مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

حماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني دراسة مقارنة

الباحث: علي صاحب تقي[١]، أ.م.د. ضرغام محمود كاظم التّميمي[٢]

[٢،١] كلية القانون، جامعة المستنصرية، بغداد، العراق

Fgg4809@gmail.com

المستخلص

تأتي أهمية هذه الدراسة نتيجة الأهمية المتزايدة لاستخدام وسائل الدفع الإلكتروني في العراق وفي العالم، ويرجع ذلك الى التحول الرقمي الكبير والمتسارع الذي شهدته المعاملات المالية والتجارية، إذ بات اعتماد المستفيد بشكل كبير على الأنظمة الإلكترونية في إنجاز تعاملاته، إلا أن هذا التطور التقني قد رافقه العديد من المخاطرة المتزايدة التي تهدد حماية المستفيد وحقوقه، وذلك في ظل تنامي جرائم الاحتيال الإلكتروني، كالاحتيال المالي ، وانتحال هوية المستفيد، واختراق البيانات الشخصية، وجاء ذلك تزامناً مع ضعف الاطار القانوني الناظم في العديد من الدول

وكشفت الدراسة من خلال منهجها المقارن أن العديد من الدول المتقدمة، كفرنسا والامارات المتحدة قد وضعت أطراً قانونية متطورة تكفل حماية المستفيد، وتضمن استقرار المعاملات الإلكترونية، في حين مازالت بعض التشريعات العربية، ومن بينها التشريع العراقي والمصري، بحاجة الى التطور التشريعي لمواكبة التطورات التقنية السريعة.

الكلمات المفتاحية:

حماية، المستفيد، المخاطر، وسائل، الدفع الالكتروني

The Protection of Beneficiaries Against Risks Arising from Electronic Payment Systems

Researcher: Ali Sahib Taqi, Asst. Prof. Dr. Dhurgham Mahmoud Kazem Al-Tamimi

College of Law, Al-Mustansiriya University, Baghdad, Iraq

Abstract:

This section examines and analyzes the topic of protecting beneficiaries within the framework of electronic payment services, as one of the most prominent issues arising from the nature of modern transactions and the risks they entail—such as cybersecurity threats, data misuse, electronic fraud, and other legal and technical challenges. The section is divided into two main parts:

The first part reviews the types of risks that may affect beneficiaries as a result of using electronic payment methods, while the second part discusses the protection mechanisms established to address these risks, whether through legal safeguards or the technical and regulatory measures imposed by relevant legislation..

Keywords:

Protection, beneficiary, risks, electronic payment methods

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

المقدمة:

شهد العالم في السنوات الأخيرة تقدماً سريعًا في مجال التكنولوجيا المالية والرقمية، كان من أبرز هذه التطورات الانتقال من وسائل الدفع التقليدية إلى أنظمة الدفع الإلكتروني، التي أصبحت جزءًا أساسيًا من الاقتصاد العالمي. هذه الأنظمة قدمت فوائد عديدة، مثل زيادة سرعة المعاملات، وتقليل التكاليف، وتسهيل حركة الأموال عبر الحدود، مما ساهم في تعزيز مكانة الاقتصاد الرقمي كعامل رئيسي في النمو. ومع ذلك، لم يكن هذا التقدم خاليًا من التحديات القانونية والمخاطر المرتبطة بالبيئة الإلكترونية، مثل ضعف البنية التحتية التقنية، والمشاكل الناتجة عن الاحتيال الإلكتروني، واختراق البيانات، وانتهاك خصوصية المستخدمين.

ومن هنا تبرز إشكالية حماية المستفيد من المخاطر الناشئة عن أنظمة الدفع الإلكتروني، إذ يُعد المستفيد الحلقة الأضعف في هذه العلاقة التعاقدية المعقدة التي تجمع بين مزوّد الخدمة والمستهلك. فمع تزايد حجم المعاملات الإلكترونية، ظهرت الحاجة الملحة إلى إيجاد قواعد قانونية رصينة وآليات رقابية فعالة تضمن توازناً بين تشجيع الابتكار المالي من جهة، وتوفير مظلة حماية قانونية للمستفيد من جهة أخرى.. وعليه فإن هذه الدراسة تسعى إلى تحليل الإطار القانوني لحماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني، عبر مقارنة التجارب التشريعية في العراق ومصر وفرنسا والإمارات، بهدف الوقوف على أوجه القصور والتميّز، واستخلاص الدروس الكفيلة بتعزيز فعالية النظام القانوني العراقي في هذا المجال.

أولًا: أهمية الموضوع:

تبرز أهمية هذا الموضوع في كونه يختص بأحد أبرز مظاهر الحياة الاقتصادية المعاصرة، ويُسلط الضوء على حقوق المستفيد باعتباره الطرف الأضعف في العلاقة التعاقدية الرقمية، في ظل تفاوت الخبرات الفنية وغياب الإحاطة القانونية الكافية لدى أغلب المستخدمين. وتتضاعف أهمية هذه الدراسة، مع انتشار حالات الاحتيال الإلكتروني واختراق البيانات الشخصية، مما يثير تساؤلات جوهرية عن مدى كفاية الحماية القانونية الحالية.

ثانيًا: هدف الدراسة:

يهدف هذا البحث إلى دراسة المخاطر الناشئة عن استخدام وسائل الدفع الإلكتروني وآليات حماية المستفيد من تلك المخاطر، مع تحليل الإطار القانوني المتعلق بهذه الوسائل بما يتناسب مع طبيعة التهديدات والتحديات العملية التي تواجه المستفيد. كما يسعى البحث إلى تقديم توصيات قانونية وعملية تعزز حماية حقوق المستفيد وتحقق توازنًا بين متطلبات التحول الرقمي وضرورة الحفاظ على سلامة المعاملات المالية الإلكترونية.

ثالثًا: مشكلة الدراسة:

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

تنصبّ إشكالية الدراسة على مدى قدرة القوانين والتنظيمات الحالية على تحقيق حماية فعّالة للمستفيد، وما هي أبرز المخاطر الناشئة عن استخدام وسائل الدفع الإلكتروني؟

ما مدى كفاية الأطر القانونية والتنظيمية المعمول بها؟

رابعاً: المنهجية :

اتّبعنا البحث المنهج التحليلي المقارن، وذلك لاستكشاف الفروقات والتشابهات في معالجة التشريعات محل الدراسة، وذلك من خلال دراسة عدد من النظم القانونية، وتحليل النصوص والتشريعات ذات الصلة، بهدف التوصل إلى نتائج علمية تسهم في تطوير المنظومة القانونية للدفع الإلكتروني، وتكفل حماية للمستفيد.

خامساً: هيكل الدراسة:

يعالج هذا المبحث مسألة "حماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني، من خلال مطلبين رئيسيين:

المطلب الأول: المخاطر الامنية والقانونية لوسائل الدفع الإلكتروني.

أما المطلب الثاني: سبل الحماية القانونية في وسائل الدفع الإلكتروني.

المطلب الأول: المخاطر الأمنية والقانونية لوسائل الدفع الالكتروني

أدى التطور التكنولوجي المتسارع إلى إحداث نقلة نوعية في مجال المعاملات المالية، إذ أصبحت وسائل الدفع الإلكتروني تمثل بديلاً أساسياً للوسائل التقليدية، لما توفره من سرعة وفعالية في إنجاز الصفقات التجارية وتيسير التداولات المالية عبر الحدود، غير أن هذا التحول الرقمي، على الرغم مما يحمله من مزايا متعددة، قد أفرز جملة من التحديات التي تتمثل في المخاطر الأمنية والقانونية المصاحبة له، فمن الناحية الأمنية، تشكل الهجمات السيبرانية، والتزوير، والاحتيال أبرز التهديدات التي تستهدف سلامة المعاملات وخصوصية البيانات، في حين تثير من الناحية القانونية إشكاليات متعلقة بضعف التشريعات الموحدة، وصعوبة إثبات الجرائم الإلكترونية، وتحديد المسؤولية عند وقوع الضرر. وعليه، فإن دراسة هذه المخاطر تكتسب أهمية بالغة في سبيل وضع آليات فاعلة للحماية وضمان التوازن بين التطور التقني ومتطلبات الأمن القانوني، بما يعزز ثقة المستفيدين في التعامل بوسائل الدفع الإلكتروني.

الفرع الأول: المخاطر الأمنية

من صور المخاطر الأمنية لوسائل الدفع الالكتروني:

أولا: الاستغلال غير القانوني لوسائل الدفع الإلكترونية:

إن الطبيعة الخاصة لبطاقة الدفع، التي تقوم مقام الموظف المصرفي في تنفيذ العمليات البنكية من قبيل سحب الأموال وتحويل الأرصدة، قد أفرزت تحديات عملية وأمنية متعددة. فقد استغل بعض محترفي الاحتيال والتزوير هذه الخصائص للدخول إلى هذا المجال واستخدام البطاقة بصورة غير مشروعة،

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

سواء في مواجهة التجار أو المؤسسات المصرفية. كما أن البطاقة قد تتيح في بعض الحالات للعميل الشرعي نفسه إمكانية اللجوء إلى وسائل احتيالية بهدف تحقيق منافع غير مستحقة. وتتجلى أبرز صور هذا الاستغلال غير المشروع في المظاهر الآتية:

١_ الحصول على بطاقة الدفع بمستندات مزورة

يُعتبر الحصول على بطاقة الائتمان عملية تخضع للقوانين والسياسات المحددة من قبل البنك المصدر ، وتتطلب تقديم المستندات اللازمة التي يجب أن تكون سليمة وصحيحة وغير مخالفة للواقع. يُمنع تماماً تقديم بيانات مُزيفة مثل أسماء وهمية أو عناوين غير صحيحة ،وكذلك تقديم ضمانات كاذبة، لما قد يترتب على ذلك من التعرض لعقوبات جنائية. بالإضافة إلى ذلك، قد يتسبب ذلك في خسائر للبنك إذا تم استخدام البطاقة بشكل مفرط لشراء السلع والخدمات بمبالغ كبيرة دون الوفاء بالالتزامات المالية، وقد يواجه البنك صعوبة في تتبع حامل البطاقة عند تقديم بيانات مزورة، مما يجبره في النهاية على تحمل قيمة المستحقات الناتجة عن هذا الاستخدام غير القانوني (السقا ا.، ٢٠٠٧، صفحة ١٦٤)

يلاحظ اذ يستعين المحتالين بمستندات إثبات شخصية مزورة للحصول على بطاقات بأسماء منتحلة وعناوين وهمية، وعادة ما يلجا محترفو هذا النوع من الجرائم الى استهداف أكثر من بنك لإصدار عدة بطاقات، لتحقيق أكبر عائد ممكن مستغلين ضعف وخبرة بعض موظفي البنك في كشف تزوير المستندات والوثائق (معروف، ٢٠١٤، صفحة ٤٨).

