدمات المصرفية الإلكترونية: تستخدم الخدمات المصرفية الإلكترونية بكثرة في عمليات غسل الأموال وخصوصاً في مرحلتي التوظيف والدمج كالتحويل الإلكتروني للأموال ودفع الفواتير... الخ .

^١ المرجع السابق، ص ٣٧٢.

^٢ د. حسام العبد، غسل الأموال في الألفية الثالثة، بحث منشور في مجلة البنوك، المجلد ١٩، العدد ٩، الأردن، ٢٠٠٢، ص ١٧.

^٣ د. حوالف عبد الصمد، مرجع سابق، ص ٣٧٢.

٤- الاتصالات الإلكترونية: تعد الاتصالات الإلكترونية من أشكال الاتصالات غير الخاضعة للقيود والضوابط والتي من أهمها البريد الإلكتروني وغرف المحادثة. وبالتالي يستطيع غاسلو الأموال استغلال هذه الوسائل في اتصالاتهم وخططهم لتنفيذ عملياتهم الإجرامية، من خلال القيام بطرح معلومات متصلة غير دقيقة حول أسعار الأسهم بهدف تضليل المستثمرين فيستغلها غاسلو الأموال في تحقيق الأرباح الطائلة والتي من شأنها أن توفر الغطاء القانوني للأموال القذرة^١.

ومن الأمثلة على استخدام الوسائل الإلكترونية في ارتكاب جريمة غسل الأموال نذكر:

- ما حدث في أمريكا حيث تمكن غاسلو الأموال من تركيب أجهزة صراف آلية مصنعة واستطاعوا من خلالها معرفة الأرقام السرية للبطاقات ثم قاموا بتزوير البطاقات واستخدامها في عمليات السحب والإيداع عن طريق أجهزة الصراف الحقيقية وبالتالي غسيل العديد من الأموال بهذه الطريقة.
- تم اكتشاف احد تجار المخدرات يقوم بعملية غسيل أمواله عن طريق فتح حسابات لبطاقات وفاء بعدة مصارف وإيداع مبالغ مالية على دفعات حتى تبدو التحويلات فيما بعد وكأنها طبيعية، ثم يقوم بالسفر إلى بلد آخر يتواجد فيه أحد شركاؤه الذي يملك محل مجوهرات يتخذة كواجهة للتضليل فيدفع له باستخدام بطاقة وفاء وهي مجرد عمليات وهمية حيث يستطيع شريكه فيما بعد تحصيل هذه المبالغ من

^١ د. أروى الفاعوري و د. ايناس قطيشات، مرجع سابق، ص ٩٤.

المصارف مصدره البطاقات ليتم بعد ذلك استخدامها في شراء مواد مخدرة^١.

• تمكنت الشرطة البريطانية في تموز عام ١٩٩٥ من ضبط عصابة متخصصة بتزوير البطاقات وعثرت على (٨٠) ألف بطاقة مزورة والتي تبين من التحقيق أنها كانت تتوي سحب مائة مليون جنيه إسترليني بواسطة هذه البطاقات من حساب عملاء حقيقيين في المصارف البريطانية وتحويل هذه الأموال مرة أخرى خارج بريطانيا بهدف إضفاء الشرعية على هذه الأموال^٢.

• الكازينوهات الافتراضية: تابعت شرطة نيويورك (FBI) هذه المواقع وركزت تحقيقها على عمليات المقامرة ومديريها، وتبين أن هذه المواقع لها مراكز على أرض الواقع وبعد خمسة أشهر من العمل المكثف، صدرت اتهامات وجرت اعتقالات بحق العديد من مدراء هذه المواقع^٣. كما انصبت الجهود على النوادي الافتراضية التفاعلية، وهي عبارة عن مواقع ويب تم تصميمها على طراز كازينو لاسفيجاس، وتوفر كل أنواع القمار وألعابه، حيث يدير هذه النوادي عدة أفراد انطلاقاً من منازلهم أو مكاتبهم و يدفعون رسوم لحكوماتهم تتراوح بين ٧٥ ألف دولار (للمراهات الرياضية) و ١٠٠ ألف دولار (للكازينوهات الافتراضية)^٤.

^١ د. أمجد الجهني، مرجع سابق، ص ٢٨.

^٢ المرجع السابق، ص ٢٨.

^٣ راجع الرابط:

[www.tartoos.com /Home page / Rtable / computer school/internet/internet basic 2/internet 80.htm](http://www.tartoos.com/Home_page/Rtable/computer_school/internet/internet_basics2/internet_80.htm)

تاريخ الزيارة ٢٠١٨/١٢/٥ الساعة ١١:٢٠ a.m

^٤ راجع الرابط: www.arablalaw.com

تاريخ الزيارة ٢٠١٨/١٢/٥ ١٢:١٥ p.m

الفرع الثاني

مراحل غسل الأموال وآثارها السلبية

حتى نتمكن من معرفة الآثار السلبية لغسيل الأموال، لابد بدايةً من التعرف على المراحل التي تتم بها هذه الجريمة وخصوصاً فيما يتعلق بالنقود الإلكترونية، وذلك على اعتبار أن النقود الإلكترونية من أكثر الوسائل تسهياً لانتشار غسل الأموال في ظل طابع السرية الذي يكتنف التعامل بهذه النقود، الأمر الذي يجعل هوية الأطراف غير معلومة وبالتالي تعذر اكتشاف هذه الجريمة.

وبناءً على ذلك سوف نتحدث عن مراحل غسل الأموال (أولاً) ثم ننتقل للحديث عن الآثار السلبية لغسيل الأموال (ثانياً).

أولاً: مراحل غسل الأموال

تتضمن عملية غسل الأموال سلسلة من الصفقات المتعددة التي تهدف إلى تمويه مصدر الأصول المالية بحيث يمكن أن تستخدم هذه الأصول وكأنها أموال شرعية ناتجة عن عمليات مشروعة، فهي جريمة تقوم على صناعة واقع مزيف وجعله حقيقي. ولهذا تكون عملية غسل الأموال جريمة يتم ارتكابها من خلال تنظيم مؤسسي يضم عدداً من الأفراد المحترفين الذين يعملون في إطار منظم ووفق هيكلية بالغة في التنفيذ والسرية، كما يمكن أن ترتكب بفعل تواطؤ بعض الموظفين بتسهيل عمليات إيداع الأموال القذرة في المصارف. وتتمثل مراحل هذه الجريمة فيما يخص النقود الإلكترونية بما يلي:

١- **مرحلة الأموال المشروعة:** ويتم في هذه المرحلة التعرف على الأموال الموجودة في مصادرها الأصلية عن طريق استخدام الوسائل الإلكترونية الحديثة، والدخول إلى أنظمة المعلومات وبرمجيات المصارف أو أية مصادر للأموال النظيفة، ومحاولة فك شفراتها السرية والبدء في التخطيط لكيفية سرقتها.

٢- **مرحلة جميع المبالغ بطرق غير مشروعة:** ويتم في هذه المرحلة السحب للأموال بطرق غير مشروعة، وباستخدام الشفرات السرية لأرقام حسابات المصارف وعملاتهم عن طريق الأجهزة الإلكترونية من حواسيب وإنترنت.

٣- **مرحلة إدارة الأموال غير المشروعة:** تستخدم في هذه المرحلة أنظمة وبرامج حاسوبية، للمساعدة في التخطيط والتنظيم والرقابة والمحافظة على الأموال غير المشروعة التي تم الحصول عليها من مصادرها الأصلية^١.

٤- **مرحلة التوظيف:** يتم التوظيف للأموال القذرة عن طريق :

أ- التحويل الإلكتروني للأموال القذرة إلى حسابات مصرفية خارجية.

ب- تحويل الأموال القذرة إلى نقود إلكترونية.

ج- الدخول الإلكتروني إلى الأسواق المالية لشراء الأسهم والسندات.

^١ محمد عبد الله، الاتجاهات الحديثة لأعمال المصارف (الصيرفة الإلكترونية) رسالة ماجستير،

٥- **مرحلة التغطية:** يتم إخفاء العلاقة بين الأموال القذرة ومصادرها الأصلية بطريقة مباشرة ودون وسيط من خلال :

أ-إبرام الصفقات المشبوهة عبر الإنترنت أو البريد الإلكتروني.

ب-إنشاء الشركات الوهمية وبأسماء وهمية والتعامل معها.

ج-الدخول إلكترونياً إلى مواقع الأسواق المالية الأولية لإصدار أسهم وسندات وهمية.

د-شراء أصول مادية ودفع ثمنها عن طريق وسائل الدفع الإلكتروني بشكل غير مشروع^١.

٦- **مرحلة الدمج :** يتم في هذه المرحلة خلق الإحساس بمشروعية الأموال القذرة ومحاولة دمجها بالدورة الاقتصادية من خلال:

أ-الإيداع الإلكتروني للنقود الناتجة من الصفقات والشركات المشبوهة في المصارف الإلكترونية.

ب-الدخول إلكترونياً إلى الأسواق المالية والقيام بعمليات البيع والشراء للأسهم والسندات.

ج-القيام بعمليات التجارة الإلكترونية.

^١ د. عبد اللطيف عبد الحميد، البنوك الشاملة (عملياتها ، إدارتها)، دار الجامعة الجديدة،

ثانياً: الآثار السلبية لجريمة غسل الأموال

تخلّف عمليات غسل الأموال آثاراً سلبية تطلّ جوانب الحياة الاقتصادية والاجتماعية والسياسية والأمنية جميعها، لكن سوف نقتصر الحديث في هذا الصدد على الجانب المصرفي فقط:

١- تؤدي عمليات غسل الأموال إلى إفساد المصارف نتيجة المعاملات غير المشروعة التي تتم فيها وما يرافق ذلك من دفع رشاوى وشراء ذمم الموظفين.

٢- تلجأ المصارف الرافضة لعمليات غسل الأموال إلى الحد من السرية المصرفية لتتمكن من مراقبة هذه العمليات ومواجهتها، فتفقد الكثير من عملائها، فليس هناك من يقبل أن يتعامل مع مصرف لا يلتزم بالسرية المصرفية أو يخرقها كثيراً مما يؤثر سلباً على النشاط المصرفي.

٣- يمكن أن يؤدي غسل الأموال إلى انهيار البورصة التي تستقبل الأموال الناتجة عن هذه الجريمة. إذ يتم اللجوء إلى شراء الأوراق المالية من البورصة من أجل إتمام مرحلة من مراحل الغسل و ليس بهدف الاستثمار كما يتم بيعها بشكل مفاجئ مما يؤدي إلى حدوث انخفاض في أسعار الأوراق المالية في البورصة ومن ثم انهيارها^١.

وبناءً عليه يمكن القول إن تطور الحياة المعاصرة قدم للإنسان وسائل جديدة تمكنه من إتمام معاملاته المالية بكل يسرٍ وسهولة، لكنّ غاسلو الأموال لم

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٧٤.

يتوانوا عن استغلال هذه الوسائل لارتكاب جرائمهم. فبدلاً من أن تسهم هذه الوسائل الحديثة في الحد من ظاهرة غسيل الأموال أو تساعد في اكتشافها، شكلت وسائل الدفع الإلكتروني بمختلف وسائلها (النقود الإلكترونية، البطاقات المصرفية، مصارف الانترنت... الخ) البيئة الخصبة والملائمة للتوسع في ارتكاب هذه الجرائم وذلك على غرار (مسألة انتهاك السرية المصرفية). الأمر الذي من شأنه أن يحدث آثار اقتصادية واجتماعية ضارة بالمجتمع ويبعث على التخوف لدى الأفراد من الإقدام على التعامل بالوسائل الإلكترونية.

وفي ختام الحديث عن التعريف بالمشكلات القانونية للدفع الإلكتروني نصل إلى نتيجة مفادها إن دخول الوسيلة الإلكترونية كأحد العناصر التقنية الرئيسة في نطاق الدفع تولد عنه ثلاثة آثار سلبية من الناحية القانونية:

حيث تمثل الأثر الأول في ظهور وسائل وأساليب جديدة في ميدان ارتكاب بعض الجرائم التقليدية المعروفة الأمر الذي وسع من نطاق هذه الجرائم ومثال ذلك (مشكلات انتهاك السرية المصرفية وغسيل الأموال).

بينما تجلّى الأثر الثاني من خلال ظهور مشكلات جديدة لم تكن معروفة من قبل كشف عنها التطور التقني في مجال الدفع (كمشكلات الشراء عبر الحدود والمشكلات التقنية التي تصيب المستهلك الإلكتروني).

في حين تبلور الأثر الثالث من خلال ظهور المشكلات التقليدية المعروفة بصيغة جديدة لم تكن معروفة من قبل كالمشكلات القانونية التي تواجه المستهلك الإلكتروني ومشكلات التهرب الضريبي. وأمام هذه المشكلات والتحديات تبرز الحاجة الملحة للبحث في سبل معالجة هذه المشكلات بغية توفير الثقة بمعاملات الدفع الإلكتروني .

الفصل الثاني

سبل معالجة المشكلات القانونية

بعد أن تعرفنا في الفصل الأول على أهم المشكلات القانونية لوسائل الدفع الإلكتروني تبرز الحاجة الملحة للتعرف على الأساليب والوسائل الكفيلة بمعالجة هذه المشكلات. وينبغي في أساليب المعالجة أن تكون موجهة بشكل مباشر لكل مشكلة من هذه المشكلات حتى تكون هذه الأساليب كفيلة بالقيام بدورها. وبشكل عام تتجلى أساليب معالجة المشكلات القانونية على النحو الآتي :

حيث تمت معالجة المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف من خلال ترتيب المسؤولية القانونية بحق من ينتهك سرية البيانات الشخصية.

أما بخصوص المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً فقد كان جوهر الحل القانوني يتجلى بالبحث في النصوص القانونية المتوفرة لغرضين:

حيث يتمثل الغرض الأول في معرفة مدى إمكانية تطويع هذه النصوص لسد بعض الثغرات التي أنتجتها وسائل الدفع الإلكتروني لمعالجة مشكلة القانون الواجب التطبيق والمحكمة المختصة.

بينما يتجلى الغرض الثاني بالبحث عن مدى إمكانية تطبيق بعض النصوص القانونية التقليدية على المستهلك الإلكتروني بغية توفير الحماية القانونية له من بعض المشكلات التقليدية التي تظهر بقالب

جديد مختلف عن الشكل التقليدي. هذا فيما يتعلق بالمشكلات التي تواجه مستخدم أداة الدفع الإلكترونية.

أما بالنسبة للمشكلات التي تواجه الاقتصاد الوطني، فلا تختلف أساليب معالجة هذه المشكلات من حيث المبدأ عن أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع. فقد تجلت أساليب معالجتها على النحو الآتي :

حيث كان الحل القانوني لمشكلة التهرب الضريبي يتجه نحو البحث عن سبل وأساليب لكيفية فرض الضريبة وتحصيلها بالنسبة لمعاملات الدفع الإلكتروني.

في حين تجلّى العلاج القانوني لمشكلة غسيل الأموال من خلال ترتيب المسؤولية القانونية بحق مرتكب هذه الجريمة.

وفي سبيل الإحاطة الشاملة بسبل معالجة المشكلات القانونية سوف نتحدث عن أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية وذلك في المبحث الأول على أن نتعرف على أساليب معالجة المشكلات التي تواجه الاقتصاد الوطني في المبحث الثاني.

المبحث الأول

أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية

تختلف أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية باختلاف صفته سواء أكان عميلاً أم مستهلكاً، ومرد هذا الاختلاف إلى أن المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف هي واحدة كونها ناشئة عن طبيعة العمل المصرفي بشكل عام بغض النظر عن دخول الوسيلة الإلكترونية، أما المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً فهي نتيجة دخول الوسيلة الإلكترونية. وبالتالي بالنسبة للمشكلات التي تواجه المستخدم كعميل هناك نصوص قانونية صريحة تعالج هذه المشكلات، أما المشكلات التي تواجه المستخدم كمستهلك إلكتروني تقوم أساليب المعالجة على البحث في مدى إمكانية تطويع النصوص القانونية لتطبيقها على هذه المشكلات بغية توفير الحماية القانونية للمستهلك الإلكتروني.

لذلك وفي سبيل التعرف على هذه الأساليب سوف نتحدث عن وسائل معالجة المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف وذلك في المطلب الأول على أن نتعرف على وسائل معالجة المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً وذلك في المطلب الثاني.

المطلب الأول

وسائل معالجة المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف

تقوم هذه الوسائل في مجملها على حماية البيانات الشخصية للأفراد ضد المحاولات غير المشروعة لانتهاكها، ولكن بعض هذه الوسائل كان عبارة عن مبادئ والتزامات تأخذ شكل التدابير الوقائية وهذا ما وجدناه لدى المشرع الأمريكي، والبعض الآخر كان عبارة عن مسؤولية قانونية تأخذ شكل التدابير العلاجية وهذا ما لحظناه لدى المشرع السوري.

لذلك وفي سبيل إغناء البحث القانوني سوف نتحدث عن الحماية القانونية للمعلومات الخاصة بالعملاء لدى المشرع الأمريكي في الفرع الأول على أن نتعرف على الحماية القانونية للمعلومات الخاصة بالعملاء لدى المشرع السوري في الفرع الثاني.

الفرع الأول

الحماية القانونية للمعلومات الخاصة بالعملاء لدى المشرع الأمريكي

أكد المشرع الأمريكي على الحماية القانونية للمعلومات الخاصة بالعملاء في العديد من النصوص القانونية إلا أن هذه الحماية تتسم بالغموض، إضافة إلى أنها عندما تتعارض مع القانون الاتحادي فإن السيادة تكون للقانون الاتحادي الأمر الذي يضعف من دورها في

حماية الخصوصية^١ ومن النصوص القانونية التي أكدت على هذه الحماية نذكر:

أولاً: قانون الحق بالخصوصية المالية

(RFPA) the right to privacy financial act: يمنع هذا القانون الحكومات الفيدرالية من الدخول أو الحصول على معلومات من السجلات المالية للعملاء، كما يمنع المصارف من الإعلان عن هذه المعلومات ما لم يتم الحصول على ترخيص مسبق من العميل^٢.

ثانياً: القانون الخاص بالتحويل الالكتروني للأموال

(EFTA) Electronic fund transfer act و **Regulation E**: يلزم كلا منهما المصارف بإبلاغ العملاء خطياً بالطريقة التي سيتم من خلالها التعامل مع المعلومات والبيانات المالية الخاصة بهم وذلك عن طريق إعطائهم الشرح اللازم حول بعض الحالات التطبيقية في هذا الإطار^٣.

ثالثاً: القانون الخاص بتقديم التقارير الائتمانية

(FCRA) the fair credit Reporting act: لقد تم بموجب هذا القانون إنشاء وكالة خاصة بإعطاء تقارير عن معلومات العملاء وهي الوحيدة المخولة بنقل مثل هذه المعلومات إلى شخص ثالث،

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٤٨٠.

^٢ هذا القانون مشار إليه لدى د. طارق حمزة، مرجع سابق، ص ٤٥٤.

^٣ هذا القانون مشار إليه لدى د. حوالف عبد الصمد، ص ٤٨٠.

على أن يكون لهذا الأخير أسباب وجيهة تبيح له الحصول على مثل هذه المعلومات أي أن يستعملها لأغراض مسموح بها. وهذا يستوجب أن يكون العميل قد أعطى موافقته الخطية في سياق معاملاته الائتمانية أو لأغراض العمل. كما يحق للأشخاص والمؤسسات المنتسبة لهذا النظام الاطلاع على هذه المعلومات شريطة أن يكون العميل قد تلقى إشعاراً بذلك وضمانات بعدم إعطاء أي معلومات لا يسمح بها^١.

ونحن من جانبنا لا نؤيد وجود وكالة خاصة بإعطاء المعلومات السرية وذلك لأن هذا الأمر يشكل نوعاً من الخرق للسرية المصرفية لأن المصرف هو الجهة الوحيدة المخولة بإعطاء المعلومات السرية في حالات محددة قانوناً أما إعطاء هذه الوكالة مثل هذا الحق فهو نوع من تعزيز انتهاك السرية وليس تعزيز الحماية.

رابعاً: قانون الخصوصية (Privacy Act 1994): لقد جاء هذا القانون بمجموعة من المبادئ الموجهة لكافة الأشخاص المتعاملين بالمعلومات الإلكترونية. وقد تم تقسيمهم إلى ثلاث فئات^٢:

الفئة الأولى: وتشمل الأشخاص المشاركين في المجال المعلوماتي. وتتسم بثلاث مبادئ:

^١ هذا القانون مشار إليه لدى د. طارق حمزة، مرجع سابق، ص ٤٥٣.

^٢ هذا القانون مشار إليه لدى د. حوالف عبد الصمد، مرجع سابق، ص ٤٨١.

- مبدأ خصوصية المعلومات: يقصد به الحصول على المعلومات الشخصية وكشفها واستخدامها بطرق تحترم خصوصية الفرد.

- مبدأ سلامة المعلومات: يقصد به عدم تغيير أو إتلاف المعلومات الشخصية بصورة غير ملائمة.

- مبدأ جودة المعلومات: يقصد به أن تكون المعلومات الشخصية دقيقة وفي الوقت الملائم ومن أجل غرض محدد.

الفئة الثانية: وتشمل الأشخاص مستخدمي المعلومات الشخصية وتتسم بخمسة مبادئ:

- مبدأ الامتلاك: يلزم هذا المبدأ مستخدمي المعلومات تقييم مدى التأثير الذي يحدثه امتلاك المعلومات أو كشفها أو استخدامها على الخصوصية.

- مبدأ الإخطار: يلزم هذا المبدأ مستخدمي المعلومات بتقديم المعلومات الكافية عن الجدوى من جمع المعلومات وما هي الخطوات التي ستتخذ لحماية سرية هذه المعلومات.

- مبدأ الحماية: يلزم هذا المبدأ مستخدمي المعلومات استخدام ضوابط فنية وإدارية مناسبة لحماية سرية المعلومات.

- مبدأ العدالة: يلزم هذا المبدأ مستخدمي المعلومات عدم استخدام المعلومات الشخصية بطرق لا تتفق مع فهم الفرد للكيفية التي تستخدم بها مالم يكن هناك مصلحة عامة اضطرارية لذلك.

- مبدأ التوعية: يلزم هذا المبدأ مستخدمي المعلومات القيام بتوعية العملاء حول كيفية الحفاظ على خصوصية المعلومات.

الفئة الثالثة: وتشمل الأفراد الذين يقدمون المعلومات. وتتضمن ثلاثة مبادئ:

- مبدأ الوعي: يقصد به أن يكون الفرد على دراية و معرفة بالجدوى من جمع المعلومات عنه، وبالخطوات التي سوف تتخذ لحماية هذه المعلومات.
- مبدأ التمكين: يقصد به تمكين الفرد من تصحيح معلوماته الشخصية غير الدقيقة أو غير الصحيحة باستخدام ضوابط فنية.
- مبدأ العدالة: يقصد به أن يكون لدى الأفراد وسيلة يتم اللجوء إليها لحماية معلوماتهم الشخصية في حال الاستخدام غير المشروع لها.

الفرع الثاني

الحماية القانونية للمعلومات الخاصة بالعملاء لدى المشرع السوري

يلتزم المصرف بموجب التشريع السوري بعدم إفشاء أي معلومة حصل عليها أثناء ممارسة نشاط العميل أو بسبب هذا النشاط وذلك باستثناء الحالات المذكورة في القانون، وإذا خالف الحظر وأفشى هذه الأسرار يكون مسؤولاً عند هذا الإفشاء ويترتب عليه مسؤولية جزائية وأخرى مدنية. وبالتالي فقد شكلت المسؤولية القانونية أحد أهم أساليب معالجة المشكلات التي تتعلق بانتهاك السرية المصرفية.

لذلك سوف نتحدث عن المسؤولية الجزائية المترتبة على انتهاك السرية المصرفية (أولاً) ثم ننتقل للحديث عن المسؤولية المدنية المترتبة على انتهاك السرية المصرفية (ثانياً).

أولاً: المسؤولية الجزائية

إن انتهاك المعلومات الشخصية للعملاء جريمة كغيرها من الجرائم، وبالتالي لابد فيها من توافر الأركان العامة لأي جريمة، وبما أن انتهاك هذه المعلومات يتم بشكل إلكتروني ينبغي توفر بعض الأركان الخاصة بها. وفي سبيل تسليط الضوء على المسؤولية الجزائية سوف نقوم بطرح عدة أسئلة ومن ثم الإجابة عنها:

١- هل أكد المشرع السوري على الحماية القانونية الخاصة بالمعلومات المعالجة إلكترونياً أم أنه اكتفى بالأحكام العامة في قانون السرية المصرفية؟

أ- لقد اعتبر المشرع السوري أن المعلومات والبيانات الشخصية والمالية محل الالتزام بالسرية المصرفية، وقد جاءت أحكام قانون السرية المصرفية بصيغة عامة ومطلقة (عبارة معلومات) دون تحديد شكل هذه المعلومات فقد تكون معلومات بشكل تقليدي أو معلومات معالجة إلكترونياً^١، وبالتالي يمكن القول أن المشرع السوري ألزم بحماية المعلومات الإلكترونية بموجب قانون السرية المصرفية وذلك لان الإطلاق يجري على إطلاقه.

ب- جاء المشرع ليقطع دابر الشك في قانون المعاملات الإلكترونية وقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية وذلك بالنص صراحة على الالتزام بحماية المعلومات الإلكترونية في

^١ المادتان ٢٩، ٢/ من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

قانون المعاملات الإلكترونية^١، وترتيب المؤيد الجزائي بحق من ينتهك حرمة هذه البيانات في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية^٢.

وبالنتيجة يمكننا القول إن المعلومات المعالجة إلكترونياً محل الالتزام بالسرية المصرفية سواء بموجب الأحكام العامة أم بموجب الأحكام الخاصة وأي إفشاء غير مشروع لها يستوجب المسؤولية.

٢- ما هي الأركان العامة لجريمة انتهاك السرية المصرفية بشكل إلكتروني ؟

تتمثل الأركان العامة في الآتي:

أ- **الركن المادي:** بما أن جريمة انتهاك السرية كغيرها من الجرائم فلا بد أن يتضمن الركن المادي العناصر الأساسية فيه وهي:

أ- **الفعل الجرمي:** قد يكون الفعل الجرمي عبارة عن نشاط إيجابي وذلك عندما يقوم المصرف أو أحد موظفيه بإعطاء المعلومات السرية لشخص لا يحق له الاطلاع على هذه المعلومات سواء أقام بهذا الإعطاء من تلقاء ذاته أو بناءً على طلب الغير وبأي وسيلة كانت، أو قد يكون نشاط سلبي عندما يقوم أحد موظفي المصرف بترك جهاز الكمبيوتر الذي يحتوي على المعلومات

^١ المادة ٢٣/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

^٢ المادتان ٩، ٢٣/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

السرية مفتوحاً أمام شخص لا يحق له الاطلاع عليها أو يشاهده يطلع على هذه المعلومات أو السجلات الإلكترونية ولا يمنعه.

ب- النتيجة الجرمية: وهي الأثر المترتب على الفعل الجرمي والمتمثل في وصول المعلومات إلى علم الغير الذي لا يحق له الاطلاع عليها.

ج- علاقة السببية بين الفعل والنتيجة: أي لا بد أن يكون نشاط الموظف الجرمي هو السبب الأساسي لوصول هذه المعلومات إلى الغير، أما لو وصلت هذه المعلومات لعلم الغير بغض النظر عن نشاط الموظف فهنا لا يوجد علاقة سببية وبالتالي لا يُسأل المصرف عن الجريمة.

ب- الركن المعنوي: يقوم الركن المعنوي لهذه الجريمة على عنصر العلم والإرادة، وإذا توفر هذين العنصرين قلنا أن الجريمة مقصودة أما إذا اختل أحد العنصرين وخصوصاً العلم تعد جريمة غير مقصودة.

٣- ما هي الأركان الخاصة بجريمة انتهاك السرية بشكل إلكتروني؟

تتمثل الأركان الخاصة في الآتي:

أ- توفر صفة خاصة بالفاعل: يشترط في الفاعل أن يكون قد علم بأسرار العميل بسبب نشاط العميل مع المصرف أو أثناء ممارسة النشاط، أما إذا كان الفاعل لم يعلم بهذه الأسرار أو لم يطلع عليها أثناء ممارسة النشاط أو بسببه فلا يسأل عن إخلاله بالسرية كونه

في هذه الحالة ملتزم أخلاقياً وليس قانونياً. وبالتالي قد يكون الفاعل من موظفي المصرف أو ممن أُسند إليه عمل في المصرف يمكنه من الاطلاع على هذه الأسرار (كمدقق حسابات المصرف أو مبرمج نظام الكمبيوتر) أو كل من اطلع على هذه الأسرار بحكم وظيفته أو صفته (كعمال النظافة أو عمال البوفيه). وتجدر الإشارة إلى أن الهاكرز أو السارق الذي يطلع على الأسرار ويفشيها يعد مسؤول جزائياً عن الجرم ولكن يسأل المصرف عن التعويض فقط وفقاً لأحكام المسؤولية التقصيرية.

ب-توافر صفة خاصة في المجني عليه: يشترط في المجني عليه أن يكون أحد عملاء المصرف على اعتبار أن للسرية المصرفية طرفان المصرف والعميل. وبالتالي لا يكفي أن يكون الإقضاء من قبل من اطلع على هذه المعلومات أو من قبل موظفي المصرف بل لا بد أن يكون المتضرر عبارة عن شخص عميل للمصرف وإذا اختل هذا الشرط لم تتوفر الجريمة^١.

ج-وجود صفة الادعاء الشخصي: لا تحرك دعوى الحق العام إلا بناءً على شكوى الفريق المتضرر^٢. وبما أن هذا الحق مقرر له فإنه يحق له التنازل عن هذا الحق وفي هذه الحالة تسقط دعوى الحق العام.

د-وجود صفة خاصة في محل الجريمة ووسيلة ارتكابها: تعد جريمة انتهاك السرية المصرفية بشكل إلكتروني من قبيل الجرائم

^١ د. بسام الزلمي، مرجع سابق ، ص ٢٤٨.

^٢ المادة ٩/ من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

المعلوماتية التي يقصد بها: (كل جريمة ترتكب باستخدام المنظومة الحاسوبية أو الشبكة أو تقع على المنظومة المعلوماتية أو الشبكة^(١)).

وبالتالي يفترض في جريمة انتهاك المعلومات الشخصية بشكل إلكتروني أن يكون محلها عبارة عن منظومة معلوماتية (المعلومات المخزنة على الشبكة) و أن تُرتكب بوسيلة إلكترونية وذلك نظراً للطبيعة الإلكترونية لمحل هذه الجريمة الأمر الذي يحتم أن تكون وسيلة ارتكابها وسيلة إلكترونية.

٤- من يتحمل المسؤولية الجزائية عن هذه الجريمة ؟

نص قانون العقوبات على أنه: «الهيئات الاعتبارية مسؤولة جزائياً عن أعمال مديريها وأعضاء إدارتها وممثليها وعمالها عندما يأتون هذه الأعمال باسم الهيئات أو بإحدى وسائلها ولكن لا يمكن الحكم عليها إلا بالغرامة والمصادرة ونشر الحكم^(٢)».

إذاً عندما يقوم الموظف بهذه الجريمة باسم الشخص الاعتباري /المصرف/ أو بإحدى وسائله يكون المصرف مسؤول جزائياً، ولكن لا يعاقب المصرف إلا بالغرامة أو المصادرة ونشر الحكم. أي يمكن القول أن المصرف مسؤول جزائياً ولكن فقط من الناحية المالية. ولكن عندما يقوم الموظف بهذه الأفعال دون استعمال اسم المصرف أو دون استعمال إحدى وسائله (يقوم بالعمل بصفته الشخصية) أو (في

^١ المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

٢٠١٢.

^٢ المادة ٢٠٩/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

حال ارتكب الجرم من قبل السارق)، فهنا (الموظف، السارق) وحده مسؤول جزائياً كون المسؤولية الجزائية شخصية، ولكن يبقى المصرف مسؤول بالتعويض عن الضرر وفقاً لأحكام المسؤولية المدنية إذا توافرت أركانها. وغالباً عندما يكون الشخص المسؤول عن الجرم معلوم الهوية تقام عليه الدعوى الجزائية أما عندما لا يكون معروفاً تقام الدعوى على المصرف. لكن في الحقيقة ومن الأفضل بالنسبة للمدعي أن يقيم الدعوى الجزائية والمدنية على المصرف معاً وبغض النظر عن الفاعل كون المصرف أكثر ملاءمة مالية.

٥- ما هي العقوبة الجزائية بحق مَنْ ينتهك البيانات الشخصية إلكترونياً؟

نص قانون السرية المصرفية على أنه: ((مع عدم الإخلال بأي عقوبة أشد يعاقب بناء على شكوى المتضرر بالحبس من ٣ أشهر إلى سنة كل من أقدم أو شرع على إفشاء معلومات.....الخ^(١))).

بينما نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه: ((يعاقب بالحبس من شهر إلى ستة أشهر وبالغرامة من مئة ألف إلى خمسمائة ألف ليرة سورية كل من

^١ المادة التاسعة من قانون السرية المصرفية رقم ٣٠/ لعام ٢٠١٠.

نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه حتى ولو كانت تلك المعلومات صحيحة^(١).

كما نص ذات القانون على أنه: "يعاقب مقدم الخدمات على الشبكة الذي يقوم بإفشاء المحتوى أو البيانات أو المعلومات المخزنة لديه مخالفاً بذلك التزامات المحافظة على سر المهنة بالغرامة من مئتي ألف إلى مليون ليرة سورية مع حفظ حق المتضرر بالمطالبة بالتعويض"^(٢).

والسؤال الذي يطرح نفسه أي من المواد سألقة الذكر تطبق؟

في الحقيقة الشخص الذي ينتهك البيانات الشخصية إلكترونياً يعاقب وفق أحكام المادة (٢٣) والمادة (٩) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية وذلك بحسب من قام بالإفشاء سواء موظفي المصرف أم الغير وذلك للمبررات الآتية:

أ- هذه الجريمة هي جريمة معلوماتية الأمر الذي يستوجب تطبيق قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية كونه قانون خاص بينما قانون السرية المصرفية قانون عام في هذا الخصوص والخاص يقيد العام.

^١ المادة /٢٣/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ المادة /٩/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

ب- جاء نص المادة التاسعة من قانون السرية المصرفية بعبارة (مع عدم الإخلال بأي عقوبة أشد ...)، كما نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه: ((إذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون تطبق العقوبة التي هي أشد^(١))).

وبالتالي فإن المشرع السوري أخذ بالحسبان أنه يمكن أن يطبق نص جزائي في أي قانون على أي جريمة معلوماتية فعمل على تلافي ذلك بالنص على تطبيق العقوبة الأشد. وبالتالي لا بد من تطبيق أحكام المادة /٢٣/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية كونها جاءت بعقوبتين (الحبس والغرامة) أما قانون السرية المصرفية فقد جاء بعقوبة واحدة (الحبس). وبالتالي فإن المؤيد الجزائي الذي جاءت به المادة /٢٣/ يطبق على كافة الأسرار الشخصية والعائلية والمالية إذا كان المنتهك للأسرار شخص من الغير (أي ليس من قبل المصرف أو موظفيه أو أي مقدم خدمات إلكتروني تابع للمصرف) كمخترقي البرامج و الهاكرز. أما إذا كان الإفشاء من قبل المصرف (موظفيه أو مقدمي خدمات الإنترنت) فإن

^١ المادة (٢٨/أ) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام

العقوبة هي الغرامة من مئتي ألف إلى مليون ليرة مع حفظ حق المضرور بالمطالبة بالتعويض^١.

وتجدر الإشارة إلى أن ما تحدثنا عنه أنفاً إنما كان في نطاق قانون السرية المصرفية السوري وقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية باعتبارهما من القوانين التي تناولت حرمة الحياة الخاصة بشكل صريح بالنسبة للعمل المصرفي ولكن إلى جانب هذه النصوص فقد أكد المشرع السوري على حماية الحياة الخاصة بمختلف أشكالها من خلال عدة نصوص قانونية نذكر منها:

- حيث جرم قانون العقوبات كل من يدخل منزل أو مسكن شخص خلافاً لإرادته أو المكوث فيه وعاقبه بالحبس مدة لا تتجاوز ست أشهر وإذا تم الفعل ليلاً أو بالكسر أو بالعنف أو باستعمال السلاح أو ارتكبه عدة أشخاص مجتمعين بالحبس من ثلاثة أشهر إلى ثلاث سنين^٢.
- جرم قانون العقوبات من كان بحكم وضعه أو وظيفته أو مهنته أو فنه على علم بسر وأفشاه دون سبب مشروع أو استعمله لمنفعته الخاصة أو لمنفعة آخر وعاقبه بالحبس سنة على الأكثر وبغرامة لا تتجاوز ٢٠٠ ليرة إذا كان من شأن الفعل أن يسبب ضرراً ولو معنوياً^٣.

^١ المادة التاسعة من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ المادة ٥٥٧/ من قانون العقوبات رقم ١٨٤/ لعام ١٩٤٩.

^٣ المادة ٥٦٥/ من قانون العقوبات رقم ١٨٤/ لعام ١٩٤٩.

- جرم قانون العقوبات كل من انتهك سرية المراسلات إذا كان مرتكب الفعل موظف في مصلحة البريد أو الاتصالات واطلع على رسالة مختومة أو أتلّفها أو أفضى بمضمونها إلى غير المرسل إليه فبعاقب بالحبس من شهرين إلى سنتين وتعامل المكالمات الهاتفية معاملة الرسائل عند الاطلاع عليها أو إفشائها أما إذا كان المطلع أو من أفشى المخابرة شخص غير المذكور في المادة السابقة فإنه يعاقب بغرامة لا تتجاوز ٢٠٠٠ ليرة^١.

نستج من النصوص السابقة أن المشرع السوري أكد على حرمة الحياة الخاصة بمختلف أشكالها (حرمة مسكن-حرمة المراسلات-الاسرار الشخصية والمهنية) في حال كان المنتهك شخص من خارج العمل المصرفي وذلك باعتبار أن هذا الحق من الحقوق المقررة بنص دستوري وقانوني في ان واحد.

ثانياً: المسؤولية المدنية

إلى جانب المسؤولية الجزائية التي قد تترتب على الإفشاء هناك مسؤولية مدنية للمطالبة بالتعويض عن الضرر المادي أو المعنوي الذي أصاب العميل من جراء الإفشاء. وعلى غرار المسؤولية الجزائية وفي سبيل تسليط الضوء على المسؤولية المدنية سوف نقوم بطرح عدة أسئلة ومن ثم الإجابة عنها:

^١ المواد ٥٦٦-٥٦٧/ من قانون العقوبات رقم ١٨٤/ لعام ١٩٤٩.

١- ما هي أحكام المسؤولية المدنية عن انتهاك المعلومات الشخصية للعملاء؟

تتخذ المسؤولية المدنية عن انتهاك المعلومات الشخصية للعملاء أحد شكلين:

أ- **المسؤولية العقدية:** تفترض العلاقة بين المصرف والعميل أن يقوم كل منهما بتنفيذ التزاماته وفق الأحكام العامة في العقود سواء تمثلت تلك العلاقة في عقد حساب مصرفي أو عقد ودیعة أو غيرها من العمليات المصرفية. حيث يجب تنفيذ العقد طبقاً لما اشتمل عليه، وكما هو معلوم أن تنفيذ العقد لا يقتصر على إلزام المتعاقد بما ورد فيه بل يتناول أيضاً ما يعد من مستلزماته وفقاً للقانون أو العرف أو طبيعة التعامل^١. وتجدر الإشارة إلى أن مثل هذه العقود قد لا تتضمن التزام بالسرية المصرفية بل يكون هذا الالتزام مفترضاً استناداً للعرف المصرفي الذي يقضي أن لا يفشي المصرف أي معلومة حصل عليها بحكم نشاط العميل أو بسبب هذا النشاط وفي حال أخل بهذا الالتزام فتتعدّد مسؤولية المصرف العقدية إذا توافرت شروطها وهي:

أ- **الخطأ:** يتمثل هذا الخطأ بالإخلال بواجب الالتزام الذي يفرضه العقد الذي أبرمه العميل مع المصرف. إذ وفقاً لهذا العقد يلتزم المصرف بأن لا يفشي أسرار عميله بل عليه المحافظة على هذه الأسرار، ومن ثم يمثل إفشاء هذه الأسرار من قبل ممثلي المصرف أو موظفيه خطأ عقدي. وقد يكون هذا الخطأ عن قصد (كمالو

^١ المادة /١٤٩/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

أُفشيت المعلومات إضراراً بالعميل) أو قد يكون غير مقصود (كما لو أرسل كشف الحساب للعميل عبر البريد الإلكتروني دون اتخاذ الاحتياطات اللازمة لتأمينه^١).

ب-الضرر: لا يكفي مجرد الإخلال بالتزام عقدي لانعقاد مسؤولية المصرف بل لا بد أن يصيب العميل ضرر من جراء الإفشاء، ويلتزم المصرف بتعويض الضرر المتوقع وفقاً للمسؤولية العقدية دون الضرر غير المتوقع وعبء إثبات هذا الضرر على عاتق العميل. وتجدر الإشارة إلى أن الضرر قد يكون مادياً أو معنوياً. حيث يتمثل الضرر المادي بالخسارة المالية التي تلحق بالشخص كما لو كان هناك من سيقرض المال للعميل وامتنع عن إقراضه بعد إن كشف المصرف عن أسرار العميل، أما الضرر المعنوي فهو مقدار ما يصيب العميل في شعوره أو عاطفته أو كرامته أو اعتباره أو مركزه الاجتماعي أو محيطه الذي يعمل فيه.

ج-علاقة السببية بين الخطأ والضرر: أي أن يكون خطأ المصرف في إفشاء أسرار العميل هو السبب المباشر للضرر الذي لحق به.

^١ مناع سعد العجمي، حدود التزام البنك بالسرية المصرفية والآثار القانونية المترتبة عن الكشف عنها، رسالة ماجستير، كلية الحقوق، منشورات جامعة الشرق الأوسط للدراسات العليا، الأردن، ٢٠١٠، ص ٨٤.

ب- المسؤولية التقصيرية: عندما يقوم المصرف بإفشاء أسرار العميل وليس هناك علاقة عقدية بينهما، فالمصرف مسؤول عن هذا الإفشاء مسؤولية تقصيرية وفقاً لأحكام القانون المدني: "كل عمل غير مشروع سبب ضرر للغير يلتزم مرتكبه بالتعويض".^١

وفي هذا الصدد ذهب القضاء الروسي إلى أنه إذا تم الإفصاح عن السرية المصرفية فيما يتعلق بشخص غير مرتبط بالمصرف بموجب أي اتفاق (كالوريث المذكور في أمر مصرفي إلى أحد المصارف) أو تم الإفصاح من قبل شخص غير مرتبط مع المصرف بعلاقة وظيفية فإن المصرف يتحمل المسؤولية التقصيرية وفقاً لقواعد القانون المدني.^٢ ومن الأمثلة على حالات المسؤولية التقصيرية نذكر:

- عندما يكون بين العميل المصرف مفاوضات بشأن عقد ما ويكشف العميل عن بعض المعلومات بسبب هذه المفاوضات، ثم تقتل هذه المفاوضات ففي هذه الحالة لا يوجد عقد وإذا أفشى المصرف أي معلومة يعد مخلّ بالتزامه وتتعقد مسؤوليته التقصيرية.
- كما لو كان هناك عقد وحصل الإفشاء بعد انتهاء العلاقة العقدية.
- لو كان العقد بين المصرف والعميل باطل فهذا لا يوجد عقد وأي إفشاء يقوم به المصرف تتعقد مسؤوليته التقصيرية.

^١ المادة /١٦٤/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

^٢ راجع الرابط: <https://www.bibliofond.ru/view.aspx?id=809399>

تاريخ الزيارة ٢٠١٩/٥/٢٢ الساعة ٢,١٥ p.m.

ويشترط في انعقاد هذه المسؤولية عدة شروط تتمثل في الآتي:

أ-الخطأ: ويتمثل في الانحراف عن السلوك المألوف للشخص المحترف إذا وجد في مثل هذه الظروف التي أحاطت بمحدث الضرر. أي أن يكون خطأ المصرف من خلال انحراف ممثليه أو موظفيه عن سلوك الرجل المهني المحترف الذي ينبغي القيام به عند إدارة شؤون المصرف^١.

ب-الضرر: لا بد من وجود ضرر للعميل، وقد يكون الضرر مادي أو معنوي لكن المصرف في هذه المسؤولية يسأل عن الضرر المتوقع وغير المتوقع.

ج-علاقة السببية بين الخطأ والضرر: أي أن يكون خطأ المصرف هو السبب في حصول الضرر للعميل.

وتجدر الإشارة إلى أن أحكام المسؤولية المدنية السالفة الذكر تطبق في نطاق المعلومات الإلكترونية وهذا ما أكدته قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية من خلال حفظ حق المضرور في المطالبة بالتعويض إلى جانب المؤيد الجزائي في حال تم الإفشاء من قبل أي مقدم خدمات على الشبكة^٢.

^١ مناع سعد العجمي، مرجع سابق، ص ٩٣.

^٢ المادة التاسعة من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

٢- هل هناك وقت محدد للالتزام بالسرية بحيث بانتهاء هذه المدة يمكن إفشاء الأسرار؟

في الحقيقة السرّ بمجرد أن يخرج إلى العلن لم يعد سرّ وبالتالي فقد مضمونه لذلك نجد أن الالتزام بالسرية المصرفية التزام دائم مدى الحياة وحتى لو انقطعت علاقة العميل بالمصرف كما في حالة الوفاة. وتجدر الإشارة إلى أن موظفي المصرف ملزمين بهذا الالتزام حتى بعد تركهم لوظيفتهم واستقالتهم (فإذا قام أحد الموظفين مثلاً وبعد انقطاع علاقته بالمصرف سواء بإرادته أم رغم عن إرادته بإفشاء أحد الأسرار العائدة لأحد عملاء المصرف فهذا يحق للعميل مقاضاة الموظف جزائياً ومطالبته بالتعويض).

٣- هل التزام المصرف بالسرية التزم بنتيجة أم ببذل عناية؟

نرى من جانبنا أنه ينبغي التمييز بين حالتين:

الحالة الأولى: إذا كان الإفشاء صادراً من قبل أحد ممثلي المصرف أو موظفيه أو من أطلع بحكم صفته أو بما تسمح القوانين والأنظمة النافذة على المعلومات السرية فهذا التزام المصرف بتحقيق نتيجة أي بمجرد حصول الإفشاء تترتب المسؤولية على المفشي والمصرف كشخص اعتباري وذلك حسب المادة (٢/ب) من قانون السرية المصرفية. وهذا الأمر منطقي كون هناك التزام على هؤلاء الأشخاص بعدم إفشاء الأسرار إضافة لخطورة وأهمية العمليات المصرفية فلو تساهل المشرع السوري بذلك لفقد الثقة بالمصارف ولتم العزوف عن التعامل مع المصارف. وتجدر الإشارة إلى أنه في حال تم الإفشاء من قبل موظفي المصرف أو من قبل أي شخص

يعمل تحت إشرافه وتوجيهه فتكون مسؤولية المصرف على أساس مسؤولية المتبوع عن أعمال التابع بشرط أن يكون قد تم الإفشاء أثناء مباشرته الوظيفية أو بسببها^١. ولكن فيما لو تم الإفشاء من قبل الموظف خارج نطاق الوظيفة أو بعد انقطاع صلته الوظيفية فلا مجال لتطبيق أحكام مسؤولية المتبوع عن أعمال التابع. وبالتالي تبقى المسؤولية المدنية على عاتق الموظف فقط ويصبح التزام المصرف التزام ببذل عناية.

الحالة الثانية: في حال تم الإفشاء من شخص غير موظف بالمصرف (كما لم تم الإفشاء من قبل أحد مخترقي شبكة الإنترنت أو ما يعرفون بالهاكرز أو فيما لو حصلت عملية سطو على المصرف وقام السارق بالاطلاع على معلومات سرية وأفشاها، أو في حال تم الإفشاء من الموظف بعد تركه الوظيفة) فهذا يصبح التزام المصرف ببذل عناية، أي هل اتخذ المصرف الاحتياطات اللازمة للحيلولة دون كشف هذه البيانات أم لا أو بمعنى آخر هل هناك حراسة على المصرف أم لا عندما وقعت عملية السطو وهل هناك عدة أنظمة على برنامج الحاسب أم لا. ومبرر ذلك كون هذه الظروف خارجة عن إرادة المصرف ولا يعقل أن يكون التزامه بنتيجة في مثل هذه الحالات عملاً بنظرية الظروف الطارئة. أي أنه إذا اتخذ المصرف كافة الاحتياطات اللازمة لمنع إفشاء السر فهذا لا يتحمل أي مسؤولية أم إذا كان قد قصر في اتخاذ الاحتياطات يكون مسؤولاً عن الإفشاء.

^١ المادة /١٧٥/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

وفي ختام الحديث عن وسائل معالجة المشكلات التي تصيب المستخدم باعتباره عميلاً للمصرف، يمكن القول أن المشرع الأمريكي كرّس الحماية القانونية للمعلومات الخاصة بالأفراد بشكل قانوني سليم مما يشكل حافزاً لدى الأفراد على التعامل بالوسائل الإلكترونية دون أي خوف من الاستخدام غير المشروع لهذه المعلومات، ويعتبر قانون الخصوصية لعام ١٩٨٤/ من أفضل القوانين من حيث كونه جاء مخاطباً لكافة المتعاملين بالوسائل الإلكترونية (مشاركون، مستخدمون، مقدمو معلومات) وفرض على عاتق كل طرف عدة التزامات و مبادئ تكرر بمجملها الحماية القانونية للمعلومات الشخصية.

أما بالنسبة للمشرع السوري فإنه كان موفقاً عندما لم يكتفِ بقانون السرية المصرفية بهدف توفير الحماية القانونية للمعلومات الإلكترونية، إنما كرّس الحماية القانونية لهذه المعلومات بموجب القوانين النازمة للمعاملات الإلكترونية (قانون المعاملات الإلكترونية وقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية). الأمر الذي من شأنه قطع دابر الشك في مسألة توفر الحماية القانونية للمعلومات الإلكترونية و لكن حبذا لو تبنى المشرع السوري المبادئ التي جاء بها قانون الخصوصية الأمريكي بموجب نصوص قانونية صريحة، الأمر الذي من شأنه أن يبين الالتزامات القانونية على عاتق كل متعامل بالمعلومات الإلكترونية و ذلك بهدف تلافي أي نزاع في هذا الخصوص.

المطلب الثاني

وسائل معالجة المشكلات التي تواجه المستخدم

باعتباره مستهلكاً إلكترونياً

تقوم هذه الوسائل في مجملها على فكرة واحدة وهي البحث والتدقيق في النصوص القانونية التقليدية والإلكترونية المتوفرة لمعرفة مدى إمكانية تطويعها وتطبيقها كأساليب معالجة لهذه المشكلات، ولكن نقطة الخلاف الوحيدة بين هذه الأساليب تتمثل في الغرض من هذا التطويع:

فبالنسبة لمشكلات الشراء عبر الحدود لعل الغرض من تطويع هذه النصوص هو سد ثغرة قانونية تتعلق بالقانون الواجب التطبيق والمحكمة المختصة.

أما بالنسبة للمشكلات المتعلقة بالمستهلك فالغرض من تطبيق النصوص القانونية هو توفير الحماية القانونية للمستهلك الإلكتروني بموجب النصوص المتوفرة سواء أكانت هذه النصوص تتعلق بالمعاملات التقليدية أم كانت تتعلق بالمعاملات الإلكترونية.

لذلك سوف نتعرف على معالجة مشكلات الشراء عبر الحدود في الفرع الأول على أن نتحدث عن حماية المستهلك الإلكتروني في الفرع الثاني.

الفرع الأول

معالجة مشكلات الشراء عبر الحدود

تتم معالجة مشكلات الشراء عبر الحدود من خلال نوعين من التدابير:

التدابير الوقائية: وهي عبارة عن إجراءات والتزامات قانونية مفروضة على عاتق الدول من أجل تلافي حدوث هذه المشكلات وهي مجال بحثنا (أولاً).

التدابير العلاجية: وهي عبارة عن حلول قانونية تم تطويعها في ضوء أحكام التشريع السوري تسهم في علاج هذه المشكلات. وهي مدار بحثنا (ثانياً).

أولاً: التدابير الوقائية

يمكن تقسيم التدابير الوقائية إلى زمرتين:

١- الالتزامات المفروضة على عاتق المشرفين على الجهات المصدرة (المصرف) في كل دولة وتتمثل في الآتي:

أ- يتطلب من الجهات النازمة لعمل الجهات المصدرة تكريس المزيد من الاهتمام بالنسبة لعمليات تقييم وضبط ومراقبة المسائل المتعلقة بتشغيل النظام والسمعة واختلاف القانون الواجب التطبيق وغيرها من المسائل التي تنتج عن التعامل بوسائل الدفع الإلكتروني، وذلك على اعتبار أن المشكلات الناشئة عن مسائل الشراء عبر الحدود لا تقل أهمية عن تلك التي تواجهها المصارف داخل الحدود الوطنية.

ب- ينبغي على الجهات المصدرة وهي بصدد تنظيم التعامل بالدفع الإلكتروني أن يراعوا تقديم خدماتهم وفقاً لمتطلبات العمل داخل أسواق مختلفة، وليس داخل السوق المحلية فحسب. وكذلك استتباط الوسائل الكفيلة بفهم حاجات المستهلكين تبعاً لاختلاف الدول التي ينتمون إليها وبحسب السلع والخدمات التي يحتاجونها^١.

ج- ينبغي على الجهات الرقابية أن تضمن حسن سير نظام الدفع الإلكتروني وعمليات الائتمان المرتبطة به ليس في حدود دولة واحدة فقط، وإنما ينبغي عليها أن تضع في حسابها المشكلات التي يمكن أن تنشأ عبر الحدود. وذلك من خلال تقييمها للمخاطر المحتملة أو التي هي موجودة فعلاً في الدول التي يمكن أن تتعامل معها، ووضع خطط طارئة في حال وجود أية صعوبات محتملة متعلقة بعرقلة الخدمات التي تقدمها في دولة من هذه الدول. وخصوصاً في حال اعتماد الجهات المصدرة على مزودي خدمات خارج بلد المصدر.

د- يجب على الجهات الرقابية الوطنية أن تلعب دوراً مهماً لمناقشة الغموض الذي يكتنف مسألة الاختصاص القضائي وتذليل العقبات التي تعترضها. وذلك على اعتبار أن هذه الجهات هي الأقدر على الابتكار ومعرفة خصوصيات النظام الداخلي للدولة التي ينشطون فيها من خلال الكشف عن الممارسات غير الآمنة وغير المشروعة، كما يمكنها تبادل المعلومات حول الابتكارات الحاصلة فيما يتعلق بالسلع والخدمات التي يتم تبادلها عبر الحدود^٢.

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٤٨٦.

^٢ د. طارق حمزة، مرجع سابق، ص ٤٥٩.

٢-التوصيات لجميع الدول و تتمثل في الآتي:

أ- ضرورة التعاون بين الدول من أجل تحديد بعض المفاهيم الخاصة بالقانون الدولي الخاص في المجال الافتراضي (كمفهوم التركيز الافتراضي للرابطة العقدية^١)، وذلك بهدف تقادي الصعوبات التي يثيرها أعمال ضوابط الاختصاص القانوني التقليدي.

ب- يفترض إزاء صعوبة التحقق من هوية أطراف العقد الإلكتروني إلزامية إدراج شرط في الوفاء الإلكتروني يلزم الطرفين الإدلاء بجميع البيانات الشخصية التي تفصح عن هويتهم، وفي حال عدم التزام أحد الأطراف بهذا الشرط يكون للطرف الآخر الحق في المطالبة بتطبيق قانونه الوطني أو أي قانون آخر يمكنه من الحصول على هدفه^٢.

ج- تطوير آليات أو منابر للتسوية، وابتداع قواعد لتحديد الاختصاص القضائي تلاءم خصوصية التعامل بالدفع الإلكتروني، وتأخذ في اعتبارها ما جرى عليه العمل بين أطرافه شريطة خضوع مثل هذه الأنظمة لإشراف جهات موثوق بها.

د- ضرورة وجود اتفاقيات دولية أو تنقيحها حتى تقبل التطبيق على وسائل الدفع الإلكتروني وكفالة توحيد تطبيق تلك الاتفاقيات. كما

^١ يقصد به تحديد النطاق العلوي الذي يبرم فيه العقد الإلكتروني بغية معرفة القانون الواجب التطبيق عليه وخصوصاً في ظل عالمية شبكة الإنترنت.

^٢ د. خالد ممنوح إبراهيم، التقاضي الإلكتروني، الدعوى الإلكترونية وإجراءاتها أمام المحاكم،

بحث منشور، ص ١٩ ومتاح على الرابط: www.Kenan online.com

تاريخ الزيارة ٢٠١٨/٨/١٧ الساعة ٦،٤٠ p.m

ينبغي أن يكون هناك اتفاق موحد يلبي حاجات المتعاملين بالدفع الإلكتروني ويسهم في مواجهة القرصنة الإلكترونية وعمليات الاحتيال التي تتم عبر الشبكة. وفي سبيل إضفاء الصفة الرسمية على هذا الاتفاق ينبغي أن يتم في إطار الجمعية العامة للأمم المتحدة وذلك تفادياً لحدوث تباين بين النصوص الدولية والوطنية من جهة وضماناً لوحدة تفسير المفاهيم المتعلقة بذلك من جهة أخرى^١.

ومن الناحية العملية فقد قدم المجلس الأمريكي للدفع عبر الحدود

(Cross Border Council) التابع لجمعية الدفع بالوسائل الإلكترونية

The Electronic Payment Association (NACHA) دليل

المستهلك للمدفوعات عبر الحدود.

(The Cross Border Payment User Guide) الذي يحتوي على الأسس التي يجب العمل بمقتضاها في سبيل تأمين أكبر قدر ممكن من الحماية للصفقات عبر الحدود. ويحتوي هذا الدليل على مجموعة من القواعد التي من شأنها مساعدة المستهلك عند تعامله مع أشخاص آخرين خارج الحدود، ومن هذه القواعد:

^١ د. عصام الدين القصبي، تنازع الاختصاص القضائي والقانوني الدوليين في مجال التجارة الإلكترونية، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد ٤، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ١٦١٨.

²The Electronic Payment Association, The Cross Border Payment User Guide. Available at:

www.nacha.org/search?opiviewsFu/text=the+cross+Border+payment+user+Guide.

أ- التزام الأطراف المنشئة للصفقات العابرة للحدود بأن يكونوا على علم ومعرفة كافية بالقواعد المطبقة في البلد الذي يوجد فيه المتعاقد الآخر، وبالتالي تكون حقوق وامتيازات الطرف المتلقي مضمونة وخاصة ما يتعلق بالترخيص والصفقات الخاطئة.

ب- يتكفل المشغل العامل عبر الحدود تأمين أكبر قدر ممكن من التنسيق بين نظام الدفع الموجود في الدولة التي انطلقت منها الصفقة وبين الطرف الآخر في دولة أخرى^١.

ج- يشدد الدليل على التزام الجهات التي تريد عقد صفقات عبر الحدود، ببعض الأطر التنفيذية التي تتماشى مع عملية الدفع عبر الحدود تلافياً لأي منازعات يمكن أن تحصل وأهم هذه الأطر:

- أن تمتلك القدرة الفنية لإجراء عمليات الدفع عبر الحدود، وينبغي أن تكون كل صفقة مستقلة عن الأخرى وأن تكون لها رمز خاص بها يميزها عن باقي الصفقات.
- العمل على امتلاك جهاز موظفين مدربين على إجراء صفقات عبر الحدود والتكيف مع الأوضاع المتغيرة والحالات الطارئة.
- التقيد والتعامل وفق المبادئ التي يقرها (مركز المقاصة للتعاملات عبر الحدود^٢) والاستثناءات التي يمكن اعتمادها بالنسبة لبلد معين لتسهيل التنسيق بين القوانين.

^١ د. طارق حمزة، مرجع سابق، ص ٤٥٨

^٢ يقصد به: عندما تكون التحويلات المالية بين دولتين مختلفتين، ينشأ تحويل مصرفي عبر الحدود حيث يتولى مركز المقاصة مهمة المقاصة المتعددة الأطراف لتسوية الصفقات بين الدولتين.

- الاطلاع على الأنظمة الوطنية الداخلية للبلدان التي سيتم التعامل معها.
- إنشاء علاقة مع أحد المشغلين عبر الحدود بهدف إتمام الصفقات^١.

د- يجب على كل مشغل بنظام الدفع عبر الحدود في الولايات المتحدة الأمريكية أن يتقيد بالآلية القانونية والإطار التنفيذي الذي يحدده هذا الدليل. أما بالنسبة للمشغلين خارج الولايات المتحدة الأمريكية، إذا أرادوا العمل بوسائل الدفع الإلكتروني داخل الولايات المتحدة، فيجب عليهم أن يتقيدوا بأحكام هذا الدليل تقادياً لأي اختلاف في تطبيق القوانين. وفي حال الرفض فإنهم سيتعرضون للمراقبة من قبل مكتب مراقبة الممتلكات الأجنبية **Office Of Foreign Assets**^٢ الذي يصدر قائمة بأسماء الجهات التي ينبغي على الأمريكيين تجنب التعامل معها تلافياً للتعرض لمثل هذه الأخطار^٣.

^١ المرجع السابق، ص ٤٦٠

^٢ يرمز له (OFAC) هو وكالة استخبارات مالية تابعة لوزارة الخزانة الأمريكية وهي تدير وتنفذ العقوبات الاقتصادية والتجارية لدعم أهداف الأمن القومي والسياسة الخارجية للولايات المتحدة وبموجب سلطات الطوارئ الوطنية الرئاسية يقوم المكتب بأنشطته ضد الدول الأجنبية وضد مجموعة من المنظمات والأفراد والكيانات الاقتصادية. تأسس عام ١٩٥٠ ولديه سلطة فرض عقوبات ضد الكيانات الاقتصادية التي تتحدى توجيهاته بما في ذلك فرض الغرامات وتجميد الأصول ومنع الكيانات الاقتصادية والأطراف من ممارسة العمل في الولايات المتحدة .

^٣ راجع الرابط: [www. Treasury.gov/about/organizational-structure/pages/office](http://www.Treasury.gov/about/organizational-structure/pages/office)

[of foreign assets-control-as px](http://www.Treasury.gov/about/organizational-structure/pages/office)

تاريخ الزيارة ٢٠١٨/٨/١٩ الساعة ١٥،٣٣م

ومن ناحية أخرى فقد ألزم الاتحاد الأوروبي المصارف وغيرها من مقدمي خدمات الدفع الإلكتروني بوجوب مواءمة الرسوم الخاصة بالمدفوعات المنجزة عبر الحدود مع مستويات الرسوم الوطنية المعتمدة في الدول الأعضاء في الاتحاد الأوروبي^١.

ثانياً: التدابير العلاجية.

تتمثل التدابير العلاجية في البحث عن الحل القانوني لمشكلة القانون الواجب التطبيق على عملية الدفع الإلكتروني، ومعرفة الجهة صاحبة الاختصاص القضائي بالنسبة لأي نزاع يصيب عملية الدفع الإلكتروني في ضوء أحكام التشريع السوري. وذلك من خلال البحث في مدى إمكانية تطبيق النصوص التقليدية على عملية الدفع الإلكتروني وتقديم المقترحات اللازمة في حال تعذر الوصول لحل قانوني. لذلك سوف نبحث بداية عن معالجة مشكلة القانون الواجب التطبيق ثم ننقل للحديث عن المحكمة المختصة بمنازعات الدفع الإلكتروني.

١- معالجة مشكلة القانون الواجب التطبيق على معاملات الدفع الإلكتروني.

ينبغي أن نشير بدايةً إلى أن عملية الدفع الإلكتروني هي عملية مصرفية إلكترونية تقوم في جوهرها على ثلاثة عقود: عقد بين المصدر والعميل (عقد الإصدار) وعقد بين المصدر والتاجر (عقد

^١ مشار إليه لدى: د. حوالف عبد الصمد، مرجع سابق، ص ٤٨٨.

(التوريد) وعقد بين العميل والتاجر (عقد البيع) وتتم ممارسة هذه العملية من قبل المصرف التقليدي أو المصرف الإلكتروني:

أ- من قبل المصرف التقليدي: يقدم المصرف التقليدي خدمة الدفع الإلكتروني من خلال أحد عقدين إما عقد تقليدي أو عقد إلكتروني وهذا الأخير يُعرّف بأنه: «اتفاق يجري انعقاده أو تنفيذه كلياً أو جزئياً بوسائل إلكترونية»^(١).

وبالنسبة للقانون الواجب التطبيق على العقد الإلكتروني، فقد نص قانون المعاملات الإلكترونية على أنه: «ما لم يوجد اتفاق بين أطراف العقد الإلكتروني على القانون الواجب التطبيق يطبق على القانون الواجب التطبيق قواعد القانون الدولي المنصوص عليها في القانون المدني»^(٢).

نجد من النصوص السابقة أن العقد الإلكتروني هو المكافئ الإلكتروني للعقد التقليدي ويخضع لأحكامه، وبالعودة إلى نصوص القانون المدني فقد نص على أنه: «يسري على الالتزامات التعاقدية قانون الدولة التي يوجد فيها الموطن المشترك للمتعاقدين، إذا اتحدا موطناً. فإن اختلفا موطناً، سري قانون الدولة التي تم فيها التعاقد. هذا إذا لم يتفق المتعاقدان، أو تبين من الظروف أن قانوناً آخر هو الذي يراد تطبيقه»^(٣).

^١ المادة الأولى من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

^٢ المادة ١١/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٠.

^٣ المادة ٢٠/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

وحيث أن عملية الدفع الإلكتروني هي عبارة عن التزامات عقدية، وبالتالي فإن القانون الواجب التطبيق على عملية الدفع الإلكتروني المقدمة من قبل مصرف تقليدي سواء بعقد تقليدي أم بعقد إلكتروني هو: قانون الإرادة التي يتفق الأطراف عليه سواء بشكل صريح أو ضمني، وفي حال عدم الاتفاق على القانون يطبق قانون الدولة التي تم فيها العقد. وليس هناك مجال للقول بتطبيق قانون الموطن المشترك إن اتحدا موطناً وذلك على اعتبار أننا نبحث عن حل لمشكلة القانون الواجب التطبيق بسبب اختلاف موطن الأطراف وتعدد القوانين الواجبة التطبيق.

وبالنسبة لتحديد مكان العقد فقد نص قانون المعاملات الإلكترونية على أنه: «يعد العقد الإلكتروني قد تم في الزمان والمكان الذي استلم فيه القبول ما لم يتفق على غير ذلك»^(١).

ب- من قبل المصرف الإلكتروني: يقدم المصرف الإلكتروني خدمة الدفع الإلكتروني من خلال عقد إلكتروني، وحتى نتمكن من معرفة القانون الواجب التطبيق على عملية الدفع الإلكتروني المقدمة من قبل المصرف الإلكتروني لابد لنا بدايةً من معرفة القانون الناظم للمصرف الإلكتروني، ومن ثم يمكننا معرفة القانون الواجب التطبيق على عملية الدفع الإلكتروني.

ونحن من جانبنا نعرف المصرف الإلكتروني بأنه كيان افتراضي يكتسب صفة التاجر ويمارس أعمال مصرفية تقليدية (سحب -

^١ المادة ١٠/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

إيداع... الخ) وأعمال مصرفية إلكترونية (إصدار نقود إلكترونية - توزيع نشرات إلكترونية... الخ) وذلك اعتماداً على الدعائم الإلكترونية.

ولعل التساؤل الذي يطل بظلاله حول ما هو القانون الواجب التطبيق على المصرف الإلكتروني؟

سوف نقوم بالإجابة على هذا التساؤل في ضوء أحكام القانون السوري.

نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه: «تطبق أحكام الفصل الثاني من هذا القانون - (المتعلق بتنظيم التواصل على الشبكة) - على أي مقدم خدمات على الشبكة له في الجمهورية العربية السورية مركز إدارة فعلي أو مركز ثابت يمارس فيه نشاطاً اقتصادياً راهناً بصرف النظر عن جنسيته وعن مكان تأسيسه ومقره الرئيس إذا كان شخص اعتباري وعن المكان الذي توجد فيه التجهيزات التقنية التي يستخدمها»^(١).

كما نص على أنه: «يعد النطاق العلوي السوري في حكم الأرض السورية في معرض تطبيق أحكام هذا القانون»^(٢).

كما نص قانون الشركات على أنه: «تسري أحكام هذا المرسوم التشريعي على جميع الشركات المؤسسة في الجمهورية العربية

^١ المادة /٢٧/ قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

^٢ المادة /٣٣/ قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

السورية وبما لا يتعارض مع أحكام الشركات المؤسسة بقانون خاص^(١).

بينما نص القانون المدني على أنه: «أما النظام القانوني للأشخاص الاعتبارية من شركات وجمعيات ومؤسسات وغيرها فيسري عليها قانون الدولة التي اتخذت فيها مركز إدارتها الرئيس الفعلي ومع ذلك إذا باشرت نشاطها الرئيس في سورية فإن القانون السوري هو الذي يسري^(٢)».

يمكننا أن نستنتج من النصوص السابقة أن القانون السوري يطبق على المصرف الإلكتروني في الحالات الآتية:

- إذا تم تأسيسه في سورية: جاء نص المادة الثانية من قانون الشركات مطلقاً يشمل جميع الشركات سواء التقليدية أم الإلكترونية المؤسسة في سورية، وعلى ذلك إن كانت الشركة الإلكترونية (المصرف الإلكتروني) تقع ضمن النطاق العلوي السوري وقد حصلت على التراخيص اللازمة^٣، فإن القانون السوري هو الذي يحكمها وبصرف النظر عن أي اعتبار آخر (المادة ٣٣/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية). مما

^١ المادة الثانية من قانون الشركات رقم ٢٩/ لعام ٢٠١١.

^٢ المادة ١٢/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٣ راجع المادة ٤/ من القانون رقم ٢٨/ لعام ٢٠٠١ الخاص بتأسيس المصارف الخاصة والمواد ١/٢-٣-٤-٥-٦-٧-٨/ من التعليمات التنفيذية للقانون رقم ٢٨/ لعام ٢٠٠١ الصادرة بالقرار رقم ٢٠٦٠/ تاريخ ٢٦/٩/٢٠٠١.

يستدعي تسجيلها في سجل الشركات في سورية واكتسابها الجنسية السورية^١.

- إذا كان له مركز إدارة رئيس أو ثابت في سورية: نلاحظ من نص المادة /٢٧/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية أن هذا القانون يطبق على أي مقدم خدمة على الشبكة (والمصرف هو عبارة عن مقدم خدمات على الشبكة) إذا كان له مركز إدارة رئيس أو ثابت وبغض النظر عن مكان تأسيسه ومقره.
- إذا كان نشاطه الرئيس في سورية: جاءت المادة /١٢/ من القانون المدني باستثناء مهم على القاعدة العامة. فالقاعدة العامة تتجسد في تطبيق قانون مركز الإدارة الرئيس، والاستثناء الذي جاءت به هذه المادة هو تطبيق القانون السوري على الحالة التي يمارس فيها الشخص الاعتباري نشاطه الرئيس في سورية. وقد جاء النص عاماً بشكل يجعل إمكانية تطبيقه على الأشخاص الاعتبارية كافة وبغض النظر عن المكان الذي تمارس فيها نشاطها سواء أكان تقليدي أم إلكتروني. وتبدو أهمية هذا الحكم استناداً إلى الاعتبارات الوطنية التي تستوجب تطبيق القوانين المحلية على الشركات الأجنبية التي تمارس نشاطها الرئيس في بلادنا. وسد محاولاتها للتهرب من أحكام القانون الوطني عن طريق تأسيسها في الخارج.

^١ المادة /١٠/ من قانون الشركات رقم /٢٩/ لعام ٢٠١١.

وعليه يمكننا أن نجد من الحالات السابقة أن القانون السوري يطبق إذا كان موقع المصرف الإلكتروني يقع ضمن النطاق العلوي السوري سواء أكان هذا الموقع هو مكان تأسيس وكان قد حصل على التراخيص اللازمة ، أم مركز إدارة إضافة للحالة التي يمارس فيها المصرف نشاطه ضمن النطاق العلوي السوري.

ولكن التساؤل المطروح فيما لو كان موقع المصرف أو أن نشاط المصرف يقع ضمن نطاق الفضاء الخارجي دون أن يتبع لدولة معينة فما هو القانون الواجب التطبيق في مثل هذه الحالة؟

في الحقيقة إذا ما أردنا تطبيق نص المادة /١٢/ من القانون المدني فهذا يعني أن نطبق قانون مركز الإدارة الرئيس، ولكن هذا الأمر لا يكاد يخلو من صعوبات جمّة خصوصاً في ظل عدم معرفة الدولة التي يقع فيها مركز الإدارة الرئيس. وبالتالي نقترح في مثل هذه الحالة أن يُطبق قانون إرادة الأطراف أو أن يُطبق قانون الدولة التي تم فيها الشهر.

وبناء على ما تقدم نجد أن المصرف الإلكتروني هو بمثابة المكافئ الإلكتروني للمصرف التقليدي ويخضع لأحكامه، الأمر الذي يعني أن المصرف الذي يقدم خدمة الدفع الإلكتروني ضمن النطاق العلوي السوري يتوجب خضوعه لأحكام القانون السوري، وبالتالي نطبق على عملية الدفع الإلكتروني في هذه الحالة أحكام المادة /٢٠/ من القانون المدني (قانون الإرادة في حال الاتفاق عليه، أو قانون الدولة التي تم فيها العقد في حال عدم الاتفاق) وذلك على النحو الذي فصلناه بالنسبة للمصرف التقليدي.

أما بالنسبة للمصرف الإلكتروني الذي يقدم خدماته في الفضاء الخارجي فلا مجال لإعمال أحكام المادة /٢٠/ من القانون المدني كونه يقدم خدماته خارج النطاق العلوي السوري وبالتالي لا يخضع لأحكام القانون السوري، وفي هذا الصدد نقترح أن يُطبق على عملية الدفع الإلكتروني في هذه الحالة إما قانون الإرادة في حال الاتفاق عليه صراحةً أو ضمناً أو قانون دولة المستفيد من عملية الدفع الإلكتروني في حال عدم الاتفاق على قانون معين باعتباره طرفاً ضعيفاً اقتصادياً مقارنةً بباقي الأطراف.

ويقصد بقانون المستفيد قانون الدولة التي يحمل جنسيتها أو قانون الدولة التي يقيم فيها بشكل معتاد، وذلك على اعتبار أن الشخص المستفيد والمراد تطبيق قانونه هو الطرف الضعيف والأقل معرفة بين الأطراف وبالتالي تطبيق قانون دولته أو محل إقامته من شأنه أن يوفر الحماية القانونية له ويسهم لحد ما في تحقيق نوع من التوازن القانوني بين الأطراف. وفي سبيل توضيح هذه الفكرة سوف نبين مثالين في هذا الخصوص :

أ- القانون الواجب التطبيق على عملية التحويل الإلكتروني للأموال:

تُطرح مسألة القانون الواجب التطبيق على التحويل الإلكتروني للأموال عندما يتم التحويل بين حسابين مصرفيين موجودين في دول مختلفة حيث تخضع كل مرحلة لقانون مختلف؟

اتجه بعض الفقه^١ إلى وجوب تطبيق قانون المستفيد من التحويل مع إبقاء قانون الأمر بالتحويل كقانون بديل عن قانون المستفيد. كما

^١ مشار إليه لدى: د. نادر عبد العزيز شافي، مرجع سابق، ص ١٨٩.

طبقت المحكمة الألمانية العليا "القانون الألماني" على التحويل الإلكتروني للأموال بين مصرفين باعتباره قانون دولة تنفيذ التحويل وقانون الدولة التي تتحقق فيها آثار التحويل^١.

ونحن من جانبنا نؤيد تطبيق قانون المستفيد على عملية التحويل الإلكتروني للأموال وذلك للمبررات الآتية:

- نص القانون المدني على أنه: (تسري على الالتزامات التعاقدية قانون الدولة التي يوجد فيها الموطن المشترك للمتعاقدين إذا اتحدا موطناً فإن اختلفا موطناً سرى قانون الدولة التي يتم فيها التعاقد هذا إذا لم يتفق المتعاقدان أو يتبين من الظروف أن قانون آخر هو الذي يراد تطبيقه^(٢)).

إذاً القانون الواجب التطبيق على العقود بشكل عام هو القانون الذي يتفق عليه صراحةً أو ضمناً، فإن لم يتفق الأطراف يطبق قانون الموطن المشترك إذ اتحدا موطناً، فإن اختلفا موطناً طُبِقَ قانون الدولة التي يتم فيها العقد. وبما أن التحويل الإلكتروني للأموال هو عبارة عن عملية محاسبية تتضمن التزامات عقدية، فإنه في ظل غياب الوجود المادي والمكاني للأطراف يُطبق قانون إرادة الأطراف أو قانون الدولة التي يتم فيها العقد (قانون المستفيد) باعتبار أن العقد لا يتم بشكل نهائي إلا بالقيد في حساب المستفيد.

^١ مشار إليه لدى: المرجع السابق، ص ١٨٩

^٢ المادة/٢٠/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

- إن عملية التحويل الإلكتروني للأموال تتم وبشكل نهائي من وقت قيدها في حساب المستفيد، وبالتالي لا بد من تطبيق هذا القانون استناداً لفكرة مكان تنفيذ هذه العملية.
- نصت المادة السادسة من القرار الأساسي الصادر عن حاكم مصرف لبنان رقم /٧٥٤٨/ تاريخ ٢٠٠٠/٣/٣٠ الخاص بالعمليات المصرفية المنفذة بوسائل إلكترونية: ((تطبق على العمليات المالية والمصرفية بالوسائل الإلكترونية وعلى المؤسسات التي تمارسها القوانين والأنظمة والتعليمات التي ترعى هذه المؤسسات أو التي ترعى العمليات المنفذة بالوسائل التقليدية غير الإلكترونية)).^(١)

وبالتالي تؤكد المادة السالفة الذكر أن مثل هذه العمليات (عملية التحويل الإلكتروني للأموال) يطبق عليها القوانين التي ترعى العمليات المنفذة بشكل تقليدي. أي أن التحويل الإلكتروني للأموال هو المكافئ للتحويل التقليدي ويخضع لأحكامه . وبالتالي لا بد من تطبيق المادة /٢٠/ من القانون المدني على النحو الذي شرحناه (قانون الدولة التي تم فيها العقد باعتباره هو ذاته قانون المستفيد كون التحويل الإلكتروني للأموال يتم بشكل نهائي أيضاً بالقيود في حساب المستفيد).

^١ مشار إليه لدى د. نادر عبد العزيز شافي، مرجع سابق، ص ١٩٠-١٩١.

ب-القانون الواجب التطبيق على المستهلك في نطاق التعاملات الإلكترونية:

لقد ظهر اتجاهان بالنسبة للقانون الواجب التطبيق على المستهلك الإلكتروني:

الاتجاه الأول: تنزعه الولايات المتحدة الأمريكية، ويرى أنصار هذا الاتجاه أن الأولوية ينبغي أن تكون لقانون دولة التاجر، وذلك تيسيراً لنشاطه ولاسيما أن تفضيل قانون دولة المستهلك يعني إيجاد عقبات كثيرة مصدرها القوانين الداخلية في كل دولة مما يحول دون فاعلية ونشاط التعاملات الإلكترونية^١.

الاتجاه الثاني: يعكس وجهة نظر الاتحاد الأوروبي، ويرى أن الأفضلية لقانون دولة المستهلك سواء فيما يتم من عقود التجارة الإلكترونية بين مستهلكين وتجار في الدول الأعضاء في الاتحاد الأوروبي أم بين دولة من هذه الدول ودول أخرى خارج الاتحاد الأوروبي. حيث يعتبر هذا الاتجاه أنه من غير المنطقي أن نطالب المستهلك كشخص طبيعي بضرورة الإلمام القانوني الكامل بمجموعة من التشريعات المتباينة في دول العالم^٢.

ونحن من جانبنا نرى أن الاتجاه الثاني هو الاتجاه الصحيح الذي يعطي الأولوية في القانون الواجب التطبيق لقانون المستهلك، فالمستهلك طرف ضعيف أمام المصارف والتجار وبالتالي حماية المستهلك هي الأساس في أي عملية تعاقدية. وتجدر الإشارة إلى أن

^١ مشار إليه لدى: عبد الله محمود، مرجع سابق، ص ١٢٩.

^٢ مشار إليه لدى: المرجع السابق، ص ١٣٠.

قانون المستهلك قد يكون قانون جنسية المستهلك أو قانون الدولة التي يقيم فيها بشكل معتاد. وتجدر الإشارة في هذا السياق إلى أن تطبيق قانون المستهلك لا يعني الخروج عن القاعدة العامة التي تقضي بتطبيق قانون الدولة التي تم فيها العقد، فقد يتصادف استلام المستهلك القبول في دولته وبالتالي تشابه قانون دولة المستهلك مع قانون الدولة التي تم فيها العقد ولكن فيما لو استلم القبول في دولة أخرى فهنا يعد قانون المستهلك استثناء من القاعدة العامة ويطبق كونه اقدر على حمايته.

ومما سبق نصل إلى نتيجة مفادها إن أحكام المادة (٢٠) من القانون المدني (قانون الإرادة أو قانون الدولة التي تم فيها العقد) هي النازمة لمسألة القانون الواجب التطبيق على عملية الدفع الإلكتروني المقدمة:

- من قبل المصرف التقليدي وذلك على اعتبار أن العقد الإلكتروني هو المكافئ للعقد التقليدي وسنداً للمادة/١١/ من قانون المعاملات الإلكترونية والمادة/٢٠/ من القانون المدني.
- من قبل المصرف الإلكتروني الذي له موقع (مركز تأسيس وحصل على التراخيص اللازمة) أو (مركز إدارة) أو (يمارس نشاطه ضمن النطاق العلوي السوري) وذلك على اعتبار أن المصرف الإلكتروني في هذه الحالات هو المكافئ للمصرف التقليدي ويخضع لأحكام القانون السوري وسنداً للمادة/١١/ من قانون المعاملات الإلكترونية والمادة/٢٠/ من القانون المدني.
- أما بالنسبة للمصرف الإلكتروني الذي يقدم خدماته في الفضاء الخارجي فإننا نقترح أن يُطبق قانون إرادة الأطراف أو قانون

دولة المستفيد باعتباره طرف ضعيف اقتصادياً مقارنةً بباقي الأطراف من عملية الدفع الإلكتروني (قانون الدولة التي يحمل جنسيتها أو قانون الدولة التي يقيم فيها بشكل معتاد) في حال عدم الاتفاق على قانون معين، كونهم من أقدر القوانين على تحقيق العدالة القانونية.

٢- المحكمة المختصة بمنازعات عملية الدفع الإلكتروني:

بعد أن تعرفنا على القانون الواجب التطبيق على عملية الدفع الإلكتروني، يثور التساؤل أيضاً حول المحكمة المختصة بنظر المنازعات الناشئة عن عملية الدفع الإلكتروني ؟

ففي ظل غياب التنظيم التشريعي لهذا الموضوع سوف نعول على الأحكام العامة في سبيل الإجابة عن هذا التساؤل.

حيث نص قانون المعاملات الإلكترونية على أنه: «تتطبق على العقود الإلكترونية القواعد المتعلقة بالاختصاص الدولي المنصوص عليها في قانون أصول المحاكمات المدنية وتعديلاتها إذا كانا طرفا العقد في بلدين مختلفين أما إذا كانا في سورية فتتطبق القواعد العامة في الاختصاص»^(١).

وحيث أن عملية الدفع الإلكتروني تقوم في مجملها على ثلاثة عقود، وبالتالي يمكن تطبيق أحكام هذه المادة عليها. وبالتالي نجد

^١ المادة ١٢/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

من نص المادة السالفة الذكر أن المشرع السوري يميز بين حالتين:

أ- حالة كون أطراف العقد في بلدين مختلفين: تطبق في هذه الحالة القواعد المتعلقة بالاختصاص الدولي المنصوص عليها في قانون أصول المحاكمات. حيث يطلق مصطلح الاختصاص العام الدولي للمحاكم على "ولاية المحاكم الوطنية في محاكمة الأجانب". فالمبدأ العام أنه لا ولاية للمحاكم الوطنية في محاكمة الأجانب الذين لا يقيمون على إقليم الدولة، لأنه لا فائدة من حكم يصدر على أجنبي ويصعب تنفيذه عليه فيها. بيد أن تطبيق هذا المبدأ قد يلحق ضرراً فادحاً بالمواطنين الذين يدخلون في تعامل مع أجنبي^١. لذلك نص قانون أصول المحاكمات السوري على الحالات التي يمكن فيها للمحاكم السورية أن تحاكم الأجنبي^٢. وبالعودة إلى نصوص هذه المواد وفيما يتعلق بالدفع الإلكتروني نجد أن المحاكم السورية تختص بمحاكمة الأجانب في الأحوال الآتية:

أ- إذا كان للمدعى عليه موطناً في سورية: تختص المحاكم السورية بمحاكمة الأجنبي إذا كان له محل إقامة أو سكن في سورية سواء أكان مكان دائم أو مؤقت أو مختار، كما تملك المحاكم صلاحية محاكمة الأجنبي الذي ليس له موطن في سورية إذا كان لأحد المدعى عليهم موطن أو سكن في سورية كما لو كان الأجنبي شريكاً أو كفيلاً

^١ د. محمد واصل، أصول المحاكمات المدنية، الجزء الأول، كلية الحقوق، منشورات جامعة دمشق، ٢٠١٠، ٢٠١١، ص ٣٨.

^٢ المواد (٣-١٠) من قانون أصول المحاكمات السوري رقم ١/ لعام ٢٠١٦.

أو له صلة حقيقية بالدعوى المرفوعة وبشرط أن يستند هذا الربط إلى ما يقوم عليه في ملف الدعوى^١.

ب- إذا نشأ الالتزام في سورية أو نفذ أو اشترط تنفيذه فيها: تملك المحاكم السورية حق محاكمة الأجنبي إذا كانت الدعوى تستند إلى أحد مصادر الالتزام وفق الآتي:

- إذا نشأ الالتزام في سورية: كأن يبرم العقد ضمن النطاق العلوي السوري.
- إذا تم تنفيذ الالتزام في سورية: كأن يبرم العقد في الخارج وينفذ في سورية أو ضمن نطاقها العلوي.
- إذا اشترط تنفيذ الالتزام في سورية: كأن يتعهد الملتزم بالعقد بتنفيذه في سورية أو ضمن نطاقها العلوي بموجب شرط في العقد.

ج- في حال قبول المدعى عليه: تختص المحاكم السورية بمحاكمة الأجنبي إذا عبّر صراحة أو ضمناً عن قبوله باختصاصها.

د- في حال اتخاذ التدابير التحفظية: تختص المحاكم السورية باتخاذ التدابير التحفظية المطلوب اتخاذها في سورية ولو لم تكن مختصة بأصل النزاع، كالدعوى المتعلقة بإلغاء الحجز الاحتياطي على أموال المدين في سورية أو وضعها تحت الحراسة القضائية.

هـ- الطلبات الفرعية: تختص المحاكم السورية بالنظر في الطلبات الفرعية أو العارضة المترتبة على الدعوى الأصلية بجميع حالات

^١ د. محمد واصل، مرجع سابق، ص ٣٩.

الاختصاص بشرط أن ترتبط بها برابطة لا تقبل التجزئة أو كان يقتضيها حسن سير العدالة^١.

ب- حالة كون أطراف العقد في سورية: تطبق في هذه الحالة القواعد العامة في الاختصاص. وبالعودة إلى هذه القواعد نجد أن القانون رقم ٢١/ لعام ٢٠١٤ نصّ على: «إحداث محكمة مصرفية بدائية و استئنافية في كل محافظة تختص بالنظر في القضايا المصرفية التي يكون أحد أطرافها مصرفاً أو مؤسسة مالية تقبل الودائع وتمنح التسهيلات الائتمانية الخاضعة لرقابة مجلس النقد والتسليف»^(٢).

كما نص على أن: «أحكام محكمة البداية تقبل الطعن بالاستئناف وأحكام محكمة الاستئناف تعتبر أحكام مبرمة»^(٣).

وبالتالي نجد أن النصوص السابقة جاءت عامة بحيث تشمل أي مصرف سواء أكان تقليدي أم إلكتروني (والمصرف هو أحد أطراف عملية الدفع الإلكتروني).

وبالنتيجة نجد أن أي نزاع يصيب عملية الدفع الإلكتروني يكون من اختصاص المحاكم المصرفية سواء وفقاً للقواعد العامة في الاختصاص (حالة كون أطراف العقد في سورية وهي الحالة النادرة أن يكون طرفا النزاع في دولة واحدة)، أم وفق قواعد الاختصاص الدولي (حالة كون أطراف العقد في بلدين مختلفين وهي الحالة الغالبة). ولكن تجدر الإشارة إلى ضرورة الانتباه لمسألة تشكيل هذه

^١ المرجع السابق ، ص ٤٥.