عمدت بعض التشريعات الحديثة الوطنية والمقارنة، ويلاحظ في القانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ بخصوص(القسم الخاص بالتزوير) حيث نص في المواد كل من (٢٨٠/٢٩٩) والمتضمنة على تجريم تزوير العملة والسندات المالية الرسمية، ويلاحظ الى عدم وجود نصوص خاصة في قانون الجرائم العراقي تتعلق بتزوير بطاقة الدفع الإلكتروني، لكنها تقع تحت نطاق الجرائم العامة المتعلقة بالتزوير المالي أو الغش بالعقود البنكية او النصب والاحتيال حسب نص المادة (٤٥٦) او حسب قانون غسل الأموال وتمويل الإرهاب رقم٣٥ لسنة ٢٠١٥ حسب نص المادة ٤٤ منه.

وقد ذهب بعض التشريعات المقارنة الى سن تشريعات تجريمة من أجل مواجهة القصور في النصوص التقليدية، أو أدراج تعديلات جديدة على التشريعات التقليدية، من أجل تجريم عمليات التزوير الواقعة على المستندات المعلوماتية، بهدف الحفاظ على الثقة الواجب توافرها في المستندات المعلوماتية، ومن أمثلة هذه التشريعات، التشريع الفرنسي الذي استحدث نصا خاصا بالتزوير المعلوماتي وهو المادة ٩/٤٦٢ من قانون العقوبات بموجب تعديل ١٩٨٨ ، غير أنه وبموجب تعديل ١٩٩٤ تراجع المشرع الفرنسي عن موقفه والغي النص الخاص بالتزوير المعلومات، وأخضعه لنصوص التزوير التقليدية (الحنيص، ٢٠١٠، صفحة ٨٦)، ويلاحظ في ذلك عن طريق محكمة الاستئناف بباريس في ٦ ديسمبر

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

٢٠٠٠، كما يوجد في القانون النقد والمال تجريم خاص، والتعليق بالممارسات الإجرامية الماسة بالاستعمال بطاقات الدفع في نص المادة(٤/١٦٣).

بالنسبة لموقف المشرع المصري، فموقفه مماثل للتشريع العراقي إذ لا يوجد نص خاص مباشرة بتزوير مستندات طلب بطاقة دفع إلكتروني، لكن قانون الجرائم الاقتصادية رقم ١٢٠ لسنة ٢٠٠٨ والعقوبات العامة رقم ٥٥ لسنة ١٩٧٣ ، اذ يعامل التزوير بصرامة، وخاصة الأوراق البنكية والعقود.

اما بخصوص موقف المشرع الاماراتي، فقد جاء القانون الاتحادي رقم ٣/١٩٨٧ (قانون العقوبات)، ومرسوم القانون الاتحادي رقم ٣٤/٢٠٢١ بشأن مكافحة الجرائم الإلكترونية، بتجريم تزوير أو استخدام بطاقات أو مستندات إلكترونية مزورة .

وأيضا نصت المادة ١٤ من قانون مكافحة الجرائم الإلكترونية رقك ٤٣ لسنة ٢٠٢١، التي تجرّم تزوير المستندات الإلكترونية، بما فيها بطاقات الدفع، مع عقوبات مالية تبدأ من ١٠٠,٠٠٠ درهم وتصل إلى ٣٠٠,٠٠٠ درهم أو الحبس.

وأيضا نصت المادة ١٥، التي تضمنت بتحديد عقوبة تزوير، أو تقليد بطاقة ائتمان أو بطاقات الدفع الأخرى، أو استخدامها دون تصريح، بعقوبة انقلاب أو غرامة من ٢٠٠,٠٠٠ إلى ٢,٠٠٠,٠٠٠ درهم .

واما فيما يتعلق بأنواع التزوير الذي قد يرد على أداة الدفع الالكترونية، فيلاحظ أنه ينقسم الى نوعين رئيسين يتماثلان مع صور التزوير الوارد على المحررات التقليدية والالكترونية، ومنها تزوير مادي وتزوير معنوي، فالتزوير المادي هو الذي يمس المحرر وشكله، ويترك له أثرا يمكن ان يدرك بالحواس وقد يتبين هذا الأثر بالحواس المجردة كما قد يظهر بالاستعانة بالخبرة الفنية، ويمكن معرفته من خلال الكشط او المحو او التأكد من خلال الرمز التعريفي الذي يسمى بالرمز السري.

اما التزوير المعنوي هو الذي يتحقق بتغير مضمون المحرر أو ظروفه أو ملابساته دون المساس بشكله أو بياناته المادية، ولا يختلف عنه أي إثر تدركه الحواس أو يستدل بها عند العبث بالمحرر أو الصك (يوسف، ٢٠١١، صفحة ١٣٧).

اما بخصوص وسائل الدفع الحديثة، فهي أيضا غير مستثناة من خطر التزوير، فحداثة تقنياتها وكيفية صناعتها، لن ولم تمنع المجرمين من البحث عن شتى الوسائل التي تتيح لهم إكمال عملياتهم .

كما يمكن أن يأخذ التزوير صورة أكثر خطورة تتمثل في تزوير بطاقة الدفع الإلكتروني ذاتها، وذلك من خلال التلاعب بالمادة المصنعة للبطاقة وأعادة انتاجها بما يجعلها شبيهة بوسائل دفع إلكترونية أخرى صحيحة المظهر، لكنها مزوّرة في حقيقتها.

٢_ استعمال المستفيد البطاقة بعد انتهاء مدة صلاحيتها:

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

كل بطاقة مصرفية فترة صلاحية معينة، وبعد انتهائها يُطلب من صاحب البطاقة إعادتها إلى البنك أو الجهة المُصدِرة، سواء لتجديدها أو للاستغناء عنها. وفي حال لم يتم ذلك، يُعتبر الامتناع عن الإعادة مخالفة قد تصل إلى حد الجرم.

عادةً، وبحسب نظام البرمجة الموجود في أجهزة الصراف الآلي المُستخدمة للسحب النقدي، تعمل الأجهزة إما على ابتلاع البطاقة أو رفضها تلقائيًا، وذلك استناداً إلى تعليمات البنك التي تُبلّغ المستخدم بضرورة تجديدها. ومع ذلك، قد تحدث حالات نادرة يتم فيها سحب الأموال من الجهاز رغم انتهاء صلاحية البطاقة، مما يترتب عليه دين على صاحبها. ويمكن التفرقة بين حالتين رئيسيتين في هذا السياق:

الحالة الأولى: إذا قام حامل البطاقة باستخدام بطاقته منتهية الصلاحية دون علم مسبق بذلك وقام بسحب النقود خطأً. في هذه الحالة، يُخضع البنك المستخدم للمساءلة القانونية حول المخالفة التي ارتكبها باعتبارها غير مقصودة.

الحالة الثانية: إذا كان حامل البطاقة يعلم مسبقاً بانتهاء صلاحيتها لكنه عمد إلى استخدامها لسحب الأموال بنية التحايل. هنا يُعَد تصرفه جريمة احتيال أو خيانة أمانة، نظراً لإصراره على التلاعب في استخدام البطاقة بشكل غير قانوني **(بوقديرة، ٢٠١٧، صفحة ١٨)**.

ذهبت محكمة النقض الفرنسية إلى تكييف هذا التصرف على أنه يشكّل جريمة خيانة الأمانة، باعتبار أن بطاقة الدفع تُعد محرراً يُسلَّم إلى المستفيد على سبيل عارية الاستعمال لأداء وظيفة محددة. وبالتالي، فإن إقدام المستفيد على الاستمرار في استخدامها رغم إخطاره بقرار سحبها يُعد بمثابة اختلاس يُلحق ضرراً بالمصرف (ليلى، ٢٠١٦، صفحة ١٣) .

٣_ إساءة استعمال المستفيد للبطاقة ملغاة الصلاحية:

إن البطاقة الملغاة هي في الأساس بطاقة مصرفية التي سلمت إلى صاحبها الشرعي(المستفيد) أستناداً الى عقد الانضمام الذي يشمل مجموعة من الشروط والالتزامات التي تفرض على المستفيد التقيد بها. ويؤدي أي إخلال من جانبه بتلك الالتزامات يفضي الى فسخ العقد من قبل البنك المُصدر، وبالتالي إلى إلغاء البطاقة. كما أن قيام الحامل الشرعي بغلق الحساب المرتبط بالبطاقة يستتبع بدوره سقوط صلاحيتها. وبمجرد صدور قرار الإلغاء من قبل الجهة المصدرة، يصبح لزاماً على حامل البطاقة إعادتها وتسليمها إلى البنك. وعليه، فإن أي استعمال للبطاقة الملغاة، سواء في عمليات السحب من أجهزة الصراف الآلي أو في تنفيذ المدفوعات، يعدّ استعمالاً غير مشروع، ويترتب على هذا الاستعمال غير المشروع نتائج قانونية متعددة، إذ قد يثير المسؤولية المدنية تجاه البنك المصدِر أو غير المتضرر، فضلاً عن إمكانية قيام المسؤولية الجزائية إذا انطوى الفعل على احتيال أو اختلاس أو أي صورة أخرى من صور الجرائم المالية (الصغير، ١٩٩٨، صفحة ٨٤_٨٥).

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

ويلاحظ في زمننا الحالي وبالتزامن مع التطور المتسارع في استحداث برمجة الصراف الآلي، فقد بات هذا الفعل لا يشكل أي جريمة؛ وذلك بالنظر إلى امكانية هذه البرامج في اكتشاف ما إذا كانت هذه البطاقة صالحة للاستخدام، أو أنها منتهية الصلاحية أم تم إلغاؤها من قبل مصدرها.

٤_ امتناع المستفيد رد البطاقة بعد طلبها من البنك:

تقوم العلاقة بين المستفيد ومصدر البطاقة الائتمانية، المتمثل في المصرف، على رابطة تعاقدية تنشأ بموجب اتفاق مُبرم بين الطرفين، تُعد بموجبه ملكية البطاقة الائتمانية منوطة بالمصرف المُصدر الذي يمنح المستفيد صلاحية استعمالها في حدود ما تقرره شروط العقد النافذ. غير أن استمرار المستفيد في الاحتفاظ بالبطاقة واستخدامها بعد إعلامه بقرار سحبها وامتناعه عن إعادتها يُعدّ تصرفاً ينطوي على خيانة للأمانة، لكونه يشكل صورة من صور الاستيلاء غير المشروع على مال مملوك للغير، وُضع تحت يده على سبيل الأمانة. ويتحقق الركن المادي لهذه الجريمة بمجرد إنكار الحائز وجود البطاقة في حيازته بهدف الإفلات من التزامه بردّها، دون أن يكون من اللازم ثبوت قيامه باستعمالها فعلياً، طالما أن المصرف قد طالبه صراحة بإرجاعها.

ومع ذلك، فقد أفرزت التقنيات المصرفية الحديثة المعتمدة في إدارة وسائل الدفع الإلكتروني آليات متقدمة تتيح للمصرف المُصدر إبطال صلاحية البطاقة موضوع النزاع، بحيث تفقد فاعليتها كلياً وتصبح غير قابلة للاستخدام في أي معاملة مالية لاحقة، ويُعد ذلك إجراءً وقائياً استباقياً يهدف إلى تعزيز حماية المصرف والحد من احتمالات إساءة استعمال البطاقة أو التحايل على الالتزامات التعاقدية المترتبة عليها (يوسف، ٢٠١١، صفحة ١٣٤).

ثانيا: الاعتداء على نظام البطاقة البنكية من طرف الغير

تتحدد اطراف التعامل في بطاقة الائتمان عادةً في كل من حامل البطاقة، والمصرف المصدر لها، والتاجر الذي يبرم معه المستفيد معاملات مالية، ووفقاً لذلك فإن المقصود بمعنى الغير هو كل من يخرج عن نطاق هذه الاطراف الثلاثة، ويكون تدخله غالباً من خلال أفعال غير مشروعة كالسرقة والتزوير والاحتيال

وفقا لذلك، فأن صور الاعتداء التي يتعرض لها نظام البطاقة البنكية من طرف الغير يمكن تصنيفها الى عدة أشكال أساسية تتمثل في: (مرابطي، ٢٠١٥، صفحة ٥١).

١_ استخدام الغير بطاقة دفع مزورة أو مسروقة:

يُعدّ كل من ينتحل صفة حامل البطاقة، سواء كان سارقًا أم مزورًا، مسؤولًا جنائيًا بموجب القانون عند استخدام البطاقة لسحب الأموال من أجهزة الصراف الآلي أو الموزعين الإلكترونيين للنقد. كما يتحمل هذا الشخص المسؤولية المدنية تجاه المتضررين، وبخاصة صاحب البطاقة الشرعي، نتيجة هذا الاختلاس (يوسف، ٢٠١١، صفحة ١٣٨).

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

ويحدث هذا النوع من السرقة على البطاقة عند ارتكاب السطو على المنازل، أو سرقة المحفظة، أو الحصول على بيانات البطاقة بطرق غير مشروعة، بما في ذلك مشاركة الرمز السري الخاص بها، أو غيرها من الوسائل، وذلك بهدف استخدامها في عمليات احتيالية (حوالف، ٢٠١٤، صفحة ٣٢٢).

قد يعمل السارق أو من يعثر على بطاقة الدفع باستخدام البطاقة لسحب الأموال من أجهزة الصراف الآلي، أو للحصول على السلع والخدمات من التجار، مما يؤدي الى إضرار مباشر بصاحب البطاقة الشرعي. في بعض الحالات، قد تُصنف هذه الأفعال وفق القانون على أنها جريمة التقاط أشياء مفقودة، إذا كان الغرض منها مجرد الاستيلاء على أشياء توافرها الحظ. إلا أنه إذا تم الاستيلاء على الأموال أو السلع باستخدام الحيلة والخداع، أو عبر إحدى الوسائل الاحتيالية المنصوص عليها قانونيًا، فإن الفعل يرتقي إلى مستوى جريمة الاحتيال والنصب، مما يترتب عليه مساءلة جنائية وفقًا للقانون، بالإضافة إلى المسؤولية المدنية تجاه المتضررين. وتُبرز هذه الوقائع أهمية تحديد الوسائل والطرق القانونية لحماية حقوق حامل البطاقة والحد من الممارسات الاحتيالية في مجال الدفع الإلكتروني.

٢_ التلاعب غير المشروع ببطاقات الدفع الإلكترونية من قبل موظفي البنك المصدر

قد يلجأ بعض موظفي البنك المصدر لبطاقات الدفع الإلكترونية إلى ممارسات غير مشروعة لتحقيق مصالح شخصية بحتة ،منفصلة تماماً عن مصالح البنك ،وذلك بغرض الاستيلاء على أموال دون وجه حق .ومن أبرز هذه الممارسات التواطؤ مع حامل البطاقة ،حيث يقوم الموظف بالتعاون مع العميل سيء النية ،مقابل مكاسب مالية ،لتمكينه من القيام بأفعال غير قانونية ،مثل إصدار بطاقة سليمة اعتماداً على بيانات مزورة بما في ذلك مستندات شخصية أو ضمانات وهمية ، وتستخدم هذه البطاقات لاحقاً في عمليات شراء كبيرة يكون البنك مسؤولاً عنها دون إمكانية استرداد قيمتها من حامل البطاقة الأصلي، كما يشمل هذا التواطؤ السماح للعميل بتجاوز الحدود المالية المقررة بموجب عقد الانضمام بين البنك والعميل ،أو القيام بسحوبات نقدية باستخدام بطاقات موقوفة التعامل أو منتهية الصلاحية. إضافة إلى ذلك، قد يتعاون موظف البنك مع التجار المعتمدين لتسهيل تجاوز الحدود المالية المقررة في إشعارات البيع، وتقديم الدعم لهم لاستخدام بطاقات وهمية أو مزورة أو منتهية الصلاحية ،مما يمكنهم من الحصول على مبالغ مالية دون وجه حق ،مع تحميل البنك المسؤولية المالية عن هذه العمليات .وفي بعض الحالات ،يتجاوز الموظف التواطؤ مع حامل البطاقة والتاجر المعتمد ،فيتعاون مع أطراف خارجية ،بما في ذلك مجموعات أو عصابات ،عبر تزويدهم بالبيانات الصحيحة لبطاقات الدفع والسحب ، مما يمكّنهم من التقليد أو الاصطناع وتحقيق مكاسب غير مشروعة على حساب البنك والعملاء. وتبرز هذه الوقائع الحاجة الملحة إلى تعزيز آليات الرقابة الداخلية للبنوك ،ووضع إجراءات صارمة للتحقق من العمليات المالية ،بهدف حماية مصالح البنك وحاملي البطاقات على حد سواء ،والحد من الممارسات الاحتيالية التي ينخرط فيها بعض الموظفين (الصغير، ١٩٩٨، صفحة ٢٧_٣٠) .

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

ثالثا: عمليات الاختراق غير المشروع في أنظمة خدمات الدفع الالكتروني(القرصنة الالكترونية)

تُعد القرصنة من اخطر الممارسات التي يقوم بها شخص أو مجموعة من الأشخاص بالقيام بعمليات مالية غير مشروعة، ويتم ذلك عن طريق الحصول على بيانات ومعلومات مستخدمي وسائل الدفع الالكتروني عن طريق قرصنة المعلومات، او ما يسمى " بالاختراق او الهاكر، وهو مصطلح يطلق على المختص بالوصول غير المصرح به الى البيانات الخاصة بالمستخدمين على أجهزتهم الشخصية، بالاستعانة بوسائل غير مشروعة، من دون الحصول على موافقة صاحب البيانات (احمد، ٢٠٢٤، صفحة ٨٦) ؛ وبذلك فالقرصنة أو الاختراق هو عبارة عن مجموعة من العمليات البرمجية التي ينفذها فرد أو مجموعة من الافراد يتم من خلال الدخول الى أحد نظم الدفع الالكتروني أو شبكة المعلومات الخاصة به ؛ بهدف الوصول على بيانات أو معلومات وسائل الدفع الالكتروني، ليتم استخدامها في وقت لاحق في عمليات دفع غير مشروعة (الرقب، ٢٠١١، صفحة ١٩٤) .

تعد قضية القرصنة أو الاختراق في عمليات الدفع الإلكتروني من القضايا الحرجة التي تتزايد نسبها مع مرور الزمن ومع تطور أساليب الدفع، فعمليات اختراق أنظمة الدفع الالكتروني أصبحت تنفذ يومياً، وبالرغم من تطور عمليات تشفير البيانات التي تقوم بها المؤسسات بهدف الحفاظ على سرية بيانات الدفع الالكتروني من خلال الانترنيت، والقيام بتوعية الافراد بعدم مشاركة أو عرض بيانات ومعلوماته وسائل الدفع الخاصة بهم على الانترنيت ومع الغرباء (الدبيسي، ٢٠٠٩، صفحة ١٨٧) .

إذ أن تداول البيانات والمعلومات الخاصة بوسيلة الدفع الالكتروني من خلال شبكة الانترنت يشتمل على مخاطر متعددة ، اذ ان شبكة الانترنت تستعمل من قبل جميع الأفراد، وهي بذلك حقٌ مشاع لا يحتكر لأحد ولذلك فأن هذه الوسائل تصبح معرضة لعمليات القرصنة او الاختراق من قبل افراد يحترفون هذه العمليات (الساعدي، ٢٠٠٧، صفحة ١٣٥) .