^٢ المادة الأولى من القانون رقم ٢١/ لعام ٢٠١٤ الخاص بإحداث محاكم مصرفية.

^٣ المادة الثانية من القانون رقم ٢١/ لعام ٢٠١٤ الخاص بإحداث محاكم مصرفية.

المحاكم بحيث ينبغي أن تضم ضمن أعضائها أشخاص ذوو خبرة بالأمور الفنية والتقنية التي تعتبر بمثابة العصب الأساسي في منازعات الدفع الإلكتروني.

ولكن التساؤل الذي يطرح نفسه: هل المحاكم المصرفية مختصة بأي نزاع يصيب عملية الدفع الإلكتروني بما في ذلك الجرائم الإلكترونية (كعمليات السرقة والاحتيال الإلكتروني)؟

عرّف قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الجريمة المعلوماتية بأنها: «جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومة المعلوماتية أو الشبكة»^(١).

أحدث المشرع السوري محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات. حيث نص القانون رقم ٩/ لعام ٢٠١٨ على أنه:

(أ) - تحدث محاكم جزائية بدائية واستئنافية للنظر في قضايا جرائم المعلوماتية وجرائم الاتصالات تملأ وظائفها من الملاك العددي لكل محافظة وتوزع بقرار من مجلس القضاء الأعلى .

ب- يشمل اختصاص المحاكم البدائية كافة الجرائم الجنحية سواء أكانت هذه الجرائم وفقاً للقواعد العامة من اختصاص محاكم البداية أم

^١ المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/

الصلح بما لا يتعارض مع أحكام الفقرة (ب) من المادة الخامسة من هذا القانون^(١).

كما نص ذات القانون على أنه: «تبقى جرائم المعلوماتية المرتبطة بجرائم تموينية أو مالية أو إرهابية أو متعلقة بأمن الدولة من اختصاص المحكمة النازرة بها موضوعاً»^(٢).

نجد من نصوص المواد السابقة أن الجرائم الإلكترونية التي تصيب عملية الدفع الإلكتروني (السرقية أو الاحتيال الإلكتروني على سبيل المثال) هي جرائم معلوماتية كونها تتم باستخدام الشبكة أو تقع على الشبكة، وبالتالي ينعقد الاختصاص في هذه الجرائم للمحاكم المحدثة بموجب القانون رقم ٩/ لعام ٢٠١٨ ما لم تكن هذه الجرائم ماسة بأمن الدولة أو جرائم تموينية أو مالية أو إرهابية حيث تبقى من اختصاص المحكمة النازرة بها موضوعاً.

وتصدر أحكام محكمة الاستئناف مبرمة في الجرائم الإلكترونية المعاقب عليها بعقوبة الغرامة فقط^(٣). كما يراعى عند توزيع العمل في

^١ المادة الثانية من القانون رقم ٩/ لعام ٢٠١٨ الخاص بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات.

^٢ الفقرة (ب) من المادة الخامسة من القانون رقم ٩/ لعام ٢٠١٨ الخاص بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات.

^٣ المادة الثالثة من القانون رقم ٩/ لعام ٢٠١٨ الخاص بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات.

محكمة النقض تخصيص غرفة للنظر في الطعون الجنحية والجناحية في جرائم المعلومات والاتصالات^١.

نستنتج مما تقدم أنه هناك جهتان قضائيتان تختصان بالنظر في المنازعات الناشئة عن عملية الدفع الإلكتروني:

أ- تختص المحاكم المصرفية بالمنازعات الناشئة عن عملية الدفع الإلكتروني وفقاً للقواعد العامة في الاختصاص أو وفقاً لقواعد الاختصاص الدولي (ومثال هذه المنازعات تحديد طبيعة الالتزامات القانونية - أو أي نزاع لا يرتق لمرتبة الجرائم الإلكترونية)

ب- تختص المحاكم المحدثّة للنظر بالجرائم الإلكترونية التي تصيب عملية الدفع الإلكتروني ما لم تكن الجرائم الإلكترونية من الجرائم الماسة بأمن الدولة أو جرائم مالية أو تموينية أو إرهابية والتي تبقى من اختصاص المحكمة النازرة بها موضوعاً، وليس في هذا الاختصاص أي تعارض مع اختصاص المحاكم المصرفية وذلك على اعتبار أن الخاص يقيد العام.

ولكن تجدر الإشارة إلى أن اختصاص المحاكم السورية بمنازعات الدفع الإلكتروني لا يعني حتماً تطبيق القانون السوري إنما يمكن للمحاكم السورية أن تطبق القانون الأجنبي على منازعات الدفع الإلكتروني.

^١ المادة الرابعة من القانون رقم ٩/ لعام ٢٠١٨ الخاص بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات.

وينبغي أن نشير إلى أن أطراف النزاع (منازعات العقود الإلكترونية) كثيراً ما يلجؤون إلى التحكيم كوسيلة لحل أي نزاع ينشأ عن هذا العقد، ويتعدون عن الطريق القضائي وذلك نظراً لخصوصية النزاعات الناشئة عن العقد الإلكتروني والتي تتطلب خبرة ودراية قانونية وتقنية في آن واحد. ويبقى هذا الحل هو الأنسب في الحالات التي يقدم فيها المصرف الإلكتروني خدمة الدفع الإلكتروني في الفضاء الخارجي أي أنه يصعب إخضاعه للنطاق العلوي السوري أو نطاق أي دولة أخرى.

وفي سبيل إغناء البحث القانوني سوف نقوم بالحديث عن المحاكم الإلكترونية باعتبارها أحد الجهات القضائية المختصة بمنازعات الدفع الإلكتروني. فقد صاحب انتشار مفهوم الحكومة الإلكترونية ظهور مصطلح جديد أطلق عليه "المحاكم الإلكترونية" وحيث أننا نتحدث في إطار الحلول القانونية لمشكلة القضاء المختص بمنازعات الدفع الإلكتروني لذلك سوف نقوم بتسليط الضوء على هذه المحاكم ولو بشكل مختصر على النحو الآتي:

١- تعريف المحكمة الإلكترونية:

تُعرف المحكمة الإلكترونية بأنها: ((حيز تقني معلوماتي ثنائي الوجود، يسمح ببرمجة الدعوى الإلكترونية، ويتألف من شبكة الربط الدولية إضافة إلى مبنى المحكمة، بحيث يتيح الظهور المكاني الإلكتروني لوحدات قضائية وإدارية وبياسر من خلاله مجموعة من القضاة مهمة النظر في الدعوى والفصل فيها بموجب تشريعات تخولهم مباشرة الإجراءات القضائية

مع اعتماد آليات تقنية فائقة الحداثة لتدوين الإجراءات القضائية وحفظها وتداول ملفات الدعوى^(١).

يلاحظ على التعريف السابق أن المحكمة الإلكترونية هي نوع من إدخال التقنيات الإلكترونية على إجراءات التقاضي بغية تبسيط هذه الإجراءات دون التخلي عن العنصر البشري (القضاة).

ونحن من جانبنا نعرّف المحكمة الإلكترونية بأنها: «كيان افتراضي يستخدم شبكة الإنترنت بغية السير في إجراءات الدعوى بشكل سريع ودون المساس بمبادئ الشفافية والعلنية التي يتطلبها إصدار الأحكام من قبل القضاة البشريين وليس من قبل الآلة أو الجهاز».

وهذا التعريف هو الأنسب برأينا وذلك للمبررات الآتية:

أ- المحكمة الإلكترونية هي أحد نتائج مشروع الحكومة الإلكترونية الذي يقوم على إدخال الوسائل التقنية ضمن مرفق العدالة.

ب- المحكمة الإلكترونية تهدف لتبسيط إجراءات الدعوى دون المساس بالمبادئ الأساسية للتقاضي.

ج- يمكن إدخال العنصر التقني إلى بعض الإجراءات في المحاكم كالتدوين الإلكتروني والتبليغ الإلكتروني والاطلاع على ملفات الدعوى عبر موقع المحكمة، إضافة إلى إمكانية تقديم الدفوع والمذكرات بشكل إلكتروني. فهذه الجوانب تمس بالإطار الإجرائي

^١ د. نهى الجلا، المحكمة الإلكترونية (٢)، بحث مقدم إلى مجلة المعلوماتية، السنة الخامسة، العدد (١٤٧)، دمشق، ٢٠١٠، ص ٥٠.

للدعوى وبالتالي إدخال التقنية عليها يسهم في توفير الوقت والتكلفة الأمر الذي يسهم بتبسيط إجراءات الدعوى.

د- لا يمكن إدخال العنصر التقني إلى بعض الإجراءات في المحاكم، إذ لا يمكن أن تحل الآلة محل القاضي وتأخذ دوره ولا يمكن التخلي عن مبادئ العلنية والشفافية. فالأحكام تصدر في جلسات علنية يحضرها الجميع وبناءً على أدلة وبراهين كونت قناعة القاضي. وبالتالي فإن هذه المبادئ لا يمكن إدخال التقنية عليها حفاظاً على سلامة مرفق العدالة.

٢- إجراءات التقاضي أمام المحكمة الإلكترونية:

أ- تبدأ الخصومة القضائية أمام المحكمة الإلكترونية كما هو الحال في التقاضي التقليدي من خلال تقديم استدعاء يحتوي على كافة البيانات الموجودة على الاستدعاء الورقي إلا أنه في الخصومة الإلكترونية تكون وثيقة الاستدعاء محررة بشكل إلكتروني ومذيلة بتوقيع إلكتروني للمدعي.

ب- يرسل الاستدعاء إلى قسم الإحالات في المحكمة المختصة من خلال شبكة الإنترنت وعبر البريد الإلكتروني حيث يتم قيدها، ويتعرف المدعي على رقم دعواه الإلكترونية في الحال^١.

ج- تقوم المحكمة بمراسلة المدعي عليه وتبليغه استدعاء الدعوى المقامة ضده خلال مدة محددة من تسجيلها. وللمدعي عليه الحق

^١ د. صفاء أوتاني، المحاكم الإلكترونية (المفهوم والتطبيق)، بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٨، العدد الأول، دمشق، ٢٠١٢، ص ١٧٤.

في رفض المثول أمام المحكمة أو القبول من خلال ملء استمارة مماثلة لاستدعاء المدعي ومذيلة بتوقيعه الإلكتروني.

د- يقع الدور المهم في ظل هذه المحكمة على عاتق موظف المحكمة المختص الذي يقوم بأتمتة المعلومات الخاصة بأي دعوى من اللحظة الأولى لتسجيلها وحتى آخر مراحلها، كما يقوم بتحديث البيانات تبعاً لتقدم إجراءات الدعوى^١.

هـ- يتم تزويد كل محامي وكل خصم ببريد إلكتروني عن موقع المحكمة بحيث يتلقى فيه المحامي طلبات المحكمة على بريده الإلكتروني. كما يمكنه الدخول إلى موقع المحكمة بهدف تقديم الدفوع والوثائق الإلكترونية أو بهدف الاطلاع على سير الدعوى.

و- بعد فحص الوثائق وسماع الدفوع يقوم القاضي البشري بجمع كافة الأدلة التي كونت قناعته ويصدر حكمه العلني في جلسة عامة يحضرها الجميع^٢.

ولعل خير مثال عن المحكمة الإلكترونية هو الحاسوب القاضي في الصين^٣. فقد أنشأت الصين و تحديداً في مدينة زيبو - إقليم شاندونج - محكمة إلكترونية تعتمد على برنامج حاسوبي

^١ د. حسن علي عثمان، هنا... المحكمة الإلكترونية، بحث منشور على موقع جريدة الأهرام ومتاح

على الرابط: www.ahram.org.eg

تاريخ الزيارة ٢٠١٩/١/١٣ الساعة ١٠,٣٠ A,m

^٢ د. صفاء أوتاني، مرجع سابق، ص ١٧٥.

^٣ مشار لهذا المثال لدى المرجع السابق، ص ١٧٤.

متطور يقوم بحفظ القوانين والأنظمة النافذة كافة فضلاً عن حفظ ظروف الإدانة المحتملة والسوابق القضائية. تبدأ الدعوى أمام هذه المحكمة بإعداد كل من الادعاء والدفاع لمعطياتهما ومطالبهما على قرصين مدمجين (CD) يملكان السعة ذاتها، ثم تدخل بيانات هذين القرصين إلى البرنامج الحاسوبي للاحتكام للقاضي الإلكتروني الذي يمكنه أن يطلب رأي القاضي البشري بخصوص بعض التفاصيل الخاصة أو تلك المتعلقة بالنواحي الإنسانية قبل أن يقوم بإصدار الحكم.

٣- متطلبات إنشاء المحاكم الإلكترونية في سورية:

لا يتوقف إنشاء محاكم إلكترونية في سورية على إصدار مرسوم أو قرار بإحداث مثل هذه المحاكم فحسب، بل قبل ذلك لا بد من تهيئة البيئة المناسبة لوجود هذه المحاكم. وبالتالي فإن إنشاء هذه المحاكم يستلزم عدة متطلبات وخطوات نجلها في الآتي^١:

أ- نشر المعلومات القضائية لأكبر عدد من المستفيدين منها: يعد الإنترنت أكثر وسائل النشر انتشاراً، حيث تنشأ مواقع إلكترونية ذات واجهات بسيطة في الدوائر القضائية في كل محافظة، و يتم من خلال تلك المواقع الحصول بسرعة على كافة المعلومات التي تهم المتقاضيين ووكلائهم دون الحاجة للسفر.

ب- التفاعل مع المتقاضين ووكلائهم: بهدف توسيع نطاق المشاركة من المتقاضين ووكلائهم وضمان تفاعلهم مع الخدمات التي تقدمها المحاكم

^١ مشار لهذه الخطوات لدى المرجع السابق، ص ٢٠١.

الإلكترونية، لا بد من السعي لتبسيط الإجراءات و تقليل النماذج و الاقتصاد على طلب المعلومات الضرورية التي تهم العمل القضائي والاهتمام برأي زوار الموقع من الأشخاص العاديين والمحامين للتحقق من أن تلك المعلومات و النماذج القضائية ما تزال قيد الاستخدام .

ج- تهيئة البيئة التحتية اللازمة لإنشاء هذه المحاكم: حيث يتطلب توفير البيئة التحتية اتخاذ ما يلي :

- تحديث التشريعات والإجراءات القضائية.
- تحديث بنك المعلومات القضائية.
- بناء بنية متطورة للشبكات.
- إعادة تأهيل الأشخاص العاملة في المجال القضائي.

د- التطبيق الكامل للمحكمة الإلكترونية: حيث يمكن إنشاء موقع إنترنت خاص بمحاكم مدينة دمشق، وتتم أتمتة المعلومات في هذه المحاكم وتحميلها على شبكة الإنترنت بواسطة برامج إلكترونية خاصة. كما يمكن إنشاء نوافذ لهذا الموقع تضم معلومات عن درجات التقاضي ومواعيد الجلسات وملفات التنفيذ وغير ذلك من الخدمات القضائية. فمن خلال الاتصال بهذا الموقع و زيارته يمكن تصفح المعلومات التي تهم المتقاضين، كما يمكن بالبريد الإلكتروني تلقي المعلومات و الوثائق المسموح بانتقالها إلكترونياً.

و نحن من جانبنا نرى بأننا في سورية بدأنا بالتطبيق الجزئي لبعض هذه المتطلبات سواء على صعيد التشريعات النازمة للمعاملات الإلكترونية أم على صعيد مشاريع الأتمتة لبعض الخدمات القضائية كمسألة التبليغ القضائي الإلكتروني، ولكن العائق الوحيد أمام التطبيق

الكلي للمحاكم الإلكترونية إنما يتمثل في عدم وجود مجتمع معلوماتي يثق بشبكة الإنترنت و بالخدمات المقدمة من قبله.

وفي ختام الحديث عن التدابير الوقائية والتدابير العلاجية لمشكلات الشراء عبر الحدود . نجد أن التدابير الوقائية من الناحية النظرية تسهم في وضع حد نهائي لمشكلة القانون الواجب التطبيق والمحكمة المختصة وإذا ما طبقت فإنها لن تسمح بحدوث أي نزاع، لكن من الناحية العملية والواقعية نجد أنه هناك صعوبة إن لم نقل استحالة في الوصول إلى اتفاق موحد بين الدول حول هذه المشكلة وخصوصاً في ظل الاختلافات السياسية والتقنية بين الدول، الأمر الذي يجعل من هذه التدابير بمثابة شعارات تفقد سندها في التطبيق.

أما بالنسبة للتدابير العلاجية فهي وإن كانت ضمن نطاق التشريع السوري فقط لكنها تسهم إلى حد كبير في علاج هذا النوع من المشكلات، الأمر الذي يكسبها أهمية كبيرة عند التطبيق وخصوصاً إذا ما تم بلورتها بشكل قانوني سليم من قبل المشرع السوري بهدف تلافى أي ثغرة قانونية لم نتمكن من معالجتها أو الانتباه لها.

الفرع الثاني

معالجة المشكلات المتعلقة بالمستهلك الإلكتروني

أدى التطور والتقدم الهائل في مجال المعلوماتية إلى تزايد الضغوط على المستهلك وذلك من أجل إغرائه للدخول في عالم التجارة الإلكترونية وإقناعه بالتعاقد من خلال شبكة المعلومات. ولما كان المستهلكون هم السواد الأعظم في المجتمع فإن الحاجة إلى حمايتهم في مجال إبرام العقد الإلكتروني تشكل ضرورة ملحة وأهمية بالغة، حيث أصبح المستهلك في ظل تزايد الإقبال على إبرام العقود والمعاملات الإلكترونية عرضة للتلاعب بمصالحه وضماناته، إذ أن التاجر وفي سبيل تسويق منتجاته وتوزيعها قد يسعى بوسائل غير مشروعة إلى تضليل المستهلك وخداعه عن طريق إيهامه بوجود مزايا غير حقيقية في تلك السلع أو عدم الاهتمام بتوفير متطلبات السلامة في منتجاته. وتتمثل أساليب حماية المستهلك الإلكتروني من خلال فرض مجموعة من الالتزامات القانونية التي ورد ذكرها في عدة نصوص قانونية نافذة للمعاملات التقليدية والإلكترونية. وتجدر الإشارة إلى أن معظم هذه الالتزامات تقع على عاتق التاجر في نطاق التعامل بالدفع الإلكتروني وذلك على اعتبار أن الشخص الذي يستخدم وسيلة الدفع الإلكتروني يمتلك صفتين: الأولى: صفة العميل وذلك عندما يكون تعامل الشخص مع المصرف للحصول على وسيلة الدفع الإلكتروني.

والثانية: صفة المستهلك وذلك عندما يدخل العميل في تعاملات مع التاجر باستخدام وسائل الدفع الإلكتروني حيث يصبح مستهلك.

وبالتالي سوف نتحدث عن الحماية المقررة بموجب القوانين واللوائح النازمة للمعاملات الإلكترونية (أولاً) ثم ننتقل للحديث عن الحماية المقررة بموجب القوانين النازمة للمعاملات التقليدية (ثانياً).

أولاً: الحماية المقررة للمستهلك الإلكتروني بموجب القوانين واللوائح النازمة للمعاملات الإلكترونية.

سوف نتحدث بدايةً عن الحماية المقررة للمستهلك الإلكتروني بموجب قانون المعاملات الإلكترونية ثم ننتقل للحديث عن الحماية المقررة بموجب اللائحة التنظيمية للضوابط والنواظم الخاصة بحماية المستهلك الإلكتروني والتسويق الإلكتروني.

١- الحماية المقررة للمستهلك الإلكتروني بموجب قانون المعاملات الإلكترونية:

ألزم قانون المعاملات الإلكترونية التاجر في نطاق العقود الإلكترونية بمجموعة من الالتزامات لمصلحة المستهلك الإلكتروني، حيث شكّلت هذه الالتزامات نوع من الحماية القانونية للمستهلك الإلكتروني. ولعلّ من أبرز هذه الالتزامات:

أ-الالتزام بالإعلام الإلكتروني

يعتبر الالتزام بالإعلام من أهم وأبرز الآليات القانونية في مجال حماية المستهلك بصفة عامة وفي مجال العقد الإلكتروني بصفة خاصة، ذلك أن هذا النوع من العقود يتم من خلال استخدام الوسائط الإلكترونية دون نقاء مادي بين أطرافه وبالتالي يكتنف هذا النوع من العقود مجموعة من المخاطر التي قد تؤثر على رضا المستهلك.

لذلك سوف نتحدث بدايةً عن تعريف الالتزام بالإعلام الإلكتروني ثم ننقل للحديث عن محددات الالتزام بالإعلام الإلكتروني

أ-تعريف الالتزام بالإعلام الإلكتروني:

اتجه جانب من الفقه إلى تعريف الالتزام بالإعلام بأنه: «الالتزام قانوني سابق على التعاقد يلتزم فيه المدين بإعلام الدائن في ظروف معينة إعلاماً صحيحاً وصادقاً بكافة المعلومات الجوهرية المتصلة بالعقد المراد إبرامه والتي تعجز وسائله الخاصة عن الإحاطة بها ليبني عليها رضاه في العقد»^(١).

كما عرف بعض رجال القانون الالتزام بالإعلام بأنه: «تنبيه أو إعلام طالب التعاقد بمعلومات من شأنها إلقاء الضوء على واقعة ما أو عنصر ما من عناصر التعاقد حتى يكون الطالب على بينة من أمره بحيث يتخذ قراره الذي يراه مناسباً على ضوء حاجته وهدفه من إبرام العقد»^(٢).

يلاحظ على التعريفين السابقين أنهم ألزموا (المدين بالالتزام بالإعلام وهو التاجر) أن يعلم طالب التعاقد (المستهلك) بكافة المسائل الجوهرية في العقد، والتي من شأنها أن تؤثر على رضا المستهلك. ولكن كلا التعريفين تناولا الالتزام بالإعلام بشكل عام دون التعرض للالتزام بالإعلام الإلكتروني .

^١ سهام إمدالو و ليلي حسن، مرجع سابق، ص ٢٨.

^٢ عبد الله محمود، مرجع سابق، ص ٤٩.

ونحن من جانبنا نعرّف الالتزام بالإعلام الإلكتروني بأنه: ((الالتزام التاجر بإعلام وتبصير المستهلك بمعلومات شاملة عن كافة العناصر الجوهرية والعناصر الثانوية المتعلقة بالعقد الإلكتروني كشخص التاجر، ثمن المنتج، مواصفات السلعة والتي من شأنها أن تؤثر على قرار المستهلك)).

وبالتالي فإن الالتزام بالإعلام الإلكتروني هو التزام قانوني يفرضه مبدأ حسن النية طالما أنه يتم بكل شفافية وأمانة. ولعل المبرر الأساسي لهذا الالتزام هو عدم المساواة بين المتعاقدين في معرفة المعلومات المتعلقة بمحل العقد والشروط المتعلقة به، فضلاً عن عدم التوازن العقدي في مثل هذه العقود بسبب اختلاف المراكز القانونية لأن الطرف الضعيف يتعرض لاستغلال الطرف القوي صاحب الخبرة. ومن هذا المنطلق يتعين على التاجر أن يفض إلى المستهلك بالمعلومات الكافية عن العناصر الرئيسية والتي يمكن للمستهلك من خلالها اتخاذ قراره بالتعاقد من عدمه.

ب- محددات الالتزام بالإعلام الإلكتروني:

يهدف الالتزام بالإعلام الإلكتروني إلى التتوير والتبصير عن طريق إدلاء التاجر بكافة المعلومات الضرورية المؤثرة في قرار المستهلك. وتتمثل محددات هذا الالتزام في الآتي:

- **تحديد شخصية التاجر:** إن عدم معرفة شخصية التاجر من أهم المشكلات التي تثير قلق المستهلك و تحدّ من إقباله على إبرام عقود الاستهلاك الإلكتروني، فبيان شخصية التاجر يوفر عنصر الأمان في التعاقد عن

بعد، لذا على التاجر تقديم معلومات واضحة للمستهلك تتعلق بهويته ومحلّه التجاري وبريده الإلكتروني، ووضعها تحت تصرف المستهلك للاطلاع عليها في جميع مراحل المعاملة. وتأكيداً على ذلك فقد قام المجلس الوطني الفرنسي بإصدار قرار يقضي بضرورة الإعلان عن كافة المعلومات المتعلقة بالتجار الوستاء على الشبكة. وذلك بغية تسهيل المهمة على المستهلك بحيث يمكن للمستهلك الرجوع إلى ذلك السجل قبل الدخول في أي علاقة تعاقدية^١.

• تحديد الوقت المحدد لصاحبة الإيجاب: يبرز هذا

المُحدد عندما يقترن الإيجاب بوقت معين. حيث إن تحديد وقت للإيجاب يشكل استثناء في نطاق العقود الإلكترونية ذلك لأن القليل من المواقع التجارية تتولى تحديد المدة اللازمة للإيجاب الصادر عنها. ولكن نظراً لأن عدم تحديد مدة للإيجاب فيه إضعاف للمركز القانوني للمستهلك إضافةً لضعفه الاقتصادي و المعلوماتي، لذلك أصبح الإيجاب الإلكتروني يقترن بوقت محدد بهدف حماية المستهلك واستمرار المعاملات الإلكترونية. ويكون الموجب ملزماً بإيجابه طيلة المدة المحددة حتى يتسنى للطرف الآخر تدبير

¹ Schuht Cristiane Feral :Les relations juridiques entre les acteurs dumarché virtuel). Les Contrats du Commerce Electronique, revue du droit des contrats,1999,p21.

مشار إليه لدى :سهام إمدالو و ليلي حسن، مرجع سابق، ص ٧١.

أموره والرد على الإيجاب بالقبول أو بالرفض. وتجدر الإشارة إلى أن سكوت الموجه إليه الإيجاب عن الرد قد يشكل قبولاً في ظروف معينة^١.

• **البيانات الأساسية عن السلعة أو الخدمة:** يقتضي التزام التاجر بالإعلام قيامه بالإفشاء إلى المستهلك بالمعلومات والبيانات الضرورية اللازمة لمساعدته في اتخاذ قراره بالتعاقد من عدمه، وأي تقصير في تزويد المستهلك بهذه المعلومات يستوجب مسؤولية التاجر^٢. وتتضمن هذه المعلومات:

❖ **الحالة القانونية للمبيع:** ويقصد بها إعلام المستهلك بكل ما على المبيع من حقوق والتزامات عينية أو شخصية تحول دون انتفاعه بالمبيع.

❖ **الحالة المادية للمبيع:** وتتضمن كافة المعلومات المتعلقة بالخصائص والأوصاف المادية للمبيع .

❖ **كيفية الاستعمال:** وتتمثل في تزويد المستهلك بالحد الأدنى من المعلومات والتي يتعذر على المستهلك استعمال السلعة بدونها.

❖ **مخاطر السلعة:** إحاطة المستهلك بالمخاطر الناجمة عن استعمال السلعة وكيفية الوقاية منه.

• **إعلام المستهلك باللغة الوطنية:** يعتبر وجوب مراعاة اللغة الأم لكل مستهلك من أشكال الحماية التي أضافتها المبادئ

^١ د. إلياس ناصيف، العقود الدولية، العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية ، بيروت، ٢٠٠٩، ص ١٠٤.

^٢ عبد الله محمود، مرجع سابق، ص ٥٨-٦٠.

القانونية المعاصرة، ليتسنى له فهم مضمون العقد الذي يريد أن يقدم عليه. إذ أوجبت المبادئ القانونية الحديثة أن يكون العقد بلغة المستهلك، حيث أن وجود مصطلحات فنية وقانونية غير مألوفة أو ذات دلالات قانونية مختلفة- في ظل عالمية الإيجاب الإلكتروني- يثير مشكلة في إعلام المستهلك وخصوصاً إذا كان النظام القانوني المتبع في دولة المستهلك يختلف عن النظام المتبع في دولة التاجر. وهذا ما أكدته قانون توبون الفرنسي^١ حيث جاء فيه: «يجب استخدام اللغة الفرنسية في الإيجاب في كل أنواع التجارة بما في ذلك التجارة الإلكترونية وبصفة خاصة في التعليمات الخاصة بالتشغيل، وشروط الضمان، ووصف المنتج أو الخدمة والفواتير والإيصالات. وينطبق هذا على الإعلانات المرئية والمسموعة أو الناطقة أو المكتوبة».

- **إعلام المستهلك بثمن السلعة أو الخدمة:** يعد الثمن من العناصر المهمة التي يعتمد عليها المستهلك مقابل حصوله على السلعة. حيث يبين المستهلك قراره في الإقدام على شراء سلعة بناءً على إمكانيته المادية ومع تمسكه في الحرص على عدم دفع أكثر من القيمة الحقيقية للسلعة. لذلك يجب على التاجر إعلام المستهلك بالمقابل النقدي لكل

^١ المادة الثانية من قانون توبون الفرنسي (LOI TOUBON) رقم (٩٤/٦٦٥) تاريخ ١٩٩٤/٨/٤ والمتعلق باستخدام اللغة الفرنسية وسمي بهذا الاسم نسبة لوزير الثقافة جاك توبون.

سلعة وقت الإيجاب الصادر عنه، وتعد المواقع الإلكترونية وسيلة مناسبة للإعلام بأسعار السلع والخدمات^١.

وقد أكد المشرع السوري على الالتزام بالإعلام في نطاق العقود الإلكترونية. حيث نص قانون المعاملات الإلكترونية على أنه:

(أ- على البائع تقديم معلومات واضحة تمكّن المستهلك من اتخاذ قراره في الشراء ومنها:

- ❖ التعريف بالبائع وعنوانه ورقم ومكان تسجيله وبريده الإلكتروني.
- ❖ وصف مفصل لمراحل إنجاز المعاملة الإلكترونية.
- ❖ نوع وطبيعة وخواص ومواصفات وسعر السلعة أو الخدمة.
- ❖ نفقات تسليم المنتج ومبلغ تأمينه والضرائب المستحقة وأي مبالغ أخرى.
- ❖ المدة الزمنية التي يكون خلالها البائع ملتزماً بالأسعار المعلن عنها.
- ❖ المعلومات الخاصة بخدمة ما بعد البيع والضمانات التجارية المتوفرة.
- ❖ طرق وإجراءات الدفع الإلكتروني.
- ❖ طرق و آجال التسليم وتنفيذ العقد والآثار المترتبة على عدم التنفيذ.
- ❖ طرق إعادة أو استبدال المنتج واسترداد المبلغ المدفوع وآجال ذلك.

^١ يحيى حسن، مرجع سابق، ص ٣٧.

❖ العملة المعتمدة في الدفع.

❖ النفقات الإضافية لاستعمال تقنيات الاتصال المتعلقة بالمعاملة.

❖ إرشادات استخدام السلعة والتحذيرات من الاستخدام الخاطئ.

ب- يشترط في أي رسالة إلكترونية موجهة إلى المستهلك أن تتضمن هوية المرسل أو من يمثله بطريقة معتمدة.

ج- يجب توفير هذه المعلومات إلكترونياً للمستهلك للاطلاع عليها في جميع مراحل المعاملة الإلكترونية^(١).

كما نص ذات القانون على أنه: ((على البائع قبل إقرار عملية البيع تمكين المستهلك بطريقة إلكترونية مناسبة من مراجعة أخطاء إدخال المعلومة والمراجعة النهائية لجميع خياراته وتمكينه من إقرار التعاقد أو تغييره أو العدول عنه حسب إرادته^(٢))).

بدايةً ينبغي أن نشير أن البائع في نطاق العقد الإلكتروني هو ذاته التاجر في نطاق عملية الدفع الإلكترونية. ويلاحظ من نص المادة ١٧/ أن المشرع السوري تبنى محددات الالتزام بالإعلام على شكل ثلاثة التزامات:

الشكل الأول: الالتزام بالتبصير قبل إبرام العقد الإلكتروني (كاسم البائع وعنوانه وبريده الإلكتروني-تفصيل مراحل إنجاز المعاملة- مواصفات وسعر المنتج).

^١ المادة ١٧/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

^٢ المادة ١٨/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

الشكل الثاني: تبصير المستهلك في مرحلة إبرام العقد الإلكتروني (كنفقات تسليم المنتج ومبلغ تأمينه- الفترة التي يلتزم فيها البائع بالأسعار- وطرق وإجراءات الدفع- طرق وأجال التسليم).

الشكل الثالث: الإعلام اللاحق على العقد الإلكتروني (كطرق إرجاع المنتج أو إيداله والضمانات المقدمة).

كما ألزمت المادة (١٨) البائع بتمكين المستهلك من مراجعة أخطائه في إدخال المعلومات وذلك بغية توفير الحماية للمستهلك قبل اتخاذ قراره النهائي.

وقد سبق أن أشرنا إلى أن الالتزام بالإعلام يقع على عاتق التاجر تجاه المستهلك، ولكن تجدر الإشارة إلى أنه وفي نطاق التعامل بالدفع الإلكتروني يقع على عاتق المصرف التزام بالإعلام تجاه مستخدم أداة الدفع (العميل بالنسبة للمصرف).

حيث أكد مجلس الرقابة على المؤسسات المالية الفيدرالية الأمريكي (FFIEC) على التزام المصرف الإلكتروني بالإعلام في مواجهة عملائه، من خلال إعلامهم بالبيانات الخاصة بالخدمات التي يقدمها. ومن أهم هذه البيانات:¹

- البيانات الخاصة بالتعريف بالمصرف وكشف هويته في مكان واضح على الموقع الإلكتروني للمصرف (كعلامته التجارية

¹ Apostolos Ath, Gkoutzinis, Internet Banking And The Law In Europe, Cambridge University Press, First Published, 2006, P184.

ورقم تسجيله ورقم قيده لدى جهة الرقابة)، حيث تفيد هذه البيانات في التأكد أنه يتعامل مع الموقع الحقيقي.

• السياسة الأمنية التي تحكم استعمال موقع المصرف والتعامل معه.

• السياسة التي تحكم الحفاظ على سرية البيانات الخاصة بالمعاملات المصرفية التي تتم عبر موقع المصرف وذلك من خلال:

- توضيح التعليمات والإرشادات التي يجب على العميل الالتزام بها أثناء التعامل مع موقع المصرف وذلك بما يتفق مع القوانين الخاصة بالسرية.

- رسم الخطوات التي يجب على العميل اتباعها أثناء إدخال البيانات الخاصة به، وتمكينه من إخفاء هذه البيانات عن المشاركين في التعامل مع موقع المصرف كمقدمي الخدمات الإلكترونية للمصرف.

ويحتل الالتزام بالإعلام في نطاق التعاملات المصرفية الإلكترونية أهمية كبيرة باعتباره الفصيل الأساسي لتحديد المسؤولية عن عمليات الاحتيال على المدفوعات وفي سبيل التوضيح نورد المثال القضائي الآتي¹:

¹Cour d' appel d' Aix-en-provence, Arrêt du 28 mars 2019, Répertoire général n° 17/18362.

ففي أحد القضايا كان هناك أحد العملاء الذين يتعاملون مع شركة (Boutique Solution) في سبيل عمليات التحويل الإلكتروني للأموال، وكانت الشركة المذكورة قد تعاقدت مع شركة (Capac) كمزود خدمة ومسؤول عن برمجة و أتمتة و قيد كافة عمليات التحويل. وبعد مضي فترة من التعاملات فوجئ العميل بحدوث نوع من الاحتيال على المدفوعات من قبل شركة (Capac) حيث عندما يقوم العميل بتحويل (١٠٠٠ يورو) تقوم شركة (Capac) بقيد المبلغ (١٠٠٠ يورو). الأمر الذي دفع العميل لإقامة دعوى على شركة (Boutique Solution) مدعياً أن العقد الذي تم توقيعه في /سبتمبر ٢٠١٥ / يلزم شركة (Boutique Solution) بضمان الاحتيال على المدفوعات فلو كان يعلم بالأنشطة الاحتيالية لشركة (Capac) لم يخاطر بمتابعة عمليات التحويل بواسطتها.

قضت المحكمة بمسؤولية شركة (Boutique Solution) عن التعويض عن كافة العمليات التي تمت في /عام ٢٠١٥ حتى بداية ٢٠١٦ / نتيجة لإخلال الشركة المتكرر في الوفاء بالتزاماتها وقد استندت المحكمة في حكمها للمبررات الآتية:

١- إن شركة (Boutique Solution) أخلّت بالتزاماتها من خلال قيد المبلغ بشكل مخالف للحقيقة بواسطة شركة (Capac)، على اعتبار أن شركة (Boutique Solution) عليها التزام بقيد المبلغ بشكل حقيقي دون أي زيادة وبغض النظر إن كان قيد المبلغ تم من قبل الشركة نفسها أو من قبل شركة (Capac) باعتبار أن العلاقة بين الشركتين تدخل في إطار الأعمال الإدارية لشركة

(Boutique Solution) والتي لا شأن للعميل بها.

٢- إن شركة (Boutique Solution) لم تمتثل لقواعد الأمن المفروضة بموجب العقد في سياق المعاملات المالية السابقة (قبل بداية عام ٢٠١٦).

٣- إن شركة (Boutique Solution) قد تجاهلت جميع المعلومات بشأن أي عمليات احتيال تم إجراؤها.

٤- إن شركة (Boutique Solution) قررت تحرير نفسها من العملية الأمنية بأكملها وتمرير المعاملات غير المضمونة.

وقد تحملت شركة (Boutique Solution) ما يقارب (٤٠٠٠٠ يورو) في غضون بضعة أيام نتيجة عمليات التحويل غير المضمونة مع شركة (Capac).

أما بالنسبة لعمليات التحويل التي تمت بعد /بداية عام ٢٠١٦/ فقد قضت المحكمة بعدم مسؤولية شركة

(Boutique Solution) عن عمليات التحويل غير المضمونة خلال هذه الفترة، ومرد ذلك إلى أن شركة

(Boutique Solution) قد نبهت وأعلنت العميل بموجب شهادة رسمية عن الأنشطة الاحتيالية لشركة (Capac). وبالتالي يتحمل العميل المسؤولية عن هذه العمليات باعتبار أن شركة (Boutique Solution) قد أوفت بالتزامها لجهة إعلام العملاء بعدم التعامل مع شركة (Capac) نتيجة الطبيعة الاحتيالية لأنشطتها.

وبناءً على ما تقدم نجد أن الالتزام بمحددات الإعلام التي سبق الحديث عنها يشكل أحد المرتكزات الأساسية لحماية المستهلك الإلكتروني، وذلك على اعتبار أن الالتزام بالإعلام والتبصير هو حلقة البداية في العقود الإلكترونية ويشمل مختلف مراحل هذه العقود بدءاً بالتفاوض مروراً بإبرام العقد وانتهاءً بتنفيذ العقد. وبالتالي فإن أي خلل أو نقص في محددات الالتزام بالإعلام من شأنه أن يلحق الضرر بالمستهلك الأمر الذي يستوجب مسؤولية التاجر عن الضرر الذي يصيب المستهلك من جراء أي خلل أو نقص في هذا الالتزام.

ب- حماية البيانات الشخصية للمستهلك الإلكتروني

تتضمن المعاملات الإلكترونية بيانات شخصية يتم إرسالها من المستهلك إلى التاجر في إطار التحقق والتأكيد على عملية البيع. وقد تكون هذه المعلومات عبارة عن بيانات اسمية أو عدة صور في شكل إلكتروني، كما قد تشمل مقر إقامة المستهلك وطبيعة عمله أو بياناته المالية. فحماية خصوصية المستهلك أمر ضروري وهذا الأمر يتطلب إيجاد الآليات التي تمنع الاستعمال غير المشروع لهذه المعلومات الناتجة عن المعاملات الإلكترونية. حيث تشكل هذه البيانات جزءاً من الحياة الخاصة للمتعاقد عبر الإنترنت فلا يجوز الإفشاء بها للغير بقصد أو دون قصد ولا يحق للتجار تداولها فيما بينهم في سبيل الترويج للسلع أو خدمات أخرى، كما لا يجوز للتاجر نفسه استخدامها بعد انتهاء العقد. لذلك تدخلت التشريعات المختلفة لتنظيم الحق في احترام الحياة الخاصة للأفراد وحظرت كل اعتداء يقع عليها، حيث وضعت مؤيدات جزائية بحق من يقوم بإفشاء البيانات الشخصية أو

ينتهك حرمة الحياة الخاصة. ومن بين التشريعات التي أكدت على حماية البيانات الشخصية المشرع السوري. حيث نص قانون المعاملات الإلكترونية على أنه: «يلتزم أطراف النشاط الاقتصادي الذين يمارسون نشاطهم بالوسائل الإلكترونية بحماية جميع المعلومات العائدة لباقي الأطراف ولا يجوز لهم التصرف أو التعامل بما من شأنه أن يحمل ضرراً مادياً أو معنوياً لأصحاب هذه المعلومات إلا بموافقة صريحة من أصحابها»^(١).

كما نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه: «يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة إلى خمسمائة ألف ليرة سورية، كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه حتى ولو كانت هذه المعلومات صحيحة»^(٢).

نستنتج من النصين السابقين أن المشرع السوري ألزم التاجر أن يحافظ على جميع المعلومات المتعلقة بالمستهلك ولا يجوز له التصرف بها. وتأكيداً على حماية البيانات الشخصية فقد فرضت المؤيدات القانونية بحق من ينتهك البيانات الشخصية للمستهلك. وتجدر الإشارة إلى أن حماية البيانات الشخصية ليس على عاتق

^١ المادة /٢٣/ من قانون المعاملات الإلكترونية رقم /٣/ لعام ٢٠١٤.

^٢ المادة /٢٣/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام

التاجر فحسب، حيث يلتزم المصرف أيضاً بحماية البيانات الشخصية للعملاء وعدم إفشائها (وقد سبق الإشارة إلى ذلك^١).

ج- الحق في العدول

يعتبر الحق في العدول من أكثر الوسائل حمايةً للمستهلك الإلكتروني، نظراً لأن المستهلك الإلكتروني لا تتوفر له الإمكانية الفعلية أو الحقيقية بمعاينة السلع أو التحقق من الأداء المناسب للخدمات. فحق العدول من الوسائل التي لجأت إليها التشريعات الحديثة لحماية رضاء المستهلك الإلكتروني، حيث يتضمن هذا الحق إعطاء فرصة للتروي والتفكير.

وفي سبيل التعرف على مضمون الحق في العدول لا بد من تعريفه وتحديد نطاقه وكيفية ممارسته بغية التعرف على آثاره وذلك على النحو الآتي:

أ-تعريف الحق في العدول:

يعد حق العدول في العقد الإلكتروني حق إرادي محض يترك تقديره للمستهلك وفقاً للضوابط القانونية. فهو حق شخصي يمارسه المستهلك وفقاً لما يراه محققاً لمصلحته.

وقد عرّف جانب من الفقه هذا الحق بأنه: «سلطة أحد المتعاقدين الانفراد بنقض العقد والتحلل منه دون توقف على إرادة ومشية الطرف الآخر»^(١).

^١ راجع ص ١٣٧ وما يليها.

في حين اتجه الفقه الفرنسي إلى تعريفه بأنه: «بمثابة الإعلان عن إرادة مضادة يعتزم من خلالها المتعاقد الرجوع عن إرادته وسحبها واعتبارها كأنها لم تكن وذلك بهدف تجريدها من أي أثر كان لها في الماضي أو سيكون لها في المستقبل»^(١).

نستنتج من التعاريف السابقة أنها بينت قدرة أحد المتعاقدين بعد إبرام العقد على المفاضلة أو الاختيار بين إتمامه أو الرجوع عنه، ويتميز تعريف الفقه الفرنسي بكونه أفضل من التعريف السابق كونه جاء محدداً لآثار ممارسة هذا الحق.

ونحن من جانبنا نعرف هذا الحق بأنه: «رخصة منحها المشرع للمستهلك باعتباره الطرف الضعيف يستطيع من خلالها أن ينقض قبوله في بعض العقود الإلكترونية دون الحاجة لتدخل الطرف الآخر أو تقديم أية مبررات»^(٢).

ب- نطاق الحق في العدول:

يرد الحق في العدول على العقود الصحيحة الملزمة لطرفي العقد الإلكتروني، وحيث أن عقود الاستهلاك الإلكترونية هي وسيلة المستهلك في الحصول على المنتجات والخدمات التي يرغب بها فلا شك أن نطاق العدول سوف ينصب على هذه العقود^(٣). وقد تبني المشرع السوري حق العدول للمستهلك بشكل قانوني. وحدد مدة ممارسة هذا الحق بمهلة عشرة أيام من تاريخ استلام البضائع أو

^(١) د. طارق كميل، مرجع سابق، ص ٧٦.

^(٢) مشار إليه لدى: إيناس بن غيده، مرجع سابق، ص ١١٥.

^(٣) المرجع السابق، ص ١١٦.

الاستفادة من الخدمة^١. وفيما يتعلق بمصاريف إعادة السلع تكون على نفقة البائع (التاجر) إذا أخل بالتزامه بالإعلام على النحو الذي بيناه سابقاً^٢ أما إذا أوفى بالتزاماته تكون المصاريف على نفقة المشتري (المستهلك)^٣. وقد اعتبر المشرع السوري أن الأحكام السابقة ليست من النظام العام وبالتالي يمكن الاتفاق على خلافها^٤. وتجدر الإشارة إلى أن المشرع السوري لم يطلق حق العدول في كافة العقود الإلكترونية، فهناك مجموعة من الحالات التي لا يمكن فيها للمستهلك ممارسة هذا الحق. حيث نص قانون المعاملات الإلكترونية:

(مع مراعاة المادة ١٧/ من هذا القانون لا يحق للمستهلك العدول عن الشراء في الحالات الآتية:

- ١- إذا استعمل السلعة أو استفاد من الخدمة مدة زمنية تتجاوز مدة التجربة المتفق عليها.
- ٢- إذا كانت السلع أو الخدمة أُعدت بمواصفات خاصة للمستهلك أو عُدلت بما يناسب طلبه.
- ٣- إذا قام المستهلك بنزع الأختام عن التسجيلات السمعية أو البصرية أو البرمجيات والمواد الإعلامية.
- ٤- في حالة شراء الصحف والمجلات والمنشورات والكتب.

^١ المادة (٢٠/أ) من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

^٢ راجع ص ١٨٩ وما يليها بهذا الخصوص.

^٣ المادة (٢٠/ب) من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

^٤ المادة (٢٠/ج) من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

٥- في حالة ظهور عيب في السلعة أو الخدمة نتيجة سوء استخدامها أو حفظها من قبل المستهلك.

٦- إذا كانت السلعة هي برمجيات محمّلة من الإنترنت إلا إذا وجد عيب فيها ولم يكن للمستهلك أي دور في ذلك^(١).

ج- كيفية ممارسة الحق في العدول:

على الرغم من أن حق العدول حق إرادي متروك لتقدير المستهلك إلا أن ممارسة هذا الحق تتطلب عدة شروط :

- يلتزم المستهلك بإخطار التاجر بأنه يرغب في العدول عن العقد ولا يشترط اتباع شكل خاص لهذا الإخطار ، فيجوز أن يكون بفاكس أو بريد إلكتروني أو في موقع التاجر أو برسالة موصى بها. ويفضل أن يتم الإخطار بأي وسيلة إلكترونية متوفرة ومن ثم يتم تأكيد الإخطار برسالة موصى بها وذلك خشية الوقوع في منازعة قانونية لاحقة مع التاجر إذا أنكر تبليغه بالعدول.
- يلتزم المستهلك أن يرد للتاجر البضاعة التي تسلمها بمقتضى العقد.
- ينبغي أن يتم العدول ضمن مهلة عشرة أيام عمل اعتباراً من تاريخ التسليم بالنسبة للبضائع ومن تاريخ الاستفادة بالنسبة للخدمات^٢.

^١ المادة (٢٢) من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

^٢ المادة (٢٠/ب) من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

د- آثار ممارسة الحق في العدول:

يترتب على ممارسة هذا الحق مجموعة من الآثار نجملها في الآتي:

بالنسبة للتاجر: إذا انقضت المدة المحددة للمستهلك لاستعمال حق العدول يصبح العقد ملزماً للطرفين وواجب التنفيذ، لكن إذا استعمل المستهلك هذا الحق خلال المدة المقررة قانوناً فإنه يترتب على ذلك التزام التاجر برد الثمن بمجرد استلام البضاعة من المستهلك وخلال مدة ٧/ أيام عمل كحد أقصى ما لم يتفق على خلافه^١.

بالنسبة للمستهلك: يعتبر حق العدول بالنسبة للمستهلك حق مجاني فإذا مارسه خلال المدة المحددة قانوناً، فلا يتحمل أي تبعات ولا يترتب عليه أي جزاء ما عدا المصاريف المتعلقة بإرجاع البضاعة طالما أن التاجر قد أوفى بالتزامه بالإعلام بالمعلومات المنصوص عليها في قانون المعاملات الإلكترونية. أما إذا أخل التاجر بالتزامه بالإعلام فتكون مصاريف إعادة البضائع على عاتقه. وطالما أن المستهلك استعمل حقه في العدول فمن الطبيعي أن يقوم بإعادة البضائع للتاجر.

بالنسبة للعقد الإلكتروني: يترتب على ممارسة حق العدول فسخ العقد وإعادة الأطراف إلى الحالة التي كانوا عليها قبل التعاقد.

^١ المادة ٢١/ من قانون المعاملات الإلكترونية رقم ٣/ لعام ٢٠١٤.

٢- الحماية المقررة بموجب اللائحة التنظيمية للضوابط الخاصة بحماية المستهلك الإلكتروني والتسويق الإلكتروني.

لقد أكدت هذه اللائحة على مجموعة من الوسائل والأساليب التي تشكل نوعاً من الحماية للمستهلك الإلكتروني في إطار العقود الإلكترونية وتتمثل هذه الحماية على النحو الآتي:

أ- الحماية في مواجهة الإعلانات المضللة.

لقد كرست هذه اللائحة سبل الحماية من الإعلانات المضللة من خلال مجموعة من الالتزامات والمحظورات التي تقع على عاتق صاحب الموقع الإلكتروني وتتمثل في الآتي:

أ- يلتزم صاحب الموقع بالإعلان عن مواصفات المنتج ونوعه وطريقة حفظه وتخزينه واستعماله ومدة صلاحيته المحددة بالمواصفات القياسية والقرارات الصادرة عن الوزارة إذا كانت طبيعة المنتج تتطلب ذلك^١.

ب- يحظر على صاحب الموقع:

- الإعلان عن إي منتج سام أو مغشوش أو فاسد أو ضار بالصحة أو منتهي الصلاحية أو مخالف للمواصفات المعتمدة.
- الإعلان عن بيع مواد أو أدوات أو سلع أو تقديم خدمات تستخدم للغش أو للتدليس.

^١ باختصار ينبغي أن يكون الإعلان واضحاً ومفصلاً باعتبار أن وضوح الإعلان الإلكتروني أحد القواعد الأساسية للحماية في مواجهة الإعلانات المضللة.

- المبالغة بوصف المنتج بما لا يتفق مع الحقيقة والواقع العملي بهدف تشجيع المستهلك على اقتناء المنتج أو تلقي الخدمة.
 - وضع أي دلالة أو إشارة تشير إلى تطبيق أحد أنظمة الجودة مالم يتم الحصول عليها من الجهة المخولة بمنحها (محلية عربية دولية).
 - استعمال أي إشارة أو علامة فارقة أو أي حق من حقوق الملكية التجارية والصناعية خلافاً لأحكام القوانين الخاصة بحماية الملكية النافذة على الموقع الإلكتروني ما لم يتم الحصول عليها من جهة مخولة بمنحها أصولاً.
 - استخدام طرق ترويج أو بيع أو شراء مخالفة للتشريعات كاستعمال أساليب توهم المستهلك بقرب نفاذ المنتج.
 - إبرام أي اتفاق أو ممارسة أي نشاط من شأنه الإخلال بحقوق المستهلك^١.
- ج- تقع على صاحب الموقع مسؤولية الإعلان عن سلع غير مطابقة للمواصفات تم إرسالها إلكترونياً من قبل أحد المنتجين أو الموردين مجهولي الهوية أو العنوان والتي تكون متداولة

^١ المادة ١٠/ من اللائحة التنظيمية للضوابط والنواظم الخاصة بحماية المستهلك الإلكتروني والتسويق الإلكتروني الصادرة بالقرار رقم ٤٧٩/ تاريخ ٢٠١٩/٢/١٧.

بشكل غير نظامي أو مهربة، كما يتحمل مسؤولية الضرر
الحاصل إذا لم يصرح عن عنوان ومكان منتجها الأصلي^١.

ب- الحماية المقررة للمستهلك أثناء تنفيذ العقد الإلكتروني.

وتتمثل هذه الحماية من خلال عدة نقاط:

أ- يقدم صاحب الموقع (منتج مستورد حلقات وساطة تجارية
بائع مفرق وكلاء توزيع مقدم خدمة) فاتورة نظامية للمشتري
(المستهلك) مهما كانت صفته يذكر فيها سعر المبيع والكمية
على أن تكون قابلة للحفظ والطباعة.

ب- في حال تعذر تسليم السلعة أو الخدمة في الزمان والمكان
المحددين لسبب قوة قاهرة يتم إشعار المستهلك بذلك ويحق له
استرجاع كامل المبلغ المدفوع كما يعفى البائع من تعويض
المستهلك لعدم تسليم السلعة أو الخدمة.

ج- يجب تطابق معلومات بطاقة بيان السلعة^٢ المعلن عنها
إلكترونياً مع بطاقة بيان السلعة المسلمة للمستهلك باللغة
العربية ويمكن استخدام لغات أخرى إلى جانب اللغة العربية^٣.

^١ المادة (١١/ب) من اللائحة التنظيمية للضوابط والنواظم الخاصة بحماية المستهلك الإلكتروني
والتسويق الإلكتروني الصادرة بالقرار رقم /٤٧٩/ تاريخ ٢٠١٩/٢/١٧.

^٢ يقصد ب بطاقة بيان السلعة: مجموعة البيانات والرموز الخطية وأي شيء تصويري أو
وصفي سواء كان مكتوباً أم مطبوعاً أم منقوشاً أم معلناً أم ملحفاً أم ملصقاً أم متضمناً أم تابعاً أم
مصاحباً لأي مادة (المادة الأولى من قانون التجارة الداخلية وحماية المستهلك رقم /١٤/ لعام
٢٠١٥).

^٣ المادة (١١/أ-ج-د-هـ) من اللائحة التنظيمية للضوابط والنواظم الخاصة بحماية المستهلك
الإلكتروني والتسويق الإلكتروني الصادرة بالقرار رقم /٤٧٩/ تاريخ ٢٠١٩/٢/١٧.

د-في حال وقوع أضرار شخصية للمستهلك نتيجة شراء منتج أو تلقي خدمة عن طريق إحدى الوسائل الإلكترونية تتم معالجة ذلك على النحو الآتي:

- يتم معالجة الموضوع بالاتفاق بين مسبب الضرر والمستهلك بشكل ودي وفق إحدى الحالات الآتية:
- ❖ التعويض على المستهلك.

- ❖ إعادة قيمة السلعة أو الخدمة التي تم استيفائها من المستهلك أو فرق القيمة في حال التراضي.
- ❖ استبدال السلعة أو إعادة تقديم الخدمة.

- في حال تعذر تطبيق الأساليب الثلاثة السابقة مباشرة بالاتفاق بين المستهلك ومسبب الضرر يتقدم المستهلك إلى الوزارة أو إلى إحدى مديرياتها في المحافظات بشكوى خطية أو إلكترونية أو هاتفية خلال ثلاثة أيام عمل كحد أقصى من وقوع الضرر ليتم تكليف الضابطة العدلية لمعالجة الموضوع وتحفظ الشكوى في حال المصالحة وتوقيع الطرفين على إلغاء الشكوى ومشاهدة الضابطة العدلية.

- في حال تعذر ذلك ينظم الضبط اللازم ويحال إلى القضاء أصولاً على أن يكون المستهلك قد تقيّد بالتعليمات الخاصة باستخدام السلع بما في ذلك الحفظ والتخزين^١.

^١ المادة ١٢/ من اللائحة التنظيمية للصوابط والنواظم الخاصة بحماية المستهلك الإلكتروني والتسويق الإلكتروني الصادرة بالقرار رقم ٤٧٩/ تاريخ ٢٠١٩/٢/١٧.

ثانياً: الحماية المقررة بموجب القوانين النازمة للمعاملات التقليدية

سوف نتحدث بدايةً عن الحماية المقررة للمستهلك الإلكتروني بموجب القانون المدني ثم ننتقل للحديث عن الحماية المقررة بموجب قانون التجارة الداخلية وحماية المستهلك.

١- الحماية المقررة للمستهلك الإلكتروني بموجب القانون المدني.

إن الحماية المقررة بموجب القانون المدني هي نوع من الدعاوى القضائية المقررة لحماية التعاقد الذي كثيراً ما يصيب إرادته مجموعة من العيوب التي تشوب رضاه أو قد تكون هذه العيوب متعلقة بالمنتج فيؤدي إلى ضياع حق التعاقد. لذلك فإن هذه الحماية ليست خاصة بالمستهلك إنما هي موجهة لأي متعاقد في ظروف معينة وفقاً للضوابط القانونية التي حددتها نصوص القانون المدني. ولكن حيث أن المستهلك الإلكتروني لا يختلف عن المستهلك التقليدي إلا من ناحية الوسيلة المستخدمة فكثيراً ما يتعرض لذات المشكلات، الأمر الذي استلزم معالجة هذه المشكلات في ضوء أحكام القانون المدني وتتمثل الحماية المقررة بموجب القانون المدني على النحو الآتي:

أ- الحماية بمواجهة الشروط التعسفية.

نص القانون المدني على أنه: ((إذا تم العقد بطريق الإذعان، وكان قد تضمن شروطاً تعسفية، جاز للقاضي أن يعدل هذه الشروط أو أن

يعفي الطرف المذعن منها، وذلك وفقاً لما تقضي به العدالة، ويقع باطلاً كل اتفاق على خلاف ذلك^(١).

كما نص ذات القانون على أنه:

(١) - يفسر الشك في مصلحة المدين.

٢- ومع ذلك، لا يجوز أن يكون تفسير العبارات الغامضة في عقود الإذعان ضاراً بمصلحة الطرف المذعن^(٢).

نستنتج من النصين السابقين أن المشرع السوري منح المستهلك الإلكتروني نوعاً من الحماية في مواجهة الشروط التعسفية، ولكن بشرط توافر الظروف والضوابط القانونية التي حددتها هذه المواد وتتمثل في الآتي:

بالنسبة للمادة /١٥٠/ تتمثل الضوابط في:

- أن يكون المستهلك الإلكتروني هو الطرف الضعيف المذعن.
- أن يكون العقد عقد إذعان: ونكون أمام عقد إذعان عندما يتعلق العقد بسلعة أو خدمة ضرورية، ويكون العقد بصيغة موحدة للجمهور كافة، كما ينبغي أن يكون هناك احتكار فعلي أو قانوني للسلعة مما يجعل من المنافسة محدودة بحيث لا يبقى للطرف الضعيف سوى القبول أو الرفض دون حق التعديل.

^١ المادة /١٥٠/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

^٢ المادة /١٥٢/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

- أن يتضمن العقد شروط تعسفية: ويتمثل معيار التعسف في اعتماد الطرف القوي على قوة نفوذه أو مركزه الاقتصادي بهدف الحصول على ميزة مجففة، وغالباً ما تتضمن عقود الإذعان شروط تعسفية.

فإذا ما توافرت الشروط السابقة فإن نص المادة /١٥٠/ يطبق على المستهلك الإلكتروني ويمنح الحماية المقررة في هذه المادة، والمتمثلة في أن يقوم القاضي بتعديل الشرط التعسفي أو إعفاء المستهلك من هذا الشرط على النحو الذي تقضي به قواعد العدالة والسلطة التقديرية للقاضي. وتجدر الإشارة إلى أن كل اتفاق على خلاف ذلك يعد باطلاً الأمر الذي يمنح حماية أخرى للمستهلك الإلكتروني.

أما بالنسبة للمادة ١٥٢ (١/١) فتتمثل الضوابط القانونية في:

- أن يكون المستهلك الإلكتروني هو الطرف المدين.
- أن تكون عبارات العقد تحوي نوع من الشك (عبارات غامضة).

أما بالنسبة للمادة (٢/١٥٢) فتتمثل الضوابط القانونية في:

- أن يكون المستهلك الإلكتروني هو الطرف الضعيف المذعن.
- أن يكون العقد قد تم بطريقة الإذعان على النحو الذي بيناه آنفاً.
- أن يحتوي العقد على عبارات غامضة.

وبناءً عليه إذا ما توافرت الضوابط القانونية السابقة فإن نص المادة /١٥٢/ يطبق على المستهلك الإلكتروني ويمنح الحماية المقررة في هذه المادة،

والمتمثلة في أن أي تفسير للعبارات الغامضة يكون لمصلحة المدين أو الطرف المُدَّعَن الأمر الذي يشكل نوع من الحماية المقررة للمستهلك الإلكتروني في مواجهة الشروط التعسفية. وبالنتيجة نجد أن الإعفاء من الشروط التعسفية أو تعديلها فضلاً عن تفسير الشك لمصلحة المدين هي نوع من أساليب الحماية المقررة للمستهلك الإلكتروني بمواجهة الشروط التعسفية وذلك إذا ما توافرت الضوابط التي حددتها النصوص القانونية.

ب-الحماية من عيوب الإرادة.

على الرغم من وجود عدة وسائل لحماية المستهلك إلا أننا نجد أن نظرية عيوب الإرادة تلعب دوراً مهماً في نطاق العقود الإلكترونية التي تتسم بالتعقيد التقني من حيث أساليب التعاقد ووسائله، أضف إلى ذلك أن الطرفين غير متكافئين على الصعيد التقني والاقتصادي مما يظهر الحاجة لإعمال عيوب الإرادة التي تتيح للمتعاقد إمكانية التمسك بإبطال العقد استناداً إلى وجود عيب في إرادته. كما أن عيوب الإرادة من السهل التمسك بها نظراً للالتزامات الكثيرة الملقاة على عاتق التاجر في هذه العقود^١. ويتصل إعمال عيوب الإرادة كوسيلة لحماية المستهلك اتصالاً وثيقاً بمدى تنفيذ التاجر لالتزامه بالإعلام لما له من تأثير على وجود رضا صحيح خال من العيوب، لأن المستهلك إذا ما قدمت له معلومات صحيحة وكافية حول المبيع أو الخدمات التي يريد التعاقد بشأنها، فإنه لن يقع في الغلط ولن يستطيع الطرف الآخر التغرير به. في حين أن عدم الالتزام بالإعلام قد يؤدي بالمستهلك إلى إبداء رضا معيب. وينبغي أن نشير إلى أن عيب الغلط وعيب التدليس من أكثر عيوب الإرادة حدوثاً في

^١ فلاح العجمي، مرجع سابق، ص ٨٩.

نطاق العقد الإلكتروني، أما بالنسبة للعيوب الأخرى (الإكراه - الغبن الاستغلالي) فهي نادرة الحدوث. حيث يعتبر الإكراه مستبعد من نطاق العقد الإلكتروني، لأن العقد الإلكتروني يتم بين طرفين يفصل بينهما مكان ويجمعهما مجلس عقد حكمي وليس حقيقي وبالتالي يكاد ينعدم الإكراه في هذه العقود. أما بالنسبة للغبن الاستغلالي فهو عيب استثنائي في نطاق العقود ونادر الحدوث في العقود الإلكترونية، كونه يتطلب استغلال الطيش البين أو الهوى الجامح وغالباً إذا ما حدث في نطاق العقود الإلكترونية يكون باستعمال أساليب وطرق احتيالية وبالتالي يمكن إبطال العقد لعلّة التدليس. ولعلّ أهم عييين يمكن ظهورهما في العقد الإلكتروني هما:

أ- عيب التدليس (التغريز):

تشكّل العقود الإلكترونية مجالاً واسعاً لإمكانية وقوع المستهلك ضحية التدليس، ولا سيما أن المستهلك يتعاقد عن بعد والسبيل الوحيد الذي يمكنه من معاينة السلعة هو مجرد صور وفيديوهات تشاهد على شاشة الكمبيوتر. حيث يعتبر تدليساً التحسينات التي يلجأ إليها المحترفون لترويج سلعهم عن طريق تغيير وتزييف صور سلعهم^١، وبالتالي يمكن للمستهلك إبطال العقد لعلّة التدليس إذا ما توافرت الشروط الآتية^٢:

- أن يكون المستهلك الإلكتروني هو الشخص المتعاقد الذي وقع ضحية التدليس.

^١ إيناس بن غيده، مرجع سابق، ص ٤٦.

^٢ المادتان (١٢٦، ١٢٧) من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

- استعمال طرق احتيالية سواء بارتكاب فعل أم بالسكوت عن واقعة وأثبت المستهلك أنه لم يكن ليتعاقد لو علم بتلك الواقعة التي سكّت عنها عمداً.
- أن يكون التدليس هو الدافع الرئيس للتعاقد من جانب الطرف المدلس عليه.
- صدور التدليس من المتعاقد أو حتى من قبل الغير إذا كان المتعاقد عالماً به أو كان من المفروض حتماً العلم به.

ب- عيب الغلط:

إن عيب الغلط أمر متصور الحدوث وخصوصاً في نطاق العقود الإلكترونية. فقد يتوهم أحد المتعاقدين بأن الطرف الآخر معروف لديه لكن يكتشف بعد ذلك بأن الشخص غير معروف وذلك إما لتشابه الأسماء أو تشابه موقع الويب الذي يعرض السلعة نفسها. والغلط المقصود في العقد الإلكتروني هو الغلط الذي لا يؤثر في وجود الإرادة إنما يعيبها فقط. وبالتالي يمكن للمتعاقد أن يتمسك بإبطال العقد لوجود الغلط إذا ما توافرت الشروط الآتية^١:

- أن يكون المستهلك الإلكتروني هو الشخص المتعاقد الذي وقع في الغلط
- أن يكون الغلط جوهري: سواء أكان الغلط جسيماً أم يتعلق بشخص المتعاقد أو صفته أم يتعلق بصفة جهرية للشيء وذلك إذا كان شخص المتعاقد أو صفته أو صفة الشيء محل اعتبار بالنسبة للمتعاقد بحيث لولاها ما أتم التعاقد ومثال ذلك:

^١ المادتان (١٢١، ١٢٢) من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

❖ كأن يتعاقد المستهلك من أجل الحصول على برنامج لحاسبه الآلي معتقداً أنه مناسب له غير أنه يكتشف بعد ذلك عدم ملائمة البرنامج للوفاء بالغرض المطلوب.

❖ كأن يقوم المستهلك بالتعاقد مع شخص آخر لرسم لوحة زيتية باعتبار هذا الشخص فنان عالمي ليتضح فيما بعد أن هذا المتعاقد ما هو إلا مبتدئ .

❖ كأن يدخل المستهلك إلى موقع إلكتروني شبيه بموقع رسمي يتعامل معه ويقوم بإبرام عقد مع شخص متوهم بأنه شخص رسمي معترف به ليتضح فيما بعد أن هذا الشخص ليس هو الشخص الرسمي المعترف به وأنه لم يكن ليتعاقد لو علم بذلك.

• أن يكون المتعاقد الآخر قد وقع في نفس الغلط أو كان على علم بهذا الغلط أو من السهل أن يتبينه.

فإذا ما توافرت الشروط المذكورة فإنه يجوز إبطال العقد لعلّة الغلط ولكن تجدر الإشارة إلى أنه لا يجوز التمسك بالغلط بما يخالف مبدأ حسن النية، حيث يبقى الشخص المتعاقد الذي وقع في الغلط ملزماً بالعقد الذي قصد إبرامه طالما أن الطرف الآخر أظهر استعداداً لتنفيذ العقد^١.

وبالنتيجة يمكننا القول إن دعوى إبطال العقد لعلّة التدليس أو الغلط تشكل أحد أساليب حماية المستهلك الإلكتروني من عيوب الإرادة، ولكن يبقى تطبيق هذه الأحكام مرهون بتوافر الشروط والضوابط القانونية التي أشارت إليها نصوص القانون المدني.

^١ المادة/١٢٥/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

ج-ضمان العيوب الخفية

يعد الالتزام بضمان العيوب الخفية من أهم الالتزامات التي تقع على عاتق التاجر، فالمستهلك الذي يتعاقد إلكترونياً مع التاجر من أجل شراء المنتج يفترض أنه خال من العيوب وصالح للغرض الذي اشتراه من أجله على نحو يمكنه من الانتفاع به، بحيث لو كان يعلم أن المبيع به عيوب تنقص من الانتفاع به لما أقدم على شرائه. وبالتالي فإن ضمان العيوب الخفية يعد وسيلة في يد المستهلك لإلزام التاجر على تسليم المبيع مطابق للمواصفات التي تم الاتفاق عليها والتي تفرضها الأعراف وطبيعة التعامل. ولكي يكون من حق المستهلك ضمان العيوب الخفية ينبغي توفر شروط معينة في العيب، كما أنه لا بد من مراعاة مدة محددة للضمان وهذا ما سوف نتحدث عنه على التوالي:

أ- شروط رفع دعوى الضمان

حتى يلتزم التاجر بضمان العيوب الخفية ينبغي توفر عدة شروط تتمثل في الآتي:

- أن يكون المستهلك الإلكتروني هو المتعاقد الذي اشترى المبيع المعيب من التاجر حتى يستفيد من الضمان في نطاق العقود الإلكترونية.
- أن يكون العيب مؤثراً: وذلك إذا لم يشتمل المبيع على الصفات التي تعهد التاجر بوجودها وقت التسليم إلى المستهلك أو إذا كان بالمبيع عيب ينقص من قيمته لدرجة أن المستهلك ما كان ليتعاقد مع التاجر لو علم بهذه العيوب^١.

^١ المادة (٤١٥ / ١) من القانون المدني رقم ٨٤ / لعام ١٩٤٩.

• أن يكون العيب خفياً: لا يضمن التاجر العيب إذا كان ظاهراً، كما أن العيب لا يكون خفياً إذا كان بإمكان المستهلك لو بذل عناية الرجل المعتاد أن يتبين العيب الموجود أو كان المستهلك عالماً بوجود هذا العيب، ما لم يثبت المستهلك أن التاجر أكد له خلو المبيع من العيب أو تعمد إخفاء العيب غشاً منه^١.

• أن يكون العيب قديماً: فالتاجر يضمن العيب الموجود وقت العقد والذي ينشأ بعد العقد وقبل التسليم أمّا العيب الذي طرأ على المبيع بعد التسليم فلا يضمنه التاجر^٢.

ب- ميعاد دعوى الضمان:

يجب على المستهلك بمجرد تسلمه للمبيع أن يفحصه وأن يخطر التاجر بما فيه من عيوب وعليه أن يخطره خلال مدة معقولة وإلا اعتبر قابلاً للمبيع بما فيه من عيوب^٣. وقد حدد المشرع السوري ميعاد دعوى الضمان بمدة سنة من تاريخ التسليم وليس من تاريخ اكتشاف العيب، فإذا اكتشف المستهلك العيب بعد انقضاء مدة سنة فلا يجوز له رفع دعوى الضمان إلا إذا اثبت أن التاجر أخفى العيب غشاً منه أو في حالة التزام التاجر بالضمان لمدة أطول^٤. وتجدر الإشارة إلى أنه يجب على المستهلك أن يعلم التاجر بالعيب خلال شهر من

^١ المادة (٤١٥/ ٢) من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٢ المادة/٤١٧/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٣ المادة/٤١٧/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٤ المادة/٤٢٠/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

ظهوره وأن يرفع الدعوى خلال ستة أشهر من يوم الإخطار إلا إذا كان هناك اتفاق يقضي بخلاف ذلك^١.

ج- المؤيد القانوني للضمان:

إذا وجد العيب الخفي وتحققت الشروط المذكورة آنفاً، وتفيد المستهلك بالمهل المحددة فإن التاجر يلزم بالضمان. وقد منح المشرع السوري المستهلك أحد خيارين بخصوص التعويض عن العيوب الخفية:

- إذا استحق بعض المبيع أو كانت خسارة المستهلك من جراء العيب جسيمة بحيث لو علم بها لما أتم العقد^٢. كان له حق المطالبة ب:

- قيمة المبيع وقت الاستحقاق.
- الفوائد القانونية من وقت الاستحقاق.
- قيمة الثمار التي ألزم المستهلك بردها لمن استحق المبيع.
- المصروفات النافعة التي لا يستطيع المستهلك أن يلزم بها المستحق.
- المصروفات الكمالية إذا كان التاجر سيء النية.
- مصروفات دعوى الضمان باستثناء ما كان بمقدور المستهلك اتقائها فيما لو أخطر التاجر.
- تعويض المستهلك عما لحق من خسارة أوقاته من كسب ويلزم المستهلك في هذه الحالة برد المبيع للتاجر مع جميع فوائده^٣.

^١ المادة/٤٢٣/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

^٢ المادة(٤١٢/٢) من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

^٣ المادة/٤١١/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

- إذا كانت الخسارة التي لحقت بالمستهلك ليست جسيمة أو قرر الاحتفاظ بالمبيع ففي هذه الحالة يقتصر حق المستهلك على المطالبة بتعويض عادل عما أصابه من ضرر^١.

د- ضمان التعرض والاستحقاق

يستفيد المستهلك الذي يتعاقد عبر الإنترنت مما هو مقرر بشأن البيع عموماً، حيث يلتزم التاجر بتمكين المستهلك من الانتفاع بالمبيع فلا يتعرض له شخصياً ولا يسمح للغير بالتعرض له أيضاً. وفي سبيل التعرف على هذا الضمان سوف نتحدث عنه على النحو الآتي:

أ- ضمان التعرض الشخصي:

يلتزم التاجر بعدم التعرض الشخصي للمستهلك، ويمكن أن يكون التعرض مادياً أو قانونياً، ومن صور التعرض الصادر عن التاجر عبر الشبكة:

- قيام مصمم برنامج الكمبيوتر المتعاقد على شرائه بإتلافه بعد تمام عملية البيع من خلال فيروس معين قام المصمم بزرعه داخل البرنامج المبيع.
- قيام التاجر المتعهد بتوريد خدمات معينة كخدمة الاشتراك في الإنترنت لأحد المستهلكين بسعر معين ثم يقوم بالتعاقد مع مستهلك آخر منافس الأول على إمداده بنفس الشيء ولكن بسعر منخفض وجودة أعلى^٢.

^١ المادة (١/٤١٢) من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٢ سهام إمدالو و ليلي حسن، مرجع سابق، ص ٤٤.

ب-ضمان التعرض الصادر من الغير:

لا يلتزم التاجر بضمان التعرض الذي يصدر من قبله فقط بل يلتزم بضمان التعرض القانوني فقط الصادر من الغير، ويكون التاجر ملزماً بالضمان ولو كان الأجنبي قد ثبت حقه بعد البيع طالما أن هذا الحق قد آل إليه من التاجر نفسه^١. ومن صور التعرض القانوني من قبل الغير عبر الشبكة^٢:

- في حالة شراء شخص لوحة فنية محملة برهن متنازع عليه بين التاجر وصاحب الرهن.
- حالة شراء براءة اختراع متنازع على تسجيلها بين التاجر والمخترع.
- حالة شراء برنامج للحاسوب لم يكن للتاجر سوى حق استعماله دون استغلاله.

ج-المؤيد القانوني للضمان:

ينبغي أن نشير بدايةً إلى أنه إذا أخطر التاجر بدعوى الاستحقاق الصادرة عن الغير وتدخل في الدعوى وتمكن من رد التعرض الصادر من قبل الغير يكون في هذه الحالة قد نفذ التزامه عينياً. أما إذا استحق المبيع للغير نتيجة عجز التاجر عن رد التعرض الصادر من قبل الغير فإنه يلتزم بالتعويض، والتعويض الذي يمنح للمستهلك من جراء الاستحقاق يختلف حسب نوع الاستحقاق:

^١ المادة/٤٠٧/ من القانون المدني رقم /٨٤/ لعام ١٩٤٩.

^٢ عبد الله محمود، مرجع سابق، ص ١١٧.

• إذا كان استحقاق المبيع كلياً أو إذا كانت خسارة المستهلك من جراء الاستحقاق جسيمة بحيث لو علم بها لما أتم العقد، كان للمستهلك المطالبة بـ:

- قيمة المبيع وقت الاستحقاق
- الفوائد القانونية من وقت الاستحقاق.
- قيمة الثمار التي ألزم المستهلك بردها لمن استحق المبيع.
- المصروفات النافعة التي لا يستطيع المستهلك أن يلزم بها المستحق.
- المصروفات الكمالية إذا كان التاجر سيء النية.
- مصروفات دعوى الضمان باستثناء ما كان بمقدور المستهلك اتقائها فيما لو أخطر التاجر.
- تعويض المستهلك عما لحق من خسارة أو فاته من كسب.
- إذا كانت الخسارة التي لحقت المستهلك ليست جسيمة أو كان الاستحقاق جزئي جار للمستهلك الاحتفاظ بالمبيع مع المطالبة بتعويض عادل عما أصابه من ضرر^١.
- إذا تمكن المستهلك من انتقاء استحقاق المبيع كله أو بعضه يدفع مبلغ من النقود أو بأداء شيء آخر للغير، كان للمستهلك العودة على التاجر بقيمة ما أداه مع الفوائد القانونية وذلك بمقابل تخلص التاجر من نتائج الضمان^٢.

وبالنتيجة يمكننا القول إن معالجة مشكلات العيوب الخفية ومشكلات استحقاق المبيع أو التعرض للمستهلك يتم عن طريق تعويض

^١ المادة/٤١١/ والمادة/٤١٢/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

^٢ المادة/٤١٠/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

المستهلك عن الضرر الذي أصابه من جراء العيوب أو الاستحقاق، ويختلف التعويض باختلاف الضرر فيما لو كان جسيماً أو ليس جسيماً ولكن يبقى الحصول على هذا التعويض مرهون بإقامة دعوى الضمان وفقاً للشروط والضوابط التي حددتها نصوص القانون المدني السوري.

٢- الحماية المقررة بموجب قانون التجارة الداخلية وحماية المستهلك.

مع مراعاة المشكلات التي تواجه المستهلك الإلكتروني والتي سبق الحديث عنها من جهة، ومن خلال استقراء نصوص قانون التجارة الداخلية وحماية المستهلك من جهة أخرى. نجد أن المشرع السوري حظر وجرم الإعلانات المضللة والتي من شأنها أن تؤدي إلى خداع المستهلك الأمر الذي يفهم منه ضمناً ضرورة أن تكون الإعلانات التجارية التقليدية أو الإلكترونية واضحة ومفصلة لكافة مواصفات السلعة أو الخدمة. وبناءً عليه تقوم قواعد حماية المستهلك في مواجهة الإعلانات الإلكترونية على قاعدتين أساسيتين:

الأولى: اشتراط وضوح الإعلان الإلكتروني

ويقصد بوضوح الإعلان الإلكتروني أن يتضمن الإعلان البيانات الكافية عن السلعة أو الخدمة المقدمة والتي من شأنها خلق تفكير واع متبصر يعمل على تكوين إرادة مستنيرة لدى المستهلك وهو بصدد الإقبال على التعاقد^١. حيث يجب في الإعلان الإلكتروني أن يكون واضح وغير غامض بحيث يتم تزويد المستهلك بمعلومات واضحة عن المنتج أو الخدمة المعروضة بما يسمح للمستهلك بإعطاء الموافقة

^١ د. طارق كميل، مرجع سابق، ص ٦٩.

على العقد عن وعي وإدراك كاملين. وتجدر الإشارة إلى أن المشرع السوري في قانون التجارة الداخلية وحماية المستهلك لم ينص على هذه القاعدة بشكل صريح إنما أشار إلى ذلك بشكل ضمني من خلال:

- حظر الإعلانات المضللة بأي وسيلة^١، وفرض المؤيدات الجزائية بحق من ينشرها^٢.
- اعتبار اللغة العربية هي الأساس في الإعلان عن المعلومات والبيانات^٣ وفرض المؤيدات الجزائية بحق من يستخدم غير اللغة العربية في الإعلان^٤.

الثانية: منع الإعلان الإلكتروني المضلل

يعد الإعلان الإلكتروني المضلل جريمة في حال توفر عنصرين اثنين:

العنصر المادي: يتكون من وسيلة دعائية وهي عبارة عن شبكة الإنترنت أو بعض الوسائل الأخرى كالهواتف النقالة والتلفاز، حيث يمكن أن تستخدم هذه الوسائل بطريقة احتيالية تضلل المستهلك وتوقعه في الغلط. كذلك يجب أن يتضمن العنصر المادي وجود معلومات مضللة أو كاذبة من شأنها إيقاع المستهلك في الغلط، وأن

^١ المادتان / ٢٢-٥٤/ من قانون التجارة الداخلية وحماية المستهلك رقم / ١٤/ لعام ٢٠١٥.

^٢ المادتان (٣٣/ب-٣٤) من قانون التجارة الداخلية وحماية المستهلك رقم / ١٤/ لعام ٢٠١٥.

^٣ المادة / ٥٣/ من قانون التجارة الداخلية وحماية المستهلك رقم / ١٤/ لعام ٢٠١٥.

^٤ المادة (٣٣/أ) من قانون التجارة الداخلية وحماية المستهلك رقم / ١٤/ لعام ٢٠١٥.

تكون المعلومات المضللة التي توقع في الغلط أحد العناصر الأساسية المكونة للسلعة أو الخدمة.

- **العنصر المعنوي:** ويتمثل هذا العنصر بالقصد الجرمي الذي هو أساس المسؤولية الجزائية، أي أن يكون القصد من وراء الإعلان المضلل هو خداع وتضليل المستهلك بهدف تحقيق غايات غير مشروعة^١.

وقد عالج المشرع السوري الإعلان المضلل من خلال مجموعة من المواد القانونية التي وردت في قانون التجارة الداخلية وحماية المستهلك وذلك على النحو الآتي:

- جاءت نصوص قانون التجارة الداخلية وحماية المستهلك بصيغة عامة وبغض النظر عن الوسيلة المستخدمة في الإعلان، الأمر الذي من شأنه أن يسمح بتطبيق هذه المواد على الإعلانات التقليدية والإلكترونية طالما أنها تحمل نوع من التضليل والخداع للمستهلك.
- حظر المشرع السوري الإعلان أو الترويج لمنتجات تحمل رموز أو أشكالاً غير مطابقة لواقع المنتج بالنسبة لمتطلبات جودته وكيفية استعماله وطرق تصنيعه وصفاته الجوهرية... الخ، والتي من شأنها أن تؤدي إلى الخداع أو التضليل وبغض النظر عن الوسيلة المستخدمة في الإعلان^٢.

^١ فلاح العجمي، مرجع سابق، ص ٦٧.

^٢ المادتان / ٢٢-٥٤/ من قانون التجارة الداخلية وحماية المستهلك رقم / ١٤/ لعام ٢٠١٥.

- عاقب المشرع السوري بالحبس مدة لا تقل عن ثلاثة أشهر وغرامة مالية من مئة ألف ليرة سورية إلى ثلاثمائة ألف ليرة سورية أو بإحدى هاتين العقوبتين ويُحكم بإغلاق المحل أو المنشأة كل من خدع المتعاقد معه بالنسبة لمتطلبات جودة المنتج وطرق تصنيعه وكيفية استعماله وبغض النظر عن الوسيلة المستخدمة في التضليل.^١
- عاقب المشرع السوري بالحبس من شهرين إلى سنة وبغرامة مالية من خمس وعشرين ألف ليرة سورية إلى خمسين ألف ليرة سورية أو بإحدى هاتين العقوبتين كل من يستخدم غير اللغة العربية في الإعلان عن المعلومات أو يصف أو يروج للمنتج بغير الحقيقة التي تعبر عن جوهره.^٢

وبالنتيجة يمكننا القول أن المؤيدات الجزائية المفروضة بموجب نصوص قانون التجارة الداخلية وحماية المستهلك شكاك الوسيلة الفعالة لحماية المستهلك الإلكتروني من الإعلانات المضللة عبر شبكة الإنترنت، وذلك نظراً لما يكتنف هذه الإعلانات من طابع جرمي من جهة ولخطورة هذه الإعلانات على ثقة المستهلك بالتعاملات الإلكترونية من جهة أخرى. وبالتالي يمكن للمستهلك إذا ما أصابه ضرر من جراء الإعلان أن يلجأ إلى القضاء وتفرض بحق المخالف العقوبات السالفة الذكر، كما تجدر الإشارة إلى أن الإعلان المضلل يشكل نوع من التدليس وبالتالي إذا ما

^١ المادتان (٣٣/ب-٣٤) من قانون التجارة الداخلية وحماية المستهلك رقم ١٤/ لعام ٢٠١٥.

^٢ المادتان (٣٣/أ-٥٣) من قانون التجارة الداخلية وحماية المستهلك رقم ١٤/ لعام ٢٠١٥.

توافرت شروطه فبإمكان المستهلك طلب إبطال العقد لعلّة التدليس.

وفي ختام الحديث عن الحماية المقررة للمستهلك الإلكتروني نجد أن المشرع السوري عمل على إحاطة المستهلك بسيّاح من الحماية من خلال مجموعة من الالتزامات القانونية المفروضة على عاتق التاجر، حيث تعد هذه الالتزامات بمثابة حقوق للمستهلك تسهم في وضع حد لأي مشكلة تواجه المستهلك في نطاق التعاملات الإلكترونية.

ولكن نأمل من المشرع السوري أن يلجأ إلى تنظيم قواعد الحماية المنصوص عليها في القانون المدني ضمن نطاق قانون المعاملات الإلكترونية وذلك بهدف جعل هذه القواعد المقررة لحماية المستهلك الإلكتروني باعتباره مستهلك وليس باعتباره متعاقد، حيث أنه إذا لم تتوافر الضوابط القانونية المنصوص عليها في هذه المواد فإنها لا تطبق على المستهلك وبالتالي يفقد الحماية المقررة بموجبها.

وبعد أن تعرفنا على أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع ننتقل للحديث عن أساليب معالجة المشكلات التي تواجه الاقتصاد الوطني.

المبحث الثاني

أساليب معالجة المشكلات التي تواجه الاقتصاد الوطني

نظراً للطبيعة الخاصة للمشكلات التي تواجه الاقتصاد الوطني من جهة، ولما تمثله هذه المشكلات من خطورة على المجتمع ككل وليس على شخص واحد من جهة أخرى. لذلك فقد كانت أساليب معالجة هذه المشكلات متنوعة ومختلفة بحيث تُعالج كل مشكلة بأسلوب:

فالنسبة لمشكلة التهرب الضريبي إن محور الانطلاق في معالجتها يقوم على البحث عن أساليب تقنية بهدف فرض الضريبة وتحصيلها على التجارة الإلكترونية والدفع الإلكتروني جزء منها.

أما بالنسبة لمشكلة غسيل الأموال فقد كانت موضع اهتمام على المستوى الدولي وعلى مستوى التشريع السوري الذي فرض مسؤولية جزائية قاسية بحق مرتكب هذا الجرم.

وبالتالي وبالرغم من أن كلا المشكلتين تواجه الاقتصاد الوطني إلا أن جوهر الخلاف بينهما يتمحور حول طبيعة وسائل معالجة هذه المشكلات، فمشكلة التهرب الضريبي معظم وسائل معالجتها عبارة عن اقتراحات وفرضيات لم تنظم بموجب نصوص قانونية وبالتالي تقبل المناقشة والجدل بشكل مستمر، أما بالنسبة لمشكلة غسيل الأموال فأسلوب معالجتها هو عبارة عن مجموعة من الالتزامات القانونية فُرضت على الصعيد الدولي على عاتق المصارف فضلاً عن ترتيب مسؤولية جزائية بموجب نصوص قانونية صريحة لا تقبل الشك على صعيد التشريع السوري.

وبناءً عليه وفي سبيل التعرف على أساليب معالجة المشكلات التي تواجه الاقتصاد الوطني سوف نتحدث عن وسائل معالجة التهرب الضريبي في المطلب الأول، ثم نتعرف على وسائل معالجة غسل الأموال وذلك في المطلب الثاني.

المطلب الأول

وسائل معالجة مشكلة التهرب الضريبي باستخدام وسائل الدفع

الإلكتروني

في ظل التحديات والمشكلات التي تنتاب مسألة فرض الضريبة على معاملات الدفع الإلكتروني، تبرز الحاجة الملحة للبحث عن الحلول القانونية الكفيلة بمعالجة هذه المشكلة أو التخفيف منها على أقل تقدير. وحيث أن معظم المشكلات المتعلقة بالتهرب الضريبي في نطاق الدفع الإلكتروني تندرج تحت أحد بندين إمّا تحديات تتعلق بكيفية فرض الضريبة أو تحديات تتعلق بكيفية تحصيل الضريبة لذلك فقد تنوعت أساليب معالجة هذه المشكلة في ناحيتين:

الناحية الأولى: معالجة المشكلة المتعلقة بكيفية فرض الضريبة وهي مجال بحثنا في الفرع الأول.

الناحية الثانية: معالجة المشكلة المتعلقة بكيفية تحصيل الضريبة وهي مدار بحثنا في الفرع الثاني.