بالنظر إلى تطور أساليب قرصنة المعلومات بطرقاً غير مشروعه في انظمة الدفع الالكتروني للتمكن من عملية الاختراق، وسحب الاموال المالية من حساب المستفيدين في وسائل الدفع الالكتروني، ويتم ذلك بعدة اساليب وطرق متعددة وكثيرة، نوجز الحديث فيها بأبرز الحالات الشائعة الآتية :

١_أسلوب قرصنة خطوط الاتصالات العالمية :

يُعدّ أسلوب قرصنة خطوط الاتصالات العالمية أحد أخطر أشكال الاعتداءات الإلكترونية التي تستهدف نظم الدفع عبر الإنترنت، إذ يقوم على اعتراض الخطوط التي تربط الحاسوب الخاص بالمشتري بالحاسوب التابع للتاجر، الأمر الذي يجعله وسيلة فعّالة لاختراق بيانات الدفع وتنفيذ عمليات مالية غير مشروعة. وتنبع خطورة هذا الأسلوب من كونه لا يقتصر على سرقة بيانات الأفراد فحسب، وإنما يمتد أثره ليهدد الثقة في منظومة التجارة الإلكترونية برمتها، ويُلقي بظلاله على التعاملات المالية الرقمية على المستوى العالمي. ويبدو أن الدافع الرئيسي وراء هذا النوع من الهجمات يتمثل في تحقيق مكاسب

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

مالية غير مشروعة، إلى جانب نزعة القراصنة إلى اختبار قدرة الأنظمة التقنية الدولية على مواجهة الهجمات وتجاوز آليات الحماية المتبعة، على الرغم من ما تتسم به هذه الآليات من تطور وتعقيد (الجهني أ.، ٢٠٠٨، صفحة ٧٧٦) .

وقد تجسدت خطورة هذا الأسلوب في عدد من الحوادث البارزة التي أثارت اهتمام الأجهزة الأمنية الدولية، إذ أعلن مكتب التحقيقات الفيدرالي الأمريكي (FBI) عن فتح تحقيق في حادثة اختراق أنظمة شركة Data Processors International، وهي إحدى الشركات المتخصصة في معالجة التحويلات المالية الإلكترونية المرتبطة ببطاقات فيزا وماستر كارد وأمريكان إكسبريس. وقد مكّن هذا الاختراق غير المصرح به من الوصول إلى الأرقام السرية الخاصة بأكثر من ثمانية ملايين بطاقة دفع إلكتروني، بعد النفاذ إلى البنية التشغيلية الداخلية للشركة، بما يكشف عن حجم التهديدات التي يمكن أن تنجم عن هذه الأساليب حين تستهدف بنى تحتية مالية عابرة للحدود (الجهني ا.، ٢٠١٠، صفحة ١٩١)

كما أكدت تقارير مركز شكاوى الإنترنت (IFCC) التابع للولايات المتحدة الأمريكية اتساع نطاق هذه الظاهرة، حيث سجل المركز خلال سنة ٢٠٠٠ ما مجموعه (٦٠٨٧) شكوى تتعلق باختراق وسائل الدفع الإلكتروني، وقدرت الخسائر المالية الناتجة عنها بنحو (٤.٦) مليون دولار، وهو ما يمثل نسبة ٣٣٪ من حجم الخسائر المترتبة على جرائم الاحتيال التقليدية في تلك الفترة (شافي، ٢٠٠٧، صفحة ٢٦٩_٢٧٠) .

وتشير هذه البيانات إلى أن قرصنة خطوط الاتصالات العالمية ليست مجرد اعتداء تقني عابر، بل هي جريمة منظمة ذات أبعاد اقتصادية خطيرة، تؤثر مباشرة على استقرار المعاملات المالية الإلكترونية، وتبرز الحاجة إلى تطوير تشريعات أكثر صرامة وتعاون دولي فعال لمواجهة هذا النمط من الجرائم، خاصة وأنها تستهدف الشركات الكبرى التي تشكل العمود الفقري للتجارة الإلكترونية العالمية

٢_انتحال صفة مواقع تجارية الكترونية للشركات والمؤسسات:

يقوم القراصنة بإنشاء مواقع الكترونية مزيفة على شبكة الانترنت لشركات ومؤسسات تجارية كبرى على أساس انها تعود لها، إذ يبدو هذا الموقع المزيف مطابقاً للموقع الأصلي، ويتم ذلك بإنشاء موقع مزيف يحتوي على كافة البيانات والمعلومات المتوفرة في الموقع الاصلي (حجازي، ٢٠٠٤، صفحة ١٣٣) .

وكذلك يعمل المخترقون على إنشاء موقع الكتروني مطابق الشبه بموقع المبيعات الأصلي، والعمل على تفعيل هذا الموقع واستقبال عروض الشراء وتقديم الخدمات للزبائن، وتحفيز الزبائن عن طريق إقامة خصومات وعروض تحفز الزبائن على الشراء وأرسال بياناتهم، لغرض قيام القراصنة بعد ذلك بالاستيلاء على بياناتهم الخاصة ببطائق الدفع الإلكتروني (الرؤوف، ٢٠١١، صفحة ٣٨) .

٣_ أسلوب الشفط من مكائن الدفع الإلكتروني:

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

تُعدّ القرصنة الإلكترونية من أخطر التحديات التي تواجه أنظمة الدفع الإلكتروني، لما تنطوي عليه من أساليب تقنية معقدة ومتجددة يصعب حصرها. فقد اعتمد المخترقون، على سبيل المثال، على أجهزة تعرف بـــ "Skimmer" يتم تثبيتها في فتحات الصرافات الآلية، حيث تقوم هذه الأجهزة بمسح بيانات بطاقات الدفع الإلكتروني – كالبطاقات الوطنية (الكي كارد) وبطاقات الماستر كارد – وتخزينها إلكترونياً، ليُعاد لاحقاً إنشاء بطاقات مُماثلة للبطاقات الأصلية تُستخدم في تنفيذ عمليات دفع غير مشروعة سواء عبر الإنترنت أو في معاملات مالية مشبوهة (الرؤوف، ٢٠١١، صفحة ٨٤) .

وفق ما سبق، فأن اساليب وطرق قرصنة واختراق وسائل الدفع الالكتروني لا يمكن حصرها ؛ لأنها اساليب متطورة ومتجددة، فقد يقوم القراصنة الإلكترونيين علاوةً على الاساليب المذكورة على تفجير مواقع الشركات التجارية المصدرة لوسائل الدفع من خلال القيام بإرسال مئات الالاف من الرسائل الالكترونية ، بحيث يشكل هذا الكم الهائل من الرسائل الالكترونية ضغطاً، ينتج عنه تفجير هذه المواقع وتشتت منظومة الحماية الخاصة به، ليقوم القرصان بعد ذلك بسحب ما يشاء من المعلومات المخزنة على هذه المواقع ، بهدف تحصيل اكبر عدد ممكن من ارقام البطاقات.

ويلاحظ، فإن أساليب القرصنة واختراق أنظمة الدفع الإلكتروني كثيرة ومتجددة يصعب حصرها بالنظر الى طبيعتها المتطورة والمتغيرة باستمرار، إذ نكتفي بهذا القدر الموجز من الأساليب.

وبعد توضيح مفهوم القرصنة الالكترونية المتعلقة بوسائل الدفع الالكتروني، وبيان أبرز الأساليب التي يستعملها القراصنة أو المحتالون للوصول الى البيانات والمعاملات المالية عبر الانترنت، مما يقتضي علينا الانتقال لبيان موقف التشريع العراقي والتشريعات المقارنة في مثل هذه الظاهرة ؛ بهدف الوقوف على درجة الحماية القانونية التي توفرها هذه التشريعات لمستخدمي أنظمة الدفع الالكتروني وحمايتهم من هذه المخاطر.

ونلاحظ ان ذلك لا يوفر الحماية الكافية للمستفيد ؛ إذ ان خطورة القيود المالية غير المشروعة تتطلب تدخلا تشريعا من خلال إلزام المُصدّر او شركات الاتصالات التي يتعامل معها، أو مع أصحاب المتاجر الالكترونية بضوابط كفيلة تضع قدراً كافياً من الحماية للمستخدمين ؛ فضلا عن ان حماية المستخدم من خلال الابلاغ عن العمليات غير المشروعة لضرورتها، الا انها ليست كافية إذ يجب ان تكون هذه الحماية سابقة على هذه العمليات فضلا عن معالجتها بعد حدوثها .

يلاحظ بدايتاً موقف المشرع العراقي بخصوص العقود المالية والتي تبرم من خلال شبكة الانترنت، فقد نصت المادة (٢/خامسا _ سابعا) في نظام خدمات الدفع الالكتروني العراقي للأموال رقم ٢ لسنة ٢٠٢٤ ، في الفقرة خامساً والمتضمنة ((تحقيق سلامة نظم الدفع الإلكتروني للحد من حالات الاختراق والوصول غير المصرح والتزوير وفرص الاحتيال بالتحويلات الإلكترونية وأي مخاطر إلكترونية محتملة

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

الحدوث)). وكما جاء في الفقرة سابعا والمتضمنة ((تعزيز امان نظم الدفع الإلكتروني باعتماد أفضل الممارسات في أمن المعلومات ومكافحة التهديدات ذات الصلة)).

وأيضا نصت المادة (١٣/سادسا) من النظام المذكور أعلاه، على ان يلتزم مقدم خدمة الدفع الالكتروني ب((تطبيق اجراءات صارمة للتحقق من هوية المستخدمين وتامين المعاملات لمنع الاحتيال)) .

وكذلك يلاحظ عند الرجوع الى المادة (١٠/اولا) من قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم ٧٨ لسنة ٢٠١٢ التي تضمنت بأن يلتزم المرخص له ب((اصدار وتسلم وحفظ شهادات التصديق الالكتروني باستعمال اليات وبرامج موثوقة من اجل حمايتها من التقليد والاحتيال)).

ويتضح مما تقدم، أن المشرّع العراقي قد اعتبر الاختراق من أبرز المخاطر التي قد تتعرض لها خدمات الدفع الإلكتروني، إذ ألزم مزوّدي هذه الخدمات باتخاذ إجراءات وقائية مناسبة تهدف إلى تحصين البيانات والمعلومات المرتبطة بخدمات الدفع الإلكتروني من مخاطر القرصنة أو الاختراق، وذلك باعتبارها حماية سابقة على العمليات المالية التي تُبرم عبر هذه الوسائل، كما أوجب على مزوّد الخدمة القيام بفحص وتحديث وتطوير الأنظمة والبرامج المستخدمة بشكل مستمر لضمان أعلى مستويات الأمان.

وان المشرّع العراقي لم يبيّن بشكل صريح الآلية القانونية لمعالجة العمليات المالية التي تتم، نتيجة القرصنة أو الاختراق، سواء من خلال تنظيم إجراءات الاعتراض التي يقدّمها المستخدم أمام الجهة المصدرة، أو عبر آلية إخطار مزوّد الخدمة بتعرض وسيلة الدفع الإلكتروني لعملية قرصنة أو احتيال أو سرقة أو فقدان.

تجدر الإشارة إلى أن المستفيد يمكنه الاستناد إلى أحكام المادة (٢٦/ثانياً) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢، والتي نصت على أن ((لا يعد الزبون مسؤولاً عن أي قيد غير مشروع يدخل على حسابه بوساطة تحويل إلكتروني ما لم يكن ناتجاً عن خطئه أو إهماله)).

إلا أن تساؤلاً مشروعاً يثور في هذا السياق، وهو، هل يمكن التحقق من هوية المستفيد أو المستخدم من خلال وسيلة الدفع الإلكتروني فقط، باعتبارها الوسيلة الوحيدة لإثبات هويته؟

نلاحظ من الإجابة على هذا التساؤل حيث ان التكنولوجية الحديثة التي تم أضافتها (شركة ماستر كارد) كفيلة يجيب عن هذا التساؤل فقد استخدمت شركة الماستر كارد تقنية جديدة ومتطورة تهدف الى حماية المستفيدين من البطاقة الذكية وتطلق على هذه التقنية (كود الامان / secure code) أذ تعتبر خدمة ال "كود الأمان (Secure Code) "من الوسائل التقنية المبتكرة، التي تهدف إلى تعزيز حماية وسيلة الدفع الإلكتروني الخاصة ببطاقات ماستر كارد، وذلك عبر تخصيص رمز فريد يمنع الاستخدام غير المشروع عند قيام المستخدم بعمليات التسوق من المتاجر الإلكترونية. ويبدأ تفعيل هذه الخدمة من خلال قيام مستخدم وسيلة الدفع بالتسجيل فيها، بحيث يلتزم بإدخال رمز الأمان في كل مرة يقوم فيها بعملية

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

شراء عبر أي متجر إلكتروني، ضماناً لحماية بيانات البطاقة من مخاطر القرصنة، ويُشابه رمز الأمان الرقمَ السري من حيث الغرض الأساسي المتمثل في توفير الحماية من تنفيذ عمليات مالية غير مشروعة، إلا أنهما يختلفان في الطبيعة والوظيفة؛ فالرقم السري يُعد الأداة الأساسية والملزمة لتعريف هوية مستخدم وسيلة الدفع الإلكتروني، ولمنحه صلاحية الدخول إلى حسابه وتفويض المصدر بتنفيذ أي عملية مالية، في حين يُعد رمز الأمان وسيلة حماية إضافية ذات طبيعة اختيارية، يمكن للمستخدم تفعيلها لزيادة مستوى الأمان، أو الاكتفاء بالرقم السري للبطاقة دون استخدامها (امان بطاقات الدفع الالكتروني master cards، ٢٠٢٥).

وتتميز هذه بقدرة كبيرة على مواجهة عمليات القرصنة والاحتيال الالكتروني ومنع قيامها ، ويتم ذلك من خلال تنفيذ غالبية عمليات الدفع الالكتروني عن طريق الصراف الآلي للنقود، أو من خلال الانترنت ، حيث أذ يتم أبلاغ المصدر من قبل هذه الاجهزة الكترونياً بوجود عملية مالية ستتم على حساب المستفيد او المستخدم في كل مرة عملية سحب من حسابه ، اذ يقوم الوسيط الالكتروني بأشعار المستفيد او المستخدم عن طريق الهاتف المحمول برمز أمان (Secure code)، فلا تقوم عملية السحب الا بعد إدخال كود او رمز الأمان الذي أرسل داخل الهاتف ، وهذا سيمنح عملية الدفع الالكتروني مستوى امان عالي (Mason, 2006, p. 28) .

وكذلك الحال مع المشرع الاماراتي، الذي أشار في النظام الرقابي للقيم المخزنة ونظام الدفع الالكتروني الصادر بناءً على مرسوم اتحادي رقم (١٤) لسنة ٢٠١٨، الذي لم ينص صراحتاً على مصطلحات مماثلة لما أوجده الفقهاء للتعبير عن الاختراق او القرصنة أو الهاكر ؛ الا انه أكد في المادة (د– ٤ – ١٠) من النظام أعلاه، على ضرورة ان يتحقق المصدر من ان وسيلة الدفع لا يمكن الوصول اليها بواسطة اشخاص غير المستخدم الذي أصدر أداة الدفع له .

والعكس من ذلك فأن موقف المشرعين الفرنسي والمصري، الذين أشارو بموقف صريح من القرصنة لعمليات الدفع الإلكتروني عبر الانترنت، اذ يعد المشرع الفرنسي في مقدمة التشريعات القانونية التي تصدت لجرائم الدفع الإلكتروني، ووضع قوانين متقنة تخص عمليات الاحتيال والقرصنة الإلكترونية، فقد ورد في قانون العقوبات الفرنسي (pénal Code) الصادر سنة ١٩٩٢ والنافذ ١٩٩٤، والذي أشار في المواد كل من (٣٢٣/١_٧) التي تناولت جرائم انتهاك أنظمة المعالجة الآلية للبيانات الالكترونية وتشمل (الدخول الغير مشروع إلى أنظمة الدفع الإلكتروني وعرقلة عمل النظام واستخراج أو تعديل البيانات الإلكترونية).

وأيضا نضم المشرع الفرنسي في قانون النقد والمال لسنة ٢٠٠٠ (Code monétaire et financier) الذي رخصة عمليات الدفع الإلكتروني لغرض حماية للمستفيدين، وهذا يمنح المشرع الفرنسي الدقة

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

والتفصيل على عكس من الامارتي، والذي أكده على حق المستفيد او المستخدم من استعادة أمواله عند وقوع عملية الاحتيال او القرصنة .

اما المشرع المصري فقد ورد في قانون تنظيم استخدام وسائل الدفع غير النقدي رقم ١٨ لسنة ٢٠١٩ ، اذ وضع هذا القانون إطاراً لتوسيع عمليات الدفع الإلكتروني، كما أكده على حماية المستفيدين من عمليات الدفع الالكتروني عن طريق ألزام على الجهات المصدرة والمرخصة لمزاولة هذه العمليات من خلال بتأمين وسائل انظمة الدفع.

ومن خلال هذا العرض يتضح أن المشرع العراقي وإن أدرك خطورة القرصنة الإلكترونية، إلا أن معالجته جاءت مقتصرة على تعزيز التدابير الوقائية من دون وضع آليات واضحة لمعالجة النتائج، في حين اتخذ المشرع الإماراتي اتجاهاً مشابهاً. أما المشرع الفرنسي فقد جمع بين الحماية الوقائية واللاحقة عبر النص على جرائم محددة وإقرار ضمانات لاسترداد الأموال، بينما ركز المشرع المصري على إلزام المؤسسات المالية بتوفير حماية مؤسسية شاملة. ويكشف هذا التباين عن حاجة النظام القانوني العراقي إلى مراجعة وتطوير نصوصه بما يتلاءم مع متطلبات الحماية الحديثة، من خلال إدماج ضمانات صريحة تكفل للمستفيدين استعادة أموالهم عند وقوع الاحتيال، وإيجاد آليات اعتراض وتعويض فعّالة، بما ينسجم مع التوجهات المقارنة ويحقق التوازن بين مصلحة مزوّدي الخدمات وحقوق المستخدمين.

الفرع الثاني : المخاطر القانونية

تعد المخاطر القانونية من أهم التحديات التي تواجه الهيئات المشرفة على وسائل الدفع، كما يمكن ان تنطوي هذه المخاطر على ما يمس بخصوصية المتعاملين بالدفع الالكتروني، والمتعلقة بالمعلومات التي يعطيها المستفيد للمؤسسة المصدرة للدفع الالكتروني، فضلا عن ذلك، استثمار البعض الأموال غير مشروعة في مشاريع ذات صبغة مشروعة أو فيما يعرف بتبيض الأموال (حوالف، ٢٠١٤، صفحة ٤٧٥)، ومن أبرز الإجراءات لمكافحة المخاطر القانونية:

اولاً: حماية الخصوصية:

نظم المشرع العراقي في المادة (١٢/سابع عشر) من نظام خدمات الدفع الالكتروني للأموال العراقي رقم ٢ لسنة ٢٠٢٤ والمتضمنة((وضع تدابير أمان محكمة لحماية أمن المعلومات وسريتها ، بما في ذلك سرية سجلات ومعلومات الزبائن وخصوصيتها ، وإجراء مراجعات دورية لضمان فاعلية هذه التدابير إضافة الى الضوابط التي يحددها البنك المركزي))، ويلاحظ أيضا في المادة(١/رابع والثلاثون) من ذات القانون اعلاه والتي نصت على أمن المعلومات ((أمن المعلومات : هي مجموعة من الاجراءات والتدابير والادوات الخاصة بحماية المعلومات واصولها وتضمن الحفاظ على سلامتها وسريتها وتوافرها ومتطلبات استخدامها والوصول اليها ، ويعد أمن البيانات والأمن السيبراني للوقاية من المخاطر الإلكترونية والاستجابة لها جزء من نطاق امن المعلومات .))،وكذلك أيضا نصت المادة (١٣/ خامساً) من ذات

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

القانون أعلاه، والمتضمنة(الالتزام بمعايير حماية خصوصية وسرية وأمن معلومات الزبون والمالية ، والبنك المركزي تحديد هذه المعايير) .

ووفقا لذلك، يجب احترام سرية البيانات الخاصة بالمستفيدين بوصفهم المستهلكين، وكذلك احترام حقهم في الخصوصية، ويقتضي ذلك الالتزام بعدم النشر، أو بث أي بيانات تتعلق بشخصياتهم أو حياتهم الخاصة، وكذلك البيانات المصرفية الخاصة بهم (حوالف، ٢٠١٤، صفحة ٤٤٦) .

ونؤكد بما جاء في الفصل الأول من رسالتي الموسومة سالفة الذكر من القانون العراقي بخصوص السرية وخصوصية المستفيدين ولاسيما بياناتهم ومعلوماتهم الشخصية، سيما في الدستور العراقي ونظام خدمات الدفع الالكتروني رقم ٢ لسنة ٢٠٢٤، وقانون التوقيع الالكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٠.