الفرع الأول

معالجة المشكلة المتعلقة بكيفية فرض الضريبة

في ظل التحول المتسارع نحو عالم الأعمال الإلكترونية، شرعت السلطات الحكومية في العديد من الدول إلى التفكير في إمكانية تطبيق القواعد الضريبية التقليدية على التعاملات الإلكترونية مع ضرورة إيجاد أساليب جديدة تواكب هذا النوع من المعاملات، واقتُرحت في هذا المجال فرض ضريبة على الاستهلاك بدلاً من فرضها على الوحدات الإنتاجية، وتطبيق ضريبة البيت إضافة إلى محاولة تصور إطار عام للضرائب في عالم المعاملات الإلكترونية وذلك على النحو الآتي:

أولاً: فرض ضريبة على الاستهلاك

يهدف هذا المقترح إلى التحول من فرض الضريبة على الدخل إلى فرض الضريبة على الاستهلاك، وذلك باعتبار أن الاستهلاك منخفض المرونة ويصعب إخفاؤه، وتساعد هذه الضريبة في جمع الضرائب من المتهربين من دفعها بما في ذلك أولئك الذين يحققون دخول مرتفعة من معاملات الدفع الإلكتروني^١. وترى منظمة التعاون والتنمية الاقتصادية (OCDE) أن فرض الضرائب على معاملات الدفع الإلكتروني ينبغي أن يستند إلى مبدأ الشفافية واليقين والكفاءة وعدم التمييز. حيث يوجد توافق دولي على أن قواعد فرض ضرائب الاستهلاك على معاملات الدفع الإلكتروني ينبغي أن تطبق في الولاية

^١ مشار إليه لدى: د. رأفت رضوان و رشا عوض و ولاء الحسيني، مرجع سابق، ص ١٥.

التي يتم فيها الاستهلاك، وهناك آليات قائمة ومعروفة لسلطات الضرائب من أجل مراقبة وجباية ضرائب الاستهلاك المتعلقة بالمنتجات المادية حتى عندما تباع عبر الحدود^١.

ولكن ينتقد هذا المقترح لكون هناك صعوبة في تتبع معاملات الدفع الإلكتروني وخصوصاً بالنسبة للمنتجات الرقمية (غير مادية)، فضلاً عن التخوف من مسألة المساس بالبيانات الشخصية للمستهلكين، كذلك فإن من شأن فرض هذه الضريبة أن تزيد الأعباء الملقاة على عاتق المستهلكين فبالإضافة إلى ثمن السلع سوف يدفعون الضرائب الأمر الذي من شأنه أن يعرقل نمو عملية الدفع الإلكتروني.

ثانياً: تطبيق ضريبة البيت (Bit – tax)

لعلّ أحد الحلول المقترحة لتنظيم معاملات الدفع الإلكتروني من الناحية الضريبية هو ضريبة البيت، حيث يتم تحصيل هذه الضريبة على أساس كمية البيت الرقمية التي يمكن استخدامها أو نقلها. وقد ظهرت ضريبة البيت منذ ١٩٩٤ و تحسب على أساس كثافة التحويل الإلكتروني للمعلومات من خلال عدد البيت المستعملة^٢. وقد نبعت الفكرة من الأهمية القصوى التي تحتلها المعلومات و البيانات في عالم اليوم حيث تعد دعامة البيئة الجديدة، فانتقال و تبادل المعلومات هو النشاط الرئيس في عملية الدفع الإلكتروني. وقد وجهت لهذه

^١ مشار إليه لدى د. علي عزوز، مرجع سابق، ص ٧٨.

^٢ المرجع السابق، ص ٧٩.

الفكرة العديد من الانتقادات^١ حيث أن فرض هذه الضريبة سينطوي عليه العديد من المشكلات، فقد ينطوي تحديد قيمة الضريبة على أساس كمية البيت المنقولة على نوع من الخداع، حيث قد تكون السلعة أو الخدمة المنقولة مؤلفة من عدد معين من البيت و بالتالي يتم فرض ضريبة منخفضة، وفي الوقت نفسه قد تكون قيمة بيع هذه السلعة أو الخدمة مرتفعة. وقد يكون الأمر مختلفاً عندما تتكون السلعة من عدد كبير من البيت و بالتالي يتم فرض ضريبة مرتفعة وفي الوقت نفسه تكون قيمة بيع هذه السلعة منخفضة. لذلك لابد من تطوير المقترح و اقتصار عملية الانتقال على نوع معين من السلع يتطلب عدد صغير من البيت و لكن قيمة بيعه مرتفعة.

ونحن من جانبنا لا نتفق مع الانتقادات التي وجهت لضريبة البيت حيث أنه ليس هناك مبرر لاقتصار هذه الضريبة على حالة معينة (حالة السلعة تتطلب عدد قليل من البيت في حين قيمة بيعها مرتفعة)، وذلك لأن من شأن هذا الأمر أن يقف عائقاً أمام تطور عملية الدفع الإلكتروني. كما أن ضريبة البيت هي نوع جديد من الضرائب يلاءم التعاملات الإلكترونية، أما الاقتصار على حالة معينة فكأننا أمام فرض ضريبة تقليدية على أساس الربح وهذا الأمر لا يلاءم مع تطور عملية الدفع. ويضاف إلى ذلك صعوبة إيجاد وسائل وأساليب تمكن من معرفة الحالات التي تخضع للضريبة والحالات التي لا تخضع للضريبة وفقاً للاقتراح الذي نادى به المنتقدين لضريبة البيت (أي معرفة أن هذه السلعة تتطلب كمية قليلة من البيت

^١ د. لطيف زيود، تحديات التجارة الإلكترونية للنظم الضريبية، بحث منشور في مجلة جامعة تشرين للدراسات والبحوث العلمية، المجلد ٢٧، العدد ٣، اللاذقية، ٢٠٠٩، ص ٢٨.

في حين قيمة بيعها مرتفعة وبالتالي تخضع للضريبة أما السلعة التي تتطلب كمية كبيرة من البيت ولكن قيمة بيعها منخفضة لا تخضع للضريبة).

ثالثاً: الإطار العام المقترح لكيفية فرض الضريبة على تعاملات التجارة الإلكترونية

قبل الحديث عن الإطار العام لكيفية فرض الضريبة لابد من طرح التساؤل التالي:

على من تفرض الضريبة ؟ على الدافع أم على المستلم؟

في الحقيقة الضريبة هي اقتطاع مالي تقتطعه الدولة من الأفراد بمناسبة ممارستهم لأنشطة اقتصادية يترتب عليها ربح معين.

وبالتالي فإن الضريبة تفرض على مستلم المال وليس دافعه باعتباره حقق ربح معين وفي نطاق الدفع الإلكتروني فإن دافع المال هو المستهلك أما مستلمه فهو التاجر وبالتالي هو الشخص الذي تفرض عليه الضريبة.

وبالعودة للإطار العام المقترح لكيفية فرض الضريبة فإن هذا الإطار يتضمن العديد من الإطارات الفرعية وتشمل :

- ١-الإطار المفاهيمي: مما لا شك فيه أن هناك العديد من المفاهيم السائدة في عالم الضرائب تحتاج إلى إعادة مراجعة بصورة تحقق انسجام هذه المفاهيم مع المتغيرات التقنية ومثال ذلك :

- مفهوم الإقليمية: و يقصد به امتداد التواجد ليشمل مقر المعلومات على شبكة الإنترنت وليس قصرها على مفهوم التواجد المكاني.
 - مفهوم العدالة الضريبية: ويقصد به عدم وجود اختلاف في أسعار الحصول على السلع نتيجة اختلاف البيئة الذي يتم تسليمها من خلاله.
 - مفهوم السلع و الخدمات: هذه المفاهيم تحتاج إلى إعادة صياغة بما لا يفرق بين النشاط التقليدي والنشاط الإلكتروني، وبالتالي يمكن أن تكون السلع مادية أو في صورة رقمية كصورة فوتوغرافية فقد تسلم بصورة مادية أو كملف رقمي^١.
- ٢-الإطار التشريعي:** ويتطلب هذا الإطار ضرورة إقرار تشريعات جديدة أو تعديل التشريعات الحالية بما يلاءم مع المتغيرات التقنية في عالم الدفع الإلكتروني ومثال ذلك :
- إقرار العقود الإلكترونية: فمن خلال منح الحجية الكاملة للعقود الإلكترونية، يمكن و بشكل أسهل مراجعة هذه العقود والتعرف على مقدار الضريبة المفروضة وذلك على خلاف النظم الورقية.
 - إقرار التشريعات الخاصة بتأمين البيانات الإلكترونية من خلال عدة أساليب تقنية كالتوقيع الإلكتروني والتشفير^٢.

^١ د. علي عزوز، مرجع سابق، ص ٨١.

^٢ المرجع السابق، ص ٨١.

٣-الإطار التنفيذي: كان النظام الضريبي في بداياته يعتمد على قيام مأموري الضرائب بمراجعته القيود الدفترية الواردة في ميزانية الشركات وحساب الأرباح والخسائر على الوثائق الأصلية، لكن التحول إلى نظام القيد الإلكتروني والعقود الإلكترونية أوجب اقتراح نظام جديد للمراجعة و هو **نظام التحقق الإلكتروني** الذي يقوم على تبادل الرسائل الإلكترونية بين الشركة تحت الفحص الضريبي و الشركات المتعاملة معها بيعاً وشراءً بمعرفة مأمور الضرائب. وتتم آلية عمل نظام التحقق الإلكتروني على النحو الآتي^١:

يقوم مأمور الضرائب بمراجعة العقود الإلكترونية سواء بنظام المراجعة الحديثة أم التقليدية، وفي حال رغبة مأمور الضرائب في التحقق من صحة أحد العقود فإنه يقوم بالضغط على زر خاص ليتم إرسال رسالة إلى الشركة التي تم التعامل معها و تتضمن هذه الرسالة طلب إرسال نسخة من العقد كما هو مخزن لدى الشركة التي تم التعامل معها، ويكون الرد من حاسب الشركة المتعامل معها عن طريق إرسال نسخة من العقد ويتم المقارنة بين العقدين، و بناءً على المقارنة يمكن قبول أو رفض المعاملة.

٤-الإطار الإجرائي: دأبت العديد من الدول على تقسيم الأنشطة المرتبطة بتحصيل الضرائب بين عدة جهات كالجمارك وإدارة الضرائب فعلى سبيل المثال تقوم مصلحة الجمارك بتحصيل الضريبة على الواردات من المستوردين عند نقطة الفحص

^١ د. رأفت رضوان و رشا عوض و ولاء الحسيني، مرجع سابق، ص ١٩.

الجمركي. لكن مع انتشار الدفع الإلكتروني و إمكانية دخول سلع غير مادية دون العبور بالمنافذ الجمركية فإننا أمام حلين^١:

- إعفاء هذه السلع من الضريبة وهو ما يخل بمبدأ المساواة الضريبية.

- فرض ضرائب على هذه السلع من خلال إيجاد تقنيات حديثة لإخضاع معاملات الدفع الإلكتروني للضريبة وذلك بواسطة مؤسسات الرقابة والإشراف على استقبال وبث الإنترنت باعتبار أن الإنترنت هو العنصر الرئيس في معاملات الدفع الإلكتروني. ونحن من جانبنا نرى أنه حتى يتم فرض الضريبة على المعاملات الإلكترونية لابد من تأييد اثنين من المقترحات الثلاثة السالفة الذكر. ففي البداية نؤيد فكرة الإطار العام المقترح لفرض الضريبة وذلك على اعتبار أن هذا الإطار بإطاراته الفرعية الأربعة يشكل نوع من التعاون بين السلطة التشريعية(من خلال إقرار القوانين المتعلقة بالمعاملات الإلكترونية)والسلطة التنفيذية(من خلال إيجاد آليات للتحقق من المعاملات الإلكترونية) وبين أفراد المجتمع (من خلال نشر الوعي حول بعض المفاهيم التي أفرزتها الثورة التقنية)، الأمر الذي من شأنه أن يوفر البيئة المناسبة لتطور عملية الدفع الإلكتروني وبالتالي تقبل فكرة خضوع معاملات الدفع الإلكتروني للضريبة.

ثم تأتي المرحلة الثانية والتي من خلالها أيدنا مقترح تطبيق ضريبة البيت (Bit tax) باعتباره من أفضل الحلول لفرض الضريبة على انتقال السلع و الخدمات عبر وسائل الدفع الإلكتروني. حيث أن هذه السلع يتم تحويلها إلى كمية من البيت و بالتالي يمكن حصر العدد الفعلي من البيت

^١ المرجع السابق، ص ٢٠.

الذي تم نقله بواسطة أساليب تقنية ونقوم بفرض الضريبة عليه، الأمر الذي يشكل نوع من الرقابة على هذه الأنشطة من جهة و يسهم في تحقيق العدالة الضريبية من جهة أخرى. و بالتالي تكون ضريبة البيت شكلاً جديداً أفرزته الثورة التقنية في مجال المعلومات بهدف إخضاع معاملات الدفع الإلكتروني للضريبة.

الفرع الثاني

معالجة المشكلة المتعلقة بكيفية تحصيل الضريبة

لقد تداعى بعض الفقهاء لتقديم اقتراحات تتضمن وسائل بديلة للقيام بعملية التحصيل الضريبي بالنسبة لمعاملات الدفع الإلكتروني، ويمكن حصر هذه الوسائل في اقتراحين:

أولاً: التحصيل عن طريق أطراف ثالثة

يمكن وفقاً لهذا المقترح اعتماد أطراف ثالثة وموثوقة كمحصلين جدد لتسهيل عملية تحصيل الضريبة على معاملات الدفع الإلكتروني و يمكن أن تكون هذه الأطراف إما:

١- وسطاء ماليين: اتجه بعض الفقهاء^١ إلى إمكانية احتساب الضريبة واقتطاعها على معاملات الدفع الإلكتروني من خلال مؤسسات مالية موثوقة كالشركات العاملة في مجال الدفع الإلكتروني (الجهات المصدرة لوسائل الدفع الإلكتروني)، وذلك عند البيع وحسب نسبة الضريبة في بلد المستهلك أو التاجر. ولا شك أن مثل هذا الاقتراح سيتطلب من تلك الشركات الاحتفاظ

^١ مشار إليه لدى د. إبراهيم كامل الشوايكة، مرجع سابق، ص ٥٢٢.

بقاعدة بيانات ضريبية للدول المختلفة إضافة إلى تقديم التجار المعلومات الضرورية حول مبيعاتهم والأطراف المعنية بعملية البيع كأرقام الحسابات وقيمة المبيعات وعناوين الأطراف.

و نحن من جهتنا نرى أن هذا الاقتراح غير دقيق وذلك على اعتبار أن هذه الشركات هي أحد أطراف عملية الدفع الإلكتروني، وبالتالي ليس من المنطقي أن تقوم كجهة محصلة للضرائب وطرف في عملية الدفع في آن واحد. لأن من شأن إلقاء هذه المهمة عليها أن يفسح المجال أمام هذه الشركات لتقرير حقها في اقتضاء الرسوم على تقديم خدمات تحصيل الضريبة. إضافة إلى أن هذه الشركات غير جاهزة فنياً للتعامل مع هذا الكم الهائل من المعلومات الأمر الذي من شأنه أن يحملها المزيد من التكاليف لإنشاء النظام المناسب وإنجازه.

٢- مزود خدمات الإنترنت ISP: اقترح بعض الفقهاء إشراك مزودي خدمات الانترنت من الناحية الفنية في تتبع جميع معاملات الإنترنت لزبائنهم كطرف ثالث موثوق للقيام بعملية فرض وتحصيل الضريبة المقررة على المعاملات الإلكترونية. ومزود خدمات الإنترنت (Internet Service provider) يرمز له اختصاراً (ISP) : وهو الشركة التي توفر لعملائها إمكانية الوصول إلى شبكة الإنترنت مقابل رسوم. ويرتبط مزود خدمة الإنترنت بعملائه باستخدام تقنية نقل البيانات المناسبة لتوصيل حزم بيانات نظام الإنترنت، مثل الاتصال الهاتفي، خط المشترك، وكابل المودم، والأجهزة اللاسلكية، والوصلات

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٦٦.

المخصصة عالية السرعة^١.

وقد يواجه هذا المقترح صعوبة تتبع محطات الوصول والمنشأ الصحيح لمعاملات الدفع الإلكتروني. فعلى سبيل المثال من الممكن أن يشتري مستهلك أمريكي منتج رقمي في هولندا من خلال مزود إنترنت في المملكة المتحدة^٢. ولكن يمكن معالجة هذه المشكلة من خلال استخدام عناوين بروتوكول الإنترنت (Internet Protocol)^٣ التي تستخدم في نقل البيانات من نقطة لأخرى باعتبار أن هذه العناوين جزء أساسي لكل نقطة وصول للإنترنت.

ثانياً: التحصيل باستخدام أساليب تقنية

قدمت اللجنة الاستشارية الأمريكية الإلكترونية^٤ مجموعة من الاقتراحات تستند بشكل أساسي على الأساليب التقنية لحل مشكلات فرض و تحصيل

¹ Gerson & Ryan A Primer on Internet Exchange Points for Policymakers and Non-Engineers Working Paper, 11 August 2012,p12.

متاح على الرابط: www.Ar.wikipedia.org/wiki/

تاريخ الزيارة ٢٠١٨/١٠/٣١ الساعة ١٠,٣٠ a.m .

^٢ د. إبراهيم كامل الشوايكة، مرجع سابق، ص ٥٢٢.

^٣ (يرمز له اختصاراً: IP) هو بروتوكول الاتصال الأساسي في حزمة بروتوكولات الإنترنت ويُشكّل الأساس الذي تعتمد عليه عملية توجيه المعلومات ضمن الشبكة، ويسمح ذلك الاتصال بين الشبكات المختلفة. راجع الرابط: www.Ar.wikipedia.org/wiki/

تاريخ الزيارة ٢٠١٨/١٠/٣١ الساعة ١٠,٣٠ a.m

^٤ أنشئت هذه اللجنة بموجب قانون حرية ضريبة الإنترنت وقد تطلب هذا القانون حصول أي توصية مقدمة للكونغرس حول ضريبة على معاملات التجارة الإلكترونية على أصوات ثلثي

الضريبة على معاملات الدفع الإلكتروني، والفكرة المشتركة لهذه الاقتراحات هي أن البرامج التقنية الإلكترونية التي ستوجد قريباً ستدمج مع معاملات الدفع الإلكتروني لتقوم بتحصيل الضريبة و تحويلها للسلطات الضريبية^١. وقد رُوج لهذه المقترحات باعتبارها متواضعة التكلفة أو على الأقل ستكون محتملة من قبل السلطات الضريبية بدلاً من تحميل عملية التحصيل للتجار. والحقيقة أنه ولغاية الآن لم يظهر بشكل مؤكد أن هذه البرامج التقنية متوفرة لتحديد قيمة الضريبة وتحصيلها ومعالجة هذه الأمور في الوقت المناسب وبتكلفة معقولة، ولم يتم دمج أية برامج تقنية مع بطاقات الدفع الإلكتروني المعروفة حالياً بغية فرض الضريبة وتحصيلها على معاملات الدفع الإلكتروني.

وفي نهاية هذه المقترحات فإننا نؤيد مقترح أن يعهد بتحصيل الضريبة إلى مزود خدمات الانترنت ISP باعتباره طرف حيادي ومستقل عن عملية الدفع الإلكتروني، كما أنه الجهة الأقدر على فرض الضريبة و خصوصاً بعدما أيدنا مسبقاً مقترح تطبيق ضريبة البيت. فمزود خدمات الانترنت هو الجهة الأقدر وصاحب الاختصاص في معرفة كمية البيت المستخدمة و من شأن ذلك أن يقضي على ظاهرة التهرب الضريبي في نطاق معاملات الدفع الإلكتروني.

أعضاء هذه اللجنة. وتتكون هذه اللجنة من ١٩ عضواً يمثلون الولايات والتجار العاملين في التجارة الإلكترونية بنسبة ثمانية أعضاء لكل منهما وثلاثة أعضاء يمثلون الحكومة الاتحادية.

^١ راجع الرابط: www.thestc.com

المطلب الثاني

وسائل معالجة مشكلة غسيل الأموال باستخدام وسائل الدفع الإلكتروني

تتميز مشكلة غسيل الأموال باستخدام وسائل الدفع الإلكتروني عن غيرها من المشكلات بصعوبة الكشف عنها وملاحقة مقترفيها، ومرد ذلك إلى الطابع الدولي التي تنسم به من جهة، وحيل التمويل التي تتم من خلالها من جهة أخرى، مما جعلها خطراً يهدد الاستقرار المحلي والدولي. فقد أصبحت هذه المشكلة من أكبر التحديات التي تواجه المجتمع الدولي في إطار التصدي للجرائم ذات الطابع الدولي خاصة في ظل تطور الوسائل التي يستعملها ويستغلها المجرمون. وقد بُذلت الكثير من الجهود الدولية في محاولة الوصول إلى الوسائل التي يمكن أن تحد من هذه الظاهرة، كما اتجهت العديد من الدول إلى إصدار تشريعات خاصة بمكافحة هذه الجريمة. لذلك وفي سبيل تسليط الضوء على وسائل معالجة هذه المشكلة سوف نتحدث عن مكافحة غسيل الأموال على المستوى الدولي في الفرع الأول ثم ننتقل للحديث عن مكافحة غسيل الأموال لدى المشرع السوري في الفرع الثاني.

الفرع الأول

مكافحة غسيل الأموال على المستوى الدولي

هناك العديد من الجهود الدولية سواء على صعيد الأمم المتحدة أم على المستوى الإقليمي (الأوروبي أو العربي) بغية مكافحة غسيل الأموال، وقد توافقت معظم الوثائق الدولية الأساسية التي تعمل في

هذا الإطار على بلورة عدد من الالتزامات الوقائية التي أعدت بغية تعزيز التعاون الدولي في هذا المجال. وتتجلى هذه المكافحة من خلال مجموعة من المعايير والتوصيات. لذلك سوف نتحدث (أولاً) عن المعايير المعتمدة لمكافحة غسيل الأموال ثم ننتقل (ثانياً) للحديث عن التوصيات في هذا الخصوص.

أولاً: المعايير المعتمدة لمكافحة غسيل الأموال

ولعل أبرز الأسس التي قامت عليها هذه الجهود^١ هي:

١- محاصرة المناطق الأكثر نشاطاً في مجال غسيل الأموال، وهي مناطق مفتوحة لحركة الأموال مما يجعلها بيئة مناسبة لغاسلي الأموال الذين يستغلون العمل في هذه المناطق نظراً لما يتوفر لها من السرية المطلقة في المصارف وخصوصاً في ظل انعدام الرقابة. ومثال هذه المناطق (سويسرا - موناكو - لوكسمبورغ - سنغافورة - هونغ كونغ).

٢- التثبت من شخص المستخدم بين العالم الحقيقي والافتراضي، إذ يعد التثبت أهم عنصر من عناصر ضمان عدم الوقوع في أنشطة غسل الأموال الحديثة وأي تقصير في عملية التثبت من شأنه أن يساعد غاسلي الأموال على الإفلات من العقاب، وذلك على اعتبار

^١ الاتفاقية العربية لمكافحة غسل الأموال و تمويل الإرهاب المحررة بالقاهرة عام ٢٠١٠.

اتفاقية الأمم المتحدة لمكافحة الاتجار بالمخدرات و المؤثرات الدولية فينا ١٩٨٨.

معاهدة المجلس الأوروبي لعام ١٩٩٠.

اتفاقية إيربول لعام ١٩٩٥.

أن غياب المعلومات الشخصية اللازمة من شأنها أن تجعل أمر تتبع الفاعل ومصادر تمويل الأموال غير المشروعة أمر مستحيل^١.

٣- وضع رقابة صارمة على النظام المصرفي، لمنع استخدامه في عمليات غسل الأموال الحديثة تحت شعار **اعرف عميلك** وذلك بحصول الجهات المصدرة على كافة البيانات المتعلقة بالمتعامل و بالصفقة التي يجريها واتخاذ الإجراءات القانونية بحق الصفقات التي تزيد عن حد معين.

٣- ضرورة وجود تعاون دولي في مجال تبادل المعلومات و ضبط المجرمين وتسليمهم وغير ذلك من المسائل ذات الصلة بجريمة غسل الأموال. كما ينبغي تعزيز التعاون بين الجهات الرقابية المختصة على الصعيد الدولي أو المحلي و بين كافة الجهات المصدرة لكشف أي عملية يشتبه بأنها تجري لغرض غسل الأموال، وهذا التعاون يتضمن نوع من الرقابة على هذه الجهات من خلال فرض عدة التزامات ينبغي التقيد بها^٢.

ثانياً: التوصيات الصادرة بخصوص مكافحة غسل الأموال

توصلت لجنة العمل المعنية بالإجراءات المالية المتعلقة بمكافحة غسل الأموال بالوسائل الحديثة (**financial action task force**)

^١ حسام العبد ، مرجع سابق، ص ٢٤.

^٢ المرجع السابق، ص ٢٥.

(FATF)^١ إلى وضع أربعين توصية حول الإجراءات التي يجب اتباعها في مواجهة هذه المشكلة، ويمكن رد الأحكام التي تناولتها التوصيات الأربعون إلى ثلاثة مجالات^٢ تتمثل في الآتي:

١- تحسين الأنظمة القانونية لمكافحة غسيل الأموال: لا بد أن تتخذ الدول كافة الإجراءات التشريعية نحو تجريم أنشطة غسيل الأموال باستخدام وسائل الدفع الإلكتروني، وأن تأخذ بعين الاعتبار تكييف هذه الجريمة على أنها من الجرائم الخطيرة^٣. كما ينبغي أن تتبنى الدول مجموعة من الإجراءات عند اكتشاف أي عملية غسل للأموال باستخدام هذه الوسائل، ومن قبيل هذه الإجراءات:

- تنفيذ الإجراءات المؤقتة مثل التجميد و الضبط لمنع أي تصرف أو نقل الأموال المغسولة.
- العمل على مصادرة الممتلكات المغسولة أو عائداتها أو الوسائل المستخدمة في ارتكاب هذه الجريمة.
- اتخاذ أي إجراءات مناسبة خاصة بالتحري.

^١ تلزم هذه اللجنة ٢٦ دولة إضافة إلى منطمتين إقليميتين، راجع الرابط :

[www.moqatel.com/open share/Behoth/Ektesad8/Ghasl_Am](http://www.moqatel.com/open_share/Behoth/Ektesad8/Ghasl_Am)

.wal/secl7/doic.cvt.htm

تاريخ الزيارة ٢٠١٨/١٢/٢٠ الساعة ٧،١٥ pm

^٢ التوصيات الأربعين متاحة على الرابط:

[www. Money laundry comapating.blogspot.com /2009/08/blog-post24.html](http://www.Money_laundry_comapating.blogspot.com/2009/08/blog-post24.html)

تاريخ الزيارة ٢٠١٨/١٢/٢١ الساعة ٩،٣٠ pm

^٣ التوصية الرابعة من التوصيات الأربعون الصادرة عن لجنة العمل المعنية بالإجراءات المالية المتعلقة بمكافحة غسيل الأموال بالوسائل الحديثة عام ١٩٩٠، المرجع السابق،

- بالإضافة إلى المصادرة والعقوبات الجنائية يجب على الدول النظر في عقوبات مالية ومدنية و/ أو دعاوى قضائية تشمل دعاوى مدنية لإبطال العقود التي يكون أطرافها على علم أن الدولة ستتضرر من هذه العقود^١.

٢-تعزيز دور النظام المالي: مما لا شك فيه أن النظم المصرفية المتطورة تشكل البيئة المناسبة لعمليات غسل الأموال الحديثة، وبالتالي بات لزاماً على المصارف أن تأخذ الحيطة والحذر بشأن العمليات المصرفية التي تقوم بها، بما يؤدي إلى سد الثغرات التي تتسلل فيها الأموال غير النظيفة. وحتى تتمكن المصارف من القيام بهذا الدور لابد من مراعاة مجموعة من الالتزامات:

أ-الكشف عن هوية المستخدمين: ينبغي على المصارف أن لا تحتفظ بحسابات مجهولة الاسم أو بحسابات وهمية، وعلى المصارف أن تتخذ التدابير اللازمة للحصول على المعلومات حول الهوية الحقيقية للأشخاص المفتوح باسمهم الحسابات إذا ما كان هناك أي شك حول هؤلاء الأشخاص (وبالتحديد عند فتح حساب أو الدخول في معاملات بصفة وكيل أو استئجار صناديق الأمانات أو في حال تنفيذ معاملات مالية بمبالغ كبيرة^٢).

^١ التوصية السابعة، المرجع السابق.

^٢ التوصية العاشرة، المرجع السابق.

ب- الاحتفاظ بالسجلات:

وتشمل هذه السجلات ما يلي:

- يجب أن تحتفظ المصارف بكافة السجلات الضرورية للعمليات المحلية و الدولية لمدة خمس سنوات على الأقل وذلك حتى تتمكن الجهات الرقابية من الحصول على المعلومات التي تطلبها على وجه السرعة.
- ينبغي أن تكون هذه السجلات مكتملة وكافية (تشمل مبالغ وأنواع العملة المستخدمة إذا وجدت) لتوفير الدليل على إقامة الدعوى الجنائية.
- يجب على المصارف أن تحتفظ بسجلات عن هوية العميل (صورة الهوية-جواز السفر-رخصة القيادة) وملفات حسابه وأعماله وذلك لمدة خمس سنوات على الأقل بعد قفل الحسابات.
- ينبغي أن تكون هذه المستندات متاحة للسلطات المحلية في إطار إقامة الدعاوى والتحقيقات الجنائية^١.
- ينبغي على المصارف أن تولي اهتماماً خاصاً بالصفقات الكبيرة والصفقات غير التقليدية والتي ليس لها غرض اقتصادي أو قانوني واضح، كما يجب التحري عن خلفية تلك الصفقات وتدوينها كتابة وجعلها متاحة لكل جهات الرقابة^٢.

^١ التوصية الثانية عشر، المرجع السابق.

^٢ التوصية الرابعة عشر، المرجع السابق.

ج-التبليغ عن المعاملات والصفقات المشبوهة: تلتزم المصارف بالسرية في علاقتها بعملائها إلا إذا قامت شبهات لدى المصارف تفيد أن أموال العميل تحصلت من نطاق إجرامي، ففي هذه الحالة ينبغي على المصارف أن تقوم بالتبليغ عن هذه الأموال إلى السلطات المختصة. وفي هذا الإطار أكدت التوصيات على ضرورة وجود نصوص قانونية تعفي المصارف وموظفيها من المسؤولية المترتبة على انتهاك السرية المصرفية عند التبليغ عن وجود حالات غسيل للأموال^١.

٤- تعزيز التعاون الدولي:

ويتجلى هذا التعاون من خلال:

- تبادل المعلومات الدولية المتعلقة بالمعاملات المشتبه فيها أو الأشخاص أو الشركات المتورطة في تلك المعاملات.
- وضع الضوابط الدقيقة للتأكد من أن تبادل المعلومات مطابق للنصوص الوطنية والدولية المتعلقة بحماية البيانات الشخصية^٢.
- تبادل المساعدات القانونية في الأمور الجنائية وذلك فيما يتعلق بإجراء التحقيق و تجميد ومصادرة الأموال القذرة^٣.
- يجب أن تعترف كل دولة أن غسيل الأموال باستخدام وسائل الدفع الإلكتروني من الجرائم الخطرة كما ينبغي أن تقوم الدول باتخاذ الإجراءات لتسليم الأشخاص المتهمين بهذه الجريمة^٤.

^١ التوصية السادسة عشر، المرجع السابق.

^٢ التوصية الثانية والثلاثون، المرجع السابق.

^٣ التوصية السابعة والثلاثون، المرجع السابق.

^٤ التوصية الأربعون، المرجع السابق.

الفرع الثاني

مكافحة غسيل الأموال وفق القانون السوري

لقد أولى المشرع السوري جريمة غسيل الأموال اهتماماً خاصاً باعتبارها من الجرائم الخطرة والتي تولد آثار سلبية على القطاع المصرفي بشكل خاص والاقتصاد الوطني بشكل عام. لذلك أصدر قانون خاص بهذه الجريمة وهو المرسوم التشريعي رقم /٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسيل الأموال وتمويل الإرهاب وقد تم تعديل بعض مواده بموجب المرسومين التشريعيين (المرسوم رقم /٢٧/ لعام ٢٠١١ و المرسوم رقم /٤٦/ لعام ٢٠١٣). وقد وسّع المشرع السوري من مفهوم غسيل الأموال وجعله شاملاً لكل فعل بقصد به:

- إخفاء أو تمويه الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو كيفية التصرف بها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها مع العلم أنها أموال غير مشروعة.
- تحويل الأموال أو استبدالها مع علم الفاعل أنه أموال غير مشروعة لغرض إخفاء أو تمويه مصدرها أو مساعدة شخص ضالع في هذا الجرم على الإفلات من العقاب.
- تملك الأموال غير المشروعة أو حيازتها أو إدارتها أو استثمارها أو استخدامها لشراء أموال منقولة أو غير منقولة أو

للقيام بعمليات مالية مع علم الفاعل أنها أموال غير مشروعة^١.

و يلاحظ من نص المادة السالفة الذكر أن المشرع السوري لم يحدد وسيلة معينة لارتكاب هذه الجريمة، الأمر الذي منح المسوغ القانوني لتطبيق كافة أحكام هذا المرسوم التشريعي على عمليات غسل الأموال باستخدام وسائل الدفع الإلكتروني. أي أن عمليات غسل الأموال التي تتم باستخدام وسائل الدفع الإلكتروني تخضع لأحكام هذا المرسوم ومن خلال استقراء نصوص هذا المرسوم نجد أن المشرع السوري اتخذ نوعين من التدابير في سبيل مكافحة هذه الجريمة:

أولاً: التدابير الوقائية

وتتمثل هذه التدابير في الآتي:

١- ألزم المشرع السوري المصارف وبعض الشركات (كشركات بناء العقارات وتجار الحلي.....الخ) أن يتم الاحتفاظ بسجلات في حالات معينة هي:

- العمليات التي تفوق قيمتها مبلغ محدد من قبل الهيئة.
- عند نشوء علاقة العمل للمتعاملين الدائمين.
- العمليات التي فيها شك حول محاولة أحد العملاء القيام بعمليات غسل الأموال.

^١ المادة (٢/أ/١٠٢،٣) من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

- حالات الشك بصحة المعلومات المصرح منها سابقاً.
- حالات حدوث تغيرات لاحقة في هوية المتعاملين^١.

٢- ألزم المشرع السوري المصارف وبعض الشركات (كشركات بناء العقارات وتجار الحلي.....الخ) التحقق من هوية المتعاملين وعناوينهم بالاستناد إلى وثائق رسمية وأن تحتفظ بهذه السجلات والوثائق لمدة خمس سنوات من تاريخ انتهاء العملية أو إنهاء العلاقة مع العميل أيهما أطول على نحو يسمح لهيئة مكافحة غسيل الأموال وتمويل الإرهاب الاستفادة من هذه الوثائق عند حاجتها^٢.

٣- ألزم المشرع السوري المصارف الوطنية وفروعها الخارجية بمراقبة العمليات التي تجريها مع المتعاملين معها لتتلافى تورطها بعمليات يمكن أن تخفي غسلاً للأموال^٣، وتحدد أصول هذه الرقابة بموجب نظام يصدر بقرار من الهيئة على أن يتضمن الأمور الآتية^٤:

^١ المادة (٤/أ) من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

^٢ المادة (٤/ب) من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسيل الأموال وتمويل الإرهاب.

^٣ المادة (٥/أ) من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

^٤ المادة (٥/ب) من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

أ- التحقق من هوية المتعاملين الحقيقيين وتحديد هوية صاحب الحق الاقتصادي و ذلك في حال:

- تم التعامل بواسطة وكيل أو عن طريق حساب مرقم أو حسابات لا يكون فيها صاحب الحساب هو صاحب الحق الاقتصادي فيها.
- كان المتعامل شخص عابر وكانت العملية تفوق مبلغ محدد من المال بقرار من الهيئة.
- حالات الشك في قيام أحد العملاء بعمليات غسيل الأموال أو في حالات الشك في صحة المعلومات المصرح بها أو حدوث تغيرات لاحقة في هوية المتعاملين أو هوية أصحاب الحقوق الاقتصادية.
- يجب عند إجراء التحويلات المالية المحلية والدولية تحديد مصدر الحوالة والمستفيد منها في جميع الحوالات الصادرة والواردة كما يجب تحديد المبرر الاقتصادي للحوالة في حال تجاوزت مبلغاً معيناً من المال يحدد بقرار من الهيئة.

ب - الاحتفاظ بصور المستندات المتعلقة بالعمليات كافة وبصور الوثائق الرسمية المتعلقة بهوية المتعاملين لمدة خمس سنوات على الأقل بعد انجاز العمليات أو إقفال الحسابات نحو يسمح لهيئة مكافحة غسيل الأموال وتمويل الإرهاب الاستفادة من هذه الوثائق عند حاجتها.

ج-تحديد المؤشرات التي تدل على احتمال وجود عمليات غسيل الأموال ومبادئ الحيطة والحذر لكشف العمليات المشبوهة.

د-التزام المصارف بعدم إعطاء معلومات مغايرة للحقيقة بغية تضليل السلطات الإدارية والقضائية.

ه-التزام المصارف بتدريب موظفيها حول طرق مراقبة العمليات المالية والمصرفية لمكافحة عمليات غسيل الأموال.

و-التزام المصارف بتعيين مسؤول أو تشكيل لجنة مسؤولة عن مكافحة غسيل الأموال على مستوى وظيفي عالٍ.

٤-ينبغي على المصارف توخي الحيلة والحذر عند تعاملها مع المصارف المراسلة لتلافي تورطها في عمليات مشبوهة من خلال جمع معلومات كافية عنها لفهم طبيعة عملها وتقييم إجراءاتها الداخلية لمكافحة غسيل الأموال وفي حال عدم القدرة على جمع هذه المعلومات يجب عدم القيام بمثل هذا التعامل^١.

٥-فرض المشرع السوري على المصارف وبعض الشركات (كشركات بناء العقارات وتجار الحلي.....الخ) إجراءات خاصة و إيلاء اهتمام خاص في حال :

أ-كون العميل أو صاحب الحق الاقتصادي شخص معرض لأخطار سياسية ويعتبر كل فرد مسند إليه منصباً عاماً أو رفيعاً في بلد أجنبي شخصاً معرضاً لأخطار سياسية.

ب-العمليات التي تتم دون وجود العميل أو عن طريق التقنيات المتطورة التي قد تتيح عدم ذكر الهوية الحقيقية.

^١ المادة (٥/د) من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

ج- المعاملات المعقدة والكبيرة الحجم على غير العادة وجميع المعاملات غير المعتادة التي لا يكون لها غرض اقتصادي ظاهر.

د- المعاملات التي تتم مع أفراد طبيعيين أو اعتباريين مقيمين في البلاد غير المتعاونة في مجال مكافحة غسل الأموال الصادرة عن مجموعة العمل المالي المعنية بغسل الأموال.

وتتمثل هذه الإجراءات الخاصة ب :

- الحصول على موافقة الإدارة العليا في هذه الجهات على قيام علاقة العمل.
- القيام بشكل مستمر بمراقبة هذه العلاقة.
- اتخاذ تدابير معقولة لتحديد مصدر الأموال^١.

ثانياً: التدابير العلاجية

تتمثل التدابير العلاجية من خلال فرض المشرع السوري للمؤيدات الجزائية بحق مرتكب هذه الجريمة. ومن خلال استقراء نصوص المرسوم التشريعي ذات الصلة نستنتج الآتي:

١- اشترط المشرع السوري لفرض العقوبة بحق مرتكب هذه الجريمة:

- أن تكون الأموال غير المشروعة ناجمة عن أحد الأفعال المحددة في المادة الأولى من هذا المرسوم.

^١ المادة السادسة من المرسوم التشريعي رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة عمليات غسل الأموال وتمويل الإرهاب.

- أن يهدف المجرم من وراء أفعاله إضفاء الشرعية على الأموال الملوثة سواء تمكن من تحقيق هذا الهدف أم لا.
- أن يكون المجرم على علم أن هذه الأموال ناجمة عن أعمال غير مشروعة ومع ذلك يريد إضفاء الشرعية عليها^١.

٢- ساوى المرسوم بين الفاعل والشريك والمتدخل والمخفي من ناحية العقوبة^٢.

٣- عاقب المشرع السوري مرتكب جريمة غسيل الأموال بالعقوبات الآتية:

- الاعتقال المؤقت من ثلاث سنوات إلى ست سنوات.
- غرامة تعادل قيمة الأموال المضبوطة على أن لا تقل عن مليون في حال تعذر ضبطها^٣.
- مصادرة الأموال الناجمة عن الجريمة وإيراداتهما والوسائط والأدوات المستخدمة^٤.
- مصادرة الأموال المحولة أو المبدلة في حال تم تبديل الأموال غير المشروعة وإذا اختلطت الأموال غير المشروعة

^١ المادة (١٤/أ) من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب.

^٢ المادة (١٤/ب) من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب.

^٣ المادة (١٤/أ) من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب.

^٤ المادة (١٥/أ) من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

بأموال أخرى مشروعة فإنها تخضع للمصادرة بحدود القيمة المقدرة للأموال غير المشروعة دون الإخلال بحق الهيئة في تجميدها ريثما يتم التحقيق بشأنها^١.

• مصادرة كافة الإيرادات والمستحقات المستمدة من الأموال غير المشروعة أو الأموال المبدلة أو الأموال التي اختلطت بالأموال غير المشروعة^٢.

• في حال ارتكاب جرم غسيل الأموال من قبل مدير الشخص الاعتباري أو أعضاء إدارته أو عماله أو بإحدى وسائله تتم معاقبة الشخص الاعتباري^٣ :

❖ بالوقف عن العمل شهراً على الأقل وستين على الأكثر الأمر الذي يترتب عليه وقف أعمال الشخص الاعتباري كافة وتبديل اسمه وأعضاء مجلس إدارته، كما يحول الوقف دون التنازل عن المحل مع الاحتفاظ بحقوق الغير ذي النية الحسنة^٤.

^١ المادة (١٥/ب) من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

^٢ المادة (١٥/ج) من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

^٣ المادة ١٧/ من المرسوم رقم ٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسيل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم ٢٧/ لعام ٢٠١١.

^٤ المادتان (١٠٨-١١٠ / ١) من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

- ❖ حل الشخص الاعتباري ويترتب على الحل تصفية أمواله وفقدان أعضاء مجلس إدارته الأهلية اللازمة لتأسيس أو إدارة شخص اعتباري مماثل^١.
- ❖ ولا تخل هذه العقوبات بالمسؤولية الجنائية للأشخاص الطبيعيين.

٤- فرض المشروع السوري عقوبة الحبس من ٣ أشهر حتى سنة وبالغرامة من ٢٥٠ ألف حتى مليون بحق المصارف و التي تخل بالتزاماتها في التحقق من هوية العملاء والاحتفاظ بالسجلات المتعلقة بالعملاء^٢.

٥- يجوز للهيئة فرض مؤيدات إدارية وغرامات مالية لا تتجاوز قيمتها مبلغ ١٠٠ مليون ليرة سورية وإجراءات علاجية صحيحة على الأشخاص الطبيعيين والاعتباريين المخالفين للالتزامات المفروضة بموجب هذا المرسوم (كالالتزامات المتعلقة بمسك السجلات والتحقق من هوية العملاء)^٣.

^١ المادتان (١٠٩-١١٠ / ٢) من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ المادة /١٧/ من المرسوم رقم /٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسل الأموال وتمويل الإرهاب.

^٣ المادة (٣/ب) من المرسوم رقم /٣٣/ لعام ٢٠٠٥ الخاص بمكافحة غسل الأموال وتمويل الإرهاب والمعدلة بموجب المرسوم التشريعي رقم /٢٧/ لعام ٢٠١١ والمعدلة بموجب المرسوم التشريعي رقم /٤٦/ لعام ٢٠١٣.

إذاً ومما تقدم نجد أن المشرع السوري كان موفقاً في هذا المرسوم التشريعي وذلك على اعتبار أنه تضمن بعض التوصيات الأربعين التي تحدثنا عنها آنفاً، كما أنه عمل على تحديد كل جزئية تتعلق بغسيل الأموال لكي لا يتمكن المجرم من الإفلات من العقاب. كما منح المشرع السوري نوع من المرونة في هذا المرسوم بحيث اعتبر أن كل إخفاء للمصدر الحقيقي للأموال غير المشروعة أو كل تملك لها مهما كانت الوسيلة المستخدمة نوع من غسيل الأموال آخذاً بالحسبان أن التطور التقني قد يكشف عن وسائل وأساليب جديدة تستخدم في ارتكاب هذا الجرم، ولكي لا يضطر إلى تعديل كلما ظهرت وسيلة جديدة لارتكاب هذه الجريمة.

وبالتالي فإن الأحكام والنصوص القانونية المتعلقة بالعقوبات المفروضة السالفة الذكر (أي وبمعنى آخر المسؤولية الجزائية) تشكل نوعاً من العلاج القانوني لعمليات غسيل الأموال باستخدام وسائل الدفع الالكتروني.

وفي ختام الحديث عن سبل معالجة المشكلات القانونية يمكننا تلخيص هذه السبل في أربعة أشكال:

الشكل الأول: شكّلت المسؤولية الجزائية الوسيلة الفعالة لمعالجة مشكلات انتهاك السرية المصرفية ومشكلات غسيل الأموال.

الشكل الثاني: تصدّت بعض النصوص القانونية النازمة للمعاملات الإلكترونية لمعالجة المشكلات التقنية التي تواجه المستهلك الإلكتروني من خلال عدة التزامات قانونية (كالالتزام بالإعلام وحق العدول)، فضلاً عن معالجة مشكلة المحكمة المختصة لجهة إحداث المحاكم الإلكترونية.

الشكل الثالث: قدّمت بعض النصوص النازمة للمعاملات التقليدية العلاج القانوني لمسألة القانون الواجب التطبيق على الدفع الإلكتروني والمحكمة المختصة بنظر منازعات الدفع الإلكتروني، فضلاً عن حماية المستهلك الإلكتروني من المشكلات القانونية التي تواجهه وذلك بشرط توافر الضوابط القانونية التي حدّتها هذه النصوص.

الشكل الرابع: يتجلى هذا الشكل بمجموعة من المقترحات لكيفية فرض الضريبة على معاملات الدفع الإلكتروني وكيفية تحصيلها، ناهيك عن المقترحات الخاصة بالقانون الواجب التطبيق بالنسبة للمصارف الإلكترونية التي تقدم خدماتها في الفضاء الخارجي.

الباب الثاني

الإطار الموضوعي للمشكلات الأمنية

بعد أن تعرفنا في الباب الأول على المشكلات القانونية وسبل معالجتها، ننتقل للحديث عن شكل آخر من المشكلات التي تتاب وسائل الدفع الإلكتروني ألا وهي المشكلات الأمنية. حيث تشكل المشكلات الأمنية أحد أهم وأخطر القضايا التي تشغل بال المتعاملين بوسائل الدفع الإلكتروني، ومرد ذلك لسببين اثنين:

الأول: الطبيعة الخاصة للنشاط المصرفي الإلكتروني بشكل عام ولعملية الدفع الإلكتروني بشكل خاص، فهذه الأخيرة تزداد فيها دواعي الأمن وذلك بالنظر إلى الطبيعة المالية التي يقوم عليها الدفع الإلكتروني والتي يزداد في ظلها انتشار الأعمال غير المشروعة، الأمر الذي من شأنه أن يمس بثقة الأفراد بوسائل الدفع مما ينعكس بشكل سلبي على السمعة التجارية للجهات المصدرة.

الثاني: هيمنة الأجهزة والبرامج الإلكترونية على آلية التعامل بوسائل الدفع الإلكترونية، فالبيئة الإلكترونية التي تنتشر فيها هذه الوسائل من شأنها أن تلوح بالكثير من المشكلات الأمنية الناتجة عن التعامل بوسائل الدفع الإلكتروني سواء أكان مرتكب هذه المشكلات من أطراف عملية الدفع أم من أطراف خارجية.

وحيث أننا في نطاق الدفع الإلكتروني ينبغي أن نشير إلى أنه فيما يتعلق بالمشكلات الأمنية، سوف تنصب معظم دراستنا بالنسبة لهذه المشكلات على وسائل الدفع التي تتجسد بكيان مادي (بطاقات الدفع الإلكترونية التي تستخدم كوسيلة للوفاء بالثمن إضافةً إلى بطاقات

السحب من أجهزة الصراف الآلي). وذلك على اعتبار أن هذه البطاقات من أكثر وسائل الدفع الإلكتروني انتشاراً في سورية والبلدان العربية، إضافة إلى أن معظم المشكلات الأمنية التي سوف نتحدث عنها ترتكب بالنسبة لبطاقات الدفع، أما بالنسبة لوسائل الدفع الأخرى ففي ظل عدم انتشارها بشكل كبير في سورية ونظراً لما تتمتع به هذه الوسائل من ميزات تقنية وفنية فضلاً عن انعدام الوجود المادي لهذه الوسائل. الأمر الذي جعل من إمكانية انتهاكها من الناحية الأمنية غاية في الصعوبة على خلاف بطاقات الدفع التي كانت عرضة للكثير من المشكلات الأمنية.

وبشكل عام يمكننا أن نجل المشكلات الأمنية لوسائل الدفع الإلكتروني في شكلين:

الشكل الأول: المشكلات التي تمس أداة الدفع الإلكترونية باعتبارها كيان مادي وتقني في ان واحد.

الشكل الثاني: المشكلات الناشئة عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية.

حيث أنه عندما تم ابتكار وسائل الدفع الإلكترونية إنما كانت بهدف مشروع يتمثل بتسوية المعاملات التجارية بوسائل إلكترونية، إلا أن التطبيق العملي كشف عن حالات كثيرة يتم من خلالها المساس بأداة الدفع الإلكترونية أو إساءة استخدام أدوات الدفع وبشكل خاص بطاقات الدفع الإلكترونية.

وأمام هذه المشكلات الأمنية لوسائل الدفع الإلكتروني وتحدياتها تبرز الحاجة الملحة للبحث عن العلاج القانوني لهذه المشكلات. وعلى غرار المشكلات القانونية ينبغي على الجهات الرقابية أن تأخذ على

عانتها مسألة وضع حد لانتشار مثل هذه المشكلات كونها تتعلق بثقة الأفراد بوسائل الدفع الإلكتروني. وبشكل عام يمكننا أن نجمل سبل معالجة المشكلات الأمنية في أسلوبين:

الأسلوب الأول: التدابير الوقائية: وهي عبارة عن مجموعة من التدابير والاحتياطات المتخذة بهدف تلافي وتجنب حدوث مثل هذه المشكلات. أي أنها تتخذ قبل حدوث المشكلة.

الأسلوب الثاني: التدابير العلاجية: وهي عبارة عن مجموعة من المؤيدات الجزائية المفروضة بحق من يرتكب هذه المشكلات ومن خلال السلطة القضائية أي أنها تتخذ بعد حدوث المشكلة.

وفي سبيل الإحاطة الشاملة بالإطار الموضوعي للمشكلات الأمنية سوف نقوم بالتعريف بالمشكلات الأمنية في الفصل الأول ثم ننتقل للحديث عن سبل معالجة هذه المشكلات في الفصل الثاني.

الفصل الأول

التعريف بالمشكلات الأمنية

تجد المشكلات الأمنية سبيلها إلى العمل المصرفي الإلكتروني بشكل عام وإلى عملية الدفع الإلكتروني بشكل خاص من خلال اتجاهين:

الأول: التهديد الداخلي

ومصدره أطراف التعامل بوسائل الدفع الإلكتروني (الحامل، التاجر، المصدر)، فهؤلاء الأشخاص بحكم خبرتهم ومعرفتهم يستطيعون ارتكاب العديد من الأعمال غير المشروعة التي تمس بوسائل الدفع الإلكتروني.

الثاني: التهديد الخارجي

ومصدره الأشخاص الذين يخرجون من دائرة أطراف التعامل بوسائل الدفع الإلكتروني (الغير) إضافةً إلى كل متعامل مع شبكة الإنترنت، فهؤلاء المتعاملين أصحاب سوابق إجرامية ونوايا خبيثة الأمر الذي يندرج بتحديات أمنية كبيرة تنتاب وسائل الدفع الإلكتروني.

وعلى الرغم من الانتشار الكبير للتهديدات الخارجية إلا أن الدراسات^١ تؤكد أن نسبة التهديد الداخلي تفوق نسبة التهديد الخارجي، وذلك بسبب امتلاك أصحاب التهديد الداخلي (أطراف التعامل بوسائل الدفع الإلكتروني) المعرفة والخبرة الكافية بنقاط الضعف والقوة لدى وسائل الدفع.

ونحن من جانبنا نعرف المشكلات الأمنية في نطاق الدفع الإلكتروني بأنها: «جملة من الأعمال غير المشروعة التي تمس بأداة الدفع

^١ مشار إليه لدى: د. علاء التميمي، مرجع سابق، ص ٢٣٧.

الإلكترونية أو تمس آلية عملها على النحو الذي من شأنه أن يسبب خسائر مادية كبيرة.)

نستنتج من التعريف السابق أن المشكلات الأمنية في نطاق الدفع الإلكتروني تتخذ أحد شكلين:

الشكل الأول: المشكلات التي تمس أداة الدفع الإلكترونية وهي مجال دراستنا في المبحث الأول.

الشكل الثاني: المشكلات التي تحدث نتيجة الاستخدام غير المشروع لبطاقة الدفع الإلكترونية وهي مدار دراستنا في المبحث الثاني.

المبحث الأول

المشكلات التي تمس أداة الدفع الإلكترونية

ويقصد بهذه المشكلات مجموعة من التحديات والأفعال الجرمية التي تواجه أداة الدفع الإلكترونية باعتبارها كيان مادي وتقني في آن واحد. فقد كشف التطبيق العملي لوسائل الدفع الإلكتروني بشكل عام ولبطاقات الدفع بشكل خاص عن إمكانية تعرضها لمجموعة من التحديات الأمنية. فنظراً لأن هذه الوسائل تتجسد بشكل مادي (بطاقات الدفع) فهي محل لبعض الجرائم التقليدية (كالسرقة والتزوير). كما أن الجانب التقني لهذه الوسائل جعلها عرضةً لأعطال تقنية وفنية، إضافة إلى أن هذه الوسائل كانت محط اهتمام قراصنة الحواسيب الأمر الذي أدى لظهور بعض الجرائم الإلكترونية في نطاقها. لذلك وفي سبيل تسليط الضوء على المشكلات التي تمس أداة الدفع الإلكترونية سوف نتحدث عن تعطل أداة الدفع وفقدانها في المطلب الأول ثم ننتقل للحديث عن القرصنة الإلكترونية في المطلب الثاني.

المطلب الأول

تعطل أداة الدفع وفقدانها

تتميز هذه المشكلة بكونها تجمع بين الشكل الإلكتروني والشكل التقليدي. حيث تعد مشكلة تعطل أداة الدفع أحد المشكلات الناتجة عن دخول العنصر التقني في نطاق الدفع. أما مشكلة فقدان أداة الدفع فهي من المشكلات التقليدية المعروفة من قبل وبالتحديد (فقدان أداة الدفع بتدخل الغير)، ولكن الطبيعة الإلكترونية لوسائل الدفع الإلكتروني

استدعت ظهور أساليب تقنية لارتكاب هذه الجريمة (كالأساليب الإلكترونية لسرقة أرقام البطاقات عبر شبكة الإنترنت)، فضلاً عن إمكانية استخدام بعض الأساليب التقليدية في بعض الأحيان (كما في حالة نشل البطاقة من المحفظة أو الجيب). وبناءً عليه سوف نتحدث عن مشكلة تعطل أداة الدفع في الفرع الأول ثم ننتقل للحديث عن مشكلة فقدان أداة الدفع في الفرع الثاني.

الفرع الأول

تعطل أداة الدفع الإلكترونية

يُقصد بتعطيل أداة الدفع ما قد يطرأ على أداة الدفع الإلكترونية من أعطال عرضية نتيجة خلل مادي أو كهربائي أو قصور في أوامر التشغيل المرتبطة بلغة البرمجة الخاصة بتصميم تلك الأداة أو قصور في عملية الصيانة، والتي يترتب عليها انحراف في سلوك أداة الدفع وقصورها في أداء وظائفها. وبالتالي نجد أن تعطل أداة الدفع الإلكترونية قد يحدث بسبب أحد عيبي:

أولاً: التعطل نتيجة لعيب في الأداة

كثيراً ما يصيب أداة الدفع الإلكترونية مجموعة من العيوب والأعطال سواء أكانت هذه العيوب عبارة عن أعطال فنية (خلل كهربائي) أم كانت عبارة عن أعطال تشغيلية (كعدم دقة تدوين المدفوعات التي تتم من خلالها أو عجزها عن نقل وحدات النقد الإلكترونية إلى التاجر المقصود أو نقلها خطأً للشخص غير المقصود). وبنتيجة هذه الأعطال يلحق بالمستخدم العديد من الأضرار ومثال ذلك (خسارته للأرصدة المخزنة على أداة الدفع، حرمانه من الحصول على السلع والخدمات نتيجة عدم تمكنه من إجراء مدفوعاته في الوقت المناسب).

ومما لا شك فيه أن تعرض المستخدم لهذه الأمور يثير مسؤولية المصدر تجاه مستخدم الأداة عن تعويض الأضرار الناشئة عن هذه الأعطال. وباستقراء عقود استخدام نظام النقد الإلكتروني والآراء الفقهية في هذا المجال يتبين لنا أن موقف مصدري وسائل الدفع الإلكتروني إزاء هذه المسألة لا يخرج عن أحد الفروض الآتية:

الفرضية الأولى: ترى هذه الفرضية ضرورة النص صراحةً على استبعاد المسؤولية عن الأضرار التي قد تصيب المستخدم نتيجة الاختلال أو الأعطال التي قد تصيب أداة الدفع. ومن أمثلة ذلك (ما قررته الفقرة الثانية من البند السابع من عقد استخدام نظام - PAYCASH - من استبعاد مسؤولية شركة CY-PHERMINT عن الخسائر الناتجة عن أسباب خارجة عن نطاق سيطرتها المباشرة والتي من بينها الأعطال التي تصيب أداة الدفع^١).

إذاً الفرض هنا أن تستبعد مؤسسة الإصدار مسؤوليتها عن تعطل أداة الدفع بصورة كلية دون البحث في أسباب هذه الأعطال وما إذا كانت هذه الأعطال راجعة لعيب في الأداة ذاتها أم كانت راجعة لخطأ من جانب المستخدم. والسبب في استبعاد المسؤولية هو عدم سيطرة هذه المؤسسات على أداة الدفع سيطرة مباشرة.

ولكن نحن من جانبنا لا نؤيد هذه الفرضية، حيث أن التعلل بكون أداة الدفع ليست تحت السيطرة المباشرة لجهة الإصدار لا يكفي لتبرير استبعاد مسؤوليتها في هذه الحالة، وذلك لكونها ملتزمة تجاه المستخدم بتزويده بأداة دفع صالحة للاستخدام.

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣١٧. و راجع الرابط:

<http://www.paycash.eu/en/agb/>

تاريخ الزيارة ٢٠١٩/٤/٣٠ الساعة ٩.٤٥ P.M

وبالتالي أي عطل يلحق بتلك الأداة - دون أن يكون هناك سوء استخدام من جانب المستخدم - يشكل إخلالاً بالالتزام. وبالتالي فإن إدراج مثل هذه الشروط ضمن عقود الاستخدام الخاصة بأداة الدفع لاستبعاد مسؤولية المصدر يعد من قبل الشروط غير العادلة وبالتالي ينبغي استبعادها وتحمل المصدر المسؤولية عن الأضرار التي تصيب المستخدم من جراء الأعطال الفنية أو أي عطل آخر طالما أن المستخدم لم يسيء الاستخدام.

الفرضية الثانية: ترى هذه الفرضية ضرورة تحمل المصدر المسؤولية عن تعويض المستخدم عن جميع الأضرار التي تلحق به بغض النظر عن مصدرها سواء أكانت أعطال فنية أم أعطال سوء استخدام^١.

ونحن من جهتنا لا نؤيد هذا التوسع في المسؤولية، حيث أن الأخذ بهذا الفرض سيساعد كثيراً على زيادة إقبال المستخدمين على استعمال تلك النظم في الوفاء بالتزاماتهم دون الخشية من ضياع حقوقهم. لكن بالمقابل سوف يشكل ذلك عبئاً ثقيلاً على عاتق المصدرين وقد يدفعهم إلى الإحجام عن هذه الوسائل رغم حداثة انتشارها، الأمر الذي ينعكس سلباً على انتشار معاملات الدفع الإلكتروني وتطورها.

ولعلّ الحل الوحيد لهذه المسألة من جانبنا يكمن في التمييز بين نوعين من الأعطال:

^١ المرجع السابق، ص ٣١٨.

• الأعطال التي تحدث نتيجة سوء الاستخدام من قبل المستخدم فهذه الأعطال لا يتحمل المصدر المسؤولية عنها طالما أنه أوفى بالتزامه المتعلق بتزويد المستخدم بكافة تعليمات الاستخدام ومحاذيره.

• الأعطال التي تصيب أداة الدفع دون أن تكون نتيجة سوء الاستخدام سواء أكانت أعطال فنية أم أعطال كهربائية أم أعطال تشغيلية، فجميعها يتحمل المصدر المسؤولية عنها كون المصدر ملتزم بتسليم أداة الدفع صالحة للاستخدام.

وبالتالي فإن من شأن هذا التمييز أن يحقق نوع من التوازن المنشود بين أطراف أداة الدفع، فمن جهة يشجع المستخدم على التعامل بهذه الوسائل دون خوف من أي ضرر يصيبه، ومن جهة أخرى يلزم المصدر باتخاذ كافة الاحتياطات لتفادي أي مشكلة. الأمر الذي ينعكس إيجاباً على تطور وسائل الدفع الإلكتروني وانتشارها. ويؤيد رأينا هذا ما نصت عليه الفقرة الثانية من المادة ١٥/ من عقد استخدام نظام (NETCASH): إن المصرف غير مسؤول عن توقف أو انقطاع خدمة الدفع الناتجة عن الاستعمال المعيب لأداة الدفع الخاصة بالمستخدم^١.

ثانياً: التعطل نتيجة لتقصير في الصيانة.

تعتمد أنظمة الدفع الإلكترونية على نظم المعلومات وتقنية شبكات الاتصال الإلكترونية، وأن الارتباط بينهما يؤدي إلى زيادة المخاطر،

^١ راجع الرابط: <http://www.netcash-uk.bnpparibas.com/gb/convention.htm>

فقد تنشأ هذه الأخطار من عدم كفاءة النظم المتبعة لمواجهة متطلبات المستخدمين، أو من السرعة في إجراء الصيانة الطارئة أو الدورية التي تتطلبها شبكات الاتصال. ومن الأخطاء الشائعة في هذا المجال:

١- الاعتماد على تقنيات غير متطورة أو تقنية واحدة مشتركة للعديد من أنظمة التشغيل أو الأجهزة المستخدمة، مما يؤدي إلى تعطيل هذه الأنظمة والشبكات المرتبطة عند حدوث أي مشكلة تتعلق بالبرمجة أو البنية التحتية الإلكترونية.

٢- الاعتماد على مصادر فنية خارج المصارف لتقديم الدعم الفني بشأن البنية الأساسية اللازمة لصيانة الشبكات وغيرها من الأجهزة المادية للمصارف الإلكترونية. فعلى الرغم من الفوائد العديدة للمصادر الفنية الخارجية فإن هذه الأخطار يمكن أن تزيد كنتيجة لارتباط الشبكات مع بعضها البعض واعتماد أنظمة الدفع على مزود خدمة وحيد^١.

وبالنتيجة يمكننا القول أن وسائل الدفع الإلكتروني كأى عنصر تقني يصيبه أعطال فنية ناتجة عن وجود عيوب في تصميم الأداة أو وجود تقصير في صيانتها، الأمر الذي يجعل الجهة المصدرة مسؤولة عن الأضرار التي تصيب المستخدم جراء هذه الأعطال. باعتبار أن هذه الجهة ملتزمة بموجب عقود استخدام بطاقة الدفع الإلكترونية بتسليم أداة جاهزة وصالحة للاستخدام وطالما أن المستخدم لم يسئ استخدامها.

^١ د. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠٠٥، ص ٣٤٢-٣٤٣.

الفرع الثاني

فقدان أداة الدفع الإلكترونية

تتعرض وسائل الدفع الإلكتروني لمشكلة فقدان أو الضياع نتيجة لأحد أمرين:

الأول: إن بعض وسائل الدفع الإلكتروني تتمثل بشكل مادي، الأمر الذي يجعلها عرضة لمخاطر فقدان بتدخل الغير (السرقه) كما هو الحال بالنسبة لبطاقات الدفع الإلكتروني، فضلاً عن عمليات السرقة عبر الإنترنت كما هو الحال عند سرقة الحسابات المصرفية عبر شبكة الإنترنت.

الثاني: تتطلب الية عمل بعض وسائل الدفع الإلكتروني إدخال الرقم السري عبر الأجهزة الإلكترونية وبالتالي قد يحصل نوع من النسيان لهذه الرموز أو إدخال خاطئ لهذه البيانات أو ضياع هذه الاداة الأمر الذي يؤدي لفقدان أداة الدفع دون تدخل الغير.

وبالتالي وفي سبيل التعرف على مشكلة فقدان أداة الدفع الإلكترونية سوف نتحدث عن فقدان بتدخل الغير (أولاً) ثم ننتقل للحديث عن فقدان دون تدخل الغير (ثانياً).

أولاً: فقدان أداة الدفع بتدخل الغير (سرقة أداة الدفع)

ينبغي أن نشير بدايةً إلى أن سرقة أداة الدفع لا تتوقف عند حد السرقة، إنما يكون الهدف من ذلك استخدام الأداة المسروقة في عمليات السحب من أجهزة الصراف الآلي أو في الوفاء لدى التجار بأثمان السلع والخدمات.

١- سرقة أداة الدفع: تعتبر جريمة السرقة من أخطر الجرائم التي يمكن أن تقع على الأموال، لأنها تؤدي إلى حرمان صاحب المال منه

بصورة كلية. حيث تتمثل السرقة في نطاق الدفع الإلكتروني من خلال عدة صور:

أ- أخذ أداة الدفع الخاصة بالمستخدم دون إرادته وتحويل الأرصدة المخزنة بداخلها بطريقة احتيالية ويمكن أن تحدث هذه الحالة عندما تسرق البطاقة من خلال السطو على المنازل أو سرقة البطاقة أمام أجهزة الصراف الآلي أو من خلال سرقة المحافظ الشخصية والتي غالباً ما تحتوي على بطاقات الصراف.

وقد كانت البطاقات المسروقة والمفقودة تشكل مشكلة رئيسة على مستوى العالم وخصوصاً في فترة انتشار الماكينات اليدوية - الماكينات التي ظهرت مع بداية انتشار وسائل الدفع الإلكتروني- حيث كانت هذه الماكينات لا تعتمد على الاتصال بل تعتمد على واجهة البطاقة لتخزين معلومات البطاقة، وعندما يتوجه التاجر إلى المصدر لمطالبته بالقيمة يكتشف أن البطاقة التي قبلها مسروقة^١.

أما اليوم ومع انتشار الأجهزة الإلكترونية -والتي يقصد بها استعمال الماكينات الإلكترونية عند التجار- حيث تعتمد هذه الأجهزة على الشريط المغنط الموجود على ظهر البطاقة والمشفّر داخله معلومات البطاقة، والتي تفيد التاجر عند عملية الاتصال عن طريق شبكة عالمية لمعرفة صلاحية البطاقة من خلال تمرير هذا الشريط، الأمر الذي يساعد التاجر في معرفة البطاقة المسروقة بسهولة.

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢٢.

ب- انتشار الأجهزة الإلكترونية في التعامل لا يعني أن عمليات السرقة لوسائل الدفع الإلكتروني لا تحدث إنما ظهر شكل جديد للسرقة يتمثل في سرقة بيانات بطاقة الدفع الإلكتروني. فالأصل أن المصرف يقوم بأخذ التزام من جانب المستخدم بأن لا يقوم بمنح الرقم السري للبطاقة لأي شخص، وذلك باعتبار أن هذا الرقم هو مفتاح القبول لسحب النقود من الحساب وذلك في أجهزة الصراف الآلي. والهدف من هذا الالتزام إنما هو حماية المستخدم من التعرض لعمليات السرقة والاحتيال والاستخدام غير المشروع من قبل الغير. ولكن كثيراً ما يحدث في عمليات الشراء عبر الإنترنت أن يُطلب من المستخدم ملء نموذج إلكتروني ببيانات بطاقته المصرفية (ومن ضمن هذه البيانات الرقم السري)، وبعد أن يحصل على الرقم السري يمكن أن يُستغل هذا الرقم من قبل الهاكرز (مخترقي الشبكة) ومن ثم سرقة الحسابات المصرفية^١. كما أنه بإمكان مخترقي الشبكات (الهاكرز) أن يقوموا باختراق مواقع المصارف الإلكترونية ومن ثم التعرف على أرقام الحسابات المالية للأشخاص وبالتالي سرقة هذه الحسابات.

ولعل خير مثال على عملية السرقة بشكل إلكتروني النزاع الذي عرض على محكمة مدينة أتشينسكي (إقليم كراسنويارسك)، في قضية تتخلص وقائعها أن سيدة روسية ادعت على سيبييريا بنك بأنه تم سحب الأموال من بطاقة الراتب التي تحملها دون علمها بمبلغ ٣١٠٠٠ روبل. وفي اليوم نفسه حدث خصم غير مصرح به من الأموال المملوكة للسيدة بمبلغ ١٣٣٠٠ روبل من بطاقة ماستر التي

^١ فطيمة ميهوبي، جرائم بطاقات الدفع الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيصر - بسكره، الجزائر، ٢٠١٥ - ٢٠١٦، ص ٤٥.

تم فتحها باسمها، حيث تم تحويل هذه الأموال وسرقتها من قبل أشخاص مجهولين. وفي ظل عدم إمكانية تحديد هوية هؤلاء الأشخاص الفاعلين، ادعت السيدة على المصرف بأن السرقة تمت نتيجة خطأ من قبله وذلك على اعتبار أن هذه السيدة لم تقم بأي عمليات على حساباتها من خلال الاتصال بالإنترنت، ولم تمنح البطاقة وكلمات المرور لأشخاص غير معروفين لها.

قضت المحكمة بضرورة إلزام المصرف المذكور بتعويض السيدة عن كافة الأضرار المادية والمعنوية التي أصابها من جراء هذه السرقة استناداً للمبررات الآتية:

- ثبت للمحكمة عدم أمان قناة الموبايل البنكي الذي يحمل الرقم ٩٠٠/ والمستخدم كقناة اتصال بين السيدة والمصرف، وحيث أن شروط العقد تشير إلى موافقة المصرف على تحمل جميع المخاطر المرتبطة بهذه القناة، الأمر الذي يشير إلى أن المصرف يقدم خدمة ذات جودة غير كافية. وبالتالي أصبح الوصول غير قانوني إلى حسابات العملاء من خلال نظام سيبيريا بنك ممكناً.
- إن عبء إثبات الظروف المعفاة من المسؤولية عن الإخفاق في الأداء أو الأداء غير اللائق، وما ينشأ عنه من ضرر، يقع على عاتق المصرف.
- في إطار هذه القضية كان سيبيريا بنك ملزماً بإثبات أنه ضمن خدمة تحويل الأموال، تم اتخاذ التدابير الكافية لضمان أمان البرنامج والأجهزة المستخدمة من قبله ولاستبعاد إمكانية سرقة هذه الأموال، ونفذت العملية المتنازع عليها فقط بسبب انتهاك

السيدة لقواعد السلامة عند استخدام حزمة الخدمات وهذا الأمر لم يتمكن سيبيريا بنك من إثباته. حيث ثبت أن السيدة لم تفقد البطاقات المصرفية والهاتف وبطاقة SIM التي تتصل بها خدمة (MobileBank)، ولم يتم تحويل الهاتف والبطاقة إلى أطراف ثالثة غير معروفة من قبلها.

- يلتزم سيبيريا بنك لضمان سلامة أموال المواطنين، بإنشاء نظام دفع إلكتروني، من شأنه أن يضمن السلامة لأموال العملاء، وبالتالي يجب أن يتحمل خطر وجود نظام دفع إلكتروني غير موثوق، والذي أدى إلى سرقة الأموال من حسابات عملائه^١.

٢- استخدام أداة دفع مسروقة أو مفقودة

تجدر الإشارة إلى أن الأمر قد لا يتوقف على عملية السرقة، بل كثيراً ما يتم طرح الأداة المسروقة في التداول وذلك من خلال استخدام البطاقة في عمليات السحب من أجهزة الصراف أو الوفاء لدى التجار.

إن استخدام الغير لبطاقة الدفع الإلكتروني في هذه الحالة هو استخدام لبطاقة صحيحة صادرة عن الجهة المختصة بإصدارها إلا أنها استعملت من قبل غير حاملها القانوني. ويحصل الغير على بطاقة دفع صحيحة من حاملها الشرعي في حالتين:

^١ القضية رقم ٢-٢٨٧٧/٢٠١٥ تاريخ ١٨ سبتمبر ٢٠١٥ ومتاحة على

الرابط: <https://moluch.ru/archive/184/47356>

تاريخ الزيارة ٢٩/٥/٢٠١٩ الساعة ١٠,٣٠ p.m

الأولى: استخدام الغير للبطاقة بعلم حاملها، وهذا الأمر لا يشكل استخدام غير مشروع كونه برضا الحامل وعلمه إلا أنها تنطوي على إخلال الحامل الشرعي بالتزاماته التعاقدية مع المصدر.

الثانية: استخدام الغير للبطاقة دون علم صاحبها، أي أن الغير قد قام بسرقة البطاقة أو عثر عليها بعد ضياعها وقد يكون عالماً بالرقم السري مع البطاقة أو غير عالم، وفي هذه الحالة يكون الاستخدام استخداماً غير مشروع^١.

وغالباً ما يكون هناك تواطؤ بين الغير الحائز على البطاقة المسروقة أو المفقودة وبين التاجر، إما بقبول الأخير لهذه البطاقة مع علمه بحقيقتها في الوفاء بأثمان السلع والخدمات أو بإصدار فواتير وهمية بموجب هذه البطاقة دون أن يقابلها بضائع أو خدمات.

وبشكل عام يكون استخدام الغير للبطاقة المسروقة أو المفقودة في إحدى حالتين:

أ- استخدام البطاقة المفقودة أو المسروقة في الوفاء لدى التاجر.

غالباً ما يلجأ الغير إلى استخدام البطاقة مستغلاً الفترة بين تاريخ تقديم البلاغ للجهة المصدرة وبين إلغاء التعامل بالبطاقة، وكثيراً ما يلجأ الغير إلى التاجر الذي يتعامل بالأجهزة اليدوية كون الحماية تكون أقل. وعندما يقوم الغير بتقديم البطاقة إلى التاجر وفاءً للمشتريات أو الخدمات، فإنه يقوم بتوقيع الفاتورة إما مقلداً لتوقيع الحامل أو يمحو توقيع الحامل عن البطاقة ويضع توقيعاً بدلاً عنه

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، دار المسيرة، الأردن، ٢٠١٠، ص ١٧٨.

ليتطابق توقيعه على البطاقة مع توقيعه على الفاتورة، وفي هذه الحالة يكون هناك جرم التزوير إلى جانب السرقة^١.

وما تحدثنا عنه آنفاً إنما يتمثل في كون الغير حائز على جسم البطاقة ولكن قد يقوم الغير بسرقة أرقام وبيانات البطاقة فقط دون علم الحامل ودون أن يكون حائز على جسم البطاقة ومن ثم يستخدمها بأحد طريقتين:

- في عملية الوفاء بشكل مباشر: ويتم ذلك بالتواطؤ بين الغير والتاجر وذلك لأن الأخير لا يقبل عملية الوفاء لأي شخص بواسطة بطاقة لم يقم بإيرازها، وتختلف عملية الوفاء هنا في حال استخدام التاجر للجهاز اليدوي أو الجهاز الإلكتروني (P.O.S):

❖ في حال تنفيذ عملية الوفاء بواسطة الجهاز اليدوي: فإن التاجر يحصل على التفويض من الجهة المصدرة بعد أن يعطيها رقم البطاقة وبياناتها، حيث لا يوجد ما يمنع الجهة المصدرة من منح التفويض للتاجر لأن الحامل لم يطلب إلغاء البطاقة كونه لم يعلم بسرقة بياناتها.

❖ أما في حال تنفيذ عملية الوفاء بواسطة الجهاز الإلكتروني: فيستغل التاجر الصلاحية الممنوحة له من المصدر، وهي إمكانية إدخال رقم البطاقة يدوياً إلى الجهاز ويستخرج فواتير وهمية ومن ثم يتقدم بالمطالبة بها إلى المصدر الذي يقوم بدفعها.

^١ المرجع السابق، ص ١٧٨.

ولعل خير مثال على ذلك: قيام موظف في أحد فنادق عمان بإدخال رقم بطاقة تعود لأحد الأشخاص يدوياً على الجهاز الإلكتروني بعد أن حصل على هذا الرقم من أحد أصدقائه الذي قام بسرقة بالرمغ من أن هذا الموظف كان يتقاضى الحساب من نزلاء الفندق نقداً .

- في عملية الوفاء بشكل غير مباشر: وهي الحالة التي يتم فيها الشراء عن طريق الإنترنت وفيها تستخدم أرقام البطاقة دون إبرازها، مما يشكل بيئة مناسبة لاستخدام بيانات البطاقات المسروقة أو المفقودة.

ب- استخدام البطاقة المسروقة أو المفقودة في سحب النقود

ينبغي أن تشير بدايةً إلى أن استخدام البطاقة المسروقة أو المفقودة في سحب النقود يتطلب معرفة الرقم السري وإلا لن يتمكن الحائز من استخدامها. حيث أن إدخال الرقم السري بشكل خاطئ ثلاث مرات يؤدي إلى سحب البطاقة من قبل الجهاز بشكل تلقائي، أما في حال التمكن من معرفة الرقم السري مع البطاقة المسروقة أو المفقودة فيمكن أن يستخدمها بأحد طريقتين:

أ- سرقة البطاقة مع رقمها السري أو العثور عليها مع رقمها السري: وهي من أخطر الحالات، حيث يتمكن الحائز لهذه البطاقة من سحب الأموال من جهاز الصراف الآلي ضمن الحد الأقصى المسموح به للسحب اليومي، وذلك قبل إبلاغ حامل للمصدر عن سرقة البطاقة أو فقدانها.

وتجدر الإشارة إلى أنه في سورية تتم معظم عمليات سرقة بطاقات الصراف العائدة للمصرف العقاري السوري دون توثيق قضائي كون معظم السارقين من أصول أو فروع أو زوج حامل البطاقة حيث كثيراً ما يقوم

الأولاد المراهقين أو الزوجة بسرقة بطاقة الصراف الآلي من آبائهم أو أزواجهم الأمر الذي لا يمكنهم من إقامة دعوى قضائية خوفاً على السمعة إضافةً إلى اعتبارهم مقصرين بالحفاظ على بطاقتهم من خلال منح الرقم السري لغيرهم. ومن الأمثلة العملية على ذلك نذكر^١:

- حدث مرة في فرع المصرف العقاري في محافظة إدلب أن سيدة ادعت على المصرف أن بطاقتها خالية من الرصيد تبين من خلال كاميرا المراقبة أن زوج السيدة قام بسحب المبلغ بعد معرفة الرقم السري.
- حدث مرة في إدارة المصرف العقاري في دمشق أن أحد الأشخاص ادعى على المصرف أن بطاقته خالية من الرصيد تبين من خلال كاميرا المراقبة أن ابنة السيد حامل البطاقة هي من سرقة البطاقة لذلك رفض السيد حامل البطاقة إقامة دعوى وذلك خوفاً على سمعتها وادعى أنه نسي أنه هو من طلب من ابنته سحب النقود من بطاقته.
- كما أنه هناك نوع من سرقة البطاقات والرصيد على أجهزة الصراف الآلي باستخدام بطاقات متعددة، حيث كثيراً ما يلجأ الجاني لاستغلال الأشخاص المتقاعدين وذوي الشهداء فيعرض عليهم المساعدة فيأخذ البطاقة من الشخص المتقاعد ويكون بيده عدة بطاقات ذات شكل واحد. يدخل إحدى البطاقات التي في يده والتي تكون خالية من الرصيد أو مزورة ثم يطلب من الشخص أن يعطيه الرقم السري، يقوم بإدخاله في الجهاز أكثر من مرة ونظراً لعدم توافق الرقم السري مع البطاقة يقوم الصراف الآلي بسحب البطاقة. يخبر الجاني المتقاعد أن بطاقته سحبت من قبل الجهاز بحجة خلل تقني أو خطأ في الرقم السري، يقوم الشخص المتقاعد بمراجعة المصرف ليُفاجئ أن بطاقته ليست هي التي سحبها

^١ أمثلة عملية تم الحصول عليها من خلال جولة ميدانية في المصرف العقاري السوري.

الجهاز إنما بقيت في يد الجاني الذي حصل على الرقم السري مع البطاقة فيقوم بسحب الرصيد ثم يستخدم هذه البطاقة مع شخص آخر وبنفس الطريقة.

وقد تكون عمليات سرقة البطاقات استغلالاً للوضع الأمني ومثال ذلك نذكر:

- تعرض صرافات المصرف العقاري للسرقة بواسطة الجرافات الآلية في مناطق ساخنة (دوما-بابا عمرو-أحياء حلب الشرقية) وسرقة ما تحتويه من نقود.
- القضية التي سرق فيها مبلغ /٢.٥ مليون ليرة سورية/ من أجهزة الصراف الآلي العائدة لمصرف سوريا والمهجر^١.

ب- سرقة رقم البطاقة السري وتشفيره على بطاقة مزورة.

وتعد هذه الحالة أكثر خطورة من الحالة السابقة، كون الحامل لا يعلم بسرقة الرقم السري للبطاقة. وبالتالي لن يقوم بإخطار المصدر لإيقاف التعامل ببطاقته من خلال برمجة جهاز الصراف الآلي لرفض البطاقة في عملية سحب الأموال، ومن ثم يقوم الغير بسحب أموال الحامل دون أن يخشى الإبلاغ عنه. وبشكل عام فإن الغير يمكنه الحصول على الرقم السري لبطاقة الحامل دون علمه بإحدى ثلاث طرق:

- إهمال الحامل. ويتمثل الإهمال في:
- كتابة الرقم السري على البطاقة وتركها في مكان ما.
- ترديد الرقم السري للبطاقة أمام الغير.

^١ راجع الرابط: <http://www.dp.new/com/pages 163768/g1.d>

مشار إليه لدى محمد الباوخ، مخاطر العمليات المصرفية والتأمين عليها، رسالة ماجستير، كلية الحقوق، جامعة دمشق، ٢٠١٦، ص ٥٨.

- إدخال الرقم السري على جهاز الصراف الآلي دون أن يتخذ الاحتياطات اللازمة.

وبنتيجة هذا الإهمال يتمكن الغير من الاطلاع على الرقم السري وحفظه دون أن يقوم بسرقة البطاقة أو دون أن يُشعر الحامل أنه حصل على الرقم السري. ومن الأمثلة العملية على ذلك نذكر:

❖ الواقعة التي حصلت في الأردن وتتلخص في أن أحد الأشخاص أضع أيام عيد الفطر بطاقة الصراف العائدة له والصادرة عن مصرف الإسكان للتجارة والتمويل وكان الرقم السري مكتوب على مغلف البطاقة وبسبب عطلة العيد لم يتم بإخطار المصرف المصدر فعرّ عليها أحدهم وتمكن من خلال البطاقة ورقمها السري سحب ألفي دينار من أربعة أجهزة للصراف الآلي^١.

❖ القضية التي تتلخص وقائعها أنه أثناء قيام صاحبة البطاقة بسحب مبلغ من جهاز الصراف الآلي كانت تردد الرقم السري أمام سائقها فقام هذا الأخير بحفظه، ولدى عودتهما إلى السيارة قام السائق بسرقة البطاقة وسحب مبلغ /٢٧٠٠٠/ درهم.

❖ قضية تتلخص وقائعها أنه بتاريخ ١٦/١١/١٩٩٤ قام أحد الأشخاص في مدينة فرنسية وأثناء تناوله الغداء مع صديقه وبحجة اختبار ذاكرتها طلب معرفة الرقم السري لبطاقته الصادرة عن المصرف الزراعي، وعندما أخبرته به قام بسرقة بطاقتها

^١ مشار لهذه القضية لدى: د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، بحث منشور من قبل المركز القضائي التخصصي، الأردن، ص ٢٦

ومتاح على الرابط: www.cojss.com/article.php?a=219

تاريخ الزيارة ٢٢/٥/٢٠١٩ الساعة ٤,٣٠ p.m

وسحب أموالها مرتين من جهازي صرّاف بمبلغ /١٥٠٠/ فرنك فرنسي في كل مرة ثم أعاد البطاقة إلى مكانها^١.

• **التجسس:** ويتجلى التجسس من خلال:

❖ وضع كاميرات مراقبة على أجهزة الصرّاف الآلي حتى يتمكن الغير من مشاهدة الحامل وهو يقوم بإدخال الرقم السري.

❖ وضع جهاز إلكتروني في مكان خفي على جهاز الصرّاف الآلي ليقوم بنقل الرقم إلكترونياً إلى جهاز آخر لحظة إدخال الحامل لرقمه السري^٢.

• **القرصنة:** وتتمثل القرصنة بالدخول غير المشروع إلى بيانات المصدر المخزنة على أجهزة الكمبيوتر، وذلك لغايات معرفة بيانات المستخدمين والأرقام السرية لبطاقتهم.

ثانياً: فقدان أداة الدفع دون تدخل الغير

كثيراً ما قد يفقد المستخدم أداة الدفع الإلكترونية الخاصة به والنقود المحملة عليها دون أي مصدر أي خطأ من الغير، وإنما يكون نتيجة لإهمال أو سهو أو خطأ من جانب حامل الأداة نفسها. ومن صور هذا الفقدان ما يلي:

١- ضياع البطاقة سواء أكانت ائتمانية أم ذكية كون البطاقة ذات طبيعة مادية ومن الممكن ضياعها.

٢- فقدان الحوافظ الافتراضية المثبتة على أجهزة الحاسب الآلي الخاصة بالمستخدم، كما في حالة تحطم الوسيط المادي كالقرص الصلب لجهاز

^١ مشار لهذه القضايا لدى: د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٨٠.

^٢ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ٢٧.

الحاسب الآلي المثبت على المحفظة أو قيام المستخدم بإلغاء البرنامج الخاص بالدفع عن طريق الخطأ^١.

٣- قيام المستخدم نفسه بتثبيت المحفظة على أكثر من جهاز حاسب آلي، وهذه الحالة خاصة بنظام (PAYCash) حيث أن هذا النظام يفرض على المستخدم تثبيت نسخة واحدة من برنامج الدفع على أحد أجهزة الحاسب الآلي الخاصة به، وإذا أراد أن يثبت نسخة أخرى من ذات البرامج على جهاز حاسب آخر فعليه أولاً إزالة النسخة التي قام بتثبيتها من قبل، ثم يقوم بعد ذلك بتثبيت النسخة الجديدة ويترتب على الإخلال بهذا الأمر إيقاف العمل بالمحفظة وخسارة الأرصدة النقدية المحملة عليها^٢.

ونظراً لأن النقود الإلكترونية في يد المستخدم تماثل النقود التقليدية، تشير نظم النقد الإلكتروني صراحة إلى أنه يترتب على فقدان أداة الدفع الخاصة به خسارة الأرصدة النقدية المخزنة عليها، ولا يمكن استرداد تلك النقود مرة أخرى. ومع ذلك تسمح بعض أنظمة النقد الإلكتروني وفق إجراءات محددة باستعادة الأرصدة النقدية إذا كان فقدان هذه الأرصدة نتيجة تحطم أو تدمير أداة الدفع أو توقفها عن العمل بصفة كلية^٣.

٤- في حال استخدام المستخدم وسائل الإدخال بطريقة خاطئة أكثر من ثلاث مرات متتالية، سترتب على ذلك حجب الاشتراك الخاص به وغلق أداة الدفع وفي هذه الحالة لا بد من اللجوء إلى المصدر لإعادة تفعيل الاشتراك وتغيير هذه الوسائل.

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢١.

^٢ راجع الرابط: <http://www.my pay cash .in/site static/terms condition>.

تاريخ الزيارة ٢٠١٩/٦/٣ الساعة ١٠.١٥ a.m.

^٣ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢٢.

٥- في حال نسيان الحامل للرقم السري، فإنه في هذه الحالة ليس بوسع المصدر تذكيره به وإنما عليه أن يطلب تسليمه بطاقة جديدة موصولة بالرمز السري^١.

٦- في حال إدخال الرمز السري للمرة الثالثة على التوالي بشكل خاطئ، تقوم الآلة بالاحتفاظ بالبطاقة تلقائياً.

وبالنتيجة وفي ختام الحديث عن مشكلة فقدان أداة الدفع كأحد التحديات الأمنية لوسائل الدفع الإلكتروني نجد أن هذه المشكلة قد تحدث بوسائل مشروعة أو وسائل غير مشروعة.