ثانياً: الحماية من غسيل الأموال:

ان العراق كسائر الدول، التي شرعت تشريعات للحماية من غسيل الأموال، إذ نظم المشرع العراقي في قانون مكافحة غسل الأموال وتمويل الإرهاب رقم ٣٩ لسنة٢٠١٥ العراقي النافذ ، أذ انه ليس بمنأى من مخاطر هذه الظاهرة الإجرامية سيما أمام التوجيهات الاقتصادية التي أصبحت امرا حتميا وضروريا للارتباط الحيوي والنفعي مع العالم وان تصادق وتوقع على الاتفاقيات المتعلقة بصدد الحماية من غسيل الأموال وتمويل الإرهاب.

ويعد قانون مكافحة غسل الأموال وتمويل الإرهاب العراقي، أخر حلقة من حلقات التعديل الذي قام بها المشرع في هذا النوع من الجرائم، وجاء ليثبت ضرورة محاربة هذا النوع من الجرائم التي أصبحت تثقل كاهل القانون، وأن المشرع العراقي وسع من نوعية الأنشطة والعمليات التي تدخل ضمن عمليات غسيل الأموال، ومن بينها إدراج بعض وسائل الدفع الإلكتروني محل الدراسة ضمن هذه الأنشطة أذ نضم في ذات القانون أعلاه في في المادة (١/خامساً) والمتضمنة((الاصول او الممتلكات التي يتم الحصول عليها باي وسيلة كانت كالعملة الوطنية و العملة الاجنبية و الاوراق المالية و التجارية و الودائع و الحسابات الجارية و الاستثمارات المالية و الصكوك و المحررات أيا كان شكلها بما فيها الالكترونية او الرقمية و المعادن النفيسة و الاحجار الكريمة و السلع و كل ذي قيمة مالية من عقار او منقول و الحقوق المتعلقة بها، و ما يتاتى من تلك الاموال من فوائد وارباح، سواء اكانت داخل العراق ام خارجه . واي نوع اخر من الاموال يقررها المجلس لأغراض هذا القانون، ببيان ينشر في الجريدة)).

وكذلك تطرق المشرع العراقي في نظام خدمات الدفع الالكتروني رقم ٢ لسنة ٢٠٢٤ بصدد هذا الموضوع في المادة (٤/١٢) والمتضمنة على((تطبيق إجراءات صارمة ومفصلة تتوافق مع قانون مكافحة غسل الأموال وتمويل الإرهاب النافذ، وإدارة مكافحة الاحتيال وغيرها، وتقديم تقارير دورية للبنك المركزي بشأن هذه التدابير)) .

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

وأيضا أكدت المادة (٢٨/١٢) من نظام خدمات الدفع الالكتروني العراقي النافذ على (التعاون مع الجهات التنظيمية المحلية والدولية في مجالات غسل الأموال ومكافحة الجرائم المالية وتبادل المعلومات).

وكذلك يلاحظ عند العودة للمشرع الاماراتي من خلال قرار مجلس الوزراء رقم (٢٤) لسنة ٢٠٢٢ بتعديل بعض أحكام قرار مجلس الوزراء رقم (١٠) لسنة ٢٠١٩ في شأن اللائحة التنفيذية للمرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨ في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، الذي عرف المستفيد الحقيقي في المادة (١) منه ((الشخص الطبيعي الذي يمتلك أو يسيطر فعلياً على العميل بشكل نهائي أو الشخص الطبيعي الذي تتم العمليات نيابةً عنه، كما يتضمن الشخص الذي يمتلك سيطرة فعلية ونهائية على شخص اعتباري أو ترتيب قانوني، سواء كان ذلك بشكل مباشر أو من خلال سلسلة ملكية أو سيطرة أو غيرها من الوسائل غير المباشرة)) .

عرفه المشرع الاماراتي البنك الوهمي في المادة ذاتها ((بنك مسجل أو مرخص له في دولة وليس له وجود مادي فيها، ولا ينتسب إلى مجموعة مالية خاضعة للتنظيم والرقابة)).

وأكده المشرع من خلال المادة (٤٤) من القانون أعلاه على غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة ((تتولى الجهات الرقابية على المنشآت المالية والأعمال والمهن غير المالية المحددة ومزودي خدمات الأصول الافتراضية، كل بحسب اختصاصه مهام الإشراف والرقابة والمتابعة لضمان الالتزام بالأحكام المنصوص عليها في المرسوم بقانون وهذا القرار والقرارات الرقابية وأي قرارات أخرى ذات صلة، وتختص بما يأتي((١_ إجراء تحديد مخاطر احتمال وقوع الجريمة في الأشخاص الاعتبارية وتقييمها وتحديثها، على أن يشمل ذلك المنشآت المالية والأعمال والمهن غير المالية المحددة وأنشطة الأصول الافتراضية وأنشطة مزودي خدمات الأصول الافتراضية.

٢_ تطبيق منهج قائم على المخاطر لضمان أن تكون تدابير منع أو تخفيف غسل الأموال وتمويل الإرهاب تتناسب مع المخاطر المحددة.

٣_ وضع التعليمات والأنظمة والنماذج الخاصة بمواجهة الجريمة للخاضعين لرقابتها عند الاقتضاء

٤_ وضع السياسات والإجراءات والضوابط اللازمة للتحقق من التزام الخاضعين لرقابتها بأحكام المرسوم بقانون وهذا القرار وأي تشريعات أخرى خاصة بمواجهة الجريمة في الدولة، وطلب المعلومات المتعلقة بتنفيذ هذا الالتزام.

٥_إجراء عمليات الرقابة والتفتيش المكتبي والميداني على المنشآت المالية والأعمال والمهن غير المالية المحددة ومزودي خدمات الأصول الافتراضية على أساس منهج قائم على المخاطر.

٦_ تحديد دورية عمليات الرقابة والتفتيش على المنشآت المالية والمجموعات المالية والأعمال والمهن غير المالية المحددة ومزودي خدمات الأصول الافتراضية بناء على ما يأتي:

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

التقييم الوطني للمخاطر، والسمات المميزة للمنشآت المالية والمجموعات المالية والأعمال والمهن غير المالية المحددة ومزودي خدمات الأصول الافتراضية، من حيث تنوعها وحجمها ودرجة حرية التصرف الممنوحة لها وفقاً للمنهج القائم على المخاطر، و مخاطر الجريمة وفهمها لها والسياسات والضوابط الداخلية والإجراءات التي تطبقها المنشآت المالية أو المجموعات المالية أو الأعمال والمهن غير المالية المحددة أو مزودي خدمات الأصول الافتراضية، و القيام بكافة التدابير التي من شأنها ضمان الالتزام الكامل للمنشآت المالية والأعمال والمهن غير المالية المحددة ومزودي خدمات الأصول الافتراضية بتطبيق قرارات مجلس الأمن المتعلقة بمنع وقمع الإرهاب وتمويله ومنع وقمع ووقف انتشار أسلحة الدمار الشامل وتمويلها، وغيرها من القرارات ذات الصلة من خلال الزيارات الميدانية والمتابعة المستمرة، والعمل على فرض العقوبات الإدارية المناسبة عند مخالفتها أو تقصيرها في تطبيق التعليمات والتحقق من أن المنشآت الخاضعة لرقابتها تعتمد وتطبق الضوابط والإجراءات والتدابير المقررة وفقاً الأحكام المرسوم بقانون وهذا القرار.

٧_التأكد من مدى خضوع المنشآت المالية الخاضعة للمبادئ الأساسية الدولية للرقابة المالية، للتنظيم والرقابة بما يتفق مع تلك المبادئ)).

المطلب الثاني: آليات حماية المستفيد في أنظمة الدفع الإلكتروني

تُشكّل الاعتداءات الواقعة على بطاقات الدفع الإلكتروني خطورة بالغة على استقرار المعاملات المالية، لما تخلّفه من خسائر اقتصادية مباشرة وانعكاسات سلبية على الثقة في أنظمة الدفع الحديثة. وتزداد خطورة هذه الاعتداءات بالنظر إلى طبيعتها التقنية، إذ ترتبط ارتباطاً وثيقاً بالأجهزة والوسائط الإلكترونية، مما يجعل مرتكبيها غالباً من ذوي الخبرة والمهارة العالية في المجال التكنولوجي، والقادرين على استغلال الثغرات التقنية بطرق يصعب كشفها بالوسائل التقليدية.

ولذلك، بات من الضروري أن تتبنى التشريعات والهيئات المالية إستراتيجيات وقائية وردعية متكاملة لمكافحة هذا النوع من الجرائم، بما يحقق حماية فعّالة للأطراف المتعاملة ويعزز الثقة في منظومة الدفع الإلكتروني، وعليه، سنستعرض من خلال هذا المطلب مختلف الإجراءات القانونية التي تهدف إلى مواجهة المخاطر الناشئة عن استخدام وسائل الدفع الإلكتروني، والحد من آثارها على المستفيدين وعلى النظام المالي بشكل عام:

الفرع الأول: مكافحة العبث في الأجهزة

تُشكّل الأجهزة الإلكترونية المستخدمة في عمليات الدفع، بما في ذلك الصرّافات الآلية وأجهزة قراءة البطاقات والبطاقات ذاتها، إحدى الركائز الأساسية لحماية أنظمة الدفع الإلكتروني. فهذه المكونات التقنية تُعدّ خط الدفاع الأول في مواجهة التهديدات الخارجية التي تستهدف سلامة وموثوقية المعاملات المالية،

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

وبالأخص في ميدان التجارة الإلكترونية الذي يتطلب درجة عالية من الأمان والثقة. وقد مرّت البطاقات الإلكترونية بمراحل من التطوير التقني، فبعدما كانت تعتمد في بداياتها على الأشرطة المغناطيسية، أُدخلت عليها الشرائح الذكية التي تحتوي على تقنيات حماية متقدمة، الأمر الذي عزّز قدرتها على مقاومة محاولات التزوير والاختراق. غير أنّ هذا التطور التقني، على أهميته، لا يكفي بمفرده لدرء المخاطر، إذ يتعيّن أن يواكبه إطار قانوني وتشريعي متطور يفرض على المؤسسات المالية والتجارية التزامات محددة، ويضمن للمستفيد حماية فعّالة من التهديدات التي قد يتعرض لها في أثناء استعماله لهذه الوسائل الحديثة في الدفع، (حوالف، ٢٠١٤، صفحة ٤٣٦). ومن وسائل تأمين عمليات الدفع الالكتروني:

اولاً: تشفير البيانات كوسيلة لتامين الدفع الالكتروني

يُعَدّ التشفير من أهم الوسائل الفنية والقانونية المعتمدة لضمان أمن المعاملات الإلكترونية، لما يؤديه من دور أساسي في صون النظم والأجهزة الإلكترونية المستعملة في مجالات النقود والتجارة الإلكترونية. وتكمن قيمته في تحقيق مبدأ السرية وحماية الحق في الخصوصية بالنسبة للمراسلات والبيانات والاتصالات المرتبطة بالصفقات الرقمية، بما يرسخ عنصر الثقة الذي يُعد شرطاً لازماً لصحة التعاملات المالية والتجارية عبر الوسائط الإلكترونية، ويستند نظام التشفير إلى آلية قانونية – تقنية قوامها تحويل البيانات من شكلها الأصلي إلى صيغة مشفرة مكوّنة من رموز وخوارزميات رياضية، بحيث تصبح غير قابلة للإدراك المباشر من الغير. ويهدف ذلك إلى منع أي اعتداء على المعلومات، وضمان عدم استخدامها على نحو غير مشروع من قبل أشخاص غير مخولين قانوناً بالاطلاع عليها أو استغلالها، وهو ما يشكل أداة لحماية حقوق المتعاقدين ودرء مخاطر المسؤولية المدنية أو الجنائية الناشئة عن انتهاك سرية البيانات.

فضلاً عن ذلك، يُوظَّف التشفير للتحقق من سلامة الرسائل الإلكترونية المتبادلة بين الأطراف في نظم الدفع، خصوصاً في ميدان النقود الإلكترونية، وذلك من خلال ضمان عدم تعرض تلك الرسائل لأي تعديل أو تحريف غير مشروع قبل وصولها إلى المستفيد الشرعي. كما يشكل التشفير وسيلة قانونية لحماية البرمجيات والمعلومات التقنية أثناء انتقالها عبر الشبكات العامة، إذ يتيح للمرسل إليه وحده الاطلاع على محتوى الرسالة. وبذلك يسهم التشفير في إرساء الضمانات القانونية التي تكفل موثوقية المعاملات الإلكترونية وتحمي أطرافها من مخاطر التلاعب أو الاختراق (التميمي، ٢٠١٠، صفحة ٦٦٩).

ثانياً: الجهات المختصة بضمان أمن البيانات:

يلزم من الجهات المعنية بالترخيص إيجاد ضمانات كفيلة بإرساء الأمان القانوني ووضع الثقة لدى المستفيد وهذا ما يتم توضيحه من خلال:

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

١_ الحصول على الترخيص بالاستعمال، أشار المشرع العراقي في المادة(٦) من نظام الدفع الالكتروني للأموال رقم (٢) لسنة ٢٠٢٤ والمتضمنة في الفقرة اولاً بأن ((لا يجوز تقديم خدمات الدفع الالكتروني الا بعد ترخيص من البنك المركزي)).

اما بحسب ماجاء في الفقرة ثانياً والمتضمنة ((على الشخص المعنوي الراغب بالحصول على الترخيص للعمل كمزود خدمة الدفع الالكتروني ويمتلك المؤهلات المطلوبة المحددة من البنك المركزي تقديم طلب الى البنك المركزي اصوليا.))، ويلاحظ ان هذه العملية تتم من خلال طلب الترخيص من الجهات المصدرة لوسائل الدفع الالكتروني، على أساس ان عمليات الدفع هذه تتم على شبكة الانترنت من قبل مزود الخدمة الالكترونية من جهة والمستفيد من جهة أخرى، والسماح له بإجراء الصفقات بواسطة هذه الوسائل، اما في حال يصعب الحصول على مثل هذا الترخيص في إثناء إجراء الصفقات وذلك لتلافي إعادة استخدام النقود مرات متعددة، حيث تقوم السلطة المركزية المصدرة بالترخيص الإجراء الصفقات على أساس المعلومات والوحدات المصدرة مسبقا (حوالف، ٢٠١٤، صفحة ٤٥٠) .

٢_ الحصول شهادة التوثيق الالكتروني (حوالف، ٢٠١٤، صفحة ٤٩) تعد جهة التوثيق الالكتروني، أو مقدم خدمات التوثيق، أو منظمة عامة، أو خاصة محايدة، أذ عرفها المشرع العراقي في المادة (١/حادي عشر) من قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢ على أنه ((شهادة التصديق بأنها الوثيقة التي تصدرها جهة التصديق وفق احكام هذا القانون والتي تستخدم لإثبات نسبة التوقيع الالكتروني الى الموقع))، اذ تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الالكترونية بإصدار شهادات الالكترونية، ويطلق على الذي يتولى عملية التصديق مقدم خدمات التصديق، ويتم تدخل الموثق الالكتروني بناء على طلب شخصين، أو أكثر، بهدف انشاء وحفظ واثبات الرسائل الالكترونية (حوالف، ٢٠١٤، صفحة ١٧٢) .

الفرع الثاني: الاجراءات الإدارية في مكافحة المخاطر الأمنية

ينبغي ان يكون هنا إجراءات خاصة لمكافحة المخاطر التي تخترق عمل الدفع الالكتروني، وذلك بوضع تدابير امنية لمنع حدوث أعمال احتيالية تخرق عمل أنظمة الدفع الالكتروني، ومن هذه الإجراءات:

اولاً: تحديد سقف لعمليات سحب البطاقة :

الأصل ان يتم تحديد سقف للبطاقة بحيث لا يمكن تجاوزه، واستثناء قد يسمح بذلك في حالات معينة والهدف من ذلك منع إفراط صاحب البطاقة خوفا من عدم إيفاءه بمصاريف المشتريات المترتبة عليه بتاريخ تسويتها المتفق عليه من البنك، وكذلك خوف من وقوعها في يد الغير ووفقا لذلك، وجب تحديد سقف لاستخدام البطاقة حيث يكون هذا التحديد سواء عند استخدامها في عمليات السحب أو الوفاء على حد سواء (بوقديرة، ٢٠١٧، صفحة ٤٩) .

مجلة دجلة للعلوم الإنسانية • المجلد ١ ،العدد ٢ (أيلول ٢٠٢٥)، ص: ٤٥٩ - ٤٨١
E- ISSN: 3079-7861 • P- ISSN: 3079-7853

وتعد البطاقة ملك لمصدرها، ومن اجل ان يحافظ المصدر على حقوقه ولضمان عدم استخدام البطاقة بطرق غير مشروعه، اذ يتمكن المصدر من إلغائها وسحب البطاقة.

ثانياً: تسجيل وسائل الدفع:

تسعى المؤسسات المصدرة لوسائل الدفع الإلكتروني إلى تسجيل البيانات الشخصية الأساسية لحاملي هذه الوسائل، كالعنوان والهوية، سواء لديها أو لدى جهة مركزية مختصة، وذلك بهدف تسهيل التحقيق في حال وقوع أنشطة احتيالية. كما تُلزم أنظمة الدفع بربط المستهلكين والتجار بحسابات مصرفية للتحقق من المعلومات المسجلة. وفي أنظمة البرمجيات، يتعين على المستخدم توثيق هويته لإتمام المعاملات الضرورية. ومن جانب آخر، يعد تسجيل الجهاز الخاص بالتاجر خطوة مهمة لما يحتويه من أرصدة أكبر من وسيلة المستفيد، مما يجعل مراقبته والتحكم في الدخول إليه ضرورة أمنية أساسية (حمزة، ٢٠١١، صفحة ٤٤١).

ثالثاً: ضبط حدود الأرصدة المخزنة في وسائل الدفع وأبعادها الزمنية:

تبذل المؤسسات المعنية بوسائل الدفع الإلكتروني جهوداً متواصلة لتعزيز مستويات الحماية والأمان في عمليات الدفع، وذلك من خلال اعتماد آليات دقيقة تحد من المخاطر المحتملة. وفي هذا السياق، تعمل هذه المؤسسات على فرض قيود محددة تتعلق بالقيم المالية التي يمكن تخزينها في وسيلة الدفع سواء كانت بحوزة المستهلك أو التاجر، فضلاً عن تحديد سقف أقصى للاستخدام عند إتمام عمليات الوفاء بواسطة البطاقة. وتجدر الإشارة إلى ضرورة التمييز بين الاستخدامات المختلفة للبطاقة، سواء عبر أجهزة الطباعة اليدوية أو من خلال أجهزة نقاط البيع الإلكترونية (POS)، نظراً لما يترتب على ذلك من آثار أمنية مختلفة.

وتكتسب هذه التدابير أهمية خاصة في البنية الأمنية لأنظمة الدفع الإلكتروني، إذ إن الغاية الأساسية منها هي الحد من حجم الخسائر الناجمة عن أي عملية احتيال ناجحة. كما تسهم بصورة غير مباشرة في تقليص دوافع الاحتيال، من خلال خفض المكاسب المالية المحتملة للمحتالين، بحيث يصبح تنفيذ عمليات غير مشروعة أكثر صعوبة وأقل جدوى (الجهني ا.، ٢٠١٠، صفحة ١١٥) .

الخاتمة

لقد تناولت هذه الدراسة موضوع حماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني – دراسة مقارنة، وهو مجال حديث ناشئ عن التطور الرقمي واعتماد الأفراد والمؤسسات على وسائل الدفع الإلكترونية، وقد أظهرت الدراسة مجموعة من التحديات القانونية المرتبطة بحماية المستفيد، بدءاً من تحديد مسؤولية مزوّد الخدمة وصولاً إلى آليات الإثبات وسبل الانتصاف، ووفقا لذلك فقد توصلنا الى عدة من النتائج والتوصيات وفق الاتي:

اولاً: النتائج:

١ _ قصور الحماية التشريعية في بعض الأنظمة القانونية أذ أظهرت الدراسة أنّ التشريعات في بعض الدول لا تزال غير كافية لمواجهة الجرائم والمخاطر المتصلة بالدفع الإلكتروني، سواء لحداثة هذه الوسائل أو لتطور الأساليب الاحتيالية بشكل أسرع من القوانين.

٢_ إن المستفيد يُعد الطرف الأضعف في علاقة الدفع الإلكتروني، مما يتطلب تكريس حماية قانونية خاصة له.

٣_ تعدد مصادر المخاطر أذ يتبين أنّ المخاطر لا تقتصر على الاختراقات التقنية أو الاحتيال الإلكتروني، بل تشمل أيضاً سوء استخدام الموظفين داخل المؤسسات المالية، وضعف وعي المستفيدين بطرق الحماية.