حيث تتمثل الوسائل المشروعة في حالة فقدان دون تدخل الغير (كما في حال ضياع البطاقة نسيان الرقم السري، إدخال الرقم السري بشكل خاطئ). في حين تتمثل الوسائل غير المشروعة بحالة فقدان بتدخل الغير من خلال السرقة التي تصيب وسائل الدفع الإلكتروني سواء أكانت هذه السرقة تقع على البطاقات ككيان مادي أم اقتصرت هذه السرقات على بيانات بطاقة الدفع. وغالباً ما ترافق عمليات سرقة بطاقة الدفع أو سرقة بياناتها استخدام لهذه البطاقة أو لبياناتها بشكل غير مشروع في عمليات الوفاء لدى التجار (وذلك كنوع من التواطؤ بين الجاني والتاجر) أو في السحب من أجهزة الصراف الآلي (وذلك في حال معرفة الرقم السري) وسواء أكانت هذه الاستخدامات في التعاملات العادية أم في التعاملات عبر شبكة الإنترنت. وتجدر الإشارة إلى أن الأمر قد لا يتوقف على سرقة أداة الدفع. بل كثيراً ما يلجأ الجناة إلى تغيير بيانات البطاقات المصرفية أو خلق بطاقات جديدة بهدف تجنب محاولات كشفهم، كما أن هناك جملة من الجرائم الإلكترونية الماسة بنظام الدفع الإلكتروني وهذا مجال بحثنا في المطلب الثاني.

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢١.

المطلب الثاني

القرصنة الإلكترونية

يعتبر الحصول على المكسب المادي هو الدافع الأساسي لارتكاب أي هجوم احتيالي في ميدان وسائل الدفع الإلكتروني، وهذا الأمر يتحقق من خلال خلق وسائل دفع مزيفة مماثلة لتلك الأصلية وتكون مقبولة من قبل المصدر والأطراف الأخرى المتعاملة بهذه الوسائل. ويتم خلق الوسائل المزيفة من خلال تزوير أدوات الدفع الإلكتروني- استخدمنا مصطلح التزوير كمصطلح مجازاً وليس كمصطلح قانوني في هذا الصدد- بمختلف أشكال التزوير (كلي أو جزئي... الخ). والنجاح في إجراء التبادلات التجارية بواسطة الوسائل المزورة مقابل نقود حقيقية من شأنه إلحاق الخسائر المادية في المصدرين والأطراف الآخرين.

غير أن الهجمات على أنظمة الدفع الإلكتروني قد تحدث أيضاً لغايات تخريبية، وذلك عن طريق أعمال تهدف إلى عرقلة هذه الأنظمة والحد من فعاليتها. وتتجلى هذه الهجمات من خلال مجموعة من الجرائم الإلكترونية التي تحدث في نطاق شبكة الإنترنت. وبناءً عليه سوف نتحدث عن تزوير وسائل الدفع الإلكتروني في الفرع الأول ثم ننتقل للحديث عن الجرائم الإلكترونية في الفرع الثاني.

الفرع الأول

تزوير وسائل الدفع الإلكتروني

لعل تزيف العملة من الظواهر الإجرامية التي وجدت في كل مكان، ومنذ أن عرف الناس العملة كوسيلة للتبادل، ظهرت معها عمليات تزوير مرافقة لها، فقد كانت عمليات تزوير العملة المعدنية تتم عن طريق التلاعب في عيارها ووزنها وتقليد الأختام والعلامات التي تحملها والتي تدل على صحتها ورسميتها. ومع ظهور العملة الورقية انتقل الاهتمام إلى تزوير هذه الأخيرة معتمدين على تقليد الأختام والرسوم الخاصة بها، وطباعة عملات مزيفة غير شرعية. أما بالنسبة لوسائل الدفع الحديثة فهي أيضاً غير مستثناة من خطر التزوير، فحداثة تقنياتها وكيفية صنعها لم تمنع المجرمين من البحث عن سبل وأساليب جديدة تتيح لهم إمكانية تزوير هذه الوسائل. وبناءً عليه وفي سبيل الإحاطة بمفهوم تزوير وسائل الدفع الإلكتروني سوف نتحدث عن تعريف التزوير المعلوماتي (أولاً) ثم ننقل للحديث عن أشكال التزوير لوسائل الدفع الإلكتروني.

أولاً: تعريف التزوير المعلوماتي

عرّف بعض الفقهاء التزوير المادي بأنه: «تغيير الحقيقة فيما أعد المحرر لإثباته يؤدي إلى إحداث ضرر وبشرط توفر نية الغش»^(١).

^١ د. محمد علي سالم ود. عباس رزوقي، الأساس القانوني لحماية بطاقة الائتمان من التزوير، بحث منشور في مجلة المحقق للعلوم القانونية والسياسية، المجلد الأول، العدد الثاني، الجزائر، ٢٠١٥، ص ١٢٤.

أما بالنسبة للتزوير المعلوماتي ونقصد به -التزوير في نطاق المعلومات المعالجة إلكترونياً-:

١- على صعيد التشريعات العربية:

نجد أن المشرع المصري تناول التزوير المعلوماتي في قانون التوقيع الإلكتروني حيث جاء فيه: «(زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر. استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك)»^(١).

وبالتالي نجد أن المشرع المصري لم يحدد مفهوم التزوير المعلوماتي بشكل واضح وصريح، وإنما اكتفى بذكر بعض الطرق التي يتم من خلالها التزوير (كالاصطناع أو التعديل) دون أن يفرد أحكام خاصة للتزوير المعلوماتي.

أما بالنسبة للمشرع السوري فقد عرّف التزوير في قانون العقوبات بأنه: «(تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي)»^(٢).

نستنتج من التعريف السابق أن المشرع السوري جاء بتعريف واضح ومفصل للتزوير لكنه اقتصر في تعريفه على المحررات المادية دون الإلكترونية، كما يمكن أن نستنتج من نصوص المواد التي عالجت التزوير أنها اهتمت بالتزوير الواقع على المحررات الرسمية^(٣).

^١ المادة (٢٣/ب-ج) من قانون التوقيع الإلكتروني المصري رقم ١٥/ لعام ٢٠٠٤/.

^٢ المادة ٤٤٣/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

^٣ المواد ٤٤٥ إلى ٤٥١/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

أما بالنسبة للتزوير المعلوماتي فقد نص قانون التوقيع الإلكتروني وخدمات الشبكة على أنه^١:

«مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر نافذ:

يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمائة ألف ليرة سورية إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:

- تزوير أو تحريف توقيع إلكتروني أو بيانات أو منظومة إنشاء توقيع إلكتروني بأي طريقة كانت.
- استعمال توقيع إلكتروني مزوراً أو منظومة إنشاء توقيع إلكتروني محرفة أو شهادة تصديق إلكتروني مزورة مع علمه بذلك».

وبالتالي نستنتج من المادة السابقة أن المشرع السوري لم يذكر تعريف خاص بالتزوير المعلوماتي، وإنما اكتفى بالحديث عن العقوبة المفروضة على من يزور أو يستعمل توقيع مزور أو منظومة إنشاء توقيع مزورة. وهذا الأمر يشكل ثغرة لدى المشرع السوري حبذا لو يتم تلافئها في أقرب تعديل يتناول قانون التوقيع الإلكتروني وخدمات الشبكة -على الرغم من صعوبة وضع تعريف للتزوير المعلوماتي في ظل تطور الوسائل التقنية- وخصوصاً أن انتشار المعاملات الإلكترونية أصبح أمر واقع لا محالة ومن الضروري التنبيه لهذا الأمر ووضع كافة الاحتمالات لمواجهة الجرائم التي ترافق انتشار هذه المعاملات على الرغم .

^١ المادة /٣١/ من قانون التوقيع الإلكتروني وخدمات الشبكة رقم /٤/ لعام ٢٠٠٩.

وفي ظل غياب تعريف تشريعي خاص بالتزوير المعلوماتي سوف نقوم بالتعويل على بعض التعاريف الفقهية.

٢- على صعيد الفقه:

فقد عرّف بعض الفقهاء التزوير المعلوماتي بأنه: «تغيير الحقيقة في المحررات المعالجة آلياً والمحررات المعلوماتية بنية استعمالها»^(١).

في حين اتجه جانب آخر إلى تعريفه بأنه: «تحريف معتمد للحقيقة في الواقع أو البيانات التي يثبتها صك أو مخطوط أو أي مرتكز الكتروني أو أي مرتكز آخر للتعبير يؤلف مستنداً بهدف إحداث ضرر مادي أو معنوي أو اجتماعي»^(٢).

نجد من التعاريف السابقة أنها أخذت بالمفهوم التقليدي للتزوير مع توسيع فكرته بإضافة محل الجريمة (المحررات الإلكترونية)، دون أن تحدد بعض الطرق التي يتم بها التزوير المعلوماتي باعتباره مفهوم جديد يحتاج إلى تحديد بعض الأمثلة عن طرق ارتكابه، كما أغفلت هذه التعاريف توفر نية الغش.

وبناءً على ما سبق نجد أن تعريف التزوير المعلوماتي يتطلب الجمع بين المفهوم التقليدي للتزوير (تغيير الحقيقة بقصد الغش وتوفير الضرر)، والعنصر الإلكتروني في هذه الجريمة (والمتمثل بمحل الجريمة وذكر بعض الطرق التي يرتكب بها هذا النوع من التزوير).

وبالتالي يمكننا أن نعرّف التزوير المعلوماتي بأنه: «تغيير الحقيقة الذي يتم بالاصطناع أو التقليد أو التعديل أو بأي شكل آخر على دعامة إلكترونية، والمرتكب بنية الغش مما من شأنه أن يرتب ضرر»^(٣).

^١ د. محمد علي سالم و د. عباس مرزوقي، مرجع سابق، ص ١٢٥.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢٤.

ثانياً: أشكال التزوير لوسائل الدفع الإلكترونية

يتمثل التزوير في نطاق وسائل الدفع الإلكتروني بشكل عام وفي نطاق بطاقات الدفع الإلكتروني بشكل خاص من خلال أشكال عدة. فقد يكون التزوير كلياً أو جزئياً أو قد يمس الإشعارات والمستندات الخاصة بوسائل الدفع أو قد يمس الماكينات أو البرمجيات الإلكترونية وهذا ما سنعالجه وفقاً للآتي:

١- التزوير الكلي: يكون التزوير الكلي للبطاقة باصطناع كلي للبطاقة كاملة. أي يتم التزوير في المادة المكونة لبطاقة الدفع سواء أكانت مكونات مادية أو إلكترونية. ويتم ذلك:

- عن طريق عمل بطاقة دفع بالكامل، تبدأ بتقليد الطباعة والنقوش والرسوم على البلاستيك، ثم تغليف البطاقة ولصق الهولوجرام، ومن ثم اصطناع الشريط الممغنط بالنسخ أو بالتشفير ولصق الشريط الممغنط وشريط التوقيع، ثم عمل الطباعة البارزة عن طريق إنشائها بمعلومات جرى الحصول عليها بطريقة غير مشروعة، ثم يتم تداول البطاقة واستخدامها في عمليات الشراء^١.
- إذا ما توفر للمزور الرقم السري المتوافق مع بطاقة ما، فإنه يمكن عمل بطاقة بلاستيكية خالية من أية بيانات ويوضع عليها شريط ممغنط بتشفير أو استنساخ بيانات صاحب البطاقة وعمل نسخ عديدة منها، ثم يجري استخدام البطاقة للحصول على أموال من جهاز الصراف الآلي.
- بالنسبة للبطاقة الذكية التي تحمل وحدات إلكترونية يمكن كذلك نسخ المفاتيح التشفيرية، وكذلك الأرصدة المخزنة في البطاقة

^١ المرجع السابق، ص ٣٢٦.

والمعلومات والبيانات الخاصة بها. وتتطوي عملية نسخ البطاقة الذكية الخاصة بالمستخدم على عدد من الخطوات المعقدة التي تقتضي وجود موارد مادية كبيرة، بالإضافة إلى أشخاص على درجة عالية من الكفاءة في هذا المجال. فمن يقوم بعملية النسخ عليه أن يحصل على بطاقة تتمتع بذات مواصفات البطاقة الأصلية من حيث نوع الرقاقة المغروسة، النظام التشغيلي، البرمجيات التطبيقية والبيانات، كما أن المعتدي قد يعيد بناء النظام التشغيلي والبرمجيات التطبيقية من خلال إعادة استخدام بطاقات منتهية الصلاحية^١.

▪ قد يكون التزوير عن طريق سرقة بطاقات كاملة التجهيز المادي من الشركات المنتجة أو من المصارف بواسطة شركاء داخل الشركة أو المصارف، ثم بيعها ومن ثم تزويرها بالطريقة سالفة الذكر.

ومن الظواهر الدالة على التزوير الكلي للبطاقة:

- اختلاف مواصفات شكل وحجم البيانات المطبوعة بالبطاقة المصطنعة عند مقارنتها بنظيرتها الصحيحة.
- عدم دقة لصق الشريط المغنط وشريط التوقيع على ظهر البطاقة حيث من الممكن نزاعها بسهولة بأظافر الإصبع.
- الميل إلى إهمال طلاء الرؤوس البارزة للطباعة النافرة.
- خلو البطاقة المصطنعة من التأمينات غير المرئية والسرية المميزة لنظيرتها الصحيحة.

^١ د. طارق حمزة، مرجع سابق، ص ٢٩٧.

- إمكانية عدم التطابق بين البيانات المشفرة على الشريط المغنط وبين البيانات المقروءة بصرياً والمطبوعة طباعة نافرة.
 - إهمال العلامات الترابطية المميزة لإصدار البطاقة الصحيحة أو الفشل في تقليدها بمواصفاتها المميزة.
 - عند فحص البطاقة وما عليها من نقوش وكتابات، يلاحظ خلوها مما تتسم به نظيرتها الصحيحة من دقة ووضوح وانتظام وتنسيق ويشوبها التقاطعات والتشوهات الطباعية^١.
- ويمكن للمزورين الحصول على المعلومات عن بطاقات الدفع (أرقامها -الجهة المصدرة-تاريخ صلاحيتها...الخ) من خلال عدة طرق:

- تقديم الرشى لموظفي الجهة المصدرة وخاصة العاملين منهم في الأقسام والدوائر ذات الصلة بإصدار البطاقات وتغذيتها أو العاملين كمحاسبين لدى المحلات الكبرى.
- الحصول على المعلومات الخاصة بالبطاقات والتي تتركز بشكل كبير في قوائم حجز الفنادق ووكالات السفر وفي الفواتير التي يتم التخلص منها في سلة المهملات.
- الدخول غير المشروع واختراق قواعد البيانات للكمبيوترات الموجودة لدى الجهات المصدرة بواسطة الانترنت^٢.

ومن الأمثلة على التزوير الكلي نذكر:

- الحادثة التي جرت بين هونغ كونغ وتايوان، حيث اتخذت عصابة إجرامية لنفسها مصنعاً لصناعة البلاستيك في منطقة

^١ فطيمة ميهوبي، مرجع سابق، ص ٤٢.

^٢ د.أ. مجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع

تابعة لمدينة (تائيبي). وبمتابعة أفراد العصابة وجد أنهم بدأوا بشراء التجهيزات المادية اللازمة لإنتاج البطاقة، وهي (الشريط الممغنط وأدوات التصوير وأحبار الطباعة، وآلة لتشفير البيانات على الشريط الممغنط وآلة تغليف للبطاقة). وكانوا يتلقون من متعاونين معهم أسماء وأرقام وشفرات لبطاقات ائتمان أصلية متداولة وينقلون البيانات إلى بطاقات مصنوعة، فيبيعونها إلى منظمات إجرامية لاستخدامها في اليابان وتايوان وهونغ كونغ. حيث ضببت السلطات التايوانية ٣٠٠ بطاقة أمريكيان إكسبريس و ٩٨١ بطاقة ذهبية و ١٥٠٠ بطاقة دائنز كلوب^١.

- من القضايا التي استخدم فيها التزوير على بطاقة مسروقة قضية حصلت في الأردن تتلخص وقائعها أنه بتاريخ ٢٠٠٣/٩/٢ تم القبض على شخص أردني الجنسية بحوزته بطاقة فيزا تم تزويرها بعد سرقتها وتبين أنه قام باستخدامها لدى ثلاث محلات تجارية بالاتفاق معهم وبعلمهم أنها مزورة وقام بسحب مبالغ مالية كبيرة وتقاسمها مع التجار.
- قام أحد الأشخاص بتزوير بطاقة فيزا بواسطة جهاز متطور وقام بتسليمها لشخص آخر الذي قام بدوره بسحب مبالغ مالية كبيرة من خلال استخدام البطاقة في إجراء عمليات بيع وهمية بالاتفاق مع أحد التجار وبعد التحقيق معه تبين أن رقم البطاقة المزورة يعود لبطاقة صحيحة حصل عليه من أحد

^١ د. منظور أحمد حاجي الأزهرى، بطاقة السحب النقدي، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ٣٧٢.

المحلات التجارية وذلك بعد استعادة هذا الرقم المخزن على الجهاز الممغنط من خلال جهاز قارئ وناسخ تم وضعه أصلاً للاحتفاظ بأرقام بطاقات فيزا للأشخاص الذين يشتررون من هذا المحل^١.

٢- التزوير الجزئي: يتمثل التزوير الجزئي من خلال تعديل بعض المكونات المادية أو الإلكترونية لبطاقة الدفع الإلكتروني، واستبدالها بمكونات أخرى تساعد المجرم على استخدام أداة الدفع. أي أن التزوير في هذه الحالة يتناول بعض العناصر وليس جميع العناصر كما في حالة التزوير الكلي. حيث يستفيد المزور في التزوير الجزئي من جسم البطاقة الحقيقية وما عليها من هولوجرام ونقوش وطباعة وكتابة آمنة، ليقوم بتزوير البطاقة بعدة صور نذكر منها:

- صهر الأرقام النافرة الحقيقية أو المنتهية الصلاحية أو إعادة قولبة الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر يتم الحصول عليه بسرقة المعلومات الخاصة بطريقة غير مشروعة.
- تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة صحيحة ومسروقة.
- قد يقوم الجاني بكشط ما على بطاقة الدفع الإلكتروني المسروقة أو المفقودة من شريط توقيع ولصق آخر بدلاً منه والتوقيع عليه بتوقيع يستطيع كتابته بطلاقة.

^١ مشار لهذه القضايا لدى: د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع

- الإبقاء على شريط التوقيع الموجود على البطاقة ولكن تقليد التوقيع الصحيح عند التوقيع على الإيصالات وفواتير الشراء أو المحو الآلي أو الكيميائي للتوقيع الأصلي أو لأجزاء منه^١.
- قد تكون بطاقة الدفع مجهزة بصورة فوتوغرافية لشخص المستخدم، فقد يلجأ الجاني إلى التخلص من هذه الصورة أو تغطيتها ووضع صورة أخرى مكانها إما بالحفر أو باللصق أو الاثنين معاً.
- الحصول على بطاقة دفع صحيحة مسروقة أو منتهية الصلاحية ثم التخلص من البيانات المطبوعة عن طريق تسخينها لدرجة الغليان وضغط الحروف البارزة حتى تختفي، ثم عمل أرقام وبيانات مطبوعة طباعة بارزة بواسطة آلة طباعة، وتشفير البيانات اللازمة بواسطة جهاز تشفير بعد محو ما عليه من بيانات قديمة^٢.
- كما كشفت الممارسات العملية عن طريقة أخرى للتزوير الجزئي وذلك عندما يقوم الغير بالاستيلاء على بطاقة أحد المستخدمين بالسرقة أو بالعثور عليها ثم يقوم بالاتصال هاتفياً مع المستخدم مدعياً أنه موظف لدى المصدر وبأنه سوف يرسل له بطاقة جديدة ولكي يتم ذلك لابد من معرفة رقمه السري فيقوم المستخدم وعن حسن نية بالإعلان عن الرقم السري ويستطيع هذا الغير بعد ذلك التغيير في بيانات البطاقة لتفادي سحبها من جهاز الصراف الآلي

^١ فطيمة ميهوبي، مرجع سابق، ص ٤٣.

^٢ المرجع السابق، ص ٤٣.

أو يمحو البيانات المسجلة على الشريط الممغنط ويستعملها بعد ذلك^١.

ومن الظواهر الدالة على التزوير الجزئي للبطاقة:

- انهيار بعض المواضع من شريط التوقيع، وظهور سطح البطاقة أسفل مواضع الانهيار نتيجة المحو الآلي والكيميائي.
- التشوه أو التقطع الظاهر على أسفل الحافة للهولجرام.
- وجود تسلخات أو بقع سوداء في مناطق الكتابة النافرة، أو عدم انتظام الرؤوس البارزة لهذه الكتابات^٢.
- الاختلاف في المسافات الأمنية للتشكيل الطباعي للأرقام والحروف والصور والأشكال المثبتة على البطاقة المزورة عن البطاقة الأصلية.
- ظهور بقع قاتمة أو بنية أو مصفرة اللون بأرضية شريط التوقيع نتيجة للمحو الكيميائي.
- عدم التصاق حواف الصورة المجسمة الثلاثية الأبعاد.
- عدم التطابق بين البيانات المشفرة على الشريط الممغنط والبيانات المقروءة بصرياً^٣.
- الاختلاف في مواصفات التشكيل الطباعي لأرقام وحروف الطباعة البارزة كما في البطاقات الصحيحة النافرة.

^١ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ٢١.

^٢ فطيمة ميهوبي، مرجع سابق، ص ٤٣.

^٣ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٦٣.

■ إذا كان شريط التوقيع قد تعرض للكشط المادي ثم جرى لصق شريط آخر في مكانه، فإن الشريط المصطنع يفتقر إلى الدقة والثبات وقد يظهر خدوش واتساخ يدل على ذلك، كما قد يظهر سيلان المادة اللاصقة في مواضع حول الشريط المصطنع^١.

ولعل خير مثال على التزوير الجزئي، قيام طالب أمريكي (١٩ عام) وبمهارة عالية بربط جهاز الكمبيوتر بآلة تشفير البيانات على الشريط الممغنط، وقد كان اشترى الآلة بـ (٦٠٠ دولار) من شركة كمبيوتر محلية و تمكن بواسطة الآلة من تزوير العديد من البطاقات حيث تم بيع كل بطاقة بـ (٤٠٠ دولار)^٢.

٣-تقليد الماكينة (ATM):

قد تأخذ جريمة التزوير في نطاق الدفع الإلكتروني شكل آخر جديد وذلك تقليد ماكينة (ATM) نفسها كما حدث في هارت فورد بولاية كونكتيكت الأمريكية. حيث قام المجرمون بتتصيب الماكينة المزيفة بشكل عادي في مجمع تجاري (Mall) وإذا أدخل المستخدمون بطاقتهم فيها خرجت لهم أوراق الإيصالات لتقديم المعذرة عن عدم قبول طلب السحب حالياً مع تسجيل بيانات البطاقة كاملاً بما فيها الرقم السري. وقد استخدمت العصا تلك الأرقام في تصنيع

^١ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ٢١.

^٢ د. رياض فتح الله بصله، جرائم بطاقة الائتمان، ط ١، دار الشروق، مصر، ١٩٩٥، ص ١٠٨.

البطاقات المزورة واستخدموها في ماكينات أخرى في ست ولايات أمريكية وسحبوا بها أموالاً كثيرة^١.

٤- تزوير الإشعارات الخاصة بوسائل الدفع الإلكتروني:

ويتمثل ذلك في عدة صور:

أ- تلاعب موظف المصرف المصدر للبطاقة في بطاقة الدفع وإشعاراتها. ومثال ذلك:

- كأن يتفق الموظف مع حامل البطاقة على إخراج بطاقة سليمة ببيانات مزورة مع علمه بذلك.
- أن يتلاعب موظف المصرف المصدر نفسه من خلال اختلاس مبالغ نقدية من المصرف في حال تقدم حامل البطاقة من أجل السحب أو الإيداع، فيقوم موظف المصرف بتزوير قيمة المبلغ ويأخذ الفارق لنفسه^٢.

ب- تزوير الإشعارات والفواتير الناتجة عن عملية البيع

ويحصل ذلك مع كبار السن حيث يقوم التاجر بخدعهم عند استعمالهم بطاقة الدفع في شراء بعض السلع فيستعمل بصمتهم على إشعار خالٍ من البيانات، ثم يقوم بتعبئته بالمبلغ الذي يريده. أو قيام التاجر بتزوير مبالغ الإشعارات بإضافة مبالغ وهمية على الإشعارات^٣، أو أن يقوم بالتلاعب في تقديم الإشعارات للحصول حيث يقدم الإشعار مرة والصورة مرة أخرى.

^١ د. منظور أحمد حاجي الأزهرى، مرجع سابق، ص ٣٧٣.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢٨.

^٣ المرجع السابق، ص ٣٢٨.

ج- تلاعب التاجر على ماكينات البيع ومثال ذلك:

■ أن يقوم التاجر باستغلال الماكينة اليدوية في الحصول على أكثر من إشعار دون علم صاحب البطاقة، بحيث يكون مطبوع عليها بيانات البطاقة ثم تقليد توقيع حامل البطاقة على تلك الإشعارات لتحصيل قيمتها فيما بعد من المصرف.

■ استخدام بطاقة مسروقة أو منتهية الصلاحية عن طريق العبث بماكينة البيع الإلكترونية والقيام بعملية بيع وهمية، وقيامه بتزوير توابع أصحاب البطاقات على الإشعارات المستخرجة من تلك البطاقات ومن ثم تحصيل قيمة هذه العمليات من المصرف^١.

د- اصدار وسائل دفع صحيحة بمستندات مزورة: يقوم الجناة في هذه الحالة بالتقدم إلى بعض فروع المصرف بمستندات إثبات شخصية مزورة للحصول على بطاقات دفع بأسماء منتحلة وعناوين وهمية، وتستخدم تلك البطاقات بعمليات سريعة ومنتالية. وعادة ما يلجأ محترفو هذا النوع من الجرائم إلى استهداف أكثر من مصرف لإصدار عدة بطاقات وبأسماء وبيانات منتحلة لتحقيق أكبر عائد ممكن، مستغلين بذلك ضعف خبرة بعض موظفي المصرف في كشف التزوير الحاصل على المستندات^٢.

٥- التزوير عن طريق التعديل في البرمجيات الإلكترونية:

ويمكن أن يتجلى التزوير في هذه الحالة من خلال عدة صور نذكر منها:

^١ د. رياض فتح الله بصله، مرجع سابق، ص ١٠٩.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٢٨.

أ-قد يجري التلاعب عن طريق تعديل الوظائف الداخلية للرقاقة الكمبيوترية كالتلاعب بالإجراءات المحاسبية مما قد يؤدي إلى عدم إتمام الحسابات وفقاً لما هو مقرر لها.

ب-تعديل أو نسخ البيانات أو البرمجيات: 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 الإلكترونية ذاتها. أما في أنظمة النقود الإلكترونية ذات البرمجيات، فيمكن تعديل البيانات المخزنة على الوسيلة التي يحوزها المستخدم إذا لم تتوفر لها حماية برمجية خاصة، كما أنه يمكن إجراء تغيير في البرمجيات لتسمح للمستخدم إجراء تعديل للبيانات على نحو غير مشروع^١.

ج- تعديل الرسائل: قد يحاول المزورون تغيير البيانات الخاصة بالوسيلة عن طريق إلغاء الرسائل الإلكترونية أو إعادة إرسالها مجدداً، كما قد يصار إلى إبدال الرسالة الأصلية بالرسالة المعدلة أو مراقبة سير هذه الرسائل بهدف القيام بهجمات تهدف إلى فك التشفير.

د- قد يحصل اعتراض للاتصالات الجارية بين الوسائل من قبل أشخاص غرباء عن الصفقة وذلك حين إرسالها عبر خطوط الاتصال أو من خلال شبكات الكمبيوتر أو من خلال الاختكاك المباشر بين الوسائل. وتجدر الإشارة إلى أن عمليات الاعتراض أو إعادة نقل

^١ د. طارق حمزة، مرجع سابق، ص ٢٩٧.

الرسائل تبدو أوضح في أنظمة الدفع ذات البرمجيات والتي تعتمد شبكة الانترنت في عملها^١.

وهذه الأشكال ليست على سبيل الحصر بل هي أكثر الأشكال شيوعاً، مع العلم بأنه قد يكشف التطور التقني عن وسائل جديدة وأساليب جديدة بالتزوير لم تكن معروفة من قبل. لذلك نأمل من المشرع السوري أن ينتبه لخطورة هذا النوع من التزوير ويعمل على تبويبه بشكل قانوني سليم.

وينبغي أن نشير إلى أن الأمر قد لا يتوقف على حد تزوير وسائل الدفع، بل قد يتجاوز الأمر هذه المرحلة إلى مرحلة أكثر خطورة تتمثل في طرح أداة الدفع المزورة في التداول أو ما يمكن تسميته باستخدام أداة الدفع المزورة سواء في السحب أم الشراء. وفي هذه الحالة نكون أمام آثار مالية واقتصادية خطيرة على المجتمع. (ولكن وفي سبيل توضيح الصورة الخاصة باستخدام أداة الدفع المزورة سوف نرجئ الحديث عنها إلى حين البحث في فكرة مكافحة التزوير كأحد الأساليب العلاجية لهذه المشكلة).

وتأكيداً على خطورة هذا النوع من الجرائم ونظراً لحدائتها سوف نقوم بعرض بعض الأمثلة عن التزوير بهدف اغناء البحث بالأمثلة العملية الكفيلة بتوضيح الصورة حول هذه الجريمة. ومن الأمثلة على ذلك نذكر:

أ- قضية حدثت وقائعها في دبي تتلخص بأنه في عام ٢٠٠٣/ قام مجموعة من الأشخاص من جنسيات عربية وآسيوية بوضع جهاز

^١ المرجع السابق، ص ٢٩٨ - ٢٩٩.

قارئ إلكتروني في فتحة إدخال البطاقة في ستة من أجهزة الصراف الآلي، وتمكنت من خلال هذا الجهاز من تسجيل بيانات مجموعة من البطاقات، وأيضاً عن طريق كاميرا صغيرة الحجم ألصقت في مكان فوق فتحة جهاز الصراف الآلي تم تصوير عملية إدخال الرقم السري وتمكن هؤلاء من إنتاج بطاقات مستنسخة لبطاقات العملاء الأصلية بواسطة جهاز نسخ، ثم قاموا باستخدام هذه البطاقات والرقم السري في سحب أموال المستخدمين من أجهزة الصراف الآلي وقد قدرت الخسارة المبدئية (١.٦) مليون درهم إماراتي^١.

ب- بتاريخ ١٩٩٨/٩/٢٩ تم القبض على مجموعة أشخاص وبحوزتهم بطاقات أمريكيان اكسبريس وفيزا مزورة تبين أنهم حصلوا عليها من خلال تأمين بطاقات فارغة من كندا، وطباعة أرقامها النافرة ومغنطتها بواسطة الآلات الموجودة بحوزتهم والتي أحضروها من أمريكا وتمكنوا بذلك من سحب مبالغ مالية كبيرة^٢.

ج- قضية حصلت في سوريا تتمثل بضبط أشخاص يمتنون تزوير بطاقات الصراف الآلي التي يتقاضى الموظفون بموجبها رواتبهم، مؤكدة أنه تم تزوير عشرات البطاقات بالتواطؤ مع موظفين في المصارف ساعدوهم في الحصول على البيانات الخاصة بهم. وأوضحت المصادر أن المزورين كانوا يستخرجون هذه البطاقات

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٥٨.

^٢ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ١٩.

ومن ثم يتقاضون رواتب الموظفين الذين حصلوا على معلومات تخصهم وخصوصاً الموظفين الذين يعيشون في مناطق ساخنة^١.

وبالنتيجة وفي ختام الحديث عن تزوير وسائل الدفع الإلكتروني باعتبارها أحد المشكلات الأمنية التي تهدد وسائل الدفع، نصل إلى نتيجة مفادها أنه وبالرغم مما تتمتع وسائل الدفع الإلكتروني من مزايا فنية وتقنية إلا أنها لم تتج من عمليات التزوير. حيث ظهر التزوير في نطاق الدفع الإلكتروني بأحد شكلين:

الأول: تزوير أداة الدفع الإلكترونية ومثالها (التزوير الكلي أو الجزئي للبطاقة، تزوير الماكينة، التزوير عن طريق تعديل البرمجيات الإلكترونية) وهو شكل جديد في نطاق التزوير يختلف عن التزوير بالشكل المادي أنتجته الثورة التقنية في قطاع المعلومات والاتصالات.

الثاني: تزوير الإشعارات والمستندات والبيانات المتعلقة بوسائل الدفع مثالها (تزوير الإشعارات، الحصول على أداة الدفع بمستندات مزورة)، وهو شكل مشابه للتزوير المادي (التزوير بالشكل التقليدي) ولا يختلف عنه إلا من ناحية محل الجريمة (المستندات والبيانات الإلكترونية).

وبعد أن تعرفنا على مشكلة التزوير لوسائل الدفع الإلكتروني ننقل للحديث عن بعض الجرائم الإلكترونية الأخرى التي تهدف للمساس بنظام الدفع الإلكتروني.

^١ راجع الرابط: www.damasnow.com

الفرع الثاني

الجرائم الإلكترونية

تواجه وسائل الدفع الإلكترونية جملة من المشكلات التي أدت إلى انعدام الثقة بها. فبالرغم من النجاح والتطور الذي عرفتة الوسائل الحديثة في الدفع إلا أنه هناك جرائم ظهرت وجعلت من نظام الدفع الإلكتروني نظام منقوص. فمع التطور الحديث والسريع للحاسب وشبكة الإنترنت وانتشارها غير المسبوق في كافة المجالات، بدأ يظهر نوع جديد من الجرائم تُسمى الجرائم الإلكترونية (Cyber crime).

ويقتضي تسليط الضوء على هذه الجرائم أن يتم التعريف بهذه الجرائم (أولاً) بغية التعرف على أنواع الجرائم الإلكترونية (ثانياً).

أولاً: تعريف الجرائم الإلكترونية

لقد ظهرت عدة تعاريف للجرائم الإلكترونية سواء على صعيد التشريعات أم على صعيد الفقه نذكر منها:

١- على صعيد التشريعات: بالنسبة للمشرع الأمريكي، فقد عرف مكتب تقييم التقنية هذه الجريمة بأنها: «الجرائم التي تلعب البيانات الحاسوبية والبرامج المعلوماتية دوراً رئيساً فيها»^(١).

يُلاحظ على التعريف السابق أنه جاء بشكل مبهم وغير واضح، بحيث لم يبين المعيار الذي اعتمده كما أنه لم يحدد الآثار المترتبة على هذه الجرائم.

^١ مشار إليه لدى: رائد يوسف، مرجع سابق، ص ١١٦.

أما بالنسبة للمشرع الفرنسي فقد عرف الجريمة الإلكترونية بأنها: (الكل من توصل لنظام المعالجة الآلية للبيانات بطريق التحايل ويُقصد بالتحايل التدخل غير المشروع، بحيث يترتب على هذا الدخول غير المشروع محو البيانات أو تعديل البيانات أو تعطيل نظام التشغيل^(١)).

نستنتج من التعريف السابق أن المشرع الفرنسي أخذ بمعيار موضوعي في تعريفه وهو محل الجريمة (الدخول غير المشروع لنظام معالجة البيانات)، كما أنه حدد الآثار التي تترتب على مثل هذه الجرائم (محو البيانات أو تعديلها أو تعطيل نظام التشغيل)، ولكن يُنقَد التعريف كونه اقتصر على معيار محل الجريمة فقط دون معيار الوسيلة الإلكترونية المستخدمة.

أما بالنسبة للمشرع السوري فقد عرف الجريمة المعلوماتية بأنها: (جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة^(٢)).

في الحقيقة ليس هناك من أي فارق بين الجريمة المعلوماتية والجريمة الإلكترونية وذلك على اعتبار أن كلاهما يتم في البيئة الإلكترونية، وتجدر الإشارة إلى أن المشرع السوري كان موفقاً في التعريف السالف الذكر كونه لم يقتصر على معيار محدد بل أخذ بمعيار الوسيلة الإلكترونية المستخدمة (ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة)، كما أخذ بمعيار موضوعي محل الجريمة (تقع

^١ المادة ٢/٤٦٢ من القانون الخاص بالجرائم المعلوماتية رقم ١٩-٨٨/ تاريخ ٥/يناير/ ١٩٨٨ والمعدل بموجب قانون العقوبات الفرنسي بتاريخ ١/مارس/ ١٩٩٤.

^٢ المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

على المنظومة المعلوماتية أو الشبكة)، وبذلك يكون قد وسّع كثيراً من نطاق الجريمة وجعلها تشمل أي جريمة حديثة قد يكشف عنها التطور التقني، إضافةً إلى شمولها للجرائم التقليدية فيما لو ارتكبت بوسيلة إلكترونية. ولكن ينتقد التعريف السابق كونه أغفل الإشارة بشكل صريح لضرورة أن يكون مرتكب هذه الجريمة شخص ذو خبرة وإن كان السياق الطبيعي لهذه الجرائم يفترض ذلك .

٢- على صعيد الفقه:

اتجه جانبٌ من الفقه إلى تعريف الجريمة الإلكترونية بأنها: «الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته للحاسب بعمل غير قانوني»^(١).

يُنتقد التعريف السابق كونه جاء مبهم وغير واضح، بحيث لم يبين المعيار الذي اعتمده فمجرد أن يكون شخص ذو معرفة بالحاسب لا يمثل معياراً كافياً لتحديد مفهوم الجريمة الإلكترونية، فأن يكون الشخص ذو خبرة عنصر أساسي في ارتكاب الجريمة لكنه ليس كافياً لتحديد مفهومها.

في حين اتجه جانبٌ آخر إلى تعريف الجريمة الإلكترونية بأنها: «الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال

^١ عمار لوصيف، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين مع الإشارة إلى التجربة الجزائرية، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، الجزائر، ٢٠٠٨ - ٢٠٠٩، ص ١١١.

بالإنترنت ويكون هدفها اختراق الشبكات والتحريف والتزوير والاختلاس والقرصنة وسرقة حقوق الملكية الفكرية^(١).

يعتبر هذا التعريف من أفضل التعاريف الفقهية كونه أخذ بمعيار الوسيلة ومعيار محل الجريمة، كما أنه جاء ببعض الأمثلة على هذه الجرائم. ولكنه أغفل الإشارة بشكل صريح إلى صفة مرتكب الجريمة وهي أن يكون ذو خبرة في ارتكاب هذه الجريمة.

وبناءً على ما سبق نرى أنه حتى يكون تعريف الجريمة الإلكترونية تعريف جامع مانع لا بد من توفر عدة أمور:

أ- أن يتم الأخذ بمعيار الوسيلة ومعيار محل الجريمة بهدف توسيع نطاق الجريمة لأكبر حد ممكن.

ب- أن يتم ذكر عنصر الشخص المحترف ذو الخبرة التقنية بشكل صريح.

ج- أن يتم ذكر بعض الآثار المترتبة على هذه الجرائم على سبيل المثال لا الحصر.

وبالتالي يمكننا أن نعرف الجريمة الإلكترونية بأنها: ((الجريمة التي لا تعرف الحدود الجغرافية، وترتكب بواسطة شخص ذو خبرة تقنية، وباستخدام الوسيلة الإلكترونية (كشبكة الإنترنت، الهاتف الجوال)، أو أنها تقع على المنظومة المعلوماتية، بهدف إلالتها أو تعطيلها أو تخريبها أو غير ذلك من الأعمال غير المشروعة)).

^(١) خديجة سلطاني، إحلال وسائل الدفع التقليدية بالوسائل الإلكترونية - دراسة حالة بنك الفلاحة والتنمية الريفية BADR - بوكالة بسكرة، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خبصره - بسكرة، الجزائر، ٢٠١٢ - ٢٠١٣، ص ١١٤.

ثانياً: أنواع الجرائم الإلكترونية

يمكن تقسيم الجرائم الإلكترونية إلى نوعين رئيسيين:
النوع الأول: يعتمد على معيار الوسيلة الإلكترونية، ويُقصد به الجرائم التي ترتكب باستخدام الوسيلة الإلكترونية.
النوع الثاني: يعتمد على معيار محل الجريمة، ويُقصد به الجرائم التي تمس منظومة المعلومات الإلكترونية. وسوف نبحث في كلا النوعين على النحو الآتي:

١- الجرائم التي تُرتكب باستخدام الوسيلة الإلكترونية.

ينبغي أن نشير بدايةً إلى أن معظم هذه الجرائم عبارة عن جرائم تقليدية، لكن دخول الوسيلة الإلكترونية كأحد أساليب ارتكابها أكسبها صفة الجرائم الإلكترونية. مع العلم أن دراستنا في هذا المجال سوف تقتصر على الجرائم ذات الصلة بعمليات الدفع الإلكتروني دون غيرها من الجرائم نظراً لتعدد أنواع هذه الجرائم وصعوبة حصرها. وتتمثل الجرائم التي تُرتكب باستخدام الوسيلة الإلكترونية في نطاق الدفع الإلكتروني فيما يلي:

أ- جرائم الاحتيال بالوسائل الإلكترونية: ويُقصد بها كل تصرف احتيالي يهدف من خلاله أحد المجرمين تحقيق مكاسب مالية عبر الوسائل الإلكترونية (كسحب الأموال من حساب أحد الأشخاص لدى المصرف أو القيام بتسديد الفواتير على حساب شخص آخر). و تتم هذه الجريمة بطريقة الهاتف الخليوي حيث تتم بواسطة تقنية (VISHING) وهي طريقة مبرمجة لإرسال رسائل معينة إلى جميع حملة الهواتف الخليوية التابعة لشركة معينة يكون نصها كالتالي: [بغرض تحسين الخدمة

المقدمة لكم من المصرف يُرجى تزويدنا بأرقام حساباتكم والرقم السري على الرقم التالي.....^١. فهناك مَنْ يقع في مصيدة المجرم ويقوم بإرسال البيانات ليقوم المجرم باستخدام هذه البيانات لإفراغ الحساب من أمواله أو استخدامها لأغراض إجرامية أخرى. ومن القضايا الشهيرة في الاحتيال الإلكتروني قضية توسون التي حصلت مع أحد مصارف الكويت، وتتخلص أحداثها بزرع برنامج في جهاز الكمبيوتر الرئيس للمصرف ليقوم بعملية التحويل المالي من حسابات بعض المستخدمين إلى حسابات قام المتهم بفتحها بنفس المصرف، ولم يتم عمل البرنامج إلا بعد مغادرته الكويت وتركه للعمل. وما أن وصل إلى بريطانيا حتى قام بتوجيه رسالة إلى المصرف لتحويل هذه المبالغ من الحسابات التي قام بفتحها إلى حساباته في بريطانيا، إلا أن الشرطة البريطانية تنبّهت لذلك وتم القبض عليه واتهامه بالحصول على الأموال بواسطة الاحتيال الإلكتروني.^٢

ب- السلب بالقوة الإلكترونية: حيث يتم استخدام الحاسب بالتلاعب بالمعلومات وذلك من خلال إدخال بيانات زائفة من جانب المتحايل، باختلاق دائنين بأجور يجب دفعها أو فواتير يجب سدادها أو باختلاق مدينين غير حقيقيين يجب عليهم سداد فواتير صادرة عن الحاسب.^٣

^١ عماد الدين عبد الحليم، المعاملات المصرفية بواسطة الهواتف النقالة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط للدراسات العليا، الأردن، ٢٠١٠، ص ٥١.

^٢ المرجع السابق، ص ٥٢.

^٣ عمار لوصيف، مرجع سابق، ص ١١٤.

ج- انتحال شخصية المتعامل الشرعي بالبيانات: وتتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية المجرم لتسهيل ارتكابه جرائم أخرى.. ويمكن أن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في المصرف أو السحب من البطاقات الائتمانية، وكثيراً ما يقوم المجرم بتغيير العنوان البريدي للضحية إلى عنوانه كي يستقبل بنفسه الفواتير والمطالبات.

كما يمكن للانتحال أن يمس بشخصية المواقع، ويقوم الفاعل بهذه الجريمة من خلال وضع نفسه في موقع بيني (بين البرنامج المستعرض للحاسب الخاص بأحد مستخدمي الانترنت و موقع web). ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي ويستطيع مراقبة أي معلومة متبادلة بين الضحية وبين الأشخاص الزائرين لهذا الموقع. كما بإمكانه سرقة هذه المعلومات وتغييرها^١.

د- الجرائم المالية الإلكترونية : وهي عبارة عن الجرائم التي تسبب أضرار مالية للشخص المستهدف من هذه الجرائم. وتأخذ الأشكال الآتية:

- عملية السرقة الإلكترونية وذلك من خلال نسخ البيانات الإلكترونية لبطاقات الصراف الآلي ثم استخدامها لسرقة أموال من حساب الضحية.

^١ المرجع السابق، ص ١٢٤.

- إنشاء صفحة إنترنت مماثلة جداً لموقع أحد المصارف الكبرى لتطلب من المستخدم إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقته.^١
- رسائل البريد الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي.^٢

٢- الجرائم التي تمس منظومة المعلومات الإلكترونية

وهي عبارة عن مجموعة من الجرائم الجديدة التي كشف عنها التطور التقني. وتتمثل هذه الجرائم في نطاق التعامل بالدفع الإلكتروني بالآتي:

- أ- **الالتقاط غير المشروع للبيانات:** يقصد به كل دخول غير مشروع إلى نظام معلوماتي معين (كالنظام الخاص بالمصارف أو التجار) بهدف التقاط البيانات الشخصية للمتعاملين عبر قنوات الاتصال. وغالباً ما يتم الالتقاط غير المشروع للبيانات بعدة طرق نذكر منها:
- أ- **التجسس المعلوماتي:** ويتمثل هذا الأسلوب في قيام قراصنة الإنترنت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الإنترنت.^٣

^١ خديجة سلطاني، مرجع سابق، ص ١١٥.

^٢ المرجع السابق، ص ١١٥.

^٣ رائد يوسف مرجع سابق، ص ١٢٢.

ب- الاحتيال (الخداع): ويتم الاحتيال عن طريق اعتراض بريد إلكتروني (E-mail) إذا كان هذا البريد يتضمن بيانات متعلقة بأرقام حساب مصرفي أو أرقام بطاقة ائتمان أو بيانات أخرى.

ج- النقاط كلمات السر: عن طريق تخمين هذه الكلمات مستفيدة من ضعف الكلمات عموماً أو شيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أو محيط العمل أو حياتهم الشخصية.^١

ب- الجرائم التخريبية: وهي الجرائم التي تستهدف تخريب البيانات والمعلومات بهدف تعطيلها عن العمل وإتلافها. وتتمثل في الآتي:

أ- اختراق الأنظمة: ويتحقق ذلك بدخول شخص غير مخول بذلك إلى نظام الكمبيوتر والقيام بأنشطة تخريبية غير مصرح له فيها، بهدف إتلاف محتويات النظام أو تعديل البرمجيات التطبيقية أو سرقة البيانات السرية.^٢ ويتحقق هذا الاختراق من خلال:

- أنشطة التخفي ويراد بها تظاهر الشخص المخترق بأنه شخص آخر مصرح له بالدخول.
- استغلال نقاط الضعف في النظام كتجاوز إجراءات الحماية.
- المعلومات التي يجمعها الشخص المخترق من مصادر أخرى، كالنتقيب في سلة المهملات للحصول على كلمات السر أو معلومات عن النظام.

^١ المرجع السابق، ص ١٢٣.

^٢ عماد الدين عبد الحليم، مرجع سابق، ص ٥٢.

ب-تصميم البرمجيات الخبيثة: يُقصد بالبرمجيات الخبيثة البرمجيات الحاسوبية المصممة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الإلكترونية أو الشبكة أو تعطيل عملها أو إبطائها أو تخريب محتوياتها أو مواردها أو جمع معلومات عنها أو عن مالكيها أو مستخدميها أو عن بياناتهم دون إذنهم أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بصورة غير مشروعة^١.

ومن الأمثلة على استخدام الفيروسات ما حدث في عام ٢٠٠٠/ عندما استطاع أحد الهواة اختراع فيروس /I love you/ والذي تمكن من إيقاع خسائر لا يمكن حصرها في ذلك الوقت. وقد كان الفيروس يعمل كقنبلة موقوتة، حيث يُفعل في تاريخ محدد بالسنة /١٤ شباط/ وكان الحل الوحيد لتفاديه أن يتم إغلاق النظام بالكامل في ذلك التاريخ^٢.

ج-زراعة نقاط الضعف: بحيث يقوم شخص غير مصرح له بزرع مدخل ما يحقق له الاختراق فيما بعد. ومن أمثلة ذلك حضان طروادة كأن يستخدم برنامج معالجة كلمات ظاهرياً بالتحريير والتنسيق للنصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي، بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتوياته^٣.

^١ المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ رشيد علام، عوائق تطور التجارة الإلكترونية في الوطن العربي/دراسة حالة الجزائر/، رسالة ماجستير، الأكاديمية العربية البريطانية للتعليم العالي، قسم إدارة الأعمال، بريطانيا، ٢٠٠٩ - ٢٠١٠، ص ٩٩.

^٣ الأعمال الإلكترونية وأمن المعلومات، مرجع سابق، ص ٥٨.

د-البريد الواغل: يقصد به أي شكل من أشكال الرسائل مهما كان محتواها والتي ترسل على الشبكة إلى الغير دون رغبة المتلقي في وصولها إليه^١. ويهدف البريد الواغل إلى عدة أغراض مثل الدعاية والإعلان أو بهدف خداع المستخدم لتقديم معلومات حساسة أو شخصية أو لإغراق الشبكة أو موقع إلكتروني أو منظومة معلوماتية^٢، كما قد يهدف في نطاق التعاملات الإلكترونية إلى ارتكاب أعمال غير مشروعة تتمثل في الآتي:

- **إنكار الخدمة:** حيث يتم إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة إلى موقع معين ، فتؤدي إلى اكتظاظ الخادم وعدم قدرته على التصرف.
- **عدم الإقرار بالقيام بالتصرف:** ويتمثل ذلك من خلال إرسال رسالة كاذبة تهدف إلى عدم إقرار الشخص المرسل أو المرسل إليه بالتصرف الذي صدر عنه^٣.

ج- **جرائم التجسس:** وهي عبارة عن مجموعة من الجرائم الهادفة إلى جمع المعلومات السرية للمستخدمين بهدف نشرها أو استخدامها بشكل غير مشروع. ويمكن أن نجمل هذه الجرائم في الآتي:

أ- **مراقبة الاتصالات:** بهدف جمع المعلومات السرية عن الأشخاص وغالباً ما تكون هذه المعلومات هي التي تسهل له مستقبلاً اختراق الأنظمة.

^١ المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادرة بالقرار رقم ٢٩٠/ لعام ٢٠١٢/.

^٣ الأعمال الإلكترونية وأمن المعلومات، مرجع سابق، ص ٥٨.

بـ-اعتراض الاتصالات: وذلك من خلال قيام الجاني بخلق نظام وسيط وهمي يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي^١ مما يمكنه من الحصول على هذه المعلومات كالأرقام السرية للبطاقات.

وفي ختام الحديث عن الجرائم الإلكترونية نصل إلى نتيجة مفادها أن الوسيلة الإلكترونية بشكل عام وأجهزة الكمبيوتر بشكل خاص تلعب أحد دورين في نطاق هذه الجرائم:

الدور الأول: قد تكون الوسيلة الإلكترونية أداة الجريمة ومثال ذلك (الاحتيال بالوسائل الإلكترونية، السلب بالقوة الإلكترونية، انتحال شخصية المتعامل الشرعي، أي جريمة تقليدية ترتكب بوسيلة إلكترونية كالجرائم المادية والجرائم الجنسية).

الدور الثاني: فقد تكون المنظومة الإلكترونية محلاً للجريمة ومثالها (الانقراط غير المشروع للبيانات، الجرائم التخريبية، جرائم التجسس). وأمام هذه التحديات والمشكلات الأمنية تبرز الحاجة الملحة للحديث عن السبل الكفيلة بمعالجتها بغية السماح بنجاح انتشار هذه الوسائل وتطويرها وهذا ما سوف نبينه لاحقاً.

بعد أن تعرفنا على المشكلات التي تصيب أداة الدفع الإلكترونية باعتبارها كيان مادي وتقني، ننقل للحديث عن الشكل الآخر من المشكلات الأمنية والتي تنشأ نتيجة استخدام أداة الدفع الإلكترونية وتتمثل بالمشكلات الناشئة عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية.

^١ المرجع السابق، ص ٥٩.

المبحث الثاني

المشكلات الناشئة عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية

تعتبر بطاقات الدفع الإلكترونية من أكثر وسائل الدفع الإلكتروني استعمالاً في الوقت الحاضر حيث تسعى المصارف من خلالها لترقية مستقبل النقود الإلكترونية، إلا أن انتشار هذه البطاقات وتزايد حجم التعامل بها صاحبه نمواً مضطرباً في الجرائم ولاسيما الاستخدام غير المشروع لهذه البطاقات.

وبين بعض الفقه^١ أنه: «عندما يخل الحامل بشروط عقد إصدار البطاقة، يؤدي هذا إلى فسخ العقد أو قفل الحساب الذي تقوم البطاقة بتشغيله، حيث يسأل الحامل جنائياً لمجرد امتناعه عن رد البطاقة أو استمراره في استخدامها بعد إلغائها من قبل المصرف المصدر لها، أو استمراره في استخدامها بعد انتهاء مدة صلاحيتها».

يُنقَد الرأي السابق لجهة محدوديته، فقد اقتصر على حالة وحيدة فقط من حالات الاستخدام غير المشروع (الاستخدام غير المشروع من جانب الحامل فقط)، مع العلم أن الاستخدام غير المشروع يكون من قبل التاجر أو المصدر أو حتى من قبل الغير.

لذلك فإننا نرى أنه من الأفضل عدم وضع مفهوم محدد للاستخدام غير المشروع لبطاقة الدفع الإلكترونية، وذلك على اعتبار أن الاستخدام غير المشروع هو عملية معقدة ومركبة لا يمكن معرفتها إلا من خلال بيان نقيضها (الاستخدام المشروع). فحالات الاستخدام

^١ رائد يوسف، مرجع سابق، ص ١٢٦.

غير المشروع هي حالات متعددة ومختلفة باختلاف الشخص مرتكب الفعل، كما أن هذه الحالات تتطور بتطور وسائل حماية البطاقة فقد تظهر حالات للاستخدام غير المشروع في المستقبل قد لا تكون معروفة في الوقت الحالي. وبالتالي فإن تحديد الاستخدام المشروع للبطاقة من شأنه أن يساعد على معرفة الحالات التي يكون فيها الاستخدام غير مشروع.

حيث يُعرّف الاستخدام المشروع بأنه: «الاستخدام الذي يتم بواسطة الحامل الشرعي والبطاقة صحيحة وفي الغرض المخصص لها وفي حدود سقفها»^١.

نستنتج من التعريف السابق أن شروط الاستخدام المشروع للبطاقة هي الآتي:

- أن يكون استخدام البطاقة من قبل حاملها الشرعي.
- أن تكون البطاقة صحيحة وغير مزورة أو تم التلاعب بها.
- أن يكون استخدام البطاقة خلال مدة صلاحيتها وفي حدود سقفها.

• أن يكون استخدام البطاقة في حدود الغرض المخصص لها.

وبالتالي فإن أي استخدام لبطاقة الدفع الإلكترونية لا تتوفر فيه الشروط السابقة يخرج من نطاق الاستخدام المشروع ويدخله في دائرة الاستخدام غير المشروع. وقد تمارس بعض طرق الاستخدام غير المشروع لبطاقة الدفع الإلكترونية من قبل أطراف البطاقة ذاتها (الحامل، التاجر، المصدر)، أو قد تمارس من قبل الغير سواء أكان هذا الاستخدام غير المشروع في عمليات السحب من أجهزة الصراف

^١ المرجع السابق، ص ١٢٧.

الآلي أم في الوفاء لدى التجار. وسواء أتم الدفع للتاجر بواسطة البطاقة مباشرة أم من خلال شبكة الإنترنت.

وبناءً على ما تقدم وفي سبيل تسليط الضوء على الاستخدام غير المشروع لبطاقة الدفع الإلكتروني سوف نتحدث عن الاستخدام غير المشروع من قبل أطراف البطاقة وذلك في المطلب الأول ثم ننتقل للحديث عن الاستخدام غير المشروع من قبل الغير وذلك في المطلب الثاني.

المطلب الأول

الاستخدام غير المشروع من قبل أطراف البطاقة

قد تستخدم البطاقة استخداماً غير مشروع من قبل أطرافها. ويقصد بهم أطراف عملية الوفاء بالبطاقة وهم الحامل الشرعي للبطاقة، والتاجر الذي يقبل التعامل بالبطاقة في الوفاء، والمصرف مصدر هذه البطاقة. وتجدر الإشارة إلى أن الاستخدام غير المشروع لا يقع من قبل المصرف ككيان اعتباري وإنما يقع هذا الاستخدام من قبل الموظفين لدى هذا المصرف. لذلك وفي سبيل التعرف على هذه الحالات من الاستخدام غير المشروع سوف نتحدث عن الاستخدام غير المشروع من قبل الحامل في الفرع الأول، على أن نتعرف على الاستخدام غير المشروع من قبل التاجر وذلك في الفرع الثاني. وأخيراً نتحدث عن الاستخدام غير المشروع من قبل موظفي المصدر في الفرع الثالث.

الفرع الأول

الاستخدام غير المشروع من قبل الحامل

يُقصد بحامل البطاقة الشخص الذي حصل عليها من المصرف وفقاً لشروط محددة في استخدامها، وبمقتضى اتفاق بينهما وهذا الاتفاق يسمح لحامل البطاقة بشراء السلع والخدمات أو السحب من أجهزة الصرّاف. وبموجب هذا الاتفاق مع المصرف يلتزم الحامل:

- بعدم تجاوز الحد المضمون من قبل المصدر سواء في السحب أم في الوفاء.
- برد البطاقة الملغاة أو منتهية الصلاحية.

غير أن الحامل الشرعي للبطاقة قد يعمل على الإخلال بهذين الالتزامين على النحو الذين يجعل من استخدام هذه البطاقة استخداماً غير مشروع. ويتجلى الاستخدام غير المشروع من قبل الحامل على النحو الآتي:

أولاً: الاستخدام غير المشروع للبطاقة خلال فترة صلاحيتها.

بالرغم من أن بطاقة الدفع الإلكترونية صالحة للاستعمال ورغم أن مستعملها هو من صدرت باسمه إلا أنه يتصور أن تستخدم بصورة غير مشروعة من قبل حاملها ويتخذ ذلك أحد صورتين:

١- الوفاء بقيمة المشتريات بالرغم من عدم وجود رصيد كافي.

تخول بطاقات الدفع الإلكترونية حاملها إمكانية استخدام هذه البطاقات كوسيلة للوفاء بقيمة المشتريات لدى التجار المعتمدين، من أجل الحصول على السلع والخدمات التي يرغب بها الحامل ودون الحاجة

لحمل النقود التقليدية. حيث يقوم المصرف المصدر بموجب الاتفاقيات الناشئة عن البطاقة، بسداد قيمة المشتريات التي حصل عليها الحامل على أن تعود الجهة المصدرة على الحامل بقيمة ما سدده للتاجر وذلك من خلال عملية الخصم من حساب الحامل. وبالتالي يتحتم على التاجر أن يحصل على التفويض من قبل مصدر البطاقة عن أي عملية بيع ومهما كان مبلغها. لذلك يبدو صعباً على الحامل تجاوز سقف البطاقة في عمليات الوفاء وذلك على اعتبار أنه إذا قِيلَ التاجر البطاقة دون الحصول على التفويض فإنه يتحمل مسؤولية ذلك هذا بالنسبة للأجهزة اليدوية. أما بالنسبة للأجهزة الإلكترونية (P.O.S) فالأمر قد يكون غاية في الصعوبة وذلك على اعتبار أن الجهاز الإلكتروني يحدد مقدار سقف البطاقة وكفاية رصيد الحامل عند تمرير البطاقة^١.

وعلى الرغم من التسليم بصعوبة تجاوز السقف المحدد للبطاقة في حال الوفاء، فقد كشفت الممارسات العملية عن قيام الحامل للبطاقة بتنفيذ مشتريات تتجاوز الحد المسموح به بسوء نية وهو يعلم بعدم كفاية حسابه في السداد أو يقوم بهذا التجاوز بنية عدم السداد ولا يتم تصحيح الوضع بتغطية قيمة التجاوزات. ففي إحدى الوقائع التي حدثت في مصر قدم أحد أصحاب الفنادق مطالبة لمصرف مصر بمبلغ ربع مليون دولار. فقام المصرف برفض المطالبة لأن البطاقة المسحوبة والعائدة لأحد رعايا دول الخليج مرفوضة عند وضعها في الجهاز الإلكتروني لعدم وجود رصيد. وعند التدقيق في البطاقة من

^١ عمار لوصيف، مرجع سابق، ص ١١٥.

قبل المصرف لمعرفة كيف تم تحويل المبلغ من حساب المستخدم لحساب التاجر، وجدوا أن تمرير البطاقة لأكثر من عشرة مرات ورفضها من قبل الجهاز الإلكتروني وإعادة تمريرها بعد ذلك يؤدي إلى قبولها من قبل الجهاز. وقد ثبت أن صاحب الفندق قام بهذه العملية مئات المرات حتى استطاع جمع المبلغ. ولدى الاستفسار من شركة فيزا العالمية أفادوا بأنهم وضعوا هذا النظام في الجهاز لكي يسمح بقبول البطاقة بعد رفضه إياه لأكثر من مرة ظناً منهم أن الحامل الذي يقوم بالتكرار كان مضطراً للشراء^١، ولكن في الحقيقة كانت النتيجة عكس ذلك وأصبحت هذه الميزة تستخدم بشكل غير مشروع من قبل الحامل.

٢- السحب من جهاز الصراف بالرغم من عدم وجود رصيد كافٍ

تقوم بطاقات الدفع الإلكترونية بالإضافة لوظيفة الوفاء بوظيفة السحب، بحيث تسمح لحاملها الشرعي بسحب النقود من أجهزة الصراف الآلي بواسطة استخدام الرقم السري وفي حدود القيمة المسموح بها من قبل الجهة المصدرة. وقد يحاول حامل البطاقة التعسف في استخدامه لهذه البطاقة ويقوم بتجاوز المبلغ المتفق عليه في السحب إلا أن جهاز الصراف الآلي معد بتعليمات من الجهة المصدرة وبالتالي لن يسمح بالصرف في هذه الحالة^٢.

^١ مشار لهذا المثال لدى: د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع

لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٣٢.

^٢ فطيمة ميهوبي، مرجع سابق، ص ٣٤.

وعلى الرغم من التقنيات العالية لأجهزة الصرّاف فقد كشفت الممارسات العملية عن إمكانية قيام الحامل الشرعي للبطاقة بالتصرف بسوء نية، فيعمل على استخدام البطاقة لدى أجهزة الصرّاف الآلي سواء بالطريقة المعتادة أو بالتلاعب في معطيات الجهاز وسحب مبالغ نقدية تتجاوز الرصيد الموجود في حسابه لدى المصرف المصدر. الأمر الذي يشكل إخلالاً بالالتزام العقدي الذي يربط المصدر بحامل البطاقة، وخاصةً إذا لم يتم الأخير بتصحيح وضعه من خلال تغطية قيمة السحوبات المتجاوز فيها.

ومن الحالات التي يتم فيها سحب الأموال من أجهزة الصرّاف من قبل الحامل متجاوزاً رصيده. هي الميزة التي تمنحها المصارف الأردنية لحملة بطاقة الفيزا الصادرة عنها عند استخدامها خارج الأردن- وهو ما يمكن تسميته قانوناً بالقرض أو الائتمان أو الاعتماد- ، حيث يمكنهم مراجعة أجهزة الصرّاف الآلي التابعة لأي مصرف من المصارف الأجنبية المتعاقدة وسحب ما مقداره ٤/ أضعاف رصيدهم. وذلك تقديراً من هذه المصارف أن حامل البطاقة في الخارج قد يحتاج لأموال تتجاوز رصيده^١. الأمر الذي استغله بعض ضعفاء النفوس الذين يكون في نيّتهم عدم العودة فيقوموا بتغذية رصيدهم ويسحبوا أضعافه في الخارج، الأمر الذي جعل من هذه الميزة نوع الاستخدام غير المشروع لبطاقة الدفع من جانب الحامل في حالة السحب حيث تتمثل المخالفة من خلال عدم قيام الحامل بالوفاء بالتزاماته وتغذية رصيده.

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٣٠.

ثانياً: الاستخدام غير المشروع للبطاقة خارج فترة صلاحيتها

ويتجلى الاستخدام غير المشروع خارج فترة صلاحية البطاقة بثلاث صور تتمثل في الآتي:

١- الاستخدام غير المشروع لبطاقة منتهية الصلاحية

البطاقة محددة الصلاحية هي البطاقة التي تسلمها الجهة المصدرة إلى الحامل بموجب عقد استخدام البطاقة، ويكون تاريخ الصلاحية مدون عليها بأرقام بارزة. وغالباً ما تصدر هذه البطاقة بتاريخ صلاحية لمدة عامين، وبحلول هذا التاريخ يمكن تجديدها بطلب من الحامل الذي يقدمه إلى المصرف المصدر والمتضمن الرغبة في تجديدها وذلك قبل حلول أجلها. وقد يقوم المصرف المصدر بتجديدها تلقائياً وذلك بالنسبة للحامل حسن النية. وعملية التجديد لا تكون بالنسبة للبطاقة ذاتها، وإنما يتوجب على الحامل الشرعي رد البطاقة محددة الصلاحية، وتسليمها إلى المصرف المصدر ومن ثم يسلمه هذا الأخير بطاقة جديدة. وقد يتجلى الاستخدام غير المشروع لبطاقة منتهية الصلاحية في عمليات السحب أو الوفاء:

أ- بالنسبة للوفاء:

■ فقد يقوم حامل البطاقة باستعمالها في الوفاء بقيمة مشترياته لدى التجار على الرغم من عدم صلاحيتها للاستعمال، وذلك إن نسي تجديدها أو احتفظ بالبطاقة القديمة رغم تسلمه البطاقة الجديدة وتعتمد شراء السلع بواسطتها حتى يحتاج فيما بعد على الوفاء للمصدر بأنه لم يقم باستخدامها.

■ قد يستخدم الحامل البطاقة المنتهية الصلاحية بصورة غير مشروعة وذلك بالاتفاق مع التاجر على قبولها إضراراً بالمصدر، وذلك بأن يقوم التاجر بتزوير تاريخ انتهاء صلاحية البطاقة على

إشعار البيع، أو يعلن عمداً عن تاريخ غير صحيح لانتهاه
صلاحية البطاقة عند طلب التفويض بالبيع من المصدر^١.

ب- بالنسبة للسحب:

فإنه من حيث المبدأ لا يتصور أن يتم السحب بواسطة بطاقة منتهية
الصلاحية وذلك لأن جهاز الصرّاف لن يقوم بإرجاع البطاقة أو على
الأقل رفضها نظراً للبرمجة المتبعة في تشغيله. ولكن قد يمكن
لحامول استعمال هذه البطاقة في السحب من أجهزة الصرّاف في حال
تأخر المصرف في إعادة برمجة ذاكرة الصرّاف الآلي لرفض أو
حجز مثل هذه البطاقات، وبالتالي لن يقوم الجهاز بالاحتفاظ بالبطاقة
أو حجزها مما يساعد الحامل على الحصول على مبالغ نقدية دون
وجه حق^٢.

ولعل السبب الرئيس لحدوث مثل هذا الاستخدام غير المشروع
بالبطاقة المنتهية الصلاحية إنما يعود لاستغلال الحامل للفترة الزمنية
الواقعة بين انتهاء صلاحية البطاقة من جهة وقيام المصدر بإبلاغ
التجار أو برمجة أجهزة الصرّاف على كيفية التعامل مع هذه البطاقة.
الأمر الذي يترتب عليه التزام المصرف بالوفاء للتاجر بقيمة
مشتريات الحامل أو تسليم جهاز الصرّاف النقود للحامل.

٢- الاستخدام غير المشروع للبطاقة الملغاة.

البطاقة الملغاة هي البطاقة المسلمة لحاملها الشرعي بناءً على
عقد مبرم بين الحامل والمصدر، والمتضمن عدة شروط

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٣٢.

^٢ رائد يوسف، مرجع سابق، ص ١٢٩.

والتزامات على عاتق الحامل ويتوجب عليه احترامها. ومن الحالات التي توجب إلغاء البطاقة نذكر^١:

- إخلال الحامل بأي التزامات تعاقدية توجب فسخ العقد و إلغاء البطاقة.
- قيام حامل البطاقة بقتل حسابه الذي تشغله البطاقة يؤدي إلى إلغائها.
- يحق للمصدر باعتباره مالك لبطاقة الدفع إلغائها بأي وقت.
- عجز أو توقف الحامل عن الدفع.
- إشهار إفلاس الحامل بحكم قضائي.
- الحجز على ممتلكات الحامل.
- وفاة الحامل.
- طلب الحامل إلغاء البطاقة.
- الإبلاغ عن سرقة البطاقة أو فقدانها.

وبمجرد إلغاء البطاقات من قبل المصدر يتوجب على الحامل إرجاعها وردها إلى المصدر. ويتم سحب البطاقة الملغاة من التعامل إما بطلبها من المصدر وتوجيه إشعار بذلك للحامل، أو عن طريق الاحتفاظ بها من قبل الصراف الآلي أو عن طريق سحبها من قبل التاجر باعتباره وكيل عن المصرف . ويتمثل الاستخدام غير المشروع للبطاقة الملغاة من قبل الحامل في الوفاء أو السحب:

أ-بالنسبة للوفاء:

قد يقوم الحامل الشرعي باستخدام البطاقة الملغاة في الوفاء بثمن السلع، الأمر الذي يشكل نوعاً من الاستخدام غير المشروع لهذه

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٤٠.

البطاقة ويترتب عليه التزام المصدر بالوفاء للتاجر بقيمة هذه المبالغ. وقد يكون هذا الاستخدام غير مشروع ناتج عن إحدى الحالات الآتية:

- قد يحدث الاستخدام غير المشروع للبطاقة الملغاة ما دام التاجر لا يعلم بإلغاء البطاقة نظراً لأن المصدر لم يزوده بآخر نشرة دورية تحذيرية تتضمن أرقام البطاقات الملغاة.
- قد يحدث الاستخدام غير المشروع ما دام التاجر قد اتصل بمركز التفويض وحصل على الإذن بإجراء التفويض ورقم التفويض وذلك بالنسبة للأجهزة اليدوية.
- قد يحدث الاستخدام غير المشروع إذا لم يقيم الجهاز الإلكتروني (P.O.S) برفض البطاقة ولم يظهر على شاشته بأن البطاقة ملغاة^١.

ب- بالنسبة للسحب:

فلا يتصور من حيث المبدأ في ظل الأنظمة الإلكترونية قبول أجهزة الصراف الآلي لعملية سحب الأموال بواسطة بطاقة ملغاة. حيث ترتبط هذه الأجهزة مباشرة بحساب الحامل. ويتم برمجتها على سحب البطاقة في حال إدخالها بها أو على الأقل رفضها. ولكن فيما لو تأخر المصرف في برمجة ذاكرة الصراف الآلي على رفض أو احتجاز البطاقة الملغاة فقد يستغل الحامل الفترة الزمنية بين إلغاء البطاقة وبين برمجة ذاكرة الصراف، الأمر الذي قد يؤدي لإمكانية سحب الأموال دون وجه حق من الصراف ونكون في هذه الحالة أمام استخدام غير مشروع لبطاقة ملغاة^٢.

^١ المرجع السابق، ص ١٤١.

^٢ رائد يوسف، مرجع سابق، ص ١٢٩.

٣- الامتناع عن رد البطاقة

إذا انتهت صلاحية البطاقة أو تم إلغاؤها وطلب المصدر من الحامل إرجاعها. فلا بد أن يلتزم الحامل برد البطاقة لمصدرها، وذلك نظراً لكون العلاقة العقدية بين المصدر والحامل تُبقي ملكية البطاقة للمصدر الذي يعهد للحامل باستخدامها. ويمثل استخدام الحامل للبطاقة بعد أن يتم الإخطار بسحبها والامتناع عن ردها نوع من الاستخدام غير المشروع للبطاقة من جهة وتبديد للشيء الذي سلم إليه على سبيل العارية من جهة أخرى، الأمر الذي من شأنه أن يدين الحامل بجرم إساءة الائتمان^١. وبالتالي يجب أن نفرق في هذا المجال بين حالتين:

الأولى: قيام الحامل باستخدام البطاقة على الرغم من إخطار المصدر له بانتهاء صلاحيتها أو إلغائها فهنا نكون أمام استخدام غير مشروع للبطاقة الملغاة أو المنتهية الصلاحية على النحو الذي بيناه آنفاً.

الثانية: مجرد امتناع الحامل عن رد البطاقة وبغض النظر عن استعمالها يكون الحامل مرتكب لجرم إساءة الائتمان كون البطاقة قد سلمت إليه على سبيل العارية. وغالباً ما يترافق الامتناع عن رد البطاقة باستخدامها في عمليات السحب أو الوفاء الأمر الذي يجعل الحامل مرتكب لجريمتين (الاستخدام غير المشروع و إساءة الائتمان).

^١ فطيمة ميهوبي، مرجع سابق، ص ٣٦.

ثالثاً: الاستخدام المقنّع لبطاقة الدفع

ويتجلى الاستخدام المقنّع بعدة صور نتحدث عنها على النحو الآتي:

١- الحصول على البطاقة بمستندات غير صحيحة

يتطلب الحصول على بطاقة الدفع الإلكتروني تقديم طالب البطاقة لطلب رسمي إلى الجهة المختصة المصدرة للبطاقة يقوم فيها بتحديد شخصيته (اسمه، لقبه، عنوانه، مهنته، حالته المادية....). فتقديم هذه المعلومات تعبير عن رغبة الطالب بإصدار بطاقة له، ولكن يتمتع المصرف بالحرية المطلقة في هذا الشأن فقد يوافق على إصدار بطاقة لطالبها أو يرفض ذلك باعتبار أن منح البطاقة للمستخدم تقوم على الاعتبار الشخصي وبالتالي قد لا يثق المصرف بالمستخدم أو بالمعلومات المقدمة من قبله لذلك له الحق برفض منحه بطاقة..

ونظراً لأهمية المعلومات المقدمة من قبل طالب البطاقة -والتي على أساسها يُمنح البطاقة أو لا يُمنح- لذلك ينبغي أن تكون المعلومات المقدمة دقيقة وصحيحة. فإذا قدم طالب البطاقة معلومات غير صحيحة وكان على ضوءها قد مُنح بطاقة الدفع الإلكتروني فإنه يكون قد خدع وغش الجهة المصدرة^١.

ويتجلى النشاط غير المشروع في هذه الحالة عندما يتقدم طالب البطاقة بمستندات شخصية مزورة منتحلاً صفة الغير أو ببيانات غير صحيحة كالعناوين الوهمية أو يتقدم بضمانات غير حقيقية. وبناءً على هذه البيانات يقوم المصرف بإصدار بطاقة لطالبها. وتجدر الإشارة إلى أن مثل هذه الحالة صعبة الحدوث وذلك في ظل وجود قاعدة (اعرف عميلك) لدى المصارف، حيث لن يقبل أي مصرف إصدار بطاقة لشخص إلا بعد جمع معلومات

^١ د. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقة الائتمان، دار الجامعة الجديدة، مصر،

٢٠٠٧، ص ١٦٤. ومشار إليه لدى رائد يوسف، مرجع سابق، ص ١٢٨.

مفصلة وشاملة عنه ولكن في حال كان هناك نوع من التواطؤ بين موظف المصرف وطالب البطاقة فهنا يمكن تصور الحصول على بطاقة بمستندات مزورة.

و يتجلى الاستخدام المقنع للبطاقة التي تم الحصول عليها بمستندات مزورة من خلال الآتي:

- طالب البطاقة حصل عليها بموجب مستندات غير صحيحة (مزورة).
- قام المصدر بمنح طالب البطاقة بطاقة صحيحة بناءً على المعلومات المقدمة.
- نتيجة حصول الحامل على البطاقة فمن الطبيعي أن يقوم باستخدام البطاقة سواء في عمليات السحب أو الوفاء.
- نتيجة استخدام هذه البطاقة سوف يتعرض المصرف لخسائر كبيرة في حين أن حامل البطاقة تمكن من التهرب من التزاماته، إما لعدم تمكن المصرف من الاستدلال على الحامل (كون المستندات المتعلقة بهويته أو عنوانه مزورة أو وهمية) أو لكون الضمانات المقدمة غير كافية.

ولعل خير أمثلة على هذه الحالة نذكر القضايا الآتية:

- في أحد القضايا قام أحد المصارف برفع دعوى ضد أحد الأشخاص يتهمه فيها بالاستيلاء على مبلغ /٤٥٩.٩٠ دولار/ ومبلغ /٧٩٠٤.٣٠ جنيهًا مصرياً/ من المصرف المذكور. وذلك لأن الشخص المذكور قام باتباع طرق احتيالية ليحصل على بطاقة فيزا كارد من المصرف بهدف استخدامها في السوق المحلية، وذلك بعد أن قدم مستندات تثبت أن دخله السنوي لا يقل عن مبلغ /٢٤٠٠٠ جنيه مصري/ حتى يتم خصم قيمة المشتريات من الدخل المذكور بشكل شهري، فضلاً عن تعهده بعدم استخدام البطاقة ما لم يكن رصيده كافياً طبقاً للعقد المبرم بينه وبين

المصرف. قام الشخص المذكور باستخدام البطاقة لدى التجار بمبالغ كبيرة دون تسديد قيمتها، فقام التجار بالعودة على المصرف بوصفه ملتزماً أساسياً بالدفع في نطاق عقد استخدام بطاقة الدفع الإلكترونية، ونتيجة للعقد المبرم بين التجار والمصرف التزم المصرف بالسداد. حيث طالب المصرف بعقاب الشخص المذكور بوصفه استعمل طرق احتيالية تمثلت بإيهام المصرف بأنه شخص مليء ولديه ضمانات كافية وأيد هذا الإيهام بالمستندات المزورة التي قدمها للمصرف^١.

- عرضت واقعة على محكمة النقض الألمانية تمثلت بقيام أحد الأشخاص بالحصول على بطاقتي الدائنز كلوب والأمريكان اكسبريس مستخدماً الطرق الاحتيالية، حيث كان عاملاً لدى أحد الصيدليات لكنه ادعى عند طلبه للبطاقة أنه صيدلي منتحلاً بذلك صفة غير صحيحة، كما قدم مستندات تثبت أنه ميسور الحال على عكس الحقيقة إذ كان معسراً. وبذلك أوقع المصدرين للبطاقتين في الغلط وحصل عليهما بفضل البيانات الكاذبة والصفة غير صحيحة. وقد أدانته محكمة النقض عن جرم الاحتيال^٢.

٢- الإبلاغ غير الصحيح عن فقد البطاقة أو سرقتها.

يقوم الحامل الشرعي للبطاقة في هذه الحالة بالإبلاغ عن سرقة البطاقة أو فقدتها في حين أنها لا تزال في حوزته ويستمر في استعمالها سواء في السحب أم في الوفاء.

^١ مشار إليه لدى: المرجع السابق، ص ١٢٨.

^٢ مشار إليه لدى: د. محمود طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، بحث مقدم لمؤتمر الأعمال المصرفية بين الشريعة والقانون، المجلد الثالث، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ١١٢٩.

فبالنسبة للسحب: يستغل الحامل الفترة بين الإبلاغ عن الفقد أو السرقة و قيام المصدر ببرمجة أجهزة الصراف الآلي لكي لا تقبل البطاقة المفقودة أو المسروقة في السحب حيث خلال هذه الفترة يمكن استغلالها للتمكن من سحب النقود كون جهاز الصراف الآلي لم يتم برمجته على سحب هذه البطاقة..

أما بالنسبة للوفاء: فقد يقوم الحامل الشرعي باستخدام البطاقة في الوفاء لدى التجار المزودين بآلة يدوية وذلك خوفاً من اكتشاف أمره عن طريق الجهاز الإلكتروني (P.O.S)، حيث لا يمكن اكتشاف الغش لدى التجار المزودين بآلة يدوية إلا في وقت لاحق عن طريق المواجهة بين التاجر والحامل. وفي كلا الحالتين يتمكن الحامل الشرعي من سحب النقود من أجهزة الصراف الآلي أو الوفاء بقيمة مشترياته لدى التجار وذلك باستخدام مقنع للبطاقة^١.

ومن الوقائع التي حدثت في هذا الشأن نذكر القضية الآتية: تتلخص وقائع هذه القضية في قيام السيد (X) سنة ١٩٧٦ بالحصول على بطاقة وفاء من شركة الدانز كلوب بفرنسا، وقام في ١٧/٨/١٩٧٦ بالإخطار عن سرقة وفاء من شركة الدانز كلوب بفرنسا، وقام بدوره بالإخطار عن فقدائها في ألمانيا في ٣/١/١٩٧٧، وفي الفترة ما بين آب عام ١٩٧٦ وكانون الثاني عام ١٩٧٧. قام باستعمال البطاقتين اللتين سبق له الإبلاغ عن فقدانهما عدة مرات وفي عدة دول وبواسطة نفس الشخص. وقد تبين للمحكمة من خلال التوقيع المزور للسيد (X) والمثبت على الفواتير بأنه

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٤٢.

هو الذي استعمل البطاقتين مع أنه سبق أن أخطر المصرف المصدر كذباً عن فقدانهما^١.

٣- التواطؤ بين الحامل والغير

ويتم التواطؤ بين الحامل الشرعي والغير من أجل التحايل على المصدر باستخدام إحدى الطريقتين:

أ- أن يقوم الحامل بإعطاء البطاقة للغير من أجل استعمالها في السحب وتزوير توقيعها، وبعد ذلك يقوم حامل البطاقة بالاعتراض على السحب ويطعن بتزويره حتى لا يخضم المبلغ المسحوب من حسابه.

ب- أن يقوم الحامل الشرعي للبطاقة بإعطاء الغير بيانات بطاقته ورقمه السري بهدف تمكينه من تزوير بطاقة على غرارها واستعمالها بشكل غير مشروع سواء في السحب أو الوفاء^٢.

ولعل خير مثال على ذلك نذكر:

- ففي أحد القضايا أقدم لبناني يقيم في أمريكا على إعطاء بطاقته إلى لبناني آخر مقيم في مصر، وقام هذا الأخير باستخدام البطاقة لسحب مبالغ مالية كبيرة من أحد المصارف وبعد تحصيل المبلغ من المصرف المصدر للبطاقة، عاد المصرف على العامل (اللبناني المقيم في أمريكا) وطالب باسترداد هذه المبالغ إلا أن الحامل الشرعي والموجود في أمريكا أثبت للمصدر أنه لم يغادر أمريكا ولم يكن موجوداً في مصر ولم يتعامل بهذه البطاقة في مصر وأن

^١ راجع: Crime, 16 Juin 1986, Revue De droit international des systemes électroniques de paiement, 1987, No.18, P.9

مشار إليه لدى د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية، مرجع سابق، ص ١٤٤.

^٢ د. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، ط١، دار الفكر الجامعي، مصر، ٢٠٠٧، ص ١٢٥.

البطاقة التي تم السحب من خلالها بطاقة مزورة، وبذلك تمكن
الحامل الشرعي من التخلص من دفع المبلغ وحصل المتهم على
البراءة كونه لم يثبت قيامه بالتزوير^١.

٤- الادعاء غير الصحيح بعدم استخدام البطاقة

وتتحقق هذه الحالة عندما يقوم الحامل باستخدام بطاقته في الوفاء أو السحب
أثناء سفره، وعند عودته لبلاده يدعي أنه لم يسافر وأنه لم يستخدم البطاقة في
البلد التي تم استخدام البطاقة فيها ويثبت ذلك عن طريق جواز سفر آخر
يحملة. ومن الأمثلة على ذلك نذكر^٢:

● قضية تتلخص وقائعها في أن أحد الأشخاص أردني الجنسية ويعمل
مديراً لفرع إحدى الشركات الأردنية الكبرى، ويحمل بطاقة فيزا بسقف
(خمسة آلاف دولار أمريكي شهرياً)، حائز على جوازي سفر أحدهما
أردني والآخر أمريكي. دخل الأردن بالجواز الأردني وغادر مستخدماً
الجواز الأمريكي إلى كوالالمبور وقام بسحب حد البطاقة الأقصى
بالكامل هناك، ثم عاد إلى الأردن بنفس الجواز (الأمريكي). حضر
للمصرف الأردني واعترض على سحب المبلغ من حسابه مدعياً بأنه لم
يغادر الأردن ولم يستخدم البطاقة في كوالالمبور، وأثبت ذلك للمصرف
بإبراز جواز سفره الأردني. فقام المصرف بإعادة المبلغ لحسابه، وتم
اكتشاف أمره عندما كرر هذا الأمر للمرة الثالثة.

وينبغي أن نشير إلى أن معظم حالات الاستخدام غير المشروع من قبل
الحامل -التي تحدثنا عنها آنفاً- إنما تحدث كنوع من سوء النية من جانبه
بقصد الكسب المادي وغير المشروع، وإلى جانب ذلك فقد يحدث الاستخدام

^١ المرجع السابق، ص ١٢٥.

^٢ مشار إليه لدى : د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقة الدفع
الإلكترونية، مرجع سابق، ص ١٤٦.

غير المشروع نتيجة تقصير حامل البطاقة في الحفاظ عليها الأمر الذي قد يؤدي إلى إمكانية استخدام البطاقة من قبل شخص آخر. ففي هذه الحالة يتحمل حامل البطاقة كامل المسؤولية عن هذا الاستخدام على الرغم من إنكاره استخدامها من قبله.

وفي هذا الصدد كان للقضاء الفرنسي حكم أشار فيه إلى أنه بما يتوافق مع التوجيه الأوروبي الصادر في ١٣/ نوفمبر ٢٠٠٧/ والذي يهدف لتعزيز الثقة بسلامة استخدام أدوات الدفع الإلكترونية، ومن خلال تفسير الأحكام الواردة في التعليمات البرمجية للمسائل النقدية والمالية في ضوء القانون الوطني الفرنسي وذلك بالنسبة لعبء وطرق الإثبات. تجد المحكمة أن الحامل الذي ينكر ترخيصه لعملية دفع تمت بطريقة احتيالية أو دون رضاه عن قصد أو عن طريق الإهمال الجسيم يتحمل كامل المسؤولية المترتبة على ذلك بما في ذلك دفع الرسوم المستوجبة على هذا الاستخدام تجاه المصرف. وبالتالي لا يمكن للحامل أن يستند لأحكام المادتين 16-113، 17-113 L/ من التوجيه الأوروبي والتي تعفيه من دفع الرسوم فيما إذا تم بالفعل استخدام أداة الدفع أو البيانات الشخصية المتعلقة بالحامل من قبل شخص آخر. ومرد ذلك إلى أنه ونظراً لمستوى الأمان الذي توفره خدمة الدفع الإلكترونية فإن أي احتيال أو إهمال جسيم في الحفاظ على ميزات الأمان الشخصية الخاصة بأداة الدفع من جانب حامل الأداة يوجب التزامه بتحمل المسؤولية ودفع الرسوم المستوجبة¹.

¹Cour de cassation, Chambre commerciale, Arrêt n° 349 du 3 Avril 2019, Pourvoi n° 18-11.293.

وبالنتيجة وفي ختام الحديث عن الاستخدام غير المشروع من قبل الحامل نجد أن صاحب البطاقة هو الحامل الشرعي لها ومن الطبيعي أن يكون له الحق باستخدام البطاقة سواء في السحب أو الوفاء. ولكن الاستخدام غير المشروع يحدث في إحدى الحالات الآتية:

- الحالة الأولى: إن محل الاستخدام غير مشروع مما يجعل الاستخدام غير مشروع (في حال كانت البطاقة ملغاة أو منتهية الصلاحية).
- الحالة الثانية: إن وسيلة الحصول على البطاقة غير مشروعة مما يجعل استخدامها غير مشروع (كالوصول على بطاقة بمستندات غير صحيحة أو الإبلاغ عن فقدانها أو سرقتها).
- الحالة الثالثة: إن استخدام هذه البطاقة مقترن بهدف غير مشروع (ك تجاوز الحد في السحب أو الوفاء أو الاستخدام المقنع للبطاقة سواء بالتواطؤ مع الغير أو الادعاء غير الصحيح بعدم استخدام البطاقة أو الامتناع عن ردها). وفي جميع هذه الحالات هناك عنصر مشترك هو النية السيئة للحامل.

إذاً وبعد أن تعرفنا على حالات الاستخدام غير المشروع لأحد أطراف التعامل ببطاقة الدفع الإلكتروني (الحامل) ننقل للحديث عن الاستخدام غير المشروع من قبل طرف آخر ألا وهو (التاجر).

الفرع الثاني

الاستخدام غير المشروع من قبل التاجر

يُقصد بالتاجر الجهة التي تقبل البطاقة من حاملها كوسيلة دفع مقابل السلع والخدمات المقدمة منها لهؤلاء المستخدمين وذلك بشرط توقيع الحامل على إشعارات البيع. ولا يحق لأي جهة قبول البطاقات في التعاملات إلا بعد التعاقد مع أحد المصدرين في هذا المجال. حيث يتولى هذا الأخير تزويد التجار بالآلات اليدوية أو الإلكترونية اللازمة لتشغيل هذه البطاقات. ومن ثم يقوم التاجر بتحصيل قيمة الفواتير من المصدر المتعاقد معه على أن تتم تسوية العملية بين المصدر والحامل عن طريق الخصم من حسابه أو تغطية قيمة المدفوعات لاحقاً. وفي إطار التعامل ببطاقات الدفع الإلكترونية يلتزم التاجر بعدة التزامات نذكر منها:

- التحقق من صحة البطاقة وصلاحياتها.
- التحقق من شخص الحامل كونه الحامل الشرعي أم لا.
- التحقق من مطابقة التوقيع على الإشعارات بالتوقيع الموجود على البطاقة.
- الحصول على تفويض لإجراء هذه العملية.

وبالتالي فإن أي إخلال بهذه الالتزامات من جانب التاجر سوف يجعل الاستخدام لهذه البطاقة غير مشروع. ويختلف الاستخدام غير المشروع من جانب التاجر تبعاً لنوعية الجهاز أو الآلة المستخدمة في التعرف على البطاقة سواء أكان جهاز يدوي أم إلكتروني. كما أنه قد يرافق استخدام بطاقة الدفع الإلكترونية مجموعة من الأخطاء الفنية التي قد تصل لحد الاستخدام غير المشروع سواء ارتكبت هذه الأخطاء من قبل التاجر أم من قبل الحامل.

وبالتالي وفي سبيل التعرف على الاستخدام غير المشروع من قبل التاجر سوف نتحدث عن الاستخدام غير المشروع بواسطة الجهاز اليدوي (التقليدي) أولاً على أن ننقل ثانياً للحديث عن الاستخدام غير المشروع بواسطة الجهاز الإلكتروني (P.O.S) ومن ثم نختم بالحديث الأخطاء الفنية التي تصاحب استخدام بطاقة الدفع الإلكتروني (ثالثاً).

أولاً: الاستخدام غير المشروع بواسطة الجهاز اليدوي.

يتجلى الاستخدام غير المشروع بواسطة الجهاز اليدوي من خلال عدة أساليب غير مشروعة نذكر منها:

١- قد يقوم التاجر بتزوير التوقع الخاصة لديه والعائدة للحامل على فواتير تتضمن مشتريات لم يقم الحامل بتنفيذها أو الحصول عليها، وبعد عملية التزوير يقدمها التاجر للمصرف المصدر من أجل تحصيل قيمتها، فيقوم المصرف بسداد هذه القيمة ويعمل مباشرة على خصمها من حساب الحامل.

٢- قد يقوم التاجر بطباعة أرقام المستخدمين المتعاملين معه على إشعارات فارغة وخالية وبيعها لتجار آخرين معتمدين من المصرف المصدر، ولكن دون طباعة رقم الآلة التي تخصه حتى يتمكن التجار الآخريين من تحصيل قيمتها بعد الحصول على الموافقة^١.

٣- قد يقوم التاجر المعتمد بشراء إشعارات بيع - من غير التي يزوده بها المصرف المصدر - من الغير، تحتوي تلك الإشعارات على أرقام بطاقات بعض المستخدمين مزورة أو تتضمن بيانات غير

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٣٤.

صحيحة. ثم يعمد التاجر لعمليات بيع وهمية ويقوم بطباعة رقم آتته ليقدم هذه الإشعارات للحصول لدى المصرف المصدر.

٤- قد يدعي التاجر تعطل الآلة الإلكترونية ويقوم بكتابة أرقام موافقات وهمية على الإشعارات حتى يتمكن من تحصيل قيمتها، ولكن هذه الحالة نادرة الحدوث بسبب سهولة كشفها من قبل المصدر^١.

٥- قد يلجأ التاجر لتقديم الفواتير للحصول أكثر من مرة باستخدام الأصل ثم الصورة أو بالتواطؤ مع الحامل فيستخدم الأصل (الخاص به) ثم يستخدم فاتورة المشتري الحامل.

٦- قد يلجأ التاجر المعتمد إلى إتمام عمليات البيع على الرغم من عدم حصوله على الموافقة من قبل المصدر، وذلك من خلال تجزئة قيمة العملية على عدة فواتير وبمبالغ أقل من الحد المسموح به والمضمون ومن ثم تحصيل قيمتها^٢.

٧- قد يلجأ التاجر المعتمد إلى تقديم إشعارات للحصول لدى المصرف المصدر بعد تغيير المبالغ الأصلية بالزيادة على غفلة من حامل البطاقة وهذه الحالة كثيرة الحدوث مع المستخدمين الأجانب.

٨- قد يقبل التاجر التعامل ببطاقة ملغاة أو منتهية الصلاحية أو مزورة وذلك بالتواطؤ مع حاملها، ومن ثم يستخدم هذه البطاقة ضمن حدود ما يسمح به المصرف المصدر.

^١ المرجع السابق، ص ٣٣٤.

^٢ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٤٦ - ١٤٧.

٩- قد يستخدم التاجر البطاقة الملغاة أو المزورة أو المنتهية الصلاحية في تحصيل فواتير بتواريخ غير حقيقية كتقديم التاريخ^١.

ومن الأمثلة العملية على مثل هذه الحالات نذكر^٢:

- ففي إحدى القضايا التي حدثت في الأردن، قام أحد الأشخاص بإحضار قسيمة دفع صادرة عن شركة فيزا الأردن إلى شخص آخر مدون عليها رقم البطاقة ولا تحمل اسم التاجر وموقعة بتوقيع أجنبي. وطلب منه أن يقوم بالتصرف بالقسيمة في أحد المحلات. وفعلاً توجه إلى محل التاجر (ع، س، أ، ف) وقام بإعطائه القسيمة والذي بدوره قام بإجراء العملية بوضع اسم التاجر وقدمها لشركة فيزا الأردن واستلم قيمتها (٢٤٥) دينار.
- (هذا المثال العملي دليل على حالة الاستخدام غير المشروع التي يقوم بها التاجر من خلال شراء سندات بيع من الغير مطبوع عليها أرقام بطاقات بعض المستخدمين).
- في إحدى القضايا التي حدثت في الأردن، قام موظفان في إحدى الشركات باستخدام أربع بطاقات فيزا مزورة تم شراؤها من أمريكا وقاما بسحب مبالغ نقدية بمقدار (٥٤٠٠ دينار).
- (هذا المثال العملي دليل على حالة الاستخدام غير المشروع التي يقوم بها التاجر من خلال استخدام التاجر لبطاقات مزورة لتحصيل فواتير وهو عالم بتزويرها).

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٣٤.

^٢ مشار لهذه الأمثلة لدى د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٤٨ - ١٤٩.

• في أحد المطاعم، سلّم أحد المستخدمين بطاقة الدفع الإلكتروني للمحاسب ليقوم بطباعة فاتورة الأكل والشرب بواسطة الآلة المخصصة لذلك. إلا أن المحاسب كان سيء النية فقام بطباعة رقم البطاقة على أكثر من فاتورة خالية من البيانات. ثم قام المحاسب بالاستيلاء على المبالغ النقدية التي دفعها زبائن آخرين للمطعم مع تحميل قيمة هذه المبالغ على الفواتير التي سبق أن طبع عليها بيانات البطاقة خلسة، ووقع عليها تزويراً ليتم تحصيل قيمتها^١.

(هذا المثال العملي دليل على حالة الاستخدام غير المشروع من قبل التاجر من خلال قيام التاجر بالتوقيع على فواتير مشتريات لم يحصل عليها المستخدمون وذلك بعد طباعة أرقام بطاقات المستخدمين على هذه الفواتير).

ثانياً: الاستخدام غير المشروع بواسطة الجهاز الإلكتروني

بدايةً ينبغي أن نشير إلى أن إمكانية الاستخدام غير المشروع للجهاز الإلكتروني أمر غاية في الصعوبة، وذلك نظراً للإمكانيات والتقنيات العالية التي تجعل من استخدام هذه الأجهزة بشكل غير مشروع أمر يسهل اكتشافه. ولكن على الرغم من ذلك فقد تمكن بعض الهواة ومحترفي الجرائم من الاستخدام غير المشروع لهذا الجهاز وذلك بواسطة بعض الأساليب غير المشروعة ونذكر منها ما يلي^٢:

^١ المرجع السابق، ص ١٤٨.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٣٥.

١- قد يقوم التاجر المعتمد بالتلاعب في البرامج الخاصة بالآلة الإلكترونية بتعطيل العمل بها أثناء عملية قراءة البطاقة حتى لا يتم اكتشاف البطاقة المزورة أو المسروقة، ومن ثم استخدامها لتحصيل قيمة فواتير تمت بموجب بطاقة مزورة أو مسروقة.

٢- قد يلجأ التاجر المعتمد لتشغيل الآلة الإلكترونية يدوياً ثم يقوم بتزوير توقيع أصحاب البطاقات على الإشعارات وإرسالها إلى المصرف المصدر للتحصيل.

٣- قيام التاجر بوضع جهاز قارئ ناسخ على جهاز البيع الإلكتروني، يقوم بنسخ بيانات البطاقة أثناء تمريرها ويقوم بطبع هذه البيانات على بطاقة أخرى يستخدمها التاجر لإجراء عمليات بيع وهمية دون أن يعلم الحامل أن بطاقته تم نسخها.

وقد كشف التطبيق العملي عن بعض هذه الحالات، نذكر منها^١:

- ففي إحدى القضايا، قام صاحب محل ساعات في الإسكندرية ونجله بالتلاعب في آلة البيع المسلمة لهما من قبل المصرف وقاما باستخدامها في عمليات بيع وهمية بموجب بطاقات مُبلّغ عن سرقتها، وتمكن بذلك من الاستيلاء على أموال من المصرف حصيلة عمليات البيع الوهمية. حيث بتفتيشهما عثر بحوزتهم على كمية كبيرة من الفواتير لكافة عمليات البيع الوهمية التي تمت بواسطة الآلة المسلمة لهما.

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٥٢-١٥٣.

• في إحدى القضايا التي حصلت في الأردن عام ٢٠١٢/، تناول أحد حاملي بطاقة الفيزا عشاءه في أحد مطاعم عمان ودفع قيمة الفاتورة بواسطة البطاقة واستلم نسخة من الفاتورة وبقيت النسخ الأخرى مع المحاسب والتي تحمل رقم البطاقة المكون من ١٦/ رقم/. قام المحاسب بالاتصال بصديق له يعمل محاسب لدى أحد الفنادق وأعطاه رقم البطاقة، وفي اليوم التالي قام أحد نزلاء الفندق من الجنسية اليمنية بدفع القيمة نقداً للمحاسب، فقام الأخير بوضع المبلغ في جيبه وأدخل رقم البطاقة الذي أعطاه إياه محاسب المطعم - يدوياً على الجهاز الإلكتروني وقدم الفاتورة لشركة فيزا الأردن التي صرفت له المبلغ.

• في إحدى القضايا التي حصلت في الأردن عام ١٩٩٩/ قام أحد التجار بالحصول على رقم بطاقة دفع إلكتروني أدخلت على الجهاز الإلكتروني بعد أن قام التاجر بوضع قارئ وناسخ داخل الجهاز للاحتفاظ بأرقام البطاقات للأشخاص الذين يتعاملون معه، ومن ثم قام بطبعه على بطاقة مزورة بواسطة آلة متطورة وتسليمها لأحد الأشخاص والذي تمكن بالاتفاق مع تاجر آخرين من إجراء عمليات بيع وهمية وصرف الفواتير من المصرف المصدر.

وينبغي أن نشير إلى أن حالات الاستخدام غير المشروع سواء من قبل الحامل أم التاجر تبقى محكومة ببند العقد الذي يربط كل منهما مع المصدر فقد يقضي العقد المذكور على سبيل المثال بإمكانية تجاوز الرصيد في الوفاء أو إعفاء التاجر من الحصول على التفويض ضمن حدود معينة) ففي هذه الحالات لا نكون أمام استخدام غير مشروع. وفي سبيل التوضيح نورد المثال القضائي الآتي:

ففي إحدى القضايا التي عرضت على القضاء الفرنسي، كان هناك حامل بطاقة دفع صادرة عن مصرف يستخدمها للوفاء بثمن مشتريات لدى التاجر عبر الآلة اليدوية. وفي إحدى العمليات أقدم الحامل على استخدام البطاقة متجاوزاً حدود الرصيد، الأمر الذي دفع المصرف إلى الامتناع عن الوفاء للتاجر مدعياً أن الحامل تجاوز الرصيد وأن التاجر لم يحصل على التفويض المطلوب. الأمر الذي دفع التاجر إلى اللجوء إلى القضاء مطالباً المصرف بكافة المبالغ المدين بها. قضت المحكمة بإلزام المصرف بدفع هذه المبالغ للتاجر وذلك استناداً للمبررات التي قدمها التاجر والمتمثلة بالآتي:

- لم يرتكب التاجر أي خطأ بقبول العمليات المعنية والتي تم التحقق من صحتها دون مواجهة أي صعوبة ودون الحاجة لطلب ترخيص.
- اعتاد المصرف على أن يقوم هذا الحامل بمعاملات كثيرة دون أي اعتراض من قبل المصرف.
- لم يرتكب التاجر أي خطأ على اعتبار أنه عادة ما يتم سداد ثمن مشتريات الحامل بموجب بطاقة الدفع، وذلك بعد التحقق من صحتها من خلال الرمز السري الخاص بها ودون الحاجة لطلب أي تفويض أو اضطرار التاجر لتنفيذ أي إجراء.
- لم يقم المصرف بتنبيه التاجر لأية عمليات احتيالية محتملة لهذه البطاقة.

- إن المبالغ المدين بها التاجر لا تتجاوز عتبة (١٠٠) يورو وبالتالي يتم ضمانها وفقاً لشروط العقد المبرم مع الحامل^١.
وبالتالي نجد من المثل السابق أننا في هذه الحالة لم نكن أمام استخدام غير مشروع لبطاقة الدفع على الرغم من تجاوز الرصيد، ومرد ذلك لشروط العقد المبرم بين المصدر والحامل. وبالتالي يبقى العقد بين المصدر والحامل أو المصدر والتاجر هو الفصيل الأساسي لتحديد حالات الاستخدام غير المشروع لبطاقات الدفع الإلكتروني.

وبعد أن تعرفنا على حالات الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، ينبغي أن نشير إلى بعض الأخطاء والهفوات التي تصاحب عملية استخدام بطاقة الدفع الإلكتروني، وتُدعى هذه الأخطاء (الأخطاء الفنية). وتجنباً للخلط بين هذه الأخطاء وحالات الاستخدام غير المشروع اقتضى الأمر الإشارة لهذه الأخطاء سواء أكانت ناشئة عن عملية الوفاء أم عن عملية السحب.

ثالثاً: الأخطاء الفنية التي ترافق استخدام بطاقة الدفع الإلكترونية

١- الأخطاء الفنية التي تحدث عن الوفاء: وتجد هذه الأخطاء مصدرها إما من التاجر أو من الحامل.

أ- الأخطاء الفنية التي يرتكبها التاجر. وتتمثل في الآتي:

¹Cour d' appel de Nouméa, Chambre commerciale, Arrêt du 7 juin 2018, Répertoire général n° 16/00093.

أ- الاختلاف بين ثمن المبيع الحقيقي والقيمة المدونة: رغم قيام التاجر بهذا الخطأ إلا أن نتائجه تقع على عاتق الحامل وذلك لأن توقيع الحامل أسفل الفاتورة يعدّ موافقة منه على القيمة المدونة.

ب- عدم الحصول على التفويض من المصدر: وبالتالي قد يتحمل التاجر مخاطر عدم قيام المصدر بالوفاء بهذه العملية^١.

ج- غياب التوقيع: الأمر الذي يجعل التاجر في موقف صعب كون المصدر غير ملزم بدفع فاتورة غير موقعة. لأنه في حال الوفاء قد يتعرض لمخاطر فيما لو عارضه الحامل.

د- اختلاف التوقيع على الفاتورة عن التوقيع المثبت على البطاقة: وفي هذا الصدد قضت محكمة استئناف باريس بقيام مسؤولية المصدر عن وفاء فواتير تحمل توقيعاً مقلداً أو مزوراً مختلفاً عن نموذج توقيع الحامل المودع لديه، حتى وإن كانت الظروف لا تمكنه من القيام بهذا الفحص لإتمام مقاصة الفواتير آلياً^٢. ونحن من جانبنا نرى أنه لا بد أيضاً من مسالة التاجر وذلك في حال كان التاجر قد أخل بالتزامه المتمثل ب التحقق من مطابقة التوقيع على البطاقة مع التوقيع على الفواتير فضلاً عن مسالة المستخدم عن جرم التزوير بالنسبة للتوقيع واستعمال الوسيلة المزورة.

هـ- التأخر في إرسال سندات البيع: ويترتب على عدم التقيد بهذه المدة من قبل التاجر سقوط حق التاجر في مطالبة المصدر بقيمة هذه السندات.

^١ رائد يوسف، مرجع سابق، ص ١٤٢.

^٢ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ١٠.

و- تمرير البطاقة على الجهاز لأكثر من مرة: ويتمثل الخطأ الفني في أن التاجر قد لا ينتظر المدة (عدة ثوان) من أجل ظهور هذه القراءات على الشاشة أو قد يتأخر ظهورها لأي سبب، فيظن التاجر أن العملية لم تنجح، فيقوم بتمرير البطاقة مرة أخرى، فيكون التاجر قد استوفى ثمن السلعة مرتين في حال قبول الجهاز لعملية التمرير الأولى^١.

ز- تنظيم الفاتورة بشكل خاطئ: إن أي أخطاء حسابية أو مادية من قبل التاجر في تنظيم هذه الفاتورة يعرضه لمخاطر عدم الوفاء من قبل المصدر. كذلك يعد من قبيل الأخطاء في تنظيم الفاتورة إذا قام التاجر بتقسيم البضاعة المباعة على عدة سندات بهدف التخلص من الحصول على التفويض وجعل كل جزء منها ضمن الحد المسموح دون الحاجة للاتصال بالمصرف وأخذ التفويض^٢.

ب- الأخطاء الفنية التي يرتكبها الحامل، وتتجلى هذه الأخطاء في الآتي:

أ - تقديم بطاقة منتهية الصلاحية: قد ينسى الحامل تجديدها، فيتقدم إلى التاجر ببطاقة منتهية الصلاحية وقد يقبلها التاجر فيما لو كانت العملية منفذة بواسطة الجهاز اليدوي، فيؤثر ذلك على قبول تسديد الفواتير من قبل المصدر^٣.

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٠٦.

^٢ المرجع السابق، ص ١٠٤.

^٣ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ١٢.

ب- التوقيع على الفاتورة بتوقيع يختلف عن التوقيع على البطاقة: قد يقوم الحامل بالتوقيع على الفاتورة بشكل يختلف عن التوقيع المثبت على البطاقة الأمر الذي قد يولد منازعات على قيمة الفاتورة فيما بعد.

ج- الخطأ في استخدام الإنترنت: ويتمثل الخطأ الفني في أن يضع المستخدم رقم البطاقة بشكل غير صحيح أو يكون العنوان المراد الإرسال إليه غير واضح ومحدد، فلا تصل السلع التي قام بشرائها. أو يقوم المستخدم بالضغط على مربع الموافقة مرتين، فتسجل لدى التاجر أن المستخدم قام بشراء السلعة مرتين خلافاً للواقع^١.

٢- الأخطاء الفنية التي تحدث عند السحب.

إذا اقتصرَت وظيفة البطاقة على سحب الأموال فإن الأخطاء الفنية تصبح نادرة الحدوث وتتمثل في الآتي:

أ- الأخطاء الفنية المتعلقة بالإيصال المسلم، وتتمثل هذه الأخطاء في الآتي:
أ - عدم التطابق ما بين الإيصال المسلم وعملية السحب المنفذة: ويتمثل هذا الخطأ عندما يكون الإيصال المطبوع لا يوضح توضيحاً صحيحاً بعض البيانات المتعلقة بعملية السحب (كالخطأ في تاريخ العملية). ويكون مصدرها مجرد قصور ميكانيكي عند طبع الإيصال. وبالتالي فهي ليست ذات نتيجة.

ب- عدم التطابق ما بين المبلغ المسلم والمبلغ المطلوب: وينتج عن هذا الخطأ إما أن يقوم الجهاز بإخراج أموال أقل من القيمة المطلوبة أو أكثر منها. ويثور بسبب هذا الخطأ منازعات تتعلق بالإثبات، حيث أن الجهاز يقوم بقيد المبلغ المطلوب في حساب المستخدم وليس المبلغ الذي تم إخراجهِ وتسلمه.

^١ المرجع السابق، ص ١٣.

فإذا كان المبلغ المسلم أقل من المبلغ المطلوب فإنه سيلحق الضرر بالحامل ويقع عليه عبء إثبات ذلك. أما إذا كان المبلغ المسلم أكثر من المطلوب فإن المصرف لن يتمكن من معرفة المستخدم الذي حصل على المبلغ الزائد إلا بعد عملية تدقيق مضمينة^١.

ب- حجز البطاقة بواسطة جهاز الصراف الآلي.

قد يقوم جهاز الصراف الآلي بحجز بطاقة المستخدم تلقائياً إما بسبب إجراءات الأمان التي يطبقها المصرف أو بسبب خطأ فني في الجهاز.

أ - حجز البطاقة بسبب إجراءات الأمان: ومن الحالات التي يقوم بسببها جهاز الصراف بحجز البطاقة نذكر^٢:

- سحب البطاقة بعد ثلاث محاولات خاطئة عند إدخال الرقم السري.
 - سحب البطاقة إذا كانت ملغاة أو منتهية الصلاحية.
 - سحب البطاقة إذا كان الحامل قد أبلغ المصرف أنها مفقودة أو مسروقة.
 - إذا لم يقم الحامل بسحب البطاقة المستخدمة من الجهاز بعد انتهاء العملية خلال مدة (٣٠) ثانية. فإن الجهاز قد يقوم بحجزها.
- وجميع الحالات السالفة الذكر قد تُنذر بإمكانية الاستخدام غير المشروع للبطاقة من قبل الغير، الأمر الذي دفع المصارف لبرمجة جهاز الصراف على حجز البطاقة في هذه الحالات.

ب- حجز البطاقة بسبب الخطأ الفني: بعد قيام الحامل بإدخال بطاقته في جهاز الصراف الآلي، وإتمام العملية بصورة صحيحة فإن الجهاز قد يقوم

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٠٩.

^٢ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ١٥.

برد بطاقة تم حجزها سابقاً، ليست بطاقة الحامل التي يحتفظ بها نتيجة لخلل في الجهاز.

وبالنتيجة وفي ختام الحديث عن الاستخدام غير المشروع من قبل التاجر، نجد أن الاستخدام غير المشروع من قبل التاجر يتطلب نوعاً من التزوير والتلاعب سواء في الآلة اليدوية أم في الآلة الإلكترونية، فضلاً عن سوء النية لدى التاجر، وقد يكون هذا الاستخدام غير المشروع بالتواطؤ مع الحامل أو دون معرفته. ولعل الفارق الوحيد بين الآلة اليدوية والآلة الإلكترونية هو أن إمكانية التزوير والتلاعب في الآلة اليدوية أمر سهل كون الإشعارات والمستندات تأخذ شكل ورقي الأمر الذي يجعل الآلة اليدوية مسرح واسع للاستخدام غير المشروع من قبل التاجر، أما الآلة الإلكترونية فنظراً للتقنيات الحديثة التي تقوم عليها فإن إمكانية التلاعب والتزوير بها يحتاج لدقة عالية وتقنيات متطورة الأمر الذي يجعل من الآلة الإلكترونية مجال ضيق للاستخدام غير المشروع، وذلك على اعتبار أن معظم هذه الآلات الإلكترونية مزودة بأجهزة للكشف عن أي عمليات تلاعب.

أما بالنسبة الأخطاء الفنية التي ترافق عملية استخدام بطاقة الدفع الإلكترونية، نجد أن هذه الأخطاء تخرج عن نطاق الاستخدام المألوف والمعتاد للبطاقة من جهة ولكنها لا تدخل ضمن نطاق الاستخدام غير المشروع من جهة أخرى، ومعيار مدى اعتبار هذه الأخطاء مجرد أخطاء فنية أو حالات استخدام غير مشروع هو حسن النية أو سوء النية لدى مرتكب هذه الأخطاء ويعود تقدير ذلك لقاضي الموضوع.

وبعد أن تعرفنا على الاستخدام غير المشروع من قبل الحامل والتاجر، ننتقل للحديث عن بعض حالات الاستخدام غير المشروع والتي تتم من قبل موظفي المصدر.

الفرع الثالث

الاستخدام غير المشروع من قبل موظفي المصدر

لا يقتصر خطر الاستخدام غير المشروع لبطاقات الدفع الإلكترونية على الحامل أو التاجر وإنما قد يصل هذا الاستخدام إلى موظفي المصارف مصدرة هذه البطاقات. فقد يقوم أحد الموظفين أو بعضهم ببعض الأساليب غير المشروعة من أجل المصلحة الشخصية المحضة والبعيدة تماماً عن مصلحة المصرف المصدر بغية الحصول على مبالغ مالية دون وجه حق. وغالباً ما تتخذ أساليب التلاعب التي تقع من موظفي المصرف المصدر أحد الأشكال الآتية:

أولاً: تواطؤ موظف المصدر مع حامل البطاقة لارتكاب أحد الأفعال الآتية:

١- إذ يتواطأ موظف المصرف مع حامل البطاقة سيء النية، ويساعده على ارتكاب بعض الأفعال مقابل الحصول على مبالغ مالية. ومثال ذلك (كأن يتفق معه على استخراج بطاقة سليمة بناءً على بيانات مزورة -كتقديم مستندات شخصية مزورة أو ضمانات وهمية- ثم يستخدم هذه البطاقة في عمليات شراء بمبالغ مالية ضخمة يلتزم المصرف بدفع قيمتها دون إمكانية تحصيلها من الحامل لعدم إمكانية الاستدلال عليه).

٢- قد يلجأ موظف المصرف بالتواطؤ مع الحامل على السماح للأخير بتجاوز الحد المسموح للبطاقة.

- ٣- قد يعتمد موظف المصرف إلى السماح للحامل بأن يجري سحبات بموجب بطاقات ملغاة أو منتهية الصلاحية^١.
- ٤- التأخر عمداً في إلغاء البطاقة من قبل الموظف المسؤول عن ذلك بعد التبليغ الكاذب عن فقد البطاقة أو سرقتها حتى يتمكن الحامل من إتمام أكبر قدر من عمليات الشراء.

ثانياً: تواطؤ موظف المصدر مع التاجر لارتكاب أحد الأفعال الآتية:

- ١- قد يلجأ موظف المصرف إلى التواطؤ مع التاجر المعتمد ويساعده في القيام ببعض الأعمال، ومثال ذلك (تجاوز الحد المسموح به المضمون من قبل المصرف المصدر على إشعارات البيع).
- ٢- قد يقدم موظف المصرف المساعدة للتاجر المعتمد بتشجيعه على استخدام إشعارات بيع صدرت استناداً لبطاقات وهمية أو مزورة أو منتهية الصلاحية.
- ٣- قد يسمح موظف المصرف للتاجر بإدخال رقم البطاقة على الجهاز الإلكتروني يدوياً، مما يسمح له بإدخال رقم البطاقة على فواتير دون وجود البطاقة عنده أصلاً^٢.

ثالثاً: تواطؤ الموظف مع الغير:

قد يتواطأ موظف المصرف مع الغير كأفراد العصابات وذلك بتزويدهم بكل ما يساعدهم على التزوير والاصطناع من خلال مدهم ببيانات بطاقات الدفع الصحيحة.

^١ رائد يوسف، مرجع سابق، ص ١٣٩.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٣٦.

ولعل من الأمثلة القضائية على عمليات الاستخدام غير المشروع من قبل موظفي المصدر نذكر:

- ففي أحد القضايا، كان هناك موظف (X) لدى شركة (IDEM-EMI) ويتميز هذا الموظف بخبرته البالغة /٢٥ عاماً/ في إجراء المعاملات المصرفية وإنشاء وسائل الدفع الإلكتروني داخل الشركة. أقدم هذا الموظف وبالتواطؤ مع أحد التجار على إجراء معاملات مصرفية غير مشروعة بواسطة بطاقة أحد المستخدمين لدى هذه الشركة وذلك في دول البلطيق. فُوجئ المستخدم بوجود نقص في رصيده نتيجة لعمليات لم يتم بإجرائها. فادعى على الشركة (IDEM-EMI) بجرم الاحتيال، لكن الشركة المذكورة أسقطت عن نفسها التهمة المنسوبة وادعت بهذا الجرم على الموظف (X) وذلك استناداً للمبررات الآتية:

- ❖ ادعت الشركة بأن (X) كان عديم اليقظة من حيث حجم العمليات المالية التي نفذت لما مجموعه (٢٠٠٠٠٠ يورو).
- ❖ كانت معظم العمليات المالية التي أجراها (X) لتحقيق مناقصة استحواذ في دول البلطيق ولم يكن للشركة أيّاً من الشركات الصغيرة والمتوسطة لها علاقات تجارية مع هذه البلدان.
- ❖ تتطلب هذه العمليات موافقة مسبقة من الشركاء بقرار يتخذ في الجمعية العامة مما يثير جرم الاحتيال بحق الموظف كون مثل هذه العمليات والمعلومات المتعلقة بها من البديهيات المعروفة لديه في ظل خبرته المصرفية بهذه المعاملات¹.

¹Cour d' appel de Douai, 2ème Chambre, Section 2, Arrêt du 14 Mars 2019, Répertoire général n° 17/00489.

- القضية التي حصلت مع أحد الأقرباء وتتلخص وقائعها في أنه كان هناك مواطن يتقاضى راتبه التقاعدي من مؤسسة التأمينات عن طريق أحد فروعها في إحدى المحافظات السورية، قام هذا المواطن بتوطين راتبه لدى أحد المصارف الخاصة العاملة في سورية باعتباره قد حصل على قرض من المصرف المذكور، نتيجة لذلك كان فرع مؤسسة التأمينات يقوم بتحويل راتب المواطن إلكترونياً إلى المصرف المذكور والذي بدوره يقوم بخصم قسط القرض من راتب المواطن وما بقي منه يتقاضاه المواطن بواسطة بطاقة صراف آلي صادرة عن المصرف المذكور. وفي ظل الأزمة وعجز فرع مؤسسة التأمينات في المحافظة عن تحويل الرواتب إلكترونياً كون هذه المحافظة من المناطق الساخنة أمنياً تم تكليف فرع آخر للمؤسسة في محافظة أخرى أمناً لتسيير التحويلات المالية المتعلقة بفرع المنطقة الساخنة. تبين لاحقاً أن هناك نوع من التواطؤ بين مدير المصرف المذكور ومديري فرعي مؤسسة التأمينات في كلا المحافظتين حيث كان في كل شهر يتم تحويل الراتب من كلا الفرعين لذات المصرف ولذات الشخص. فيقوم المصرف بخصم قسط القرض من الراتب المحول من فرع المنطقة الآمنة أما بالنسبة للراتب المحول من فرع المنطقة الساخنة فكان يقوم بوضعه كوديعة في حساب لصالح المصرف ليتم الاستفادة منه بالتواطؤ بين مدير المصرف ومديري الفرعين المذكورين. وبالتالي يمكن القول أن مدير المصرف ومديري فرعي مؤسسة التأمينات مسؤولان عن الاستخدام غير المشروع من خلال تواطؤ فيما بينهم، وذلك باعتبار أن مدير المصرف قد أخل بالعرف المصرفي الذي يقضي التزامه بإعلام فرع المنطقة الساخنة أنه يتلقى تحويلات الرواتب مرتين، كما أن كل من مديري الفرعين أخلو

بالواجب الوظيفي الذي يقضي بإعلام كل طرف الطرف الآخر أنه يقوم بتحويل الراتب لذات المصرف ولذات الشخص في آن واحد.

وفي ختام الحديث عن الاستخدام غير المشروع من قبل موظفي المصدر، نجد أن هؤلاء الموظفين لا يقومون بالاستخدام غير المشروع كما هو الحال بالنسبة للحامل والتاجر، ومرد ذلك لكون البطاقة غير موجودة في حيازتهم، فأفعالهم لا تشكل نوعاً من التعدي على نظام الدفع الإلكتروني وتقتصر على التواطؤ مع الحامل أو التاجر أو الغير بغية تسهيل الاستخدام غير المشروع من جانب هؤلاء المذكورين. حيث ينبغي أن نشير إلى أن أغلب حالات الاستخدام غير المشروع إنما تتم نتيجة تواطؤ بين الحامل وموظفي المصدر أو التاجر وموظفي المصدر، كون هؤلاء الموظفين هم القادرون على تغطية عمليات الاستخدام غير المشروع التي تتم من قبل الحامل أو التاجر وبأساليب السابق ذكرها.

هذا فيما يتعلق بالاستخدام غير المشروع من قبل أطراف الدفع الإلكتروني، ولكن الاستخدام غير المشروع لا يقتصر على أطراف الدفع فحسب، فكثيراً ما يكون هذا الاستخدام من قبل أطراف خارجة عن دائرة التعامل بنظام الدفع، بهدف التعدي على هذا النظام والحصول على المنفعة المادية بشكل غير مشروع وهذا الاستخدام غير المشروع مجال دراستنا في المطلب الثاني.

المطلب الثاني

الاستخدام غير المشروع من قبل الغير

يُقصد بالغير الشخص الأجنبي عن العقود الناشئة عن استخدام بطاقة الدفع الإلكتروني. أي كل شخص خارج عن دائرة أطراف البطاقة (الحامل والتاجر المعتمد والمصرف المصدر). وبالتالي لا يعد من الغير حامل البطاقة التابعة ولا العاملين لدى التاجر والمصدر كون هؤلاء الأشخاص خاضعين لإشراف ورقابة أطراف البطاقة وذلك بالنسبة للأفعال الواقعة منهم أثناء ممارستهم لأعمالهم أو بسببها. وغالباً ما يلجأ الغير إلى استخدام البطاقة استخداماً غير مشروع من أجل الحصول على أموال ليست له في الأصل، وفي سبيل ذلك يقوم بعدة أساليب وحيل تمكنه من ذلك سواء أكان ذلك من خلال التعاملات العادية أم باستخدام أجهزة الصراف الآلي أم عبر شبكة الإنترنت.

وبالتالي وفي سبيل الإحاطة بمعظم حالات الاستخدام غير المشروع من قبل الغير، سوف نتحدث عن الاستخدام غير المشروع في التعاملات العادية في الفرع الأول، ثم ننتقل للحديث عن الاستخدام غير المشروع عبر أجهزة الصراف الآلي وذلك في الفرع الثاني، على أن نختم الحديث عن الاستخدام غير المشروع عبر شبكة الإنترنت وذلك في الفرع الثالث.

الفرع الأول

الاستخدام غير المشروع في التعاملات العادية

يقصد بالتعاملات العادية التعاملات التي تأخذ صورة الوجود المادي سواء أكان ذلك بالنسبة لوجود مادي لأطراف العلاقة أم بالنسبة للسلع والفواتير الناتجة عن استخدام بطاقة الدفع الإلكتروني. ويأخذ الاستخدام غير المشروع من قبل الغير في التعاملات العادية والمألوفة عدة أشكال نذكر منها ما يلي:

١- قد يقوم الغير بسرقة البطاقة من حاملها الشرعي وسرقة رقمها السري بهدف استخدامها إما من أجل الحصول على مشتريات لدى التجار أو استخدامها في سحب النقود من أجهزة الصراف الآلي وذلك قبل اكتشاف السرقة والتبليغ لدى المصدر من قبل الحامل الشرعي. وكل ما يقوم به الغير سارق البطاقة من نفقات قبل اكتشاف السرقة والتبليغ إلى المصدر تُخصم من حساب الحامل^١.

٢- قد يحصل الغير على البطاقة دون أن يلجأ لسرقتها. كأن يجدها أو يعثر عليها بعد ضياعها من حاملها ثم يقوم باستخدامها للحصول على أموال من أجهزة الصراف الآلي أو يستخدمها لدى التاجر، وخاصةً إذا ما عثر بالإضافة إلى البطاقة على رقمها السري (كما لو كان هذا الرقم السري مكتوب على البطاقة نفسها أو على لاصقة ورقية). وكل استخدام لهذه البطاقة يخصم من حساب الحامل طالما أن الأخير تأخر في اكتشاف الضياع أو تأخر في إبلاغ المصدر بفقدانها.

^١ راجع: د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع

الإلكتروني، مرجع سابق، ص ١٧٨-١٨١.

٣- قد يلجأ الغير إلى سرقة بطاقة تتضمن بيانات صحيحة ويعمل على تزويرها، ومن ثم استخدام البطاقة المزورة في عمليات السحب والوفاء. ولا تتطلب عملية التزوير دائماً بطاقة مزورة، بل قد يلجأ محترفو التزوير وهواته إلى بعض الأساليب من أجل تحقيق غايتهم كالاستعانة بسلات المهملات الخاصة لدى التجار أو لدى أجهزة الصراف والتي تحتوي على نسخ الكوبون المتخلفة عن الاستعمال^١.

٤- قد يعتمد الغير إلى التواطؤ مع الحامل الشرعي للبطاقة للحصول على أموال بشكل غير مشروع دون المصرف والتاجر. وذلك بتسليم الحامل الشرعي بطاقته للغير الذي يعتمد لتزوير توقيع الحامل واستخدام البطاقة لدى التجار المعتمدين. وحتى لا يتحمل الحامل سوء النية تلك النفقات المنفذة بالتواطؤ يسارع إلى إجراء معارضة لدى المصرف المصدر^٢.

وفي ختام الحديث عن الاستخدام غير المشروع من قبل الغير في التعاملات العادية، نجد أن هذا الاستخدام لا يخرج عن الأفعال غير المشروعة والمألوفة وبالتحديد عمليات السرقة والتزوير لبطاقات الدفع الإلكتروني. ولكن حتى يتم هذا الاستخدام لا بد أن يرافق عملية السرقة معرفة الرقم السري للبطاقة وأن يرافق عملية التزوير معرفة بالبيانات الصحيحة حتى يمكن تزويرها أو معرفة التوقيع الصحيح للحامل الشرعي وذلك في حال التواطؤ بين الحامل والغير.

^١ راجع د: أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع سابق، ص ١٩-٢١.

^٢ راجع د: عبد الفتاح بيومي حجازي، مرجع سابق، ص ١٢٤-١٢٥.

وبالتالي نجد أن هذا الاستخدام غير المشروع في نطاق بطاقات الدفع الإلكتروني لا يكتسب أي خصوصية مميزة وقد سبق الحديث عن السرقة والتزوير في نطاق أدوات الدفع الإلكتروني^١.
والآن ننقل للحديث عن الاستخدام غير المشروع من قبل الغير عبر أجهزة الصراف الآلي.

الفرع الثاني

الاستخدام غير المشروع عبر أجهزة الصراف الآلي

نظراً لما تتطلبه تعاملات الصراف الآلي من إدخال المستخدم الرقم السري كإثبات لشخصيته قبل التصريح بسحب النقود، فقد اعتبرت تعاملات الصراف الآلي دوماً آمنة. إلا أن الواقع العملي كشف عن عمليات استخدام غير مشروعة تتم من خلال أجهزة الصراف الآلي أدت لحصول المجرمين على المبالغ النقدية بشكل مباشر. وحتى تتم عمليات الاستخدام غير المشروع لا بد من وجود عدة طرق للحصول على معلومات بطاقة الصراف الآلي وتتمثل هذه الطرق في الآتي:

أولاً: كتابة الرقم السري على البطاقة: قد يقوم بعض المستخدمين (وخصوصاً كبار السن) بكتابة الرقم السري على البطاقة أو على أي مستندات يكون فيها الرقم واضحاً للشخص الذي يسرق البطاقة أو يجدها بعد فقدانها فلا يجد صعوبة في استخدامها.

ثانياً: إعطاء الرقم السري للغير: غالباً ما يفصح حاملو البطاقات عن الرقم السري إلى أشخاص آخرين مما يجعل إمكانية الاستخدام غير المشروع أمر سهل. ومثال ذلك (قيام حامل البطاقة بالإفصاح عن الرقم السري لأحد أقاربه الذي يستغل ذلك لتزوير بطاقة واستخدامها

^١ راجع ص ٢٧٣ وما يليها (السرقة) + ص ٢٨٨ وما يليها (التزوير).

بشكل غير مشروع، قيام حامل البطاقة بالإفصاح عن الرقم السري للغير أمام جهاز الصراف طالباً منه المساعدة في سحب النقود، فيقوم الغير بسرقة البطاقة أو استغلال الرقم في تزوير بطاقة مماثلة مما يمكنه من استخدام هذه البطاقة بشكل غير مشروع^١.

ثالثاً: ربط جهاز قراءة آخر على جهاز الصراف

يقوم مرتكبو هذه العملية بربط جهاز قراءة بطاقة آخر فوق فتحة الصراف الآلي، يمكنهم من قراءة المعلومات الموجودة على الشريط المغناطيسي للبطاقة بواسطة جهاز ثانٍ وتسجيلها على رقاقة ذاكرة عندما يتم إدخال البطاقة في فتحة الصراف الآلي. بعد ذلك يمكن الحصول على الرقم السري بواسطة كاميرا صغيرة جداً يتم وضعها في مكان استراتيجي على رف الصراف الآلي بحيث يكشف منطقة لوحة الأرقام الخاصة بالرقم السري^٢. أو قد يتم وصل آلة قراءة البطاقات إلى لوحة المفاتيح المستخدمة لإدخال الرقم السري وبالتالي تسجل معلومات البطاقة كاملة عند قيام المستخدم بأية معاملة.

رابعاً: وضع واجهة جهاز صراف مزور

وتتكون هذه الواجهة من شاشة، رف مجهز بلوحة مفاتيح، قارئ بطاقة، درج للنقد، شعار المصدر.

وتستخدم هذه الواجهة لتغطية واجهة الجهاز الأصلي. وعندما يستخدم الحامل هذه الآلة ظناً منه أنها أصلية فلا يدرك أنها تسجل معلومات بطاقته وتقوم بإرسالها فوراً لجهاز استقبال موجود على مقربة من

^١ أمثلة عملية وواقعية قد تصادف أي شخص يتعامل ببطاقات الصراف الآلي.

^٢ بشرى سلامة، المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الوفاء، رسالة ماجستير، كلية الحقوق، جامعة دمشق، ٢٠١٠ - ٢٠١١، ص ٧٦ - ٧٧.

جهاز الصراف الآلي. ويمكن أن يصرف جهاز الصراف المزور نقوداً وقد يكفي برد البطاقة وفقاً لمستوى التنفيذ والتصميم المستخدم^١.

خامساً: الحلقة اللبنانية

تعود هذه التسمية لعصابة لبنانية مختصة بسرقة الحسابات المصرفية. وبموجب هذا الأسلوب يتم إدخال جهاز في فتحة الآلة. حيث يقوم بحجز البطاقة الأصلية وعندما يبدأ المستخدم بالتعامل يقوم شخص قريب من حامل البطاقة بمراقبة عميلة إدخال الرقم السري، وبسبب الجهاز الذي تم وضعه تحجز البطاقة ويعتقد الحامل أن جهاز الصراف قد ابتلع البطاقة، وعندما يغادر الحامل يقوم الشخص بإخراج الجهاز والبطاقة، فتصبح البطاقة والرقم السري بحوزته. وبهذا يتمكن المجرمون من إجراء عمليات غير مشروعة تقتطع من رصيد صاحب البطاقة^٢.

بعد أن تعرفنا على بعض الطرق التي يمكن من خلالها للغير الحصول على معلومات بطاقة الصراف دون وجه حق، ننقل للحديث عن الاستخدام غير المشروع من قبل الغير عبر شبكة الإنترنت، باعتبار أن شبكة الإنترنت ذات طابع خاص الأمر الذي يجعل من الاستخدام غير المشروع عبرها ذو أهمية كبيرة، كونه يتعلق بمدى الأمان للتعاملات التي تتم من خلال هذه الشبكة.

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ٢٠١.

^٢ تريبز منصور، بطاقات الدفع الإلكتروني، الاحتراز دائماً واجب، بحث منشور في مجلة الجيش اللبناني، العدد ٣٣٢، ٢٠١٣، ص ٣٥٢. متاح على الرابط:

www.Lebarmy.gov.lb/ar/news/?34398

تاريخ الزيارة ٢٠١٩/٩/١٢ - الساعة ١١.١٥ A.M

الفرع الثالث

الاستخدام غير المشروع عبر شبكة الإنترنت

في ظل غياب الوجود المادي للتعاملات عبر شبكة الإنترنت، يعتمد الاستخدام غير المشروع عبر شبكة الإنترنت على غرض وحيد هو النقاط بيانات بطاقات الدفع الإلكتروني وأرقامها، بغية استخدام هذه البيانات بشكل غير مشروع. وقد تمكن الهواة ومحترفي التعامل عبر شبكة الإنترنت (HACKERS) من التقاط أرقام بطاقات الدفع الإلكتروني الخاصة ببعض المستخدمين وذلك باستخدام عدة طرق وأساليب نجلها في الآتي:

أولاً: الاختراق غير المشروع لمنظومة الاتصالات العالمية

يُقصد بمنظومة الاتصالات مجموعة الخطوط التي تربط الحاسب الآلي للمشتري بذلك الخاص بالتاجر. ويُعد هذا الأسلوب من أخطر ما يهدد نظام الدفع الإلكتروني وذلك لأن الهدف الأساسي لهذا الاختراق إنما يتمثل في عدة أمور:

- رغبة محترفي إجرام التقنية وقرصنة البطاقات في قهر نظام التقنية والتفوق على الحماية المقررة لها.
- قيام هؤلاء المحترفين بنشر هذه المعادلات لبيان الكيفية التي يمكن من خلالها الحصول على الأرقام الخاصة ببطاقات الدفع الإلكتروني المملوكة للغير وذلك عبر موقعهم على شبكة الإنترنت^١. ومن الوقائع التي حدثت في هذا الشأن نذكر^٢:

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٣٤١.

^٢ مشار إليها لدى: المرجع السابق، ص ٣٤١.

- في عام ٢٠٠٤ أعلن مكتب التحقيق الفيدرالي أنه يحقق في حادث اختراق أجهزة كمبيوتر، تم من خلاله سرقة ٨/ ملايين بطاقة دفع من شركة /FBI/ التي تجري عملية تحويل مالية لشركة فيزا وماستر كارد وأمريكان اكسبريس، والتي تعرضت لاختراق نظام العمل من طرف خارجي غير مصرح له بالدخول على النظام.
- كما أعلنت شركتا فيزا وماستر كارد، أن أحد قراصنة الكمبيوتر استطاع اختراق ٢,٢/ مليون حساب تابع لمستخدمين، واستطاع المجرم أن يتجاوز أنظمة تأمين شركة تقوم بإنجاز التعاملات الخاصة للبطاقتين نيابةً عن التجار.

ثانياً: أسلوب التجسس

حيث يقوم قراصنة الكمبيوتر بموجب هذا الأسلوب باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمصارف العاملة على شبكة الإنترنت. وبالتالي يتمكنوا من الحصول على ما يريدون من المعلومات ومنها المتعلقة ببطاقات الدفع التي استخدمت في التعاملات عبر شبكة الانترنت. ومن الأمثلة التي حدثت في الشأن نذكر^١: ما قام به طالبان جامعيان في مدينة بور سعيد المصرية من سحب مبلغ نصف مليون جنيه من رصيد أحد عملاء المصارف الحكومية عن طريق شبكة الإنترنت، واستخدما هذه المبالغ في مشاهدة أفلام متنوعة على الإنترنت. وتبين أنهم استطاعوا معرفة الرقم السري لحساب المستخدم على الشبكة عن طريق التجسس واستغلاله في مشاهدة هذه الأفلام عبر الإنترنت.

^١ د. أمجد الجهني، جرائم بطاقات الدفع الإلكتروني عبر شبكة الإنترنت، مرجع سابق، ص ٢٤.

ثالثاً: تقنية تفجير الموقع المستهدف

ويعتمد هذا الأسلوب على ضخ مئات الآلاف من الرسائل الإلكترونية (E-mails) من جهاز الحاسب الآلي للمجرم إلى الجهاز المستهدف، بهدف التأثير على ما يُعرف (بالسعة التخزينية). حيث يشكل هذا الكم الهائل من الرسائل الإلكترونية ضغطاً يؤدي في المحصلة إلى تفجير الموقع العامل على الشبكة وتشتت المعلومات والبيانات المخزنة فيه، لننتقل بعد ذلك إلى الجهاز الخاص بالمجرم. وبالتالي يتمكن هذا المجرم من حرية التجوال في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام وبيانات ومعلومات خاصة ببطاقات الدفع المملوكة للغير^١. ويوجّه هذا الأسلوب بشكل خاص للحواشيب المركزية للمصارف والمطاعم والفنادق ووكالات السفر بهدف تحصيل أكبر عدد ممكن من أرقام البطاقات.

رابعاً: تخليق أرقام البطاقات

ويقصد بهذا الأسلوب تخليق أرقام بطاقات الدفع اعتماداً على إجراء معادلات رياضية وإحصائية. حيث يعتمد هذا الأسلوب على أسس رياضية في تبديل وتوفيق لأرقام حسابية تؤدي في النهاية لنتائج معينة هو الرقم السري لبطاقات متداولة. ليتم استخدام هذه الأرقام السرية في معاملات غير مشروعة عبر الشبكة^٢.

وقد ظهر في القرن الماضي نشاط تخليق أرقام بطاقات صحيحة منسوبة لبعض المصارف عن طريق برامج الحاسب التي يتم تسويقها

^١ بشرى سلامة، مرجع سابق، ص ٧٣.

^٢ د. أمجد الجهني، جرائم بطاقات الدفع الإلكتروني عبر شبكة الإنترنت، مرجع سابق، ص ٢٤.

من خلال بعض مواقع القرصنة على شبكة الإنترنت. حيث يكفي مجرد الدخول على هذه المواقع لإنزال برامج معينة على جهاز الحاسب. ليتم في المرحلة الثانية تشغيله وإدخال رقم بطاقة صحيحة، ليتولى البرنامج بعد ذلك عملية التخليق لأرقام بطاقات تصل لمئة رقم بطاقة صحيحة منسوبة للمصرف ذاته (الذي صدرت عنه البطاقة الصحيحة). ومن ثم يتم استخدام تلك الأرقام في عمليات غير مشروعة (كدمجها مع بطاقة مزورة، أو تلقينها لأشرطة ممغنطة لبطاقات منتهية الصلاحية)، واستخدام هذه البطاقات في إجراء معاملات والنتيجة خصم قيمة هذه المعاملات من رصيد صاحب البطاقة الأصلي التي تحمل ذات الأرقام الصادرة عن ذات المصرف^١.

ونظراً لخطورة هذا الأسلوب وانتشاره أصبح الرقم السري للبطاقة كضمانة وحيدة لعدم اختراق البطاقة وإساءة استعمالها موضع شك وتخوف من مدى فعالية وأمان الرقم السري للبطاقة.

خامساً: تبادل المعلومات

يتمثل هذا الأسلوب بقيام قراصنة الكمبيوتر بتبادل المعلومات التي يحصلون عليها عن أرقام البطاقات وعن أفضل الطرق للدخول غير المشروع، والكيفية التي يمكن من خلالها الحصول على المعلومات المطلوبة من أجل التوسع في استخدام الأرقام التي يتم الحصول

^١ نجاح محمد فوزي، وعي المواطن العربي تجاه جرائم الاحتيال (بطاقات الدفع الإلكتروني نموذجاً)، الرياض، ٢٠٠٧، ص ١٠٧ - ١٠٨.

عليها. ومن الأمثلة على ذلك نذكر^١: الواقعة التي حصلت في الأردن والتي تتلخص في أن شخص يدعى (س. ع. ع. ش) يحوز أرقام بطاقات دفع دولية مسروقة، ويقوم باستخدامها عبر شبكة الإنترنت لشراء البرامج والأفلام المتنوعة. وبتفتيش منزله تم ضبط جهاز كمبيوتر ولوحات الكترونية وأشرطة (FLOPPY-CD)، وبالتحقيق معه أفاد بأنه حصل على أرقام البطاقات المسروقة من شخص في بريطانيا.

سادساً: أسلوب الخداع

ويتم هذا الأسلوب من خلال إنشاء مواقع وهمية على شبكة الإنترنت على غرار المواقع الأصلية للمصارف الموجودة على الشبكة ويظهر هذا الموقع وكأنه الموقع الأصلي الذي يقدم الخدمة. ولكي يُنشأ هذا الموقع يقوم القراصنة بالحصول على بيانات الموقع الأصلي كافة من شبكة الإنترنت. ومن ثم يتم إنشاء الموقع الوهمي مع تعديل البيانات التي سبق الحصول عليها بشكل غير مشروع - وذلك في الموقع الأصلي - حتى لا يظهر أن هناك ازدواجاً بالمواقع^٢. ويتحقق الضرر في هذا الأسلوب باستقبال الموقع الوهمي الخاص بالقراصنة على شبكة الإنترنت لكافة المعاملات التي يقدمها الموقع الأصلي ومن هذه المعلومات (بيانات بطاقة الدفع الإلكتروني). ومن ثم يتسنى للقراصنة الاطلاع على هذه المعلومات والاستفادة منها بشكل غير مشروع

^١ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، مرجع

سابق، ص ٣٤

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٣٤٢.

على نحوٍ يضر بسمعة الجهات صاحبة الموقع الأصلي ويفقد الأفراد الثقة بالتعاملات الإلكترونية. ومن صور الخداع:

قيام القراصنة بصفتهم الجهات المصدرة لبطاقات الدفع الإلكتروني بإرسال رسائل إلكترونية يطلبون فيها من المستقبلين تجديد المعلومات الخاصة بهم (الاسم، العنوان، معلومات البطاقة)، وإرسالها إلى الموقع مرة أخرى بحجة أنهم هم الجهة المصدرة للبطاقة وبذلك يحصلون على أرقام البطاقات^١.

وقد يتجلى الاستخدام غير المشروع من قبل الغير ضمن ميزة الموبايل البنكي أو الهاتف المحمول كأحد وسائل الدفع الإلكتروني، فقد كشف التطور التقني عن ظهور خدمة الموبايل البنكي والتي تمكن المستخدم من خلالها التحكم بحساباته المصرفية عبر رقم هاتف محمول مزود للمستخدم من قبل المصرف وبالتنسيق مع شركة الاتصالات ذات الصلة، وحيث أن هذا الرقم مخصص لحماية مصالح المستخدم قبل كل شيء لذلك ينبغي عليه أن يخطر المصرف بأي إلغاء في رقم هذا الهاتف من قبله.

ول نكون في هذه الحالة أمام حالة استخدام غير مشروع من قبل الغير، وذلك لأنه في حالة إنهاء العقد لتوفير خدمات الاتصالات المتنقلة (أي عندما يلغي المستخدم رقم هاتفه المحمول)، يقوم مشغل الاتصالات بعد مرور فترة زمنية معينة بنقل هذا الرقم لشخص آخر. وطالما لم يتم تعطيل الخدمة المصرفية عبر الرقم السابق للهاتف المحمول سيحصل المشترك الجديد على الحق باستخدام الأموال الموجودة في حساب المستخدم والتي حدثت نتيجة لعدم إبلاغ المصرف بالمعلومات حول إلغاء المستخدم رقم هاتفه. وفي هذه الحالة من الاستخدام غير المشروع نكون أمام احتمالين:

^١ بشرى سلامة، مرجع سابق، ص ٧٤.

الأول: أن ترفض المحاكم تعويض المستخدم عن المعاملات التي يجريها الغير بواسطة الهاتف المحمول للمستخدم، وذلك على أساس أن الأخير انتهك شروط العقد عندما لم يخطر المصرف بإلغاء رقم هاتفه المحمول. وذلك لأنه في مثل هذه الحالة ليس للمصرف أي شك أن أمر تحريك الحسابات المصرفية للمستخدم قد صدر من الغير طالما أن المستخدم لم يخطر المصرف بإلغاء رقم هاتفه.

الثاني: أن يتحمل المصرف المسؤولية عن هذا الاستخدام غير المشروع ويعوض المستخدم عن الضرر، وذلك على اعتبار أن المصرف لم يوف بالتزاماته بضمان السرية للمعلومات المتعلقة بالهاتف المحمول للمستخدم كما أن إرادة العميل لم تتجه للتخلص من هذه الأموال أو تحريكها.

وقد كان للقضاء الروسي موقف حاسم في هذا الخصوص. حيث ذهب القضاء الروسي إلى أن يتم توزيع المسؤولية في هذه الحالة على كل من المستخدم والمصرف وشركة الاتصالات:

فالمستخدم قد أخل بالتزامه بإخطار المصرف بالإلغاء الأمر الذي لا يتوافق مع مبدأ حسن النية في تنفيذ الالتزامات التعاقدية، على النحو الذي يجعل المستخدم متعسفاً في استخدام حقه في الإلغاء.

ويتحمل كل من المصرف وشركة الاتصالات المسؤولية وذلك لكونهم أطراف قوية اقتصادياً في حين أن المستخدم يعد طرفاً ضعيفاً بالنسبة لهم هذا من جهة، كما يلتزم المصرف وشركة الاتصالات بتبادل المعلومات عند انتهاء العقد لتوفير خدمات الاتصالات المتنقلة أو استبدالها من جهة أخرى، فعدم تبادل

المعلومات في هذه الحالة يعد نوعاً من الإخلال بالالتزامات العقدية^١.

ونحن من جانبنا نؤيد القضاء الروسي في هذا القرار وذلك لكونه من أكثر القرارات تحقيقاً للعدالة، باعتباره يوزع المسؤولية بين الأطراف الثلاثة مراعيًا في ذلك الخطأ المرتكب من جانب كل طرف.

وتجدر الإشارة إلى أن كل ما تحدثنا عنه آنفاً إنما هي عبارة عن الطرق والأساليب غير المشروعة التي يمكن من خلالها التقاط أرقام وبيانات بطاقات الدفع الإلكتروني. حيث أن هؤلاء المجرمين بعد قيامهم بالاستيلاء على أرقام البطاقات يقومون باستخدامها استخداماً غير مشروع وذلك على النحو الآتي:

- استخدام تلك البيانات لتلقيها على أشرطة ممغنطة تعود لبطاقات منتهية الصلاحية، باستخدام وحدة تكوين إلكترونية في حالة التزوير الجزئي أو تلقيها لبطاقات خام لتبدو وكأنها بطاقة صحيحة ومن ثم استخدامها في عمليات السحب أو الوفاء.
- استخدام البيانات المسروقة في تمويل عمليات شراء عبر شبكة الإنترنت أو لسرقة حسابات المستخدمين على الشبكة.
- الاتجار بالبيانات المسروقة أو تبادلها مع الآخرين من خلال المنتديات الخاصة عبر الإنترنت^٢.

^١ القضية رقم (٨٢-٥٧٩/٥٠.N1) تاريخ ٢٥/٧/٢٠١٩ ومتاحة على الرابط:

<https://moluch.ru/archive/184/47356>

تاريخ الزيارة: ٣١/٥/٢٠١٩ الساعة ٩،١٢ p.m

^٢ بشرى سلامة، مرجع سابق، ص ٧٨.

وفي ختام الحديث عن الاستخدام غير المشروع من قبل الغير عبر أجهزة الصراف الآلي وعبر شبكة الإنترنت، نجد أن التطورات التقنية والدقة العالية التي حرصت الجهات المصدرة لبطاقات الدفع الإلكتروني على توفيرها في نظام التعاملات عبر شبكة الإنترنت لم تكن بمنأى عن الاستخدام غير المشروع، حيث تمكن هواة الجريمة ومخترقي شبكة الإنترنت من ابتداع أساليب ووسائل كفيلة بالحصول على أرقام بطاقات الدفع الإلكتروني ومن ثم استخدام هذه الأرقام بمختلف العمليات غير المشروعة، الأمر الذي انعكس سلباً على الأفراد والجهات المصدرة. فبالنسبة للأفراد أدت الأساليب غير المشروعة إلى تخوف الأفراد من التعاملات عبر شبكة الإنترنت وفقدان الثقة بأمان هذه المعاملات، أما بالنسبة للجهات المصدرة فإن فقدان ثقة الأفراد انعكس سلباً على سمعة هذه الجهات وتطلب منها في ذات الوقت توفير الوسائل والبدائل الكفيلة بتأمين المعاملات عبر شبكة الإنترنت من خطر قرصنة الشبكة.

أما بخصوص الاستخدام غير المشروع من قبل الغير، نجد أن عمليات الاستخدام غير المشروع عبر شبكة الإنترنت أكثر خطورة وشيوعاً من عمليات الاستخدام غير المشروع في التعاملات العادية والتعاملات عبر أجهزة الصراف، والسبب أن هذه الأخيرة قد تحدث عندما يوجد خلل أمني ما (مناطق ساخنة أو مناطق مزدحمة) فضلاً عن سهولة اكتشاف مثل هذه الحالات. أما بالنسبة لعمليات الاستخدام غير المشروع عبر شبكة الإنترنت فهي ترتكب من قبل محترفي الجريمة وبأساليب تقنية الأمر الذي يجعل أمر اكتشافها غاية في

الصعوبة، إما لأن الضحية أو الجهات المصدرة ذات مكانة مرموقة فلا تفصح عن ذلك أو لصعوبة تقفي مثل هذه الجرائم التي تفتقر للوجود المادي، فضلاً عن الخسائر الكبيرة التي تولدها هذه الجرائم وبزمن قصير جداً.

أما المشكلات الأمنية لوسائل الدفع الإلكتروني، نجد أن هذه المشكلات مشكلات جديدة لم تكن معروفة من قبل، كشف عنها التطور التقني وتتلخص هذه المشكلات في ثلاثة أشكال:

الشكل الأول: المشكلات التي تؤدي لتعطيل أداة الدفع نتيجة لخلل أصاب العنصر التقني ولكن لا تشكل هذه المشكلات جرماً جزائياً ومثالها (تعطل أداة الدفع، الأخطاء الفنية التي ترافق استخدام بطاقة الدفع).

الشكل الثاني: المشكلات التي تحدث نتيجة لأعمال غير مشروعة ترتكب من قبل أطراف الدفع الإلكتروني (الحامل، التاجر، المصدر) وتشكل جرماً جزائياً. وتتميز هذه المشكلات بجديتها واستقلاليته عن الجرائم التقليدية المعروفة، كون هذه المشكلات تحدث نتيجة للتلاعب بأداة الدفع كأحد العناصر التقنية التي كشف عنها التطور التقني ومثالها (حالات الاستخدام غير المشروع لأداة الدفع من قبل الأطراف).

الشكل الثالث: المشكلات التي تحدث نتيجة لأعمال غير مشروعة ترتكب من قبل الغير وتشكل جرماً جزائياً. وتظهر هذه المشكلات بصورتين:

الأولى: مشكلات جديدة لم تكن معروفة من قبل كشف عنها التطور التقني ومثالها (حالات الالتقاط غير المشروع لأرقام البطاقات عبر شبكة الإنترنت أو أجهزة الصراف، الجرائم الإلكترونية).

الثانية: مشكلات تقليدية تظهر بقالب وصيغة جديدة في نطاق الدفع الإلكتروني. ومثالها (السرقه، والتزوير لوسائل الدفع الإلكتروني).
وتتميز الصورتان السابقتان بارتباطهم الوثيق مع بعضهما البعض من ناحية الغرض، فالغير الذي يسرق أو يزور أداة الدفع إنما يهدف إلى استخدامها بشكل غير مشروع سواء بالسحب أو الوفاء. وكذلك الأمر فإنّ الغير الذي يلتقط أرقام البطاقات إنما يهدف الاستخدام غير المشروع سواء في السحب أو الوفاء.

وأمام هذه التحديات والمشكلات تبرز الحاجة إلى البحث عن سبل وأساليب وقائية أو علاجية تسهم بمعالجة هذه المشكلات سواء تمثلت هذه الوسائل بأساليب تقنية أم تمثلت بترتيب المسؤولية الجزائية بحق من يرتكب هذه المشكلات. وهذا ما سنتحدث عنه في الفصل الثاني من هذا الباب.

الفصل الثاني

سبل معالجة المشكلات الأمنية

بعد أن تعرفنا في الفصل الأول على المشكلات الأمنية تبرز الحاجة الملحة للتعرف على سبل معالجة هذه المشكلات. وذلك على اعتبار أن معالجة هذه المشكلات هي الضمانة الوحيدة لانتشار وسائل الدفع الإلكتروني وتطورها الأمر الذي يكسب هذه السبل أهمية كبيرة. وحيث أننا في نطاق البيئة الإلكترونية فقد حرصت الجهات الرقابية والجهات المصدرة لوسائل الدفع الإلكتروني على توفير مجموعة من الأساليب القانونية والتقنية الكفيلة بتجنب حدوث المشكلات الأمنية أو الكفيلة بمعالجتها في حال حدوثها. وبشكل عام تتلخص أساليب معالجة المشكلات الأمنية في أسلوبين:

الأسلوب الأول: التدابير الوقائية

وتتمثل هذه التدابير بمجموعة من الوسائل الاحتياطية المتخذة في سبيل تجنب حدوث مثل هذه المشكلات، سواء أكانت هذه الوسائل تقنية (كالتوقيع الإلكتروني وتأمين البيانات) أم كانت هذه الوسائل إدارية ومثالها (وسائل التخفيف من السرقة، ووسائل الكشف عن التزوير، ووسائل التخفيف من الاستخدام غير المشروع).

الأسلوب الثاني: التدابير العلاجية

وتتمثل هذه التدابير بالبحث في التكييف الجزائي للمشكلات الأمنية بهدف فرض المؤيدات الجزائية الرادعة بحق مرتكب هذه المشكلات، سواء أكانت هذه المؤيدات منصوص عليها في نصوص قانون العقوبات أم في نصوص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية. وذلك على اعتبار أن المشرع السوري جرم

بعض الأفعال التي تجسد المشكلات الأمنية بموجب نصوص خاصة في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية ، في حين أغفل الإشارة إلى تنظيم غيرها من هذه المشكلات بموجب نصوص خاصة. الأمر الذي تطلب العودة لنصوص أحكام قانون العقوبات باعتباره من القوانين العامة لمعرفة مدى إمكانية تطبيق هذه الأحكام العامة على المشكلات الأمنية لوسائل الدفع الالكتروني.

وفي سبيل الإحاطة الشاملة بسبل معالجة المشكلات الأمنية سوف نتحدث عن التدابير الوقائية في المبحث الأول ثم ننتقل للحديث عن التدابير العلاجية في المبحث الثاني.

المبحث الأول

التدابير الوقائية

بما أن عملية الدفع الإلكتروني هي حيلة التزاوج بين قطاع المصارف والثورة التقنية في مجال الاتصالات والمعلومات، فقد حرصت الجهات المصدرة على توفير مجموعة من الخصائص والميزات التقنية والإدارية الكفيلة بالتقليل من حدوث المشكلات الأمنية. وتتمثل التدابير الوقائية كأحد الأساليب المتخذة لتجنب حدوث المشكلات الأمنية في نوعين:

- النوع الأول: التدابير التقنية وهي مجال دراستنا في المطلب الأول.
- النوع الثاني: الوسائل الإدارية وهي مدار دراستنا في المطلب الثاني.

المطلب الأول

التدابير التقنية

نظراً لما تتطلبه عليه المشكلات الأمنية من دخول الوسيلة الإلكترونية كأحد العناصر التقنية الرئيسية في نطاق معاملات الدفع الإلكتروني، لذلك حرصت الجهات المصدرة لوسائل الدفع على إيجاد مجموعة من الوسائل والأساليب التقنية الكفيلة بتجنب حدوث المشكلات الأمنية. حيث تلعب هذه الأساليب دور الضامن للمتعاملين بوسائل الدفع ضد أي محاولات للمساس بنظام الدفع الإلكتروني. وتتمثل التدابير التقنية المتخذة كتدابير لتجنب حدوث المشكلات الأمنية في نوعين :

- الأول: نظام التوقيع الإلكتروني وهو مجال دراستنا في الفرع الأول.
- الثاني: نظام تأمين البيانات وهو مدار بحثنا في الفرع الثاني.

الفرع الأول

نظام التوقيع الإلكتروني

عرف المشرع السوري التوقيع الإلكتروني بأنه: «جملة بيانات تدرج بوسيلة إلكترونية على وثيقة الكترونية وترتبط بها وتتخذ شكل حروف أو أرقام أو رموز أو أي شكل آخر مشابه ويكون لها طابع منفرد تسمح بتحديد شخص الموقع وتميزه عن غيره وينسب إليه وثيقة الكترونية بعينها»^(١).

ويتخذ التوقيع الإلكتروني أشكالاً متعددة (كالتوقيع بالقلم السري، التوقيع البيومتری، التوقيع الرقمي)^(٢).

كما أقر المشروع السوري الحجية القانونية للتوقيع الإلكتروني في نطاق المعاملات الإلكترونية حيث جاء فيه:

أ- للتوقيع الإلكتروني المصدق، المدرج على وثيقة إلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للأدلة الكتابية في أحكام قانون البيانات، إذا روعي في إنشائه وإتمامه الأحكام المنصوص عليها في هذا القانون، والنواظم والضوابط التي يصدرها الوزير، بناءً على قرار مجلس إدارة الهيئة، المنصوص على إحداثها في الفصل الثالث من هذا القانون^(٣).

نجد من النص السالف الذكر أن التوقيع الإلكتروني يتمتع بالحجية المقررة للأدلة الكتابية ولكن هذه الحجية ليست مطلقة بل مقيدة

^١ المادة الأولى من قانون التوقيع الإلكتروني وخدمات الشبكة رقم/٤/ لعام ٢٠٠٩.

^٢ راجع: د. محمد سعيد إسماعيل، مرجع سابق، ص ١٩٣. + عمار لوصيف، مرجع سابق، ص ٩٤. د. بسام شيخ العشرة و د. حنان مليكة، التجارة الإلكترونية، مرجع سابق، ص ٥٧.

^٣ المادة الثامنة من قانون التوقيع الإلكتروني وخدمات الشبكة رقم/٤/ لعام ٢٠٠٩.

بشروط، حيث نص قانون التوقيع الإلكتروني في هذا الخصوص على أنه:

يعد التوقيع الإلكتروني المصدق المدرج على وثيقة الكترونية، مستجمعاً للشروط المطلوبة للحجية في الإثبات وهي:

أ- ارتباط التوقيع بالموقع وحده دون غيره، وكفايته للتعريف بشخص الموقع.

ب- سيطرة الموقع وحده دون غيره على منظومة إنشاء التوقيع الإلكتروني.

ج- ارتباط التوقيع الإلكتروني بالوثيقة الإلكترونية ارتباطاً لا يمكن إحداث أي تعديل أو تبديل على الوثيقة دون ظهور أثر قابل للتدقيق والكشف^١.

وما يهمنا في نطاق دراستنا معرفة الدور الذي يلعبه التوقيع الإلكتروني كأحد التدابير الوقائية لتجنب حدوث المشكلات الأمنية، ويقتضي معرفة هذا الدور التعرف على العلاقة بين التوقيع الإلكتروني ووسائل الدفع الإلكتروني.

وفي إطار بيان هذه العلاقة سوف يتم الحديث عن تطبيقات التوقيع الإلكتروني على وسائل الدفع الإلكتروني (أولاً) ثم ننتقل للحديث عن استخدام التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني (ثانياً).

أولاً: تطبيقات التوقيع الإلكتروني على وسائل الدفع الإلكتروني

تزامن ظهور التوقيع الإلكتروني مع استعمال بطاقة الائتمان في عمليات السحب أو إجراء المشتريات أو الحصول على الخدمات، ثم

^١ المادة الثالثة من قانون التوقيع الإلكتروني وخدمات الشبكة رقم ٤/ لعام ٢٠٠٩.

اتسعت دائرته لتشمل عمليات الشراء عن بعد سواء عن طريق الهاتف أم شبكة الإنترنت^١. كما أن التوقيع الإلكتروني مرشح للتغلغل في حياتنا أكثر فأكثر من خلال مشروع الحكومة الإلكترونية، لكن ما يهم في هذا المقام تطبيقات التوقيع الإلكتروني على وسائل الدفع الإلكتروني وهذا ما سيتم التطرق إليه من خلال الآتي:

١- بطاقات الدفع الإلكتروني: من أقدم المجالات التي يستخدم فيها التوقيع الإلكتروني هو مجال بطاقات الائتمان والتي بدأ استعمالها لدى محطات الوقود والمحلات التجارية الكبرى. ومن أهم هذه البطاقات - إلى جانب بطاقة الائتمان - ما يلي:

أ- البطاقات المغناطيسية: تلعب بطاقة الشريط المغناطيسية دوراً مهماً ومركزياً في الكثير من الصفقات التجارية الإلكترونية. حيث أن المعلومات المخزنة باستخدام المعايير الدولية لتشفير البيانات الرقمية على شريط مغناطيسي مقروء من قبل جهاز الصراف الآلي بطريقة تتيح فك الشيفرة الموجودة على الشريط المغناطيسي المثبت على البطاقة^٢.

ب- البطاقات الذكية: وهي تشبه بطاقات الصراف الآلي ذات الشريط المغناطيسي، غير أنها تحتوي على كمية كبيرة من المعلومات التي تتضمنها كل بطاقة ويتم معالجتها بشكل دقيق ويمكن الولوج بهذه البطاقة إلى شبكة الإنترنت، واستعمال البرامج التلفزيونية المدفوعة الأجر. ويمكن أن نقسم البطاقات الذكية إلى مجموعتين^٣:

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٤١٨.

^٢ د. سميحة القليوبي، الأوراق التجارية، دار النهضة العربية، مصر، ١٩٩٩، ص ٣٠٥.

^٣ د. حوالف عبد الصمد، مرجع سابق، ص ٤١٩.

الأولى: البطاقة الذكية ذات الرقاقة الإلكترونية: حيث تسمح هذه البطاقة بالتحقق من حامل البطاقة بإدخال الرقم السري. وتعمل هذه البطاقة بنظام (Off-Line) أي غير متصل، حيث تتم إضافة المعلومات الجديدة بعد الانتهاء من المعاملات البنكية الإلكترونية.

الثانية: البطاقة التي تحتوي على وحدة معالجة مركزية: حيث تعمل هذه البطاقة بنظام (On-Line) أي الاتصال المباشر، حيث تتميز هذه البطاقات بقابليتها لإضافة ومعالجة المعلومات الجديدة.

ويكون تطبيق التوقيع الإلكتروني في نطاق البطاقات بأشكالها المختلفة على النحو الآتي^١:

- إدخال البطاقة التي تحتوي البيانات الخاصة بالمستخدم في الجهاز المخصص لها، وإذا كان التعامل عبر شبكة الإنترنت يكون التعامل بإدخال البيانات التي يتطلبها جهاز الحاسب.
- كتابة الرقم السري المخصص لصاحب البطاقة.
- إصدار الأمر للقيام بالعملية المراد إتمامها وبالضغط على المفتاح المخصص يكتمل التعبير عن الإرادة في قبول إتمام العملية.

وبالتالي فإن كل بطاقة بلاستيكية تعمل عن طريق إدخال الرقم السري الذي لا يعلم به سوى المستخدم ويعتبر بديلاً عن التوقيع التقليدي.

٢- الشيكات الإلكترونية: الشيكات الإلكترونية هي شيكات تصدرها الحواسيب الإلكترونية. يستغنى فيها عن التوقيع الكتابي

^١ د. إبراهيم الدسوقي أبو ليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ٣٢.

الذي يضعه الأمر بسحبها بالتوقيع الإلكتروني باستخدام تقنية المفتاح الخاص والعام بحيث يقوم المستفيد بعد استلامه الشيك بالتوقيع عليه بالمفتاح الخاص ويرسله للمصرف الخاص به والذي يكون لديه نسخة عن المفتاح العام لكي تتمكن من فهم الرسالة (الشيك الإلكتروني) وتبادلها مع المصرف المسحوب عليه لتسوية العملية^١.

٣- سندات الشحن الإلكترونية: تعد سندات الشحن الإلكتروني من أهم وثائق عقد النقل البحري، وقد ظهرت مع انتشار استخدام الوسائل التقنية في مجالات التجارة الدولية. وتبنت اتفاقية هامبورغ (Hamburg)^٢ صراحةً التوقيع الإلكتروني في إصدار سندات الشحن لغرض مسابقة متطلبات التجارة الحديثة التي تحتاج للسرعة من أجل زيادة وتيرة التبادل التجاري^٣. وتجري عملية تحويل البضاعة باستخدام سندات الشحن الإلكترونية المذيلة بتوقيع رقمي. حيث يتم ذلك عن طريق المفتاح الخاص وهو عبارة عن شيفرة تقنية تكفل صحة وسلامة الإرسال الإلكتروني، ويتم تغيير المفتاح الخاص مع كل تحويل للبضائع، وعلى حائز المفتاح الخاص إخطار الناقل باعتزامه نقل حق البضاعة لشخص آخر، فيقوم الناقل (الذي يملك

^١ محمد يوسف، الشيك الإلكتروني (تداوله-حجيته)، بحث منشور في مجلة جامعة البعث، المجلد ٣٨، العدد ٢٠، ص ٢٠١٦، ص ٧٥-٧٨.

^٢ اتفاقية الأمم المتحدة للنقل البحري والبضائع الموقعة في هامبورغ في ٣١ مارس ١٩٧٨ والتي تُسمى قواعد هامبورغ ودخلت حيز التنفيذ في ١/ نوفمبر ١٩٩٢ واعتباراً من أكتوبر ٢٠١٤ تم التصديق على الاتفاقية من قبل ٣٤ دولة من ضمنها سورية.

^٣ المادة (٣/١٤) من اتفاقية الأمم المتحدة للنقل البحري والبضائع الموقعة في هامبورغ في ٣١ مارس ١٩٧٨

المفتاح العام) بعد تأكيد الإشعار بإرسال وصف وخصائص البضائع إلى الحائز الجديد، وعندما يقبل يُعطى مفتاحاً خاصاً جديداً، ويعدّ كما لو حصل على سند الشحن الورقي^٢.

وعليه فإن المفتاح الخاص (التوقيع الإلكتروني) يحل محل التوقيع التقليدي في عملية إصدار سند الشحن وفي عملية تداوله.

وبالنتيجة يمكن القول أن التوقيع بالرقم السري والتوقيع الرقمي هما الشكّلين الأكثر انتشاراً في نطاق وسائل الدفع الإلكتروني من حيث استخدامه كبديل عن التوقيع التقليدي لإتمام المعاملات الإلكترونية.

وفي هذا الخصوص ذهبت محكمة التحكيم العليا للاتحاد الروسي إلى أنه عند تنفيذ مستند الدفع باستخدام أنظمة الدفع الإلكترونية، يشهد المصرف بالحق في التصرف في الأموال عن طريق تحديد صحة التوقيع الرقمي الإلكتروني. وبالتالي فإن التطابق بين التوقيع الرقمي على أمر الدفع والتوقيع الرقمي المحفوظ لدى المصرف دليل على أن أمر الدفع صادر عن الحامل الشرعي. وبالتالي أي خطأ أو غلط في أوامر الدفع الصادرة و الممهورة بتوقيع رقمي يتحمل الحامل

^١ يتمثل التوقيع الرقمي باستخدام تقنية المفاتيح العام والخاص، فهو عبارة عن منظومة إلكترونية تسمح لكل شخص طبيعي أو معنوي بأن يكون لديه مفتاحين منفردين أحدهما عام متاح إلكترونياً، والثاني خاص يتمثل بأداة إلكترونية خاصة بصاحبها تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الاحتفاظ بها على بطاقة ذكية مؤمنة. حيث يقوم مرسل العملية الإلكترونية بكتابة بيانات الرسالة (سند الشحن) والتوقيع عليها إلكترونياً باستخدام مفتاحه الخاص. فتُحوّل الرسالة إلى أرقام حسابية غير مفهومة، ثم يقوم بإرسال الرسالة موقعة مع مفتاحه العام إلى المرسل إليه فيقوم هذا الأخير بفك الشفرة باستخدام المفتاح العام للمرسل ليتمكن من قراءة الرسالة.

^٢ د. إبراهيم الدسوقي أبو ليل، مرجع سابق، ص ٣٦.

الشرعي تبعاتها فيما لو كانت هذه الأوامر صادرة من غير الحامل طالما أن المصرف اتخذ كافة الاحتياطات المطلوبة للتحقق من صحة التوقيع الرقمي^١.

أي أن القضاء الروسي جعل من التطابق بين التوقيع الرقمي للحامل والتوقيع الرقمي المحفوظ لدى المصرف قرينة لمصلحة المصرف في اعتبار أن أوامر الدفع الإلكترونية صادرة عن الحامل الشرعي. وهذا أمر طبيعي طالما أن أداة الدفع الإلكترونية في حوزته وهو المسؤول عن الحفاظ على هذه الأداة بكافة مستلزماتها بما في ذلك التوقيع الرقمي الخاص بهذه الأداة.

ثانياً: استخدام التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني

تختلف كيفية استخدام التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني بحسب النزاع القانوني المنبثق عن الإخلال بالعلاقات القانونية الناشئة عن أطراف العقد، فاستخدام التوقيع الإلكتروني في إثبات العلاقة الموجودة بين المستخدم والمصدر، يختلف عن النزاع القائم بين المصدر والتاجر. وهذا ما سيتم التطرق إليه وفقاً لآتي:

١- العلاقة بين المصدر والمستخدم

إذا ما شك المستخدم بوجود خطأ ما يتعلق بعمليات السحب من حسابه النقدي الإلكتروني الخاص به، يجب عليه إبلاغ المصدر بذلك

^١ القضية رقم 57-98-11/7162-A تاريخ ١ ديسمبر ٢٠١١ متاحة على

الرابط: <https://sudact.ru/regular/doc/6lRf3y3dKTmO>

وبأسرع وقت ممكن. وفي هذه الحالة يقوم المصدر بالتأكد من صحة مزاعم المستخدم، فإذا تأكد ادعاؤه يقوم المصدر بتصحيح الوضع عن طريق تصحيح الأخطاء. أما إذا تطلب الأمر المزيد من التحقق والفحص، ففي هذه الحالة يقوم المصدر بزيادة رصيد المستخدم في حدود المبلغ محل النزاع بشكل مؤقت لحين بيان النتيجة النهائية^١. فإذا جاءت النتيجة النهائية لهذا الفحص بعدم وجود أخطاء ولم يقتنع بذلك المستخدم، ففي هذه الحالة ينبغي على المصدر أن يثبت صحة نسبة عمليات السحب التي أُجريت إلى المستخدم.

وهنا تظهر أهمية التوقيع الإلكتروني في صورة التوقيع باستخدام الرقم السري /Code pin/. ذلك أن كل مستخدم يختار كلمة أو عبارة خاصة به مكونة من عدد كبير من الحروف والأرقام أو كليهما معاً، ويحتفظ به في مكان آمن وبشكل مشفر لمنع الغير من الاطلاع عليه. وحيث أن وسائل الدفع الإلكتروني لا يمكن تحميلها إلا على أدوات الدفع الخاصة التي يزود المصدر المستخدمين بها لتمكينهم من التعامل بوحدة النقد التي تصدرها. لذلك يجب أن تتوفر أداة الدفع والرقم السري معاً، ليتمكن الحامل من سحب النقود من الحساب المرتبط بهذه الأداة^٢.

ومن المعروف أن الحامل الشرعي للأداة هو الوحيد الذي يعرف الرقم السري وهو المخول الشرعي باستخدامها. وبالتالي فإن إدخال البيانات الشخصية مع الرقم السري والضغط على المفتاح المخصص للموافقة على عملية السحب إنما جميعها تدل على نسبة عمليات

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٤٢٢.

^٢ المرجع السابق، ص ٤٢٢.

السحب للحامل الشرعي ولا يفيد ادعاء الحامل قيام شخص من الغير باستعمال وسائل الدفع الخاصة به لأن ذلك دليل على وجود خطأ من جانب الحامل ويفتح المجال لعمليات النصب والاحتيال في السحب من حساب النقد الإلكتروني.

ولكن قد يحدث أن يقر المستخدم باستخدام وسائل الدفع الخاصة به، لكنه يدعي وجود خطأ في مفردات حسابه من النقد الإلكتروني مثلاً (كما لو ادعى وجود زيادة في المبالغ المقيدة عن تلك التي تم سحبها بالفعل ويدعم هذا الادعاء وجود اختلاف بين ما هو مدون في السجلات الإلكترونية وبين ما سحب بالفعل). ففي هذه الحالة الأخيرة تتعقد مسؤولية المصدر لأن الاختلاف دليل على وجود خلل في نظام النقد الإلكتروني ذاته^١.

٢- في العلاقة بين التاجر والمصدر

تظهر أهمية التوقيع الإلكتروني في هذا الفرض في حال وجود نزاع مثلاً بين التاجر والمصدر يتمحور حول مطالبة التاجر للمصدر باسترداد النقود الإلكترونية التي في حوزته (أي تحويل النقود الإلكترونية لنقود تقليدية) فادعى المصدر أن هذه النقود مزيفة لا قيمة لها، فهنا يقع عبء الإثبات على المصدر أن النقود مزيفة وقد سبق استعمالها وأن التاجر قد قصر في التحقق من مدى صحة النقود، فإذا فشل المصدر في إثبات زيف النقود وتقصير التاجر، فعليه أن ينفذ التزامه بتحويل هذه الوحدات الإلكترونية لنقود حقيقية. أما في حال نجاحه في إثبات ادعائه فهنا ينتقل عبء الإثبات إلى التاجر. لكنه بإمكان التاجر التخلص من المسؤولية بإثبات أحد أمرين:

^١ د. محمد سعيد إسماعيل، مرجع سابق، ص ١٨٤.

الأول: أنه قام بجميع الإجراءات اللازمة للتأكد من صحة النقود المستخدمة في عملية الدفع وذلك بالاتصال بقاعدة البيانات المركزية الخاصة بالمصدر، ولم تشر إلى وجود هذه النقود ضمن قائمة النقود المزيفة. ويتم ذلك بطريقة آلية ومسجلة على برنامج تلقي المدفوعات الخاص بالتاجر^١. فإذا أثبت ذلك فهذا يدل على ضعف إجراءات الأمان التي يتخذها المصدر لكشف صحة النقود وتثبت مسؤولية المصدر عن الإخلال بالتزامه.

الثاني: إذا تمكن التاجر من نسبة النقود إلى المصدر، ولن يتمكن من ذلك إلا بالاعتماد على فكرة التوقيع الرقمي. حيث أن كل وحدة من وحدات النقد الإلكتروني تحمل توقيعاً خاصاً بجهة الإصدار أو تحمل رقماً متسلسلاً يختلف عن بقية الأرقام^٢. وبالتالي يطلب التاجر من المصدر تقديم مفاتيح التشفير الخاصة بها إضافة لتقديم قائمة الأرقام المتسلسلة للنقود المصدرة وذلك في سبيل إثبات شرعية هذه النقود.

حيث تجدر الإشارة إلى أن التوقيع الرقمي يستخدم في بعض النظم للتحقق من وحدات النقد الإلكتروني كما هو الحال في نظام /DIGI CASH/ حيث يقوم المصدر بتوقيع كل وحدة من وحدات النقد باستخدام المفتاح الخاص. فإذا تلقى التاجر هذه الوحدات يقوم بالتحقق من الأرقام المتسلسلة الخاصة بها، كذلك التحقق من صحة التوقيع الرقمي باستخدام المفتاح العام. فإذا أثبت صحة التوقيع فإن ذلك دليل على صحة وحدات النقد الإلكتروني^٣.

وبالنتيجة نجد أن التوقيع بالرقم السري والتوقيع الرقمي من أكثر أشكال التوقيعات انتشاراً في نطاق التعامل بوسائل الدفع الإلكتروني كبديل عن التوقيع

^١ د. أحمد السيد لبيب إبراهيم، الدفع بالنقود الإلكترونية (ماهيته - تنظيمه القانوني) دراسة تحليلية ومقارنة، دار الجامعة الجديدة، مصر، ٢٠٠٩، ص ٣٦٩.

^٢ د. محمد سعيد إسماعيل، مرجع سابق، ص ١٦٢.

^٣ د. أحمد السيد لبيب إبراهيم، مرجع سابق، ص ٣٧٠.

التقليدي لإتمام المعاملات الإلكترونية. حيث ينتشر التوقيع بالرقم السري في مجال بطاقات الدفع الإلكتروني باعتباره الشكل الملائم لهذه البطاقات، كما أنه يلعب دوراً كبيراً في إثبات مشروعية عمليات السحب أو صحة عمليات الدفع وذلك عندما يثور نزاع حول وجود اختلاف في الحساب النقدي للحامل.

أما التوقيع الرقمي فهو ينتشر في مجال الشيكات الإلكترونية وسندات الشحن الإلكترونية في عقود التجارة البحرية والدولية، كما أنه يستخدم كفيصل حاسم عندما يكون هناك نزاع حول مشروعية وحدات النقد الإلكتروني بين المصدر والتاجر.

وبعد أن تعرفنا على الشكل الأول من التدابير التقنية تنتقل للحديث عن شكل آخر من هذه التدابير ألا وهو (تأمين البيانات).