٤_تعدد المخاطر التي تهدد المستفيد، وتشمل: الاختراقات الأمنية، سرقة الهوية، الاحتيال المالي، فشل الأنظمة التقنية، وسوء استخدام بياناته الشخصية.

٣_ اختلاف مستوى الحماية بين التشريعات المقارنة أذ يلاحظ بعض الدول قد اعتمدت أنظمة حماية متقدمة كالتشفير الإلزامي، ووضع حدود للمبالغ، وإجراءات التحقق المزدوج، بينما ما زالت دول أخرى تفتقر إلى هذه الضمانات.

٤_ محدودية فعالية الحماية التقنية وحدها بالرغم من أهميتها، فإن الإجراءات التقنية (مثل التشفير أو المصادقة الثنائية) لا تكفي دون وجود إطار قانوني ملزم يحدد المسؤولية ويوفر للمستفيد وسائل الانتصاف عند وقوع الضرر.

٥_ غياب الوعي القانوني لدى المستفيد من خلال الدراسة والزيارات الميدانية اذ يلاحظ أنّ الكثير من المستفيدين لا يعرفون حقوقهم أو وسائل الحماية المتاحة لهم عند وقوع اعتداءات إلكترونية، مما يضعف من فعالية الضمانات الموضوعة.

٦_ لا تزال بعض التشريعات المحلية عاجزة عن مواكبة التطور السريع في وسائل الدفع الإلكتروني، مما يُضعف من فعالية الحماية القانونية المتاحة للمستفيد.

٧_ تُعد المعايير التقنية (مثل التشفير والتحقق الثنائي) أداة مهمة في حماية المستفيد، لكنها لا تُغني عن ضرورة وجود تشريع واضح وصارم يحدّد المسؤوليات ويضمن الحقوق.

٨_ نلاحظ وجود تفاوت كبير في النظم القانونية في تحديد طبيعة العلاقة بين المستفيد ومزود خدمة الدفع، وهو ما يؤثر على طرق الرجوع والتعويض عند وقوع الضرر.

ثانياً: التوصيات

١_ تطوير التشريعات الوطنية من خلال سن أو تعديل القوانين الوطنية بما يتلاءم مع المستجدات التقنية، خصوصاً في مجال تحديد المسؤولية المدنية والجنائية لمزودي خدمات الدفع الإلكتروني.

٢_ تعزيز التعاون الدولي لأن الجرائم الإلكترونية عابرة للحدود، توصي الدراسة بتبني اتفاقيات ثنائية وإقليمية ودولية لتبادل المعلومات وتوحيد آليات الملاحقة القانونية.

٣_ إلزام المؤسسات المالية بوسائل حماية متقدمة من خلال فرض استخدام التشفير القوي، وآليات المصادقة متعددة العوامل، وتحديث الأنظمة بشكل دوري لمواجهة الاختراقات.

٤_ توصي الدراسة بإنشاء هيئات متخصصة لمتابعة التزام البنوك وشركات الدفع بمعايير الأمان، وفرض جزاءات عند الإخلال به. من خلال تفعيل دور الرقابة والإشراف

٥_ التوسع في نشر الثقافة القانونية والتقنية للمستفيدين عبر حملات توعية رسمية ومؤسساتية لتوضيح حقوق المستهلك، وطرق حماية بياناته، وكيفية تقديم الشكاوى عند وقوع اعتداءات.

٦_ تعزيز وسائل الانتصاف للمستفيد من خلال إنشاء آليات سريعة للتقاضي أو لجان تسوية منازعات متخصصة في الجرائم والمشكلات الناشئة عن الدفع الإلكتروني، بما يضمن إعادة الحقوق بأسرع وقت ممكن.

٧_تعزيز دور الهيئات الرقابية في مراقبة مقدمي خدمات للدفع وضـــمان امتثالهم لمعايير الأمن والشفافية.

٨_فرض التزامات واضحة على مزودي خدمات الدفع بشأن حماية بيانات المستفيد، مع تقنين العقوبات في حال الإخلال.

٩_نشر التوعية القانونية والتقنية بين المستفيدين حول كيفية الاستخدام الآمن لخدمات الدفع الإلكتروني.

قائمة المصادر او المراجع:

أولاً: المراجع العربية

الكتب:

١. أمجد حمدان الجهني. (٢٠١٠). المسؤولية المدنية عن الاستخدام غير المشروع للبطاقات الدفع الإلكتروني (ط. ١). عمان: دار المسيرة للنشر والتوزيع.

٢. أسامة حمدان الرقب. (٢٠١١). جرائم النصب والاحتيال: الأساليب والمظاهر. عمان – الأردن: دار يافا العلمية للنشر والتوزيع.

٣. إيهاب فوزي السقا. (٢٠٠٧). الحماية الجنائية والأمنية لبطاقات الائتمان. مصر: دار الجامعة الجديدة.

٤. جميل عبد الباقي الصغير. (١٩٩٨). الحماية الجنائية المدنية لبطاقات الائتمان الممغنطة. القاهرة: دار النهضة العربية.

٥. حسام طاهر داود. (د.ت). الحاسب وآمن المعلومات. الرياض: مكتبة الملك فهد، معهد الإدارة العامة.

٦. علاء التميمي. (٢٠١٠). التنظيم القانوني للبنك الالكتروني على شبكة الانترنت. الإسكندرية: دار الجامعة الجديدة.

٧. عبد الفتاح بيومي حجازي. (٢٠٠٤). التجارة الإلكترونية وحمايتها القانونية (الكتاب الأول). مصر: دار الفكر الجامعي.

٨. عبد الفتاح بيومي حجازي. (٢٠٠٥). التوقيع الإلكتروني في النظم القانونية المقارنة (ط. ١). مصر: دار الفكر الجامعي.

٩. طارق محمد حمزة. (٢٠١١). النقود الإلكترونية كإحدى وسائل الدفع: تنظيمها القانوني والمسائل الناشئة عن استعمالها (ط. ١). بيروت – لبنان: منشورات زين الحقوقية.

١٠. نادر عبد العزيز شافي. (٢٠٠٧). المصارف والنقود الإلكترونية. طرابلس – لبنان: المؤسسة الحديثة للكتاب.

١١. وائل الدبيسي. (٢٠٠٩). دليل العمليات الإلكترونية في القطاع المصرفي: الواقع والآثار القانونية. بيروت – لبنان: اتحاد المصارف العربية.

١٢. محمد طارق عبد الرؤوف. (٢٠١١). جريمة الاحتيال عبر الإنترنت: الأحكام الموضوعية والأحكام الجنائية (ط. ١). بيروت: منشورات الحلبي.

المقالات والدوريات:

١. أمجد حمدان الجهني. (٢٠٠٨). جرائم بطاقات الدفع الالكتروني. بحث مقدم لمؤتمر المعاملات الالكترونية التجارة الالكترونية – الحكومة الالكترونية، مركز الإمارات والدراسات الإستراتيجية، جامعة الإمارات، ٧٧٦. الامارات: عبر شبكة الانترنت.
٢. عبد الله خيري أحمد. (٢٠٢٤). اختراق خصوصية الآخرين عبر منصات التواصل الاجتماعي في الفقه الإسلامي. مجلة البحوث القانونية والاقتصادية، ٦٠(٣).
٣. عبد الجبار الحنيص. (٢٠١٠). الاستخدام غير المشروع لبطاقات الائتمان الممغنطة من وجهة نظر القانون الجزائي. مجلة دمشق للعلوم الاقتصادية والقانونية، ٢٦(١).
٤. جليل الساعدي. (٢٠٠٧). تنازع القوانين في التعاقد عبر شبكة الإنترنت. مجلة العلوم القانونية، (١).
٥. بن تركي ليلى. (د.ت). الحماية الجنائية للبطاقات الممغنطة. مجلة العلوم الإنسانية، ٤٦(أ).

الرسائل الجامعية:

١. خولة بوقدور. (٢٠١٨/٢٠١٧). الجرائم الواقعة على بطاقة الدفع الإلكتروني (رسالة ماجستير). جامعة العربي بن مهيدي.
٢. سماح شعبور، & مصباح مرابطي. (٢٠١٦/٢٠١٥). وسائل الدفع الإلكتروني في الجزائر: واقع وتحديات (رسالة ماجستير). جامعة العربي تبسي.
٣. مونية معروف. (٢٠١٥/٢٠١٤). جرائم بطاقة الائتمان الإلكترونية (رسالة ماجستير). جامعة العربي بن مهيدي.
٤. واقد يوسف. (٢٠١١). النظام القانوني للدفع الإلكتروني (رسالة ماجستير). جامعة معمري.
٥. حوالف عبد الصمد. (د.ت). النظام القانوني لوسائل الدفع الإلكتروني (أطروحة دكتوراه). جامعة أبو بكر بلقايد.

التشريعات والقوانين:

١. جمهورية مصر العربية. (٢٠٠٨). قانون الجرائم الاقتصادية رقم (١٢٠) لسنة ٢٠٠٨.
٢. جمهورية مصر العربية. (٢٠١٨). قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨.
٣. جمهورية مصر العربية. (٢٠١٩). قانون تنظيم استخدام وسائل الدفع غير النقدي رقم (١٨) لسنة ٢٠١٩.
٤. جمهورية العراق. (٢٠١٢). قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (٧٨) لسنة ٢٠١٢.
٥. جمهورية العراق. (٢٠١٥). قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (٣٩) لسنة ٢٠١٥.
٦. جمهورية العراق. (٢٠٢٤). قانون خدمات الدفع الإلكتروني للأموال رقم (٢) لسنة ٢٠٢٤.
٧. دولة الإمارات العربية المتحدة. (١٩٨٧). القانون الاتحادي رقم (٣) لسنة ١٩٨٧ (قانون العقوبات).
٨. دولة الإمارات العربية المتحدة. (٢٠٢١). مرسوم القانون الاتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الجرائم الإلكترونية.
٩. فرنسا. (١٩٩٢). قانون العقوبات (Code pénal).
١٠. فرنسا. (٢٠٠٠). قانون النقد والمال.

المصادر الإلكترونية:

١. MasterCard. 27(د.ت). أمان بطاقات الدفع الإلكتروني MasterCard SecureCode. تاريخ الاسترداد: ١٧ مايو ٢٠٢٥ من:
٢. http://www.mastercard.com/eg/ar/consumer/securecode-faq.html

ثانياً: المراجع الأجنبية

1. Stephen Mason. (n.d.). Op. cit.