الفرع الثاني

تأمين البيانات

يجري تأمين البيانات من خلال مجموعة من البرامج والبروتوكولات الأمنية التي تعمل كمصفاة للبيانات الإلكترونية، بحيث تقوم بترشح البيانات وتصفيتها بهدف ضمان المرور الآمن لهذه البيانات وتجنب عمليات الانتهاكات والاختراقات غير المشروعة أثناء التعاملات الإلكترونية. وبشكل عام يمكننا أن نميز بين نوعين من أساليب تأمين البيانات:

أولاً: برامج تأمين البيانات

وتشمل هذه البرامج ما يلي:

١- كلمات المرور: تعد كلمة المرور من أكثر الطرق التي يعتمد عليها المصرف للتحقق من شخصية المستخدم عند دخوله على موقع

المصرف أو عند قيامه بطلب إحدى الخدمات المصرفية التي يقدمها المصرف. وذلك نظراً لما تتمتع به هذه التقنية من قبول عام وسهولة في الاستعمال من جانب المستخدمين من ناحية، كما أنها ذات قدرة على التكيف مع أنظمة العمل المختلفة من ناحية أخرى. وتُعرف كلمة المرور بأنها: «شكل من أشكال التحقق السري من شخصية المستخدم، وذلك بهدف التحكم في عملية الدخول للمصرف الإلكتروني، والتي تُحفظ بعيداً عن الاطلاع من قبل الأشخاص غير المسموح لهم بالتعامل مع المصرف الإلكتروني»^(١).

ويفرض استخدام كلمة المرور مجموعة من الالتزامات على عاتق المستخدم والمصرف.

فبالنسبة للمستخدم:

- يلتزم بالحفاظ على كلمة المرور ضد أي محاولة للتعرف عليها من قبل الغير.
 - يلتزم المستخدم دائماً بتوخي الحذر الشديد عند تعامله مع المواقع الإلكترونية أو أثناء تعامله عبر شبكة الإنترنت وعدم الدخول إلى مواقع غير موثقة أو معتمدة^(٢).
- أما بالنسبة للمصرف:
- يلتزم بمراقبة مدى طول كلمة المرور التي يقوم المستخدمون باستعمالها ومتطلبات تركيبها.
 - يلتزم بالسيطرة على كل طرق الدخول للمصرف الإلكتروني والخروج منه.

^(١) د. علاء التميمي، مرجع سابق، ص ٦٤٦.

^(٢) خديجة سلطاني، مرجع سابق، ص ١٠٧.

- يلتزم بمراعاة انتهاء صلاحية كلمة المرور وحالات إلغائها في حال انتهاكها^١.
- وتتعدد الطرق التي يمكن من خلالها انتهاك سرية كلمة المرور ومن أشهر هذه الطرق:
- اقتحام الملفات الخاصة بكلمة المرور والتي قد يحتفظ بها المستخدم على الكمبيوتر الخاص به.
- النقاط كلمة المرور أثناء استخدامها من قبل المستخدم، حيث قد يلجأ المستخدم إلى استخدام كلمة مرور واحدة لعدة استخدامات على شبكة الإنترنت، الأمر الذي يأخذه المعتدي في اعتباره عند تخمين هذه الكلمة.

٢- **الخادم المفوض:** يقوم بدور الوسيط بين الشبكات المؤمنة والشبكات غير المؤمنة. فعن طريقه يستطيع صاحب المصرف رصد حركة موظفيه على شبكة الإنترنت، كما يمكن التحكم في عملية الدخول إلى موقع معين عن طريق إعطائه أمراً بعدم الدخول إلى الموقع المعين ذاته، فعندما يرغب أحد العاملين الدخول إلى الموقع يمنعه المفوض. وغالباً ما يتم اقتران الجدران النارية مع الخادم المفوض لضمان التحكم في عمليات الدخول والخروج وتحقيق التأمين الكامل للشبكة^٢.

^١ انظر أحد نماذج البنوك العاملة على شبكة الإنترنت، متاح على الرابط:

Bank of internet USA, privacy policy, January, 200 b, [www. Bank of internet.com/privacy policy.aspx](http://www.Bank of internet.com/privacy policy.aspx).

تاريخ الزيارة ١٧/١٠/٢٠١٨ - الساعة ٩.٢٥ P.M

^٢ عمار لوصيف، مرجع سابق، ص ٩٩.

٣- **الجدران النارية:** تلعب الجدران النارية دوراً محورياً في مجال تأمين البيانات، حيث تعمل كحاجز صد في مواجهة جميع المسارات القادمة للمصرف من شبكة الإنترنت، كما تمنع دخول الأخطار القادمة من شبكة الإنترنت إلى الشبكة الداخلية الخاصة بالمصرف، وذلك من خلال التأكد والتحقق من هذه المسارات ثم تحديد ما إذا كان يسمح لها بالمرور من عدمه.

وتعرّف هذه الجدران بأنها: (مجموعة من الأنظمة توفر وسيلة أمنية بين الإنترنت وشبكة المؤسسة الداخلية حيث تجبر جميع عمليات الدخول إلى الشبكة الداخلية والخروج منها للمرور عبر هذا الجدار الذي يتصدى لجميع محاولات الدخول للشبكة دون صفة^(١)).

ويتميز جدار الحماية بمجموعة من الميزات^(٢):

- يجب أن يتم كل مرور من الخارج إلى داخل الشبكة أو الخروج منها عبر جدار الحماية.
- يسمح بالمرور للمصرح له فقط كما هو معرف في سياسة الأمن المحلية.
- يكون الجدار نفسه مستثنى من الاختراق.

كما يتكون جدار الحماية من مجموعة من المكونات الأساسية^(٣):

- السياسة الأمنية: مجموعة القواعد الأمنية الواجب تطبيقها من قبل الجهة المصدرة الراغبة بحماية شبكتها عند ربطها بالإنترنت.

^(١) د. حوالف عبد الصمد، مرجع سابق، ص ٤٦٦.

^(٢) خديجة سلطاني، مرجع سابق، ص ١٠٢.

^(٣) شيروف فضيلة، أثر التسويق الإلكتروني على جودة الخدمات المصرفية دراسة حالة بعض البنوك في الجزائر، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، الجزائر، ٢٠١٠، ص ١٠٧.

- مرشحات الحزم: المقصود بترشيح الحزم حماية الشبكات الداخلية للبلدان والشركات من الثغرات الأمنية الناتجة عن بنية بروتوكولات الاتصالات المستخدمة في شبكة الإنترنت، من خلال مراقبة حزم البيانات الداخلية من الشبكة العالمية إليها.
 - بوابة التطبيقات: وهي البرامج والخدمات الشبكية التي تساعد المستخدم في الدخول إلى حواسيب أخرى في الشبكة أو تمكنه من نقل أو تصفح المعلومات الموجودة في شبكة الإنترنت.
- وبالنتيجة فإن الهدف الأساسي لهذه البرامج هو التغلب على أكبر قدر ممكن من الثغرات الأمنية، من خلال بناء قناة اتصال توجه عليها المراسلات والمعلومات المتبادلة مع شبكة الإنترنت لمراقبتها والسيطرة على خروجها أو تحولها من وإلى شبكتها الخاصة وفق أسس وقواعد يتم تحديدها من قبل الجهات المصدرة.

ثانياً: بروتوكولات تأمين البيانات.

تتعرض التجارة الإلكترونية لمجموعة من مخاطر القرصنة والاختراق عبر الشبكة، هذا ما دفع بعض من مؤيدي تطوير التجارة الإلكترونية بصفة عامة والدفع الإلكتروني بصفة خاصة، إلى وضع العديد من البروتوكولات الأمنية بهدف تأمين المراسلات عبر الإنترنت من جهة ومنح الثقة للمتعاملين من جهة أخرى مما يساعد على تطوير نظام الدفع الإلكتروني. ولعل أهم هذه البروتوكولات:

١- بروتوكول الحركات المالية الآمنة (Set)

(Secure Electronic transaction). يهدف هذا البروتوكول لضمان الحفاظ على أمن البيانات أثناء إجراء الحركات المالية

عبر شبكة الإنترنت. ويستخدم هذا البروتوكول برمجيات تُدعى **برمجيات المحفظة الإلكترونية**، حيث تحتوي هذه الأخيرة على رقم حامل البطاقة والشهادة الرقمية التابعة له، أما التاجر فتكون له شهادة رقمية صادرة من أحد المصارف المعتمدة. ويستخدم كل من الحامل والتاجر الشهادة الرقمية التابعة له بهدف التحقق من هوية الآخر عند إجراء الحركة المالية عبر الإنترنت^١. ولا يمكن للتاجر مشاهدة رقم البطاقة الائتمانية أثناء استعمال بروتوكول الحركات المالية الآمنة، حيث ترسل الصيغة المشفرة لهذا الرقم إلى مصدر هذه البطاقة للموافقة على إجراء الحركة المالية مع التاجر، بحيث تضمن هذه الطريقة عدم عرض الرقم كما تمنع أي تعديل غير مرخص به أثناء إرسال البيانات. ويعتمد نظام (Set) على قيام جهة ذات ثقة عالية (هيئة الاعتماد) على إنشاء وحدة استخراج هويات إلكترونية لكل من المستخدم والتاجر على أن تستخرج هذه الهويات بطريقة مضمونة بعد التأكد من هوية المستخدم ويتم حفظها وتداولها بطريقة مؤمنة^٢. ويتمتع هذا النظام بالكثير من الضمانات منها:

- السرية: من خلال تشفير مضمون الرسالة والمعلومات المتعلقة بها.
- التحقق من شخصية المستخدم والتاجر.
- حماية خصوصية المستخدم بعدم تتبع نوعية مشترياته.
- التكاملية: ضمان أن الرسالة المرسله هي نفسها الرسالة المستقبلة.

^١ خديجة سلطاني، مرجع سابق، ص ١٠٦.

^٢ رائد يوسف، مرجع سابق، ص ١٦٦.

٢- بروتوكول الطبقات الأمنية (SSL) [Secure socket layer]

أدخل من طرف شركة

NET SCAPE COMMUNICATION CORP، ومصمم لضمان إجراء عمليات آمنة على غرار نظام (set) غير أنه يسمح بمعرفة هوية التاجر دون المستخدم، الأمر الذي يربك التجار بل وقد يربك المستخدم نفسه الذي يتعين عليه إرسال رقم بطاقته للتاجر على الخط إذ قد يؤدي ذلك إلى استعمال رقمه من طرف غيره. وأهم ميزة في هذا البروتوكول هي البساطة في الاستعمال فهو لا يتطلب توفير أجهزة خاصة فهو متوفر ضمن برامج التعامل مع الإنترنت مثل (INTERNET EXPLORER MS أو NET SCAPE أو OPERA أو MICROSOFT^٢). كما أن تكلفته أقل مقارنة بالتكلفة في بروتوكول Set. إن هذه المزايا جعلت من بروتوكول SLL واسع الاستعمال لدى معظم رواد الإنترنت خاصة المشتريات الصغيرة كتحميل بعض البرامج أو تحميل الكتب أو دفع تكاليف التشغيل^٣.

^١ عمار لوصيف، مرجع سابق، ص ٣٠٧.

^٢ د. رحيم حسين وهواري معراج، الصيرفة الإلكترونية كمدخل لعصرنة المصارف الجزائرية، مداخلة في الملتقى الوطني الأول للمنظومة المصرفية الجزائرية والتمويلات الاقتصادية ١٤ - ١٥ ديسمبر ٢٠٠٤، بحث منشور في مجلة المحاسب المجاز، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة الشلف، الجزائر، ص ٣٢٥ متاح على الرابط:

www.ratoul.viola.net/resumcoll.htm

تاريخ الزيارة ١٧/١٠/٢٠١٨ - الساعة ١٠.٣٠ A.M

^٣ المرجع السابق، ص ٣٢٦

٣- تقنية الحماية 3DS: بهدف تطوير الدفع الإلكتروني قامت مؤسسة فيزا بتطوير هذا النظام لتعزيز عملية الدفع عن طريق البطاقات الائتمانية. فهو نظام يوفر أعلى مستويات الحماية لعمليات الدفع عبر الإنترنت. فيساهم في تخفيض نسبة الأخطار والمشكلات التي تحدث خلال عملية الشراء عبر الإنترنت، وذلك من خلال تمكين المصارف المتخصصة في إصدار البطاقات من التحقق من هوية الشخص الذي قام بإجراء المعاملة الإلكترونية كما توفر تقنية 3DS حماية إضافية كون العمليات الإلكترونية تتم أمام الشخص مباشرة^١. وتعتمد هذه التقنية على نظام التشفير (SLL) ومأخذ (Merchant server) لتمرير المعلومات والتأكد من هوية الحامل خلال عمليات الشراء التي تتم عبر الخط. ويجمع هذا النظام بين السهولة ومرونة التطبيق، كما يوفر الانتقال الآمن لنفاصيل الحساب وتخفيض نسبة الأخطاء^٢. وبالنتيجة نجد أن برامج تأمين البيانات وبروتوكولاتها تهدف إلى التحقق من هوية المستخدم وضمان الانتقال الآمن للمعلومات والبيانات عبر شبكة الإنترنت، وذلك بهدف تجنب الكثير من الجرائم الإلكترونية (كعمليات السرقة عبر الإنترنت وعمليات الانتحال للشخصية وعمليات الاختراق للبرامج والأنظمة).

وفي ختام الحديث عن التدابير التقنية، نجد أن دور التوقيع الإلكتروني في نطاق المشكلات الأمنية يتمثل في ضمان الثقة بمعاملات الدفع الإلكتروني من خلال استخدامه بشكله التوقيعي بالرقم

^١ رائد يوسف، مرجع سابق، ص ١٦٩

^٢ المرجع السابق، ص ١٧٠.

السري والتوقيع الرقمي كبديل عن التوقيع التقليدي في إتمام المعاملات الإلكترونية (وخصوصاً المعاملات التي تتم بواسطة البطاقات المصرفية والأوراق التجارية الإلكترونية)، فضلاً عن اللجوء إليه عندما يثار أي نزاع حول وجود اختلاف في الحساب النقدي أو حول كون النقود الإلكترونية نقود مزيفة.

أما بالنسبة لبرامج وبروتوكولات تأمين البيانات فيتمثل دورها في نطاق المشكلات الأمنية من خلال استخدامها كوسائل للتحقق من هوية المستخدم وضمان الحركة الآمنة للمعلومات الإلكترونية، بهدف تجنب الكثير من الجرائم الإلكترونية (كعمليات السرقة وانتحال الشخصية وعمليات الاختراق للبرامج والأنظمة). وبالتالي تجد هذه البرامج والبروتوكولات مجالها في نطاق عمليات الشراء عبر الإنترنت أكثر من البطاقات المصرفية.

ولكن تبقى هذه التدابير في إطار التدابير الوقائية التي تهدف لتلافي حدوث هذه المشكلات دون معالجتها بشكل صريح.

المطلب الثاني

الوسائل الإدارية

تتمثل الوسائل الإدارية بمجموعة من الإجراءات والالتزامات المتخذة من قبل الجهات الرقابية أو الجهات المصدرة لوسائل الدفع الإلكترونية وذلك بهدف التقليل من حدوث بعض المشكلات الأمنية التي تنطوي على خطورة كبيرة. وبالتالي فقد وجهت هذه الأساليب إلى كل من السرقة (وهي مجال بحثنا في الفرع الأول) والتزوير (وهي مدار بحثنا في الفرع الثاني) فضلاً عن الاستخدام غير المشروع وذلك في (الفرع الثالث).

الفرع الأول

الوسائل المتخذة بالنسبة للسرقة

لا تقتصر أسباب السرقة في العالم الافتراضي على ذكاء ودهاء الأشخاص الذين يقومون بذلك، وإنما يساعدتهم في بعض الحالات إهمال أو قصور المعرفة لدى الأشخاص الذين يرتادون الإنترنت. لذلك تحرص الجهات الرقابية على تزويد المصارف العاملة على شبكة الإنترنت بمجموعة من الإشارات الخاصة التي يجب اتباعها للحد من احتمال حصول أعمال احتيالية تؤدي إلى سرقة الحسابات عبر شبكة الإنترنت.

وفي هذا الخصوص أورد التقرير الصادر عن المؤسسة الأمريكية لضمان الودائع FDIC^١ بعض الخطوات ينبغي على المصارف أن تعتمد في سبيل تقليص احتمالات السرقة عبر الإنترنت^٢ وتتمثل في الآتي:

١- تحسين مستوى الكلمات السرية التي يستعملها المستخدم للتصديق على الصفقات المنجزة من قبله حتى يصعب اختراقها. ومثال ذلك (إلزام المستخدم استعمال نوعين من الخصائص المعتمدة من قبله في الكلمات السرية كاستعمال أرقام وأحرف لتشكيلها بدلاً من اعتماد خاصية واحدة).

^١ الوكالة الفيدرالية لضمان الودائع : Federal Deposit Insurance Corporation هي الشركة الأمريكية التي تؤمن الودائع في الولايات المتحدة ضد فشل المصارف وقد أنشئت عام ١٩٣٣ للحفاظ على ثقة الأفراد وتشجيع الاستقرار في النظام المالي من خلال تعزيز الممارسات المالية السليمة.

^٢ مشار إليه لدى د. طارق حمزة، مرجع سابق، ص ٤٤٤ - ٤٤٥.

٢- استخدام البرمجيات التي تقوم بمهام المسح بهدف الحماية بمواجهة هجمات التصيد. ويمكن لهذه البرامج أن تقلص من سرقة حسابات وسائل الدفع الإلكتروني سواء تعلق الأمر ببطاقات الدفع أم بالنقود الإلكترونية.

٣- نشر التوعية وكذلك تقوية البرامج التعليمية للمستخدمين لمساعدتهم على تجنب الوقوع ضحايا أعمال احتيالية عبر شبكة الإنترنت، كأعمال التصيد التي تؤدي إلى سرقة الحسابات وغيرها من أشكال سرقة الهوية، واتخاذ التدابير المناسبة لوضع حد أقصى لمسؤوليتهم في هذا المجال.

٤- التركيز على موضوع تبادل المعلومات بين مختلف القطاعات التي تنظم عمليات الدفع عبر الإنترنت.

وفي مقابل هذه الخطوات فإن التقرير الصادر عن لجنة البنى التحتية للمعلومات المالية والمصرفية FBIIC^١ ومركز تنسيق الخدمات المالية FSSCC^٢، قدم ثمانى خطوات إضافية ينبغي على المصارف اعتمادها لتجنب وقوع المستخدمين ضحايا السرقة^٣ وتتمثل في الآتي:

١- إعطاء رسائل البريد الإلكتروني طابعاً شخصياً خاصاً بالمستخدمين، وذلك بهدف إعطائهم ضمانات أكثر بخصوص شرعية البريد الإلكتروني.

٢- التأكيد على المستخدمين بأن المصارف لن تطلب إليهم الدخول إلى عنوانها الإلكتروني لإدخال معلوماتهم الشخصية.

^١ FBIIC اختصاراً لـ Financial and Banking Information Infrastructure Committee

^٢ FSSCC اختصاراً لـ Financial Service Sector Coordinating Council

^٣ مشار إليه لدى: المرجع السابق، ص ٤٤٥ - ٤٤٦.

٣- ينبغي على المصارف مراجعة الاستثمارات التي تمت تعبئتها عبر عنوانها الإلكتروني، وعدم الطلب إلى المستخدم تقديم معلومات موجودة في ملفاتها.

٤- التحديث الدائم للموقع الإلكتروني لضمان استمرارية ثقة المستخدم بشرعية الموقع.

٥- تذكير المستخدمين بوجوب استخدام الوسائل والبرامج الحديثة عند إجرائهم للصفقات.

٦- يجب على المصارف أن تزود المستخدمين برقم هاتف محلي لإجراء اتصال بالمصرف في حال وجود أي طارئ.

٧- التأكد من عدم خلط المستخدم بين الموقع الشرعي للمصرف وبين موقع آخر وهمي، وذلك عن طريق اعتماد أسماء متشابهة بين المصارف والوكالات التابعة لها.

٨- إنشاء علامة تجارية خاصة بالمصارف بهدف حمايتها من انتحال الغير لشخصية هذه المصارف، وبالتالي احتمال تأثيره على المستخدمين الذين يتعاملون معهم على سبيل الخطأ.

كما أنه وفي سبيل مواجهة مشاكل السرقة والضياع، فقد تم وضع مركز خاص بهذه الحالات يتلقى الاتصالات لمدة ٢٤/٢٤ ساعة وهو مركز تابع لشركة SATIM، والذي بمجرد أن يتلقى اتصال لضياع أو سرقة بطاقة معينة يقوم بوضع البطاقة في حالة معارضة. لكن إذا لم يتلق هذا المركز التأكيد الكتابي من طرف الحامل أو المصرف على ضياع أو سرقة البطاقة خلال مدة ١٥/ يوم فسيقوم برفع الحجز عن البطاقة وتصبح المسؤولية على عاتق الحامل أو المصرف^١.

^١ سليمة مغني، وسائل الدفع الإلكترونية وانعكاساتها على الوطن العربي والجزائر خاصة، رسالة ماجستير، جامعة خميس مليانة، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٣-٢٠١٤، ص ٧٥.

هذا فيما يتعلق بالوسائل المتخذة بالنسبة للسرقة أما بالنسبة للوسائل المتخذة بالنسبة للتزوير فهي مجال بحثنا في الفرع الثاني.

الفرع الثاني

الوسائل المتخذة بالنسبة للتزوير

لا تكمن المشكلة في تزوير أو نسخ بطاقات الدفع الإلكتروني بشكل عام والنقود الإلكترونية بشكل خاص. وإنما تتجلى المشكلة عند إعادة استخدام هذه النقود المزيفة في تسوية المعاملات المالية الإلكترونية أو الحصول على قيمتها من الجهة المصدرة حيث يثور التساؤل حول مسألتين:

أولاً: كيفية اكتشاف التزييف في نطاق النقود الإلكترونية

تختلف أساليب كشف التزييف الذي أصاب النقود الإلكترونية باختلاف الدعامة الإلكترونية:

١- ففي نظام النقود الإلكترونية القائم على آلية الحوافظ الافتراضية^١ التي تستعمل للدفع عبر شبكة الإنترنت مباشرة:

يقوم التجار المتعاملون بهذا النقد بالاتصال بقاعدة البيانات المركزية الخاصة بجهة الإصدار بصدد كل عملية دفع. حيث تحتفظ هذه القاعدة بجميع الأرقام التي تم إصدارها من الجهة المصدرة وتلغي الوحدات التي تم استعمالها. ومتى ظهرت الأرقام المتسلسلة لوحداث النقد المستخدمة في الدفع في قاعدة البيانات، فهذا دليل على صحتها

^١ المحفظة الافتراضية هي مجموعة من الوحدات الإلكترونية المخزنة بذاكرة الكترونية حيث يتم شحن تلك الذاكرة بهذه الوحدات الإلكترونية القابلة للوفاء.

وأنها أصلية أما في حالة العكس فهي مزيفة وبالتالي يتمتع على التاجر قبولها^١.

٢- أما في نظام النقد الإلكتروني القائم على البطاقات الذكية:

فالتعامل مع مشكلة التزوير مع هذه البطاقات يتم بإحدى الطريقتين:
الأولى: تكمن عن طريق تضمين البطاقة الذكية رقاقة خاصة تحتفظ بقاعدة بيانات قادرة على اكتشاف عملية التزوير يُطلق عليها تعبير (رقاقة المراقبة). حيث تحتوي هذه الرقاقة على قاعدة بيانات مصغرة تتضمن كل المعلومات المتعلقة بالوحدات التي زُورت بواسطة البطاقة. فإذا قام الحامل بتزوير بعض هذه الوحدات بهدف استخدامها مجدداً، فإن الرقاقة ستكشف المحاولة وتمنع الصفقة وأي محاولة لإزالة هذه الرقاقة ستؤدي إلى تدمير البطاقة بكاملها^٢.

الثانية: تعتمد هذه الطريقة على التوثيق المالي الذي يقوم به المصدر للكشف عن حالات التزوير. ويقصد بالتوثيق المالي (إجراء مقارنة بين ما تم إنفاقه باستخدام البطاقة ومجموع الأرصدة النقدية الافتراضية التي يمكن تخزينها عليها)، حيث يمثل الفارق بينهما مدفوعات احتيالية ناشئة عن تزوير وحدات النقد الإلكتروني وإعادة إنفاقها مرة أخرى^٣. وتتم آلية التوثيق المالي من خلال آلية تستخدم فيها المفاتيح التشفيرية الخاصة بها والتي من خلالها يتم الكشف عن حالات التزوير وتحديد هوية الشخص الذي قام بالتزوير. ويترتب على هذا النوع من المراقبة النشطة والفعالة لمدفوعات النقود

^١ د. حوالف عبد الصمد مرجع سابق، ص ٤٧٢.

^٢ د. أحمد السيد لبيب إبراهيم، مرجع سابق، ص ٣١٧.

^٣ المرجع السابق، ص ٣١٧.

الإلكترونية تزويد المتعاملين بها بدرجة عالية من اليقين بأن أي محاولة للتزوير سيتم الكشف عنها ومساءلة مرتكبها.

ثانياً: حكم التعامل بالنقود المزيفة.

لعل التساؤل الذي يطرح نفسه في هذا المجال حول ما هو حكم التعامل بالنقود المزيفة فيما لو نجح أحد المستخدمين في تسوية التزاماته بهذه النقود. فما هي العقوبة المفروضة بحقه؟ وهل يعد هذا الوفاء صحيحاً مبرئاً للذمة وبالتالي يمكن للتاجر الرجوع على المصدر بقيمة هذه النقود أو في حال تمكن الحامل من استبدال النقود المزيفة بنقود تقليدية فهل يمكن للمصدر الرجوع على الحامل ومطالبته بالرد؟

١- بالنسبة للنقود التقليدية

في الحقيقة نص المشرع السوري على الجرائم المخلة بالنقود العامة في الباب الخامس من قانون العقوبات وهي تقوم في جوهرها على الكذب الذي يتناوله المشرع بالتجريم عندما يتناول شكلاً معيناً وتعد هذه الجرائم من الجرائم المضرة بالمصلحة العامة لما تمثله من وحدة المصلحة التي يقع عليها الاعتداء (الثقة التي يضعها افراد المجتمع في النقود) لأهميتها في تعاملاتهم اليومية والتي يكسبها القانون أهمية خاصة. وقد هدف المشرع السوري من وراء تجريم كل اعتداء يتناول العملة بما فيها التزييف والتزوير والتقليد إلى حماية الثقة العامة التي ينبغي توفرها في العملة لكي تؤدي دورها كأداة وفاء في التعاملات المحلية والدولية على حد سواء ولما تمثله

هذه الأفعال من اعتداء على حق الدولة في سك العملة وإصدارها باعتباره من الحقوق المقررة لها قانوناً وينبغي أن نشير بدايةً إلى أن المشرع السوري قد جرم في نطاق تزيف العملة أو تقليدها الأفعال الآتية:

- كل تقليد عملة ذهبية أو فضية أو أي أوراق عملة أخرى متداولة قانوناً أو عرفاً في سورية أو أي دولة لأخرى بقصد ترويجها.
- كل من اشترك وهو عالم بأمره بإصدار العملة المقلدة أو ترويجها أو إدخالها إلى سورية أو أي بلد أجنبي^١.
- كل من أقدم بقصد ترويج عملة متداولة قانوناً أو عرفاً على تزيفها إما بإنقاص وزنها أو بطلائها بطلاء يتوهم منه أنها أكثر قيمة.
- كل من اشترك وهو على بينة من الأمر بإصدار عملة مزيفة أو بترويجها أو إدخالها إلى سورية أو أي بلد أجنبي^٢.
- كل من قلد أوراق نقد أو زور أو حرّف في قيمة هذه الأوراق بقصد ترويجها.
- كل من اشترك وهو عالم بأمره بإصدار أوراق مقلدة أو ترويجها أو إدخالها إلى سورية أو إلى بلد أجنبي^٣.
- كل من صنع أو عرض أو نقل بقصد الاتجار قطع معدنية مقلدة أو أي عملة متداولة قانوناً أو عرفاً في سورية أو في أي

^١ المواد/٤٣٠-٤٣١/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ المادة/٤٣٢/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٣ المادة/٤٣٣/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

بلد أجنبية أو أي أوراق مطبوعة قد يقع التباس بينها وبين الورق النقدي أو أوراق المصارف الوطنية أو الأجنبية^١.

- كل من قبض عن حسن نية نقود مزيفة ومن ثم روج لها بعد أن تحقق من عيوبها^٢.
- كل من أعاد التعامل بعملات أو نقود بطل التعامل بها وهو عالم بأمره^٣.
- كل من صنع الآلات أو أدوات معدة لتقليد أو تزيف العملة أو تزويرها أو حصل عليها بقصد استعمالها أو اقتنى تلك الأدوات^٤.

وبالنتيجة نجد أن المشرع السوري قد جرم كل فعل من شأنه المساس بالعملة الوطنية أو الأجنبية (تزيف-تزوير-تقليد-ترويج أو الاشتراك في هذه الجرائم)، أما فيما يتعلق بحكم التعامل بهذه النقود (النقود المزيفة) فإننا نميز بين حالتين:

الحالة الأولى : من قبض نقود مزيفة عن حسن نية (أي أن من قبض هذه العملة وكان يجهل حقيقتها عند القبض و يعتقد أنه نقود صحيحة وليست مزيفة) لذلك لجأ للتخلص منها بما لا يلحق له ضرر وإن كان في ذلك ضرر للغير ففي هذه الحالة يعاقب وفق أحكام المادة /٤٣٦/ بعقوبة مخففة.

^١ المادة /٤٣٥/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ المادة /٤٣٦/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٣ المادة /٤٣٧/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٤ المادة /٤٣٨/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

الحالة الثانية: لو كان عالماً بأنها نقود مزيفة وقت القبض ومع ذلك روج لها ففي هذه الحالة لا تطبق عليه أحكام المادة (٤٣٦) وإنما يعاقب بعقوبة ترويح للعملة المزيفة (المادة ٤٣٠ بدلالة المواد ٤٣١-٤٣٢) (٤٣٣-٤٣٢)

٢- بالنسبة للنقود الإلكترونية

في الحقيقة لم نلاحظ أي نص قانوني يجرم التزيف في نطاق النقود الإلكترونية - وإنما جرم المشرع السوري التزوير في نطاق بطاقات الدفع الإلكترونية واستعمال الوسيلة المزورة في السحب أو الوفاء^١ - وهذه ثغرة لدى المشرع السوري لذلك نأمل ان يتناولها في أقرب تعديل يخص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، لذلك سوف نعول على الناحية المدنية باعتبار ان التعامل بالدفع الإلكتروني تحكمه علاقة عقدية. وفي هذا الصدد فقد نص القانون المدني على أنه:

١- في العقود الملزمة للجانبين، إذا لم يوف أحد المتعاقدين بالتزامه، جاز للمتعاقد الآخر بعد أعذاره المدين أن يطالب بتنفيذ العقد أو بفسخه مع التعويض في الحالتين، إن كان له مقتضى.

٢- ويجوز للقاضي أن يمنح المدين أجلاً إذا اقتضت الظروف ذلك، كما يجوز له أن يرفض الفسخ إذا كان ما لم يوف به المدين قليل الأهمية بالنسبة إلى الالتزام في جملته^٢.

وبعملية اسقاط للنص السابق على التعامل بالنقود الإلكترونية المزيفة نستنتج الاتي:

^١ المادة (٢٢/ب-١٠٢) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم

١٧/ لعام ٢٠١٢.

^٢ المادة ١٥٨/ من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

حيث أن التعامل بالنقود الإلكترونية تحكمه عقود مبرمة بين الأطراف ويترتب على هذه العقود عدة التزامات قانونية وأي اخلال بهذه الالتزامات يستوجب إما إعادة الوفاء بهذا الالتزام أو فسخ العقد . وبما أن الوفاء بنقود مزيفة يشكل نوعاً من الاخلال بهذه الالتزامات لذلك ينبغي النظر إلى هذا الوفاء وكأنه لم يكن لما ينطوي عليه من غش، فالغش يفسد كل شيء ويجعل الطرف المتعاقد مخالفاً بالتزاماته الأمر الذي يستوجب إعادة دفع الثمن أو فسخ العقد مع المطالبة بالتعويض في كلا الحالتين وذلك لأن الوفاء بنقود مزيفة غير مبرر للذمة. ولكن تطبيق أحكام هذه المادة في نطاق النقود الإلكترونية يستوجب شرطين:

الأول: أن لا ينسب إلى الطرف الذي يحتج بالغش أي إهمال أو تقصير في اكتشاف حقيقة النقود المزورة لحظة الوفاء.

الثاني: أن لا ينسب إلى الطرف الذي يحتج بالغش أي إهمال أو تقصير في اتخاذ إجراءات الرجوع على القائم بالدفع في وقت معقول.

وفي هذا الصدد استقر القضاء الأمريكي على أن الدفع الذي يتم باستخدام عملات مزورة ينظر إليه باعتباره كأن لم يكن، وذلك لما ينطوي عليه من غش^١.

إذاً وبالنتيجة يمكننا القول إن الغش يفسد كل شيء ويجعل الوفاء غير مبرر للذمة، وبالتالي بإمكان أي شخص (التاجر أو المصدر) أن يحتج بمواجهة هذا الوفاء طالما أنه لم ينسب له أي إهمال في التحقق من حقيقتها أو في الرجوع على الدافع.

والآن ننقل الحديث عن الوسائل المتخذة بالنسبة للاستخدام غير المشروع.

١. طارق حمزة، مرجع سابق، ص ٤٤٧.

الفرع الثالث

الوسائل الإدارية المتخذة لتلافي الاستخدام غير المشروع

لا تقتصر هذه الوسائل على الجهات المصدرة فحسب وإن كانت هي الجهة المسؤولة عن تلافي الاستخدام غير المشروع، بل على العكس يلتزم كل من الحامل والتاجر باتخاذ مجموعة من الوسائل والتدابير التي تأخذ شكل التزامات قانونية على عاتقهم بهدف التقليل من حدوث الاستخدام غير المشروع. لذلك وفي سبيل التعرف على الوسائل الإدارية لتلافي الاستخدام غير المشروع سوف نتحدث عن الوسائل الإدارية المتخذة من قبل المصدر (أولاً) ثم ننتقل للحديث عن الوسائل الإدارية المتخذة من قبل الحامل (ثانياً) على أن نتعرف (ثالثاً) على الوسائل الإدارية المتخذة من قبل التاجر.

أولاً: الوسائل الإدارية المتخذة من قبل المصدر.

تتطوي الوسائل الإدارية المتخذة من قبل المصدر على مجموعة من الإجراءات نجلها في الآتي:

١- وضع قيود (حدود) على القيم المخزنة وتاريخ عملها

في سبيل حماية وسائل الدفع الإلكتروني تعمل الجهات المصدرة على اتخاذ عدة أمور:

أ- وضع حدود للقيم التي يمكن تخزينها على وسيلة الدفع الموجودة في حوزة المستخدم أو التاجر.

ب- بالنسبة للوفاء: نفرق عند استخدام البطاقة في جهاز يدوي أو في جهاز إلكتروني (P.O.S):

فإذا استخدمت البطاقة في جهاز يدوي فإن السقف المسموح به لجميع البطاقات هو (صفر)، وبالتالي يجب الحصول على تفويض من

المصدر عن كل عملية مهما كان مبلغها. ويشكل هذا الأسلوب نوع من رقابة المصدر على استخدام البطاقة في الوفاء لأنه بهذه الطريقة لا يمكن للتاجر معرفة رصيد البطاقة.

أما إذا استخدمت البطاقة في جهاز إلكتروني فإنه عند تمرير البطاقة يظهر على الجهاز فيما إذا كانت العملية المراد الوفاء بها ضمن حدود الرصيد أو تتجاوزه، فإذا كانت متجاوزة يظهر على الشاشة كلمة (رفض) ما لم يحصل التاجر على تفويض من المصدر عن هذه العملية^١.

أما بالنسبة للسحب من أجهزة الصرّاف الآلي: فإن أغلب الجهات المصدرة تسعى لوضع حد أقصى لمقدار المبلغ الذي يمكن سحبه يومياً من أجهزة الصرّاف الآلي، كنوع من الرقابة التي تمارسها الجهات المصدرة على بطاقات الدفع الإلكتروني بهدف تلافي الاستخدام غير المشروع. ويختلف هذا الحد باختلاف البطاقة أو باختلاف الجهات المصدرة (فعلى سبيل المثال الحد الأقصى لبطاقة الصرّاف الآلي الصادرة من المصرف العقاري / ٦٠ ألف / بينما الحد الأقصى لبطاقة الصرّاف من المصرف التجاري / ٧٠ ألف / في سورية).

ب-تعتمد معظم الجهات المصدرة إلى وضع حدود لصلاحيّة البطاقة وهذا من شأنه الحد من عمليات الاحتيال، كون وسيلة الدفع المعدلة بطريقة احتيالية ستكون صالحة للعمل خلال فترة محددة فقط وبذلك يمكن أن يحد من أضرارها.

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني ، مرجع سابق، ص ١١٦.

وتعد هذه الطرق السالفة الذكر من العوامل الأمنية البالغة الأهمية بالنسبة لأنظمة الدفع الإلكتروني. حيث تسهم في تحقيق هدفين:
 الأول: تمكّن الطرق السابقة من احتواء حجم الخسائر التي يمكن أن تلحق بوسيلة الدفع نتيجة أعمال احتيالية ناجحة.
 الثاني: يتمثل في ردع محاولات الاحتيال من خلال تقليص الكسب المادي للمحتالين، فأى مهاجم سيكون بحاجة لنسخ أو تعديل أكبر عدد ممكن من وسائل الدفع، لكي يحصل على منفعة مالية مقابل الجهود المبذولة في الاختراق^١.

٢- سحب البطاقة

طالما أن البطاقة ملك للمصدر ويلتزم الحامل عند نهاية العقد بإعادتها للمصدر ما لم يتم تجديد العقد، فإنه يحق للمصدر سحب البطاقة كنوع من الوسائل الإدارية التي تهدف لحفظ حقوق المصدر ولضمان عدم استخدام البطاقة بطريقة غير مشروعة بعد إلغائها. ويكون سحب البطاقة من قبل أحد جهتين:

أ- سحب البطاقة عن طريق المصدر: يحق للمصدر أن يقوم بإلغاء البطاقة والطلب من حاملها أن يقوم بإعادتها له في أي وقت دون إبداء أية أسباب ودون الحاجة إلى إخطار وهذا الحق ممنوح له باعتباره مالكاً للبطاقة. لكن وفي الواقع حتى يتمكن المصدر من سحب البطاقة لا بد أن يكون إلغائها مستنداً لأسباب جوهرية يخشى معها بقاء البطاقة مع حاملها وإلا عدّ المصدر متعسفاً في استعمال حقه ويتوجب عليه التعويض. وسحب البطاقة لا يكون فقط من الحامل وإنما من أي شخص تكون البطاقة في حوزته كالورثة^٢.

^١ د. طارق حمزة، مرجع سابق، ص ٤٤٠ - ٤٤١.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٤٦٨.

وكما أن سحب البطاقة يكون بالطلب من المصدر بالطرق العادية، فإنه يكون كذلك بالطرق الفنية كبرمجة الصراف الآلي على سحب البطاقة في الحالات الآتية^١:

- إذا تم إدخال الرقم السري بشكل خاطئ ثلاث مرات.
- إذا تم الإبلاغ عن فقد البطاقة أو سرقتها.
- إذا لم يتم الحامل باستلام البطاقة بعد إعادتها من جهاز الصراف خلال (٣٠) ثانية.

حيث تقوم الغاية من سحب البطاقة في الحالات السابقة على فكرة الحد من الاستخدام غير المشروع للبطاقة في مثل هذه الحالات.

ب- سحب البطاقة عن طريق التاجر: يتفق المصدرون للبطاقة بصفته مالكين لها مع التجار بصفتهم وكلاء على أن يقوموا بسحب البطاقة لحساب المصدر، وذلك مقابل صرف مكافآت لهم عن كل بطاقة لتشجيعهم على سحبها. ويكون سحب البطاقة من قبل التاجر للأسباب الآتية^٢:

- إذا كانت البطاقة غير صالحة أو تالفة.
- إذا كانت البطاقة ضمن البطاقات الواردة أرقامها في الكشف التحذيري الموزع على التجار.
- إذا لم يكن مبرز البطاقة هو الحامل الشرعي لها أو شك التاجر في كيفية الحصول عليها.

٣- تسجيل وسائل الدفع

تعتمد الجهات المصدرة لوسائل الدفع الإلكتروني إلى تسجيل معلومات شخصية متعلقة بهوية وعنوان حامل وسيلة الدفع لديها أو لدى

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١١٨.

^٢ د. حوالف عبد الصمد، مرجع سابق، ص ٤٦٨.

السلطة المركزية. حيث من شأن هذا التسجيل أن يساهم في تسهيل إجراء التحقيقات في حال حصول نشاطات احتيالية. ولعل من أهم الوسائل التي تعتمد من خلالها أنظمة الدفع الإلكترونية لتثبيت شخصية المستخدم، هي وجوب ربط المستخدمين والتجار بحساب مصرفي وذلك بمقارنة هذه المعلومات مع مثيلاتها التي تم تدوينها عند التسجيل. أما في أنظمة البرمجيات فعلى المستخدم أن يسجل هويته لدى المصدر لأجل إجراء الصفقات الضرورية الأخرى^١.

وتجدر الإشارة إلى أن تسجيل الجهاز الخاص بالتاجر يبدو أمر غاية في الأهمية، فهو يحتوي على حد أعلى من الأرصدة يتجاوز في ذلك الرصيد الذي في وسيلة الدفع الخاصة بالمستخدم وبالتالي فإن الدخول لهذا الجهاز ومراقبته أمر ضروري لتلافي الاستخدام غير المشروع لوسيلة الدفع الإلكترونية.

٤- تعليق عمل النظام

تسعى العديد من أنظمة وسائل الدفع الإلكتروني وخاصة أنظمة النقود الإلكترونية إلى إيجاد آليات تعمل على تغيير المفاتيح التشفيرية بصورة فورية حال تعرضها لعمليات نصب واحتيال. ولعل التدبير الأكثر فعالية في هذا المجال يتمثل في استبدال البطاقة مكان أخرى أو برنامج مكان آخر إذا حصل شك بشأن تصميم البطاقة أو كان البرنامج معيباً. كما أن مشغلي النظام قد يلجؤون في مواجهة الأعمال الاحتيالية إلى إيقاف عمل كافة الأجهزة والوسائل واستردادها

^١ د. طارق حمزة، مرجع سابق، ص ٤٤١.

وبالتالي تعليق عمل النظام، ولكن هذا الحل قد يردع الاستخدام الاحتمالي لكنه يؤدي لإلحاق الخسارة بالنظام برمته^١.

٥- اللوائح السوداء لوسائل الدفع المرفوضة

ويقصد باللوائح السوداء مجموعة من الأرقام التسلسلية لوسائل دفع مشكوك في صحتها توضع من قبل الجهات المصدرة. حيث تستخدم هذه اللوائح للتحقق من البطاقات عند إجراء الصفقات مما يؤدي إلى سحب البطاقات غير المشروعة من التداول، وذلك من خلال توزيع هذه اللوائح على التجار لمنع إجراء الصفقات بالبطاقات المشكوك بها أو التي تحمل رقماً تسلسلياً ورد في اللائحة. ويتم نشر المعارضة للبطاقات المرفوضة على النحو الآتي^٢:

أ- بالنسبة للجهاز اليدوي: يتم نشر هذه المعارضة لدى التجار المزودين بالجهاز اليدوي عن طريق تزويدهم بقوائم تتضمن أرقام البطاقات غير المقبولة. ومن ثم يلتزم التاجر بمطابقة رقم البطاقة المقدمة له مع الأرقام الواردة في قائمة المعارضة، فإن لم تكن من ضمنها قُبلت البطاقة وإن كانت من ضمنها سُحبت البطاقة. وأي إخلال من جانب التاجر بهذا الالتزام يجعله متحماً عبء ذلك من خلال عدم صرف قيمة الفاتورة من قبل المصدر.

ب- بالنسبة للجهاز الإلكتروني (P.O.S): يتم نشر المعارضة في هذه الحالة بشكل إلكتروني، حيث يتم تزويد الجهاز الموصول بكمبيوتر المصدر بأرقام البطاقات غير المقبولة، وبمجرد تمريرها على الجهاز يقوم تلقائياً بتحديد ما إذا كانت البطاقة مقبولة أم لا.

^١ المرجع السابق، ص ٤٤٣.

^٢ د. أمجد الجهني، المسؤولية المدنية عن الاستخدامات غير المشروعة لبطاقات الدفع الإلكتروني، مرجع سابق، ص ١٢٠.

ج- بالنسبة لأجهزة الصراف الآلي: يتم نشر المعارضة من خلال برمجة جهاز الصراف الآلي الموصول بكمبيوتر المصدر على عدم قبول البطاقات المسروقة أو المفقودة في سحب النقود وعدم إعادتها.

ثانياً: الوسائل الإدارية المتخذة من قبل الحامل.

تتمثل هذه الوسائل بمجموعة من الالتزامات القانونية التي يلتزم بها الحامل بهدف المحافظة على البطاقة من الضياع أو السرقة أو بهدف المحافظة على الرقم السري حتى لا تقع البطاقة في يد غير صاحبها فيقوم باستخدامها بشكل غير مشروع. وتتلخص هذه الوسائل في الآتي^١:

- ١- وضع البطاقة في مكان آمن وأن لا تترك في مكان تسهل فيه سرقتها أو ضياعها.
- ٢- أن لا يقوم الحامل بإعطاء البطاقة لأي شخص حتى لو كان أحد أصوله أو فروعه.
- ٣- أن لا يقوم بكتابة الرقم السري على جسم البطاقة أو أي ورقة منفصلة وإنما يجب حفظه غيباً.
- ٤- يجب على الحامل أن لا يقوم بترديد الرقم السري أمام أي شخص وأن يحرص أن لا يشاهده أحد وهو يقوم بإدخاله في جهاز الصراف.
- ٥- يجب على الحامل عدم ترك الوصل المطبوع من جهاز الصراف وأن يقوم بإتلافه كونه يحتوي على رقم حسابه.
- ٦- يجب على الحامل أن لا يرمي نسخ الفاتورة التي يعطيها التاجر له بل عليه الاحتفاظ بها كونها تحتوي على رقم البطاقة.

^١ د. أمجد الجهني، جرائم بطاقات الدفع الإلكتروني عبر شبكة الإنترنت، مرجع سابق، ص ٣٤.

- ٧- يجب على الحامل عدم استخدام بطاقته لدى المحلات التجارية الصغيرة أو المشكوك فيها.
- ٨- يجب على الحامل إبلاغ المصدر فوراً وبأى وسيلة عند فقد البطاقة أو ضياعها ومن ثم يؤكد الإبلاغ خطياً.
- ٩- على الحامل عند الشك أن الرقم السري قد عُرف أن يطلب من المصدر إلغاء البطاقة.
- ١٠- أن يحرص الحامل على أن لا يكون في حسابه إلاّ مبالغ قليلة حتى لا تكون الخسارة كبيرة في حال السحب من الغير.
- ١١- على الحامل أن يطلب من المصدر بأن لا يسمح للتاجر بتجاوز الرصيد إلا إن كان هو شخصياً من قام بالاتصال بالمصدر.
- وإلى جانب هذه الوسائل، ينبغي على الحامل أن يتخذ عدة أمور قبل إجراء أي عملية شراء أو طلب خدمة عن طريق الإنترنت وتتمثل في الآتي^١:
- ١- تأكد الحامل من وجود اتصال آمن وذلك بالتأكد من وجود كلمة (<https://> بدلاً من <http://>) في بداية عنوان الموقع.
- ٢- التأكد من وجود القفل المغلق في أسفل نافذة المتصفح.
- ٣- التأكد من موثوقية الموقع الذي يتعامل معه فلا يعطي رقم البطاقة لمواقع غير معروفة حتى ولو كان الاتصال آمناً بل يجب التعامل مع المواقع الموثوقة.
- ٤- بعد إتمام العملية يطبع الصفحة التي تحتوي على العملية التي قام بها حتى يتمكن من معرفة ماله وما عليه.

^١ المرجع السابق، ص ٣٥

- ٥- عند وصول كشف حساب بطاقة الدفع على الحامل التأكد من جميع المبالغ التي تم تسجيلها على البطاقة.
- ٥- المحافظة على كلمة السر وعدم حفظها على الجهاز وأن لا يسمح للمتصفح بتذكرها.
- ٦- أن يحرص الحامل على استخدام النسخ الحديثة من المتصفحات التي تم إصلاح الثغرات الأمنية فيها.

ثالثاً: الوسائل الإدارية المتخذة من قبل التاجر

التاجر هو المستهدف الأول من عملية استخدام بطاقة الدفع الإلكتروني استخداماً غير مشروع، كونه هو من سيتحمل الخسائر المالية وربما الدعاوى القانونية. لذا فإن عليه القيام بالإجراءات الآتية:

١- عند تنفيذ عملية الوفاء بواسطة البطاقة فعلى التاجر:

- أ- الطلب من الشخص مقدم البطاقة هويته الشخصية فإن لم يكن الحامل الشرعي فعليه أن يرفض الوفاء بها.
- ب- عدم تجزئة العملية الشرائية الواحدة إلى أكثر من تمريرة واحدة للبطاقة على الجهاز.
- ج- في حال عدم التمكن من تمرير البطاقة على الجهاز فعلى التاجر أن يقوم بختم البطاقة بواسطة الجهاز اليدوي أو رفض البطاقة.
- ء- التثبت من وجود توقيع على البطاقة وقت الشراء، فإن لم يكن عليها توقيع فإنه بإمكان التاجر الطلب من الحامل التوقيع عليها بعد التثبت من هويته.
- هـ- عدم اعتماد رمز التفويض على المعاملة إلا من خلال الجهاز الذي لدى التاجر أو مركز التفويض لدى المصدر.

و- في حال أظهر الجهاز عبارة اتصل بنا أو راجع جهة الإصدار عند تمرير البطاقة، فلا يحاول التاجر تمرير البطاقة مرة أخرى، وعليه الاتصال بمركز التفويض للاستفهام عن الموضوع^١.

٢- على التاجر أن يتأكد من الأمور الآتية:

- أ- أن البطاقة سليمة وسارية المفعول.
- ب- سلامة الشريط المخصص للتوقيع على البطاقة.
- ج- مطابقة رقم البطاقة والتوقيع المدون عليها مع الإيصال الموقع.
- د- البيانات المسجلة على البطاقة مطابقة لبيانات حاملها (الاسم، الجنس، العمر).

٣- أن لا يقبل التاجر:

- أ- أي بطاقة تالفة أو معدل عليها أو ذات شكل غير متعارف عليه.
- ب- أي بطاقة لا تحتوي علامات الضمان.
- ٤- على التاجر أخذ الحيطة من الحامل الذي يتصرف كالاتي:
 - أ- يخرج البطاقة من جيبه بدلاً من محفظته.
 - ب- يقوم عشوائياً بانتقاد سلعة دون الاهتمام بالسعر أو الجودة.
 - ج- يقوم بعمليات شراء صغيرة ومتعددة تبقيهم ضمن الحد الآمن.
 - ٤- يقوم بشراء أغراض ثمينة بواسطة بطاقة صدرت حديثاً.
 - هـ- يبرز جواز سفر لا يوجد عليه ختم لدخول البلاد.
 - و- لا يستطيع تقديم أي هوية عند طلبها.
 - ي- يظهر عليه سلوك عصبي أو تعرق مفرط أو استعجال^٢.

^١ د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني،

مرجع سابق، ص ١٢٤.

^٢ المرجع السابق، ص ١٢٥.

٥- يجب على التاجر أن يكون على علم ودراية فنية بخصائص ومميزات البطاقات المستخدمة حتى يتمكن من اكتشاف أي عمليات تلاعب تصيب هذه البطاقات.

وتجدر الإشارة إلى إخلال الحامل بهذه الالتزامات يجعله مقصراً في التزاماته وبالتالي قد يتعرض لإمكانية عدم قيام المصدر بالوفاء أو تغطية قيمة السلع التي حصل عليها المستخدم بواسطة البطاقة.

وفي ختام الحديث عن الوسائل الإدارية نجد أنها تتطوي على مجموعة من الالتزامات والإجراءات التي كانت للجهات المصدرة النصيب الأكبر منها وإذا ما طبقت بشكل صحيح فإنها تسهم في التقليل من حدوث هذه المشكلات أو اكتشافها ولكن تبقى هذه الوسائل عاجزة عن توفير الحماية الكافية ومرد ذلك إلى أن تطبيق هذه الوسائل الإدارية يتطلب شروط:

الأول: أن يعلم المستخدم أو التاجر بحدوث هذه المشكلات.

الثاني: أن لا يكون المستخدم أو التاجر قد أخل بالتزاماته المفروضة بموجب عقود استخدام وسائل الدفع الإلكتروني.

الثالث: أن يخطر المصدر بهذه المشكلات في سبيل اتخاذ الوسائل المناسبة. ويزداد هذا الأمر صعوبة في نطاق التعاملات الالكترونية التي تقوم في جوهرها على انعدام الوجود المادي وبالتالي من الصعب جداً تقفي أثر هذه الجرائم. وبالنتيجة يمكن القول أنه وفي ظل التفوق التقني لقرصنة الحواسيب في اختراق برامج تأمين البيانات وبروتوكولاتها من جهة وما تتطلبه تطبيق الوسائل الإدارية من التزامات وشروط، تبقى التدابير الوقائية عاجزة عن توفير الحماية الفعالة للمستخدمين والتجار من عمليات السرقة والتزوير والاستخدام غير المشروع الذي ينتاب وسائل الدفع الإلكتروني، الأمر الذي يدفعنا للبحث في المسؤولية الجزائية كأحد التدابير العلاجية للمشكلات الأمنية.

المبحث الثاني

التدابير العلاجية

في ظل عدم فعالية التدابير الوقائية لتكريس العلاج الشامل للمشكلات الأمنية، ظهرت المسؤولية الجزائية كأحد التدابير العلاجية الفعالة باعتبار أن معظم المشكلات الأمنية تتطوي على أفعال جرمية غير مشروعة. ولكن ترتيب المسؤولية الجزائية يتطلب البحث في التكيف الجزائي لهذه المشكلات بغية معرفة مدى إمكانية تطبيق النصوص العقابية النازمة للمعاملات التقليدية أو الإلكترونية على هذه المشكلات. حيث تشكل المسؤولية الجزائية الوسيلة الفعالة والتدبير العلاجي الأكثر وقعاً وأهمية لمعالجة حالات الاستخدام غير المشروع وذلك نظراً للمؤيدات التي تفرض بحق الجاني.

وفي نطاق دراستنا سوف نقتصر الحديث على المسؤولية الجزائية دون المدنية وذلك للمبررات الآتية:

أ- تقوم المسؤولية الجزائية على فرض العقوبات الجسدية والمالية بحق الجاني الأمر الذي يكون له تأثير قوي على الجاني لردعه عن إتيان مثل هذه الأفعال أما المسؤولية المدنية فتبقى أقل وقعاً كونها تقتصر على التعويض المادي.

ب- هناك قاعدة في قانون الأصول الجزائية مفادها أن الجزائي يعقل المدني وهذا يعني أن القاضي الجزائي بإمكانه أن يحكم إلى جانب العقوبة الجزائية بالتعويض المدني.

لذلك سوف نقتصر الحديث على المسؤولية الجزائية دون المسؤولية المدنية باعتبار أن المسؤولية الجزائية أكثر ردة وفعالية في علاج حالات الاستخدام غير المشروع.

وبالتالي وفي سبيل التعرف على المسؤولية الجزائية كأحد التدابير العلاجية للمشكلات الأمنية سوف نتعرف على المسؤولية الجزائية بالنسبة للمشكلات التي تمس أداة الدفع الإلكترونية في المطلب الأول ثم ننتقل للحديث عن المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية في المطلب الثاني.

المطلب الأول

المسؤولية الجزائية بالنسبة للمشكلات التي تمس أداة الدفع الإلكترونية

تتمثل المسؤولية الجزائية من خلال البحث في السبل والأساليب الكفيلة بمعالجة مشكلات التي تمس أداة الدفع بمختلف أشكالها (السرقه - التزوير - الجرائم الإلكترونية). بحيث يتم البحث في التكيف الجزائي لكل مشكلة من هذه المشكلات الثلاثة في ضوء أحكام قانون العقوبات وقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، بهدف معرفة مدى إمكانية تطبيق أحكام هذه القوانين على هذه المشكلات وبالتالي مدى نجاحها في معالجة هذه المشكلات. لذلك سوف يتم الحديث عن مكافحة السرقه في الفرع الأول ثم ننتقل للحديث عن مكافحة التزوير في الفرع الثاني على أن نختم الحديث بمكافحة الجرائم المعلوماتية في الفرع الثالث.

الفرع الأول

مكافحة السرقة

في سبيل تسليط الضوء على العقوبة المقررة بمواجهة السرقة وبالتالي المساهمة في وضع حل جذري لهذه المشكلة، سوف نبحث في عدة فرضيات وذلك على اعتبار أن الأمر قد لا يتوقف على سرقة الأداة بل قد يتمثل بطرح الأداة في التداول أو ما يمكن تسميته استعمال الوسيلة المسروقة أو المفقودة. لذلك سوف نبحث في هذه الفرضيات على النحو الآتي:

أولاً: سرقة بطاقة الدفع الإلكترونية

تتمثل هذه الفرضية في قيام الجاني بسرقة بطاقة الدفع فالسؤال الذي يطرح نفسه ما هو الحكم القانوني لهذه السرقة في قانون العقوبات أو في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية؟ عرّف المشرع السوري السرقة بأنها: «أخذ مال الغير المنقول دون رضاه»^(١).

نستنتج من التعريف السابق أن أركان جريمة السرقة التي تقع على بطاقة الدفع الإلكتروني هي:

١- الركن المادي: يقوم الركن المادي للسرقة على:

فعل الأخذ كنشاط إجرامي إيجابي، يؤدي إلى نتيجة هي حيازة السارق للشيء محل السرقة بإخراجه من حيازة مالكه أو حائزه دون رضاه أو علمه أو بعلمه ولكن دون رضاه إذ تعرض للإكراه والتهديد من قبل السارق، كما أنه لا بد من وجود علاقة سببية

^(١) المادة ٦٢١/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

بين فعل الأخذ ونتيجة الحيازة أي أن يكون فعل الأخذ أدى مباشرة لتحقيق هذه النتيجة.

٢- محل السرقة: لا تقع جريمة السرقة إلا على مال مادي منقول يصلح للتملك. والمقصود هنا (بطاقة الدفع الإلكتروني كجسم مادي منقول)، كما أن الوحدات النقدية الإلكترونية المخزنة داخل البطاقة تصلح بحد ذاتها أن تكون محل لجريمة السرقة باعتبار أنها بيانات يمكن أن يكرس لها وجود مادي.

٣- الركن المعنوي: يجب أن يتوفر القصد الجرمي في حق السارق، ويتمثل هذا القصد بالعلم والإرادة معاً، فالعلم بأن المال المسروق مملوك للغير والإرادة بأن يتم فعل الأخذ للمال أو الشيء (محل السرقة) بإرادة حرة سليمة خالية من أي عيب يعدمها أو يعيبها بنية التملك للشيء المسروق وحرمان صاحبه منه بصفة نهائية وظهور السارق عليه بمظهر المالك^١. فإذا قام السارق بسرقة بطاقة الدفع من صاحبها واتجهت نيته إلى تملكها فإنه يكون مرتكباً لجريمة السرقة. بغض النظر عن السبب الذي دفعه لذلك و سواء أكان يعلم السارق بالرقم السري للبطاقة أم لا.

أما بخصوص العقوبة المفروضة بحق السارق، فإننا ومن خلال استقراء نصوص قانون العقوبات لم نجد نص خاص بسرقة بطاقات الدفع الإلكتروني، كما أننا لم نلاحظ في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية أي نص يجرم

^١د. ثناء المغربي، الوجهة القانونية لبطاقات الائتمان، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ٩٧٩.

سرقة بطاقات الدفع الإلكتروني (وهذه ثغرة لدى المشرع السوري ينبغي تلافيتها)، وإنما وجدنا نص يجرم الحصول دون وجه حق على بيانات أو أرقام بطاقات الدفع الإلكتروني^١ (وهذه ليست مجال بحثنا الآن). فحيث أن جريمة سرقة بطاقة الدفع الإلكتروني غير مذكورة بشكل خاص في قانون العقوبات، الأمر الذي استدعى تطبيق أحكام المادة /٦٣٤/ منه والتي جاء فيها: ((كل سرقة أخرى غير معينة في هذا الفصل تستوجب عقوبة الحبس مع الشغل من شهر إلى سنة والغرامة حتى /١٠/ آلاف ليرة)).

وبالتالي يعاقب سارق بطاقة الدفع الإلكترونية بالحبس مع الشغل من شهر إلى سنة والغرامة حتى /١٠/ آلاف ليرة، ما لم تتوفر أحد ظروف تشديد العقوبة كما لو ارتكبت سرقة الأداة بواسطة شخصين أو تهديد سلاح أو غير ذلك من الظروف^٢ عند ذلك تشدد العقوبة للأشغال الشاقة المؤقتة أو المؤبدة.

ثانياً: فقدان أداة الدفع

تتمثل هذه الفرضية في حال ضاعت أو فقدت بطاقة الدفع الإلكتروني من يد حاملها ثم تمكن أحد الأشخاص من إيجادها والتقاطها ولكن امتنع عن ردها على الرغم من علمه بصاحبها. فالسؤال الذي يطرح نفسه حول (ما هو الحكم القانوني في مثل هذه الحالة)؟

بالعودة لنصوص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية لم نلاحظ وجود أي نص يتناول حالة فقدان بطاقة الدفع (وهذه

^١ المادة (٢٢ /أ) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

^٢ راجع المواد /٦٢٢ - ٦٢٣ - ٦٢٤/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

ثغرة لدى المشرع السوري ينبغي تلافيها) وإنما وجدنا نص يجرم استعمال وسيلة مفقودة (وهي ليست مجال بحثنا الآن). الأمر الذي تطلب منا العودة لنصوص قانون العقوبات، وباستقراء نصوص مواده نجد أنه نص في أحد مواده على أنه: «كل من أمتلك أو اختلس أو رفض أن يرد أو كتم لقطة أو شيء منقول دخل في حيازته غلطاً أو بصورة طارئة أو بقوة قاهرة، يعاقب بالحبس من ٣ أشهر إلى سنتين وبالغرامة حتى ربع قيمة الردود والعطل والضرر على أن لا تقل الغرامة عن ٢٠٠٠/ ليرة»^(١).

نستنتج من النص السابق أنه يطبق على من يجد بطاقة الدفع الإلكترونية ويمتنع عن ردها لصاحبها أو ما يمكن تسميته بكتم اللقطة. إذاً كتم اللقطة جريمة مستقلة تتمثل أركانها في:

١- **محل الجريمة:** أي شيء منقول (البطاقة) ولكن بشرط أن تكون دخلت حيازته عن طريق الخطأ أو لظرف طارئ أو قوة قاهرة، أما إذا تخلف الشرط المذكور أي أن يكون قاصداً أخذ البطاقة فإننا نكون في هذه الحالة أمام جريمة سرقة.

٢- **الركن المادي:** يتمثل هذا الركن بالاستيلاء على بطاقة الدفع وعدم ردها لصاحبها.

٣- **الركن المعنوي:** ويتمثل هذا الركن بالعلم والإرادة. فالعلم أي أن يكون عالم أن هذه البطاقة تعود لشخص معين، والإرادة أن يمتنع عن ردها وهو قاصد ذلك بهدف حرمان مالكيها منها، أما إذا انتفى العلم بصاحب البطاقة فلا مجال لتوفر الجرم^(٢).

^(١) المادة ٦٥٩/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

^(٢) د. محمد نجم، المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الائتمان، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ١١٧٠.

وبالتالي إذا فقد صاحب البطاقة بطاقته نتيجة هفوة أو غلط أو إهمال منه، ثم عثر عليها الجاني (الغير) وكتمها أو امتنع عن ردها لصاحبها أو أنكر عثوره عليها، فهنا يتوافر في حقه جريمة كتم اللقطة المنصوص عليها في المادة /٦٥٩/، والعقوبة هي الحبس من /٣/ أشهر إلى سنتين والغرامة حتى ربع قيمة الردود والعطل والضرر على أن لا تقل عن /٢٠٠٠/ ليرة.

ثالثاً: استعمال وسيلة دفع مسروقة أو مفقودة

ينبغي أن نشير إلى أن استعمال وسيلة الدفع المسروقة أو المفقودة هي نشاط مستقل عن جريمة السرقة أو كتم اللقطة في هذه الفرضية، أي أن الشخص السارق أو كاتم اللقطة شخص مختلف عن الشخص المستعمل، أي أن السارق أقدم على إعطاء الوسيلة المسروقة أو المفقودة لشخص آخر بهدف استعمالها. وحيث أن بطاقات الدفع الإلكتروني قد تستخدم في الوفاء لدى التجار بئمن المشتريات أو قد تستخدم للسحب من أجهزة الصراف لذلك سوف يتم معالجة التكيف الجزائي لكلا الحالتين بهدف الوصول لعلاج جذري لهذه المشكلات.

١- استعمال الوسيلة المفقودة أو المسروقة في الوفاء لدى التجار

عند قيام الغير بسرقة البطاقة أو الاستيلاء عليها بعد فقدانها، فإنه يتجه عادة إلى إعطائها لشخص آخر بهدف استخدامها فوراً مستغلاً بذلك الفترة الواقعة بين تاريخ تقديم البلاغ إلى الجهة المصدرة وبين قيام الجهة المصدرة بإلغاء التعامل بالبطاقة أو التعميم عليها من خلال الأجهزة الإلكترونية (P.O.S) الموجودة لدى التجار والمربوطة بالأجهزة الإلكترونية للمصدر أو قبل توزيع القوائم التي تحمل أرقام البطاقات الملغاة. وغالباً ما يلجأ الغير إلى التعامل بالبطاقة المفقودة أو المسروقة لدى التجار الذين يستخدمون الأجهزة اليدوية،

لأن الحماية للبطاقة تكون أقل بكثير من الحماية الممنوحة للأجهزة الإلكترونية. وعند القيام بهذه العملية نكون أمام احتمالين:

أ- لم تتح للجاني فرصة سرقة البطاقة وإنما اكتفى بسرقة بياناتها:

في هذه الحالة لا يمكن أن تتم عملية الوفاء ما لم يكن هناك تواطؤ بين التاجر والجاني، حيث أن التاجر عادة لا يقبل إتمام عملية الشراء ما لم يبرز البطاقة. وهذا الأمر يتطلب أن يكون التاجر مستخدماً لجهاز يدوي حيث يتمتع بصلاحيّة إدخال البيانات بشكل يدوي ويحصل على تفويض الجهة المصدرة والتي لا يوجد لديها ما يمنع من منح التفويض لأن حامل البطاقة لم يطلب من المصدر إلغاء البطاقة أو وقف التعامل بها لكونه لا يعلم أصلاً بسرقة بياناتها^١.

وفي هذه الحالة يلاحق الجاني بجرم سرقة بيانات بطاقة الدفع والذي نص عليه قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية حيث جاء فيه: (أ- يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة من خمسمائة ألف ليرة إلى مليوني ونصف مليون ليرة سورية كل من حصل دون وجه حق على بيانات أو أرقام بطاقات دفع باستخدام الأجهزة الحاسوبية أو الشبكة^(٢)).

وسيلحق الجاني أيضاً بجرم آخر هو الاحتيال عبر الشبكة بمواجهة المصرف والذي يعتبر التاجر شريكاً فيه. حيث نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه:

أ- يعاقب بالحبس من ثلاث إلى خمس سنوات وبالغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية كل من استولى باستخدام الأجهزة

^١ بشرى سلامة، مرجع سابق، ص ٩٣.

^٢ المادة (٢٢/ أ) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

الحاسوبية أو الشبكة على مال منقول أو عقار أو معلومات أو برامج ذات قيمة مالية أو سند يتضمن تعهد أو إبراء أو أي امتياز مالي آخر وذلك عن طريق خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه بأي وسيلة كانت.

ب- وتكون العقوبة الاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية في الحالات التالية:

١- إذا وقعت الجريمة على ثلاثة أشخاص فأكثر

٢- إذا تجاوز مبلغ الضرر مليون ليرة سورية.

٣- إذا وقع الاحتيال على مصرف أو مؤسسة مالية.

ج- ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي^١.

وبعملية إسقاط النص السابق على هذه الحالة نجد أن:

الجاني بالاشتراك مع التاجر حصل على مال منقول (الحصول على السلعة أو الخدمة)، باستخدام الأجهزة الحاسوبية أو الشبكة (حيث كما هو معلوم أن بطاقة الدفع يتم تمريرها على جهاز يدوي أو إلكتروني أي بمعنى آخر تعمل باستخدام جهاز حاسوبي يدوي أو إلكتروني اعتماد على شبكة الإنترنت)، وقد تم هذا الاستيلاء عن طريق خداع المصرف ومن خلال التلاعب بالمنظومة المعلوماتية (الجهاز اليدوي أو الإلكتروني). حيث تمثل الخداع بادعاء الجاني أنه الحامل الشرعي للبطاقة أي استعمل اسم مستعار أو صفة كاذبة، أما التاجر فقد ادعى أنه تم إبراز البطاقة له وأنه اطلع على بياناتها وسجل هذه البيانات مستغلاً ثقة

^١ المادة (٢١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

المصرف به، فالمصرف ألزمه أن يقوم بالاطلاع على البطاقة وفوضه بإدخال بياناتها بشكل يدوي مما يوحي بأن البطاقة فعلاً كانت أمام التاجر.

وبالنتيجة فإن فعل كل من الجاني والتاجر أدى إلى الاستيلاء على الأموال من خلال استعمال أرقام بطاقة دفع عائدة للغير باستخدام الجهاز الحاسوبي والشبكة وذلك عن طريق خداع المصرف وهذا ما يجعل جرم الاحتيال عبر الشبكة قائم بحق كل منهم. وبالتالي يعاقب الجاني بالاعتقال المؤقت والغرامة من والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية وذلك طالما أن الاحتيال وقع على المصرف ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط الضرر حقه الشخصي^١.

إذاً وبالنتيجة فإن الحالة التي يقوم فيها الغير بالاستيلاء على بيانات البطاقة فقط تجعل الجاني مرتكب لجريمتين في آن واحد: جريمة سرقة بيانات بطاقة الدفع وجريمة الاحتيال عبر الشبكة بالاشتراك مع التاجر وذلك عند استخدام هذه البيانات في عمليات الشراء. وبالتالي فإننا نكون أمام اجتماع مادي ويطبق النص الأشد. جريمة سرقة بيانات بطاقة الدفع يعاقب عليها بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة من خمسمائة ألف حتى مليوني ونصف مليون ليرة. أما جريمة الاحتيال يعاقب عليها بالاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية وذلك طالما أن الاحتيال وقع على المصرف كما أنه ولا تطبق

^١ المادة (٢١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي في جريمة الاحتيال عبر الشبكة. وبرأينا الشخصي فإننا نطبق العقوبة المقررة لجريمة الاحتيال عبر الشبكة باعتباره النص الأشد.

ب- أن يكون الجاني استولى على البطاقة وأصبحت بحوزته:

في هذه الحالة يقوم الجاني بتقديم البطاقة للتاجر للوفاء بقيمة المشتريات، وهنا ينخدع التاجر بهذه البطاقة عندما لا يكون لديه جهاز اتصال مباشر يوضح له أن البطاقة مسروقة أو مفقودة ولم يكن قد وصلت إليه القائمة التي تحمل أرقام البطاقات المسروقة أو المفقودة^١.

استقر الفقه في هذه الحالة^٢ على أن الجاني يُلاحق تحت وصف الاحتيال لاتخاذ صفة كاذبة بإيهامه التاجر أنه الحامل الشرعي للبطاقة وأنه مالك الرصيد وبالتالي فقد انتحل اسم كاذب وهو اسم حامل البطاقة. ونتيجة للعمل الاحتيالي الذي أتاه الجاني يقوم التاجر بإتمام المعاملة استناداً إلى الصفة المتمثلة في كونه الحامل الشرعي للبطاقة.

كذلك يتحقق في فعل الجاني جريمة التزوير في محرر كون الجاني بتوقيعه على الفاتورة يكون قد زور توقيع الحامل الشرعي للبطاقة. وبالتالي يجتمع وصف الاحتيال مع التزوير.

^١ بشرى سلامة، مرجع سابق، ص ٦٤.

^٢ د. عبد الجبار الحنيص، الاستخدام غير المشروع لبطاقة الائتمان المغنطة من وجهة نظر القانون الجزائي، بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٦/، العدد الأول، دمشق، ٢٠١٠، ص ٨٣.

وعلى الرغم من التسليم بصحة ما جاء به الفقه من تكييف جزائي لهذا الجرم، إلا أن المشرع السوري استبعد هذا التكييف حيث نص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنه:

(ب- يعاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية كل من استعمل بطاقة دفع مزورة أو مسروقة أو مفقودة في الدفع أو سحب النقود^(١). ونحن من جهتنا نؤيد ما ذهب إليه المشرع السوري وذلك للاعتبارات التالية:

- إن المشرع السوري كان موفقاً حين اعتبر أن جريمة استعمال بطاقة مسروقة أو مفقودة جرم مستقل نظراً لخطورة هذا النوع من الجرائم من جهة ولحدثة ظهوره من جهة أخرى.
- نُظِم هذا الجرم بنص خاص في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية والخاص يقيد العام الأمر الذي يستتبع استبعاد تطبيق أحكام قانون العقوبات.
- تنظيم المشرع السوري لهذا الجرم بنص خاص من شأنه أن يوفر حماية للمجني عليهم من خلال سهولة التطبيق بخلاف ما إذا ترك تنظيم الأمر لقانون العقوبات، حيث قد يجد القاضي صعوبة في تطبيق أحكام الاحتيال على هذه الجرائم وبالتالي يفلت المجرم من العقاب.
- تطبيق أحكام المادة /٢٢/ لا يشكل نوع من التناقض مع أحكام قانون العقوبات، وذلك على اعتبار أن قانون تنظيم التواصل

^١ المادة (٢٢ / ب، ٢) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم

على الشبكة ومكافحة الجريمة المعلوماتية نص على أنه: ((إذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون تطبق العقوبة التي هي أشد^(١))).

وبالمقارنة بين عقوبة جريمة استعمال بطاقة مسروقة أو مفقودة (الحبس من ثلاث إلى خمس سنوات والغرامة من خمسمائة ألف حتى مليوني ونصف مليون ليرة) وبين عقوبة الاحتيال (الحبس من ثلاث سنوات إلى خمس سنوات والغرامة من عشرة آلاف إلى خمسين ألف ليرة^(٢)). وبين عقوبة التزوير (الحبس من سنة إلى ثلاث سنوات وبغرامة أقلها /٢٠٠٠/ ليرة سورية^(٣)) نجد أن عقوبة جريمة استعمال بطاقة مسروقة أو مفقودة هي الأشد وبالتالي هي التي تطبق.

وبالنتيجة نجد أن استعمال بطاقة مسروقة أو مفقودة في عملية الدفع لدى التجار تستوجب التمييز بين أمرين:

الأول: في حال كان الجاني حائز على بيانات البطاقة فقط فهنا يعاقب بجرم سرقة بيانات بطاقة الدفع وجرم الاحتيال عبر الشبكة ويطبق النص الأشد (الاحتيال عبر الشبكة).

الثاني: في حال كان الجاني حائز على البطاقة بشكل كامل فهنا يعاقب بجرم استعمال وسيلة دفع مسروقة أو مفقودة في الدفع.

^١ المادة (٢٨ / أ) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

^٢ المادة /٦٤١/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٣ المادة /٤٦٠/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

٢- استعمال البطاقة في عمليات سحب النقود

في هذه الحالة فإن وجود البطاقة بين يدي الجاني لا يكفي للاستيلاء على الأموال من جهاز الصراف ما لم يكن عالماً بالرقم السري للبطاقة، باعتبارها من الخطوات الضرورية لإتمام عملية السحب. حيث أن إدخال الرقم السري بشكل خاطئ ثلاث مرات سيؤدي إلى سحب البطاقة تلقائياً من قبل الجهاز. ونحن في حالتنا هذه نعالج مسألة كون الشخص مستعمل البطاقة شخص مختلف عن السارق أو كاتم اللقطة وعالم بالرقم السري لها. فما هو الحكم القانوني لهذه المسألة؟

استقر رأي الفقه^١ على أن الجاني الذي يستعمل بطاقة مسروقة أو مفقودة في سحب النقود يسأل عن جرم الاحتيال ويستبعد وصف السرقة في هذه الحالة على اعتبار أن تسليم النقود كان إرادياً، فالجهاز مبرمج لتسليم النقود إلى من يقوم باتباع الخطوات اللازمة لذلك، ويسأل الجاني عن جريمة الاحتيال لكونه أقدم على اتخاذ صفة كاذبة وهي صفة الحامل الشرعي للبطاقة.

أما بالنسبة للمشرع السوري فقد نص في قانون تنظيم التواصل عبر الشبكة ومكافحة الجريمة المعلوماتية على أنه: «يعاقب بالحبس من ثلاث سنوات إلى خمس سنوات والغرامة من خمسمائة ألف ليرة إلى مليوني ونصف مليون ليرة سورية كل من استعمل بطاقة مسروقة أو مفقودة في سحب النقود»^(٢).

^١ مشار إليه لدى: بشري سلامة، مرجع سابق، ص ٩١

^٢ المادة (٢٢/ب، ٢) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

نستنتج من النص السابق أن المشرع السوري اتجه إلى تجريم استعمال وسيلة مفقودة أو مسروقة في السحب بموجب نص خاص وبالتالي فقد استبعد التكيف الفقهي السائد.

ونحن من جهتنا نؤيد المشرع فيما ذهب إليه من استبعاد تكيف الجرم على أنه احتيال وذلك للمبررات التي سلف ذكرها عند الحديث عن استعمال وسيلة مسروقة في الوفاء لدى التجار من كون الجرم من الجرائم الخطيرة والمستقلة فضلاً عن كون النص الخاص يقيد النص العام، يضاف إلى ذلك أننا نرى أنه من الصعب التسليم بالقول أن استخدام البطاقة في عمليات السحب هو احتيال، لأن الفعل تم بمواجهة آلة وليس إنسان والاحتيال يحتاج لمناورة احتيالية توجه إلى شخص تدفعه إلى تسليم أمواله نتيجة انخداعه بالأساليب التي اتبعها الجاني، وهذا لا يمكن تصوره تجاه آلة لا إدراك لها. وكل ما تم في حقيقة الواقع هو عبارة عن خطوات اتخذها الجاني وترتب عليها وقوع عملية تسليم النقود، وبالتالي فالتسليم لم يكن نتيجة الخدعة التي أتاها الجاني والتي مفادها أنه صاحب البطاقة الحقيقي، فالتسليم كان سيتم بغض النظر عن الشخص الذي يستخدم البطاقة سواء كان حامل البطاقة الحقيقي أم غيره.

وبالنتيجة نجد أن استعمال وسيلة مسروقة أو مفقودة في سحب النقود، يشكل جرم خاص نُظِمَ بواسطة قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بموجب نص قانوني صريح مما يستبعد تكيفه على أنه احتيال.

وينبغي أن نشير إلى أن معظم حالات استعمال وسيلة الدفع الإلكترونية (البطاقة) سواء في عملية السحب أم الوفاء لدى التجار عالجنها من جهة كون أن السارق أو كاتم البطاقة شخص مختلف

عن مستعمل البطاقة، ولكن فيما لو كان السارق هو ذاته مستعمل البطاقة ففي هذه الحالة نكون أمام اجتماع جرائم (جريمة السرقة أو كتم البطاقة) + (جريمة استعمال بطاقة مسروقة أو مفقودة) وفي هذه الحالة نطبق النص الأشد. وغالباً النص المتعلق بجريمة استعمال بطاقة مسروقة أو مفقودة كونه الأشد عقوبة.

إذاً وفي نهاية حديثنا عن مكافحة السرقة، نجد أن المشرع السوري كان سباقاً في التنبيه لخطورة هذه الجرائم وعمل على تنظيم هذه الجرائم بموجب نصوص قانونية صريحة. لكن أغفل المشرع السوري مسألة مهمة تتعلق بجريمة سرقة بطاقة الدفع أو كتمها حيث تعرض لجريمة الحصول على بيانات أو أرقام البطاقات دون وجه حق فقط، وترك السرقة وكتم اللقطة لأحكام قانون العقوبات. لذلك حبذا لو يتم تعديل النص القانوني المتعلق بذلك لتصبح المادة /٢٢/ فقرة أ/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على النحو الآتي:

((يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية:

- كل من حصل دون وجه حق على بطاقة الدفع الإلكتروني أو كتم لقطتها.
- تفرض العقوبة نفسها بحق من يحصل دون وجه حق على أرقام أو بيانات بطاقة الدفع الإلكتروني باستخدام الأجهزة الحاسوبية أو الشبكة)).

الفرع الثاني

مكافحة التزوير

بداية سوف يتم الحديث عن التكييف الجزائي لمن يقوم بتزوير بطاقات الدفع الإلكتروني ثم يتم الانتقال للحديث عن التكييف الجزائي لمن يستعمل هذه البطاقة المزورة سواء في السحب أو الوفاء. حيث أن المشرع السوري نظم التزوير في العديد من النصوص القانونية الأمر الذي يتطلب معرفة التكييف الجزائي لهذا الجرم بغية معرفة النص القانوني الواجب التطبيق وبالتالي إيقاع العقوبة بحقه.

أولاً: عقوبة تزوير بطاقات الدفع الإلكترونية

لقد نظم المشرع السوري التزوير في ثلاثة قوانين (قانون العقوبات، وقانون التوقيع الإلكتروني وخدمات الشبكة، وقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية). لذلك سوف يتم بحث هذه النصوص القانونية لمعرفة مدى انطباقها على صور تزوير بطاقات الدفع الإلكتروني وذلك على النحو الآتي:

١- **في قانون العقوبات:** باستقراء نصوص قانون العقوبات والتي عالجت التزوير^١، نجد أن جميع هذه المواد كانت موجهة للتزوير الذي يقع على الأوراق والمخطوطات الورقية الملموسة وبشكل خاص المحررات الرسمية الصادرة عن الموظفين والجهات العامة. ومن خلال استقراء صور التزوير (السالفة الذكر)^٢ نجد أننا يمكن أن نطبق من نصوص قانون العقوبات النص الآتي:

^١ راجع المواد من ٤٤٣/ حتى ٤٦٠/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

^٢ راجع ص ٢٩٢ وما يليها بخصوص أشكال التزوير في نطاق الدفع الإلكتروني.

(١) من ارتكب التزوير في أوراق خاصة بإحدى الوسائل المحددة في المادتين /٤٤٥ و ٤٤٦/ عوقب بالحبس من سنة إلى ثلاث سنوات وبغرامة أقلها /٢٠٠٠/ ليرة سورية^(١).

لقد سبق وأن تمت الإشارة إلى أن أحد صور التزوير هي تزوير الإشعارات والمستندات المتعلقة بوسائل الدفع الإلكتروني وكذلك الحصول على وسيلة دفع إلكترونية بمستندات مزورة^(٢). وبالتالي نجد أن النص السالف الذكر يمكن أن يطبق على هاتين الصورتين من التزوير ولكن بشروط:

- أن تكون هذه المستندات والإشعارات عبارة عن محررات ورقية ملموسة أي أنها ليست محررات إلكترونية.

- أن يقع التزوير بإحدى الطرق الآتية:

-إساءة استعمال إمضاء أو ختم أو توقيع مزور.

-ما يرتكب من حذف أو إضافة أو تغيير في مضمون المحرر^(٣).

-إثبات وقائع كاذبة على أنها صحيحة.

-تحريف أي واقعة سواء بإغفال أمر أو إيراد أمر غير صحيح^(٤).

ولعل خير أمثلة على عملية التزوير في هذه المستندات (تزوير توقيع أو ختم، تحريف بيانات شخصية أو أي بيانات ذات صلة بالاعتبارات المالية للأشخاص، تزوير الأرقام والمبالغ المالية في الإشعارات

^١ المادة /٤٦٠/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ راجع ص ٣٠٠ وما يليها في هذا الخصوص.

^٣ المادة /٤٤٥/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٤ المادة /٤٤٦/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

بإضافة أو حذف، تزوير التوقيع على فواتير الشراء فيما لو استخدمت البطاقة المزورة في الوفاء لدى التجار).
وبالتالي إذا ما توفرت الشروط السابقة ووقع التزوير فإن نص المادة يطبق على تزوير الإشعارات والمستندات أو على حالة الحصول على وسيلة دفع بمستندات مزورة ويعاقب الجاني بالحبس من سنة إلى ثلاث سنوات وبغرامة أقلها /٢٠٠٠/ ليرة سورية.

٢- في قانون التوقيع الإلكتروني وخدمات الشبكة: باستقراء نصوص قانون التوقيع الإلكتروني وخدمات الشبكة، نجد أنه تناول تزوير التوقيع الإلكتروني وتزوير المحررات الإلكترونية بشكل خاص دون غيرها حيث جاء فيه:

(أ- مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر نافذ يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمائة ألف ليرة سورية إلى مليوني ليرة سورية كل من قام قصداً بارتكاب أحد الأفعال التالية:

٢- تزوير أو تحريف توقيع الإلكتروني أو بيانات أو منظومة إنشاء توقيع إلكتروني بأي طريق كان.

٣- استعمال توقيع إلكتروني مزور أو منظومة إنشاء توقيع إلكتروني محرقة أو شهادة تصديق إلكتروني مزورة مع علمه بذلك.

٥- تقديم أوراق أو معلومات مزورة أو غير صحيحة بقصد الحصول على شهادة تصديق إلكتروني أو تعليق العمل فيها أو إلغائها.

ج- وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار على الأقل وعلى شبكات المعلومات الإلكترونية المفتوحة وذلك على نفقة المحكوم عليه^(١).
وبعملية إسقاط لهذا النص على صور التزوير نجد أن هذا النص يطبق على:

- حالة تزوير الإشعارات والمستندات فيما لو كانت هذه الإشعارات أو المستندات محررة بشكل إلكتروني ووقع التزوير على التوقيع الإلكتروني.
 - حالة الحصول على وسيلة دفع بمستندات مزورة فيما لو كانت هذه المستندات محررة بشكل إلكتروني ووقع التزوير على التوقيع الإلكتروني.
 - حالة الشراء عبر الإنترنت حيث أن المشتري لا بد من توقيع على فواتير الشراء لذلك قد يلجأ لتزوير التوقيع الإلكتروني.
- إذاً وبالنتيجة يمكن القول أن النص السالف الذكر يُطبق على ذات الصور الذي يُطبق عليها النص الوارد في قانون العقوبات، ولكن مع مراعاة الاختلاف في كون نص قانون العقوبات يُطبق على المحررات الورقية الملموسة أما نص قانون التوقيع الإلكتروني يُطبق على المحررات الإلكترونية وسواء أكان التزوير واقع على التوقيع أم المستندات. ولكن ينبغي أن نشير إلى اقتصار القانونين على بعض الصور البسيطة للتزوير دون التعرض لصور التزوير الكلي أو الجزئي والتي تكفل قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بمعالجتها.

^(١) المادة /٣١/ من قانون التوقيع الإلكتروني وخدمات الشبكة رقم/٤/ لعام ٢٠٠٩.

٣- في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية:

نص هذا القانون صراحة على تزوير بطاقات الدفع الإلكترونية بشكل صريح حيث جاء فيه: «يعاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية كل من قام بتزوير بطاقة الدفع»^(١).

يمكن القول وبمنظرة سريعة أن هذا النص جاء عاماً ليشمل كل تزوير يمس بطاقة الدفع الإلكترونية، وفي سبيل تفصيل هذا النص القانوني سوف نقوم ببيان أركان جريمة تزوير بطاقة الدفع الإلكتروني على النحو الآتي:

أ- محل الجريمة: إن محل الجريمة هو بطاقة الدفع الإلكترونية بما تحتويه من بيانات ومعلومات إلكترونية ومكونات مادية.

ولعل التساؤل الذي يطرح نفسه حول هل تعد بطاقة الدفع الإلكترونية بما تشتمل عليه من بيانات إلكترونية محرراً وبالتالي تخضع للتزوير؟

في الواقع لقد ظهر لدينا اتجاهين في هذا المجال:
الأول^٢: يرى أن بطاقة الدفع الإلكترونية لا تعد محرراً وبالتالي لا تخضع للتزوير. حيث يذهب هذا الرأي إلى اعتبار أن المحرر الذي يقوم عليه التزوير هو ورقة مكتوبة ولا شيء غيرها يصلح للتزوير، بينما بطاقة الدفع الإلكترونية ينتفي عنها هذا الوصف باعتبارها قطعة مصنعة من البلاستيك. واستندوا إلى المبررات الآتية:

^(١) المادة (٢٢ ب/١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^(٢) من أنصار هذا الرأي: بشرى سلامة، مرجع سابق، ص ١١٥ - ١١٦.

- المحرر هو ورقة مكتوبة ومقروءة بمجرد الاطلاع عليها.
 - تتنفي مقومات المحرر بالنسبة لبيانات بطاقات الدفع الإلكترونية لعدم إمكانية رؤيتها بالعين المجردة أو بطريقة اللمس ولا يمكن الاطلاع عليها إلا باستخدام وسائل خاصة لقراءة المعلومات المعالجة إلكترونياً.
 - أغلب النصوص الجزائية التي جرمت التزوير لم يرد فيها ذكر إلا لما يُعرف بالأوراق أو المخطوط دون أن يتم التطرق إلى مثل هذا النوع من البطاقات وبالتالي لا يجوز التوسع في تفسير النصوص الجزائية.
- الثاني^١: يرى أنصار هذا الرأي أن بطاقة الدفع الإلكترونية تعتبر محرر وبالتالي تخضع للتزوير. فالبيانات التي تتضمنها البطاقة هي بيانات مكتوبة تعبر عن مجموعة من الأفكار والمعاني الصادرة عن شخص أو جهة أخرى، وبالتالي فإن أي تغيير ينال تلك البيانات يعد تزويراً حتى ولو كانت هذه البطاقة مصنوعة من البلاستيك. واستندوا إلى الحجج الآتية:
- إن أي تغيير في البيانات المعالجة إلكترونياً يعد تزويراً، ومن ثم يمكن قراءة هذه البيانات وفقاً للقواعد والإجراءات الخاصة بها.
 - القول بعدم توافر صفة المحرر على بطاقة الدفع الإلكترونية يؤدي إلى الخلط بين ضرورة معرفة مدلول المحرر بحاسة العين ومدى ظهور هذا المدلول.

^١ من أنصار هذا الرأي: د. عمر سالم، الحماية الجنائية لبطاقة الوفاء (دراسة مقارنة)، ط ١، دار النهضة العربية، مصر، ١٩٩٥، ص ٣١.

- من غير المنطق القول بخفاء معنى المحرر عن العين المجردة واحتياجه إلى إجراءات خاصة ينفي وجوده.

ونحن من جانبنا نذهب إلى اتجاه وسط بين الاتجاهين السابقين مع الميل إلى الرأي الثاني أكثر من الرأي الأول. حيث نعتبر أن بطاقة الدفع الإلكترونية بما تشتمل عليه من مكونات مادية وبيانات معالجة إلكترونياً هي عبارة عن (محرر من نوع خاص) يخضع للتزوير. فبطاقة الدفع الإلكتروني تعد محرراً نظراً لأن:

- المحرر هو كل مكتوب يتضمن علامات يمكن أن ينتقل بها معنى من شخص إلى آخر، ويتطلب إفراغه بشكل كتابي، ولا عبء بنوع المحرر سواء أكان مصنوع من الورق أو البلاستيك ولا عبء بالمادة التي كتب عليها أو بطريقة الكتابة سواء بخط اليد أم بالآلة الكاتبة، وكما هو معلوم بطاقة الدفع الإلكترونية تشتمل على بيانات (الاسم - شعار المصدر - رقم البطاقة....الخ).
- عدم إمكانية تطبيق أحكام قانون العقوبات والمتعلقة بالتزوير على بطاقة الدفع الإلكترونية ليس من شأنه استبعاد صفة المحرر عنه.
- كشف الواقع العملي عن حالات كثيرة لعمليات تزوير بطاقة الدفع الإلكترونية وهذا يؤكد أنها محرر.

كما تعد بطاقة الدفع الإلكتروني محرر من نوع خاص:

- إن بطاقة الدفع الإلكتروني أحد نتائج الثورة التقنية في مجال المعلومات والاتصالات.
- يتم تزوير بطاقة الدفع الإلكترونية بأساليب وطرق تختلف عن التزوير العادي، حيث يقوم التزوير العادي على تغيير الحقيقة بالحك أو المحو أو الإضافة أو التعديل بينما تزوير بطاقة الدفع

الإلكتروني يتم بطرق خاصة (اصطناع - تقليد - تغيير الصورة.... وهذا ما سوف نبثه لاحقاً).

• وجود أساليب خاصة لتزوير بطاقة الدفع الإلكترونية جعل أمر كشف هذا التزوير يتم بأساليب خاصة و حديثة كأجهزة الكمبيوتر.

• لجوء المشرع السوري لتنظيم بطاقة الدفع الإلكترونية واستعمال البطاقة المزورة بموجب نص خاص^١، تأكيداً على أن بطاقة الدفع الإلكترونية هي محرر من نوع خاص فهي محرر يخضع للتزوير ولكن لا يمكن أن تطبق عليه أحكام قانون العقوبات لذلك لجأ المشرع السوري إلى تنظيمها بنص خاص.

ب-الركن المعنوي: تعد جريمة تزوير بطاقة الدفع الإلكترونية من الجرائم العمدية التي تقتضي توافر القصد الجنائي لدى الجاني الذي ينبغي أن يكون معاصراً لارتكاب الفعل الجرمي. والقصد الجنائي في جرائم تزوير بطاقات الدفع الإلكترونية يتحقق حينما يعلم الجاني بتوافر جميع العناصر التي تقوم عليها جريمة تزوير بطاقة الدفع الإلكترونية وأن ما يقوم به من تزوير من شأنه إحداث ضرر بالآخرين وأن تتصرف إرادته إلى هذا السلوك والنتيجة المترتبة عليه^٢.

ج-الركن المادي: يتكون الركن المادي لجريمة التزوير من عنصر أساسي هو تغيير الحقيقة. حيث لا يتصور وقوع التزوير دون حدوث

^١ المادة (٢٢/ب) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

^٢ د. عمر سالم، مرجع سابق، ص ٣٠.

تغير للحقيقة باستبدالها بما يخالفها. وتغيير الحقيقة ينصب على البطاقة عند تزويرها، ويشمل هذا التغيير بيانات البطاقة سواء أكانت (بيانات حاملها الشرعي أم رقم البطاقة المطبوع عليها أم التاريخ المطبوع عليها)، كما قد يمتد التغيير إلى الشريط المغنط الموجود عليها. ويتم التغيير باستخدام عدة طرق وأساليب نذكر منها:

أ- **اصطناع بطاقة الدفع الإلكترونية:** يقصد بالاصطناع خلق الجاني بطاقة جديدة لا وجود لها سابقاً ومن ثم نسبتها إلى مصرف أو جهة تمنحها لا علاقة لها بها ولم تصدر عنها. ويتم صنع البطاقة عن طريق قيام الجاني بوضع الإشعارات عليها، ومن ثم تغليفها بعد وضع الشريط المغنط والشريحة الرقائقية الموجودة بجسم البطاقة وشريط التوقيع، ثم يتم وضع تلك البيانات كل بحسب موقعه الأصلي على جسم البطاقة، ثم تبدأ بعد ذلك طباعة الأرقام والأحرف النافرة على جسم البطاقة عن طريق إنشائها وفقاً للمعلومات التي حصل عليها الجاني بطرقه الخاصة^١.

ب- **التقليد:** يقصد بالتقليد البطاقة صناعة بطاقة دفع شبيهة بالبطاقة الأصلية. وتقليد البطاقة يتطلب وجود بطاقة صحيحة أو منتهية الصلاحية لتمكن الجاني من تزويرها عن طريق تقليد ما عليها من أرقام أو أحرف بأرقام أخرى حصل عليها بطرق غير مشروعة، أو قيامه بتقليد الشريط المغنط الموجود على ظهر البطاقة ونسخ بيانات البطاقة الأصلية إلى البطاقة المزورة. وتتم العملية إلكترونياً أو أن

^١ د. ممدوح العنزي، الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، المجلد ٣١/، العدد ٦٢/، السعودية، ٢٠١٥، ص ٦١.

يقوم بمحو البيانات المخزنة فيه ومن ثم إعادة تشفيره ببيانات أخرى جديدة وصحيحة. وبعد انتهاء الجاني من عملية نقل البيانات إلى الشريط الممغنط فإنه قد يستخدم طريقة أخرى وهي ما تُسمى بطريقة الكشط، وذلك بقيامه بوضع شريط آخر بدلاً منه متضمناً توقيعاً أو أن يقوم بمحو التوقيع الأصلي المثبت على شريط التوقيع ووضع توقيعاً بدلاً عن توقيع الحامل الأصلي وغالباً ما تتم عملية محو التوقيع باستخدام مواد كيميائية^١.

ج- تغيير بيانات البطاقة: وهو إحدى طرق التزوير المادي لبطاقات الدفع الإلكترونية، ويحدث أن يتم التغيير بقيام الجاني بوضع اسمه مكان صاحب البطاقة الأصلي، وذلك بتغيير الأحرف البارزة للاسم على جسم البطاقة أو بزيادة تلك الأحرف أو محوها نهائياً ومن ثم تغيير اسم حاملها إلى اسمه. كما أن تغيير بيانات البطاقة قد يشمل الشريط الممغنط المثبت على ظهرها أو تغيير بيانات البطاقة المقروءة عن طريق إضافة كلمة أو حذف أو شطب ومثال ذلك تعديل التاريخ المسموح من خلاله استخدامها.

وبشكل عام فإن تغيير بيانات البطاقة يتخذ إحدى الطرق الآتية^٢:

- التغيير بالتعديل: ويتحقق ذلك عن طريق الحك أو الشطب أو حذف بيان من بيانات البطاقة ووضع بيانات أخرى محل البيانات التي تم إخفاؤها بالحك أو بالشطب والحذف كتعديل تاريخ الصلاحية.

^١ د. عمر سالم، مرجع سابق، ص ٧٧.

^٢ د. ممدوح العنزي، مرجع سابق، ص ٦٣.

- التغيير بالإضافة: عن طريق إضافة كلمة أو حرف أو رقم للبطاقة.

- التغيير بالحذف: عن طريق محو كلمة أو فقرة أو حرف بطريقة فنية لا تترك بالعين المجردة أو إزالتها بمواد كيميائية.

- تغيير الصورة أو استبدالها بصورة أخرى: ويُقصد به وضع صورة مكان صورة الحامل الأصلي للبطاقة أو تغييرها مستخدماً أحدث الطرق دون أن ينال جسم البطاقة أي تلف.

وبالنتيجة إذا ما توفرت الأركان الثلاثة السالفة الذكر فإن الجاني يعد مرتكباً لتزوير بطاقة الدفع الإلكتروني وفق أحكام قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية ويعاقب بالحبس من ثلاث سنوات إلى خمس سنوات وبالغرامة من خمسمائة ألف ليرة إلى مليوني ونصف مليون ليرة.

وفي ختام حديثنا عن تزوير بطاقة الدفع الإلكترونية، نجد أن المشرع السوري قد نظم صور التزوير في ثلاثة قوانين. حيث تكفل قانون العقوبات بمعاقبة من يُزور الإشعارات والمستندات الورقية إضافة إلى حالة الحصول على وسيلة الدفع بمستندات مزورة (المادة ٤٦٠)، بينما تكفل قانون التوقيع الإلكتروني وخدمات الشبكة بتجريم من يُزور الإشعارات والمستندات الإلكترونية وخصوصاً تزوير التوقيع الإلكتروني إضافة إلى حالة الحصول على وسيلة الدفع بمستندات مزورة (المادة ٣١)، أما بالنسبة لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية فقد جرم تزوير بطاقات الدفع بشكل صريح المادة (٢٢/ب، ١)، وبالتالي تكفل كل قانون من القوانين السابقة الذكر بمعالجة صورة من صور التزوير.

ولكن بقيت حالة التزوير عن طريق تعديل البرمجيات الإلكترونية (كتعديل الرقاقة الكمبيوترية، اعتراض الرسائل الإلكترونية، تعديل الرسائل الإلكترونية) إضافةً إلى حالة تزوير أجهزة (ATM) خارج نطاق أي نص قانوني يجرمها.

لذلك نأمل من المشرع السوري تلافى هذا التنوع القانوني في تنظيم صور التزوير واقتصر على تنظيمها في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية باعتباره القانون الخاص بهذه الجريمة من جهة، والعمل على تجريم حالة التزوير عن طريق تعديل البرمجيات الإلكترونية وحالة تزوير أجهزة (ATM) من جهة أخرى وهذا الأمر لا يتطلب سوى تعديل بسيط للمادة (٢٢/ب، ١)، من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية لتصبح على النحو الآتي:

يُعاقب بالحبس من ثلاث سنوات إلى خمس سنوات وبالغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية :

١- كل من قام بتزوير بطاقة دفع أو أية بيانات أو إشعارات أو مستندات متعلقة بها.

٢- كل تزوير أو تعديل غير مشروع يتناول أجهزة الصراف الآلي أو البرمجيات الإلكترونية بهدف تعطيلها عن عملها.

ثانياً: عقوبة مستعمل بطاقة دفع إلكترونية مزورة

قد لا يتوقف الأمر على تزوير بطاقة الدفع فحسب بل يدق ناقوس الخطر عندما يتم طرح هذه الأداة في التداول، حيث أن مزور أداة الدفع الإلكترونية يبتغي من وراء ذلك استخدام هذه الأداة بشكل غير مشروع سواء في السحب من أجهزة الصراف أم في الوفاء لدى

التجار. وقد يلجأ إلى ذلك بواسطة شخصياً أو بواسطة شخص من الغير. ولذلك وفي سبيل الإحاطة الشاملة بهذا الموضوع سوف يتم البحث في عدة فرضيات على النحو الآتي:

١- استعمال الغير بطاقة الدفع المزورة في السحب من أجهزة الصراف الآلي:

على الرغم مما تتميز به أجهزة الصراف الآلي من الدقة في تنفيذ المعلومات التي تزود بها فضلاً على أن مكونات البطاقة تقوم على تشفير المعلومات الأمر الذي يجعل استعمال بطاقة مزورة أمراً صعباً جداً، لكن ومع ذلك تمكن الجناة من استخدام البطاقة المزورة في سحب النقود من أجهزة الصراف الآلي. ولقد كان الاختلاف واضحاً لدى الفقه والقضاء حول إعطاء التكييف القانوني لفعل من يستعمل بطاقة مزورة في عمليات السحب الأمر الذي تطلب منا التعرض لذلك ثم نبين رأينا الشخصي في ضوء أحكام القانون السوري.

أ- **تكييف الفعل على أنه احتيال:** ذهب بعض الفقه^١ إلى أن استخدام الغير بطاقة مزورة في سحب النقود من أجهزة الصراف الآلي يعد مرتكباً لجريمة الاحتيال مستثنين في ذلك إلى أن استعمال البطاقة المزورة بمثابة استخدام طرق احتيالية لخداع الجهاز الآلي الذي يقوم بسحب النقود. وهو ما قضت به محكمة النقض الفرنسية من أن الجهاز الآلي لتوزيع النقود يمكن خدعه لأنه

^١ د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، ١٩٩٢، ص ١٠٨ + د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة، مصر، ٢٠٠٠، ص ٥٣٣.

يوجد خلفه صاحبه (موظف الجهاز)^١، كما أدانت محكمة استئناف باريس من استعمال البطاقة المزورة عن جريمة الاحتيال وعاقبته بالحبس سنة وبغرامة.... فرنك تطبيقاً لنص المادة /٤٠٥/ جنائي^٢.

إن الأخذ بهذا الرأي يستوجب أن يعاقب الجاني وفق أحكام المادة /٦٤١/ من قانون العقوبات السوري والتي جاء فيها:

(كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء فاستولى عليها احتيالاً

إما باستعمال الدسائس،

أو بتفليق أذوبة أيدها شخص ثالث ولو عن حسن نية،

أو بطرف مهد له المجرم أو ظرف استفاد منه،

أو بتصرفه بأموال منقولة أو غير منقولة وهو يعلم أنه ليس له صفة للتصرف بها،

أو باستعماله اسم مستعار أو صفة كاذبة،

عوقب بالحبس من ثلاث سنوات إلى خمس سنوات وبالعقوبة من عشرة آلاف ليرة إلى خمسين ألف ليرة ولا يستفيد المحكوم من الأسباب المخففة التقديرية أو وفق التنفيذ أو وفق الحكم النافذ إلا في حالة إزالة الضرر^٣).

وفقاً لهذا الرأي يعد الجاني مرتكباً للاحتيال نتيجة استعمال الدسائس واستعمال اسم مستعار أو صفة كاذبة بأنه الحامل الشرعي للبطاقة.

¹Crime 19 MAI 1987 GP. 31 JANV. et 2 FEV 1988, Somm, P8.

مشار لهذا الحكم لدى حوالم عبد الصمد، مرجع سابق، ص ٥٥٨.

²Tribe Paris 306 – 1987.

مشار لهذا الحكم لدى د. محمود طه، مرجع سابق، ص ١١٤٤.

ولكن نحن من جانبنا لا نؤيد هذا الرأي ونعتبر أن فعل الجاني لا يُعد احتيالياً وذلك للمبررات الآتية:

- إن الطرق الاحتياطية التي أشار إليها المشرع السوري يجب أن تربط بين شخصين هما الجاني والمجني عليه، وفي حالتنا هذه لا يتحقق هنا فالعلاقة التي تنشأ عن استخدام بطاقة مزورة في السحب تنشأ بين الجاني وبين الصراف الآلي، ومهما اتصف الصراف من صفات الدقة في تنفيذ العمليات المصرفية لن يرقى لمستوى العقل البشري.
- عندما حُدِّدت أساليب الاحتيال كان الغرض منها أن تكون هذه الأساليب موجهة للإنسان وليست للألة.
- تجريم الفعل على أنه احتيال فيه تحميل للنصوص الجزائية أكثر من اللازم، باعتبار أن المشرعين بشكل عام عالجوا حالات الاحتيال بين الأشخاص وليس بين شخص وآلة، والأخذ بغير ذلك سوف يكون عن طريق القياس وهذا أمر محظور في النصوص الجزائية.
- يقوم الركن المادي للاحتيال على قيام الجاني باستعمال أساليب محددة بهدف إيقاع الغير في غلط ودفعه لتسليم أمواله، أي أن تسليم الأموال يكون عن وعي وإدراك نتيجة لوقوع الغير في الغلط. وهنا في حالتنا هذه التسليم ليس نتيجة الدسائس أو الصفة الكاذبة إنما نتيجة طبيعية لكل من يتبع الخطوات اللازمة للحصول على الأموال وبالتالي انعدام علاقة السببية بين الفعل والنتيجة.
- القول بأن الاحتيال موجه لموظفي المصرف فيه تحميل للنصوص أكثر من اللازم، لأن الاحتيال يتطلب علاقة مباشرة

بين الجاني والمجني عليه إضافة إلى أن الجهاز لا يعود في كل عملية صرف إلى صاحبه، وإنما يتم تنفيذ العملية طالما أن المعلومات متطابقة مع ما تم تلقيه من معلومات ووجود صاحب الجهاز خلفه أمر غير واقعي في ضوء آلية عمله. وبالنتيجة استبعاد تكيف استعمال بطاقة مزورة في السحب على أنه احتيال.

ب- تكيف الفعل على أنه سرقة بمفتاح مصطنع: يرى بعض الفقه المصري^١ مسائلة مرتكب هذه الجريمة عن جريمة سرقة مشددة لاستعماله مفتاح مصطنع. واستندوا في ذلك إلى أن المال خرج من حيازة المجني عليه بغير رضاه، وأن البطاقة المزورة تُعد من قبيل المفتاح المصطنع. على أساس أن المفتاح المصطنع هو كل أداة تقوم بذات الوظيفة التي يقوم بها المفتاح بغض النظر عن شكلها أو حجمها أو المادة المصنوع منها. خاصة وأن البطاقة في حقيقتها مجرد أداة للوصول إلى سحب النقود من الحساب، فالجهاز يعتبر خزانة نقود والرقم السري لبطاقة الدفع هو المفتاح الذي يفتح به الجاني خزانة النقود. وقد أيد القضاء البلجيكي^٢ هذا الرأي وذهب إلى مسائلة مستعمل البطاقة المزورة عن جريمة سرقة بمفتاح مصطنع.

إن الأخذ بهذا الرأي يستوجب أن يعاقب الجاني وفق أحكام المادة ٦٢٥/ من قانون العقوبات السوري والتي جاء فيها: «يعاقب بالأشغال الشاقة كل من أقدم على السرقة في الأماكن المقفلة المصانة بالجدران

^١ د. محمد حماد مرهج الهيتي، الحماية الجزائية لبطاقات الائتمان، دار النهضة العربية، مصر، ٢٠٠٩، ص ٣٧١. و د. هدى قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، مصر، ٢٠٠٩، ص ١٣٤.

^٢ مشار إليه لدى المرجع السابق، ص ٤١٧.

مؤهلة كانت أم لا سواء بواسطة الخلع أو التسلق في الداخل أو الخارج أو باستعمال المفاتيح المصطنعة^١.

وعلى غرار التكييف السابق فإننا من جانبنا لا نؤيد هذا التكييف ونرى أن فعل الجاني لا يعد سرقة مشددة بمفتاح مصطنع وذلك للمبررات الآتية:

- تسليم النقود قد تم إرادياً من قبل الجهاز الآلي لتوزيع النقود بمجرد إدخال البطاقة وكتابة الرقم السري وليس خلسة.
 - البطاقة الإلكترونية لا تعد مفتاحاً مصطنعاً لأن المفتاح المصطنع هو تلك الأداة المستخدمة من قبل الجاني في فتح قفل الباب الخارجي للمكان سواء أكان مفتاحاً مقلداً أم مفتاحاً حقيقياً لباب قلده صاحبه واستعاض عنه بغيره فعثر عليه السارق. وهذا المفتاح يستخدم للدخول إلى المكان الذي سوف ترتكب فيه واقعة السرقة، وهذا لا يتحقق في البطاقة الإلكترونية فهي لا تستعمل في الدخول لمثل هكذا مكان بل هي أداة الجريمة نفسها.
 - القول بأن بطاقة الدفع بمثابة مفتاح مصطنع نوع من القياس وهذا لا يجوز قانوناً.
- وبالنتيجة استبعاد تكييف فعل الجاني على أنه سرقة بمفتاح مصطنع.

ج- تكييف الفعل على أنه استعمال محرر مزور: يرى بعض الفقهاء^١ أن استعمال بطاقة مزورة في السحب يشكل نوع من استعمال محرر مزور ويعاقب وفق هذا الجرم لتوافر أركان هذه الجريمة :

^١ من أنصار هذا الرأي د. محمود طه، مرجع سابق، ص ١١٤٥ و د. حوالف عبد الصمد، مرجع سابق، ص ٥٥٩.

فمحل الجريمة: يرد على محرر مزور وهو بطاقة الدفع المزورة.
الركن المادي: يتمثل بالنشاط المادي لهذه الجريمة في أن يحتج بالمحرر المزور على أنه صحيح وهو ما حدث في هذه الحالة. حيث استعملها حائزها في سحب النقود وانخدع الجهاز بهذه البطاقة وبالتالي تمكن الجاني من سحب النقود بواسطة هذه البطاقة من الجهاز.

الركن المعنوي: يتمثل بتوفر القصد الجنائي لدى مستعملها فهو يعلم أنها مزورة وتتصرف إرادته إلى استعمالها فيما زورت من أجله (سحب النقود). وقد أيد هذا الرأي القضاء في إمارة الشارقة حيث أصدرت محكمة استئناف الشارقة حكماً أدانت فيه أحد الأشخاص بجريمة استعمال محرر مزور عند شرائه لهاتف متحرك ببطاقة مزورة^١.

والأخذ بهذا الرأي يستوجب أن يعاقب الجاني وفق أحكام المادة /٤٤٤/ من قانون العقوبات السوري والتي جاء فيها: ((يعاقب بعقوبة مرتكب التزوير نفسها من استعمل المزور وهو عالم بأمره)).

ونحن من جانبنا لا نؤيد هذا التكييف الفقهي وذلك للمبررات الآتية:

- بالعودة لنصوص قانون العقوبات والتي عالجت موضوع التزوير، نجد أن أحكام المواد موجهة للمحررات الورقية بشكل عام والمحررات الرسمية بشكل خاص. وقد سبق الإشارة إلى أن بطاقة الدفع الإلكترونية محرر من نوع خاص^٢ وبالتالي لا يمكن أن نطبق أحكام قانون العقوبات على

^١ حكم محكمة استئناف الشارقة تاريخ ٢٠٠٣/٦/٣ مشار إليه لدى بشرى سلامة، مرجع سابق، ص ١٠٥.

^٢ راجع ص ٤٤١-٤٤٢.

هذه البطاقة، الأمر الذي يستبعد إمكانية مساءلة الجاني عن استعمال محرر مزور.

- اتجه المشرع السوري إلى تنظيم هذا الجرم بموجب أحكام المادة (٢٢/ب، ٢) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية حيث جاء فيها: (يعاقب بالحبس من ثلاث سنوات إلى خمس سنوات والغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية كل من استعمل بطاقة مزورة أو مسروقة أو مفقودة في الدفع أو سحب النقود).

في الحقيقة يشكل النص السابق دليلاً حاسماً وحجة مقنعة أن المشرع السوري استبعد جميع التكييفات السابقة واعتبر هذا الجرم جريمة مستقلة منظمة بشكل قانوني خاص. وتجدر الإشارة إلى أن المشرع السوري كان موقفاً في هذه الخطوة وذلك للحجج الآتية:

- تعد هذه الجريمة من الجرائم الحديثة التي كشف عنها التطور التقني الأمر الذي يستوجب تبويبها بشكل قانوني.
- تعد هذه الجريمة من الجرائم الخطرة والمنتشرة بكثرة، الأمر الذي استوجب تنظيمها بشكل خاص تجنباً لمحاولات المجرمين الإفلات من العقاب.
- تعد هذه الجريمة من الجرائم الخاصة والتي تتم بأساليب وطرق خاصة يصعب كشفها بالعين المجردة الأمر الذي شكل حاجة ملحة لتدخل المشرع السوري لتنظيمها وتبويبها بشكل قانوني سليم.
- أدرك المشرع السوري عدم كفاية أحكام قانون العقوبات والنصوص الجزائية الأخرى لتنظيم هذا النوع من الجرائم،

لذلك كان لابد من التدخل بقانون خاص ينظمها تلافياً لأي نقص في التشريعات أو أية مشكلات قد تصاحب هذا النوع من الجرائم.

وبالنتيجة تعد جريمة استعمال بطاقة مزورة في سحب النقود من أجهزة الصراف الآلي جريمة مستقلة وخاصة تخضع لأحكام قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

٢- استعمال الغير لبطاقة مزورة في الوفاء لدى التجار:

نعالج في هذه الفرضية الحالة التي يقدم فيها الغير على استعمال بطاقة مزورة للوفاء بأثمان السلع والخدمات لدى التجار، حيث يقبل التاجر الوفاء بالبطاقة ظناً منه أنها بطاقة سليمة وليست مزورة أو مقلدة. أما في حال كان التاجر سيء النية (أي يعلم حقيقة البطاقة) فإنه سيكون شريك للجاني في جرائمه التي يرتكبها.

لقد ظهر في تكييف هذه الحالة اتجاهين:

الأول: يذهب أنصار هذا الاتجاه^١ إلى مساءلة مستعمل البطاقة المزورة في عمليات الوفاء لدى التجار عن جرم الاحتيال. فقد شكل فعل الجاني في هذه الحالة الركن المادي لجريمة الاحتيال استناداً إلى أنه استعمل صفة غير حقيقية، فهذه البطاقة مزورة ولا تعود له مدعياً بذلك أنه صاحب البطاقة الحقيقي. مما أوقع التاجر في وهم أدى إلى إقناعه بأن هناك رصيد لهذه البطاقة، وأنه صاحب الحق بالتصرف بها باعتباره صاحب البطاقة وهذا ما يخالف الواقع. كما أن الجاني عزز الاعتقاد المغلوط الذي خلقه لدى التاجر بأن قام بإبراز البطاقة

^١ من أنصار هذا الاتجاه: بشرى سلامة، مرجع سابق، ص ١٢٦ - ١٢٧ و د. أحمد حسام طه تمام، مرجع سابق، ص ٥٣٣.

إلى التاجر وقدمها على أنها صادرة من جهة معينة مما أوقع التاجر في الغلط الذي ترتب عليه تسليمه البضاعة.

الثاني: يذهب أنصار هذا الاتجاه^١ إلى مساءلة مستعمل البطاقة المزورة في الوفاء عن جريمة التزوير وجريمة استعمال محرر مزور.

فبالنسبة لجريمة التزوير إن الخطوات التي تمر بها عمليات الشراء بالبطاقة لدى التاجر من شأنها أن تجعل الجاني مسؤول عن جريمة التزوير. وذلك على اعتبار أن إحدى الخطوات المطلوبة لاستعمال البطاقة في الوفاء تقوم على طلب التاجر من مستعمل البطاقة التوقيع على قوائم الشراء بعد تقديمه البطاقة والتأكد من إمكانية تمرير عملية الشراء إذا كان مبلغ الصفقة ضمن الحد المسموح وكان رصيد المستخدم يسمح بذلك. وانطلاقاً من وجوب التوقيع على قوائم الشراء فإن من يستعمل بطاقة مزورة عليه أن يوقع بذات نموذج التوقيع الموجود على شريط التوقيع وإلا انكشف أمره. وهو في هذه الحالة إما أن يقلد نموذج التوقيع الموجود على شريط التوقيع عندما لا يتم التلاعب بهذا الجزء، أو التوقيع بتوقيعه عندما يتم التلاعب بهذا الجزء ووضع توقيع من يستعملها على شريط التوقيع بدلاً من توقيع مالكها الشرعي عند التزوير. وهو في كلا الحالتين ينسب التوقيع إلى صاحب البطاقة الأصلي على اعتبار أن تزوير البطاقة تم على غرار بطاقة صحيحة.

أما بالنسبة لجريمة استعمال محرر مزور فيتمثل محل الجريمة بالبطاقة المستعملة المزورة بينما يتمثل الركن المادي بقيام الجاني

^١ من أنصار هذا الاتجاه: د. محمود طه، مرجع سابق، ص ١١٤٥ و د. حوالف عبد الصمد، مرجع سابق، ص ٥٥٩.

بتقديم البطاقة المزورة إلى التاجر مدعياً أنها بطاقة صحيحة ومقبولة من الجهة المصدرة بغية الحصول على ما يريد. في حين يتجلى الركن المعنوي لهذه الجريمة في علم الجاني بتزوير البطاقة واتجاه إرادته إلى استعمالها فيما زودت من أجله.

ونحن من جانبنا لا نؤيد من قال بمسائلة الجاني عن استعمال محرر مزور وذلك على اعتبار أن البطاقة هي محرر من نوع خاص وبالتالي هناك صعوبة في تطبيق أحكام قانون العقوبات بهذا الخصوص (وقد سبق الإشارة إلى ذلك^١).

ومع ذلك فإننا نحترم ونقدر الآراء الفقهية التي نادى بمسائلة الجاني عن جرم التزوير بالنسبة للتوقيع على الفواتير وعن جرم الاحتيال، وذلك لدقة المبررات والحجج التي ساقها أنصار هذه الآراء فقد تقدموا بمجموعة من الحجج المقبولة منطقياً. ولكن في الحقيقة فإننا نؤيد المشرع السوري فيما ذهب إليه من استبعاد التكييفات السابقة واعتبار هذه الجريمة جريمة مستقلة منظمة بنص خاص بموجب قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية حيث جاء فيه: «يعاقب بالحبس من ثلاث سنوات إلى خمس سنوات والغرامة من خمسمائة ألف ليرة إلى مليوني ونصف مليون ليرة من كل من استعمل بطاقة دفع مزورة أو مسروقة أو مفقودة في الدفع أو سحب النقود»^(٢).

وتجدر الإشارة إلى أن المشرع السوري كان موفقاً في هذه الخطوة وذلك للمبررات الآتية:

^١ راجع ص ٤٤١-٤٤٢.

^٢ المادة (٢٢/ب، ٢) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

- إن المشرع السوري كان موفقاً حيث اعتبر أن جريمة استعمال بطاقة مزورة جرم مستقل نظراً لخطورة هذا النوع من الجرائم من جهة ولحدثة ظهوره من جهة أخرى.
- تُنظم هذا الجرم بنص قانوني خاص في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية والخاص يقيد العام الأمر الذي يستتبع استبعاد تطبيق أحكام قانون العقوبات.
- تنظيم المشرع السوري لهذا الجرم بنص خاص من شأنه أن يوفر حماية للمجني عليهم من خلال سهولة إمكانية التطبيق بخلاف إذا ما ترك تنظيم الأمر بقانون العقوبات، حيث قد يجد القاضي صعوبة في تطبيق أحكام الاحتيال على هذه الجرائم وبالتالي يفلت المجرم من العقاب.
- إن تطبيق أحكام المادة /٢٢/ لا يشكل نوع من التناقض مع أحكام قانون العقوبات وذلك على اعتبار أن قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية تدارك الأمر وجاء فيه «إذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون تطبق العقوبة التي هي أشد^(١)».
- وبالمقارنة بين عقوبة استعمال بطاقة مزورة (الحبس من ٣ حتى ٥ سنوات والغرامة من ٥٠٠ ألف حتى مليون ونصف مليون ليرة سورية)، وبين عقوبة الاحتيال (الحبس من ٣ حتى ٥ سنوات والغرامة من عشرة آلاف حتى ٥٠ ألف ليرة^(٢)) وبين عقوبة

^(١) المادة (٢٨/ أ) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

^(٢) المادة /٦٤١/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

التزوير (الحبس من سنة إلى ثلاث سنوات وبغرامة أقلها /٢٠٠٠/ ليرة سورية^١) نجد أن عقوبة استعمال بطاقة مزورة هي الأشد وهي التي تطبق.

٣- استعمال البطاقة المزورة في السحب من أجهزة الصراف أو الوفاء لدى التجار من قبل مزورها:

في معظم الأحيان إن الذي يقوم بتزوير بطاقة الدفع الإلكترونية هو نفسه من يقوم باستعمالها فيما زورت من أجله سواء في السحب أم الوفاء. وفي هذه الحالة نكون أمام تعدد للجرائم فالجريمة الأولى هي تزوير بطاقة دفع إلكترونية أما الجريمة الثانية فهي استعمال بطاقة دفع مزورة في السحب أو الوفاء. ويلاحق المجرم بالجرمين ويعاقب بالجرم ذو الوصف الأشد. وتجدر الإشارة إلى أن التعدد قد يكون معنوياً أو مادياً.

فالتعدد المعنوي: وذلك إذا تم التزوير والاستعمال بفعل واحد، كأن يوقع المتهم على الفواتير لدى أحد التجار، فالتوقيع تزوير واستعمال للبطاقة في آن واحد.

أما التعدد المادي: وذلك إذا ارتكبت الجريمة بفعلين مستقلين، وهذا التعدد قد يكون مرتبطاً ارتباطاً غير قابل للتجزئة متى ارتكبت الجريمتان لغرض واحد (مثل تغيير اسم صاحب البطاقة واستعمالها). كما قد يكون ارتباطاً بسيطاً إذا لم يكن لغرض واحد (كمن استعمل بطاقة مزورة لتحقيق أغراض لم تكن في ذهنه وقت تزويرها^٢).

وبالنتيجة فإن استعمال البطاقة المزورة من قبل مزورها سواء في السحب أم في الوفاء يجعل المجرم أمام تعدد للجرائم ويلاحق بالوصف الأشد، حيث أن

^١ المادة /٤٦٠/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ د. طارق حمزة، مرجع سابق، ص ٣٦٩.

كلا الجرمين يخضعان لنفس العقوبة المادة (٢٢/ب ١،٢) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية. فالعقوبة هي الحبس من ثلاث سنوات حتى خمس سنوات والغرامة من خمسمائة ألف ليرة حتى مليوني ونصف مليون ليرة سورية. وفيما لو كان التزوير بالنسبة للتوقيع على الفواتير وكان الموقع هو نفسه من استعمال البطاقة المزورة في الوفاء، فالعقوبة هي ذاتها المنصوص عليها في المادة /٢٢/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية باعتبارها الأشد مقارنةً بعقوبة التزوير في نطاق التعاملات المادية الحبس من سنة إلى ثلاث سنوات وبغرامة أقلها /٢٠٠٠/ ليرة سورية^١ أو عقوبة مزور التوقيع الإلكتروني^٢. وفي ختام الحديث عن مكافحة التزوير، نجد أن المشرع السوري قد جرم تزوير بطاقة الدفع الإلكترونية كما جرم استعمال بطاقة الدفع المزورة سواء في السحب أم الوفاء بموجب نص خاص في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية تلافياً لأي نزاع. ولكن أغفل تجريم تزوير البيانات والإشعارات المتعلقة ببطاقة الدفع بموجب قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، وترك الأمر لأحكام قانون العقوبات (المادة ٤٦٠) وقانون التوقيع الإلكتروني وخدمات الشبكة (المادة ٣١). كما أغفل المشرع السوري الإشارة لحالة تزوير أجهزة (ATM) وحالة التزوير عن طريق تعديل البرمجيات الإلكترونية بأي نص قانوني ناظم للمعاملات التقليدية أو الإلكترونية. لذلك نأمل من المشرع السوري أن يتدارك هذه النقاط في أقرب تعديل وفي ضوء الاقتراحات التي تقدمنا بها في متن الدراسة.

^١ المادة /٤٦٠/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ المادة /٣١/ من قانون التوقيع الإلكتروني وخدمات الشبكة رقم /٤/ لعام ٢٠٠٩.

الفرع الثالث

مكافحة الجرائم الإلكترونية

ينبغي أن نشير بدايةً إلى أن السرقة والتزوير فضلاً عن الاستخدام غير المشروع لبطاقات الدفع الإلكترونية هي جميعاً من أشكال الجرائم الإلكترونية. ولكن نظراً لخطورة هذه الأشكال من جهة وتعدد صورها ومظاهرها فقد أثرنا الحديث عنها بشكل مستقل. أما فيما يتعلق بخصوص مكافحة الجرائم الإلكترونية فسوف نقصر الحديث على بعض الجرائم الماسة بأنظمة الدفع الإلكتروني والتي يصعب إدراجها تحت أي شكل من الأشكال الثلاثة السابقة. حيث تكفل المشرع السوري في قانون تنظيم التواصل على الشبكة ومكافحة الجرائم المعلوماتية بتنظيم هذه الجرائم بشكل قانوني سليم. لذلك سوف نقوم بالحديث عن هذه الجرائم بشكل مختصر بغية تسليط الضوء عليها في ضوء أحكام التشريع السوري وتتمثل هذه الجرائم في الآتي:

أولاً: مكافحة الجرائم التي ترتكب باستخدام وسيلة إلكترونية

وتتمثل هذه الجرائم في الآتي:

١- الاحتيال عبر الشبكة: جرم المشرع السوري هذا الفعل في قانون تنظيم التواصل على الشبكة ومكافحة الجرائم المعلوماتية حيث جاء فيه:

أ- يعاقب بالحبس من ثلاث إلى خمس سنوات وبالغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية كل من استولى باستخدام الأجهزة الحاسوبية أو الشبكة على مال منقول أو عقار أو معلومات أو برامج ذات قيمة مالية أو سند يتضمن تعهد أو إبراء أو أي امتياز

مالي آخر وذلك عن طريق خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه بأي وسيلة كانت.

ب- وتكون العقوبة الاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية في الحالات التالية:

١- إذا وقعت الجريمة على ثلاثة أشخاص فأكثر.

٢- إذا تجاوز مبلغ الضرر مليون ليرة سورية.

٣- إذا وقع الاحتيال على مصرف أو مؤسسة مالية.

ج- ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي^١.

تطبق أحكام هذه المادة على جرائم الاحتيال عبر الشبكة بقصد إلحاق ضرر مالي بالغير ولا تختلف هذه الجريمة عن جريمة الاحتيال الاعتيادية إلا من ناحية كونها تتم باستخدام الأجهزة الحاسوبية أو الشبكة في خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه^٢.

٢- الجرائم التقليدية التي ترتكب باستخدام الشبكة: نظراً للتطور التقني أدرك المشرع السوري إمكانية ارتكاب أي جريمة تقليدية باستخدام الشبكة لذلك عمل على تجريم كافة الجرائم التقليدية التي ترتكب باستخدام الشبكة وذلك من خلال النص الآتي:

ب- يضاعف الحد الأدنى للعقوبة المقررة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة في إحدى الحالتين التاليتين:

^١ المادة (٢١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادرة بالقرار رقم ٢٩٠/ لعام ٢٠١٢.

- ١- إذا ارتكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة
- ٢- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة عليها^١.

أراد المشرع السوري من النص السابق توحيد النص التشريعي وتطبيقه على الجرائم التقليدية التي ترتكب باستخدام الشبكة أو تقع على الشبكة أو أي منظومة معلوماتية بقصد التأثير على عملها ومثال ذلك (الذم والقذح عبر الشبكة، التهديد عبر الشبكة... الخ).

ولكن ينتقد النص السابق من ناحية أنه عاقب على الجرائم التقليدية التي ترتكب باستخدام الشبكة بمضاعفة الحد الأدنى للعقوبة فقط وفي ذلك مخالفة للنصوص الجزائية، وذلك على اعتبار أن مضاعفة الحد الأدنى من شأنه أن يجعل هذا الحد أكبر من الحد الأعلى. لذلك حبذا لو أن المشرع أكد على مضاعفة الحد الأدنى والأعلى في هذه الجرائم أو أن ينص على مضاعفة الحد الأدنى على أن لا تتجاوز الحد الأعلى للعقوبة.

ثانياً: مكافحة الجرائم التي تمس منظومة المعلومات الإلكترونية.

كرّس المشرع السوري مجموعة من المؤيدات الجزائية بحق بعض الجرائم الماسة بمنظومة المعلومات الإلكترونية. ومن هذه الجرائم نذكر:

- ١- الدخول غير المشروع لمنظومة معلوماتية: من خلال استقراء نصوص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة

^١ المادة (٢٨/ب) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/

المعلوماتية^١ نجد أن المشرع السوري قد عاقب من يخرق جهازاً حاسوبياً أو منظومة معلوماتية أو موقعاً إلكترونياً (بما في ذلك منظومة الدفع الإلكتروني) عن طريق الشبكة دون أن يملك الصلاحية أو التصريح اللازم للقيام بذلك وبشرط توفر القصد الجرمي. كما تشدد العقوبة في حال أضيف إلى الاختراق المذكور نسخ أو تشويه أو إفشاء لأي من المعلومات التي جرى الحصول عليها ومثال ذلك سرقة الحسابات عبر شبكة الإنترنت^٢.

٢- **إعاقة الوصول إلى الخدمة:** عاقب المشرع السوري على هذا الجرم بموجب قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية^٣. وتتمثل أركان هذه الجريمة في الآتي:

- محل الجريمة: أي منظومة معلوماتية أو شبكة أو أي خدمات أو برامج أو مواقع إلكترونية.
- الركن المادي: أي فعل من شأنه أن يؤدي إلى إعاقة الدخول إلى منظومة معلوماتية، أو تعطيل وظائفها كلياً أو جزئياً، أو أي فعل من شأنه أن يؤدي إلى منع الدخول إلى هذه المنظومة، وبأية وسيلة كانت سواء أكانت بتخريب البرمجيات أم بقطع الاتصال عن المنظومة المعلوماتية أم بإغراق المنظومة المعلوماتية بما يفوق

^١ المادة ١٥/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادرة بالقرار رقم ٢٩٠/ لعام ٢٠١٢.

^٣ المادة ١٧/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

طاققتها). وفي نطاق عملية الدفع الإلكتروني لعل خير مثال على ذلك أي فعل من شأنه أن يؤدي إلى تعطيل جهاز القارئ الخاص ببطاقة الدفع الإلكترونية أو أي فعل من شأنه أن يؤدي إلى تعطيل جهاز الحاسوب وعجز المستخدم عن الوصول إلى حسابه المصرفي).

• الركن المعنوي: القصد العام أي أن يعلم الفاعل بجريمته وإرادة هذا الجرم.

٣-اعتراض المعلومات: حيث عاقب المشرع السوري كل من أقدم قصداً و بوجه غير مشروع على اعتراض أو التقاط المعلومات المتداولة على منظومة معلوماتية أو على الشبكة أو التتصت عليها بوسائل معلوماتية، وذلك عند نقلها من أو إلى أو في منظومة معلوماتية سواء جرى استغلال هذه المعلومات لاحقاً أم لا.

كما أنه جرم كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة، سواء أكان ذلك باستخدام البريد الإلكتروني أم بانتحال أسماء أو محتوى مواقع إلكترونية أم بأي وسيلة أخرى^١. وتعد هذه الجريمة أحد الأفعال التي تشكل انتهاكاً للسرية المصرفية في نطاق الدفع الإلكتروني (وقد سبق الحديث الأثر السلبي لتقنية المعلومات على الحياة الخاصة للأفراد في الباب الأول^٢).

٤- تصميم البرمجيات الخبيثة واستخدامها: نظم المشرع السوري هذا الجرم بموجب قانون تنظيم التواصل على الشبكة ومكافحة الجريمة

^١ المادة/١٨/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

٢٠١٢.

^٢ راجع ص ٢٩ وما يليها.

المعلوماتية^١ وتتمثل هذه الجريمة بأي فعل أو نشاط من شأنه أن يؤدي لتصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية أو بأي استخدام للبرمجيات الخبيثة أيّاً كان نوعها وبأي وسيلة كانت بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة. وجريمة تصميم أو استخدام البرمجيات الخبيثة من الجرائم القصدية التي تتطلب توافر العلم والإرادة.

وفي هذا الصدد اعتبرت محكمة التحكيم العليا للاتحاد الروسي أن وجود برامج ضارة أو خبيثة على القرص الصلب للمستخدم يشير إلى أن المستخدم لم يتخذ التدابير المناسبة لضمان أمان المعدات المستخدمة لإجراء التسويات من خلال نظام الدفع الإلكتروني. الأمر الذي أدى للوصول غير المصرح به إلى المعلومات السرية للمستخدم وبالتالي لا يكون المصرف مسؤولاً عن انتهاك البيانات الشخصية للمستخدم و يتحمل الأخير تبعة تقصيره^٢.

٥- إرسال البريد الواعل: جرم المشرع السوري كل من أقدم على إرسال بريد واعل إلى الغير سواء أكان ذلك بقصد الترويج أم التسويق أم الإغراء أم أي غرض آخر إذا كان المتلقي لا يستطيع إيقاف وصوله أو كان إيقاف وصوله مرتبطاً بتحمل المتلقي نفقات

^١ المادة /١٩/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.

^٢ القضية رقم 19532-٢٠١٢ تاريخ ٢٠١٢/١٠/٤ ومتاحة على الرابط:

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>

تاريخ الزيارة ٢٠١٩/٦/١٧ الساعة ٤,١٠ a.m

إضافية^١. أما إذا كان استخدام البريد الواعل بهدف خداع المستخدمين على الشبكة أو منظومة معلوماتية للحصول على معلومات شخصية أو سرية فتطبق أحكام المادة (١٨) من هذا القانون (اعتراض المعلومات)، أما إذا كان استخدام البريد الواعل بهدف خداع المستخدمين على الشبكة أو منظومة معلوماتية للحصول على مال منقول أو إسناد تتضمن تعهد أو إبراء فتطبق أحكام المادة (٢١) من هذا القانون (الاحتيال عبر الشبكة)^٢.

وفي ختام حديثنا عن مكافحة المشكلات التي تمس أداة الدفع بأشكالها الثلاثة (السرقه، التزوير، الجرائم الإلكترونية)، نصل إلى نتيجة مفادها أن المشرع السوري نظم هذه الجرائم بشكل قانوني سليم (وهذه نقطة تحتسب للمشرع السوري)، ولكن المشكلة الوحيدة التي تواجه هذه النصوص هي صعوبة التطبيق العملي لهذه النصوص. فلكي تطبق هذه النصوص لا بد من اكتشاف هذه الجرائم وتجدر الإشارة إلى أن أمر كشف هذه الجرائم تكتفه بعض الصعوبات والمتمثلة بالآتي:

- إمكانية الدخول من عدة أماكن: فالمتعامل عبر الإنترنت لا يحتاج لمكان محدد للدخول بل أي مكان يوجد فيه جهاز كمبيوتر وخط اتصال يمكن للشخص الدخول للشبكة.
- سرعة العملية: حيث لا يحتاج المجرم إلى أكثر من بضع دقائق لاختراق موقع والتلاعب به ومغادرته قبل أن يتم تعقبه.

^١ المادة/٢٠/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

٢٠١٢.

^٢ التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادرة

بالقرار رقم ٢٩٠/ لعام ٢٠١٢.

- تباعد المسافات: فقد يكون الموقع الإلكتروني في مكان والمخترق في مكان آخر في ظل عالمية الشبكة.
 - عدم وجود هوية محددة: ففي بعض الحالات لا يمكن معرفة هوية المخترق.
 - عدم وجود قوانين دولية موحدة: حيث توجد معايير موحدة للاستخدام أما قوانين موحدة فلا يوجد، فلو افترضنا اكتشاف أحد المخترقين بدولة مغايرة لدولة الشركة التي تم اختراقها فليس بالضرورة وجود قوانين موحدة للتعامل مع المخترق.
 - عدم وجود دلائل مادية لإثبات هذه الجرائم.
 - إمكانية إتلاف بيانات جهاز الكمبيوتر: في حال شعور المخترق بإمكانية تعقبه يستطيع إتلاف بيانات جهازه بالنقر على أحد الأزرار مما يجعل عملية تعقبه عديمة الجدوى.
 - الحسابات المحمية: حيث تشكل هذه الحسابات بيئة مناسبة للمخترق حيث يستطيع المخترق استخدام هذه الحسابات دون الخوف من تعقبه.
 - عدم الإبلاغ عن الاختراقات: هناك الكثير من الشركات لا تبلغ عن الاختراقات التي تعرضت لها وتفضل تحمل خسائر كبيرة عوضاً عن فقدان ثقة عملائها.
- لذلك ينبغي السعي لتذليل هذه العقبات إلى أدنى حد بغية توفير البيئة المناسبة لتطبيق النصوص القانونية الخاصة بهذه الجرائم.
- بعد أن تعرفنا على المسؤولية الجزائية للمشكلات التي تمس أداة الدفع ننتقل للحديث عن المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية.

المطلب الثاني

المسؤولية الجزائية عن الاستخدام غير المشروع

لبطاقة الدفع الإلكترونية

في ظل تعدد الأشكال والمظاهر التي يمكن من خلالها استخدام البطاقة بشكل غير مشروع سواء من قبل أطراف الدفع أم من قبل الغير. لذلك اقتضى علاج هذه المشكلات البحث في التكييف الجزائي لكل فعل من أفعال الاستخدام بغية معرفة المؤيدات الجزائية المطبقة على الجاني سواء في ضوء أحكام قانون العقوبات أم في ضوء أحكام قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

وفي سبيل التعرف على المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية سوف نتحدث عن المسؤولية الجزائية لأطراف عملية الدفع الإلكتروني في الفرع الأول ومن ثم ننتقل للحديث عن المسؤولية الجزائية للغير في الفرع الثاني.

الفرع الأول

المسؤولية الجزائية لأطراف عملية الدفع الإلكتروني

سبق الإشارة إلى أن حالات الاستخدام غير المشروع قد تقع من قبل أطراف العلاقة أو قد تقع من قبل الغير، وبالنسبة لأطراف العلاقة فإن حالات الاستخدام غير المشروع من قبل الحامل تشكل أكثر الأساليب خطورة، على اعتبار أن الحامل بإمكانه وبسهولة أن يقوم بعمليات استخدام غير مشروعة نظراً لكون الوسيلة في حيازته فضلاً عن معرفته الكاملة بكافة نقاط ضعف وقوة هذه الوسائل. في حين أن عمليات الاستخدام من قبل التاجر أو المصدر (الموظفين) تتطلب

خبرة وتقنية في التلاعب بالأجهزة والمعدات فضلاً عن وجود نوع من التواطؤ والتلاعب سواء مع موظفي المصدر أو مع الحامل، الأمر الذي يجعل حدوث حالات استخدام غير مشروع من قبل التاجر والمصدر أقل حدوثاً مقارنة بعمليات الاستخدام غير المشروع من قبل الحامل أو الغير.

وفي سبيل التعرف على المسؤولية الجزائية لأطراف الدفع الإلكتروني سوف نتحدث عن المسؤولية الجزائية للحامل (أولاً) ومن ثم ننتقل للحديث عن المسؤولية الجزائية للتاجر والمصدر (ثانياً).

أولاً: المسؤولية الجزائية للحامل.

سبق وأن أشرنا إلى أن الحامل قد يستخدم بطاقة الدفع الإلكتروني بشكل غير مشروع بصور وأشكال متعددة، لذلك يقتضي معالجة هذه الأشكال على أن يتم التعرف على التكيف الجزائي لكل فعل من هذه الأفعال بغية ترتيب المؤيدات الجزائية المنصوص عليها في النصوص القانونية النازمة للمعاملات التقليدية أو الإلكترونية. لذلك وفي سبيل تسليط الضوء على المسؤولية الجزائية للحامل عن الاستخدام غير لمشروع لبطاقة الدفع سوف نتحدث عن الآتي:

١- مسؤولية الحامل الجزائية عن استخدام البطاقة بما يجاوز الرصيد

قد يقدم الحامل على استخدام البطاقة بما يجاوز الرصيد سواء في السحب أو الوفاء:

أ- تجاوز الرصيد في السحب من أجهزة الصراف الآلي: ظهر في هذا الصدد ثلاثة اتجاهات فقهية، تقتضي بمسؤولية الحامل جزائياً عن

تجاوز الرصيد في السحب ولكن كان هناك اختلافاً فقهيّاً حول التكييف الجزائي:

أ- **تكييف الفعل على أنه سرقة:** يرى بعض الفقه^١ أن حامل البطاقة الذي يتجاوز رصيده في السحب من أجهزة الصرّاف الآلي يتحمل المسؤولية الجزائية عن جريمة السرقة، وقد استندوا في تكييفهم إلى المبررات الآتية:

■ إن جهاز الصرّاف الآلي لا إرادة له ويقتصر دوره على تنفيذ تعليمات موظفي المصرف المسجلة ابتداءً في ذاكرته، ويشبهون دور هذا الجهاز بدور الصغير غير المميز أو المجنون الذي يسلم مالا لشخص آخر وبالتالي لا يُعتد بإرادته ولا يعتبر تسليمه إرادياً.

■ إن سحب الحامل لمبالغ تتجاوز رصيده باستخدام البطاقة يشبه حالة المدين الذي يضع محفظة بين دوائيه ليأخذ لنفسه الدين المستحق، إلا أن الدائن يتجاوز ما هو مستحق دون رضا المدين. ويستندون إلى حكم محكمة النقض الفرنسية التي أيدت فيه تحقق وصف السرقة في هذه الحالة والقائم على انعدام الرضا لدى المدين عن أخذ المبلغ الزائد عن الدين، الأمر الذي يسمح بتكييف فعل حامل البطاقة على أنه جريمة سرقة^٢.

■ إن التسليم الإرادي من قبل المصرف فقط على المبلغ المستحق لحامل البطاقة وهو ما يشكل رصيده القائم في الحساب، أما فيما

^١ مشار إليه لدى د. جميل عبد الباقي الصغير، مرجع سابق، ص ٧٥ و د. محمد حماد مرهج الهيتي، مرجع سابق، ص ٢٠٧.

^٢ مشار لهذا الحكم لدى: المرجع السابق، ص ٧٧. Crime, 21 avril, 1994 j.c.p1965.

يجاوز ذلك فإن إرادة المصرف لم تتجه للرضا عن التسليم مما يحقق وصف السرقة.

وعلى صعيد القضاء فقد اتجه القضاء الاسترالي إلى مقاضاة حامل البطاقة الذي يجاوز الرصيد في السحب عن جريمة السرقة، حيث قضت المحكمة العليا في استراليا في حكم صادر لها عام ١٩٨٦ بانطباق وصف السرقة على سلوك حامل البطاقة الذي يسحب نقوداً من أجهزة الصرّاف الآلي بما يجاوز الرصيد^١.

ونحن من جانبنا، نرى أن فعل حامل البطاقة الذي يتجاوز رصيده في السحب لا يشكل سرقة وذلك استناداً للمبررات الآتية:

- عرّف المشرع السوري السرقة على أنها: «أخذ مال الغير المنقول دون رضاه»^٢.

نستنتج من التعريف السابق أن أركان السرقة تتمثل في الآتي:

الركن المادي: يتجلى في أخذ مال الغير المنقول دون رضاه ويترتب على ذلك نتيجة تتمثل بخروج الشيء من حيازة المجني عليه ودخوله في حيازة الجاني. أما الركن المعنوي: يتمثل بالعلم بالفعل وإرادة الفعل.

وبالتالي إن عملية أخذ مال من الصرّاف متجاوزاً الرصيد لا تشكل سرقة وذلك لكون عنصر الرضا متوفر في التسليم. حيث أن جهاز الصرّاف الآلي التابع للمصرف تم برمجته على أساس معلومات معينة، بحيث يمكن للحامل سحب النقود متى أراد ذلك مستخدماً البطاقة. وبناءً على إدخال المعلومات يستجيب الجهاز لكل طلب مطابق مهما كان الحامل قد تجاوز رصيده البنكي، طالما أن المصدر لم يبرمج الصراف الآلي على

¹Wasik(martin),crime and computer,p110.

مشار إليه لدى: بشرى سلامة، مرجع سابق، ص ١٨.

^٢ المادة ٦٢١/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

رفض تسليم الأوراق النقدية التي يطلبها متجاوزاً في ذلك حدود رصيده، وباستجابة الصراف الآلي لطلب الحامل حتى لو تجاوز الرصيد، يعني أن عملية التسليم كانت إرادية وبرضا من المصرف المصدر الذي لم يُجبر على التسليم حتى وإن كان هناك غش من الحامل. وبالتالي فإن وجود رضا في التسليم ينفي عن الفعل فكرة السرقة.

- إن القياس الذي لجأ إليه مؤيدو تكييف الفعل على أنه سرقة سواء القياس المتعلق باعتبار جهاز الصراف بمثابة المجنون، أو قياس حالة تجاوز الرصيد على حالة المدين الذي يضع محفظة في يد الدائن، أمر غير مقبول في نطاق القانون الجزائي باعتبار أنه لا جريمة ولا عقوبة إلا بنص قانوني.

- القول بأن التسليم تم من جهاز لا إرادة له ولا وعي أمر غير مقبول، وذلك لأن من قام بالتسليم فعلياً هم موظفو المصرف باعتبارهم ممثلين للشخص الاعتباري الذي يملك المال. وبالتالي هم أشخاص ذوو صفة قانونية تمكنهم من إعطاء التعليمات لمبرمجي الجهاز ليقوموا ببرمجته على تسليم المال بمجرد اتباع خطوات معينة. وبالتالي هؤلاء أشخاص ذوو إرادة حرة وواعية بينما الجهاز مجرد ذراع آلي للمصرف.

- القول بأن الآلة تشبه المجنون أمر غير مقبول، لأن تشبيه الآلة بالمجنون يعني أن جميع التصرفات لا ترتب أي آثار قانونية. ولكن في نطاق تسليم المال من جهاز الصراف الآلي فإن التسليم في حدود الرصيد الدائن أمر صحيح منتج لآثاره القانونية، أما المجنون فجميع تصرفاته لا ترتب آثاراً قانونية. وبالتالي لا يمكن تجزئة الإرادة واعتبار التسليم صحيح في حدود الرصيد الدائن، بينما لا نعتد بالتسليم عندما يجاوز الرصيد.

وبالنتيجة يمكن القول أن تكيف فعل الحامل عندما يجاوز الرصيد على أنه سرقة أمر غير مقبول قانوناً. وما يؤيد موقفنا ما قضت به محكمة (Lyon) من أن قيام الحامل بالسحب من جهاز الصراف الآلي بواسطة بطاقته يترتب عليه قيد المبلغ المسحوب في الجانب المدين من حسابه ولا يتغير الوضع في حالة عدم كفاية الرصيد، بحيث يمكن القول إن التسليم في كل الحالات كان إرادياً من قبل الجهة المصدرة لأن جهاز الصراف الآلي يقوم بتنفيذ تعليمات المصرف مما ينفي وجود سرقة لهذه الأموال.

كما قضت محكمة الاستئناف (Angers) بأن قيام الحامل بتجاوز الرصيد عند السحب من جهاز الصراف لا يشكل سرقة، لأن تسليم المال كان إرادياً وليس رغماً عن حائزه ولا يغير من الأمر شيئاً أن يكون مرتكب الفعل قد حصل بطريق الغش^١.

ب- تكيف الفعل على أنه احتيال: يرى بعض الفقه^٢ أن حامل البطاقة الذي يقدم على استخدامها للسحب بما يجاوز الرصيد يمكن ملاحقته تحت وصف الاحتيال. وحجتهم في ذلك أن الاحتيال بصفة عامة هو نوع من الخداع وإيقاع للآخر بالغلط إضراراً به. حيث أن حامل البطاقة عندما يقوم بالسحب بما يجاوز الحد المسموح من قبل

^١ Angers, 2, December, 1980, D. 1981, I.R.P. 383. J.C.P. 1981, IV, P375-R.S.C-1982, 129-obs-P-Bouflat.
Lyon. 1 juill 1981-R.S.C 1982, 619.

مشار لكلا الحكمين لدى د. محمد سامي الشوا، الجرائم المعلوماتية للتعدي على الذمة المالية للغير، بحث مقدم لدى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣، ص ١٠٨٣.

^٢ مشار إليه لدى د. حوالف عبد الصمد، مرجع سابق، ص ٥١٩ و بشرى سلامة، مرجع سابق، ص ٢٤.

المصرف يكون قد ادعى صفة غير صحيحة وهي أن له رصيد دائن في المصرف خلافاً لواقع الحال وقد أيد هذه الصفة بوسيلة احتيالية (تقديم البطاقة).

ونحن من جهتنا نرفض ما ذهب إليه الفقه من تكييف جزائي ونرى بعدم إمكانية مساءلة الحامل عن جرم الاحتيال وذلك لأن الحامل لم يقم بخداع الجهاز بأي وسيلة من الوسائل المحددة للاحتيال^١ فهو صاحب البطاقة والحامل الشرعي لها وبالتالي لم ينتحل أي صفة كاذبة على الرغم من أن الحصول على المال تم نتيجة لخداع أو تلاعب بالجهاز، كما أن هذه الأساليب موجهة للإنسان وليس الآلة.

وما يؤيد موقفنا ما قضت به محكمة النقض الفرنسية من أن تجاوز الحامل الحد المسموح له به لا يعد طريقة احتيالية ولا خدعة مسرحية فلا تقوم جريمة الاحتيال^٢.

كما ذهبت محكمة استئناف (Angers) إلى أن استيلاء الحامل على مبالغ تجاوز رصيده عن طريق وضعها في أحد أجهزة الصراف الآلي لا ينطوي على الطرق الاحتياطية اللازمة لقيام جريمة الاحتيال، إذ تفترض هذه الطرق توافر عنصر خارجي أو حبكة مسرحية أو تدخل من جانب الغير، بحيث إذا تخلفت هذه العناصر تعذر القول بأن تسليم المبالغ إلى حامل البطاقة قد تم نتيجة وسائل غير مشروعة^٣.

^١ المادة /٦٤١/ من قانون العقوبات رقم /١٤٨/ لعام ١٩٤٩.

^٢ Cass, crime, 7 Juin 2000. et-tc. Paris 9 Mai 1972. revu. trim dr. com 1975, p15..

مشار إليه لدى: د. حوالف عبد الصمد، مرجع سابق، ص ٥٢٠.

^٣ Angers, 2, December, 1980, D. 1981, I.R.P. 383. J.C.P. 1981, IV, P375-R.S.C-1982, 129-obs-P-Bouflat.

مشار لهذا الحكم لدى د. محمد سامي الشوا، مرجع سابق، ص ١٠٨٣.

ج - **تكييف الفعل على أنه إساءة الائتمان:** يرى جانب من الفقه^١ أن حامل البطاقة الذي يستخدمها للسحب بما يجاوز الرصيد ينبغي أن يلاحق جزائياً وفق أحكام إساءة الائتمان. على اعتبار أن الحامل أساء استعمال البطاقة التي سلمت إليه مقترنة بشرط عدم تجاوز الرصيد، والحامل يكون كالأمين على استعمال البطاقة وعليه استعمالها وفقاً لشروط العقد المبرم بينه وبين المصرف. وبالتالي إذا أساء الحامل استخدام البطاقة وقام بسحب مبلغ يجاوز رصيده يعد مرتكباً لجريمة إساءة الائتمان.

كما أن بعض الفقه^٢ يرى إمكانية تجريم فعل حامل البطاقة على أساس جريمة إساءة الائتمان، وذلك من خلال الاستناد لموضوع تسليم شيء في حرز مغلق ومن صورها استيلاء متسلم المفتاح على شيء من محتويات المكان المقفل بهذا المفتاح، كالبائع الذي قد سلم المشتري مفتاح المخزن لكي يأخذ بضاعته التي اشتراها فقط فيأخذ بضاعة أخرى. فالحامل سمح له المصرف بالدخول إلى مخزن النقود وأخذ ما يملك من النقود فقط إلا أن الحامل أخذ أموال أخرى غير التي يملكها.

ونحن من جانبنا نرى أنه لا يمكن التسليم بأن حامل البطاقة يلاحق بموجب إساءة الائتمان على أساس أن تصرفه يكون كتصرف من يستولي على شيء في حرز مغلق ومن صورها استيلاء متسلم المفتاح على شيء من محتويات المكان المغلق بهذا المفتاح، والسبب أن هذه الحالة تمت إثارتها في الفقه في إطار جريمة السرقة وليس في إطار جريمة إساءة الائتمان .

^١ مشار إليه لدى: د. علي عبد القادر قهوجي، الجرائم المتعلقة باستخدام البطاقة الممغنطة، ورقة عمل مقدمة لمؤتمر الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، المجلد الثالث، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٣، ص ٣٥٤.

^٢ مشار إليه لدى: د. محمد حماد مرهج الهييتي، مرجع سابق، ص ٢٢٣.

ولكن نرى أن الحامل الذي يقدم على استخدام البطاقة في السحب متجاوزاً رصيده يسأل عن جرم إساءة الائتمان وفق أحكام المادة/٦٥٦/ من قانون العقوبات السوري وذلك لتوفر أركانها:

محل الجريمة: يتمثل محل الجريمة بمال منقول (المال الذي حصل عليه المستخدم متجاوزاً رصيده).

الركن المادي: باستقراء الحالة العملية^١ التي يمكن من خلالها حدوث هذا السحب نجد أن المصرف مصدر البطاقة قد سمح للمستخدم سحب أربع أضعاف رصيده في الخارج على أن يقوم بتغذيته لدى العودة أي أن المال سلم للمستخدم على سبيل عارية الاستعمال، فقام المستخدم باختلاس هذا المال وامتنع عن رده، أي أن الركن المادي لهذه الجريمة متوفر.

الركن المعنوي: يتمثل بالعلم بالفعل وإرادة هذا الفعل.

وبالتالي نجد أن أركان جريمة إساءة الائتمان متوفرة بحقه ويعاقب الجاني بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة تتراوح بين ربع قيمة الردود والعطل والضرر وبين نصفها على أن لا تنقص عن ٢٠٠٠ ليرة.

إضافةً إلى المسؤولية الجزائية فإن الحامل مسؤول مدنياً وفق أحكام المسؤولية العقدية عن تعويض الضرر الذي أصاب المصرف من جراء ذلك كونه أخل بالتزامه العقدي والمتمثل باستخدام البطاقة ضمن حدود رصيده^٢.

^١ لمزيد من التفصيل راجع ص ٣٢٥.

^٢ لمزيد من التفصيل بخصوص المسؤولية العقدية راجع ص ١٤٧ وما يليها.

ب- تجاوز الرصيد في الوفاء لدى التجار

إلى جانب حالة السحب من أجهزة الصّراف الآلي، فقد يُقدم الحامل على استخدام البطاقة للوفاء بثمن المشتريات لدى التجار متجاوزاً بذلك رصيده الدائن. الأمر الذي يثير التساؤل حول ما هو التكييف الجزائي لفعل الحامل في هذه الحالة ؟

لقد ظهر في هذا الخصوص موقف فقهي وموقف قضائي مخالف له على النحو الآتي:

الموقف الفقهي: يرى أصحاب هذا الاتجاه^١ أنه إذا كانت قيمة السلع والخدمات التي استعملت البطاقة للوفاء بها قد تجاوزت الحد الذي يضمنه المصرف للتاجر فإن فعل الحامل ينطوي تحت وصف الاحتيال. فتقديم البطاقة للتاجر وهو المجني عليه - باعتبار أن المصرف لا يلتزم برد القيمة التي تجاوزت الحد الأقصى للضمان - يشكّل برأيهم وسيلة احتيالية لإقناع التاجر بوجود رصيد وهمي.

الموقف القضائي: يرى القضاء الفرنسي^٢ أنه ينبغي مساءلة الحامل عن جريمة إساءة الائتمان، وبالتالي فإن حامل البطاقة الذي يستخدمها بما يجاوز حدود رصيده الدائن لا يتعدى كونه مدين لم يقم بالوفاء. وبالتالي فهو أشبه بالمستعير الذي لم يقم برد الشيء المعار لصاحبه.

ونحن من جانبنا نرى بعدم إمكانية مساءلة الحامل عن جرم الاحتيال وذلك للحجج الآتية:

▪ لا ينطبق وصف الاحتيال على فعل حامل البطاقة في حال استخدامها بما يجاوز الرصيد سواء أكان المتضرر هو التاجر أو

^١ مشار إليه لدى د. حوالف عبد الصمد، مرجع سابق، ص ٥٢٢.

^٢ مشار إليه لدى بشرى سلامة، مرجع سابق، ص ٢٨.١٠٩، p109، (Lionel) Hanachowize

المصرف. فالقول إن فعله يشكل جريمة احتيال لا بد فيه من توافر إحدى صور الاحتيال التي نص عليها المشرع السوري /المادة ٦٤١/.

▪ القول إن حامل البطاقة مدعي لصفة كاذبة بأنه صاحب رصيد وهمي لا يمكن التسليم بصحتها لأن حامل البطاقة رصيده حقيقي ولكن غير كافٍ.

▪ إظهار الحامل للبطاقة مجرد دعم للأكاذيب التي ردها ولكن ليست مستقلة عنها وإنما هي مندمجة بموضوع الكذب. وبالنتيجة استبعاد وصف الاحتيال لتخلف الركن المادي على النحو الذي بيناه آنفاً.

أما بالنسبة لإساءة الائتمان فإننا نؤيد القضاء الفرنسي في تكييفه، ونرى بأن الحامل الذي يقوم على استخدام البطاقة متجاوزاً رصيده في الوفاء يسأل عن جرم إساءة الائتمان وفقاً لأحكام المادة ٦٥٦/ من قانون العقوبات السوري وذلك لتوفر أركانها المتمثلة في الآتي:

محل الجريمة: يتمثل محل الجريمة بمال منقول (المال الذي حصل عليه المستخدم متجاوزاً رصيده) واستخدمه للوفاء بثمن السلع والخدمات.

الركن المادي: باستقراء الحالة العملية^١ التي يمكن من خلالها حدوث هذا الوفاء نجد أن الجهة مصدرة البطاقة وضعت هذه الميزة المتمثلة بإمكانية الوفاء على الرغم من عدم وجود رصيد كاف كنوع من توفير المال في يد الحامل كونه قد يكون مضطر على الشراء وليس

^١ لمزيد من التفصيل راجع ص ٣٢٣-٣٢٤.

معه نقود كافية، أي أن المال سلم على سبيل عارية الاستعمال إلا أن المستخدم اختلس هذا وامتنع عن رده وتغطية الحساب، أي أن الركن المادي لهذه الجريمة متوفر.

الركن المعنوي: يتمثل بالعلم بالفعل وإرادة هذا الفعل.

وبالتالي نجد أن أركان جريمة إساءة الائتمان متوفرة بحقه ويعاقب الجاني بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة تتراوح بين ربع قيمة الردود والعطل والضرر وبين نصفها على أن لا تنقص عن ٢٠٠٠ ليرة.

إضافةً إلى المسؤولية الجزائية فإن الحامل مسؤول مدنياً وفق أحكام المسؤولية العقدية عن تعويض الضرر الذي أصاب المصرف من جراء ذلك كونه أخل بالتزامه العقدي والمتمثل باستخدام البطاقة ضمن حدود رصيده^١.

وبالنتيجة يمكننا القول أن حامل البطاقة الذي يستخدمها في السحب أو الوفاء متجاوزاً رصيده - على الرغم من التسليم بصعوبة حصول مثل هذه الحالات - يسأل عن جرم إساءة الائتمان على النحو الذي بيناه آنفاً.

٢- مسؤولية الحامل الجزائية عن استخدام بطاقة ملغاة أو منتهية الصلاحية

على غرار حالة تجاوز الرصيد فقد يتم استخدام البطاقة الملغاة أو المنتهية الصلاحية في السحب أو الوفاء:

^١ لمزيد من التفصيل بخصوص المسؤولية العقدية راجع ص ١٤٧ وما يليها.

أ- استخدام البطاقة الملغاة أو المنتهية الصلاحية في السحب

إن استخدام البطاقة الملغاة أو المنتهية الصلاحية لسحب النقود من جهاز الصراف الآلي يبدو مستحيلاً وغير متصور في ظل الاحتياطات التي يضعها المصرف على أجهزة الصراف عند إلغاء البطاقة. حيث تقوم هذه الأجهزة بسحب البطاقة تلقائياً أو رفض العملية لكون هذه الأجهزة ترتبط مباشرةً بحساب الحامل لدى المصرف، وبالتالي فإنها سوف ترفض تسليم أوراق النقود التي يطلبها الحامل^١.

وبالتالي فإن تصرف حامل البطاقة لا يمكن أن يشكل جريمة من الناحية العملية في الوقت الحاضر بسبب نجاح التقنيات الحديثة في برمجة أجهزة الصراف الآلي لاكتشاف البطاقة الملغاة غير الصالحة للاستخدام، ومن ثم سحبها وعدم إرجاعها لصاحبها. كما تجدر الإشارة إلى أن عمليات الاستخدام غير المشروع في هذا النوع من البطاقة لا يمكن أن تحدث إلا في حالة وحيدة وهي حالة استغلال الفترة بين إلغاء البطاقة أو انتهاء صلاحيتها وبين برمجة جهاز الصراف على سحب البطاقة^٢. ولكن وعلى فرض تمكن الحامل من السحب خلال هذه الفترة بالبطاقة الملغاة أو المنتهية الصلاحية. فهل يسأل جزئياً في ضوء النصوص الحالية؟

نحن نرى من جانبنا بعدم إمكانية مساءلة الحامل جزئياً وفق أحكام العقوبات:

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٥٣١.

^٢ راجع ص ٣٢٦ وما يليها بخصوص الاستخدام غير المشروع للبطاقة الملغاة والمنتهية الصلاحية.

فبالنسبة للسرقة: إن عملية أخذ المال ببطاقة ملغاة أو منتهية الصلاحية لا تشكل سرقة، وذلك لكون التسليم تم برضا على اعتبار أن الحامل استخدم الجهاز في ضوء الاستخدام العادي، وبالتالي فإن التسليم يكون إرادياً وبرضا من المصرف المصدر الأمر الذي ينفي معه الركن المادي للسرقة.

أما بالنسبة للاحتيال: كذلك الأمر لا يشكل فعل الحامل احتيالياً، باعتبار أن الحامل استخدم البطاقة في حدود نطاق وظيفتها العادية دون أي احتيال. كما أن الاحتيال يتطلب توفر وسائل محددة في المادة /٦٤١/ الأمر الذي يتطلب أن تكون هذه الأساليب موجهة للإنسان وليس الآلة. وبالتالي نستبعد تكيف الفعل على أنه احتيال.

وبالنسبة لإساءة الائتمان: فكذلك الأمر يستبعد هذا التكيف باعتبار أن المال لم يكن بحوزة الجاني لكي يقوم باختلاسه، كما أن إساءة الائتمان تتطلب أن يكون المال سَلَمَ وفقاً لعقد من العقود المحددة بالمادة /٦٥٦/ والمعلوم أن البطاقة سُلِّمَت للحامل على أساس عقد من العقود المحددة وليس المال الصادر من جهاز الصراف الآلي.

وبالنتيجة نخلص إلى أن حامل البطاقة الملغاة أو المنتهية الصلاحية والذي يستخدمها في السحب من أجهزة الصراف الآلي لا يلاحق جزائياً في ضوء أحكام قانون العقوبات المتعلقة بالسرقة والاحتيال وإساءة الائتمان، كما أننا لم نلاحظ وجود أي نص قانوني خاص ينظم هذه الحالة في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة

المعلوماتية على خلاف حالة استعمال الوسيلة المسروقة أو المفقودة أو المزورة التي نظمت بنص خاص.

ولكن يمكننا القول أن الحامل الذي يقدم على استخدام بطاقة ملغاة أو منتهية الصلاحية في السحب من جهاز الصراف الآلي يسأل عن جرم الاحتيال عبر الشبكة لتوفر أركانها والمتمثلة في الآتي:

محل الجريمة: المنظومة المعلوماتية الخاضعة لسيطرة المجني عليه (جهاز الصراف الآلي الخاضع لسيطرة المصرف).

الركن المادي: قام الجاني (الحامل) باستخدام بطاقة الدفع الملغاة أو منتهية الصلاحية والتي تعمل عبر الشبكة في جهاز كمبيوتر (جهاز الصراف الآلي) وتمكن من الحصول على مال منقول دون وجه حق (النقود التي سحبها بواسطة هذه البطاقة) عن طريق أساليب ووسائل أدت إلى خداع المنظومة المعلوماتية (جهاز الصراف الآلي) وجعله يقبل البطاقة ويصرف النقود على الرغم من إلغاء البطاقة أو انتهاء صلاحيتها.

الركن المعنوي: ويتمثل في علم الحامل بفعله وإرادة هذا الفعل. وبالنتيجة نجد أن أركان جريمة الاحتيال عبر الشبكة متوفرة بحق الحامل الذي يقدم على استخدام بطاقة ملغاة أو منتهية الصلاحية في السحب من جهاز الصراف الآلي وطالما أن هذا الجهاز تابع للمصرف الأمر الذي يجعل هذا الاحتيال واقعاً على المصرف وبالتالي يعاقب الحامل بالاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي.

ب- استخدام البطاقة الملغاة أو المنتهية الصلاحية في الوفاء لدى التجار

بدايةً ينبغي أن نشير إلى نقطتين مهمتين:

الأولى: إذا كانت وسيلة الدفع تحمل تاريخ انتهاء صلاحية أو في حال أخبرت الجهة المصدرة التاجر بإلغاء البطاقة، ففي هذه الحالات يكون التاجر ملزم بعدم قبول هذه البطاقات كون بإمكانه التحقق من صلاحيتها. وفي حال قبل هذه البطاقة فإنه من الناحية المدنية ليس للتاجر أي حقوق لدى الجهة المصدرة ويتحمل تبعات فعله، أما من الناحية الجزائية فإنه يعد شريكاً للحامل في حال نسب للحامل أي جرم.

الثانية: إذا كانت وسيلة الدفع لا تحمل تاريخ صلاحية أو في حال لم تُخبر الجهة المصدرة التاجر بإلغاء البطاقة. ففي هذه الحالة يكون التاجر حسن النية (وذلك بعد أن يكون قد بذل جهده لتحقيق من صلاحية البطاقة). وبالتالي يحق له العودة على الجهة المصدرة والمطالبة بقيمة الفواتير. ولا يُعد شريكاً للحامل من الناحية الجزائية.

ما سوف نتحدث عنه في هذه الحالة هو الفرضية الآتية: الحامل وحده يعلم بإلغاء البطاقة أو انتهاء صلاحيتها، في حين أن التاجر الذي قُدمت له كان حسن النية فقد قبلها باعتبارها بطاقة لا تزال سارية المفعول. فالتساؤل المطروح حول ما هو التكييف الجزائي لحامل البطاقة الملغاة أو المنتهية الصلاحية والتي تُستخدم في الوفاء

لدى التجار؟

لقد ظهر في هذا الخصوص اتجاهين:

الاتجاه الأول: يرى أنصار هذا الاتجاه^١ أن فعل الحامل لا يمكن أن يبقى بعيداً عن المسؤولية الجزائية فهو بفعله قد أثرى على حساب غيره وحصل على أموال ليس له الحق في الاستيلاء عليها وذلك تم من خلال الأساليب التي لجأ إليها. فنشاطه يعد مكوناً لجريمة الاحتيال ويستند هذا الاتجاه في تبرير موقفه للحجج الآتية:

- ظهر حامل البطاقة باستعماله للبطاقة الملغاة أو المنتهية الصلاحية باعتباره صاحب صفة كاذبة، وذلك كون إلغاء البطاقة أو انتهاء صلاحيتها يخلع عنها صفتها كأداة للوفاء ويزيل أي صفة للشخص الذي يستخدمها، وإقدامه على استخدام البطاقة يُعتبر تأكيداً لصفة زالت بعد الإلغاء. وبالتالي يكفي بمجرد الادعاء بهذه الصفة لتحقيق جريمة الاحتيال.
- إن حامل البطاقة الذي يعلم بإلغاء البطاقة ويتقدم للتاجر بالبطاقة لتسوية معاملته يكذب وإلى جانب أنه يكذب يدعم كذبه باستعمال أحد الوسائل الاحتيالية التي حددها المشرع لقيام جريمة الاحتيال وهذه الوسيلة هي إبراز مستندات منسوبة للغير.

الاتجاه الثاني: يرى أنصار هذا الاتجاه^٢ أن فعل حامل البطاقة من شأنه أن يثير بحقه المسؤولية عن إساءة الائتمان، وهذا ما ذهب إليه بعض المحاكم الفرنسية حيث رأت أن حامل البطاقة إذا استمر باستخدامها بعد إلغائها فإنه يُسأل عن جريمة إساءة الائتمان، إذ إن الاستعمال الذي تقوم به إساءة الائتمان هو ذلك الاستعمال الذي لا

^١ مشار إليه لدى: د. طارق حمزة، مرجع سابق، ص ٣٥٦ و د. علي عبد القادر قهوجي، مرجع سابق، ص ٣٦٢.

^٢ مشار إليه لدى: بشرى سلامة، مرجع سابق، ص ٥٦.

يجوز أن يصدر من غير المالك بحيث أن الجاني بات ينظر لنفسه نظرة المالك.

بالنسبة لإساءة الائتمان:

نحن من جانبنا نرى أن حامل البطاقة الذي يستخدمها في الوفاء لدى التجار بعد إلغائها أو انتهاء صلاحيتها لا يسأل عن جريمة إساءة ائتمان، لأن محل الائتمان هو البطاقة ذاتها ولكن ما يجري بحثه في هذه الحالة كون حامل البطاقة الملغاة يقدم على استخدامها لدى التجار لتسوية معاملاته. وبالتالي يترتب على ذلك استيلائه على أموال دون وجه حق.

أما بالنسبة للاحتيال:

نحن من جانبنا ومع احترامنا للرأي الذي نادى بمساءلة الحامل عن جرم الاحتيال إلا أننا نرى أن الحامل الذي يقدم على استخدام بطاقة دفع ملغاة أو منتهية الصلاحية في الوفاء لدى التجار يسأل جزئياً عن جرم الاحتيال عبر الشبكة وذلك لتوفر أركان هذه الجريمة والمتمثلة في الآتي:

محل الجريمة: التاجر والمنظومة الخاضعة لسيطرته والمتمثلة ب (جهاز يدوي أو جهاز إلكتروني لقراءة البطاقة).

الركن المادي: قام الجاني (الحامل) باستخدام بطاقة الدفع الملغاة أو منتهية الصلاحية والتي تعمل عبر الشبكة في جهاز كمبيوتر (جهاز يدوي أو إلكتروني) وتمكن من الحصول على مال منقول دون وجه حق (السلع التي اشتراها من التاجر) عن طريق أساليب ووسائل أدت إلى خداع التاجر والمنظومة المعلوماتية الخاضعة لسيطرته (جهاز يدوي أو إلكتروني) من خلال قبول البطاقة على الرغم من إلغائها أو انتهاء صلاحيتها وبالتالي فقد ظهر حامل البطاقة بصفة

كاذبة، حيث أوهم التاجر أن البطاقة لا تزال سارية المفعول وأنه ما زال له صفة حقيقية على البطاقة الأمر الذي أدى لخداع التاجر. الركن المعنوي: ويتمثل في علم الحامل بفعله وإرادة هذا الفعل. وبالنتيجة نجد أن أركان جريمة الاحتيال عبر الشبكة متوفرة بحق الحامل الذي يقدم على استخدام بطاقة دفع ملغاة أو منتهية الصلاحية في الوفاء لدى التاجر ويعاقب بالحبس من ثلاث إلى خمس سنوات وبالغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي^١.

ولكن فيما لو أن التاجر كان عالماً بإلغاء البطاقة أو انتهاء صلاحيتها وأقدم على التواطؤ معه من خلال التلاعب وخداع الجهاز اليدوي أو الإلكتروني لقبول البطاقة على الرغم بإلغاء البطاقة أو انتهاء صلاحيتها بهدف الحصول على مال من المصرف بشكل غير مشروع، فإن الحامل والتاجر يسألان عن جرم الاحتيال عبر الشبكة ويعاقبان الاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية كون الاحتيال موجه للمصرف.

وبالنتيجة نجد أن حامل البطاقة الملغاة أو المنتهية الصلاحية والذي يقدم على استخدامها سواء في السحب أو الوفاء يسأل عن جرم الاحتيال عبر الشبكة لكونه استخدم بطاقة الدفع كوسيلة لخداع التاجر أو جهاز الصراف الآلي بهدف الحصول على المال دون وجه حق. وبما أن إلغاء البطاقة أو انتهاء صلاحيتها يفقد الحامل صفة الحامل الشرعي ويجعله شخص من الغير الأمر الذي يجعل هذا الحامل

^١ المادة (٢١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

مسؤولاً مدنياً عن تعويض الضرر الذي سببه للمجني عليه (التاجر أو المصرف) وفقاً لأحكام المسؤولية التقصيرية^١.

٣- المسؤولية الجزائية للحامل بالنسبة للامتناع عن رد البطاقة

يتضمن عقد تسليم البطاقة لحاملها التزام من قبل الحامل بردها إلى المصدر عندما يتم إلغاء البطاقة أو عند انتهاء صلاحيتها. والأسباب التي تدفع المصارف للمطالبة برد البطاقة قد تكون أسباب تجارية تتمثل في إمكانية استخدام مادة البطاقة في تصنيع بطاقات أخرى مما يقلل من التكلفة أو قد تكون أسباب احترازية تتمثل بمنع الحامل من استخدام البطاقة في الفترة بين إلغائها وبين التعميم على التجار. ولعل التساؤل المطروح يتمثل حول ماهية التكييف الجزائي لقيام الحامل بالامتناع عن رد البطاقة؟

تتمثل الفرضية في هذه الحالة على النحو الآتي: قام المصدر بإلغاء البطاقة أو انتهت صلاحيتها دون تجديد، وكان هناك إخطار للحامل من قبل المصدر بهذا الإلغاء، فطالب المصدر الحامل برد البطاقة إلا أن الأخير امتنع عن ردها واحتفظ بالبطاقة. فما هو التكييف الجزائي لفعله؟

يرى بعض الفقه^٢ أن امتناع الحامل عن رد البطاقة يجعله مسؤول وفق أحكام إساءة الائتمان. وذلك استناداً للشرط الوارد في العقد المبرم بين الحامل والمصدر والقاضي بملكية الجهة المصدرة للبطاقة من لحظة إصدارها وطيلة فترة استعمالها، وبالتالي فإن الحامل ملزم

^١ لمزيد من التفصيل بخصوص المسؤولية التقصيرية راجع ص ١٤٩ وما يليها.

^٢ مشار إليه لدى: د. محمد حماد مرهج الهيتمي، مرجع سابق، ص ١٦٧ - ١٦٨ و د. محمود طه، مرجع سابق، ص ١١٣٥.

بردها للمصدر عند الطلب. وبالتالي فإن ذلك يصلح سنداً قانونياً يمكن أن تؤسس عليه المسؤولية الجزائية.

إذ إن حامل البطاقة وبموجب هذا الشرط _ شرط ملكية البطاقة للمصدر - يكون حائزاً للبطاقة على سبيل الأمانة فقط، وعليه واجب ردها للجهة المالكة لها بمجرد الطلب، وعدم ردها من شأنه أن يؤدي لتحقيق جريمة إساءة الائتمان بحقه، كونه بذلك كتم أو اختلاس المال الذي سُلّم إليه على سبيل الأمانة بسوء نية.

ونحن من جانبنا نؤيد الفقه في تكييفه، وذلك لتوفر أركان هذه الجريمة، فقد نص قانون العقوبات على أنه: «كل من أقدم قصداً على كتم أو اختلاس أو إتلاف أو تمزيق سند يتضمن تعهداً وإبراء أو شيء منقول آخر سُلّم إليه على وجه الوديعة أو الوكالة أو الإجازة أو على سبيل العارية أو الرهن أو لإجراء عمل لقاء أجر أو دون أجره شرط أن يعيده أو يقدمه أو يستعمله في أمر معين يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة تتراوح بين ربع قيمة الردود والعطل والضرر وبين نصفها على أن لا تتقص عن ٢٠٠٠ ليرة»^١.

فالحامل امتنع عن رد بطاقة الدفع إلى المصرف رغم ثبوت علمه بالإخطار المرسل إليه من قبل المصرف بالرد، حيث تسلم هذه البطاقة للحامل بموجب عقد مع المصدر يسمح له على سبيل عارية الاستعمال، استخدامها وإعادةها بعد انتهاء العقد أو إلغائه وتظل البطاقة ملكاً للجهة المصدرة وليس للحامل.

كما أن بطاقة الدفع تعد من قبيل الأشياء المنقولة ذات طبيعة مادية وهو ما تقع عليه جريمة إساءة الائتمان.

^١ المادة ٦٥٦/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

كما أن الركن المعنوي لهذه الجريمة يتوافر بقيام الحامل بالاستيلاء على البطاقة مع العلم والإرادة وبذلك يتحقق القصد العام، وامتناعه عن إعادتها للمصدر رغم طلبها - حتى ولو لم يستعملها بعد ذلك - يعد اختلاس أو كتم وهو أحد صور النشاط الجرمي لجريمة إساءة الائتمان، الأمر الذي يكشف عن نيته في نقل الحياة للبطاقة من حياة ناقصة إلى حياة كاملة وبذلك يتحقق القصد الخاص.

نستنتج مما سبق أن احتفاظ الحامل بالبطاقة بعد إلغائها أو انتهاء صلاحيتها رغم طلبها من قبل المصدر، يكون قد ارتكب جرم إساءة الائتمان ويعاقب بالحبس من ٦ أشهر/ إلى ٣ سنوات/ وبغرامة تتراوح بين ربع قيمة الردود والعطل والضرر وبين نصفها على أن لا تنقص عن ٢٠٠٠/ ليرة/.

٤- المسؤولية الجزائية للحامل عن الاستخدام المقنع لبطاقة الدفع:

وتتمثل بإحدى صورتين:

أ- المسؤولية الجزائية للحامل عن الاستخدام بعد الادعاء بسرقة أو ضياع بطاقة الدفع.

للتقليل من مخاطر ضياع البطاقة أو سرقتها، فإن عقد إصدار البطاقة ينص على إلزام الحامل بالمحافظة عليها وإخطار الجهة المصدرة بفقدائها أو سرقتها بأي وسيلة كانت ومن ثم تأكيد هذا الإخطار بشكل مكتوب. ولكن ما نقصده في هذه الحالة هو الفرضية الآتية:

فقد يحدث أن يبلغ الحامل الجهة المصدرة بفقد البطاقة أو سرقتها، ثم يستخدمها بعد ذلك في السحب أو الوفاء وقبل أن يقوم المصرف ببرمجة أجهزة الصراف أو قبل أن يتم إخطار التاجر بعدم قبول هذه

البطاقة المبلغ عن فقدانها أو سرقتها. ولعل التساؤل حول ما التكيف الجزائي مثل هذه الحالة؟

تقتضي الإجابة على هذا التساؤل التمييز بين حالتين:

أ: حالة الوفاء لدى التجار: ويتجلى الاستخدام غير المشروع بأحد شكلين^١:

▪ كثيراً ما يقع التواطؤ بين الحامل والتاجر، حيث يتفقان على إخطار المصرف بفواتير مبيعات بمبالغ كبيرة، ثم يدعي الحامل أن بطاقته مفقودة أو مسروقة، وأنه لم يشتري شيئاً من السلع، فتكون مسؤولية الوفاء بقيمة السلع على المصرف، ثم يتقاسم الحامل مع التاجر المبلغ النقدي بعد صرفه من المصرف.

▪ قد يرتكب الحامل وحده هذه الجريمة دون تواطؤ مع التاجر. وذلك بقيام الحامل بتنفيذ كل ما يجب عليه في حال فقد البطاقة أو سرقتها من معارضة لدى المصرف مصدر البطاقة، مع إبلاغ السلطات المختصة، ثم يقدم على استخدامها لدى التجار المزودين بآلة الطباعة اليدوية خوفاً من اكتشاف أمره عن طريق الجهاز الإلكتروني، بحيث لا يمكن اكتشاف الغش عبر الجهاز اليدوي إلا في وقت لاحق عن طريق المواجهة بين التاجر والحامل. وقد يتحقق الغش لدى التاجر من خلال ادعاء الحامل استعجاله أو أنه إذا لم يبع له التاجر فهناك غيره أو أن مظهره يوحي بالنقطة فيخلج التاجر من مراجعتها.

وفي كلا الحالتين: يسأل الحامل عن جريمة الاحتيال عبر الشبكة لتوفر أركانها والمتمثلة في الآتي:

^١ د. حوالف عبد الصمد، مرجع سابق، ص ٥٣٣.

محل الجريمة: التاجر والمنظومة الخاضعة لسيطرته والمتمثلة ب (جهاز يدوي أو جهاز إلكتروني لقراءة البطاقة).

الركن المادي: قام الجاني (الحامل) باستخدام بطاقة الدفع بعد الادعاء بسرقتها أو فقدها والتي تعمل عبر الشبكة في جهاز كمبيوتر (جهاز يدوي أو إلكتروني) وتمكن من الحصول على مال منقول دون وجه حق (السلع التي اشتراها من التاجر) عن طريق أساليب ووسائل أدت إلى خداع التاجر والمنظومة المعلوماتية الخاضعة لسيطرته (جهاز يدوي أو إلكتروني) من خلال قبول البطاقة على الرغم من الادعاء بسرقتها أو فقدها وبالتالي فقد ظهر حامل البطاقة بصفة كاذبة، حيث أوهم التاجر أن البطاقة لا تزال سارية المفعول وأنه ما زال له صفة حقيقية على البطاقة الأمر الذي أدى لخداع التاجر.

الركن المعنوي: ويتمثل في علم الحامل بفعله وإرادة هذا الفعل. وبالنتيجة نجد أن أركان جريمة الاحتيال عبر الشبكة متوفرة بحق الحامل الذي يقدم على استخدام البطاقة بعد الادعاء بسرقتها أو فقدها في الوفاء لدى التاجر ويعاقب بالحبس من ثلاث إلى خمس سنوات وبالغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي.

ولكن فيما لو أن التاجر كان عالماً بالادعاء الكاذب وأقدم على التواطؤ معه من خلال التلاعب وخداع الجهاز اليدوي أو الإلكتروني لقبول البطاقة بهدف الحصول على مال من المصرف بشكل غير مشروع، فإن الحامل والتاجر يسألان عن جرم الاحتيال عبر الشبكة

ويعاقبان الاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية كون الاحتيال موجه للمصرف^١.

كما تجدر الإشارة إلى أن الحامل يسأل إلى جانب الاحتيال عن جرم التزوير، باعتبار أن إبلاغه عن فقد البطاقة أو سرقتها أفقده صفته كحامل شرعي وبالتالي يعد من الغير، وهذا يعني أن توقيعه على فواتير الشراء يعد من قبل التزوير ويعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة أقلها ٢٠٠٠ ليرة^٢.

وبالتالي فإن استخدام الحامل لبطاقة الدفع بعد الادعاء بسرقتها أو ضياعها في الوفاء لدى التجار ينطبق عليها نصين جزائيين /جرم الاحتيال عبر الشبكة+ جرم التزوير/ وبالتالي نكون أمام اجتماع جرائم مادي ويطبق النص الأشد وفي حالتنا هذه يطبق النص المتعلق بالاحتيال عبر الشبكة.

ب: حالة السحب من أجهزة الصراف الآلي: إن عملية استخدام البطاقة بعد الادعاء بسرقتها أو فقدانها في السحب من أجهزة الصراف الآلي، أمر نادر الحدوث في ظل التقنيات الحديثة التي يتم من خلالها برمجة أجهزة الصراف على سحب البطاقة بمجرد إدخالها. ولكن المشكلة تحدث عند استغلال الحامل الفترة بين الادعاء بسرقتها أو فقدانها وبين برمجة هذه الأجهزة على رفض البطاقة وسحبها. فما هو التكليف الجزائي لفعل الحامل في هذه الحالة؟

^١ المادة (٢١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام ٢٠١٢.

^٢ المادة ٤٦٠/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

على غرار حالة استخدام البطاقة في الوفاء لدى التجار بعد الادعاء بسرقتها أو فقدها فإن الحامل الذي يقدم على استخدام بطاقة في السحب من أجهزة الصراف الآلي بعد الادعاء بسرقتها أو فقدها يسأل جزائياً عن جريمة الاحتيال عبر الشبكة لتوفر أركانها المتمثلة في الآتي:

محل الجريمة: المنظومة المعلوماتية الخاضعة لسيطرة المجني عليه (جهاز الصراف الآلي الخاضع لسيطرة المصرف).

الركن المادي: قام الجاني (الحامل) باستخدام بطاقة بعد الادعاء بسرقتها أو فقدها والتي تعمل عبر الشبكة في جهاز كمبيوتر (جهاز الصراف الآلي) وتمكن من الحصول على مال منقول دون وجه حق (النقود التي سحبها بواسطة هذه البطاقة) عن طريق أساليب ووسائل أدت إلى خداع المنظومة المعلوماتية (جهاز الصراف الآلي) وجعله يقبل البطاقة ويصرف النقود على الرغم من الادعاء بفقدها أو سرقتها

الركن المعنوي: ويتمثل في علم الحامل بفعله وإرادة هذا الفعل. وبالنتيجة نجد أن أركان جريمة الاحتيال عبر الشبكة متوفرة بحق الحامل الذي يقدم على استخدام بطاقة في السحب من جهاز الصراف الآلي بعد الادعاء بفقدها أو سرقتها وطالما أن هذا الجهاز تابع للمصرف الأمر الذي يجعل هذا الاحتيال واقعاً على المصرف وبالتالي يعاقب الحامل بالاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف مليون ليرة سورية ولا تطبق الأسباب المخففة التقديرية إلا إذا اسقط المضرور حقه الشخصي^١.

^١ المادة (٢١) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

وبالنتيجة نجد أن حامل البطاقة والذي يقدم على استخدامها سواء في السحب أو الوفاء بعد الادعاء بسرقتها أو فقدها يسأل عن جرم الاحتيال عبر الشبكة لكونه استخدم بطاقة الدفع كوسيلة لخداع التاجر أو جهاز الصراف بهدف الحصول على المال دون وجه حق .
وبما أن الادعاء بفقد البطاقة أو سرقتها يفقد الحامل صفة الحامل الشرعي ويجعله شخص من الغير الأمر الذي يجعل هذا الحامل مسؤولاً مدنياً عن تعويض الضرر الذي سببه للمجني عليه (التاجر أو المصرف) وفقاً لأحكام المسؤولية التقصيرية^١.

ب- المسؤولية الجزائية للحامل بالنسبة لحصوله على بطاقة الدفع بصورة غير مشروعة:

يتم الحصول على بطاقة عن طريق تقديم طلب من الشخص طالب البطاقة للجهة المصدرة، يبين فيه رغبته في الحصول على وسيلة الدفع. وغالباً ما يكون هذا الطلب في شكل نموذج يقوم طالب البطاقة بملء البيانات المطلوبة، وإزاء أهمية هذه البيانات وجب على طالب البطاقة تقديم معلومات صحيحة، ولكن الفرضية في هذه الحالة تتمثل على النحو الآتي: تقدم الشخص بطلب للحصول على بطاقة دفع من الجهة المصدرة، ولكن كانت المعلومات المقدمة غير صحيحة (كالمعلومات المتعلقة بالملاءة المالية)، ونتيجة هذه المعلومات أصدرت الجهة البطاقة. فلعل التساؤل المطروح حول ما هي المسؤولية الجزائية للشخص عن تقديم معلومات غير صحيحة في سبيل الحصول على بطاقة الدفع؟

^١ لمزيد من التفصيل بخصوص المسؤولية التقصيرية راجع ص ١٤٩ وما يليها.

إن الشخص الذي يقوم بالحصول على وسيلة دفع إلكترونية أياً كان نوعها عن طريق غش وخداع الجهة المصدرة، باستخدامه مستندات مخالفة للحقيقة. والتي من شأنها إحداث الأمل بقدرته على تسديد قيمة العمليات والمشتريات التي سيقوم بها مستعملاً تلك الوسيلة، (كما لو ادعى الشخص أنه ميسور الحال وقدم مستندات تثبت ذلك). وكان عالماً بأن هذه البيانات التي أدلى بها من شأنها حمل الجهة المصدرة على إصدار البطاقة له، ومع ذلك أقدم على فعله. فإنه يسأل جزائياً عن جرم الاحتيال لتوفر أركانه:

حيث أن هذا الشخص حمل الجهة المصدرة على تسليمه مال منقول (بطاقة دفع) باستعمال اسم مستعار أو صفة كاذبة (الادعاء أنه ميسور الحال وقدم مستندات تثبت ذلك أو ادعى أنه تاجر معروف)، وكان على علم بان تقديمه لهذه المستندات غير الصحيحة من شأنها حمل الجهة المصدرة على منحه البطاقة وأراد ذلك.

وبالتالي نجد أن أركان جرم الاحتيال متوفر بحقه ويعاقب بالحبس من ٣ سنوات إلى ٥ سنوات/ وبالغرامة من ١٠ آلاف إلى ٥٠ ألف ليرة/، ولا يستفيد المحكوم من الأسباب المخففة التقديرية أو وقف التنفيذ أو وقف الحكم النافذ إلا في حالة إزالة الضرر^١.

كما تجدر الإشارة إلى أنه غالباً ما يترافق الحصول على البطاقة بمستندات غير صحيحة نوع من التزوير في الوثائق والمستندات المقدمة، الأمر الذي يدين الحامل بجرم التزوير إلى جانب جرم الاحتيال ويعاقب على التزوير بالحبس من سنة إلى ثلاث سنوات وبغرامة أقلها ٢٠٠٠/٢^٢.

^١ المادة ٦٤١/ من قانون العقوبات رقم/١٤٨/ لعام ١٩٤٩.

^٢ المادة ٤٦٠/ من قانون العقوبات رقم/١٤٨/ لعام ١٩٤٩.

وفي هذه الحالة نكون أمام اجتماع جرائم مادي ويطبق النص الأشد وفي حالتنا هذه يعاقب بعقوبة الاحتيال.

وتأكيداً على ما ذكرنا، فقد عرضت واقعة على محكمة النقض الألمانية^١، حيث قام أحد الأشخاص بالحصول على بطاقتي الدائنز كلوب والأمريكان اكسبريس، مستخدماً الطرق الاحتيالية، حيث كان عاملاً في أحد الصيدليات لكنه ادعى عند طلبه للبطاقة أنه صيدلي منتحلاً بذلك صفة غير صحيحة. كما قدم مستندات تثبت أنه ميسور الحال على عكس الحقيقة إذ كان معسراً، وبذلك أوقع المصدرين للبطاقتين في الغلط وحصل عليهما بفضل البيانات الكاذبة التي يقدمها، وقد أدانته محكمة النقض عن جريمة الاحتيال.

ثانياً: المسؤولية الجزائية للتاجر والمصدر.

سبق وأن أشرنا إلى أن عمليات الاستخدام غير المشروع من قبل التاجر أو المصدر قليلة الحدوث مقارنة بغيرها من حالات الاستخدام غير المشروع، لذلك سوف نتحدث بشكل مختصر عن المسؤولية الجزائية لهؤلاء الأطراف.

١- بالنسبة للتاجر: من خلال النظر بأساليب الاستخدام غير المشروع من قبل التاجر سواء عبر الآلة اليدوية أم الجهاز الإلكتروني، نجد أن معظم هذه الأساليب تقوم على أحد شكلين^٢:

أ- التلاعب بالآلة اليدوية أو الإلكترونية: إن التلاعب بالآلة اليدوية أو الجهاز الإلكتروني يجعل التاجر مسؤول عن جرم إساءة

^١ مشار إليه لدى د. حوالف عبد الصمد، مرجع سابق، ص ٥٣٤.

^٢ راجع ص ٣٣٩ وما يليها بخصوص الاستخدام غير المشروع من قبل التاجر.

الائتمان، باعتبار أن هذه الآلة أو الجهاز سلمت للتاجر على سبيل عارية الاستعمال، وبالتالي يعاقب التاجر وفق أحكام المادة /٦٥٦/ من قانون العقوبات التي نصت:

(الكل من أقدم قصداً على كتم أو اختلاس أو إتلاف أو تمزيق سند يتضمن تعهداً أو إبراءً أو شيء منقول آخر سلم إليه على وجه الوديعة أو الوكالة أو الإجازة أو على سبيل العارية أو الرهن أو لإجراء عمل لقاء أجره أو بدون أجره شرط أن يعيده أو يقدمه أو يستعمله في أمر معين يعاقب بالحبس من ٦ أشهر إلى ٣ سنوات وبغرامة تتراوح بين ربع قيمة الردود والعطل والضرر بين نصفها على أن لا تتقص عن /٢٠٠٠/ ليرة.

من تحليل النص السابق نجد الآتي:

❖ الآلة اليدوية أو الجهاز الإلكتروني شيء منقول سلم للتاجر على سبيل عارية الاستعمال ويلتزم التاجر برده للمصدر كونه مالك له.

❖ التلاعب الذي يُقدم عليه التاجر يشكل نوعاً من الإتلاف بالمفهوم الواسع باعتبار أن التلاعب يهدف إلى إتلاف الجهاز وجعله يقبل التعامل ببطاقات غير صحيحة بهدف الحصول على أموال غير مشروعة.

❖ التاجر الذي يقدم على فعل ذلك يكون عالماً بفعله وقاصداً إتيانه بهدف الكسب المادي غير المشروع.

وبالتالي نجد من التحليل السابق أن النص المتعلق بإساءة الائتمان يطبق على التاجر الذي يتلاعب بالآلة اليدوية أو الإلكترونية. وبالتالي يُعاقب بالحبس من ٦/ أشهر إلى ٣ سنوات/ وبغرامة تتراوح بين

ربع قيمة الردود والعطل والضرر وبين نصفها على أن لا تنقص عن /٢٠٠٠/ ليرة.

ب-تزوير التواقيع أو الفواتير: إن التاجر الذي يرتكب مثل هذه الأفعال يعاقب وفق أحكام المادة /٤٦٠/ والتي جاء فيها: (من ارتكب التزوير في أوراق خاصة بإحدى الوسائل المحددة في المادتين /٤٤٥/ و /٤٤٦/ عوقب بالحبس من سنة إلى ثلاث سنوات وبغرامة أقلها /٢٠٠٠/ ليرة).

وبالعودة لنص المادتين /٤٤٥/ و /٤٤٦/ نجد أن وسائل التزوير هي:

- إساءة استعمال إمضاء أو خاتم أو بصمة وإجمالاً توقيعته على إمضاء مزور إما بصنع صك أو مخطوط.
- ما يرتكبه من حذف أو إضافة أو تغيير في مضمون صك أو مخطوط.
- تدوين مقولات غير التي صدرت عن المتعاقدين.
- إثبات وقائع كاذبة أو غير معترف بها على أنها صحيحة أو معترف بها أو بتحريفه واقعة بإغفال أو إيراد على وجه غير صحيح.
- إساءة استعمال إمضاء على بياض أتمن عليه.

وكما هو معلوم فإن التزوير الذي يقوم به التاجر يندرج تحت أحد أسلوبيين:

إما تزوير (توقيع أو ختم الحامل) أو إضافة أو تغيير في مضمون الفاتورة، وبالتالي فإن هذين الأسلوبين يندرجان ضمن وسائل التزوير، كما أن الفواتير هي من الأوراق الخاصة. وبالنتيجة يُعاقب التاجر الذي يقدم على تزوير التواقيع أو الفواتير وفق أحكام المادة /٤٦٠/ من قانون العقوبات. كما تجدر الإشارة إلى أنه إذا ترافق

التلاعب بالجهاز مع تزوير في التوقيع أو الفواتير فإننا نكون أمام اجتماع جرائم مادي ويُعاقب التاجر وفقاً للنص الأشد.

٢- بالنسبة لموظفي المصدر: من خلال استعراض حالات الاستخدام غير المشروع من قبل موظفي المصدر^١، نجد أن في مجملها تتطوي على نوع من التواطؤ مع الحامل أو التاجر أو الغير بهدف تسهيل الاستخدام غير المشروع سواء تسهيل تجاوز الرصيد أم تسهيل التلاعب بالآلة أم تزويد الغير بأرقام البطاقات، وبالتالي فإن هذا التواطؤ يجعل موظفي المصدر شركاء للفاعل الأساسي (الجاني في عملية الاستخدام غير المشروع) وبالتالي يعاقب بعقوبته. فعلى سبيل المثال إذا كان التاجر يعاقب وفق أحكام إساءة الائتمان أو التزوير وكان هذا الموظف قد سهل التلاعب أو التزوير فإنه يعاقب وفق أحكام إساءة الائتمان أو التزوير أيضاً.

وبغية التبويب القانوني لعمليات الاستخدام غير المشروع من قبل التاجر وموظفي المصدر نقترح على المشرع السوري أن يضيف مادة قانونية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية تتناول هذه النقطة ونقترح فيما يلي نص المادة:

((يعاقب بالحبس من ثلاث إلى خمس سنوات وبالغرامة من خمسمائة ألف ليرة إلى مليوني ونصف مليون ليرة سورية:

- كل تاجر يتلاعب بالجهاز اليدوي أو الإلكتروني بغية تعطيله عن عمله أو يتلاعب بالإشعارات والفواتير بأي وسيلة كانت.

^١ راجع ص ٣٥٣ وما يليها بخصوص الاستخدام غير المشروع من موظفي المصدر.

- كل موظف لدى الجهة المصدرة سهل الاستخدام غير المشروع لبطاقة الدفع بأي وسيلة كانت)).

وتجدر الإشارة إلى أنه فضلاً عن المسؤولية الجزائية لأطراف عملية الدفع، فإن عمليات الاستخدام غير المشروع تشكل نوعاً من الإخلال بالالتزامات التعاقدية المفروضة بموجب عقود استخدام وسيلة الدفع وبالتالي يكون الجاني مسؤول مدنياً عن تعويض الضرر الذي أصاب المجني عليه وفقاً لأحكام المسؤولية العقدية والتي تقوم على الإخلال بالتزام عقدي، أو قد تكون المسؤولية تقصيرية كما لو كانت البطاقة ملغاة أو منتهية الصلاحية.

وفي ختام الحديث عن المسؤولية الجزائية لأطراف عملية الدفع الإلكتروني نجد أن المشرع السوري في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية جرم معظم عمليات الاستخدام غير المشروع بموجب نصوص قانونية خاصة. حيث تصدت المادة (٢١) المتعلقة بالاحتيال عبر الشبكة لمعظم عمليات الاستخدام غير المشروع لبطاقة الدفع سواء في السحب من أجهزة الصراف الآلي أم في الوفاء لدى التجار، فقد كان لمرونة نص هذه المادة -من خلال عدم تحديد وسيلة محددة لارتكابها فضلاً عن المساواة بين خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرته- الأثر الكبير في شمولها لمعظم عمليات الاستخدام غير المشروع، كما جاء قانون العقوبات بأحكامه وخصوصاً الأحكام المتعلقة بالاحتيال وإساءة الائتمان والتزوير لتشمل بعض حالات الاستخدام غير المشروع لبطاقة الدفع الإلكتروني من قبل أطراف الدفع.

وبعد أن تعرفنا على المسؤولية الجزائية لأطراف عملية الدفع عن الاستخدام غير المشروع ننتقل للحديث عن المسؤولية الجزائية للغير عن الاستخدام غير المشروع.

الفرع الثاني

المسؤولية الجزائية للغير

سبق وأن أشرنا إلى أن الغير يلجأ إلى الاستخدام غير المشروع لوسائل الدفع الإلكتروني من خلال ثلاث مراحل (التعاملات العادية، التعاملات عبر أجهزة الصراف الآلي، التعاملات عبر شبكة الإنترنت).

فبالنسبة للتعاملات العادية: لا تثير هذه التعاملات إشكالية، باعتبار أن معظم أساليب الاستخدام غير المشروعة في هذه التعاملات تقوم على عمليات السرقة أو التزوير، (وقد سبق لنا الحديث عن المسؤولية الجزائية لهذه الأفعال^١).

أما بالنسبة للتعاملات عبر شبكة الإنترنت والتعاملات عبر أجهزة الصراف الآلي: فيتمثل الاستخدام غير المشروع في هذه التعاملات من خلال مجموعة من الأساليب تهدف إلى الاستيلاء أو الالتقاط غير المشروع لأرقام بطاقات الدفع بهدف استخدامها بشكل غير مشروع (كالسحب من أجهزة الصراف أو الوفاء لدى التجار، أو تزوير هذه الأرقام ووضعها على بطاقة فارغة... الخ^٢).

ولعل الإشكالية الرئيسة في التعاملات عبر شبكة الإنترنت أو عبر أجهزة الصراف الآلي تتمثل حول المسؤولية الجزائية للغير الذي يستولي على أرقام البطاقات في هذه التعاملات ؟

^١ راجع ص ٤٢١ وما يليها بخصوص المسؤولية الجزائية عن السرقة و ص ٤٣٥ وما يليها بخصوص المسؤولية الجزائية عن التزوير.

^٢ راجع ص ٣٦١ وما يليها بخصوص الاستخدام غير المشروع عبر أجهزة الصراف الآلي و ص ٣٦٤ وما يليها بخصوص الاستخدام غير المشروع عبر شبكة الإنترنت.

يرى بعض الفقه أن الغير الذي يستولي على أرقام بطاقات الدفع في نطاق التعاملات عبر شبكة الإنترنت أو عبر أجهزة الصراف الآلي يكون مسؤولاً عن جريمة السرقة لهذه الأرقام واستندوا في ذلك للمبررات الآتية:

❖ تصلح المعلومات المتعلقة ببطاقات الدفع لأن تكون محل لجريمة السرقة باعتبار أن هذه المعلومات ذات قيمة اقتصادية كبيرة، فهي بمثابة الطاقة الكهربائية التي لجأ المشرع السوري إلى تجريم سرقتها على الرغم من أنها ليست من طبيعة مادية.

❖ إن طبيعة الشيء محل السرقة هي التي تحدد طبيعة الأسلوب الذي سوف يتبعه الجاني للقيام بفعل الأخذ، فمثلاً الاستيلاء على تيار كهربائي يختلف عنه في حال الاستيلاء على كتاب.

❖ إن طبيعة الشيء محل السرقة هي التي تحدد كيفية خروج الشيء من ذمة الشخص، فإذا كان الشيء مادياً فإن إنقاص الذمة لا يكون إلا بخروجه من ذمة صاحبه، إما إذا كان الشيء من طبيعة معنوية (كالمعلومات المتعلقة ببطاقات الدفع) فإن إنقاص الذمة لا يكون بخروجه من ذمة صاحبه، بل يتحقق ذلك بإنقاص قيمة هذه المعلومات حيث أن صاحبها لم يعد هو المالك الوحيد لها على الرغم من أن أصل المعلومة لا زال لديه.

ونحن من جانبنا لا نؤيد تطبيق أحكام السرقة بحق الغير الذي يستولي على أرقام بطاقات الدفع وذلك للحجج الآتية:

❖ عرّف المشرع السوري السرقة بأنها: أخذ مال الغير المنقول دون رضاه^٢. وبالتالي تتطلب المشرع السوري أن يكون محل الجريمة شيء

^١ مشار إليه لدى: د. علي عبد القادر القهوجي، مرجع سابق، ص ٦٤ و بشرى سلامة، مرجع سابق، ص ٨١.

^٢ المادة ٦٢١/ من قانون العقوبات رقم ١٤٨/ لعام ١٩٤٩.

منقول ذو طبيعة مادية، والمنقول كل ما يمكن تحريكه ونقله من مكان لآخر دون أن يتعرض لتلف أو تغيير معالمه^١. والمعلومات المتعلقة ببطاقة الدفع ذات طبيعة معنوية وبالتالي لا تصلح أن تكون محل لجريمة السرقة، وذلك باعتبار أن المعيار الذي اعتمدته المشرع السوري معيار مادي وليس معيار اقتصادي.

❖ إن فعل الأخذ في جريمة السرقة، يتطلب القيام بمجموعة من الحركات والأفعال بهدف الاستيلاء على المنقول، وبالتالي فإن فعل الأخذ ذو طبيعة مادية بخلاف المعلومات المتعلقة ببطاقة الدفع ذات الطبيعة المعنوية.

❖ تتطلب جريمة السرقة إنقاص ذمة الشخص بانتقال الحيازة من المالك إلى الجاني، أما في نطاق المعلومات المتعلقة ببطاقة الدفع ليس هناك انتقال للحيازة، إنما هناك نوع من التزام بين الحيازتين، حيث بقيت هذه المعلومات بذمة صاحبها وأشغلت ذمة أخرى بها بنفس الوقت.

❖ القول إن فعل الأخذ يتناسب مع طبيعة الشيء محل السرقة أمر غير دقيق باعتبار أن النصوص القانونية المتعلقة بالسرقة جاءت واضحة ولا تتحمل أي تأويل أو تفسير. فهذه النصوص جاءت للمنقولات المادية دون المعنوية بشكل واضح وصريح وأي خروج عن هذه الأحكام نوع من الاستثناء والمعلومات المتعلقة ببطاقة الدفع لم تدرج ضمن هذه الاستثناءات، الأمر الذي ينبغي عدم التوسع في تفسير هذه النصوص.

وما يؤيد موقفنا هذا لجوء المشرع السوري لتنظيم هذه الحالة بموجب نص خاص في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، حيث جاء فيه: «يُعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية، كل من حصل دون

^١ المادة (٨٤) بمفهوم المخالفة) من القانون المدني رقم ٨٤/ لعام ١٩٤٩.

وجه حق على بيانات أو أرقام بطاقات دفع باستخدام الأجهزة الحاسوبية أو الشبكة^(١).

نستنتج من النص السابق أن المشرع السوري أدرك عدم إمكانية تطبيق أحكام قانون العقوبات على حالة الاستيلاء غير المشروع على أرقام بطاقات الدفع، فجاء النص السالف الذكر كنوع من توفير الحماية الجزائية للمتعاملين ببطاقات الدفع عبر شبكة الإنترنت أو عبر أجهزة الصراف الآلي.

حيث يتمثل الركن المادي في هذه الجريمة بحصول الجاني أو استيلائه دون وجه حق على بيانات أو أرقام بطاقة الدفع باستخدام الأجهزة الحاسوبية أو الشبكة، وينتج عن هذه الأفعال حصول الجاني على الأرقام والمعلومات الخاصة بالبطاقة كما أنه لا بد أن يكون هناك علاقة سببية بين الفعل والنتيجة.

ويتميز النص القانوني السالف الذكر بكونه لم يحدد وسيلة معينة لارتكابه فعبارة باستخدام الأجهزة الحاسوبية أو الشبكة مفهوم واسع يندرج تحته أي جهاز أو وسيلة إلكترونية. وبالتالي يمكن القول إن معظم الأساليب الوارد ذكرها في نطاق الاستخدام غير المشروع عبر شبكة الإنترنت أو عبر أجهزة الصراف تصلح لأن تكون وسيلة لارتكاب هذه الجريمة، باعتبار أن هذه الوسائل تدرج ضمن المفهوم الواسع لمصطلح الأجهزة الحاسوبية أو الشبكة. بينما يتمثل الركن المعنوي في علم الفاعل بطبيعة فعله وإرادته له.

وبالنتيجة يمكن القول إن الغير الذي يستولي على أرقام بطاقات الدفع عبر شبكة الإنترنت أو عبر أجهزة الصراف الآلي يُعاقب وفق أحكام المادة (٢٢) /أ/ بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة من خمسمائة ألف إلى مليوني ونصف مليون ليرة سورية.

^(١) المادة (٢٢/أ) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧/ لعام

وفي ختام الحديث عن سبل معالجة المشكلات الأمنية نجد أن هذه الأساليب تندرج ضمن ثلاثة أشكال:

الشكل الأول: التدابير التقنية

وهي أحد التدابير الوقائية التي تتمثل بمجموعة من البرامج والخطوات التقنية المتخذة من قبل الجهات المصدرة في سبيل إتمام المعاملات الإلكترونية من خلال التحقق من هوية المستخدم وتجنب عمليات الدخول غير المشروع أو الاستيلاء على البيانات بشكل غير مشروع سواء في البطاقات المصرفية أم في عمليات الشراء عبر الإنترنت.

الشكل الثاني: الوسائل الإدارية وهي أيضاً أحد التدابير الوقائية التي تتمثل بمجموعة من الالتزامات المفروضة على أطراف الدفع الإلكتروني وبشكل خاص الجهات المصدرة وذلك بهدف التقليل من حدوث بعض المشكلات كالسرقة والاستخدام غير المشروع أو بهدف اكتشاف بعض المشكلات كالتزوير.

الشكل الثالث: المسؤولية الجزائية: شكلت المسؤولية الجزائية المنصوص عليها بموجب نصوص قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية أو قانون العقوبات، أهم أساليب المعالجة الفعالة للمشكلات الأمنية من خلال ترتيب المؤيدات الجزائية بحق الجاني سواء أكان من أطراف عملية الدفع الإلكترونية أم من الغير.

الخاتمة

بعد أن انتهينا من دراسة موضوع الرسالة المعنون ب: (الحلول القانونية لمشكلات الدفع الإلكتروني-دراسة تطبيقية على بطاقات الدفع الإلكترونية) نبين ما توصلنا إليه من نتائج ثم نعرض أهم المقترحات:

أولاً: النتائج

بالنسبة لمظاهر المشكلات القانونية:

١-ينتاب مستخدم أداة الدفع نوعين من المشكلات:

- فباعتباره عميلاً للمصرف: تعد مشكلة انتهاك البيانات بشكل إلكتروني أحد التحديات القانونية التي تواجهه وذلك نظراً لتعدد الوسائل والأساليب التقنية التي يمكن من خلالها انتهاك البيانات.
- أما باعتباره مستهلكاً إلكترونياً: فهناك نوعين من المشكلات:
- ❖ مشكلات جديدة كشف عنها التطور التقني (كمشكلات الشراء عبر الحدود والتحديات التقنية)،
- ❖ مشكلات تقليدية تواجه أي متعاقد ظهرت بقالب جديد (المشكلات القانونية).

٢-يواجه الاقتصاد الوطني نوعين من التحديات القانونية باستخدام وسائل الدفع الإلكتروني:

- مشكلة التهرب الضريبي وذلك في ظل عدم وجود موقف واضح ومحدد من مسألة خضوع معاملات الدفع للضريبة من جهة فضلاً عن وجود مجموعة من المشكلات والتحديات التقنية

والقانونية التي تواجه فرض الضريبة على هذه المعاملات من جهة أخرى.

- **مشكلة غسيل الأموال** ذلك من خلال استخدام وسائل الدفع كأساليب حديثة لارتكابها نظراً لسهولة تداول الأموال غير المشروعة بواسطة هذه الوسائل دون أي قيود ورقية أو جغرافية ودون أن تترك أي أثر يدل عليها.

بالنسبة لسبل معالجة المشكلات القانونية:

٣-شككت المسؤولية الجزائية أحد أهم التدابير العلاجية لبعض المشكلات القانونية وبالتحديد:

- **مشكلة انتهاك السرية**: حيث كرست المسؤولية القانونية بشكليها الجزائي والمدني بشكل صريح بموجب أحكام(المادتين ٩-٢٣)من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.
- **مشكلة غسيل الأموال**: حيث كرست المسؤولية الجزائية بموجب أحكام المرسوم رقم ٣٣/ لعام ٢٠٠٥ وتعديلاته و ذلك تحت طابع المرونة في المصطلحات الأمر الذي منحها المسوغ القانوني لتطبيق أحكام هذا المرسوم على هذا النوع من غسيل الأموال.

٤-تمثل العلاج القانوني لمشكلة القانون الواجب التطبيق والمحكمة المختصة على النحو الاتي:

- **بالنسبة لمشكلة القانون الواجب التطبيق**: فقد تمثل العلاج بتطبيق قانون الإرادة أو قانون الدولة التي تم فيها العقد وذلك بالنسبة لعمليات الدفع المقدمة من قبل مصرف تقليدي أو مصرف إلكتروني له مركز تأسيس وحصل على التراخيص اللازمة أو مركز إدارة

فعلي أو يباشر نشاطه ضمن النطاق العلوي السوري وذلك سنداً للمادة (١١ من قانون المعاملات) والمادة (٢٠ من القانون المدني).

• أما بالنسبة لمشكلة المحكمة المختصة: تختص المحاكم المصرفية والمحاكم المتخصصة بجرائم المعلوماتية والاتصالات بمنازعات الدفع الإلكتروني كل حسب اختصاصه وذلك سنداً للمواد (١٢ من قانون المعاملات) والمادة (٢) من القانون الخاص بإحداث المحاكم المصرفية والمواد (٢،٥) من القانون الخاص بإحداث المحاكم المتخصصة بجرائم المعلوماتية والاتصالات.

٥- كرس المشرع السوري الحماية القانونية للمستهلك الإلكتروني كمتعاقد من خلال مجموعة من الالتزامات القانونية ومجموعة من الدعاوي القضائية والمؤيدات الجزائية سواء بموجب القوانين النازمة للمعاملات الإلكترونية أم بموجب القوانين النازمة للمعاملات التقليدية.

٦- إن منح المصرف المركزي الحق الحصري في إصدار النقود الإلكترونية أسوة بالنقود التقليدية من شأنه أن يسهم في تحقيق التوازن الاقتصادي بين النقود الإلكترونية والنقود التقليدية، كما من شأن ذلك أن يسهم في حل الخلاف حول القوة الإبرائية للنقود الإلكترونية حيث تتحول قوتها الإبرائية من القوة الاتفاقية إلى القوة القانونية وذلك على اعتبار أن النقود الإلكترونية شكل جديد كشف عنه التطور التقني إلى جانب النقود التقليدية وكتابية وتؤدي ذات الوظائف التي تؤدي النقود التقليدية.

بالنسبة لمظاهر المشكلات الأمنية:

٧- تعد مشكلة فقدان بطاقة الدفع وتزويرها أحد أهم التحديات الأمنية الناشئة عن المساس بأداة الدفع باعتبارها عنصر تقني ومادي في آن واحد.

• فقد تحدث مشكلة الفقدان:

- ❖ بوسائل مشروعة دون تدخل الغير (كضياع البطاقة أو ادخال الرقم السري بشكل خاطئ).
- ❖ بوسائل غير مشروعة وبتدخل الغير (كسرقة بطاقة الدفع أو سرقة بياناتها بهدف استخدامها في السحب أو الوفاء).

• بينما تتخذ مشكلة التزوير شكلين:

- ❖ تزوير جديد كشف عنه التطور التقني (كتزوير بطاقة الدفع-تزوير عن طريق تعديل البرمجيات الإلكترونية).
- ❖ تزوير مشابه للتزوير التقليدي ولا يختلف عنه إلا من ناحية محل الجريمة (كتزوير الاشعارات والمستندات الناشئة عن التعامل ببطاقة الدفع أو المتعلقة بالحصول عليها).

٨--تتمثل مشكلة الاستخدام غير المشروع لبطاقة الدفع كأحد التحديات الأمنية الناشئة عن المساس بعمل أداة الدفع الإلكترونية (بطاقة الدفع) في مظهرين:

• فقد ترتكب من قبل الأطراف:

- ❖ فالحامل قد يسيء استخدام البطاقة خلال فترة صلاحيتها (من خلال تجاوز الرصيد في السحب أو الوفاء)، أو خارج فترة الصلاحية (استخدام بطاقة ملغاة أو منتهية الصلاحية)، أو من خلال الاستخدام المقنع (ادعاء غير الصحيح بعدم استخدام البطاقة).
- ❖ كما أن التاجر قد يرتكب الاستخدام غير المشروع من خلال التلاعب بالأجهزة اليدوية أو الإلكترونية لتقبل بطاقة مزورة أو

منتهية الصلاحية أو من خلال تزوير توقيع الحامل أو بيانات بطاقته على فواتير وهمية .

قد ترتكب من قبل الغير: من خلال سرقة البطاقة أو تزويرها أو قد يلجأ إلى مجموعة من الأساليب التقنية بهدف الحصول على أرقام وبيانات بطاقات الدفع في سبيل استخدامها بشكل غير مشروع ومثال ذلك (وضع جهاز قارئ في جهاز الصراف - اختراق منظومة الاتصالات) بالنسبة لسبل معالجة المشكلات الأمنية:

١٠- تتجلى التدابير الوقائية بمجموعة من التدابير التقنية (التوقيع الإلكتروني و برامج وبروتوكولات تأمين البيانات) ومجموعة من الوسائل الإدارية (إجراءات والتزامات) الهادفة إلى تلافي حدوث المشكلات الأمنية من خلال التحقق من هوية المستخدم وضمان الانتقال السليم للمعلومات عبر الشبكة.

١١- كُرس العلاج القانوني **لمشكلة سرقة بطاقة الدفع الإلكترونية** من خلال ترتيب المسؤولية الجزائية بحق الجاني:

- عن جريمة استعمال الوسيلة المسروقة في السحب أو الوفاء في حال كان الجاني حائزاً على البطاقة واستخدمها (سنداً للمادة ٢٢/ب/٢ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية).
- عن جريمة الحصول دون وجه حق على أرقام وبيانات بطاقة الدفع وجرم الاحتيال عبر الشبكة في حال كان حائزاً على بيانات البطاقة دون جسمها واستخدم هذه البيانات (سنداً

للمادة ٢٢/أ والمادة ٢١ من قانون تنظيم التواصل على الشبكة).

- أما سرقة البطاقة ككيان مادي دون استعمالها أو كتم لقطة البطاقة فيسأل الجاني وفق أحكام قانون العقوبات (سنداً للمادة ٦٣٤ بالنسبة للسرقة والمادة ٦٥٩ بالنسبة لكتم اللقطة).

١٢- كُرس العلاج القانوني لمشكلة تزوير بطاقة الدفع الإلكترونية من خلال ترتيب المسؤولية الجزائية بحق الجاني:

- عن جرم تزوير بطاقة الدفع أو جرم استعمال الوسيلة المزورة في السحب أو الوفاء (سنداً للمادة ٢٢/ب/١-٢ من قانون تنظيم التواصل على الشبكة).
- أما بالنسبة للجاني الذي يزور الاشعارات والمستندات الناشئة عن التعامل ببطاقة الدفع أو المتعلقة بالحصول عليها فإن كانت هذه المستندات ورقية يسأل عن جرم التزوير وفق أحكام قانون العقوبات (سنداً للمادة ٤٦٠) أما إن كانت المستندات إلكترونية فيسأل وفق أحكام قانون التوقيع الإلكتروني وخدمات الشبكة (سنداً للمادة ٣١).

١٣- كُرس العلاج القانوني لمشكلة الاستخدام غير المشروع لبطاقة الدفع الإلكترونية من خلال ترتيب المسؤولية الجزائية على النحو الآتي:

- فالحامل الذي يقدم على ذلك يسأل عن:
- ❖ جريمة الاحتيال عبر الشبكة (سنداً للمادة ٢١ من قانون تنظيم التواصل على الشبكة) في حال استخدام بطاقة ملغاة أو منتهية

- الصلاحية في السحب أو الوفاء أوفي حالة الاستخدام المقنع) استخدام البطاقة بعد الادعاء غير الصحيح بفقدائها أو سرقتها).
- ❖ عن جرم إساءة الائتمان في حال امتنع عن رد البطاقة أو استخدام البطاقة بما يجاوز الرصيد في السحب أو الوفاء(سنداً للمادة ٦٥٦ من قانون العقوبات).
- ❖ عن جريمة الاحتيال في حال الحصول على البطاقة بمستندات مزورة (سنداً للمادة ٦٤١ من قانون العقوبات).
- أما بالنسبة للتاجر الذي يقدم على الاستخدام غير المشروع فيسأل وفق أحكام قانون العقوبات عن جرم إساءة الائتمان بالنسبة للتلاعب بالأجهزة وعن جرم التزوير بالنسبة للتلاعب بالفواتير والتوقيعات.
 - في حين يسأل الغير عن جرم الحصول دون وجه حق على أرقام وبيانات بطاقات الدفع بالنسبة لحالات الاستخدام غير المشروع من قبله(سنداً للمادة ٢٢/أ من قانون تنظيم التواصل على الشبكة).

ثانياً: المقترحات

١- بالنسبة للمصرف الإلكتروني الذي يقدم خدماته في الفضاء الخارجي نقترح أن يطبق عليه قانون الإرادة أو قانون دولة المستفيد (قانون الدولة التي يحمل جنسيتها أو قانون الدولة التي يقيم فيها بشكل معتاد) كونه من أقدر القوانين على تحقيق العدالة .

٢- نأمل من المشرع السوري أن يلجأ إلى تنظيم قواعد الحماية المنصوص عليها في القانون المدني ضمن نطاق قانون المعاملات الإلكترونية وذلك بهدف جعل هذه القواعد المقررة لحماية المستهلك الإلكتروني بصفته مستهلك وليس بوصفه متعاقد حيث أنه إذا لم تتوافر الضوابط القانونية المنصوص

عليها في هذه المواد فإن هذه المواد لا تطبق على المستهلك وخصوصاً أن التوجهات الحديثة تتطلع نمو التوسع في نطاق التعاملات الإلكترونية.

٣- بالنسبة لمسألة فرض الضريبة وتحصيلها على معاملات الدفع الإلكتروني نقترح بدايةً تبني الإطار العام لكيفية فرضها بغية توفير البيئة المناسبة لفرضها، أما بالنسبة لنوعها نقترح تطبيق ضريبة البيت وأن يعهد بتحصيلها لمزودي خدمات الإنترنت باعتبارها شكل جديد أفرزته الثورة التقنية وباعتبار أن هذه الجهة هي الأقدر على تحديد كمية البيت المستخدمة، أما بالنسبة للدولة صاحبة الحق بفرض الضريبة فإنه بدايةً ينبغي وجود معايير موحدة بين الدول ومن ثم يعهد بفرض الضريبة إما للدولة التي تم فيها العقد أو الدولة التي يحمل المكلف جنسيتها.

٤- نأمل من المشرع السوري تعديل المادة (٢٢) من قانون تنظيم التواصل على الشبكة بفقرتيها (أ-ب) على النحو الذي شرحناه في متن الرسالة وذلك لجعل الفقرة (أ) تشمل حالة سرقة بطاقة الدفع وكنتم لقطتها، وجعل الفقرة (ب) تشمل حالات تزوير الاشعارات وتقليد أجهزة ATM والتزوير عن طريق تعديل البرمجيات الإلكترونية دون ترك هذه الحالات لأحكام قانون العقوبات.

٥- نأمل من المشرع السوري إضافة مادة جديدة على قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على النحو الذي شرحناه في متن الرسالة تجرم حالات الاستخدام غير المشروع من قبل التاجر و من قبل موظفي المصدر بغية التبويب القانوني السليم لكافة حالات الاستخدام غير المشروع دون ترك ذلك لأحكام قانون العقوبات.

المراجع القانونية

أولاً: باللغة العربية

١- الكتب:

- د. إبراهيم الدوي، التجارة الإلكترونية، دراسة تطبيقية على المكتبات، مطبوعات مكتبة الملك فهد الوطنية، السعودية، ٢٠١٠.
- د. أحمد السيد لبيب إبراهيم، الدفع بالنقود الإلكترونية (ماهيته - تنظيمه القانوني) دراسة تحليلية مقارنة، دار الجامعة الجديدة، مصر، ٢٠٠٩.
- د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، ٢٠٠٠.
- د. أحمد سفر، أنظمة الدفع الإلكترونية، ط١، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٨.
- د. أروى الفاعوري ود. إيناس قطيشات، جريمة غسيل الأموال (المدلول العام و الطبيعة القانونية) دراسة مقارنة، دار وائل للنشر، الأردن، ٢٠٠٢.
- د. إلياس ناصيف، العقود الدولية، العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٩،
- د. أمجد الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، دار المسيرة، الأردن، ٢٠١٠.

- د. بسام شيخ العشرة و د. حنان مليكه، التجارة الإلكترونية
، منشورات الجامعة الافتراضية، دمشق، ٢٠١١-٢٠١٢.
- د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا
الحديثة، دار النهضة العربية، مصر، ١٩٩٢.
- د. حمود محمد غازي الحمادة، العلاقات التعاقدية الناشئة عن
بطاقات الدفع الإلكتروني، المركز العربي للنشر
والتوزيع، مصر، ٢٠١٧.
- د. روكس رزق، السر المصرفي، ط١، المؤسسة الحديثة
للكتاب، لبنان، ١٩٩٥.
- د. رياض فتح الله بصله، جرائم بطاقة الائتمان، ط١، دار
الشروق، مصر، ١٩٩٥.
- د. سميحة القليوبي، الأوراق التجارية، دار النهضة العربية،
مصر، ١٩٩٩.
- د. سمير بالي، السرية المصرفية، منشورات الحلبي الحقوقية
، لبنان، ٢٠٠٢.
- د. شريف غنام، محفظة النقود الإلكترونية، دار الجامعة
الجديدة، مصر، ٢٠٠٧.
- د. شريف سعيد كامل، مكافحة غسيل الأموال في التشريع
المصري، دار النهضة العربية، مصر، ٢٠٠٢.

- د. طارق حمزة ، النقود الإلكترونية كأحدى وسائل الدفع(تنظيمها القانوني-المسائل الناشئة عن استعمالها)، ط١ ، منشورات زين الحقوقية ،لبنان، ٢٠١١.
- د. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، ط١، دار الفكر الجامعي، مصر، ٢٠٠٧.
- د. عبد اللطيف عبد الحميد ،البنوك الشاملة (عملياتها ، إدارتها (، دار الجامعة الجديدة، مصر، ٢٠٠١.
- د. عبد اللطيف عبد الحميد، العولمة و اقتصاديات البنوك، دار الجامعة الجديدة، مصر، ٢٠٠٣.
- د. علاء التميمي، التنظيم القانوني للبنك الإلكتروني على شبكة الإنترنت، دار الجامعة الجديدة ، مصر، ٢٠١٢.
- د. علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية، دراسة قانونية، لا يوجد دار نشر، ١٩٨٩.
- د. عمر سالم، الحماية الجنائية لبطاقة الوفاء، ط١، دار النهضة العربية، مصر، ١٩٩٥.
- د. فواز صالح، مصادر الالتزام، الجزء الأول، كلية الحقوق، منشورات جامعة دمشق، ٢٠١٢.
- د. محمد حماد مرهج الهيتمي، الحماية الجزائية لبطاقات الائتمان، دار النهضة العربية، مصر، ٢٠٠٩.
- د. محمد واصل ، أصول المحاكمات المدنية، الجزء الأول، كلية الحقوق، منشورات جامعة دمشق، ٢٠١٠، ٢٠١١ .

- د. نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، ٢٠٠٧.
- نجاح محمد فوزي، وعي المواطن العربي تجاه جرائم الاحتيال (بطاقات الدفع الإلكترونية نموذجاً)، الرياض، ٢٠٠٧.
- د. هشام رستم، قانون العقوبات ومخاطر المعلومات، ط١، مكتبة الآلات الحديثة، مصر، ١٩٩٢.
- د. هدى قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، مصر، ٢٠٠٩.

٢-الأبحاث:

- د. إبراهيم الدسوقي أبو ليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣.
- د. إبراهيم كامل الشوابكه، ضريبة المبيعات على التجارة الإلكترونية، بحث منشور في مجلة علوم الشريعة والقانون، المجلد ٣٤/، الجامعة الأردنية، عمان، ٢٠٠٧، متاح على الرابط: _____

www.Journals.ju.edu.jo/Disasat/Law/article

[/view /612/610](#)

تاريخ الزيارة : ٣٠/١٠/٢٠١٨ الساعة ٣:٤٥ pm

▪ د. أديب ميالة و د. مي محرز، السرية المصرفية في التشريع السوري، بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٧، العدد الأول، دمشق، ٢٠١١.

▪ د. أمجد الجهني، الاستخدامات غير المشروعة لبطاقات الدفع الإلكترونية من قبل الغير، بحث منشور من قبل المركز القضائي التخصصي، الأردن، متاح على الرابط: www.cojss.com/article.php?a=219

تاريخ الزيارة ٢٠١٩/٥/٢٢ الساعة ٤,٣٠ p.m.

▪ د. أمجد الجهني، جرائم بطاقات الدفع الإلكترونية عبر شبكة الإنترنت، بحث منشور لدى مركز الدراسات القضائي التخصصي، الأردن. متاح على الرابط: <http://www.cojss.com/article.php?a=219>

تاريخ الزيارة ٢٠١٨/٤/١٢ الساعة ١٠,٣٠ p.m.

▪ تريز منصور، بطاقات الدفع الإلكترونية، الاحتراز دائماً واجب، بحث منشور في مجلة الجيش اللبناني، العدد ٣٣٢، ٢٠١٣. متاح على الرابط: www.Lebarmy.gov.lb/ar/news/?34398

تاريخ الزيارة ٢٠١٩/٩/١٢ - الساعة ١١.١٥ A.M.

▪ د. ثناء المغربي، الوجهة القانونية لبطاقات الائتمان، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة

والقانون، المجلد الثالث، جامعة الإمارات العربية المتحدة،
دبي، ٢٠٠٣،

■ جوشوا بارون، أنجيلا أوماهوني، دايفيد مانهايم ، وسينثيا ديون-شفارتس، تداعيات العملة الافتراضية على الأمن القومي ،بحث منشور من قبل مؤسسة RAND،الولايات المتحدة الأمريكية،٢٠١٥، متاح على الرابط:

<http://www.rand.org/nsrd/ndri/centers/isdp.html>

تاريخ الزيارة ٢٠/١/٢٠٢٠ الساعة ١٢,٣٠ a.m

■ د. حسام العبد، غسيل الأموال في الألفية الثالثة، بحث منشور في مجلة البنوك، المجلد ١٩، العدد ٩، الاردن، ٢٠٠٢.

■ د. حسن علي عثمان، هنا...المحكمة الإلكترونية، مقال منشور على موقع جريدة الأهرام، و متاح على الرابط:
www.ahram.org.eg

تاريخ الزيارة ١٣/١/٢٠١٩ الساعة ١٠,٣٠ A,m

■ د. خالد ممدوح إبراهيم، التقاضي الإلكتروني، الدعوى الإلكترونية وإجراءاتها أمام المحاكم، بحث منشور، و متاح على الرابط: www.Kenanonline.com

تاريخ الزيارة ١٧/٨/٢٠١٨ الساعة ٦,٤٠ p.m .

■ د. رأفت رضوان و رشا عوض و ولاء الحسيني، الضرائب في عالم الأعمال الإلكترونية، بحث منشور في مجلة التنمية

والسياسات الاقتصادية، المجلد ٢، العدد ٢، الكويت،
٢٠٠٠،

■ د. رحيم حسين وهواري معراج، الصيرفة الإلكترونية كمدخل
لعصرنة المصارف الجزائرية، مداخل في ملتقى الوطني الأول
للمنظومة المصرفية الجزائرية والتمويلات الاقتصادية ١٤ - ١٥
ديسمبر ٢٠٠٤، بحث منشور في مجلة المحاسب المجاز، كلية
العلوم الإنسانية والعلوم الاجتماعية، جامعة الشلف، الجزائر،
متاح على الرابط: www.ratoul.viola.net/resumcoll.htm.
تاريخ الزيارة ١٧/١٠/٢٠١٨ - الساعة ١.٣٠ A.M.

■ د. رمضان صديق محمد، مشكلات الضريبة على دخل
التجارة الإلكترونية والحلول الممكنة، بحث منشور في
مجلة الحقوق، العدد الثالث، السنة السادسة والعشرون
، الكويت، ٢٠٠٣.

■ د. صفاء أوتاني، المحاكم الإلكترونية (المفهوم التطبيق)،
بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية و
القانونية، المجلد ٨، العدد الأول، دمشق، ٢٠١٢.

■ د. طارق كميل، حماية المستهلك في التعاقد عبر شبكة
الإنترنت، بحث منشور في مجلة الجامعة العربية الأمريكية
للبحوث، المجلد الأول، العدد الأول، الجزائر، ٢٠١٤.

■ د. عبد الباسط أبو الوفا، سوق النقود الإلكترونية (الفرص -
المخاطر - الآفاق) ، بحث منشور في مجلة مصر
المعاصرة ، العدد ٤٧١-٤٧٢، مصر، ٢٠٠٣.

- د. عبد الجبار الحنيص، الاستخدام غير المشروع لبطاقة الائتمان الممغنطة من وجهة نظر القانون الجزائي، بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٦/، العدد الأول، دمشق، ٢٠١٠.
- د. عصام الدين القصبي، تنازع الاختصاص القضائي والقانوني الدوليين في مجال التجارة الإلكترونية، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد ٤، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣.
- د. علي عزوز، جباية المعاملات الإلكترونية (المشاكل والحلول)، بحث منشور في مجلة الردة لاقتصاديات الأعمال، العدد الأول، جامعة الشلف، الجزائر، ٢٠١٥.
- د. علي عبد القادر قهوجي، الجرائم المتعلقة باستخدام البطاقة الممغنطة، ورقة عمل مقدمة لمؤتمر الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، المجلد الثالث، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٣.
- د. لطيف زيود، تحديات التجارة الإلكترونية للنظم الضريبية، بحث منشور في مجلة جامعة تشرين للدراسات والبحوث العلمية، المجلد ٢٧، العدد ٣، اللاذقية، ٢٠٠٩.

- مادة معلوماتية حول الأعمال الإلكترونية وأمن المعلومات، المركز الوطني للمعلومات، اليمن، ٢٠٠٥، ومتاح على الرابط: www.arablaw.org تاريخ الزيارة ٢٠١٨/٧/٢٠ الساعة ١٥، ١٦.P.M.

- د. محمد شريف توفيق و د. نعيم حنا ،أساليب تنفيذ عمليات التجارة الإلكترونية والتحاسب الضريبي عنها ،بحث منشور، ومتاح على الرابط: www.kenanaonline.com تاريخ الزيارة ٢٠١٨/١٠/١٨ الساعة ١٥، ١٠ a.m.

- د. محمد علي سالم ود. عباس رزوقي، الأساس القانوني لحماية بطاقة الائتمان من التزوير، بحث منشور في مجلة المحقق للعلوم القانونية والسياسية، المجلد الأول، العدد الثاني، الجزائر، ٢٠١٥.

- د. محمد سامي الشوا، الجرائم المعلوماتية للتعدي على الذمة المالية للغير، بحث مقدم لدى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣.

- د. محمد نجم، المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الائتمان، بحث مقدم إلى مؤتمر الأعمال

المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث،
جامعة الإمارات العربية المتحدة، دبي، ٢٠٠٣.

■ محمد يوسف، الشيك الإلكتروني (تداوله-حجيته)، بحث
منشور في مجلة جامعة البعث، المجلد ٣٨، العدد ٢٠،
حمص، ٢٠١٦،

■ د. محمود طه، المسؤولية الجنائية عن الاستخدام غير
المشروع لبطاقة الائتمان، بحث مقدم لمؤتمر الأعمال
المصرفية بين الشريعة والقانون، المجلد الثالث، جامعة
الإمارات العربية المتحدة، دبي، ٢٠٠٣.

■ د. ممدوح العنزي، الحماية الجنائية لبطاقات الدفع الإلكتروني
من التزوير، بحث منشور في المجلة العربية للدراسات
الأمنية والتدريب، المجلد ٣١/، العدد ٦٢/، السعودية،
٢٠١٥.

■ د. منظور أحمد حاجي الأزهرى، بطاقة السحب النقدي، بحث
مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة
والقانون، المجلد الأول، جامعة الإمارات العربية المتحدة، دبي،
٢٠٠٣.

■ د. نهى الجلا، المحكمة الإلكترونية (٢)، بحث مقدم إلى مجلة
المعلوماتية، السنة الخامسة، العدد (١٤٧)، دمشق، ٢٠١٠.

■ نهى الموسوي وإسراء الشمري، النظام القانوني للنقود
الإلكترونية، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية،
العراق، المجلد ٢٢، العدد الثاني، ٢٠١٤.

٣- الرسائل العلمية:

أ- رسائل الدكتوراه:

- د. بسام الزلمي ، غسيل الأموال والسرية المصرفية، رسالة دكتوراه، كلية الحقوق، جامعة دمشق، ٢٠١٠.
- د. حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ٢٠١٤ - ٢٠١٥.
- د. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠٠٥.
- د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠٠٧.

ب- رسائل الماجستير:

- إيناس بن غيده، الحماية المدنية للمستهلك في العقود الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد - تلمسان، الجزائر، ٢٠١٤-٢٠١٥.

- بشرى سلامة، المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الوفاء، رسالة ماجستير، كلية الحقوق، جامعة دمشق، ٢٠١٠ - ٢٠١١.
- خديجة سلطاني، إحلال وسائل الدفع التقليدية بالوسائل الإلكترونية - دراسة حالة بنك الفلاحة والتنمية الريفية BADR- بوكالة بسكرة، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيصره- بسكرة، الجزائر، ٢٠١٢ - ٢٠١٣.
- رائد يوسف، النظام القانوني للدفع الإلكتروني، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري تيزي، الجزائر، ٢٠١١.
- رشيد علام، عوائق تطور التجارة الإلكترونية في الوطن العربي/دراسة حالة الجزائر/، رسالة ماجستير، الأكاديمية العربية البريطانية للتعليم العالي، قسم إدارة الأعمال، بريطانيا، ٢٠٠٩ - ٢٠١٠.
- سليمة مغني، وسائل الدفع الإلكترونية وانعكاساتها على الوطن العربي والجزائر خاصة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة خميس مليانة، الجزائر، ٢٠١٣-٢٠١٤.
- سهام إمدالو و ليلي الحسن، حماية المستهلك الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميره -بجاية، الجزائر، ٢٠١٢-٢٠١٣.

- شيروف فضيلة، أثر التسويق الإلكتروني على جودة الخدمات المصرفية، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، الجزائر، ٢٠١٠.
- عبد الله محمود، حماية المستهلك في التعاقد الإلكتروني، رسالة ماجستير، كلية الحقوق، جامعة النجاح الوطنية، فلسطين، ٢٠٠٩.
- عماد الدين عبد الحليم، المعاملات المصرفية بواسطة الهواتف النقالة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط للدراسات العليا، الأردن، ٢٠١٠،
- عمار لوصيف، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين مع الإشارة إلى التجربة الجزائرية، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، الجزائر، ٢٠٠٨ - ٢٠٠٩.
- فراس بلحة، محفظة النقود الإلكترونية، رسالة ماجستير، منشورات كلية الحقوق، جامعة دمشق، دمشق، ٢٠١٥.
- فطيمة ميهوبي، جرائم بطاقات الدفع الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيصره- بسكرة، الجزائر، ٢٠١٥ - ٢٠١٦.

- فلاح العجمي، الحماية المدنية للمستهلك في العقد الإلكتروني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط للدراسات العليا، الأردن، ٢٠١١.
- محمد الباوخ، مخاطر العمليات المصرفية والتأمين عليها، رسالة ماجستير، كلية الحقوق، جامعة دمشق، ٢٠١٦.
- محمد ذوابة، عقد التحويل المصرفي الإلكتروني، رسالة ماجستير، منشورات دار الثقافة للتوزيع ، مصر، ٢٠٠٨.
- محمد عبد الله ، الاتجاهات الحديثة لأعمال المصارف (الصيرفة الإلكترونية) رسالة ماجستير ، كلية الاقتصاد، جامعة دمشق، دمشق ٢٠١١.
- مناع سعد العجمي، حدود التزام البنك بالسرية المصرفية والآثار القانونية المترتبة عن الكشف عنها، رسالة ماجستير، كلية الحقوق، منشورات جامعة الشرق الأوسط للدراسات العليا، عمان، الأردن، ٢٠١٠.
- ناهد الهندي، النظام القانوني للنقود الإلكترونية، رسالة ماجستير ،كلية الحقوق، منشورات جامعة دمشق ، دمشق ، ٢٠١١.
- نورا الجزراوي، أثر استعمال النقود الإلكترونية على العمليات المصرفية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط للدراسات العليا، الاردن، ٢٠١١.

- يحيى حسن، التنظيم القانوني للعقود الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة النجاح الوطنية، فلسطين، ٢٠٠٧.

٤-القوانين:

أ-القوانين السورية:

- القانون المدني رقم /٨٤/ لعام ١٩٤٩.
- الدستور السوري الصادر في ٢٧ شباط لعام ٢٠١٢.
- قانون الإعلام الصادر بالمرسوم التشريعي رقم /١٠٨/ لعام ٢٠١١.
- قانون النقد الأساسي رقم /٢٣/ لعام ٢٠٠١.
- القانون رقم /٢٨/ لعام ٢٠٠١ الخاص بتأسيس المصارف الخاصة.
- قانون العقوبات رقم /١٨٤/ لعام ١٩٤٩.
- المرسوم التشريعي رقم /٣٣/ لعام /٢٠٠٥/ المتعلق بمكافحة غسل الأموال و تمويل الإرهاب والمعدل بموجب المرسوم التشريعي رقم /٢٧/ لعام ٢٠١١ والمرسوم التشريعي رقم /٤٦/ لعام ٢٠١٣.
- قانون التجارة رقم /٣٣/ لعام ٢٠٠٧.
- قانون التوقيع الإلكتروني رقم /٤/ لعام ٢٠٠٩.
- قانون السرية المصرفية رقم /٣/ لعام ٢٠١٠.

- قانون الشركات رقم/٢٩/لعام ٢٠١١.
- القانون رقم /١٣/ لعام ٢٠١٢ المتعلق بإحداث الشركة السورية للمدفوعات الإلكترونية.
- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم /١٧/ لعام ٢٠١٢.
- قانون المعاملات الإلكترونية رقم /٣/ لعام ٢٠١٤.
- القانون رقم /٢١/ لعام ٢٠١٤ الخاص بإحداث محاكم مصرفية.
- قانون التجارة الداخلية وحماية المستهلك رقم /١٤/ لعام ٢٠١٥.
- القانون رقم /٢٨/ لعام ٢٠٠١ الخاص بتأسيس المصارف الخاصة.
- قانون أصول المحاكمات رقم /١/ لعام ٢٠١٦.
- القانون رقم /٩/ لعام ٢٠١٨ الخاص بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات.

ب-القوانين العربية:

- قانون سرية المصارف اللبناني رقم / ٦ / لعام ١٩٥٦.
- قانون سرية الحسابات بالبنوك المصري رقم /٢٠٥/ لعام

- قانون التوقيع الإلكتروني المصري رقم /١٥/ لعام /٢٠٠٤/.
- قانون حماية المستهلك المصري رقم /١٨١/ لعام ٢٠١٨.
- قانون الممارسات التجارية الجزائي رقم /٠٢-٠٤/ لعام ٢٠٠٤.

ج-القوانين الأجنبية:

- القانون الفرنسي الخاص بالجرائم المعلوماتية رقم /١٩-٨٨/ تاريخ ٥/يناير/ ١٩٨٨ والمعدل بموجب قانون العقوبات الفرنسي بتاريخ ١/مارس/١٩٩٤.
- قانون توبون الفرنسي (LOI TOUBON) رقم /٩٤-٦٦٥/ تاريخ ١٩٩٤/٨/٤
- قانون الاستهلاك الفرنسي المعدل بتاريخ ٣٠ يناير ٢٠٢٠.

د-الاتفاقيات والقرارات:

- اتفاقية الأمم المتحدة للنقل البحري والبضائع الموقعة في هامبورغ في ٣١ مارس ١٩٧٨ والتي تُسمى قواعد هامبورغ ودخلت حيز التنفيذ في /١/ نوفمبر ١٩٩٢.
- التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادرة بالقرار رقم /٢٩٠/ لعام /٢٠١٢/.

- اللائحة التنظيمية للضوابط والنواظم الخاصة بحماية المستهلك الإلكتروني والتسويق الإلكتروني الصادرة بالقرار رقم /٤٧٩/ تاريخ ٢٠١٩/٢/١٧.
- القرار رقم /٥٢/ تاريخ ٢٠١٩/٨/٢ الصادر عن مصرف سورية المركزي المتضمن شروط الترخيص لتأسيس شركات تعمل في مجال الدفع الإلكتروني.
- التعليمات التنفيذية للقانون رقم /٢٨/ لعام ٢٠٠١ الصادرة بالقرار رقم /٢٠٦٠/ تاريخ ٢٠١١/٩/٢٦.

ه-التوجيهات الأوربية والتوصيات:

- التوصيات الأربعين الصادرة لجنة العمل المعنية بالإجراءات المالية المتعلقة بمكافحة غسل الأموال بالوسائل الحديثة متاحة على الرابط:
www.Money_laundry_comapating.blogspot.com/2009/08/blog-post24.html
تاريخ الزيارة ٢٠١٨/١٢/٢١ الساعة ٩,٣٠ pm
- التوجيه الأوربي رقم (٨٤/٤٥٠) الصادر في ١٠/٩/١٩٨٤ الخاص بالإعلان الكاذب أو المضلل.
- التوجيه الأوربي رقم /١٣/ الصادر في ٥ نيسان ١٩٩٣ بشأن الشروط التعسفية في العقود المبرمة مع المستهلكين.
- التوجيه الأوربي رقم /٤٦/ لعام ٢٠٠٠ المتعلق بالقيام بأعمال مؤسسات النقود الإلكترونية والرقابة الحصينة على تلك المؤسسات.

٥-المواقع الإلكترونية:

- <http://www.paycash.eu/en/agb/>.
- <http://www.netcashuk.bnpparibas.com/gb/convention.htm>.
- [http://www .my pay cash .in/site static/terms condition](http://www.my pay cash .in/site static/terms condition).
- Bank of internet USA, privacy policy, January, 200 b, [www. Bank of internet.com/privacy policy.aspx](http://www.Bank of internet.com/privacy policy.aspx).
- www.tartoos.com /Home page / Rtable / computer school/internet/ internet basic 2/internet 80.htm.
- www.arablawn.com.
- <https://www.bibliofond.ru/view.aspx?id=809399>.
- [www.Treasury.gov/about/organizational-strure/pages/office of foreign assets-control-as px](http://www.Treasury.gov/about/organizational-strure/pages/office of foreign assets-control.aspx).
- www.Ar.wikipedia.org/wiki/.
- www.thestc.com
- www.moqatel.com/openshare/Behoth/Ektesad8/GhaslAm wal/secl7/doic.cvt.htm.
- www.damasnow.com

ثانياً: باللغة الانكليزية

1-Books:

- Apostolos Ath, Gkoutzinis, Internet Banking And The Law In Europe, Cambridge University Press, First Published, 2006.
- Dave Chaffey, E. business and E. commerce Management, strategy, implementation and practice, third Edition, prentice Hall, New jersey, U.S. 2006.
- Ross Cranston. Principles of banking law. Second Edition. Oxford University Press. 2003.

2-article

- Marvin Kirsner, Taxation Of Electronic Commerce's, Internet Tax Advisor , Vol 1 , Issue12, USA.

3-Reports

- Electronic monetary institute working Group on Eui Emi 1994.Available at:

[http\\www.int \pub\ pdf\ annrep\ ar 1994 : en.pdf](http://www.int \pub\ pdf\ annrep\ ar 1994 : en.pdf)

تاريخ الزيارة ٢٠١٨/١٠/٨ الساعة ٨,١٥ p.m.

- Gerson & Ryan A Primer on Internet Exchange Points for Policymakers and Non-Engineers Working Paper, 11 August 2012. Available at:

www.Ar.wikipedia.org/wiki/

تاريخ الزيارة ٢٠١٨/١٠/٣١ الساعة ١٠,٣٠ a.m

- Malte Kreuger, Offshore E- Money Issuers and Monetary policy, First Monday, December, 2005. Available at:

**http:// www, first monetary – org issuer – 10/
/kruger ? index – html.**

تاريخ الزيارة ٢٠١٨/٨/١ الساعة ١٠,٣٠ a.m

- The Electronic Payment Association, The Cross Border Payment User Guide. Available at:

**www. nacha.org/ search? opiviews Fu/text= the +
cross + Border + payment + user + Guide.**

تاريخ الزيارة ٢٠١٨/٨/١٨ الساعة ١٢,٣٠ p.m

- The Report of the Consumer Electronic Payments, Task Force, Treasury Of The United States, 1998, available at: **www.federal**

reserve.gov.

تاريخ الزيارة ٢٠١٨/٧/٢٥ الساعة ١٠,٤٠ a.m

ثالثاً: باللغة الفرنسية

1-article

- Simon Woodside, La fiscalité du commerce électronique, Une réalité virtuelle, Centre de politique et d'administration fiscales؛

Dispensable sur :

http://www.observateurocde.org/news/archivestory.php/id/391/La_fiscalite9_du_commerce_E9lectronique:_Une_r_E9alit_E9_virtuelle.html

تاريخ الزيارة ٢٠١٩/١٠/١١ الساعة ١٠,٣٠ a.m.

- William Fox , E-Commerce In The Context Of Declining Sale+ Tax Bales, National Tax Journal ،

Dispensable sur :

www.cber.bus.utk.edu/e-comm.pdf

تاريخ الزيارة ٢٠١٩/١٠/٨ الساعة ١١,٣٠ a.m.

2-RAPPORTS:

- Groupe Des Dix – Monnaies Electroniques; la protection des consommateurs. Application de la loi de surveillance et question en Transfrontalière, Rapport du Groupe de travail sur la monnaie électronique, 1997.Disponible sur;

www.bis.org,

تاريخ الزيارة ٢٠١٨/٨/١٢ الساعة ٢,٣٠ p.m.

2-Les Juris Prudence's:

- Guillaume Hublot :*Le dispositif FATCA applicable en France*, Droit et Patrimoine, N° 231, 1er Décembre 2013.
- Annabelle Pando:*Comptes PayPal : les précisions de Bercy*, Lamiline Droit et Patrimoine, N° 231, 1er Décembre 2013.
- Frédérique Perrotin: *Fraudefiscale : les exigences de la Cour des comptes* Droit et Patrimoine, N° 232, 15er Décembre 2013.
- Tribunal, 7ème Chambre, Arrêt du 30 juin 2016, Affaire n° T-491/07 RENV.
- Cour d' appel de Nouméa, Chambre commerciale, Arrêt du 7 juin 2018, Répertoire général n° 16/00093.
- Cour d' appel de Douai, 2ème Chambre, Section 2, Arrêt du 14 Mars 2019, Répertoire général n° 17/00489.
- Cour d' appel d' Aix-en-provence, Arrêt du 28 mars 2019, Répertoire général n° 17/18362.
- Cour de cassation, Chambre commerciale, Arrêt n° 349 du 3 Avril 2019, Pourvoi n° 18-11.293.

رابعاً: باللغة الروسية

الاجتهادات القضائية

- القضية رقم 57-98-11 / A40-7162 تاريخ
٢٠١١/١٢/١، متاحة على الرابط:

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>

تاريخ الزيارة ٢٠١٩/٦/٩ الساعة ١١,٤٥ p.m

- القضية رقم ٢-٢٠١٢/٩٢٥ تاريخ ٢٠١٢/٢/٥، متاحة على
الرابط :

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>

تاريخ الزيارة ٢٠١٩/٥/٢٢ الساعة ١٠,١٥ a.m

- القضية رقم A53-19532 تاريخ ٢٠١٢/١٠/٤ ومتاحة
على الرابط:

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>

تاريخ الزيارة ٢٠١٩/٦/١٧ الساعة ٤,١٠ a.m

- القضية رقم ٢-٢٠١٥/٩٣٦ تاريخ ٢٠١٥/٦/٨، متاحة على
الرابط: _____

<https://sudact.ru/regular/doc/6lRf3y3dKTmO>

تاريخ الزيارة ٢٠١٩/٥/٢٢ الساعة ١١,٣٠ a.m

■ القضية رقم ٢-٢٨٧٧/٢٠١٥ تاريخ ١٨/٩/٢٠١٥، متاحة

على الرابط: <https://moluch.ru/archive/184/47356>

تاريخ الزيارة ٢٩/٥/٢٠١٩ الساعة ١٠,٣٠ p.m

■ القضية رقم (٨٢-٥٠.N١/c٧٩) تاريخ ٢٥/٧/٢٠١٩

، متاحة على الرابط:

<https://moluch.ru/archive/184/47356>

تاريخ الزيارة: ٣١/٥/٢٠١٩ الساعة ٩,١٢ p.m

الفهرس

صفحة	الموضوع
١	المقدمة
١١	الباب الأول: الإطار الموضوعي للمشكلات القانونية للدفع الإلكتروني
١٣	الفصل الأول: التعريف بالمشكلات القانونية للدفع الإلكتروني
١٥	المبحث الأول: المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية
١٥	المطلب الأول: المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف
١٦	الفرع الأول: التعريف بالالتزام بالسرية المصرفية
١٨	أولاً: النطاق الشخصي للالتزام بالسرية المصرفية.
٢٢	ثانياً: النطاق الموضوعي للالتزام بالسرية المصرفية
٢٩	الفرع الثاني: الأثر السلبي لتقنية المعلومات على الحياة الخاصة للأفراد
٣٠	أولاً: العوامل المتحركة بمسألة الخصوصية
٣٣	ثانياً: المعالم الرئيسية لمخاطر الحواسيب على الحياة الخاصة للأفراد
٤٠	المطلب الثاني: المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً
٤٠	الفرع الأول: مشكلات الشراء عبر الحدود
٤١	أولاً: مشكلة الدفع في أكثر من دولة
٤٤	ثانياً: مشكلة القانون الواجب التطبيق والمحكمة المختصة
٤٩	ثالثاً: المشكلات المرافقة لانتشار النقود الإلكترونية
٦٧	الفرع الثاني: المشكلات التي تواجه المستهلك الإلكتروني كمتعاقد
٦٨	أولاً: المشكلات التقنية
٧١	ثانياً: المشكلات القانونية

٩١	المبحث الثاني: المشكلات التي تواجه الاقتصاد الوطني
٩٢	المطلب الأول: مشكلة التهرب الضريبي باستخدام وسائل الدفع الإلكتروني
٩٣	الفرع الأول: مدى خضوع معاملات الدفع الإلكتروني للضريبة
٩٣	أولاً: الاتجاه المعارض لفرض الضريبة على هذه المعاملات
٩٧	ثانياً: الاتجاه المؤيد لفرض الضريبة على هذه المعاملات
١٠٢	الفرع الثاني: التحديات التي تواجه فرض الضريبة على معاملات الدفع الإلكتروني
١٠٢	أولاً : تحديات قانونية
١٠٧	ثانياً: تحديات تقنية
١١٢	المطلب الثاني: مشكلة غسيل الأموال باستخدام وسائل الدفع الإلكتروني
١١٥	الفرع الأول: الأساليب الحديثة في ارتكاب غسيل الأموال
١١٥	أولاً: غسيل الأموال بواسطة النقود الإلكترونية والبطاقات المصرفية
١٢٠	ثانياً: غسيل الأموال بواسطة بعض الأساليب المصرفية الأخرى
١٢٤	الفرع الثاني: مراحل غسيل الأموال وآثارها السلبية
١٢٤	أولاً: مراحل غسيل الأموال
١٢٧	ثانياً: الآثار السلبية لغسيل الأموال
١٢٩	الفصل الثاني: سبل معالجة المشكلات القانونية
١٣١	المبحث الأول: أساليب معالجة المشكلات التي تواجه مستخدم أداة الدفع الإلكترونية
١٣٢	المطلب الأول: وسائل معالجة المشكلات التي تواجه المستخدم باعتباره عميلاً للمصرف
١٣٢	الفرع الأول: الحماية القانونية للمعلومات الخاصة بالعملاء لدى المشرع الأمريكي
١٣٣	أولاً: قانون الحق بالخصوصية المالية
١٣٣	ثانياً: القانون الخاص بالتحويل الإلكتروني للأموال
١٣٣	ثالثاً: القانون الخاص بتقديم التقارير الائتمانية
١٣٤	رابعاً: قانون الخصوصية

١٣٦	الفرع الثاني: الحماية القانونية للمعلومات الخاصة بالأفراد لدى المشرع السوري
١٣٧	أولاً: المسؤولية الجزائية
١٤٦	ثانياً: المسؤولية المدنية
١٥٤	المطلب الثاني: وسائل معالجة المشكلات التي تواجه المستخدم باعتباره مستهلكاً إلكترونياً
١٥٥	الفرع الأول: معالجة مشكلات الشراء عبر الحدود
١٥٥	أولاً: التدابير الوقائية
١٦١	ثانياً: التدابير العلاجية
١٨٧	الفرع الثاني: معالجة المشكلات المتعلقة بالمستهلك الإلكتروني
١٨٨	أولاً: الحماية المقررة للمستهلك الإلكتروني بموجب القوانين واللوائح النازمة للمعاملات الإلكترونية.
٢١١	ثانياً: الحماية المقررة بموجب القوانين النازمة للمعاملات التقليدية.
٢٢٩	المبحث الثاني: أساليب معالجة المشكلات التي تواجه الاقتصاد الوطني
٢٣٠	المطلب الأول: وسائل معالجة مشكلة التهرب الضريبي باستخدام وسائل الدفع الإلكتروني
٢٣١	الفرع الأول: معالجة المشكلة المتعلقة بكيفية فرض الضريبة
٢٣١	أولاً: فرض ضريبة على الاستهلاك.
٢٣٢	ثانياً: تطبيق ضريبة البيت (Bit –tax).
٢٣٤	ثالثاً: الإطار العام المقترح لكيفية فرض الضريبة على تعاملات التجارة الإلكترونية
٢٣٨	الفرع الثاني: معالجة المشكلة المتعلق بكيفية تحصيل الضريبة
٢٣٨	أولاً: التحصيل عن طريق أطراف ثالثة.
٢٤٠	ثانياً: التحصيل باستخدام أساليب تقنية.
٢٤٢	المطلب الثاني: وسائل معالجة مشكلة غسيل الأموال باستخدام وسائل الدفع الإلكتروني
٢٤٢	الفرع الأول: مكافحة غسيل الأموال على المستوى الدولي
٢٤٣	أولاً: المعايير المعتمدة لمكافحة غسيل الأموال
٢٤٤	ثانياً: التوصيات الصادرة بخصوص مكافحة غسيل الأموال

٢٤٩	الفرع الثاني: مكافحة غسيل الأموال لدى المشرع السوري
٢٥٠	أولاً: التدابير الوقائية
٢٥٤	ثانياً: التدابير العلاجية
٢٦١	الباب الثاني: الإطار الموضوعي للمشكلات الأمنية
٢٦٥	الفصل الأول: التعريف بالمشكلات الأمنية
٢٦٧	المبحث الأول: المشكلات التي تمس أداة الدفع الإلكترونية
٢٦٧	المطلب الأول: تعطل أداة الدفع وفقدانها
٢٦٨	الفرع الأول: تعطل أداة الدفع الإلكترونية
٢٦٨	أولاً : التعطل نتيجة لعباب في الأداة.
٢٧١	ثانياً: التعطل نتيجة لتقصير في الصيانة
٢٧٣	الفرع الثاني: فقدان أداة الدفع الإلكترونية
٢٧٣	أولاً: فقدان أداة الدفع بتدخل الغير (سرقة أداة الدفع)
٢٨٤	ثانياً: فقدان أداة الدفع دون تدخل الغير
٢٨٧	المطلب الثاني: القرصنة الإلكترونية
٢٨٨	الفرع الأول: تزوير وسائل الدفع الإلكتروني
٢٨٨	أولاً: تعريف التزوير المعلوماتي
٢٩٢	ثانياً: أشكال التزوير لوسائل الدفع الإلكتروني
٣٠٦	الفرع الثاني: الجرائم الإلكترونية
٣٠٦	أولاً: تعريف الجرائم الإلكترونية
٣١٠	ثانياً: أنواع الجرائم الإلكترونية.
٣١٩	المبحث الثاني: المشكلات الناشئة عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية
٣٢١	المطلب الأول: الاستخدام غير المشروع من قبل أطراف البطاقة
٣٢٢	الفرع الأول: الاستخدام غير المشروع من قبل الحامل

٣٢٢	أولاً: الاستخدام غير المشروع للبطاقة خلال فترة صلاحيتها.
٣٢٦	ثانياً: الاستخدام غير المشروع للبطاقة خارج فترة صلاحيتها.
٣٣١	ثالثاً: الاستخدام المقنع لبطاقة الدفع
٣٣٩	الفرع الثاني: الاستخدام غير المشروع من قبل التاجر
٣٤٠	أولاً : الاستخدام غير المشروع بواسطة الجهاز اليدوي
٣٤٣	ثانياً: الاستخدام غير المشروع بواسطة الجهاز الإلكتروني.
٣٤٧	ثالثاً: الأخطاء الفنية التي ترافق استخدام بطاقة الدفع الإلكترونية
٣٥٣	الفرع الثالث: الاستخدام غير المشروع من قبل موظفي المصدر
٣٥٣	أولاً: تواطؤ موظف المصدر مع حامل البطاقة
٣٥٤	ثانياً: تواطؤ موظف المصدر مع التاجر
٣٥٤	ثالثاً: تواطؤ الموظف مع الغير
٣٥٨	المطلب الثاني: الاستخدام غير المشروع من قبل الغير
٣٥٩	الفرع الأول: الاستخدام غير المشروع في التعاملات العادية
٣٦١	الفرع الثاني: الاستخدام غير المشروع عبر أجهزة الصراف الآلي
٣٦١	أولاً: كتابة الرقم السري على البطاقة
٣٦١	ثانياً: إعطاء الرقم السري للغير
٣٦٢	ثالثاً: ربط جهاز قراءة آخر على جهاز الصراف
٣٦٢	رابعاً: وضع واجهة جهاز صراف مزور
٣٦٣	خامساً: الحلقة اللبنانية
٣٦٤	الفرع الثالث: الاستخدام غير المشروع عبر شبكة الإنترنت
٣٦٤	أولاً: الاختراق غير المشروع لمنظومة الاتصالات العالمية
٣٦٥	ثانياً: أسلوب التجسس
٣٦٦	ثالثاً: تقنية تفجير الموقع المستهدف

٣٦٦	رابعاً: تخليق أرقام البطاقات
٣٦٧	خامساً: تبادل المعلومات
٣٦٨	سادساً: أسلوب الخداع
٣٧٥	الفصل الثاني: سبل معالجة المشكلات الأمنية
٣٧٧	المبحث الأول: التدابير الوقائية
٣٧٧	المطلب الأول: التدابير التقنية
٣٧٨	الفرع الأول: نظام التوقيع الإلكتروني
٣٧٩	أولاً: تطبيقات التوقيع الإلكتروني على وسائل الدفع الإلكتروني
٣٨٤	ثانياً: استخدام التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني.
٣٨٨	الفرع الثاني: تأمين البيانات
٣٨٨	أولاً: برامج تأمين البيانات.
٣٩٢	ثانياً: بروتوكولات تأمين البيانات
٣٩٦	المطلب الثاني: الوسائل الإدارية
٣٩٧	الفرع الأول : الوسائل المتخذة بالنسبة للسرقة
٤٠٠	الفرع الثاني : الوسائل المتخذة بالنسبة للتزوير
٤٠٠	أولاً: كيفية اكتشاف التزييف في نطاق النقود الإلكترونية.
٤٠٢	ثانياً: حكم التعامل بالنقود المزيفة مقارنة بالنقود التقليدية.
٤٠٧	الفرع الثالث: الوسائل الإدارية المتخذة لتلافي الاستخدام غير المشروع
٤٠٧	أولاً: الوسائل الإدارية المتخذة من قبل المصدر.
٤١٣	ثانياً: الوسائل الإدارية المتخذة من قبل الحامل.
٤١٥	ثالثاً: الوسائل الإدارية المتخذة من قبل التاجر.
٤١٩	المبحث الثاني: التدابير العلاجية
٤٢٠	المطلب الأول: المسؤولية الجزائية بالنسبة للمشكلات التي تمس أداة الدفع الإلكترونية

٤٢١	الفرع الأول: مكافحة السرقة
٤٢١	أولاً: سرقة بطاقة الدفع الإلكترونية
٤٢٣	ثانياً: فقدان بطاقة الدفع الإلكترونية
٤٢٥	ثالثاً: استعمال وسيلة دفع مسروقة أو مفقودة
٤٣٥	الفرع الثاني: مكافحة التزوير
٤٣٥	أولاً: عقوبة تزوير بطاقات الدفع الإلكترونية
٤٤٦	ثانياً: عقوبة مستعمل بطاقة دفع إلكترونية مزورة
٤٦٠	الفرع الثالث: مكافحة الجرائم الإلكترونية
٤٦٠	أولاً: مكافحة الجرائم التي ترتكب باستخدام وسيلة إلكترونية
٤٦٢	ثانياً: مكافحة الجرائم التي تمس منظومة المعلومات الإلكترونية
٤٦٨	المطلب الثاني: المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الدفع الإلكترونية
٤٦٨	الفرع الأول: المسؤولية الجزائية لأطراف عملية الدفع الإلكتروني
٤٦٩	أولاً: المسؤولية الجزائية للحامل
٤٩٦	ثانياً: المسؤولية الجزائية للتاجر والمصدر
٥٠١	الفرع الثاني: المسؤولية الجزائية للغير
٥٠٧	الخاتمة
٥١٥	المراجع القانونية
٥٤١	الفهرس